St. Pölten University of Applied Sciences

/informatik & security

/fh/// st. pölten

Open Source Intelligence (OSINT)

Evaluieren und Vergleichen von Tools

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Dominik Burak
is181806

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Mag. Dr. Simon Tjoa

St. Pölten, 05.06.2020

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

St. Pölten, 05.06.2020

(Unterschrift Autor/Autorin)

Danksagung

Ich bedanke mich ganz herzlich bei meinem Betreuer Herrn FH-Prof. Dr. Simon Tjoa. Er hat mich bei Fragen zur Arbeit tatkräftig unterstützt und war auch in dringenden Fällen immer zur Stelle. Ohne diese Unterstützung hätte diese Arbeit nie die jetzige Detailtiefe erhalten.

Ein weiterer Dank gilt meinen Studienkollegen Herrn Marcus Szing, BSc sowie Herrn Thomas Pointner, BSc für die gute Zusammenarbeit in dem gesamten Studium.

Ein großer Dank gilt meiner Familie und meiner Freundin, welche mich die gesamte Zeit unterstützt haben.

Zusammenfassung

Diese Arbeit beschäftigt sich mit der Gegenüberstellung von verschiedenen OSINT-Tools, welche für die Informationsbeschaffung eines Ziels, wie beispielsweise ein Unternehmen oder eine Person eingesetzt werden können. Die Informationen können von Suchmaschinen oder Foren gesammelt und anschließend in Beziehung gestellt werden. Aufgrund der zahlreichen Tools für die Informationsbeschaffung, wurde die Auswahl an Tools für diese Arbeit beschränkt. Entscheidend war, dass nur Tools verglichen werden, welche auf der virtuellen Maschine „Kali-Linux“ sowie „Buscador2“ vorhanden sind. Um die Tools anhand ihrer Eigenschaften und Funktionen miteinander vergleichen zu können, wurden zuerst einige Kriterien definiert. Diese Kriterien wurden anschließend dazu verwendet, um eine Gegenüberstellung und einen Vergleich der Tools durchführen zu können. Der Fokus der Scans lag auf der Domain fhstp.ac.at und der Twitter Seite der Fachhochschule St. Pölten, sowie auf den selbst erstellten, Fake Social Media Profilen. Durch die passiven OSINT-Scans wird gezeigt, welche Informationen mit den jeweiligen Tools über ein Ziel gefunden werden können. Für das Sammeln der Informationen wurden ausschließlich passive Scans verwendet.

Ein Ziel dieser Arbeit ist es, die ausgewählten OSINT-Tools zu analysieren, sowie zu überprüfen, welche öffentlich, frei zugänglichen Informationen damit gesammelt werden können. Im Anschluss daran wird gezeigt, welche Angriffe auf Basis der gesammelten Informationen möglich sind. Ein weiteres Ziel ist eine Matrix bereitzustellen, in der die ausgewählten Tools gelistet und anhand der zuvor definierten Kriterien überprüft werden. Die Matrix soll bei der Auswahl eines Tools unterstützen indem verschiedene Funktionen und Eigenschaften, sowie eine Auflistung der sammelbaren Informationen dargestellt werden. Zu diesen Informationen gehören beispielsweise „Namen von Personen“, „E-Mail-Adressen“ oder „IP-Adressen“, die mit den jeweiligen Tools gefunden werden konnten. Neben der Analyse zur Sammlung von Informationen über Unternehmen wurden auch Social Media Plattformen mit einigen dieser ausgewählten Tools untersucht. Dabei wurde analysiert, inwieweit die Tools in der Lage sind durch passive Scans der Domain und öffentlichen Informationen, auf Social Media Plattformen Informationen zu Personen, sowie dessen geteilten Kommentaren zu sammeln.

Abstract

This paper focuses on the comparison of different OSINT tools, which can be used to gather information about a target, such as a company or a person. The information can be collected by search engines or forums and put into relation afterwards. Because of the numerous tools for information gathering, the variety of tools for this work has been limited. It was essential to compare only tools which are available on the virtual machine "Kali-Linux" and "Buscador2". To compare the tools based on their properties and functions, several criteria were first defined. These criteria were used to compare and contrast the tools. The focus of the scans was on the domain fhstp.ac.at and the Twitter page of the University of Applied Sciences St. Pölten, as well as on the self-created, fake social media profiles. The passive OSINT scans show which information can be found about a target with the tools. Only passive scans were used to collect the information.

One aim of this thesis is to analyse the selected OSINT tools and to check which public, free-access information can be collected with them. Afterwards it is shown which attacks are possible on the basis of the collected information. Another goal is to offer a matrix in which selected tools are listed and checked against the previously defined criteria. The matrix should support the selection of a tool by listing different functions and properties as well as a list of the collectable information. This information includes, for example, "names of persons", "e-mail addresses" or "IP addresses" that could be found with the tools. The matrix is designed to help select a tool by listing various functions and properties and listing the information that can be gathered. In addition to the analysis for the collection of information about companies, also social media platforms were analysed with some of these selected tools. It was analysed how tools are able to collect information about persons and their shared comments by passive scans of the domain and public information on social media platforms.

Inhaltsverzeichnis

Ehrenwörtliche Erklärung 2
Danksagung 3
Zusammenfassung 4
Abstract 5
Abbildungsverzeichnis 8
Tabellenverzeichnis 10

1. EINLEITUNG 11

1.1. Problemstellung 14
1.2. Motivation 16
1.3. Forschungsfragen 17
1.4. Methodik 17
1.5. Aufbau der Arbeit 18

2. BACKGROUND 20

3. RELATED WORK 25

4. ENTWICKLUNG VON OPEN SOURCE INFORMATIONEN IM ALLGEMEINEN 28

4.1. Open Source Intelligence 28
4.2. Open Source Intelligence Cycle 29
4.3. OSINT und Threat Intelligence 32
4.4. Cyber Kill Chain 35
4.5. Reconnaissance Phase 37
4.6. Vorteile/Nachteile von OSINT 39
4.7. Einsatzgebiete 40
4.8. Intelligence Collections und Angriffsarten 41
4.9. Marketing Intelligence 49

5. TESTUMGEBUNG UND BESCHREIBUNG DER KRITERIEN 50

5.1. Ausgangslage 50
5.2. Aufbau der Testumgebung und ihre Eigenschaften 51
5.2.1. Kali-Linux Testumgebung 51
5.2.2. Buscador2 Testumgebung (VMWare OVA) 51
5.3. Kriterien 52
5.3.1. Plattformen 52
5.3.2. GUI /CLI (Graphical User Interface/Command Line Interface) 52
5.3.3. Import-Format 53
5.3.4. Export-Format 53
5.3.5. Updates 53
5.3.6. Such- und Filtermöglichkeiten 53
5.3.7. Kosten 53
5.3.8. Informationen 54
5.3.9. Korrektheit der Daten 54
5.3.10. Berichtsverwaltung 54
5.3.11. Darstellungsfunktion 54
5.3.12. Rückverfolgbarkeit (von Personen/Unternehmen) 54
5.3.13. Attacken 55

6. EVALUIERUNG VON DEN TOOLS 56

6.1. Maltego 57

6.1.1. Beschreibung ... 57
6.1.2. Allgemein ... 57
6.1.3. Kriterien Beschreibung ... 58
6.1.4. Praktischer Test ... 60
6.1.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests ... 63
6.1.6. Ergebnisse und Fazit ... 64
6.2. THEHARVESTER ... 65
6.2.1. Beschreibung ... 65
6.2.2. Allgemein ... 65
6.2.3. Kriterien-Beschreibung ... 65
6.2.4. Praktischer Test ... 67
6.2.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests ... 69
6.2.6. Ergebnisse und Fazit ... 70
RECON-NG ... 70
6.3.1. Beschreibung ... 70
6.3.2. Allgemein ... 70
6.3.3. Kriterien-Beschreibung ... 70
6.3.4. Praktischer Test ... 72
6.3.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests ... 74
6.3.6. Ergebnisse und Fazit ... 74
6.4. SPIDERFOOT ... 78
6.4.1. Beschreibung ... 78
6.4.2. Allgemein ... 78
6.4.3. Kriterien-Beschreibung ... 81
6.4.4. Praktischer Test ... 83
6.4.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests ... 86
6.4.6. Ergebnisse und Fazit ... 86
6.5. TINFOLEAK ... 91
6.5.1. Beschreibung ... 91
6.5.2. Allgemein ... 91
6.5.3. Kriterien-Beschreibung ... 91
6.5.4. Praktischer Test ... 93
6.5.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests ... 99
6.5.6. Ergebnisse und Fazit ... 99
6.6. TWITTER-SCRIPT/TWITTER-EXPORTER ... 99
6.6.1. Beschreibung ... 99
6.6.2. Allgemein ... 99
6.6.3. Kriterien-Beschreibung ... 99
6.6.4. Praktischer Test ... 101
6.6.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests ... 103
6.6.6. Ergebnisse und Fazit ... 103

7. OSINT USE CASE ... 104

8. AUSWERTUNG & INTERPRETATION DER ERGEBNISSE ... 123

9. BEANTWORTUNG DER FORSCHUNGSFRAGEN ... 133

10. CONCLUSION ... 136

LITERATURVERZEICHNIS ... 137

Abbildungsverzeichnis

Abbildung 1 Intelligence Cycle 30
Abbildung 2 Cyber Kill Chain 35
Abbildung 3 Twitter Protect your Tweets 56
Abbildung 4 Maltego Twitter Scan 60
Abbildung 5 Maltego Twitter Scan 2 61
Abbildung 6 Maltego Big Picture 61
Abbildung 7 Maltego Big Picture Legende 61
Abbildung 8 Maltego DNS Scan 62
Abbildung 9 Maltego Personen/E-Mail-Adresse Scan 63
Abbildung 10 TheHarvester Dashboard 68
Abbildung 11 TheHarvester E-Mail Scan 68
Abbildung 12 TheHarvester Host Scan 69
Abbildung 13 TheHarvester Scanergebnis Auszug 69
Abbildung 14 Recon-NG Brute Hosts Einstellungen 73
Abbildung 15 Recon-NG Results Summary 73
Abbildung 16 Recon-NG Show Workspaces 74
Abbildung 17 Recon-NG Show Contacts 75
Abbildung 18 Recon-NG Hosts/IP-Adressen Auszug 75
Abbildung 19 Recon-NG Activity Summary 76
Abbildung 20 Spiderfoot Scans Übersicht 78
Abbildung 21 Spiderfoot New Scans 79
Abbildung 22 Spiderfoot New Scan By Required Data 80
Abbildung 23 Spiderfoot New Scan By Module 80
Abbildung 24 Spiderfoot Graph 81
Abbildung 25 Spiderfoot fertiger Scan Karub Kinimod 83
Abbildung 26 Spiderfoot Kinimod Karub Account on External Site 84
Abbildung 27 Kinimod Karub Instagram Account 84
Abbildung 28 Kinimod Karub Reddit Account 84
Abbildung 29 Spiderfoot Kinimod Karub Scan Ergebnis 85
Abbildung 30 Spiderfoot Twitter Kinimod Karub 85
Abbildung 31 Spiderfoot Gesamtscan-Übersicht 86
Abbildung 32 Spiderfoot Scans Kinimod Karub vs. Karub Kinimod 87
Abbildung 33 Spiderfoot Scan Karub Kinimod 87
Abbildung 34 Spiderfoot Scan Kinimod Karub 87
Abbildung 35 Spiderfoot False Positive Flag 88
Abbildung 36 Spiderfoot Gesamtergebnis 1 88
Abbildung 37 Spiderfoot Gesamtergebnis 2 89
Abbildung 38 Spiderfoot Gesamtergebnis 3 89
Abbildung 39 Spiderfoot offene Ports 89
Abbildung 40 Tinfoleak starten 93
Abbildung 41 Tinfoleak Tool Dashboard 94
Abbildung 42 Tinfoleak Webbrowser 94
Abbildung 43 Twitter FH Username 95
Abbildung 44 Tinfoleak Webbrowser-Scanergebnis 96
Abbildung 45 Tinfoleak Tool-Scanergebnis 97
Abbildung 46 Tinfoleak Client Applications 1 98
Abbildung 47 Tinfoleak Client Application 2 98
Abbildung 48 Tinfoleak Top Hashtags 98
Abbildung 49 Twitter-Script starten 101

Abbildung 50 Twitter-Script Twittername-Eingabe 101
Abbildung 51 Twitter-Script Tweets sammeln 102
Abbildung 52 Twitter-Script Photos sammeln 102
Abbildung 53 Twitter-Script erstellter Ordner mit Dateien 103
Abbildung 54 MISP Feeds 109
Abbildung 55 MISP Events 109
Abbildung 56 MISP Edit Event 109
Abbildung 57 MISP Threat Level Einstellungen 110
Abbildung 58 MISP Dashboard 110
Abbildung 59 MISP Edit Sharing Group 111
Abbildung 60 MISP Sharing Group 111
Abbildung 61 MISP Add Server 112
Abbildung 62 MISP Server 112
Abbildung 63 MISP Event mit Kunden teilen 113
Abbildung 64 TheHarvester gefundene Hosts mit IP 117
Abbildung 65 Shodan Portscan Ergebnis 118
Abbildung 66 TheHarvester Scanergebnis ohne Versionsnummer 118
Abbildung 67 Recon-NG Scanergebnis von Hosts und IP ohne Versionsnummern 118

Tabellenverzeichnis

Tabelle 1 Beschreibungssprache TIP 23
Tabelle 2 Institute TIP 24
Tabelle 3 OSINT Informationen 32
Tabelle 4 TI-Plattformen 34
Tabelle 5 Vorteile und Nachteile von OSINT 40
Tabelle 6 Angriffsarten 48
Tabelle 7 Informationen bei Angriffen auf Organisation vs. Personen 49
Tabelle 8 Erstellte Fake-E-Mail Adressen 63
Tabelle 9 Spiderfoot Kosten 82
Tabelle 10 Welche Informationen können mit dem Tool gesammelt werden 104
Tabelle 11 Ergebnisse der Tool-Evaluierung 1 126
Tabelle 12 Ergebnisse der Tool-Evaluierung 2 127
Tabelle 13 Ergebnisse der Tool-Evaluierung 3 128
Tabelle 14 Ergebnisse der Tool-Evaluierung 4 129
Tabelle 15 Ergebnisse der Tool-Evaluierung 5 130

1. Einleitung

Die Anzahl der Daten und Informationen, welche im Internet frei verfügbar sind, werden stetig mehr. Ein Grund an den zunehmenden Daten liegt darin, dass Unternehmen vermehrt das Internet nutzen, um ihre Produkte und Services im Internet anzubieten. Damit Mitarbeiter/Innen auf diese Services auch aus der Ferne zugreifen können, werden von Unternehmen oft Virtual Private Network (VPN) eingesetzt, damit wird das Arbeiten von Zuhause ermöglicht. Dadurch können Angreifer/Angreiferinnen diese starke Vernetzung und Abhängigkeit an das Internet für Angriffe verwenden.
Ein beliebtes Ziel für Angriffe sind KMUs (kleine und mittelständische Unternehmen), da in diesen Unternehmen weniger Personen, Ressourcen oder Kompetenzen vorhanden sind und daher weniger in die Sicherheit von Services investiert werden kann. [1] Ebenso steigt die Anzahl an Daten durch Internet of Things (IoT) und die verschiedenen Smart-Devices, welche Informationen jeglicher Art erzeugen wie Gesundheitsdaten oder Geolocations. [2] [3]

Da von Organisationen immer mehr Services und IT-Systeme durch das Internet zugänglich gemacht werden, müssen diese einem besonderen Schutz unterliegen. Jegliche Arten von Schwachstellen wie beispielsweise Fehlkonfigurationen oder Zero-Day-Exploits kann ein/e Angreifer/in verwenden, um ein Ziel anzugreifen, diese Informationen können durch die Reconnaissance-Phase gesammelt werden. In dieser Phase wird Information-Gathering durchgeführt, um verschiedene öffentlich frei zugängliche Daten und Informationen über ein Ziel zu sammeln und zu speichern.

Unternehmen können ebenso von OSINT (Open Source Intelligence) profitieren, indem sie kontrollieren, welche Informationen und Daten im Internet zugänglich sind. Dies kann einem Unternehmen zeigen, ob kritische Informationen im Internet ersichtlich sind. Da durch die Verwendung von OSINT ermöglicht wird Schwachstellen, welche nach außen sichtbar sind, zu erkennen und diese zu beheben, spielt dieses Thema eine große Rolle. [4] Bei diesen Informationen und Daten handelt es sich meist um firmeninterne Daten oder personenbezogene Daten, welche nicht für die Öffentlichkeit verfügbar sein sollten. [5] Dadurch, dass Unternehmen OSINT-Tools verwenden können, kann gesehen werden, welche Informationen ein/e Angreifer/Angreiferin sammeln kann. Ein Unternehmen kann somit OSINT verwenden, um präventive Maßnahmen basierend auf die gefundenen Informationen für den Schutz der Infrastruktur zu setzen.

Es gibt bei dieser Phase zwei verschiedene Arten von Scans, “Aktive-Scans” und “Passive-Scans”, diese werden später in der Arbeit genauer beschrieben. Diese Arbeit konzentriert sich auf die “Passive-Scans”, welche durch OSINT ermöglicht wird. Bei einem aktiven Scan, wie beispielsweise einem Port-Scan wird eine Beziehung zu dem Ziel hergestellt, dies geschieht bei einem passiven Scan nicht, hier werden verschiedene Informationen gesammelt, ohne mit dem Ziel direkt zu kommunizieren.

OSINT ist auch im Bereich von Social Media Plattformen sehr wichtig. Social Media Plattformen haben grundsätzlich die Idee, dass sich Menschen schnell untereinander austauschen können. Dabei werden oft auch sehr sensible Informationen und Interessen über Personen oder Unternehmen preisgegeben und veröffentlicht. Durch falsche Privatsphären-Einstellungen besteht die Möglichkeit, dass diese Informationen nicht nur zwischen vertrauenswürdigen Personen verfügbar sind. Solche sensiblen Informationen können von Angreifern verwendet werden, um Personen zu überwachen und Informationen zu sammeln. Es können beispielsweise Name, Geburtsdatum, Wohnadresse, E-Mail-Adresse und Vorlieben gesammelt werden. Facebook hat im Jahre 2010 die Default-Einstellungen so

eingestellt, dass alle hochgeladenen und geposteten Berichte und Bilder für alle User verfügbar waren, somit waren alle sensiblen Informationen sichtbar. [6]
Ebenso kann OSINT von Einbrechern verwendet werde, was ein Bericht von Jahre 2010 belegt. [7] Hier wurden mehrere Personen über Facebook von Einbrechern ausspioniert. Als die Personen auf der Plattform den Urlaub angekündigt haben, haben die Einbrecher leichtes Spiel gehabt und sind in die Wohnungen und Häuser eingebrochen. Auch von Anwälten werden vermehrt Social Media Plattformen überprüft, um mehr Informationen über die andere Person zu finden. [8]

Wie oben beschrieben, kann Information Gathering von jeder Person durchgeführt werden und beispielsweise für Cyber-Angriffe verwendet werden, indem alle wichtigen und relevanten Informationen über ein Ziel gesammelt werden. Die gesammelten Informationen können anschließend für die Durchführung von Cyber-Angriffen verwendet werden. Eine detaillierte Übersicht von verschiedenen Informationen, welche gesammelt werden können, ist in Kapitel 8 „*Auswertung & Interpretation der Ergebnisse*“ gegeben. Um eine Übersicht verschiedener Tools zu bekommen, kann die Internetseite “OSINT Framework” [9] verwendet werden. Auf dieser Seite sind verschiedene Frameworks für das Sammeln von Informationen hinterlegt. Die heutzutage am Markt verfügbaren und angebotenen Tools für die verschiedenen Einsatzgebiete sind vielfältig und können unterschiedliche Eigenschaften und Funktionsweisen aufweisen, da mit jedem Tool reichliche Informationen gesammelt werden können.

Ein wichtiges Gebiet stellt das OSINT-Verfahren dar, indem nach bestimmten Begriffen gesucht und diese daraus resultierenden Informationen gesammelt werden. OSINT bedient sich dabei an frei zugänglichen Informationen, welche beispielsweise frei und öffentlich im Internet zu finden sind. Ein praktisches Beispiel aus dem Alltag ist, dass ein/e Personalchef/in vor Bewerbungsgesprächen, im Internet nach öffentlichen Daten von einem Bewerber oder einer Bewerberin sucht. [10]

Mittlerweile haben sich verschiedenste Tools und Methoden entwickelt, um OSINT Informationen zu generieren oder bereits bestehende OSINT Informationen zu empfangen.
Bei der Generierung von OSINT Informationen können Tools, wie beispielsweise “Maltego” oder “Recon-NG” verwendet werden, um nach öffentlichen und frei zugänglichen Informationen aus unterschiedlichen Social Media Plattformen oder dem Internet, zu suchen. Es können auch Tools wie “Shodan” und “Censys” verwendet werden, dadurch ist es möglich, fehlerhafte Netzwerkeinstellungen zu erkennen. Einige Tools können gleichzeitig Informationen sammeln und Beziehungen in Form von Grafiken zwischen den gefundenen Informationen herstellen.

Beispielsweise werden auf Social Media Plattformen von Personen oft unwissend oder sorglos persönliche und private Daten gepostet, diese können von Tools gesammelt und anschließend für einen Angriff verwendet werden. Selbiges gilt für Unternehmen, wenn Daten von IT-Systemen über das Internet verfügbar sind, können diese von Angreifern/innen als erste Schritte verwendet werden, um den Angriff vorzubereiten und Daten von dem Ziel zu erlangen. [4]

Diese Tools ermöglichen eine erleichterte oder sogar automatisierte Suche nach Informationen zu Personen, Unternehmen und IT-Systemen. Umso mehr Informationen über das Gegenüber gesammelt werden, desto genauer kann ein Angriff vorbereitet werden. Dementsprechend ist dieser Angriff dann auch meist auf ein Unternehmen oder eine Person zielgerichtet.

Es besteht die Möglichkeit, bereits bestehende OSINT Informationen mit den Tools zu empfangen, welche durch den Einsatz von Plattformen wie beispielsweise Malware Information Sharing Plattform (MISP) oder Open Threat Exchange (OTX) ermöglicht werden. In weiterer Folge kann durch den Einsatz von OSINT ein Unternehmen die IT-Sicherheit in ihrer Infrastruktur verbessern.

Von KMUs wird ein Hindernis in der Zeit gesehen, um sich mit diesem Thema und den Tools auseinander zu setzen. Es ist möglichweise nicht bekannt wie die Tools in der Reconnaissance Phase für das Sammeln von den Informationen eingesetzt werden können. Ein weiteres Hindernis ist, dass möglicherweise nicht bekannt ist, welche Informationen mit den Tools gesammelt werden können und welche Angriffe mit den gesammelten Informationen ermöglicht werden. Meist ist auch nicht bekannt, wie die OSINT-Tools in der Information Gathering Phase eingesetzt werden können und wie sich die einzelnen Tools untereinander unterscheiden.

Dadurch, dass möglichweise das Hintergrundwissen zu den verschiedenen Tools fehlt, ist nicht bekannt, welche Vorteile und Nachteile durch die Verwendung der Tools entstehen können, sowie welchen Schutz die Tools für ein Unternehmen und dessen Infrastruktur bringen können und wie die Tools im Unternehmen schlussendlich eingesetzt werden können.

1.1. Problemstellung

Die zahlreich vorhandenen Open Source Tools für OSINT können von Unternehmen oder Personen verwendet werden, um erste Erkenntnisse der im Internet zugänglichen Informationen zu bekommen. Dadurch wird es ermöglicht herauszufinden, welche Informationen im Internet öffentlich frei zugänglich über Unternehmen oder Personen sind. Diese öffentlichen Informationen können ebenso von einem Angreifer oder einer Angreiferin missbraucht werden und für eine gute Angriffsbasis sorgen.

Mit den Informationen, welche über das Internet frei zugänglich sind, kann von einem Angreifer oder einer Angreiferin “Information Gathering” betrieben werden. Ein Problem ist, dass Unternehmen oft selber nicht wissen, welche Daten im Internet über ihr Unternehmen verfügbar sind.
Damit können anschließend die gefundenen Informationen und Daten mit Personen oder Unternehmen in Verbindung gebracht werden. Dadurch ist es möglich intelligente Informationen zu erstellen, welche sich aus verschiedenen Informationen wie beispielsweise Name von Personen, Domain Name, Telefonnummern, Hostname, Organisationen/Unternehmen oder E-Mail-Adressen ergeben, diese kann von öffentlichen Quellen gesammelt und miteinander verknüpft werden. [11] [12]
Durch die Scans der jeweiligen Tools können weiters verschiedene Schwachstellen von Unternehmen gefunden werden. Diese Scans können von einem Unternehmen selber durchgeführt werden, um die möglichen Angriffsflächen zu reduzieren, indem die gefundenen Schwachpunkte von IT-Mitarbeitern geschlossen werden. Jedoch können ebenso Angreifer die vorhandenen OSINT-Tools verwenden. Somit können gefundene Schwachstellen und Informationen einen Angreifer oder Angreiferin dabei unterstützen einen Angriff vorzubereiten.

Einige Probleme, die sich in diesem Bereich ergeben können, sind beispielsweise, die Lesbarkeit der Bedrohungen, aber auch die Einfachheit der Erstellung von OSINT-Informationen. [13] Weiters sollten Bedrohungen rasch zwischen Unternehmen sowie in Abteilungen ausgetauscht werden können. Hier können Threat Intelligence Plattformen (TIPs) als Unterstützung eingesetzt werden.
Ein weiteres Problem ist, dass bei KMUs oft die Ressourcen und die Kompetenzen fehlen, da die Mitarbeiter mit dem laufenden Betrieb beschäftigt sind. Daher besteht oft das Problem, dass Mitarbeiter sich nicht auf das Analysieren von verschiedenen Tools für die Unternehmenssicherheit konzentrieren können. Problematisch kann deren Kategorisierung, aber auch die Mengen von Informationen sein, welche gespeichert werden können. [14]
Da es wenige Berichte und Vergleiche der verfügbaren Tools gibt, welche auf dem Markt verfügbar sind, ist es für Unternehmen schwer sich mit diesem Thema zu beschäftigen, da oftmals die Zeit dafür fehlt. Ebenso fehlt es an einer Übersicht, welche Funktionen die jeweiligen Tools haben und welche Informationen damit gesammelt werden können.

Ein weiteres Problem stellt das ”leichte” Teilen von Informationen auf Social Media Plattformen da. Hier können möglicherweise Mitarbeiter auf verschiedenen Plattformen firmeninterne Daten veröffentlichen. Es ist oft den Mitarbeitern nicht bewusst, dass ein Angreifer diese Daten mittels einfachen Tools sammeln kann und diese Informationen anschließend gegen das Unternehmen verwenden kann. [15]

Die Intention dieser Arbeit ist, eine solche Übersicht der aktuellen OSINT-Tools, in einer State of the Art Analyse, am Markt zu erheben. In dieser Arbeit werden vorhandene Tools anhand von zuvor definierten Kriterien überprüft und miteinander verglichen. Dadurch soll einem Unternehmen die Möglichkeit gegeben werden, sich einen Überblick über die Tools zu beschaffen. Danach werden ausgewählte Tools in einer Matrix anhand vordefinierter Kriterien verglichen, gegenübergestellt und eine Empfehlung für unterschiedliche Einsatzgebiete gegeben. Dadurch entsteht für ein Unternehmen eine Übersicht der analysierten Tools und deren verschiedenen Funktionalitäten.

Weiters wird zu den jeweiligen OSINT-Tools eine Beschreibung durchgeführt und jedes Tool in der Praxis auf dessen Tauglichkeit und Verwendbarkeit getestet.
Ebenso werden durch die Tests, welche in der Praxis durchgeführt worden sind, einem Unternehmen gezeigt, wie diese Tools angewendet werden können, um einen Scan auf das eigene Unternehmen durchzuführen und mögliche Schwachstellen zu erkennen.

1.2. Motivation

Das Thema OSINT (Open Source Intelligence) sowie die Verwendung von Threat Intelligence wird heutzutage ein immer wichtigeres Thema. Das Thema wurde für diese Arbeit ausgewählt, da es ein sehr aktuelles und wichtiges Gebiet ist. Weiters besteht schon seit langer Zeit Interesse an einer detaillierten Forschung in diesem Bereich. Zu Beginn dieser Arbeit werden, die allgemeinen Punkte dieses Themas beschrieben, welche in Kapitel 2 „*Background*" zu sehen sind.

Diese Publikation soll als Unterstützung für KMUs dienen, welche sich aufgrund der wenigen Ressourcen oder des Budgets mit diesem Thema nicht beschäftigen können. Es soll weiters Personen dienen, welche sich in diesem Gebiet mehr Wissen aneignen möchten. Auch wurde während der Recherchen und der Vorbereitung auf dieses Thema herausgefunden, dass es kaum Arbeiten gibt, welche sich mit dem Vergleichen von verschiedenen Tools auf dem Gebiet von OSINT beschäftigen. Dadurch soll eine Übersicht über die analysierten Tools geschaffen werden und somit eine Entscheidungshilfe gegeben werden.
Weiters fehlt meistens den gefundenen Publikationen, welche in Kapitel 3 „*Related Work*" beschrieben sind, der praktische Test der Tools. Durch den praktischen Test der analysierten Tools wird einem Leser das benötigte Hintergrundwissen gegeben, welches für das Auswählen des Tools benötigt wird. Es werden verschiedene Schritte abgebildet oder textuell erklärt, welche einer Person bei der Erstverwendung eines Tools für Zeitersparnis sorgt. Weiters wurde auf verschiedenen Social Media Plattformen ein User angelegt, dies dient dazu, um einem Leser zu zeigen, welche Gefahren das Veröffentlichen von "Informationen" mit sich bringen kann. Um die Kritikalität vor Augen zu führen, wurde ebenso eine Untersuchung und ein Scan von der Fachhochschule durchgeführt, womit gezeigt wird, welche Informationen und Daten ein Angreifer mit Tools speichern kann. Mit diesen Analysen eines Tools kann dessen derzeitiges Potenzial herausgefunden werden.

Da der Fokus in dieser Arbeit auf das Vergleichen der Tools gelegt wird, können KMUs diese Arbeit als Entscheidungshilfe für die Auswahl von Tools ansehen. Ein solcher Vergleich ist wie oben beschrieben in wenigen Arbeiten vorhanden. Daher soll der durchgeführte Vergleich der Tools anhand von eigens definierten Kriterien Abhilfe verschaffen und eine Übersicht der analysierten Tools bieten. Durch die daraus erstellte Matrix kann ein Unternehmen ein Tool aussuchen, welches auf die gewünschten Anforderungen ausgelegt ist. Ein solcher Vergleich wird als Tabelle in Kapitel „*Auswertung & Interpretation der Ergebnisse*" gegenübergestellt.
Weiters wird untersucht, welche Informationen mit den jeweiligen Tools gefunden werden können, damit können Unternehmen und Personen das Tool anhand dessen auswählen. Ebenso gibt es wenige Arbeiten, welche sich mit der Kombination von Angriffsarten und den analysierten Tools beschäftigen. Dazu wurden in dieser Arbeit verschiedene Angriffsarten ausgewählt. Diese Angriffsarten spiegeln sich anhand der Informationen, welche mit den analysierten Tools gefunden werden können, wider und sollen auf die Kritikalität hinweisen. Damit dient diese Arbeit ebenso dazu, um zu sehen, welche Informationen von einem Angreifer benötigt werden, um einen Angriff auf eine Person oder ein Unternehmen durchzuführen.
Es sollen durch diese Arbeit das Verständnis, aber auch die Einblicke in das Thema gegeben werden. Dadurch soll die Einfachheit gezeigt werden, um an Informationen von einem Ziel zu kommen, aber zugleich die Grenzen der Tools aufgezeigt werden, da nicht alle Informationen gesammelt werden können. Daher wird in dieser Arbeit eine wichtige Phase von OSINT behandelt, welche die Reconnaissance Phase ist. Dies soll einem Leser in Kombination mit den analysierten Tools zeigen, welche Möglichkeiten bestehen, um mit einem "passiven" Scan an Informationen eines Ziels zu gelangen. Das theoretische Kapitel schafft einem Leser das benötigte Hintergrundwissen und es soll darin ebenso die Aktualität des Themas sowie dessen Herausforderungen zeigen.
Durch das Demonstrieren und Vergleichen der analysierten Tools, werden deren Funktionalitäten dabei genauer beschrieben und erklärt und als Matrix abgebildet.

1.3. Forschungsfragen

1. Wie kann die Reconnaissance-Phase für Information-Gathering bei den ausgewählten Tools eingesetzt werden?

    a. Welche Informationen können mit den kostenlosen OSINT Tools gesammelt werden?
    b. Welche Angriffe können mit den gefundenen Informationen durchgeführt werden?
    c. Wie kann die Information Gathering Phase durchgeführt werden?
    d. Inwiefern können die Open Source Tools für die Information Gathering Phase eingesetzt werden und wie unterscheiden sich die jeweiligen Tools in deren Funktionen?

2. Inwiefern entstehen durch die Verwendung von OSINT Vorteile und Nachteile und wie kann dies zum Schutz der Infrastruktur eines Unternehmens beitragen?

    a. Inwiefern können die ausgewählten Tools in einem Unternehmen eingesetzt werden?

3. Wie können Use-Cases dabei helfen, mit Open Source Intelligence Schwachstellen zu finden und wie kann dadurch das Unternehmen abgesichert werden?

1.4. Methodik

In den vorherigen Kapiteln wurden Ziele dieser Arbeit definiert. Um diese Ziele zu erfüllen und die damit verbundenen Forschungsfragen zu beantworten, müssen zuerst Kriterien definiert werden. Nachdem die Kriterien definiert worden sind, ist es möglich die ausgewählten Tools zu analysieren und eine Gegenüberstellung vorzunehmen. Es wurden durch Online-Recherchen sowie aus Fachliteraturen, Kriterien abgeleitet und an die Arbeit angepasst, womit darauffolgend eine genaue Analyse durchgeführt werden kann.

Nachdem die Kriterien, nach welchen die Tools evaluiert und geprüft werden, definiert worden sind kann im Detail geprüft werden, wieweit die Tools die Kriterien und dahinterliegenden Funktionen erfüllen, womit ein erstes Fazit gezogen werden kann. Danach ist es möglich, die Tools und deren Funktionalität auf die Praxistauglichkeit im Alltag zu prüfen.

Im letzten Schritt wird nochmals genauer auf die gefundenen und analysierten Kriterien des jeweiligen Tools eingegangen und ein Vergleich untereinander durchgeführt. Dies erfolgt auf der zuvor durchgeführten Analyse. Anschließend können zu den Tools Empfehlungen für Personen und Unternehmen gegeben werden.

Das Thema OSINT umfasst einen großen Bereich, daher musste eine Einschränkung durchgeführt werden, um den Rahmen dieser Arbeit nicht zu überschreiten. Es wurden in dieser Arbeit nur “kostenlose Tools" analysiert. Da verschiedene “kostenlose Tools” zur Verfügung stehen, wurden hier Tools gewählt, welche in Fachliteraturen und in Online-Foren sowie in diversen Communities verwendet werden. Weiters haben die eigen definierten Kriterien, welche in Kapitel 5.3 „*Kriterien*“ beschrieben werden, als Einschränkung gedient.

Durch die zuvor definierten Kriterien, welche auch eine Beschreibung enthalten, ist es möglich eine Eingrenzung des Themas zu schaffen, sodass ein Vergleich zwischen den analysierten Tools durchgeführt werden kann.

Für einen Vergleich ist es notwendig, dass die Funktionalitäten der jeweiligen Kriterien beschrieben werden. Nachdem die Funktionalitäten der Tools überprüft und beschrieben worden sind, ist es möglich eine Matrix davon zu erstellen und diese aufzuzeigen. Dies soll Unternehmen unterstützen, um auf einen Blick die jeweiligen Kriterien und deren damit verbundenen Funktionen auf zu zeigen. Damit können schneller die Tools für den jeweiligen Einsatzbereich und deren Anforderungen gefunden werden. Zuletzt werden verschiedene Anwendungsfälle der einzelnen Tools gegeben, um einem Leser einen Bezug zu dem Tool und dessen Einsatzmöglichkeiten bereit zu stellen.

1.5. Aufbau der Arbeit

Der Aufbau der Arbeit ist in folgende Kapitel geteilt.
Im ersten Kapitel der Arbeit wird auf die Problemstellung, Zielsetzung, Forschungsfrage sowie die Methodik eingegangen.

Das Kapitel zwei “Background” dient als allgemeine Beschreibung des Themas sowie zu der Arbeit direkt. Ebenso werden hier verschiedene Begrifflichkeiten beschrieben, welche für die Arbeit in den weiteren Kapiteln benötigt werden.

Im dritten Kapitel wird speziell auf die Related Work eingegangen. Es werden in diesem Kapitel gefundene Arbeiten beschrieben und verglichen. Durch den Vergleich sollen die Gemeinsamkeiten aber ebenso die Unterschiede der Arbeiten zum Vorschein kommen.

Anschließend wird im vierten Kapitel auf die Open Source Informationen eingegangen und eine Erklärung zu den Informationen gegeben. Dieses theoretische Kapitel dient dazu, um Hintergrundwissen von OSINT zu erlangen und den Stand der Technik zu beschreiben.
Weiters wird in diesem Kapitel allgemein auf die Entwicklung von Open Source Information (OSINT) eingegangen und wie es sich bis jetzt weiterentwickelt hat.
Zusätzlich wird auch die Wichtigkeit von OSINT für bestimmte Unternehmen und Organisationen beschrieben. Außerdem wird auch auf die verschiedenen Typen von OSINT eingegangen und mittels Erklärungen genauer definiert. Ebenso wird hier auf den Unterschied von Offensive und Defensive OSINT eingegangen, da diese Begriffsunterscheidung eine wichtige Rolle spielt. Zeitgleich wird in diesem Kapitel der genaue Ablauf des OSINT Prozesses erklärt. Ergänzend wird auch beschrieben, welche Schritte notwendig sind, um mittels OSINT an Daten zu kommen und diese anschließend verarbeiten zu können. Dieses Kapitel beinhaltet weiters als Unterpunkt eine genaue Erklärung der Schritte für die Analyse von gesammelten OSINT-Daten.

Es wird auch auf die Social Media Plattformen und deren Mächtigkeit hingewiesen, da sehr viele Daten durch sorgloses Posten von Personen gesammelt werden können. Gleichzeitig wird hier auf die Vorteile von OSINT eingegangen und diese beschrieben. In dem Unterpunkt dieses Kapitels wird darauf hingewiesen, dass heutzutage OSINT schon unbewusst verwendet wird und weiters wird auf den OSINT-Cycle eingegangen.
Es wird ebenso in diesem Kapitel auf verschiedene Angriffsarten eingegangen, sowie eine genaue Erklärung zu den jeweiligen Angriffsarten abgegeben. Hier werden die Verteidigungsarten und Sicherheitssoftwares erörtert und eine Beschreibung zu den jeweiligen Punkten gegeben. Zudem behandelt es zwei verschiedene Sichtweisen. Einerseits wird hier die Sichtweise von einem Angreifer oder einer Angreiferin und der benötigten Schritte, sowie der Prozess für das Sammeln der benötigten Informationen beschrieben, andererseits wie sich ein/e Verteidiger/in gegen einen Angriff schützen kann.

Im fünften Kapitel wird zuerst die Infrastruktur der Testumgebung erörtert, auf welcher die Tools getestet worden sind. Außerdem findet hier auch die Gegenüberstellung der Tools und deren

gefundene Kategorien statt. Hier werden die definierten Kriterien beschrieben, nach denen die Tools analysiert und gegenübergestellt worden sind und anschließend im Detail erklärt.

Im sechsten Kapitel werden die ausgewählten Tools evaluiert. In diesem Kapitel setzt sich daher auch der Fokus auf die Forschungsfragen. Hier findet eine Beschreibung der jeweiligen Tools statt. Anschließend werden die definierten Kriterien und deren dazugehörigen Eigenschaften beschrieben. Es wird für jedes der Tools ein praktischer Test durchgeführt, womit das Tool auf dessen Tauglichkeit im Praxisbetrieb und Alltag getestet wird. Zuletzt wird auf die Herausforderungen und Erkenntnisse eingegangen, welche sich während dem Testen des Tools gezeigt haben. Es wird ein Fazit über das Tool gegeben und dessen Vorteile und Nachteile aufgezeigt.

Im Kapitel sieben werden verschiedene Use Cases beschrieben, welche durch die Verwendung von OSINT abgedeckt werden. Ebenso wird ein Use Case beschrieben, welcher für diese Arbeit ausgelegt worden ist. Es findet weiters in diesem Kapitel ein Vergleich der analysierten Tools statt.

Kapitel acht befasst sich mit der Auswertung und den Forschungsfragen. Es werden die verschiedenen Vorgänge wie beispielsweise zu der Tool Findung beschrieben. Auf welcher Grundlage die Evaluierung liegt und es wird das Modell der Evaluierung dargestellt.

In Kapitel neun werden die aufgestellten Forschungsfragen beantwortet.

Kapitel zehn behandelt die Conclusion und die durch die Arbeit entstandenen aufbauenden Forschungsgebiete.

2. Background

Dieses Kapitel dient dazu, um einen Überblick über die Arbeit zu verschaffen und prägnant Begrifflichkeiten zu beschrieben.

Allgemein:
Es gibt eine Menge von Social Media Plattformen, welche massenhaft Informationen über Personen enthalten. Diese privaten und sensiblen Informationen werden oft sorglos und unbedacht von Personen publiziert. Da die Menge an Informationen, welche in das öffentliche Netz gestellt werden, stetig größer wird, können immer mehr persönliche Informationen abgefragt werden. Das ist möglich, weil durch das Internet keine Grenzen geboten werden und immer und überall, neue Posts erstellt werden und Informationen verteilt werden können.
Diese gesammelten Informationen können als Vorbereitung für Cyber-Angriffe verwendet werden. Dies betrifft aber nicht nur Personen die Informationen über sich selber preisgeben, sondern auch Unternehmen die Informationen wie Backups oder sensitive Informationen auf Servern speichern. Bei diesen könnte es zu einer falschen oder fehlerhaften Konfiguration kommen, womit die Daten in das Internet gelangen können oder darüber zugreifbar sein können. Es können ebenso Mitarbeiter unbewusst Informationen über IT-Services und IT-Systeme veröffentlichen, welche ein/e Angreifer/in für den Angriff verwenden kann.
Durch das Sammeln firmeninterner Informationen ist es möglich, dass gegenüber anderen Unternehmen ein Wettbewerbsvorteil entsteht. Da immer mehr Informationen und Daten im Internet verfügbar sind, müssen daher auch Unternehmen handeln und diese Informationen für sich verwenden, um einen Vorteil gegenüber der Konkurrenz aufzubauen.

Um in dieser Arbeit keine sensiblen Informationen zu verwenden, wurden Fake-Profile auf Social Media Plattformen erstellt. Durch das Fake-Profil wird somit die Möglichkeit gegeben, ein realitätsgetreues Vorgehen durchzuführen, welches das Sammeln und Speichern von Informationen inkludiert, ohne dass dabei sensible Informationen eines Users in diese Arbeit gelangen.
Damit soll gezeigt werden, wie einfach Angreifer mit Tools an sensible Informationen kommen können und profilbezogene Daten eines einzelnen Users speichern können.
Für Testzwecke wurde die Twitter-Seite der Fachhochschule St. Pölten in diese Tests mit einbezogen, um an einer produktiven Twitter-Seite die Funktionalitäten der analysierten Tools zu testen.

In dieser Arbeit wurden jegliche Tests in der “passiven” Scan Form durchgeführt, dadurch wird es ermöglicht, die verfügbaren Daten im Internet zu sammeln, ohne dass das Ziel dies bemerkt. [16]

Die analysierten OSINT-Tools können einerseits von Unternehmen aber auch von einzelnen Personen verwendet werden, um Recherchen über Unternehmen durchzuführen und somit die Systeme und Informationen zu schützen. Die Resultate und Analysen der Scans können ebenso von Unternehmen verwendet werden, um Systeme und Informationen des Unternehmens zu schützen. Die OSINT-Tools können intern eingesetzt werden, um Schwachstellen zu erkennen und mögliche Datenlecks oder kritische Systemlücken zu finden.
OSINT wird ebenso von militärischen Organisationen verwendet, um der Sicherheit in einem Land beizutragen sowie gegen Terrorismus-Bekämpfung mitzuwirken. Problematisch ist, dass ebenso kriminelle und terroristische Organisationen Zugriff auf diese Tools haben und dieselbe Möglichkeit besteht, diese Informationen sammeln zu können.

Um in dieser Arbeit mehr Informationen mit den analysierten OSINT-Tools zu finden, wurden folgende API-Keys (Application Programming Interface) bei den Tools, welche einen dieser Keys unterstützen, beigefügt:

- Hunter.io
- AbuserIPDB
- builtwith.com
- botscout.com
- Shodan
- Zetalytics

Es sind keine weiteren API-Keys verwendet worden, da diese oft mit separaten Kosten verbunden sind.

Laut einem Bericht von “Gartner” werden zum Jahr 2020 bis zu 20 Millionen IoT-Geräte (Internet of Things) erwartet, daher ist dieses Thema umso wichtiger. Im Vergleich dazu waren es im Jahr 2016 nur 6,3 Millionen IoT-Geräte, die mit dem Internet verbunden waren. Laut diesem Trend werden die Daten, welche über Personen verfügbar sind, immer mehr. Dementsprechend können sich Angreifer immer besser auf gezielte Angriffe vorbereiten. Weiters ist auch zu beachten, dass dadurch eine erhebliche Speicherkapazität durch die rasend steigende Nutzung von IoT-Geräten vorhanden sein muss. Es werden bis zu 44 Zettabytes im Jahr 2020 erwartet. [17]
Weiters wurde gesagt, dass im Jahre 2025 bis zu 80 Milliarden Geräte mit dem Internet verbunden sein werden. Zurzeit sind es 11 Milliarden Geräte (Stand 2016) die mit dem Internet verbunden sind, laut Konferenz sollten es bis 2020 knapp 30 Milliarden Geräte sein. Es werden daher immer mehr Digitale-Daten im Umlauf sein, welche ein Angreifer/Angreiferin sowie normale Personen für sich verwenden können. Ein Beispiel was auf der Konferenz kundgemacht wurde, dass das Auto „Ford GT“ bereits 50 Sensoren enthält und 28 Mikroprozessoren, das Auto kann innerhalb von einer Stunde 100GB an Daten erzeugen. Es wird aber betont, dass Merkmale wie Sicherheit, Standards sowie Kosten die Weiterentwicklung des Marktes von IoT begrenzen. [18]

Threat Intelligence:
Um einen Überblick über mögliche TI-Plattformen und deren Funktionalitäten zu bekommen sind diese anschließend beschrieben worden. In Kapitel 4.3 „*OSINT und Threat Intelligence*“ ist eine weitere Beschreibung sowie eine weitere Tabelle 4 „*TI-Plattformen*“ erstellt worden, um die Unterschiede der jeweiligen Plattformen zu zeigen.

MISP: Bei dem Begriff MISP handelt es sich um „Malware Information Sharing Plattform“. Auf der Homepage von MISP wurde publiziert, dass bereits 6000 Unternehmen weltweit MISP verwenden. [19]
Es handelt sich bei MISP um eine Open-Source-Software um Bedrohungen und Cybersicherheitsindikatoren auszutauschen. Mittels des Tools können Daten gesammelt, gespeichert und zum Korrelieren von Indikatoren, welche in Kapitel 4.3 „*OSINT und Threat Intelligence*“ beschrieben sind, verwendet werden. Dies ist sehr nützlich gegen diverse Finanzbetrüger, Sicherheitslücken aber auch gegen Terrorismus. [20]
Die Lizenz, unter der die Plattform läuft, ermöglicht eine kostenlose Verwendung der Software. Die Plattform dient ebenso dazu, um Bedrohungen im Detail zu beschreiben, da MISP beispielsweise die Beschreibungssprache STIX anbietet.
Auf der MISP Webseite werden verschiedene Feed Provider angeboten, welche einem einen kostenlosen Austausch von Feeds ermöglichen. [21]
Als Import sowie Export-Formate werden von dem Tool ”MISP-JSON”, ”JSON” und ”CSV” unterstützt. Das MISP-JSON Format dient dazu, um einen Austausch zwischen MISP-Plattformen oder Unternehmen zu ermöglichen. Es wird von der Plattform ermöglicht, dass die Feeds über die API (Application Programming Interface) durchsucht werden können. Diese Plattform wird in Kapitel 7 „*OSINT Use Case*“ genauer beschrieben und in der Praxis getestet.

OTX: Bei OTX handelt es sich um “Open Test Sequence eXchange”. Diese Plattform ermöglicht Sicherheitsforschern einen Austausch von Bedrohungen. OTX bietet einen öffentlichen Zugang um einen weltweiten Zugang für Sicherheitsforscher sowie Sicherheitsexperten zur Verfügung zu stellen. Somit können Bedrohungsdaten aktiv ausgetauscht werden. Es wird dadurch die Verbreitung neuer Bedrohungsinformationen beschleunigt. [22] OTX ist eine Online Plattform welche kostenlos verwendet werden kann. Das Erhalten von Feeds ist bei dieser Plattform kostenlos. Es können weiters die Feeds adaptiert werden und anschließend verteilt werden. Von dem Tool werden verschiedene Such- und Filtermöglichkeiten angeboten. Es kann beispielsweise nach Indikatoren gesucht werden und es kann ebenso nach Textzeichenfolgen gesucht werden. Es werden verschiedene Import-Formate angeboten wie E-Mails, PDF-Dateien, Log-Dateien, OpenIOC und STIX. Ebenso werden verschiedene Export-Formate wie JSON, CSV, STIX und OpenIOC zur Verfügung gestellt.

X-Force Exchange: Hier handelt es sich um ein IBM-Produkt welches 2015 eingeführt worden ist. Es beinhaltet über 20 Jahre lang gesammelte Bedrohungsinformationen, welche frei zugänglich bereitgestellt werden. Die IBM X-Force Exchange Bedrohungsdatenplattform dient dazu, dass Sicherheitsexperten Bedrohungsindikatoren suchen können, um die Reaktionszeit auf Bedrohungen zu verkürzen. Da eine Cloud-Lösung bereitgestellt wird, kann diese Plattform auf jegliche Unternehmensgröße bereitgestellt und skaliert werden. Die Plattform kann kostenlos benutzt werden und es können im Monat bis zu 5000 Datensätze abgefragt werden, wenn dieser Wert überschritten wird muss von einem Unternehmen die kommerzielle Lösung verwendet werden. Weiters wird ermöglicht, dass von Drittanbietern weitere Threat Intelligence Feeds eingebunden werden. [23]
Bei der Verwendung von der Plattform X-Force fallen bis zu einer Abfragemenge von 5000 Datensätzen im Monat keine weiteren Kosten an. Es werden verschiedene Such- und Filtermöglichkeiten zur Verfügung gestellt, welche Indikatoren oder CVE (Common Vulnerabilities and Exposures) sein können. In der verwendeten kostenlosen Version von X-Force Exchange ist es nicht möglich gewesen Feeds zu importieren. Als Export-Funktion wird STIX 1.x und 2.x zur Verfügung gestellt.

Anschließend werden noch zusätzliche TI-Plattformen und dessen Sprachen beschrieben, damit ein Überblick gegeben werden kann, welche jedoch nicht weiter in dieser Arbeit behandelt werden.

Beschreibungssprachen für Cyberbedrohung:
In dem folgenden Abschnitt werden vier verschiedene TIPs Sprachen beschrieben und in einer Tabelle wiedergegeben.

OpenIOC: Es handelt sich hierbei um ein Framework, welches ermöglicht Informationen über Bedrohungen in einem maschinenlesbaren Code auszutauschen. Die Sprache von OpenIOC (Open Indicatiors of Comprimise) ist XML, womit eine Anpassung der Informationen durchgeführt werden kann. Ein Tool wäre Loki, damit kann automatisiert nach IoCs gesucht werden. [24] [25]

STIX: Bei dem Begriff STIX handelt es sich um „Structured Threat Information eXpression“. Mittels STIX wurde ein Standard mit einer Standardsprache erschaffen, welche für die Beschreibung von Bedrohungen verwendet werden kann. Diese Sprache ist weiters Maschinen und Menschen lesbar. Das bedeutet, dass die Bedrohungen in maschinelle Prozesse hinzugefügt werden können. Hinter der weiteren Entwicklung von STIX steht das Unternehmen OASIS (Organization for the Advancement of Structured Information Standards). Es gibt zwei Versionen von STIX, STIX 1 basiert auf einer XML-Struktur. Die STIX 2 Version ist die neuere Version, welche auf JSON basiert. [26] [27]

TAXII: Bei TAXII handelt es sich um den Begriff „Trusted Automated eXchange of Intelligence Information“. Es ist ein Standard, um beispielsweise in einem Unternehmen die Abwehr von Cyberangriffen zu verbessern. TAXII bietet einer Person die Möglichkeit, Beschreibungssprachen von Bedrohungen wie STIX unter weiteren Personen oder Instituten zu verteilen. [28]

IODEF: Der Begriff IODEF (Incident Object Description Exchange Format) wurde in dem RFC 5070 beschrieben. Hier handelt es sich um ein Format, welches zur Darstellung von gemeinsam ausgetauschten Sicherheitsinformationen zwischen CSIRTS (Computer Security Incident Response Teams) dient. IODEF dient ebenso zur Verbesserung von Arbeitsabläufen, da durch die Gemeinschaft der Community oder Parteien eine bessere Fähigkeit vorhanden ist, um Vorfälle zu lösen. [29]

Beschreibungssprachen für Cyberbedrohung	**Import**	**Export**	**Beschreibung**	**Bereitstellung**
OpenIOC	-	OTX	x	
STIX 1	OTX, MISP	OTX, MISP, X-Force-Exchange	x	
STIX 2	OTX	OTX, X-Force-Exchange	x	
TAXII				x
IODEF			x	

Tabelle 1 Beschreibungssprache TIP

Beschreibung der Tabelle:

Import:
Hier wird geprüft, ob die Beschreibungssprachen in die Plattformen wie “MISP”, “OTX” oder “X-Force-Exchange" importiert werden können.

Export:
Hier wird geprüft, ob die Beschreibungssprachen in “MISP”, “OTX” oder “X-Force-Exchange" exportiert werden können.

Beschreibung:
Hier wird gezeigt, ob diese als Beschreibungssprache gilt, dies wird anschließend mit einem “x” in der Tabelle markiert.

Bereitstellung:
Dieses Kriterium prüft, ob die Sprache zur Bereitstellung von Informationen gilt, dies wird mit einem “x” in der Tabelle markiert. Hier wird geprüft ob es möglich ist, die Feeds zu verteilen und für weitere Personen zur Verfügung zu stellen.

Cyberbedrohungs-Institute: In dem folgenden Abschnitt werden zwei Cyberbedrohungs-Institute beschrieben und in einer Tabelle wiedergegeben.

CIRCL: Das CIRCL-Institut (Computer Incident Response Center Luxembourg), ist eine Initiative der Regierung. Es dient dazu, um auf Bedrohungen und Vorfälle im Bereich der Computersicherheit zu reagieren und diese zeitnah zu erfassen und zu melden. Unternehmen, Personen und Organisationen in Luxemburg können sich bei Vorfällen an CIRCL wenden. Es dient als vertrauenswürdiger Ansprechpartner für die Behandlung und Unterstützung bei Cyber Angriffen. Ebenso wurde eine detaillierte Beschreibung in RFC 2350 durchgeführt. [30] [31]

CSSA: Hier handelt es sich um einen im November 2014 von sieben deutschen Großfirmen gegründeten Verein namens CSSA (Cyber Security Sharing & Analytics). Das Ziel des Vereines ist es, sich durch die Zusammenarbeit besser vor Cyber Angriffen sowie Bedrohungen zu schützen. Es wird als Fokus der Austausch sowie die Analyse von Bedrohungen im Kreis der 13 Mitglieder gelegt, sowie auf den gemeinsamen Aufbau von Threat Intelligence. Dadurch sollen Bedrohungen schneller erkannt werden, um Angriffe schneller abwehren zu können.

Es werden Bedrohungsinformationen, die beispielsweise durch die Analyse einer Cyberattacke erkannt worden sind, als sogenannte Threat Intelligence Feeds an die weiteren Mitglieder weitergegeben. Es können ebenso die externen Threat Intelligence Bedrohungsinformationen von den Mitgliedern empfangen werden. [32]

Institute	Beschreibungs-sprachen /Tools	Mitglieder	Kosten	Gratis Feeds
CIRCL	SMILE	-***	Nein	Ja
CSSA	MISP	13	Ja*	Nein**

Tabelle 2 Institute TIP

*Die 13 Mitglieder zahlen dieselben Kosten und haben daher die gleichen Rechte.
**Die Feeds werden geschlossen unter den 13 Mitgliedern, welche einen Beitrag dafür zahlen, geteilt.
***Es ist eine Organisation, bei welcher sich Personen melden können und Probleme mitteilen können, daher ist es nicht möglich, eine konkrete Anzahl von Mitgliedern zu nennen.

Beschreibung der Spalten:

Sprachen:
Dieses Kriterium soll beschreiben, welche Beschreibungssprachen oder Tools von den Instituten unterstützt und verwendet werden, um Feeds zu teilen.

Mitglieder:
Bei diesem Kriterium wird aufgezeigt, wie viele Mitglieder die Institute innehaben.

Kosten:
Das Kriterium Kosten soll zeigen, ob ein Institut das Empfangen von Feeds kostenlos ermöglicht, oder ob dafür Kosten entstehen. Kosten können beispielsweise Mitgliederbeiträge sein, welche für das Empfangen von den Feeds gezahlt werden müssen.

Gratis Feeds:
Durch dieses Kriterium soll gezeigt werden, ob von dem Institut das Verteilen von Feeds kostenlos angeboten wird. Dabei wird geprüft, ob die Feeds vom Institut auch kostenlos an private Personen zur Verfügung gestellt werden, welche nicht dem Institut angehören.

3. Related Work

Das Thema Open Source Intelligence (OSINT) hat in der heutigen Zeit an großer Bedeutung gewonnen, daher wurden bereits vorhandene Arbeiten mit dieser verglichen.

Joost Hendricksen hat in seiner Arbeit [33] den Fokus auf die Methoden und das Erstellen eines Users anhand der gefundenen OSINT-Daten gelegt und auf Prototypen sowie einer Modellimplementierung gesetzt. Bei den Modellen werden verschiedene Daten und Informationen aus “Google”, “Facebook”, “Twitter” und “LinkedIn” gesammelt, um Verdächtige auszuforschen. In dieser Arbeit wird ebenso über die Verbesserungen des Modells berichtet und über die durchgeführten Fehlerkorrekturen. Durch diese Arbeit ist ein automatisiertes Modell entwickelt worden, um Datenanalysten bei der digitalen Profilerstellung zu unterstützen. Weiters wird darauf hingewiesen, dass die automatisierte Benutzerprofilerstellung noch in den Anfängen steckt und weiter ausgereift werden muss.

Lilian Mitrou hat in der Arbeit [34] den Fokus auf die Social Media Plattformen sowie auf Social Networks gelegt. Es wird beschrieben, dass viele der Online verfügbaren Daten und Informationen gespeichert werden können und für eine Vielzahl von Zwecken wie beispielsweise dem Erstellen von Benutzerprofilen oder Verhaltensanalysen herangezogen werden können. Weiters wird beschrieben, wie das Web 2.0 und Social Media Plattformen als Werkzeug verwendet werden können, um Informationen aus geglaubten anonymen Daten zu rekonstruieren. Durch das Rekonstruieren von anonymen Daten können beispielsweise am Arbeitsplatz oder im sozialen Umfeld Ausgrenzungen entstehen oder Vorurteile gegen Personen gebildet werden. Es wird in der Arbeit auf Einfachheit der Speicherung von Informationen und das daraus resultierende Verwenden solcher Informationen hingewiesen. Forscher verwenden die Daten und Informationen, um das Verhalten von Personen in der digitalen Welt zu erforschen. Außerdem wird auch auf die staatliche Überwachung und auf die Profilerstellung von Social Media Nutzern eingegangen.

Pak und Paroubek haben in ihrer Arbeit [35] den Fokus auf Twitter und dessen Microblogging gelegt. Es wird die Stimmungsanalyse sowie die Meinungsforschung beschrieben und wie diese auf Microblogging eingesetzt werden kann. Microblogging ist in der heutigen Zeit eine sehr beliebte Kommunikationsmethode. In deren Arbeit konzentrieren sie sich nur auf Twitter, da dies die beliebteste Plattform für Microblogging darstellt.
Viele Personen schreiben über deren aktuelle Lebenslage, andere schreiben über Themen, die sie gerade beschäftigen und diskutieren über diese. Es werden ebenso verschiedene religiöse sowie politische Ansichten von Menschen gepostet. Diese Informationen stellen eine wichtige Quelle für Microblogging und dessen Analyse dar. Somit können solche Informationen für Marketing oder Soziale-Studien verwendet werden. Für die Untersuchung der Stimmungsanalyse wurden Textbeiträge mit positiven und negativen Gefühlen sowie objektive Texte gesammelt. Es wurden insgesamt 300000 Textbeiträge von Twitter gesammelt. Mit den gesammelten Texten der Tweets wird eine linguistische Analyse durchgeführt, um zu zeigen wie eine Stimmungsanalyse aufgebaut werden kann.

Adedoyin-Olowe hat sich in der Arbeit [36] mit zwei weiteren Personen auf Data Mining Techniken konzentriert und diese analysiert. Er weist darauf hin, dass in den letzten Jahren Social Media Plattformen immer mehr Aufmerksamkeit erlangen. Diese Menge an Informationen kann zu Problemen wie “Unkorrektheit“, “unkontrollierbare Mengen“ und “Dynamic“ führen. Es wird jedoch darauf hingewiesen, dass durch Data Mining Techniken die Probleme wie ”Menge”, ”Unkorrektheit” und ”Dynamik” der Posts verbessert werden können. Die Data Mining Techniken in dieser Arbeit verwenden verschiedene Machine Learning Lernmethoden wie unüberwacht (unsupervised),

halbbeaufsichtigt (semi-supervised) und überwacht (supervised). Es wird auch auf die Meinungsanalyse in den Social Media Plattformen eingegangen und die Clustering Methode ”Homophilie-Clustering“ erwähnt. Social Media Plattformen sind relevante Quellen für den Austausch von Inhalten, hier entstehen ebenso Bewertungen von Menschen, Beobachtungen, Gefühlen sowie Meinungen und Gefühlsäußerungen. Durch die Stimmungsanalyse, welche in dieser Arbeit behandelt wird, sollen die Erwartung, Beobachtungen und die Einstellung von Menschen gegeben werden, um eine Richtung der Bevölkerung oder verschiedener Interessensgruppen zu erkennen. Es wird in dieser Arbeit ebenso auf ”Themenerkennung und Verfolgung in sozialen Netzwerken” eingegangen und es werden verschiedene Techniken diesbezüglich beschrieben.

Mittal und weitere Personen beschreiben in dieser Arbeit [37] ”CyberTwitter”. Dies ist ein System, welches zur Entdeckung sowie zur Analyse von Cybersicherheitsinformationen auf Twitter dient. Sie weisen darauf hin, dass viele der Daten in normalen Textquellen enthalten sind, welche mit OSINT assoziiert werden. Somit können Informationen aus Zeitungen, Video-Sharing-Plattformen, Blogs aber auch aus Social Media Plattformen wie beispielsweise Twitter, Reddit oder Stack Overflow erhalten werden. Aus diesen Quellen können Sicherheitslücken und mögliche Bedrohungen erkannt werden. Durch die Menge an Informationen, ist es nicht möglich dies manuell zu analysieren, daher müssen diese automatisiert verarbeitet und extrahiert werden. Durch die Echtzeitinformationen, welche in Twitter gegeben sind, ist es bereits möglich gewesen bei Veranstaltungen bedeutende Erkenntnisse wie Erdbeben, Terroranschläge oder Waldbrände zu gewinnen. Weiters werden auch von ethischen Hackern neu entdeckte Sicherheitslücken veröffentlicht. Diese Arten von Informationen sind für Analysten von großer Bedeutung.
Das Framework von CyberTwitter ist darauf ausgelegt, dass eine rechtzeitige Warnung der Bedrohung an Sicherheitsanalysten generiert wird. Diese Warnungen können anschließend für weitere Sicherheitssysteme eingesetzt werden.

Viele der analysierten Arbeiten beschäftigen sich ausschließlich mit Twitter und einem dazu entwickelten Framework oder einem Modell mit diesem anschließend Data Mining Prozesse durchgeführt werden können. Eine der analysierten Arbeiten beschäftigt sich mit Social Media Plattformen, jedoch werden in dieser keine OSINT-Tools verglichen. Ebenso wurde eine Arbeit analysiert, welche sich mit Stimmungs- sowie Meinungsanalysen beschäftigt.

In Gegensatz zu den gefundenen Arbeiten, unterscheidet sich diese Arbeit von den bestehenden Arbeiten, da diese den Fokus auf das Erfassen und Speichern von öffentlichen Daten mithilfe von OSINT-Tools legt und die jeweiligen Tools und deren Funktionalitäten beschrieben werden. Um dies durchführen zu können, werden verschiedene Tools analysiert und in der Praxis getestet. Dadurch kann demonstriert werden, welche Daten mit den jeweiligen Tools gespeichert und erfasst werden können. Es wurde in dieser Arbeit zudem der Fokus auf die Reconnaissance Phase des Cyber Kill Chain gelegt, welche für das Information Gathering (Sammeln von Daten) zuständig ist. Dadurch werden die analysierten Tools behandelt, sowie die Reconnaissance Phase.

Mit der anschließenden Bewertung sowie der Beschreibung von den jeweiligen Tools und deren Funktionen ist es einem Unternehmen möglich, ein Tool für einen bestimmten Anwendungsbereich sowie den benötigten Anforderungen zu finden. Es werden ebenso die verschiedenen Vorteile sowie Nachteile eines Tools aufgelistet und die analysierten Tools in der Praxis getestet. Somit muss ein Unternehmen keine separaten praktischen Tests und Recherchen über die Tools durchführen. Weiters wird in der Arbeit ein Vergleich der analysierten Tools durchgeführt. Für den Vergleich sind eigene Kriterien durch Fachliteraturen und Online-Recherchen für die analysierten Tools abgeleitet worden, welche im Weiteren für die Gegenüberstellung und den Vergleich der Tools verwendet

werden. Es werden zudem die verwendeten Tools und deren Handhabung beschrieben. Mit diesen Hintergrundinformationen der jeweiligen Tools soll eine gute Basis über den Umgang mit Tools geschaffen werden. Ebenso wird erläutert, wie diese Tools eine Sammlung und Speicherung von OSINT-Daten durchführen können.

Es wurde weiters ein praktischer Teil in dieser Arbeit durchgeführt. Dafür wird ein Fake-User auf diversen Plattformen erstellt, welche in Kapitel 6 „*Evaluierung von den Tools*“ aufgelistet sind. Es werden verschiedene Interaktionen, wie beispielsweise Kommentare schreiben, Kommentare liken oder Freunde hinzufügen, durchgeführt. Mit den durchgeführten Interaktionen wird erforscht, mit welchen der ausgewählten Tools ein Profiling von Personen durchgeführt werden kann und welche Informationen aus den Interaktionen gesammelt werden können.

Somit besteht die Opposition zu dieser Arbeit, dass sich bei dieser Publikation auf die Tools und deren Vergleiche mittels der Kriterien konzentriert wird. Im praktischen Teil dieser Arbeit wird erforscht, welche Informationen mit den Tools über einen erstellten Test-User gesammelt werden können. Weiters ist die Beschreibung der jeweiligen Tools und deren Handhabung von großer Bedeutung, um schneller an die Informationen zu gelangen.

4. Entwicklung von Open Source Informationen im Allgemeinen

In diesem Kapitel werden die theoretischen Bereiche von Open Source Intelligence (OSINT) erläutert. Es werden verschiedene Prozesse, Zyklen und Abläufe von OSINT erklärt. Weiters werden die Vorteile aber auch Nachteile aufgelistet. Generell werden die Informationen genannt, welche durch OSINT gesammelt und gespeichert werden können. Es wird ebenso Threat Intelligence und dessen Verbindung mit OSINT beschrieben. Hier werden im Detail die verschiedenen Plattformen beschrieben, welche dazu dienen, um Threats (Bedrohungen) zu beschreiben und diese zu verteilen. Ebenso wird auf die verschiedenen Typen von OSINT eingegangen. Diese Typen dienen dazu, um zu beschreiben, auf welche Art die Informationen gesammelt werden können.

Ein wichtiges Kapitel in diesem Abschnitt ist der Cyber Kill Chain. Hier werden die einzelnen Phasen beschrieben. In den jeweiligen Phasen werden separate Gegenmaßnahmen beschrieben. Es wird weiters im Detail auf die Recon-Phase (Reconnaissance-Phase) eingegangen.
Auf diese Phase wurde in dieser Arbeit ebenso ein Fokus gelegt, da durch diese Phase die jeweiligen Informationen mittels passiven Scans gesammelt werden können.

Zuletzt wird auf die jeweiligen Einsatzgebiete von OSINT eingegangen. Es werden die verschiedenen Intelligence Collections sowie Angriffsarten beschrieben. Durch die Beschreibung der verschiedenen Angriffsarten sollen die Möglichkeiten sowie deren Vielfältigkeit hervorgehoben werden. Es wird ebenso auf die Gemeinsamkeiten von OSINT und Marketing Intelligence eingegangen. Ebenso werden die Angriffsinformationen von einer Organisation im Gegensatz zu einer Person verglichen.

4.1. Open Source Intelligence

Open Source Intelligence (OSINT) hat sich in den letzten Jahren immer mehr in Unternehmen etabliert. Es wird von Unternehmen verwendet, um Risiken zu erkennen aber auch dafür, dass eine Einschätzung von möglichen Risiken, Schwachstellen und Bedrohungen vollzogen werden kann.

OSINT ist für viele Unternehmen eine kostengünstige Variante, um aktuelle Bedrohungsinformationen zu erlangen. [38] Viele von den Tools, die für OSINT verwendet werden können, bieten bis zu einem gewissen Grad ihre Dienste kostenlos an. Wenn von dem Unternehmen hingegen erweiterte Funktionen verwendet werden möchten, können Kosten in unterschiedlicher Höhe anfallen. [39]

Durch OSINT ist es möglich verschiedene Angriffe durchzuführen wie beispielsweise auf Unternehmen, aber auch auf Personen. Ein Angriff oder das Ausforschen auf/von Personen kann in der heutigen Zeit relativ leicht stattfinden, da auf Social Media Plattformen sehr viel „gepostet“ wird. Einer Statistik zufolge vermerkt Twitter ca. 500 Millionen Tweets am Tag. [40]
Aber es können auch andere Plattformen als Social Media Plattformen für OSINT verwendet werden, beispielsweise können Webseiten wie „Stack Overflow“ [41] oder “GitHub“ [42] verwendet werden, da hier oft Codeausschnitte von einem Mitarbeiter einer Firma „gepostet“ werden, welcher Rückschlüsse auf die Firma geben kann. Weiters können Informationen über ein Unternehmen von deren Stellenausschreibungen ergattert werden, da Firmen teilweise spezielle Ausschreibungen für neue Mitarbeiter tätigen über Systeme, die in ihrem Unternehmen verwendet werden.
Umso genauer eine Stellenausschreibung beschrieben ist, wie beispielsweise für welches System ein Mitarbeiter gesucht wird, desto genauer können Angreifer die eingesetzten Systeme ausfindig machen.
Hier können beispielsweise gefundene Schwachstellen über das verwendete System des Ziels als Angriffspunkt genommen werden. Somit gewinnt das Wort „Viktimisierung“ immer mehr von Bedeutung, da sich die Angriffe häufen und damit eine auch besser werdende Angriffsmethode

verwendet wird. Für Social Media Plattformen wird meist Social Media Intelligence (SOCMINT) verwendet um Informationen über Personen oder auch Firmen, welche auf diesen Plattformen vertreten sind, zu ergattern. Um eine tiefere und genauere Analyse von Daten zu bekommen wird OSINT verwendet, da diese vielseitiger sind. Mittels OSINT ist es möglich verschiedene Informationen zu verbinden und ein gesamtes Bild zu bekommen. [43]

Durch OSINT besteht die Möglichkeit, dass die öffentlichen Daten, welche von Personen online in Social Media Plattformen preisgegeben werden oder aus anderen öffentlichen Quellen gesammelt werden und anschließend als Vorbereitung für einen Angriff verwendet werden können. OSINT ist ein sehr großes Thema in der Cybersicherheit. Aber auch im militärischen, geschäftlichen und unternehmerischen Umfeld sind diese Informationen ein wichtiges Thema. Weiters geben viele Unternehmen Auftraggebern den Auftrag, Konkurrenzfirmen auszuforschen, um dem Wettbewerber voraus zu sein. Das Militär verwendet OSINT, um den Terrorismus zu unterbinden und Informationen über Gegner oder mögliche Angriffsziele zu bekommen. [44] Aber auch Marketingabteilungen können die gesammelten Daten verwenden um die Dienste und Services sowie Produkte direkt an den Konsumenten anzupassen, auf dies wird genauer im Kapitel 4.9 „*Marketing Intelligence*“ eingegangen. OSINT-Daten sind von Personen oder Unternehmen öffentlich gestellte Informationen ohne Anspruch auf Schutz der Privatsphäre. [45]

Die Vorteile von OSINT sind, dass wenig Risiko besteht, um an Daten zu kommen. Wenn Daten von einer Person oder einem Unternehmen zur Verfügung gestellt werden ohne einen Schutz dieser Daten, dann können diese Informationen von jeder Person verwendet werden.
Somit ist es nicht mehr notwendig vor Ort nach den Informationen zu suchen, sondern es können die Informationen aus öffentlichen Quellen genommen werden. Weiters ist es eine sehr kostengünstige Variante, um an Informationen zu kommen, im Vergleich zu anderen Datenerfassungsmethoden oder Datenerfassungsquellen.

Ein großer Vorteil ist die leichte Zugänglichkeit zu den Daten, egal wo man sich befindet, ist es möglich sich die aktuellsten Informationen anzuschauen.
Auch Finanzermittler können sich an den OSINT-Informationen bedienen, da es dadurch ermöglicht wird Steuerhinterziehung durch das Überwachen der Social Media Konten zu erkennen.

Da es in der heutigen Zeit immer mehr gefälschte Waren Online zu kaufen gibt, kann OSINT hier auch ein unterstützendes Thema sein. Es können somit gefundene „Fake-Shops“ gesperrt werden.

Ein weiterer Vorteil von OSINT ist das Aufrechterhalten der nationalen Sicherheit sowie der politischen Stabilität. Durch das Einsetzen von OSINT in einem Land, kann genauer auf die Bedürfnisse der Menschen eingegangen werden, da man sich eine Übersicht über deren Bedürfnisse bilden kann und somit schneller darauf reagieren kann. Somit ist es möglich auf Konflikte schneller zu reagieren oder an die Bevölkerung eine rasche Warnung abzugeben.
Ebenso ist das Teilen von OSINT-Informationen möglich. Da diese Informationen öffentlich und frei zugänglich sind, besteht keine Sorge wegen dem Urheberschutz. [46]

4.2. Open Source Intelligence Cycle

Der bildlich dargestellte “Cycle” in Abbildung 1 „*Intelligence Cycle*“ soll als Veranschaulichung gelten, um den Prozess hinter dem Begriff “OSINT” zu beschreiben. Dieser Cycle besteht aus 6 verschiedenen Phasen.
Die United States Intelligence Community verwendet einen 5 Schritte-Cycle, da hier das “Feedback” weggelassen wird. Da Feedback jedoch ein wichtiger Punkt ist, womit eine kontinuierliche Verbesserung durchgeführt werden kann, wurde der 6 Schritte-Cycle beschrieben. [47] [48]

Dieser Cycle soll den Prozess von OSINT und dessen benötigte Schritte beschreiben, welche benötigt werden, um eine Daten- und Informationssammlung durchzuführen. Der Zyklus der Informationsbeschaffung ist ein wichtiger Prozess, da dieser dazu dient um aus Rohdaten, fertige Informationen zu erstellen. Hier sind die unten angeführten Schritte zu beachten, welche einen Informationsbeschaffungs-Zyklus ausmachen. [49]

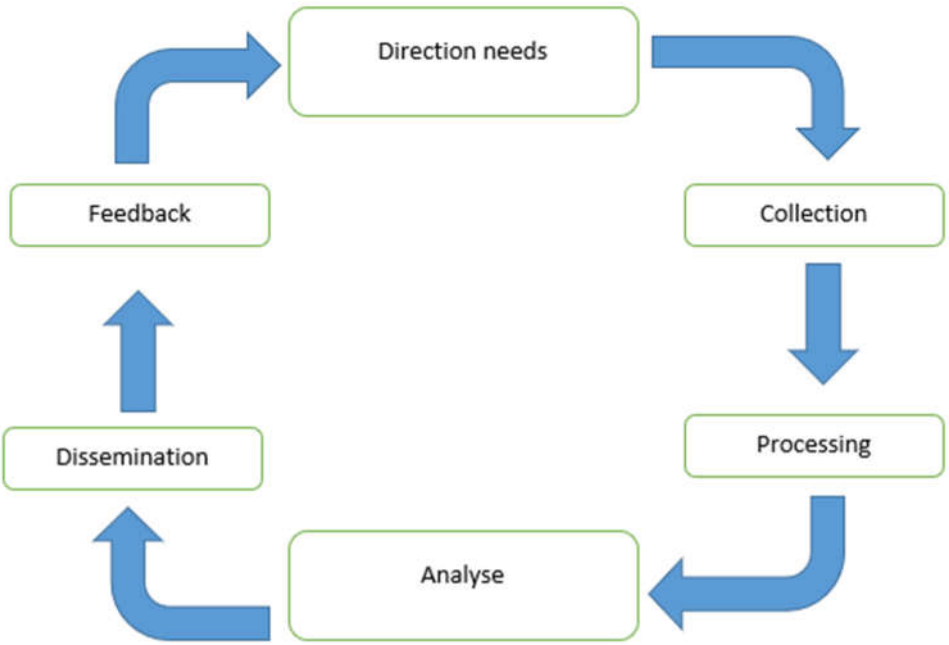


Abbildung 1 Intelligence Cycle

- **Direction needs**: In der Phase “Direction needs” befinden sich noch weitere Punkte wie beispielsweise “Planung” und “Requirements”. Diese Phase dient dazu, um die Anforderungen vom Entscheidungsträger festzulegen, damit das gewünschte Ziel erreicht werden kann. Dazu muss gewusst werden, woher Daten gesammelt werden können. Daher müssen potenzielle Quellen durchsucht werden, welche die benötigten Informationen enthalten können. Hier wird der Anfang und das Ende des Zyklus bestimmt, da für den Anfang bestimmte Erhebungsanforderungen erstellt werden und für das Ende wird aus den erhobenen Informationen eine fertige Intelligenz erwartet, welche eine Entscheidung unterstützt. [50]

- **Collection (Harvesting)**: Die Phase “Collection” kann erst begonnen werden, wenn definiert worden ist, welche Daten über ein Ziel benötigt werden und auf welches Ziel der Fokus gelegt wird. Dies ist eine sehr wichtige Phase, da es Unterschiede von den benötigten Informationen gibt, je nach der Art des Ziels. Hier ist es wichtig viele verschiedene Informationen (Rohdaten) zu sammeln aus den verschiedensten öffentlichen frei zugänglichen Quellen, die für eine fertige Intelligenz benötigt werden.

- **Processing**: In der Phase “Processing” müssen die gesammelten Informationen im Detail überprüft werden, bevor die Daten zu einer weiteren Analyse weitergegeben werden. Hier müssen die Informationen beispielsweise übersetzt, entschlüsselt und interpretiert werden. Somit wird eine bessere Datenqualität für die Verarbeitung gegeben.

- **Analyse**: Die Phase “Analyse” dient dazu um die übersetzten, entschlüsselten und interpretierten Daten zu analysieren. Eine Analyse der Daten ist notwendig, da diese oft widersprüchlich oder fehlerhaft sind. Daher müssen Spezialisten die Relevanz, Zuverlässigkeit und Gültigkeit dieser Daten prüfen. Somit können anschließend die Daten miteinander verbunden werden, womit diese ein Ganzes ergeben und als intelligente Informationen dienen. Hier müssen einerseits die Daten integriert werden aber andererseits auch eine Auswertung der Daten stattfinden. Somit können die Daten mittels eines OSINT-Tools aufbereitet werden und eine Analyse der Daten durchgeführt werden. Es werden die Basisdaten in fertige Intelligenz umgewandelt.

- **Dissemination**: In der Phase “Dissemination” findet die Verteilung der fertigen Intelligenz an den Verbraucher statt. Diese Informationen können dann an bestimmte Gruppen/Organisationen/Personen/Abteilungen verteilt werden.

- **Feedback**: In der Phase “Feedback” sollte ein Gespräch und eine Überprüfung mit dem Auftraggeber stattfinden ob die Daten, welche gesammelt wurden genügen, um das Ziel zu erreichen oder ob weitere Schritte notwendig sind.

Es sind im Internet verschiedene Definitionen über OSINT vorhanden, relativ umfangreich wird es von dem Buch “OSINT in the Context of Cyber-Security" [51] erklärt. Hier wird OSINT als ein Prozess aus unterschiedlichen Tätigkeiten beschrieben wie beispielsweise der Sammlung und Analyse von öffentlich verfügbaren Informationen:
“the scanning, finding, collecting, extracting, utilizing, validation, analysis, and sharing intelligence with intelligence-seeking consumers of open sources and publicly available data from unclassified, non-secret sources” (Fleisher 2008; Koops et al. 2013)

Generell muss gesagt werden, dass der Begriff OSINT folgende Unterpunkte beinhaltet: Scannen, Finden, Sammeln, Extrahieren, Verwendung, Validierung, Analyse und der Austausch von Erkenntnissen. Dies dient dazu, um die Daten von den Bedrohungen so aufzubereiten, damit diese auch bei einem Austausch leicht weiterverwendet werden können. [Quelle190818x16329]

OSINT Informationen können für unterschiedliche Anwendungsgebiete eingesetzt werden [52]:

- “Offensive”: Darunter wird eine Art von Informationsbeschaffung verstanden, welche auch unter dem englischen Begriff “Information Gathering” bekannt ist. Dieser Schritt dient zur Beschaffung von öffentlich frei zugänglichen Informationen und kann in weiterer Folge auch zur Vorbereitung einer Attacke dienen. Diese Phase wird in Abbildung 2 „*Cyber Kill Chain*“ dargestellt und ist auch als Reconnaissance Phase bekannt.

- “Defensive”: OSINT Informationen können bei der Abwehr von Cyber Attacken behilflich sein. Es wird von verschiedenen Organisationen angeboten kostenlos oder auch kostenpflichtig Informationen zu verteilen und bereit zu stellen. Diese geteilten Informationen können einem Unternehmen das Wissen und die Informationen bieten, um die Abwehr von Cyber Attacken zu verbessern. Dazu gibt es weiters eine Cyber Kill Chain mit sieben Phasen, welche in der Abbildung 2 „*Cyber Kill Chain*“ zu sehen sind. Hier wird versucht die Attacke bereits in einer Anfangsphase abzuwehren, womit der Schaden durch den Angriff verringert werden kann [QUELLE].

Die Charakteristik von OSINT Informationen sind unstrukturierte Informationen. Diese Informationen und Daten können von unterschiedlichen öffentlich frei zugänglichen Quellen empfangen werden [Quelle190818x1629].

Anschließend werden verschiedene Beispiele von OSINT Informationen aufgelistet. Diese Beispiele von OSINT-Informationen dienen dazu, um erste Erfahrungen und Erkenntnisse über das Ziel zu erlangen:

• Name einer Person	• Telefonnummer
• E-Mail-Adresse	• Username
• Meta-Daten	• Wohnadresse (physikalische Adresse)
• IP-Adresse	• Domain
• Sensitive Informationen (Zugangsdaten)	• Standorte
• Ports	• Freunde
• Posts auf Social Media Plattformen	

Tabelle 3 OSINT Informationen

Das Sammeln und Speichern von diesen gefundenen Informationen über das Ziel ist ein wichtiges Verfahren. Mit diesen gesammelten Informationen können Angriffe gezielter durchgeführt werden. Umso mehr Informationen gesammelt werden können, desto besser kann ein Angriff geplant und durchgeführt werden.

Es gibt verschiedene OSINT Typen [46], welche in dem nachfolgenden Absatz genauer beschrieben werden:

- **Internet**: Das Internet bietet unterschiedliche Arten an, um an verschiedenste Informationen zu gelangen. Es gibt eine Vielzahl von Blogs, Foren sowie Verteilungsdienste wie YouTube oder Facebook.

- **Massenmedien**: Ein weitverbreitetes Spektrum zur Übertragung von Informationen ist das Fernsehen und Radio. Damit können viele Personen erreicht werden.

- **Geolocation**: Durch die heutigen Technologien ist es ebenso möglich mittels Google-Maps genaue Standorte fest zu stellen.

- **Fotos/Videos**: Eine weitere Möglichkeit ist auch das Extrahieren von Metadaten von Fotos und das Sammeln dieser Informationen.

4.3. OSINT und Threat Intelligence

Klassische Indikatoren, Indicator of Compromise (IoC) haben meist wenig Entscheidungsgrundlage, da diese meist nur wenige Informationen besitzen oder lose und ohne Zusammenhänge verarbeitet werden. Weiters haben sich in diesem Bereich verschiedene Begriffe etabliert, welche in diesem Kapitel im Detail beschrieben werden. Ebenso erfolgt eine Beschreibung der einzelnen Threat Intelligence Plattformen, womit ein prononcierter Überblick der aktuellen Plattformen gegeben werden, welche in Kapitel 2 „*Background*“ beschrieben sind.

Im Bereich der Computer-Forensik wird von klassischen Indikatoren gesprochen, welche auch als Indicator of Compromise (IoC) bezeichnet werden. [53] IoCs enthalten ein “Artefakt” einer Bedrohung, welches in einem IoC beschrieben wird und IoCs werden meist durch eine Cyberattacke als Incident erstellt, indem ein stattgefundener oder versuchter Angriff analysiert wird. Die Erkenntnisse und die gefundenen Merkmale werden als “Artefakte” in IoC beschrieben, beispielsweise zählen darunter Hash-Werte oder IP-Adressen. Auch bei den passiven Tools können IoCs verwendet werden, die bereits durch andere Organisationen beschrieben wurden und von passiven Tools heruntergeladen werden, um Attacken im Unternehmen aufzuspüren oder proaktiv abzuwehren.

Es werden bei IoC im Bereich von Threat Intelligence Information kontextuelle Erweiterungen hinzugefügt, welche durch STIX standardisiert beschrieben werden. Damit wird eine Bedrohung lesbar und kann auch automatisiert verarbeitet werden. Durch diese einheitliche Beschreibung der Informationen, können diese auch weitergegeben werden an Personen oder Unternehmen, dies wäre beispielsweise mit TAXII möglich.
Cyber Threat Intelligence (CTI) Informationen oder auch Threat Intelligence (TI) sollen gegenüber den klassischen Indicator of Compromise (IoC) eine neue Möglichkeit darstellen, um Bedrohungen zu beschreiben und diese rasch zu verteilen. Dabei versucht TI wesentlich mehr Informationen zu sammeln, zu speichern und die Beziehung zwischen den Informationen herzustellen als IoC. Daher wird der Einsatz von Threat Intelligence Informationen immer wichtiger, da diese mehr Informationen und Details als klassische IoCs anbieten können. [54]

Es muss unterschieden werden zwischen **IoC** (Indicators of Comprimise) und **IoA** (Indicators of Attack). Unter dem Begriff IoC wird eine kontextuelle Erweiterung eines Angriffes und deren Artefakte verstanden, womit eine Beschreibung einem Angriff beigefügt wird. Bei IoA wird versucht, die Absichten eines Angreifers zu erkennen, unabhängig davon was bei dem Angriff für Schadsoftware oder Code verwendet worden ist. Es wird hier gezeigt, wie ein Angreifer vorgegangen ist, um sich Zugriff auf das System zu verschaffen, aber auch wie die Kennwörter gespeichert und die Daten anschließend gefiltert worden sind. Bei IoC fallen Begriffe wie Malware, Signaturen, Exploits, Vulnerabilitäten und IP-Adressen darunter. Bei IoA fallen Begriffe wie Code Execution, Persistance, Stealth, Command Control und Lateral Movement darunter. [55] [56]
Es kann zwischen Tools der Erzeugung und Verwendung von Threat Intelligence Informationen unterschieden werden. Bei den Tools der zur Verwendung von TI-Informationen werden immer häufiger sogenannte TI-Plattformen (TIP) eingesetzt [QUELLE SANS].

Die Beschreibungen von Threat Intelligence und OSINT ist ein wichtiger Aspekt in dieser Thematik. Wichtige Begriffe im Bereich von OSINT sind:

- OpenIOC (Open Indicator of compromise)
- STIX (Structured Threat Information eXpression)
- MISP (Malware Information Sharing Plattform)
- TAXII (Trusted Automated eXchange of Intelligence Information)
- OTX (Open Threat Exchange)

Hier werden zwischen Tools zur Beschreibung und Verwendung unterschieden, diese werden in Kapitel 2 „*Background*“ genauer beschrieben. OpenIOC und STIX sind Sprachen zur Beschreibung und Verknüpfung unterschiedlicher OSINT Informationen zur Erstellung von Threat Intelligence Informationen. Es dient dazu, um es für Maschinen und Menschen lesbar zu machen.
OTX und MISP sind Plattformen, über welche bereits fertige Sammlungen und verknüpfte OSINT Informationen über bestimmte Attacken und Bedrohungen heruntergeladen und verteilt werden können.

Die im Kapitel 2 „*Background*“ beschriebenen TI-Plattformen werden anschließend anhand einer Tabelle verglichen.

Tools	Kosten der Plattform	Kosten der Feeds	Import-Format	Export-Format	Suchmöglichkeiten	Cloud-Unterstützung
MISP	kostenlos	kostenlos	MISP-JSON, JSON, CSV	MISP-JSON, CSV, JSON	Es wird ermöglicht die Feeds über die API zu durchsuchen	Nein
OTX	kostenlos	kostenlos	E-Mails, PDF, Log-Dateien, OpenIOC, STIX	JSON, CSV, STIX, OpenIOC	Es können Indikatoren gesucht werden, sowie eine Textzeichenfolge verwendet werden	Nein
X-Force Exchange	kostenlos	kostenlos*	in der Verwendeten kostenlosen Version gab es keine Möglichkeit einen Import durchzuführen	STIX 1.x und 2.x	Es können Indikatoren sowie nach CVE gesucht werden	Ja

Tabelle 4 TI-Plattformen

*es können im Monat 5000 Datensätze kostenlos abgefragt werden

4.4. Cyber Kill Chain

Die Cyber Kill Chain [57] [58] [59] [60] besteht aus mehreren Ketten und jeder Teil dieser Kette bildet eine Phase. Es werden weiterfolgend die verschiedenen Phasen der Kette erklärt und im Detail beschrieben.

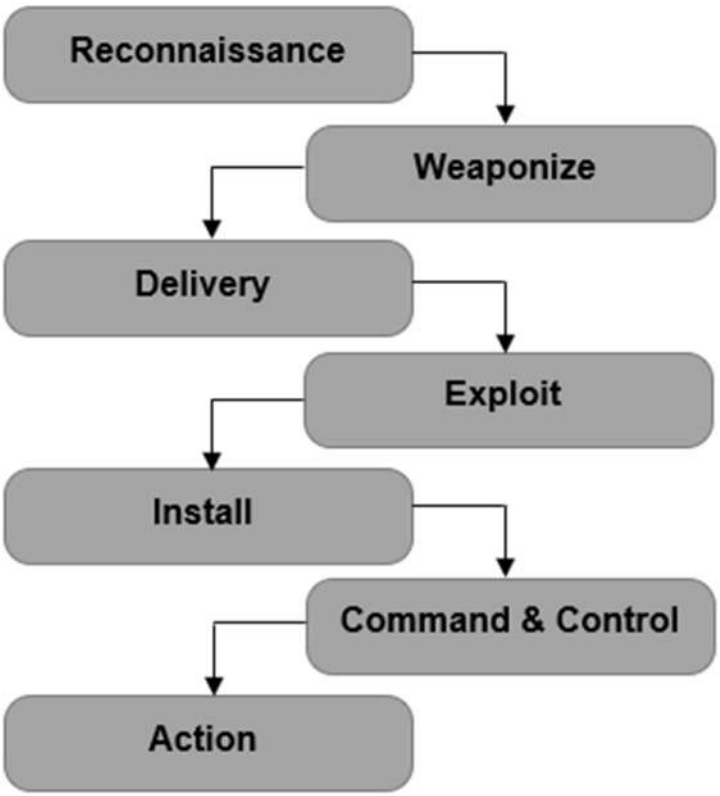


Abbildung 2 Cyber Kill Chain

1) **Reconnaissance (Aufklärung)** – In dieser Phase werden verschiedene Daten über das Ziel gesammelt, ein Ziel kann eine Person oder ein Unternehmen sein. Diese Phase beinhaltet das Durchsuchen von verschiedenen öffentlich zugänglichen Seiten wie Blogs, Social Media Plattformen, Webseiten und Mail-Listen, um Informationen über das Ziel zu erlangen. Diese Daten sind für die weiteren Phasen von großer Bedeutung. Durch diese Phase werden die Informationen gesammelt und gespeichert, um zu bestimmen, wie das Ziel angegriffen werden kann und ob Sicherheitslücken gefunden werden können.

   Es kann hier aber noch unter zwei verschiedenen Varianten unterschieden werden:
   - Passive Reconnaissance bedeutet, dass Daten über das Ziel gesammelt werden, ohne dass das Ziel es mitbekommt. Hierzu zählen Informationen wie Domain Name, Social Netzwerke oder öffentliche Dokumente.
   - Active Reconnaissance bedeutet, dass schon im Detail Informationen über das Ziel gesucht werden und die Möglichkeit besteht, dass das Ziel dies mitbekommt. Hierzu zählen Informationen wie Fingerprints, Port Scanning, Spam-Nachrichten oder Phishing Mails.

   Gegenmaßnahmen: Die Angriffsfläche kann minimiert werden, indem öffentliche Informationen verringert werden. Es können verdächtige Suchaktivitäten ausgewertet werden.

2) **Weaponize (Bewaffnen)** – Hier wird von einem Angreifer versucht mit den Informationen, welche in der Reconnaissance Phase gespeichert wurden, einen Angriff vorzubereiten und die Schwachstellen des Zieles zu finden. Der Angreifer versucht in dieser Phase mittels einem Remote Access Tool sich einen unbemerkten Zugang zu dem Ziel zu verschaffen. Wenn der Angreifer einen unbemerkten Zugang hergestellt hat, ist es möglich Ergebnisse über das beispielsweise positive Eindringen zu dem Ziel zurückzugeben. Exploits von Betriebssystemen oder Programmen sind in dieser Phase sehr wichtig, da somit der Angriff und die „Bewaffnung" aufgebaut werden können.

   Gegenmaßnahmen: Es kann auf mögliche Angriffsversuche geachtet werden. Weiters können die Systeme auf Malware überprüft werden.

3) **Delivery (Bereitstellung)** – Die Delivery Phase ist das Herzstück der Kette, da sie für das erfolgreiche Durchführen eines Angriffes zuständig und verantwortlich ist. In dieser Phase werden potenzielle Informationen über das Ziel benötigt, um einen Angriff erfolgreich zu planen und durchführen zu können. In den meisten Fällen ist es nötig, dass vom Ziel eine Interaktion durchgeführt werden muss, damit ein geplanter Angriff erfolgreich ist. Hierfür müssen beispielsweise Links oder Dateien geöffnet werden, welche mit einem bösartigen Code versehen sind. Weiters wäre ein Angriff über „E-Mail Anhänge", „Phishing Angriffe", „Downloads" und „USB/Festplatten“ möglich. So könnte beispielsweise ein USB-Stick bei einem Unternehmen absichtlich “vergessen” werden, diese enthält allerdings einen Schadcode, welcher sich beim Verbinden mit dem Computer verbreitet. Ebenso bei Downloads können Schadcodes hinter einem falschen Namen versteckt werden. Weiters können Phishing Attacken und E-Mail-Anhänge mit einem Schadcode versendet werden. Wenn der Anhang ausgeführt wird, verbreitet sich der Schadcode auf dem PC.

   Gegenmaßnahmen: Es können mittels Tools Angriffswege überwacht werden. Es können mögliche Angriffe als Beispiel hergenommen werden, um die Systeme dagegen abzusichern.

4) **Exploit** – In dieser Phase hat das Ziel einen der zuvor erwähnten Angriffe ermöglicht. Somit ist es dem Angreifer möglich, Zugriff auf das System des Ziels zu bekommen. Damit ein Exploit funktioniert, müssen einige Bedingungen erfüllt sein. Das Ziel muss die Software oder das Betriebssystem verwenden für welches der Exploit gilt. Es dürfen keine Updates oder Versionsänderungen durchgeführt werden, da ansonsten möglicherweise der Exploit behoben worden ist. Zuletzt darf der mögliche Virenscanner eines Ziels den Exploit nicht erkennen. Es ist möglich Online auf der CVEs-Seite [61] (Common Vulnerabilities and Exposure) zu schauen, welche Exploits aktuell sind.

   Gegenmaßnahmen: Mittels Schulungen können die User sensibilisiert werden, damit diese keine „nicht vertrauensvollen“ Links oder Daten öffnen.

5) **Install** – Die Install Phase hat sich in den letzten Jahren stark weiterentwickelt. Dies ist ersichtlich an den Hostbasierten-Sicherheitsmaßnahmen IDS (Intrusion Detection Systems), welche vermehrt in Einsatz kommen. Der Angreifer versucht in dieser Phase eine Malware zu installieren um eine „Backdoor" (Hintertür), was ein alternativer Zugang zu einer Software bedeutet, herzustellen. Es werden von Angreifern „Dropper“ oder „Downloads“ verwendet, um Zugriff auf das Ziel zu bekommen. Mittels einem „Dropper“ welches ein selbst ausführbares Schadprogramm ist, werden die benötigten Funktionen auf dem Ziel installiert. Es wird weiters versucht die Sicherheitskontrollen am Ziel zu überlisten, damit der Angriff nicht erkannt wird.

Gegenmaßnahmen: Es werden die Installationen von den Usern kontrolliert. Weiters werden Aktivitäten der User und Berechtigungen kontrolliert. Wenn verdächtige Handlungen ersichtlich sind, können diese sofort gesperrt werden.

6) **Command & Control** – Hier wird vom Angreifer versucht, Kommunikationskanäle zu finden und diese zu öffnen. Dadurch wird es dem Angreifer ermöglicht auf das Ziel von der Ferne zuzugreifen. Damit ist es dem Angreifer möglich, verschiedene Befehle auszuführen, um Daten und Informationen von dem Ziel zu speichern.

   Gegenmaßnahmen: Es werden die Kommunikationskanäle überprüft ob verdächtige Kanäle offen sind. Weiters können Malware Aktivitäten untersucht werden.

7) **Action** - In dieser Phase wird von dem Angreifer probiert, weitere Zugänge oder Berechtigungen von dem Ziel zu bekommen Damit können in weiterer Folge Dateien zerstört oder kopiert und somit gespeichert werden.

   Gegenmaßnahmen: Es werden nach User-Interaktionen gesucht, welche verdächtig sind. Weiters können forensische Untersuchungen und Analysen durchgeführt werden. Im Falle eines Angriffes wird ein Notfallprogramm eingeleitet, welches den Schaden eindämmen kann.

Jede dieser Phasen hat einen Zusammenhang zu einer oder mehreren Phasen. Die Phase 1 (Recon), 2 (Weaponize) und 3 (Deliver) hängen zusammen und dienen dazu, dass Angreifer die Vorteile einer schwachen Sicherheit bei dem Ziel nutzen. Damit dies nicht geschieht, sollten möglichst wenige Informationen über Systeme öffentlich verfügbar sein. Um dies zu verhindern besteht die Möglichkeit Angriffsversuche und Angriffswege zu prüfen und zu beheben.

Bei den Phasen 3 (Deliver) und 4 (Exploit) werden vom angegriffenen Ziel keine Warnungen vom Intrusion Detection System (IDS) bemerkt.
Um dies zu verhindern sollte das Unternehmen auf Schwachstellen überprüft werden und diese beseitigt werden. Hierfür können beispielsweise CVE (Common Vulnerabilities and Exposures) Meldungen durchsucht werden und mit den Systemen, welche im Unternehmen im Einsatz sind, verglichen werden.

In den Phasen 3 (Deliver), 4 (Exploit) und 5 (Install) ist es dem Angreifer möglich, durch die nicht herausgegebenen Warnungen unentdeckt auf dem Zielsystem in sensible Bereiche des Systems zu gelangen. Es können in dieser Phase Installationen von Usern protokoliert werden, damit können verdächtige Installationen erkannt werden.

In Phase 6 (Command & Control) und 7 (Action) werden von dem angegriffenen System die Meldungen des Intrusion Detection System (IDS) verfehlt, somit kann der Angreifer ungehindert Daten von dem Ziel speichern. Um dies zu verhindern ist es wichtig zu überprüfen ob Kommunikationskanäle geöffnet worden sind, welche nicht benötigt werden.

4.5. Reconnaissance Phase

In diesem Abschnitt wird im Detail auf die Reconnaissance Phase [57] eingegangen, welche für das Information Gathering zuständig ist. Diese Phase ist die grundlegendste Phase, um Informationen über ein Ziel zu bekommen und zu speichern. Diese Informationen werden für die weiteren Phasen des Cyber Kill Chain benötigt. In dieser Phase werden die im Internet, frei öffentlich zugänglichen Informationen über ein Ziel gesammelt und gespeichert. Hier passiert die “Identifikation”, “Auswahl” sowie das “Profiling“ von dem Ziel.

Das Modell hilft einem Incident Response Team, da durch das Cyber Kill Chain Framework die Möglichkeit besteht, einen Angriff in verschiedene Phasen zu gliedern. Das Framework besteht aus sieben verschiedenen Phasen, welche im nächsten Kapitel 4.4 „*Cyber Kill Chain*“ im Detail beschrieben und analysiert werden. Dadurch können Angriffe in kleineren Phasen analysiert und vorbereitet werden. Dies ist sehr hilfreich von der Angreifer-Sicht sowie von der Defensiven-Sicht.

In der Reconnaissance Phase werden verschiedene Informationen über ein Ziel gesammelt. Unter einem Ziel können Unternehmen sowie Personen verstanden werden.
In dieser Phase werden anschließend verschiedene öffentliche und frei zugängliche Informationen von verschiedenen Quellen über das Ziel aus dem Internet gesammelt. Vor einem Angriff müssen möglichst viele Informationen über ein Ziel gesammelt werden. Diese Informationen müssen anschließend auf die Gültigkeit und Korrektheit geprüft werden, daher ist diese Phase eine der langandauerndsten Phasen, da hier auch viele falsche Informationen gesammelt werden, welche aussortiert werden müssen. Ebenso muss auf die Quellen geachtet werden, welche für die Suche verwendet werden.

In der Reconnaissance Phase muss zwischen zwei verschiedenen Arten von Informationsgewinnung unterschieden werden, da es “passive” und “aktive” Scans gibt.
Es besteht durch OSINT gegenüber den anderen verfügbaren Tools ein Vorteil, da es in die Kategorie des passiven Information Gathering der Reconnaissance Phase eingestuft wird. Das bedeutet, dass es sich hierbei um ein “leises” (passives) Sammeln von Informationen über das Ziel handelt. Durch den passiven Scan wird keine direkte Beziehung gegenüber dem Ziel hergestellt. [62] Bei einem “lauten” (aktives) Sammeln von Informationen, wie zum Beispiel bei einem Port-Scan, wird eine Beziehung gegenüber dem Ziel hergestellt, somit bekommt dieser das Sammeln mit.
Es ist wichtig, dass bei einem aktiven Scan die Einwilligung des Unternehmens gegeben ist, da es ansonsten als Angriff zählt und strafbar ist. Bei der Verwendung eines passiven OSINT-Scans wird eine solche Einwilligung nicht benötigt, da die Informationen aus dem Internet gesammelt und gespeichert werden, welche mit dem Scan erhältlich sind.
Diese gefundenen Daten können von verschiedenen Personen durch deren aktiven Scans zur Verfügung gestellt werden und anschließend, durch den passiven Scans gesammelt werden, daher bekommt das Ziel ein Tracken nicht mit, da es ein “leiser” Angriff ist.

Um einem Angreifer diese Phase schwerer zu machen, kann mit OSINT-Tools überprüft werden, welche Informationen von einer Person oder einem Unternehmen nach außen verfügbar sind.
Es sollten keine Informationen über Personen wie beispielsweise E-Mail-Adressen sowie deren Name öffentlich verfügbar sein sowie deren Positionen in einem Unternehmen. Weiters sollten keine Informationen über Systeme und deren Software-Versionen sowie deren Patch-Level ersichtlich sein.

Port-Scan Erklärung [63]:
Bei einem Port-Scan wird überprüft, welche Ports in einem Netzwerk offen sind. Diese Art von Scan fällt unter die Kategorie “aktive” Scans. Mit dem Wissen über offene Ports in einem Netzwerk können Angriffe besser vorbereitet werden und helfen somit einem Angreifer.

Incident Response Team Erklärung [64]:
Ein Incident Response Team kann dabei helfen, verschiedene Arten und Auswirkungen von möglichen Bedrohungen auf das Unternehmen zu verringern. Durch dieses Team können Reaktionen auf mögliche Vorfälle gebildet werden. Es werden weiters Sicherheitsverletzungen analysiert und dementsprechende Maßnahmen oder Sicherheitsmaßnahmen ergriffen. Generell besteht ein Team aus einem “Manager”, “Sicherheitsanalysten” und “Bedrohungsforschern”.

4.6. Vorteile/Nachteile von OSINT

In diesem Abschnitt werden einige Vorteile aber auch deren Nachteile bei der Verwendung von OSINT dargestellt. Mit OSINT können einige positive Eigenschaften erzielt werden, diese positiven Vorteile bringen jedoch auch ihre Nachteile mit sich. [38] [65] [66]

Zuerst wird auf die positiven Eigenschaften von OSINT eingegangen. OSINT ermöglicht Personen, auf eine einfache Art und Weise das Sammeln von Daten und Informationen über ein Ziel. Ein weiterer Vorteil von OSINT ist, dass die Daten, die gefunden werden können, speicherbar und anschließend verfügbar sind. Das heißt, nachdem eine Suche stattgefunden hat, können diese Daten gespeichert und für Analysezwecke weiterverwendet werden. Das Teilen von den gesammelten Daten und Informationen ist mit OSINT sehr leicht, da es wenige Sicherheitsbeschränkungen gibt, außer Lizenzen und Urheberrecht, welches beachtet werden muss. Dementsprechend können die Daten schnell geteilt werden. OSINT ist eine sehr kostengünstige Variante, um Daten und Informationen zu sammeln. Es müssen bei OSINT keine menschlichen Handlungen wie beispielsweise bei HUMINT durchgeführt werden, welches ein persönliches Risiko mit sich mitbringen kann. Daher ist es eine sichere Variante für jede Person, da verschiedene Informationen über das Internet abgefragt werden können und somit kein persönliches Risiko besteht. Weiters ist es eine sehr vertrauenswürdige Methode, da jegliche Daten, welche gesammelt werden, beispielsweise auf Autor oder deren Quellen überprüft werden, um die Daten validieren zu können. Eine sehr wichtige Eigenschaft ist, dass die Informationen und Daten jederzeit und überall verfügbar sind. Es können mittlerweile die Informationen und Daten auch schon mobil gesammelt und verteilt werden. Ebenso können diese gefundenen Informationen für eine nationale Sicherheit sorgen und für eine Unterstützung einer langfristigen Strategie verwendet werden. Weiters können OSINT-Daten und Informationen auch für die Kontrolle der Unternehmenssicherheit verwendet werden.

Jedoch gibt es nicht nur positive Eigenschaften bei der Verwendung von OSINT. Einer der wesentlichen Nachteile im Bereich von OSINT sind die Mengen an Daten, welche zugänglich sind, wodurch es unmöglich wird, dass alle relevanten Informationen abgerufen werden können. Durch die großen Mengen an Daten ist der nächste kritische Punkt der Speicherverbrauch, dieser wird dadurch immer größer.
Es wird die Suche nach relevanten Informationen dadurch erschwert, da möglicherweise kein Überblick mehr besteht. Bevor die Daten verwendet werden können, wird viel Zeit benötigt, um diese Daten zu analysieren und zu korrigieren. Ein weiterer Kritikpunkt sind die möglicherweise falschen Informationen, welche bei einer umfassenden Analyse aussortiert werden müssen. Es besteht weiters die Möglichkeit, dass sich gefundene Quellen und Informationen ändern.

Die Tabelle 5 „*Tabelle 5 Vorteile und Nachteile* von OSINT“ gibt in die Vorteile und Nachteile bei der Verwendung von OSINT in einer Übersichtlichen Art wieder, welche oben beschrieben worden sind.

Vorteile	**Nachteile**
Einfaches Sammeln von Informationen/Daten	Menge
Verfügbarkeit	Speicherverbrauch
Speicherbarkeit	Suche
Wenige Sicherheitsbeschränkungen	Zeit für das Analysieren/Bereinigen
Schnelle Datensammlung	Falsche Informationen
Kostengünstig	Quellen und Informationen können sich ändern
Sicheres Verfahren für Personen	
Vertrauenswürdige Methode	
Jederzeit abrufbar/verfügbar	
mobil	
Sicherheit für ein Unternehmen	

Tabelle 5 Vorteile und Nachteile von OSINT

4.7. Einsatzgebiete

In diesem Kapitel werden verschiedene Einsatzgebiete von OSINT beschrieben. Es soll damit gezeigt werden, in welchen Gebieten es bereits aktiv ist und als unterstützende Methode eingesetzt wird.

Anschließend werden verschiedene Bereiche aufgelistet, welche OSINT sowie dessen Tools verwenden um, für die Einsatzgebiete Informationen sammeln. [4]
In dem Bereich von Penetration Tests [67] werden verschiedene Informationen über beispielsweise Infrastrukturen oder Webseiten gesucht. Diese Informationen müssen sortiert und analysiert werden. Hierbei können OSINT-Tools helfen, womit Informationen sauber aufbereitet werden können. Es gibt verschiedene Tools wie beispielsweise “Sublist3r” mit denen es ermöglicht wird, Angriffsbereiche grafisch abzubilden, dieses Tool kann auf GitHub [42] heruntergeladen werden. Ebenso ist OSINT in der Cyber Kill Chain ein integriertes Modell. Es wird als Defensive-Methode verwendet, um mögliche Angriffe durch die gewonnenen Informationen frühzeitig zu stoppen. Es können verschiedene OSINT-Informationen mit unterschiedlichen Tools wie beispielsweise Maltego, TheHarvester und Spiderfoot gefunden werden. Diese gefundenen Daten können für weitere Analysen in einem Unternehmen verwendet werden, um dieses zu schützen und Schwachstellen zu finden und diese zu schließen.
Ebenso ist OSINT ein kaum wegzudenkendes Gebiet bei ethischem Hacken. Hier können von “friedlichen” Angreifern verschiedene Scans durchgeführt werden, um ein Unternehmen auf mögliche Schwachstellen zu überprüfen. Hier können mögliche veraltete Versionen oder Geräte erkannt werden, welche von einem Angreifer/Angreiferin für einen Angriff verwendet werden können.

Anbei werden einige OSINT-Tools gelistet, welche es ermöglichen Informationen, welche in Kapitel 6 „*Evaluierung von den Tools*“ beschrieben werden, zu sammeln. Es wurden diese Tools gewählt, da diese bereits vorinstalliert auf virtuellen Maschinen vorhanden sind. Somit müssen keine weiteren Handlungen wie beispielsweise Installationen oder Updates von Person durchgeführt werden, um eines dieser Tools zu verwenden.

- Maltego
- TheHarvester
- Spiderfoot
- Recon-NG
- Shodan
- Tinfoleak

Im Internet werden verschiedene Thread Intelligence Open Source Plattformen angeboten, welche kostenlos im Unternehmen eingesetzt werden können. Die Verwendung dieser Tools sorgen in einem Unternehmen für einen proaktiven Schutz gegen Cyberattacken und können für eine rasche Verteilung von Bedrohungen eingesetzt werden. Diese Thread Intelligence Plattformen sind genauer in Kapitel 2 „*Background*“ sowie in 4.3 „*OSINT und Threat Intelligence*“ beschrieben:

- MISP
- OTX
- X-Force Exchange

Diese Plattformen greifen auf eine Community zurück. An dieser Community können sich Menschen aus der ganzen Welt beteiligen und Bedrohungsinformationen über diese Tools verteilen. Das Ziel der Plattformen ist es, einen proaktiven Schutz für ein Unternehmen zu schaffen. Daher wird versucht, Bedrohungen so rasch wie möglich, an möglichst viele Menschen, Unternehmen oder Abteilungen zugänglich zu machen. Dementsprechend können Unternehmen auf diese Bedrohungsinformationen reagieren und einen Schutz der eigenen Infrastruktur gegen diese Bedrohung etablieren.

4.8. Intelligence Collections und Angriffsarten

In diesem Kapitel werden verschiedene Arten von Angriffen und Intelligence Collections aufgelistet und beschrieben [48] [68] [69] [70].

Intelligence Collections:

- **HUMINT**: Der Begriff HUMINT bedeutet Human Intelligence (menschliche Intelligence). Darunter ist das Sammeln von diversen Informationen aus menschlichen Quellen zu verstehen. Hier können Daten, Informationen von Posts oder Fotos gesammelt werden.

- **IMINT**: Unter dem Begriff IMINT ist Imagery Intelligence zu verstehen. Das bedeutet es werden verschiedene Informationen über Satellitenbilder sowie Bilder von Luftaufnahmen gesammelt.

- **MASINT**: Hinter diesem Kürzel “MASINT” steckt der Begriff Measurement and Signatures Intelligence. In diesem Begriff stecken einige weitere Unterbegriffe wie RADINT (Radar Intelligence), ACOUSTINT (Acoustic Intelligence), NUCINT (Nuclear Intelligence) und viele mehr. Hier werden Informationen von Sensoren, Raum, Wellenlänge, Zeit und weiteren Faktoren gesammelt. [71]

- **SIGINT**: Unter dem Begriff SIGINT ist Signals Intelligence zu verstehen. Das bedeutet, dass beispielsweise Rundfunk-Signale oder Radarsysteme aber auch Informationen von Handymasten gesammelt werden. Es werden verschiedene Informationen von elektronischen Signalen oder Systemen gesammelt. In diesem Begriff sind weitere Unterkategorien enthalten wie, beispielsweise COMINT (Communications Intelligence) oder ELINT (Electronic Intelligence). [72] [73]

- **SOCINT**: Dieser Begriff “SOCINT” bedeutet Social Intelligence. Als Fokus werden bei SOCINT Informationen von Social Media gespeichert. Hier wird vor allem auf Seiten wie Facebook, Snapchat, LinkedIn, Instagram aber auch Partnerportale als Informationsquellen herangezogen. Durch SOCINT können Firmen Wettbewerber ausforschen und versuchen an Projekt-Daten zu gelangen. [74] [75]

Angriffsarten:
In diesem anschließenden Abschnitt werden verschiedene Angriffsarten beschrieben. Es werden hier Angriffsarten beschrieben, welche sich mit den sammelbaren Informationen der analysierten Tools ergeben.
Mit den Informationen die mit den Tools, welche in Kapitel 6 „*Evaluierung von den Tools*“ beschrieben werden, gesammelt werden können, können einige der anschließend beschriebenen Angriffsarten durchgeführt werden.
Beispielsweise können mit gesammelten E-Mail-Adressen mit einem Tool gesammelt werden, damit besteht die Möglichkeit Spoofing oder Phishing Attacken durchzuführen.

Wie oben erwähnt, werden bei den verschiedenen Angriffsarten die Informationen wie beispielsweise “IP-Adresse”, “DNS” oder “E-Mail-Adresse" angegeben, damit ersichtlich ist, welche Informationen der analysierten Tools bei den jeweiligen Angriffsarten verwendet werden können.

Da wesentlich mehr Informationen bei einem Angriffsvektor gelistet werden können, musste dies eingegrenzt werden, daher wurden bei den Angriffsvektoren nur die Informationen gelistet, welche mit den analysierten Tools gefunden werden können.

- **Gezielte Angriffe**: Unter „gezielten Angriffen“ ist ein Angriff zu verstehen, welcher sich auf bestimmte Personen, Unternehmen, Systeme oder Software richtet. Mittels eines solchen Angriffs können Informationen extrahiert werden oder Vorgänge von einer Zielmaschine gestört werden. Mit einem solchen Angriff können Systeme gestoppt werden und dem Unternehmen somit Schaden zugefügt werden. Für diesen Angriff können beispielsweise Name, Telefonnummer und E-Mail-Adresse eines Opfers verwendet werden, damit besteht die Möglichkeit, sich als Kollege auszugeben und einen Mitarbeiter zu täuschen. Weiters können auch Spear-Phishing sowie Phishing Angriffe durchgeführt werden und auf eine Interaktion eines Mitarbeiters gehofft werden, welcher beispielsweise auf eine solche Mail antwortet oder Inhalte herunterlädt oder Anhänge öffnet. [76]

- **Hacking**: Unter dem Begriff „Hacking“ wird das unbefugte Eindringen in ein Computersystem oder ein Netzwerk verstanden. Jene Person, welche die Aktivitäten durchführt, wird als Hacker bezeichnet. Es ist ein großer Überbegriff für die weiteren Angriffsarten. Bei diesem Angriff werden alle möglichen Informationen, welche über das Ziel gefunden werden können, verwendet. Somit können von einem Angreifer alle gefundenen Informationen für einen Angriff verwendet werden, womit beispielsweise Schwachstellen von einem Unternehmen für einen Angriff gefunden werden können. [77]

- **Identity Theft**: Bei diesem Angriff wird die Identität einer anderen Person verwendet und verschiedene Aktivitäten durchgeführt. Somit wird beispielsweise versucht, mittels eines falschen Namens einen Kredit von einer Bank zu bekommen oder an Zugangsdaten von einem System zu gelangen. Aber auch Angriffe wie CEO-Fraud können hier stattfinden, das bedeutet, dass sich eine Person als “Chef” ausgibt und beispielsweise eine Geldzahlung anfordert. Ebenso können falsche Sozialversicherungsnummern verwendet werden. Dieser Angriff benötigt Informationen wie beispielsweise Telefonnummer, Name und E-Mail-Adresse. Durch diese Informationen können Identitäten zusammengestellt werden und jemand kann sich als eine andere Person ausgeben. [78]

- **Spoofing**: Bei diesem Angriff wird versucht beispielsweise E-Mails von einem Unternehmen nachzubilden. Es werden von einem Angreifer die E-Mails von Unternehmen so nachgebaut, dass Opfer diese als “echt” empfinden und möglicherweise ihre Daten preisgeben. Es können auch Geräte manipuliert werden, damit es den Anschein hat, dass das Gerät in das Netzwerk

gehört, obwohl dieses nicht autorisiertes ist. Um diesen Angriff durchzuführen können verschiedene Informationen verwendet werden wie beispielsweise DNS-Einträge, IP-Adressen und E-Mail-Adressen. Durch diese verschiedenen Einträge und Adressen ist es möglich, ein Netzwerk zu täuschen, um eingegebene Zugangsdaten zu bekommen. [79]

- **DoS/DDoS**: Bei einem DoS (Denial of Service) Angriff wird das Ziel verfolgt, die Systeme „lahm zu legen“, hier wird nur ein Gerät für den Angriff verwendet. Hingegen werden bei einem DDoS (Distributed Denial of Service) Angriff mehrere Geräte für einen Angriff verwendet um das System „lahm zu legen“. Für diesen Angriff können IP-Adressen verwendet werden, welche in der Reconnaissance-Phase gefunden worden sind. Somit können an die IP-Adresse des Ziels ”unzählige” Pakete gesendet werden und das Ziel somit gestört werden. Aus diesem Grund ist das Ziel nicht mehr in der Lage auf ”richtige” Pakete zu antworten. [79]

- **Cyber Terrorism**: Dieser Angriff hat als Hauptziel das Zerstören von beispielsweise einem Computersystem, Daten oder Programmen. Es können beispielsweise IKT (Informations- und Kommunikationstechnologien) als Ziel gesehen werden. Hier handelt es sich meist um “Cyberspace”-Terroristen. Um diesen Angriff durchführen zu können, werden beispielsweise DNS-Einträge und Webseiten benötigt. Diese Informationen über das Ziel können aus der Reconnaissance Phase gesammelt werden. Es können somit Opfer auf eine falsche Webseite weitergeleitet werden, welche Propaganda enthalten. [80] [81]

- **Malware**: Eine Malware ist eine schädliche Software, die einem Computer/Gerät Daten unbrauchbar machen kann oder Daten stehlen kann. Für diesen Angriff können beispielsweise folgende Informationen von der Reconnaissance-Phase verwendet werden wie E-Mail-Adressen (Anhänge) und Webseiten (Nachrichten, Infizieren). Durch E-Mail-Anhänge oder Webseiten, welche es erlauben Informationen oder Dateien herunter zu laden, kann die Schadsoftware verteilt werden. [82]

- **Würmer**: Hier handelt es sich um eine Art von Malware, welche sich alleine von einem zu dem anderen Computer verteilt. Es ist möglich, dass sich dieser selber repliziert und muss somit nicht an ein Softwareprogramm angehängt werden. Eine Übertragung und Infizierung könnte mittels Softwareschwachstellen oder Spam-E-Mails stattfinden. Opfer können sich gegen einen solchen Angriff schützen, indem sie die neueste Version des Betriebssystems haben und es auf dem aktuellen Stand halten mit neuesten Updates. Weiters sollten sich Opfer immer bewusst sein, welche E-Mail Anhänge sie öffnen da diese auch Schadcodes für diesen Angriff enthalten können. Würmer können über (Spam)E-Mails, verteilt werden. Diese E-Mail-Informationen können in der Reconnaissance-Phase gespeichert werden. Ebenso können diese auch über Instant-Messaging verteilt werden. [83]

- **Pharming**: Diese Attacke ist ähnlich zu Phishing, nur dass bei diesem Angriff die Domain so umgewandelt wird, damit diese auf eine gefälschte Webseite umleitet. Somit ist es möglich einem Opfer damit einen Virus oder Trojaner einzuspielen da diese beispielsweise ihre Zugangsdaten eingeben, weil sie der Meinung sind, auf der richtigen Webseite zu sein. Es können ebenso DNS-Server infiziert werden, somit werden mehrere Benutzer auf die gefälschte Webseite weitergeleitet. Bei diesem Angriff würde einem Opfer selbst das manuelle Eingeben der Internetadresse nicht helfen, da automatisch die Weiterleitung auf die gefälschte Internetseite durchgeführt wird. Hierfür müssen von einem Opfer Anti-Malware Lösungen verwendet werden. Somit können meistens keine Host-Dateien geändert werden. Dieser Angriff benötigt beispielsweise E-Mail-Adressen oder Webseiten, welche in der Reconnaissance-Phase gefunden werden können. Durch die E-Mail-Adresse können verschiedene Angriffe wie CEO Fraud durchgeführt werden und es kann sich bei einem

Mitarbeiter als ”Chef” ausgegeben und Geld angefordert werden. Ebenso können ”schädliche” Links in einem E-Mail hinzugefügt werden. Weiters können ”falsche” Webseiten erstellt werden, um ein Opfer zu täuschen und die Eingabedaten zu speichern. [79]

- **Phishing/Spear Phishing**: Bei diesem Angriff, geht der Angreifer so vor, dass er eine betrügerische E-Mail versendet. Diese E-Mail sieht aus wie die originale E-Mail von einem Unternehmen/Anbieter, daher schöpfen einige Personen keinen Verdacht einer Täuschung. Wenn das Opfer den Link in dem E-Mail öffnet, wird es auf eine gefälschte Webseite weitergeleitet, welche aber der Originalwebseite gleicht. Hier wird gebeten, vertrauenswürdige Daten einzugeben. Diese Daten werden gespeichert und für weitere kriminelle Handlungen verwendet. Oft werden solche Angriffe verwendet, um Kreditkarteninformationen oder persönliche Daten eines Opfers zu bekommen. Ein Unternehmen kann Mitarbeiter mit speziellen Schulungen schützen um diese auf “Fake-Emails” aufmerksam zu machen und besser zu erkennen. Bei Phishing helfen keine Sicherheitslösungen. Für diesen Angriff können die gefundenen E-Mail-Adressen oder Webseiten verwendet werden. Es bietet die Möglichkeit beispielsweise CEO Fraud zu betreiben. Bei einer Spear-Phishing Attacke wird der Angriff gezielt auf eine Person oder eine Gruppe gerichtet. [79]

- **Ransomware**: Bei diesem Angriff, werden Daten/Computer des Opfers verschlüsselt und es wird anschließend Lösegeld gefordert, damit diese Daten auf dem Computer wieder freigegeben werden. Oft wird hier ein Zeitlimit gesetzt, bis wann das Geld überwiesen werden muss, ansonsten kann es sein, dass die Daten nicht mehr zu retten sind. Dieses Zeitlimit hilft Angreifern, beim Opfer einen Stress auszulösen, da nach dem abgelaufenen Limit möglicherweise die Daten gelöscht werden könnten. Es ist nicht sicher, ob nach dem Zahlen des Betrages die Daten wieder freigegeben werden oder nicht. Dieser Angriff benötigt beispielsweise E-Mail-Adressen oder Webseiten, welche in der Reconnaissance Phase gefunden werden können. Somit können E-Mails mit einem schadhaften Anhang versehen werden und an das Opfer gesendet werden, oder es können auf Webseiten ”Drive-by-Downloads" ausgeführt werden. Ebenso können verschiedene Exploits verwendet werden, welche durch die gesammelten Informationen ersichtlich sind. Unter einem Drive by Download wird das unbewusste Herunterladen von einer Software verstanden. Hier können beispielweise auch Schadsoftware unbewusst runtergeladen werden. [84]

- **Scareware**: Bei diesem Angriff handelt es sich um eine Art von Malware. Bei diesem Angriff wird versucht, dass der Angreifer eine Software herunterladet oder sogar kauft. Dies wird mittels Anzeigen probiert, welche mit Popups angezeigt werden, dass auf dem Computer Probleme gefunden worden sind und diese behoben werden sollten. Anschließend kann, um diese Probleme zu beheben, Geld von dem User gefordert werden. Es kann dafür entweder der Bildschirm gesperrt werden, oder es können Pop-Ups erscheinen. Dafür können beispielsweise Webseiten verwendet werden, um diese Meldungen oder Popups anzuzeigen, diese Meldungen können beispielsweise wie Windows Meldungen aussehen, damit der User keinen Verdacht einer Fake-Meldung schöpft. [84] [85]

- **Adware und Spyware**: Bei einer **Adware** handelt es sich um ein/e Programm/Software, bei diesen werden zusätzlich Komponenten auf dem System installiert, dies ist auch als Malvertising bekannt. Durch das Installieren von zusätzlichen Komponenten der Software kann beispielsweise die Startseite des Browsers missbraucht werden und das Opfer auf andere Webseiten weiterleiten oder es kann der User mit verschiedenen Werbungen überschwemmt werden. Es ist sehr schwer eine Adware zu deinstallieren, da sie sich sehr in das System integrieren. Bei einer **Spyware** wird der Computer und/oder die Internetverbindung des Opfers überwacht. Hier ist beispielsweise die Rede von Keyloggern welche die Eingaben, die auf der

Tastatur getätigt werden, aufzeichnen. Somit können Passwörter und Benutzername oder Kontonummer und Pin eines Opfers ausgeforscht werden. Um diese Angriffe durchzuführen, können Webseiten eines Ziels verwendet werden, welche in der Reconnaissance Phase gefunden werden können. Es können somit Personen auf falsche Webseiten weitergeleitet werden, welche möglichweise virenbelastet sind oder auf verschiedene ”Fake-Webseiten”. Es können auf Webseiten Pop-Up Meldungen eingeblendet werden, welche ”schwer” zum Schließen sind. Weiters kann durch Adware auch Spyware installiert werden. [86]

- **Trojaner**: Bei diesem Angriff handelt es sich um einen schadhaften Code oder eine Software, welche vertrauenswürdig ausschaut, doch womit die Kontrolle des gesamten Computers übernommen werden kann. Trojaner schaden dem Netzwerk oder den Daten, welche sich auf dem Gerät befinden. Es wird versucht das Opfer dazu zu animieren, Malware auf dem Gerät zu installieren. Wenn das Opfer anschließend die Malware installiert hat, kann der Trojaner auf dem Computer diverse Tätigkeiten durchführen, wie senden, lesen, starten oder löschen von Dateien. Opfer können sich schützen, indem sie die neueste Version des Betriebssystems installieren, da Angreifer oft Lücken in alten Versionen ausnützen. Ebenso sollte das Opfer eine Firewall verwenden, um sich gegen solche Angriffe zu schützen. Bekannte Trojaner wären beispielsweise Crypto-Locker oder Bank-Trojaner. Um diesen Angriff durchführen zu können, können beispielsweise E-Mail-Adressen verwendet werden. Hier kann ein Anhang mit einem Schadcode beigefügt werden, somit besteht die Möglichkeit, dass das Opfer diesen Anhang runterlädt und sich somit die Schadsoftware auf dem PC ausbreiten kann. Dies kann ebenso über einen Drive by Download stattfinden. Unter einem Drive by Download wird das unbewusste Herunterladen von einer Software verstanden. Hier können beispielweise auch Schadsoftware unbewusst runtergeladen werden. [87]

- **Virus**: Bei einem Virus handelt es sich um eine schädliche Software, welche sich ohne Kenntnis des Benutzers verbreitet. Meistens verbreitet sich ein Virus über E-Mail-Anhänge, welche durch das Öffnen aktiviert werden. Falls solche infizierten E-Mails weitergeleitet werden, kann dies verheerende Folgen haben und mehrere Personen infizieren. Für diesen Angriff können verschiedene Informationen verwendet werden, welche in der Reconnaissance-Phase gefunden werden können. Es kann die gefundene E-Mail-Adresse verwendet werden und an diese ein E-Mail mit einem Schadcode im Anhang gesendet werden oder eine Webseite als ”Fake-Webseite” nachgebaut werden und beispielsweise einen Download anbieten, wodurch aber ein Virus installiert wird. [88]

- **Opportunistische Angriffe**: Hier handelt es sich um einen Angriff einer Person, welche nach dem erfolgreichen Eindringen in ein System, alle möglichen Daten, die gefunden werden können, abspeichert. Bei diesem Angriff stehen die Schwachstellen eines Systems oder einer App im Fokus, welche genutzt werden können, um einen Angriff durchzuführen. Für diesen Angriff können verschiedene Informationen der Reconnaissance Phase verwendet werden, wie beispielsweise Namen, E-Mail-Adresse oder DNS-Einträge. [89] [90]

- **Cyber Vandalism**: Bei diesem Angriff steht das Zerstören oder das Beschädigen von Daten, Netzwerken oder Computern im Vordergrund. Es können beispielsweise Malware Angriffe erstellt werden, um Daten auf dem Zielsystem zu zerstören. Für diesen Angriff können beispielsweise Informationen wie IP-Adresse, Webseiten, Name und DNS-Einträge, verwendet werden. Hier können beispielsweise verschiedene Weiterleitungen auf ”Fake Seiten” durchgeführt werden, welche möglicherweise den Ruf des Unternehmens schaden können. Weiters besteht die Möglichkeit, beim Eindringen in das System des Unternehmens Daten zu beschädigen oder zu löschen. [91]

- **Cyber Stalking**: Bei dieser Attacke wird gezielt auf Personen eingegangen. Hier werden Personen exzessiv ausgeforscht und versucht so viele Informationen wie möglich zu sammeln wie beispielsweise deren Vorlieben oder Aktivitäten. Für diesen Angriff kann eine Personensuche auf verschiedenen Plattformen durchgeführt werden. Diese Angriffe finden meistens über Chatrooms oder Social Media Plattformen statt. Um diesen Angriff durchführen zu können, können Informationen der Reconnaissance Phase verwendet werden, wie beispielsweise E-Mail-Adresse, Name und Telefonnummer eines Ziels. [92] [93]

- **Spam**: Hier handelt es sich um ungewollte/unerwünschte Nachrichten. Diese Nachrichten werden an Personen gesendet, ohne dass diese zuvor eingewilligt haben. In diesen Nachrichten können sich verschiedene Inhalte verbergen. Es können beispielsweise Werbeinhalte enthalten sein, aber es können auch Schadsoftware enthalten sein. Für diesen Angriff können beispielsweise E-Mail-Adressen verwendet werden, welche in der Reconnaissance-Phase gefunden worden sind. [94]

- **Man-in-the-Middle**: Bei diesem Angriff schaltet sich ein Angreifer zwischen die Kommunikation von zwei Personen. Somit kann der Angreifer die Nachrichten, die ausgetauscht werden, abhören und sich als einer der beiden Personen ausgeben. Somit können beispielsweise falsche Rechnungen an die zweite Person gesendet werden. Für diesen Angriff können verschiedene Attacken wie ARP-Spoofing oder DNS-Spoofing verwendet werden. Dafür kann von einer Person ein eigenes Netzwerk aufgestellt werden, um diese Daten zu bekommen. [79]

- **ARP-Spoofing**: Dies ist eine Art von Man-in-the-Middle Attacke. Es wird hier die ARP-Tabelle des Netzwerks angegriffen. Hier werden falsche ARP-Pakete an das System gesendet, um sich zwischen die zwei kommunizierenden Systeme zu schalten und den Datenverkehr zu ändern. Um diesen Angriff durchzuführen, werden ARP-Adressen benötigt, welche in der Reconnaissance Phase gefunden werden können, um ein Netzwerk zu täuschen und mögliche Zugangsdaten, welche von Personen eingegeben werden, zu bekommen. [95]

- **Social-Engineering**: Bei dieser Attacke wird meist das fehlende technische Wissen von einem User ausgenutzt. Beispielsweise kann eine Person bei der Eingabe des Usernamens und des Passwortes beobachtet werden. Bei dieser Angriffsvariante wird kein technisches Wissen benötigt. Eine weitere Variante könnte das Versenden von Phishing-E-Mails sein. Hier werden gefälschte E-Mails an einen User gesendet. Diese E-Mails sehen für das Opfer aus, wie echte E-Mails von beispielsweise der Bank, dadurch erhoffen sich die Angreifer die Eingabe von privaten Daten. Für diesen Angriff können verschiedene personenbezogenen Daten von Scans verwendet werden. Beispielsweise E-Mail-Adresse, Namen von Personen, Freunde und Geolocation. [79]

- **Domain Hijacking**: Bei diesem Angriff werden von einem Angreifer die Registrierungsdaten geändert. Hierfür werden Informationen des Domain-Inhabers gesammelt, diese werden anschließend verwendet, um bei der Registrierungsstelle eine Änderung oder eine Übernahme des Registrars anzufordern. Um diesen Angriff durchzuführen, können E-Mail-Adressen und Webseiten, welche in der Reconnaissance-Phase gefunden worden sind, verwendet werden. Dadurch bietet sich die Möglichkeit ebenso Phishing Angriffe durchzuführen. [96]

- **DNS-Flood-Attack**: Bei diesem Angriff handelt es sich um eine Art von einem DDoS-Angriff. Hier wird der DNS-Server einer Domäne geflutet, um die eigentliche Auflösung der Domäne zu unterbrechen. Es ist oft schwer diesen Angriff von einem normalen Datenverkehr zu unterscheiden. Für einen DNS-Flood-Angriff können DNS-Einträge, welche in der

Reconnaissance Phase gefunden werden können, verwendet werden. Durch diesen Angriff werden die DNS-Auflösungen gestört und es ist nicht möglich, die gewünschte Seite zu öffnen. [97]

- **DRDoS**: Bei dem DRDoS (distributed reflective denial of service) Angriff wird das Opfer nicht direkt von dem Angreifer angegriffen. Das bedeutet, dass der Angreifer die Datenpakete nicht direkt an das Opfer sendet, sondern an den Internetdienst. Hier trägt der Angreifer die Absende-Adresse des Opfers ein. Um diesen Angriff durchführen zu können, können DNS-Einträge verwendet werden, welche in der Reconnaissance Phase gefunden werden können. Anschließend werden UDP-Pakete mit falscher IP-Adresse gesendet, um die Quelle des Angreifers zu verbergen. [98]

- **Exploits**: Hier handelt es sich um ein Schadprogramm, welche möglicherweise einen ausführbaren Code oder Sicherheitslücken enthalten, welche ausgenützt werden können. Für diesen Angriff können verschiedene Informationen wie beispielsweise Versionen oder Systeminformationen verwendet werden. Somit können möglicherweise Schwachstellen, welche über das verwendete System gefunden werden, ausgenützt werden. [99]

Anschließend wird eine vereinfachte Tabelle gezeigt. Die Tabelle 6 „Angriffsarten“ dient dazu, um aufzuzeigen, dass obwohl es sich um unterschiedliche Angriffsarten handelt, sich die benötigten Informationen für einen Angriff überschneiden. Es wurden die gängigsten Informationen einer Angriffsart beigefügt.

Angriffsarten	Benötigte Informationen/Daten* für einen Angriff:	Angriffsarten	Benötigte Informationen/Daten* für einen Angriff:
Gezielte Angriffe	Name, Telefonnummer, E-Mail-Adresse	**Trojaner**	E-Mail-Adresse
Identity Theft	Name, Telefonnummer, E-Mail-Adresse, Bilder, Twitter-Username, Follower/Freunde	**Virus**	E-Mail-Adresse, Webseite
Spoofing	DNS, IP-Adresse, E-Mail-Adresse	**Opportunistische Angriffe**	E-Mail-Adresse, DNS-Einträge
DoS/DDoS	IP-Adresse	**Cyber Vandalism**	Name, IP-Adresse, Webseite, DNS
Cyber Terrorism	DNS, Webseite	**Cyber Stalking**	E-Mail-Adresse, Name, Telefonnummer, Tweets, Follower/Freunde
Malware	E-Mail-Adresse, Webseite	**Spam**	E-Mail-Adresse
Würmer	E-Mail-Adresse, Webseite	**Man-in-the-Middle**	ARP-Adressen
Pharming	E-Mail-Adresse, Webseite	**ARP-Spoofing:**	ARP-Adressen
Phishing	E-Mail-Adresse, Webseite	**Social-Engineering**	E-Mail-Adresse, Name, Freunde, Geolocation, Tweets, Twitter-Username, Follower/Freunde
Ransomware	E-Mail-Adresse, Webseite	**Domain Hijacking**	DNS, E-Mail-Adresse, Webseite
Scareware	Webseite	**DNS-Flood-Attack**	DNS
Adware	Webseite	**DRDoS**	DNS

Tabelle 6 Angriffsarten

* Es bestehen weit mehr Informationen/Daten mittels denen die Angriffe vollzogen werden können, daher wurden nur Informationen/Daten, welche mit dem analysierten Tool gesammelt werden können, angeführt.
Die Social Media Daten sind einerseits die Bilder, aber auch die Tweets und Follower sowie die Freunde, welche von den Tools gesammelt werden könnten. Es sind die jeweiligen Daten bei den persönlichen Angriffen wie “Identity Theft”, “Cyber Staking” und “Social-Engineering” hinzugefügt worden.

Angriffe auf Organisationen im Gegensatz zu Angriffen auf Personen

In diesem Absatz wird der Vergleich zwischen einem Angriff auf eine Organisation oder dem Angriff auf einen Mitarbeiter aufgezeigt. Zuerst werden bei diesen Angriffen Daten über das Ziel gesammelt, diese werden anschließend verbunden. Es ist ersichtlich, dass es bei den unterschiedlichen Angriffszielen dennoch Zusammenhänge bei den Informationen gibt. [100]

Informationen bei Angriff auf Organisation	Informationen bei Angriff auf Personen
E-Mail-Adresse	E-Mail-Adresse
Telefonnummer	Telefonnummer
Lieferanten/Verkäufer	Wohnadresse
Interne Dokumente	Adresse der Arbeit
Sicherheitsinformationen	div. Informationen (Interessen, Beziehungen)
geistiges Eigentum	
sensible Informationen der Organisation	

Tabelle 7 Informationen bei Angriffen auf Organisation vs. Personen

4.9. Marketing Intelligence

In diesem Abschnitt wird auf die Verbindung von OSINT und C/MI (Competitive Intelligence und Marketing Intelligence) eingegangen. Die Verbindung dieser zwei Informationen wird für Unternehmen immer wichtiger, da Angebote durch die verfügbaren Informationen über Personen immer "personalisierter" an die Kunden angepasst werden können.

Online Shops können das Kaufverhalten von Usern speichern. Dadurch kann von einem Unternehmen die Ausgangslage ausgebaut werden, um eine Online-Seite direkt auf die Kunden und deren Verhalten aufzubauen. So können beispielsweise die Suchbegriffe, welche von Usern verwendet werden, gespeichert werden. Ebenso können die Angebote an bestimmte Anlässe wie Weihnachten oder Ostern ausgelegt werden. Weiters können auch Social Media Plattformen überwacht werden, dadurch ist es möglich direkt auf verschiedene Stimmungen und Verhalten von Kunden zu handeln und den Online-Shop dementsprechend anzupassen. Es wird von Unternehmen auch die Meinungen zu dem Unternehmen überwacht, somit kann die Wahrnehmung des Unternehmens oder des Shops analysiert werden. Wichtig ist dies auch für Startups, da neue Entwicklungen oder Produkte bewertet werden können. Ein Problem stellt aber die Identifizierung der Identität eines Benutzers dar. So können beispielsweise Produkte durch "falsche" Kommentare eine schlechte Bewertung bekommen. [101]

Durch Marketing Intelligence wird es den Marketingabteilungen ermöglicht die Kontrolle zurückzuerhalten und es können die benötigten Daten analysiert werden. Dadurch ist es möglich eine datenbasierte Entscheidungsfindung durchzuführen. Es werden alle möglichen Daten, die gesammelt werden konnten, zusammengefasst. Eine Zusammenfassung wird benötigt, um anschließend eine Datenanalyse durchführen zu können. Marketingabteilungen müssen oft schnell agieren, daher sollten sie schon vorgefertigte Lösungen für bestimmte Ereignisse haben. Es wird eine zentrale Speicherstelle benötigt, in dieser können die gesammelten Informationen gespeichert werden. [102]

5. Testumgebung und Beschreibung der Kriterien

5.1. Ausgangslage

In diesem Kapitel wird auf den “passiven” Scan von OSINT eingegangen. Bei einem passiven Scan werden öffentlich verfügbare Informationen und Daten über ein Ziel gesucht und gesammelt ohne dass das Ziel etwas davon mitbekommt. Die Informationsbeschaffung erfolgt durch sogenannte Information-Gathering Tools, welche in Kapitel 6 „*Evaluierung von den Tools*“ beschrieben sind.
In dieser Arbeit werden ausschließlich Open Source Tools in der kostenlosen Version verwendet und getestet. In den durchgeführten Tests und Analysen der Tools ergeben sich Unterschiede der jeweiligen Funktionalitäten eines Tools, welche in Kapitel 8 „*Auswertung & Interpretation der Ergebnisse*“ in einer Tabellenform aufgezeigt werden.

Es ist wichtig zu erwähnen, dass in keiner Hinsicht ein Angriff oder eine Schwachstelle der gefundenen Informationen getestet wird. Diese Arbeit legt den Fokus auf die Reconnaissance Phase und den “passiven” Scan. In dieser Phase wird Information Gathering durchgeführt, somit werden verfügbare Informationen gesammelt und gespeichert. In dieser Arbeit werden daher nicht die weiteren Phasen der “Cyber Kill Chain” [57] behandelt. Somit sind die erwähnten und potenziellen Lücken oder Schwachstellen nur mögliche “Gefährdungen” und keine getesteten und somit bestätigten Gefahren.

Durch die steigende Menge an frei zugänglichen Informationen, welche im Internet frei verfügbar sind, ist die Wichtigkeit von OSINT rasant gestiegen, dementsprechend gibt es auch verschiedene Tools, um diese Informationen zu sammeln. Da es eine Vielfalt von OSINT-Tools gibt, welche ein Sammeln von Informationen ermöglichen, ist die Gegenüberstellung sehr hilfreich und unumgänglich, um die einzelnen Tools differenzieren zu können.

Um die jeweiligen Eigenschaften und Funktionen aufzuzeigen, sowie die Informationen, die mit den Tools gesammelt werden können, wird ein/e Fake Profil einer Person auf unterschiedlichen Social Media Plattformen angelegt. Mit dem Profil werden anschließend verschiedene Handlungen wie beispielsweise auf Twitter einige Tweets erstellt und weiteren erstellten Fake-Usern/in gefolgt.
Dadurch soll eine reale Umgebung kreiert werden, welche überprüft und analysiert werden kann. Aus Datenschutzgründen wurden die Tests anhand der “Fake-User” durchgeführt, um keine Informationen von realen Personen in diese Arbeit einfließen zu lassen.

Die jeweiligen analysierten Tools haben verschiedene Spezialisierungen. Beispielsweise wurden Tools überprüft, welche auf Social Media Plattformen spezialisiert sind, inwieweit es möglich ist Kommentare, Freundschaftsanfragen sowie Posts eines Users nachzuverfolgen. Dadurch können genauere Überprüfungen erzielt werden da ersichtlich ist, wie beispielsweise ein Profil mit weiteren Plattformen und Freunden verbunden sein kann.

Beim Information Gathering mittels der analysierten Tools, ist auch der Fokus auf die Fachhochschule St. Pölten gelegt worden. Hier wird mittels der Tools getestet, welche Informationen frei zur Verfügung stehen und gesammelt werden können. Beispielsweise wird geschaut ob Personen, Geräte, eingesetzte Systeme, IP-Adressen oder Informationen über Finanzen gefunden werden können. Um die Social Media Plattformen zu analysieren, wird die Twitter-Seite der Fachhochschule auf mögliche Informationen durchsucht.

Für das weitere Vorgehen wird eine Beschreibung und ein Test der jeweiligen Tools durchgeführt, um zu zeigen, welche Funktionen unterstützt werden, sowie welche Informationen mit den jeweiligen Tools gefunden werden können. In einem weiteren Schritt werden die Tools in Tabelle 11 „*Ergebnisse*

der Tool-Evaluierung 1“ bis 15 „*Ergebnisse der Tool-Evaluierung 5*“ auf deren Unterschiede verglichen. Des Weiteren wird auf deren Funktionalitäten bei der Suche nach freien sowie öffentlich zugänglichen Daten im Internet geachtet. Dadurch kann jedes Tool nach deren positiven, aber auch negativen Eigenschaften beurteilt werden. Es werden dadurch die Unterschiedlichkeiten aber auch die möglichen Gemeinsamkeiten zwischen Tools erkannt.
Die Scans werden mit den Default-Einstellungen der Social Media Plattformen getestet, denn es ist davon auszugehen, dass die wenigsten Personen diese Einstellungen sofort nach dem Erstellen des Accounts ändern. [103]

Der Artikel “Do You Know Who’s Watching you?” [6] zeigt beispielsweise, wie die Default-Einstellungen von Unternehmen vorgegeben werden. Ersichtlich ist, dass es 2005 noch strikter gehandhabt wurde. Die weiteren Jahre zeigen, dass die Default-Einstellungen immer lockerer und öffentlicher werden. Im Jahr 2010 sind diverse Tätigkeiten, welche von einem User durchgeführt werden wie beispielsweise das Online stellen von Fotos sowie Posts für jeden User sichtbar, aufgrund der Default-Einstellungen.
Es kann zu Einschränkungen und Abweichungen beim Information-Gathering kommen, anhand der jeweiligen Konfiguration der Sicherheits- und Privacy-Einstellungen von Online-Plattformen.

Es wird anhand der Fallbeispiele im Kapitel 7 „*OSINT Use Case*“ gezeigt, wie die analysierten OSINT-Tools bei der Suche nach Schwachstellen behilflich sein können. Weiters wird gezeigt, wie es möglich ist, eine/n User/in auf deren Tätigkeiten sowie Posts und Freundschaften zu überprüfen bevor beispielsweise ein Arbeitsgeber eine Person zu einem Vorstellungsgespräch einlädt. Ebenso wird auf die Angriffsart Phishing eingegangen und anhand eines Beispiels erklärt.

5.2. Aufbau der Testumgebung und ihre Eigenschaften

Die unten angeführten Details der Testumgebung beschreiben unter welchen Voraussetzungen und Versionen die Tools getestet werden.

5.2.1. Kali-Linux Testumgebung

Eine der verwendeten Testumgebungen für das Analysieren der Tools ist die virtuelle Maschine mit der Linux Distribution “Kali-Linux”. Bei dem Testsystem, welches für die diversen Tests und die Untersuchungen der Tools verwendet wird, handelt es sich um die Version „Linux DB 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64 GNU/Linux“. Es wurde sich für diese Distribution entschieden, da bereits einige der analysierten Tools vorinstalliert sind.
Bei “Kali-Linux” handelt es sich um eine Distribution, welche für forensische Untersuchungen verwendet werden kann. Kali-Linux stellt eine Vielzahl von Information-Gathering Tools bereit, welche wie vorhin erwähnt, vorinstalliert sind, dadurch wird sich der Aufwand einer separaten Installation erspart. Diese Distribution besteht bereits seit 2013 und wird durch kontinuierliche Updates und erneuerte Versionen auf dem aktuellen Stand gehalten. Die Distribution wurde von “Mati Aharoni” und “Devon Kearn” entwickelt. Laut Statistiken ist Kali-Linux das meistbekannteste Penetrationtesting-Tool. [104]

5.2.2. Buscador2 Testumgebung (VMWare OVA)

Es wurde eine weitere virtuelle Maschine für diverse Analysen der Tools herangezogen. Hierbei handelt es sich um das Tool “Buscador2”, dieses wurde als OVA-Image heruntergeladen und direkt in eine virtuelle Maschine eingespielt. Hier handelt es sich um eine vorkonfigurierte virtuelle Maschine, welche von “David Westcott” und “Michael Bazzell” erstellt wurde. Auf dieser virtuellen Maschine sind bereits wichtige OSINT Tools vorinstalliert, welche ebenso im Zuge dieser Arbeit überprüft und analysiert worden sind. Die Systemdaten der verwendeten virtuellen Maschine sind ”Debian

GNU/Linux 9 (stretch)" sowie " Linux 4.9.0-8-amd64". Diese virtuelle Maschine basiert auf Ubuntu und bietet eine Reihe von OSINT-Tools, Datenschutz-Tools und Erfassungs-Tools. Weiters wird von den Betreibern der virtuellen Maschine ein Podcast "The Privacy, Security & OSINT Show" betrieben. Diese Podcasts werden jeden Freitag zur Verfügung gestellt. Diese virtuelle Maschine wird seit Jänner 2019 nicht mehr aktualisiert, daher wird empfohlen eine eigene virtuelle Maschine laut dem publizierten Buch „Open Source Intelligence Techniques (7th edition)" zu erstellen. [105] [106]

5.3. Kriterien

In diesem Kapitel werden die Kriterien, welche aus detaillierten Recherchen, Literaturen und verschiedenen Publikationen extrahiert wurden aufgelistet und diese werden gegen die ausgewählten Open Source Tools getestet. Die extrahierten Kriterien wurden anschließend an die Arbeit angepasst und definiert um einen Vergleich sowie eine Analyse durchführen zu können. Daher gelten die Kriterien als Ausgangsbasis, um die Tools zu analysieren. Der Vergleich der ausgewählten Tools wird anhand einer Matrix dargestellt, welches in Kapitel 8 „*Auswertung & Interpretation der Ergebnisse*" zu sehen ist. Mit der erstellten Matrix wird ein Überblick über die Funktionalitäten sowie der Eigenschaften der Tools geschaffen.
Zur Beschreibung der Eigenschaften und Funktionalitäten werden objektive Kriterien abgeleitet, die für die Bewertung der Tools angewendet werden.

Folgende Kriterien werden als Übersicht im späteren Verlauf beschrieben:

- Plattformen
- GUI /CLI (Graphical User Interface/Command Line Interface)
- Import-Formate
- Export-Formate
- Updates
- Such- und Filtermöglichkeiten
- Kosten - Lizenzkosten und Schulungskosten
- Informationen
- Korrektheit der Daten
- Berichtsverwaltung
- Darstellungsfunktionen (Darstellung von Informationen)
- Rückverfolgbarkeit (von Personen/Unternehmen)
- Attacken

5.3.1. Plattformen

Das Kriterium "**Plattformen**" zeigt, welche Betriebssysteme die ausgewählten Tools unterstützen. Dies stellt eine wichtige Kategorie für Firmen dar, damit diese das Tool auf ihrem Endsystem verwenden können. Es wurden die gängigsten Betriebssysteme als Vergleich genommen, diese sind Windows, Linux sowie Mac.
Um dieses Kriterium zu vergleichen und eine Bewertung durchführen zu können, wird kontrolliert und analysiert, welche der drei oben genannten Plattformen unterstützt werden.

5.3.2. GUI /CLI (Graphical User Interface/Command Line Interface)

Das Kriterium „**GUI/CLI**" spielt für viele Anwender/innen möglicherweise eine große Rolle, da von den Personen eine Administration über eine GUI oder eine CLI durchgeführt werden muss. Um dieses Kriterium zu vergleichen wird bei den jeweiligen Tools analysiert, ob eine CLI oder eine GUI zur Verfügung gestellt wird.

5.3.3. Import-Format

Das Kriterium „**Import-Format**“ ist für viele Anwender/innen eine nützliche Funktion. Es ermöglicht ihnen beispielsweise ein Importieren von diversen, zuvor durchgeführten Scans oder Tests. Dadurch kann eine Zeitersparnis für eine Person entstehen, da die zuvor durchgeführten Scans anschließend in das gewünschte Tool importiert werden können, um weitere Analysen mit den Informationen durchzuführen. Daher wird bei jedem der ausgewählten Tools verglichen, welche Import-Formate von dem Tool ermöglicht werden. Diese Formate können anschließend mit den restlichen Tools verglichen werden. Hier wird überprüft ob beispielsweise Import-Formate wie “csv”, “JSON” oder “xml” ermöglicht werden.

5.3.4. Export-Format

Das Kriterium „**Export-Format**“ schafft eine Arbeitserleichterung der einzelnen Anwender. Es kann eine unterstützende Funktion sein, wenn beispielsweise gefilterte und strukturierte Daten und Informationen gesucht worden sind und diese nach einem Scan abgespeichert werden können.
Durch dieses Kriterium wird geprüft, ob es mit dem Tool möglich ist, die Daten für ein weiteres Arbeiten zu exportieren. Dies bringt den Vorteil, wenn weitere Analysen mit den gefundenen Informationen durchgeführt werden sollen, diese Informationen in ein anderes Tool erneut einzubinden.
Dieses Kriterium wird anhand der angebotenen Export-Formate des jeweiligen Tools bewertet. Hier wird überprüft, welche Export-Formate ein Tool bereitstellt, wie beispielsweise "csv”, “PDF/Textfile” oder JSON.

5.3.5. Updates

Das Kriterium „**Updates**“ ist für die Sicherheit aber auch die Aktualität eines Tools sehr wichtig. Für Anwender/innen, welche ein Tool verwenden, welches durch konstante Updates gepflegt wird, können folgende Vorteile entstehen. Es können durch konstante Feature-Updates einer Person weiterführende Features geboten werden, welche für eine weitere und detailliertere Analyse benötigt werden. Dadurch können auch die Stabilität sowie die Aktualität des Tools sichergestellt werden. Als Bewertung wird bei jedem analysierten Tool angeführt, in welchem Abstand das letzte Update durchgeführt wurde. Weiters wird kontrolliert, welche Updates durchgeführt worden sind, wie beispielsweise Sicherheitsupdates, Bug-Fixes oder Design-Updates. Da ständig Änderungen im Internet entstehen, müssen die Tools und deren Feature immer auf die neueste Technik aktualisiert werden. Ebenso muss das Produkt selber auf Schwachstellen überprüft werden und diese auch durch Aktualisierungen behoben werden.

5.3.6. Such- und Filtermöglichkeiten

Das Kriterium welches für Anwender/innen, eines Tools wichtig sein kann, ist die „**Such- und Filtermöglichkeit**“ von Daten. Dies ist wichtig, da die Datensätze, welche gespeichert werden, meist viele Informationen enthalten. Durch einen Filter oder einer Suchmöglichkeit wird einer Person angeboten die gesammelten Informationen leichter zu durchsuchen. Weiters können beispielsweise selber zusammengebaute Filter abgespeichert werden, welche für weitere Suchmöglichkeiten verwendet werden können. Auch ist es wichtig, nach welchen Suchmöglichkeiten in dem jeweiligen Tool gesucht oder gefiltert werden kann. Die möglichen Suchoptionen sind beispielsweise IP-Adressen, Namen sowie gefundene Informationen von Social Media Plattformen zu suchen und zu filtern. Es wird überprüft ob es möglich ist, das Scan Ergebnis zu filtern oder zu durchsuchen.

5.3.7. Kosten

In dieser Arbeit sind nur kostenlose Open Source Tools analysiert worden. Dennoch wurde sich das Kriterium „**Kosten**“ genauer angeschaut. Dieses Kriterium ist wichtig, da die kostenlosen Versionen

der Tools meist nicht ausreichen, da hier die Limitierungen bestehen wie beispielsweise, dass kostenlose Tools nicht kommerziell verwendet werden dürfen oder die Anzahl der erlaubten Suchanfragen schnell überschritten sind. Daher ist die Evaluierung der Kosten für ein Unternehmen von großer Bedeutung und es wurden die Tools und dessen Preisklasse analysiert. Weiters werden zu den Lizenzkosten auch die Schulungskosten analysiert, da bei einer produktiven Verwendung im Unternehmen möglicherweise eine Schulung für den/die Mitarbeiter/in benötigt wird. Bei diesem Kriterium wird überprüft, wie viele Kosten anfallen, wenn ein Tool produktiv in einem Unternehmen eingesetzt wird und ebenso dessen Schulungskosten.

5.3.8. Informationen

Das Kriterium „**Informationen**“ dient dazu, um herauszufinden, welche Informationen mit den analysierten Tools gefunden und gespeichert werden können. Da oft unterschiedliche Informationen für einen Angriff benötigt werden ist dieses Kriterium von großer Bedeutung. Es wird eine Auflistung erstellt, welche Informationen und Daten mit dem jeweiligen Tool gesammelt werden können. Daher wird zu jedem der Tools beschrieben, welche Informationen gesammelt werden können und in welcher Art diese Informationen, Hinweise über das gewünschte Ziel geben können. Dadurch kann in weiteren Schritten auch bestimmt werden, welche Angriffe durchgeführt werden können. Hier wird geprüft ob beispielsweise Informationen wie IP-Adressen, DNS, Personennamen, E-Mail-Adressen gesammelt werden können.

5.3.9. Korrektheit der Daten

Das Kriterium “**Korrektheit der Daten**” soll zeigen, wie viele falsche und richtige Informationen in einem Scan-Ergebnis vorhanden sind. Dadurch soll gezeigt werden, wie viel Aufwand entsteht, um ein Scan-Ergebnis zu bereinigen um anschließend “korrekte” Daten zu erhalten. Da in dieser Arbeit keine Angriffe getestet werden und somit kein direktes Ergebnis ersichtlich ist ob beispielsweise eine Information stimmt, kann dieses Kriterium nur anhand von Annahmen bewertet werden. Hier kann stichprobenmäßig getestet werden, ob beispielsweise die gefundenen Informationen einer Person oder einem Unternehmen zugeordnet werden können. Die Korrektheit der Daten wurde nur anhand eines Ziels geprüft, daher besteht die Möglichkeit, dass diese Bewertung bei anderen Zielen unzutreffend ist und mehr “falsche” Einträge gefunden werden.

5.3.10. Berichtsverwaltung

Das Kriterium “**Berichtsverwaltung**” soll zeigen, welche Möglichkeiten nach einem Scan-Ergebnis gegeben sind. Dadurch soll gezeigt werden, wie die Wiederverwendbarkeit eines Scan-Ergebnisses ist und ob diese übersichtlich dargestellt wird. Hier wird geprüft, ob nach der Durchführung eines Scans das Ergebnis weiterverwendet werden kann.

5.3.11. Darstellungsfunktion

Das Kriterium “**Darstellungsfunktion**” soll die Darstellung von Scan-Ergebnissen beschreiben. Damit soll gezeigt werden, welche Darstellungsformen ein Tool anbietet um ein Ergebnis eines Scans anzuzeigen. Hier wird beispielsweise geprüft, ob das Ergebnis als Tabelle oder Textfile ausgegeben wird.

5.3.12. Rückverfolgbarkeit (von Personen/Unternehmen)

Das Kriterium “**Rückverfolgbarkeit**” soll zeigen, ob die Möglichkeit besteht, mit den gesammelten Informationen Rückschlüsse zu einer Person zu finden. Dadurch soll die Richtigkeit der Informationen, sowie die Informationsqualität der Scans unter Beweis gestellt werden. Hier wird überprüft, ob es

möglich ist, mit den gefundenen Informationen Rückschlüsse auf eine Person zu bekommen wie beispielsweise, weitere Social Media Accounts oder Firmen E-Mail-Adressen. Aber auch, ob es möglich ist mit Scans persönliche Informationen zu sammeln.

5.3.13. Attacken

Das Kriterium “**Attacken**” dient dazu, um herauszufinden, welche Attacken mittels der gesammelten Informationen der diversen Tools ermöglicht werden. Hier soll gezeigt werden, welche Informationen gesammelt werden können. Aus diesen sammelbaren Informationen werden anschließend die möglichen Attacken abgeleitet.

6. Evaluierung von den Tools

In diesem Kapitel werden die ausgewählten Tools im Detail beschrieben. Zuerst erfolgt eine Beschreibung der einzelnen Tools, anschließend werden die einzelnen Kriterien der jeweiligen Tools ausgearbeitet. Durch die Ausarbeitung und dem Test der jeweiligen Tools ist es möglich zu überprüfen inwieweit die Kriterien erfüllt werden können. Darauffolgend wird analysiert, welche Informationen mit den Tools für die Angriffsarten, die im Kapitel 4.8 „*Intelligence Collections und Angriffsarten*“ beschrieben wurden, gesammelt werden konnten. Daraus ergeben sich die möglichen Angriffe, welche durchgeführt werden können.

Nachdem die Tools beschrieben worden sind, werden diese in der Praxis auf die definierten Kriterien sowie der Tauglichkeit und Verwendbarkeit getestet. Ebenso werden die jeweiligen Vorteile sowie Nachteile von einem Tool angeführt.

In dieser Arbeit ist der Fokus auf Information Gathering mittels OSINT Tools gelegt. Damit sich die Scans nur im legalen Bereich der Informationsbeschaffung bewegen, werden nur “passive” Scans[1] durchgeführt und keine “aktiven” Scans.
Um eine weitere Analyse der Tools durchführen zu können und eine Matrix davon zu erstellen, müssen die zuvor definierten Kriterien analysiert und ausgewertet werden. Somit ist die Möglichkeit gegeben, eine Gegenüberstellung und einen Vergleich der jeweiligen Tools durchzuführen.

Die Social Media Scans in diesem Abschnitt sind mit den Default-Einstellungen eines Social Media Profils durchgeführt worden, da diese Einstellungen unmittelbar nach der Erstellung eines Accounts aktiv sind. Der Grund für das Belassen der Default-Einstellungen ist, dass die Anwender/innen möglicherweise kein Wissen darüber haben, welche Informationen überhaupt mit den Default-Einstellungen für andere Personen sichtbar sind.
Bei Twitter ist beispielsweise nach dem Erstellen eines Accounts die Funktion “Deine Tweets schützen (Protect your Tweets)” nicht standardmäßig aktiv, welches in Abbildung 3 „*Twitter Protect your Tweets*“ zu sehen ist. Das heißt, es sehen die Tweets nicht nur “Follower”, sondern die geposteten Tweets sind öffentlich verfügbar. Ein weiteres Kriterium ist möglicherweise, dass User nicht wissen, welche Einstellungen gesetzt werden können oder gesetzt werden müssen und welche Standardeinstellungen generell gesetzt sind. Teilweise ist erkenntlich, dass die Standardeinstellungen schlecht gesetzt sind, womit bereits viele Informationen ausgelesen werden können. Durch falsch gesetzte Privacy Einstellungen können beispielsweise Firmen ihre eigenen Mitarbeiter ausspionieren. Weiters können Unternehmen vor einem Vorstellungsgespräch Recherchen über den Bewerber durchführen und sich im Vorhinein schon Informationen über diese Person speichern.

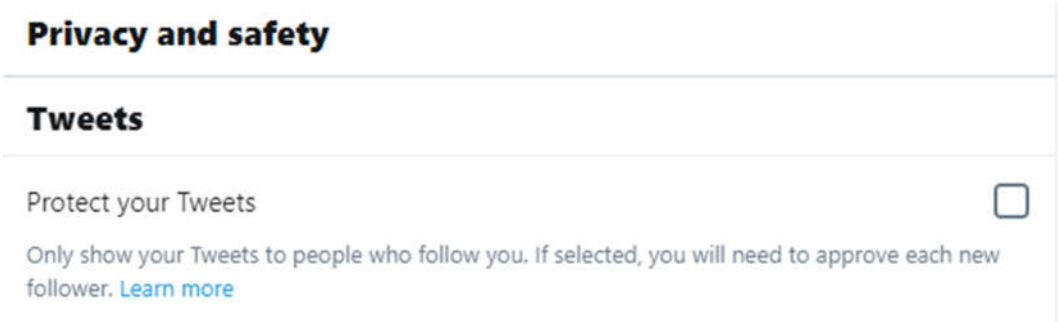


Abbildung 3 Twitter Protect your Tweets

[1] Die durchgeführten Scans und dessen Ergebnisse sind in der beigelegten CD ersichtlich.

* Die durchgeführten Scans und dessen Ergebnisse sind in der beigelegten CD ersichtlich.
In Kapitel 7 „*OSINT Use Case*“ werden verschiedene Anwendungsbeispiele beschrieben, welche mit den analysierten Tools und den gefundenen Informationen durchführbar sind.
In den Beispielen wird auf das Finden von Schwachstellen in einem Unternehmen, sowie auf Phishing Angriffe und auf die Gefahren von Social Media Plattformen eingegangen.

6.1. Maltego

6.1.1. Beschreibung

Zu Beginn wurde das Tool „Maltego“ im Detail geprüft. Das Tool wurde auf der virtuellen Maschine Kali-Linux „*Linux DB 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64 GNU/Linux*“ getestet.
Das Tool ist bereits standardmäßig auf der virtuellen Maschine enthalten, daher war eine manuelle Installation nicht notwendig. Die initiale Einrichtung des Tools konnte mit diversen Anleitungen aus dem Internet durchgeführt werden. [107] [108]
Von dem Tool werden verschiedene Hinweise und Beschreibungen gegeben, um die Einrichtung zu vereinfachen. Das Tool bietet drei verschiedene Versionen an, davon ist eine kostenlos. In dieser Arbeit wurde die kostenlose Version “Maltego Community Edition 4.2.7.12570” verwendet.
Dies ist die Community Version, welche folgende Limitierungen im Gegensatz zu der kommerziellen Version aufweist, wie beispielsweise:

- Keine kommerzielle Nutzung
- Kein technischer Support
- Max. 12 Transformationen [109]

Nachdem die Version ausgewählt worden ist, wird ein Account erstellt. Mit diesem Account wird sich anschließend im Tool eingeloggt. Falls für Personen bei der Verwendung des Tools Unklarheiten entstehen, stellt das Tool eine umfangreiche und kostenlose Dokumentation zur
Verfügung, damit können Fragen geklärt werden.
Die vorhandenen Dokumentationen sind sehr verständnisvoll geschrieben und es gibt weiters noch Videos, welche sich mit den Tools beschäftigen und es erklären.
Das Tool ist für einen „Beginner/in“ sehr leicht gehalten und gibt etliche Hinweise und Beschreibungen der jeweiligen Funktionen. Um eine bessere Handhabung und ein besseres Verständnis für das Tool zu bekommen, werden Kurse für verschiedene Schwierigkeiten angeboten.

6.1.2. Allgemein

Bei diesem Tool handelt es sich um ein Datensammlungsprogramm. Das Tool sammelt verschiedene öffentliche Informationen aus dem Internet. Diese gesammelten Daten werden anschließend in einer Grafik dargestellt in welcher die Verbindungen sowie Zusammenhänge der gefundenen Informationen ersichtlich sind. Das Tool bietet für weniger erfahrene Personen eine gute Grundlage, da die verschiedenen Scan Funktionen beschrieben sind. So können beispielsweise Webseiten, Suchmaschinen sowie Datenbanken und Social Media Accounts wie Twitter durchsucht werden. Die jeweils neu gefundenen Informationen eines Scans können wie oben bereits erwähnt, Zusammenhänge erkennen und sich automatisch in Verbindung mit bereits gefundenen Informationen bringen. Somit ist es möglich ein “Big Picture” eines Unternehmens oder einer Person zu erstellen. Es werden somit die Ergebnisse für eine Person in einer übersichtlichen Form dargestellt.

Um erste Informationen über ein Ziel zu bekommen, werden verschiedene Möglichkeiten für einen Scan angeboten wie “Telefonnummer”, “Domain”, “E-Mail-Adressen”, “Alias”, “Organisationen”, “Personengruppen”, “Unternehmen”, “DNS” sowie “IP-Adressen” und “Daten” und “Dokumente”.

Eine wichtige Funktion des Tools ist die Import- und Export Funktion. Es wird von dem Tool ermöglicht einen Scan als “xls”, “xlsc” (Excel Spreadsheets) und “csv” (Comma-separated values) zu importieren. Als Export Funktion bietet das Tool beispielsweise ein PDF/Textfile oder “csv”-File.
Das hat den Vorteil, dass die gesammelten Informationen in einem von Menschen lesbaren Format exportiert werden können.

6.1.3. Kriterien Beschreibung

Zuerst wird das Kriterium „**Plattform**“ analysiert. Das Tool „Maltego“ wird auf den Plattformen „Windows“, „Linux“ sowie „iOS/MAC“ unterstützt.
Da alle gängigen Plattformen unterstützt werden, können Anwender/innen ihre gewohnte Umgebungsplattform verwenden und es muss keine neue Plattform verwendet werden.

Anschließend wird das Kriterium “**GUI/CLI**” geprüft. Es wird von dem Tool eine GUI bereitgestellt. Die GUI bietet sowohl erfahrenen wie auch eher unerfahrenen Personen eine intuitive Bedingung und Übersicht der einzelnen Funktionen. Es wird keine CLI von dem Tool zur Verfügung gestellt.

Das nächste Kriterium behandelt das „**Import-Format “** von Dateien in das Tool. Das Tool ermöglicht das Importieren von “csv”-Dateien und es sind weiters keine Limitierungen der Einträge des importierten Files gegeben. Um dies zu testen wurde eine Liste erstellt, welche mit 1000 Einträgen befüllt worden ist, hier sind keine Probleme bei dem Importiren des Files aufgetreten. Weiters können auch noch “Entitäten” von anderen Scans eines Users importiert werden.

Nach dem das Kriterium “Import-Format” überprüft worden ist, wurde weiters auch das Kriterium „**Export-Format “** überprüft. Es werden von diesem Tool eine Vielzahl von Export-Möglichkeiten gegeben, wie „xls“, “xlsx“ sowie „csv“ Daten.

Das Kriterium „**Updates**“ hat bei diesem Tool einen sehr hohen Stellenwert. Nach Überprüfung der regelmäßigen Updates, welche aus den Change-Logs hervorgehen, wurden regelmäßige Update-Intervalle festgestellt. Es werden kontinuierlich Sicherheitsupdates und Bugfixes durchgeführt. Weiters wird das Tool regelmäßig mit neuen Funktionen ausgestattet. Das letzte Update wurde am 12.11.2019 durchgeführt (Stand 15.11.2019). [110]

Bei dem Kriterium „**Suchmöglichkeit und Filtermöglichkeit“** ist es mittels „Maltego“ möglich, direkt in dem Tool nach verschiedenen Informationen zu suchen. Dadurch bietet das Tool die Möglichkeit, dass nach einem Scanvorgang beispielsweise nach DNS, IP-Adressen, Personen und E-Mails gesucht werden kann. Weiters wird die Möglichkeit gegeben, den gesamten Suchverlauf und die damit verbundenen Ergebnisse und Informationen abzuspeichern. Diese können als Bild (PNG, nur in der Pay-Version), Excel (Tabelle), Report (PDF) sowie ein XML File abgespeichert werden. Jedes dieser heruntergeladenen Files ist durchsuchbar in einem von Menschen lesbaren Format.

Anschließend wird sich das Kriterium „**Kosten“** genauer angeschaut und beschrieben. Bei Maltego sind drei Versionen verfügbar. Es gibt eine “Maltego XL”-Version, diese kommt auf einen Preis von 1799€ jährlich. Die zweite kostenpflichtige Version ist die “Maltego Classic”-Version, diese kommt auf einen Preis von 899€ p.a. Es gibt weiters eine kostenlose Version des Tools, dies wäre “Maltego CE”. Die “Maltego CE”-Version ist die Community Version des Tools, welche ein paar Einschränkungen beinhaltet. Es handelt sich hier um eine nicht kommerzielle Version. Weiters sind Limitierungen vorhanden im Bereich von Entitäten und Transformationen, welche zurückgegeben werden können und es sind keine Grafikexportfunktionen möglich.
Bei einem Trainingskurs welcher direkt auf der Webseite von Maltego angeboten wird, liegt der Preis von einer Schulung für zwei Tage bei 15.000€. Es wurden weitere Schulungen mit einer Preisspanne von 390€ bis 1999€ gefunden, welche ebenso meist zwei Tage dauern. [111]

Das Kriterium “**Informationen“** ist bei dem Tool ausgeprägt, da es einem die Möglichkeit bietet, die gefundenen Daten zu exportieren und beispielweise in Excel zu importieren.
Maltego kann folgende Informationen sammeln:

- Personen/Namen/E-Mail-Adressen/Alias
- Gruppen von Personen (Social Media Netzwerke)
- Unternehmen
- Organisationen
- Webseiten
- DNS/Domains/Internet-Infrastrukturen
- Verbindungen/Zugehörigkeiten
- Dokumente/Files

Das Kriterium “**Korrektheit der Daten**” wurde anschließend analysiert. Das Tool ermöglicht das Sammeln von verschiedenen Informationen. Bei diesen Informationen wie beispielsweise der Namenssuche können “falsche” Einträge gefunden werden, diese müssen anschließend entfernt werden. Dennoch haben die gefundenen Informationen eine hohe Korrektheit. Es wurden die gefundenen E-Mail-Adressen anhand der Webseite der Fachhochschule verglichen. Weiters wurden die Ergebnisse mit dem Fake Social Media Profil verglichen. Die gefundenen Informationen waren einer Person oder dem Fake-User zuordbar.

Darauffolgend wurde das Kriterium “**Berichtsverwaltung**” analysiert. Es wird ermöglicht ein PDF über einen durchgeführten Scan zu erzeugen, ebenso können “XLS” und “CSV” Formate exportiert werden. Durch diese Vielfalt können die Berichte der Scans für weitere Untersuchungen verwendet werden.

In weiterer Folge wird das Kriterium “**Darstellungsfunktionen**” überprüft. Dadurch, dass verschiedene Export-Formate angeboten werden, können die Berichte beispielsweise in Tabellenformat oder auch als Textfile/PDF angezeigt werden. Somit ist eine übersichtliche Darstellung der Ergebnisse möglich und die durchgeführten Scans sind für Menschen lesbar.

Das Kriterium “**Rückverfolgbarkeit**” wurde anschließend geprüft. Jeder durchgeführte Scan mit dem Tool, wird übersichtlich mittels einer Punkte-Grafik ausgegeben, welche in Abschnitt 5.1.4 ersichtlich ist. Bei jedem weiteren Scan von einem Ziel werden die Verbindungen untereinander automatisch neu verknüpft. Jeder Knoten, welcher eine Verbindung darstellt, kann separat kopiert und im Detail analysiert werden. Durch diese Verknüpfungen entsteht eine übersichtliche Strukturierung der Ergebnisse. Je nachdem welche API-Keys verwendet werden und auf welche Suchkriterien sich spezialisiert wird, können verschiedene Informationen über ein Ziel gefunden werden. Mit den gesammelten Informationen können Recherchen über Personen oder Unternehmen stattfinden. Ebenso können Angriffsziele, auf mögliche Schwachstellen überprüft werden.

Für welche „Attacken“ können die gefundenen Informationen verwendet werden:
Mit den Informationen, die aus dem Tool generiert werden können, ist es möglich verschiedene Angriffsarten durchzuführen. Beispielsweise können an die im Scan gefundenen E-Mail-Adressen Phishing-E-Mails gesendet werden. Durch die versendeten Phishing Mails kann auch Ransomware in den Anhängen von E-Mails verteilt werden. Es ermöglicht Angreifern auch eine Malware wie Virus und Würmer an die Mail Adresse zu senden, welche meist als Anhänge und in legitimen Office-Dokumenten oder in Links versteckt werden können. Ein weiterer Angriff könnte Identity Theft sein. Dies wird durch das Zusammenführen von verschiedenen personenbezogenen Informationen ermöglicht. Eine weitere Angriffsart ist das Cyber Stalking, dies ist durch das Preisgeben von verschiedenen Informationen auf diversen Social Media Plattformen möglich. Diese Angriffsarten sind im Detail in Kapitel 4.8 „*Intelligence Collections und Angriffsarten*“ beschrieben.

6.1.4. Praktischer Test

Anschließend wurde das Tool auf die Praxistauglichkeit geprüft. Es wurden in diesem Beispiel keine Änderungen der Default-Einstellungen vorgenommen. In den praktischen Tests konnte Maltego den für den Test erstellten Kommentar “sun is up #goodmorning” erfolgreich finden und direkt mit dem User “Kinimod Karub” in Verbindung bringen, von dem dieser Kommentar erstellt wurde, siehe Abbildung 4 „Maltego Twitter Scan“.

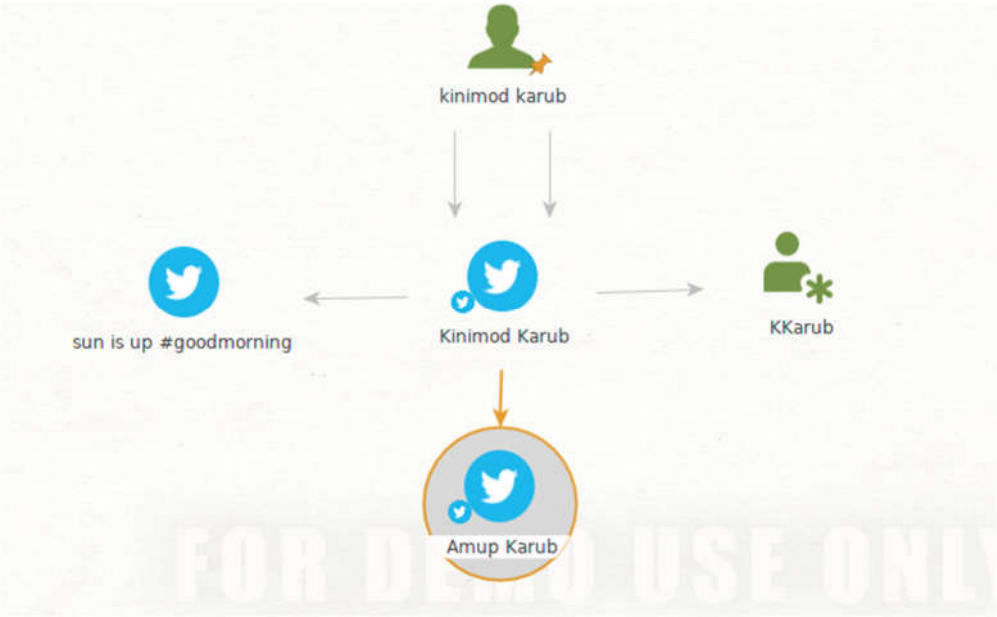


Abbildung 4 Maltego Twitter Scan

Weiters wurde in den Tests eine Follow-Anfrage (Freundschaftsanfrage) an einen neuen Twitter-User mit dem Namen “Amup Karub” gesendet.
Mit diesem Test soll geprüft werden, welche Informationen mit dem Tool gesehen und gesammelt werden können, um verschiedene Verknüpfungen zu bilden. Daher wird überprüft ob die Follow-Anfrage mit dem Tool zu erkennen ist. Nach einer neuen Suche konnte sowohl der zuvor angelegte Kommentar von User “Kinimod Karub” erneut gefunden werden, weiters wurde auch über den User “Kinimod Karub” die Kommentare vom User “Amup Karub” gefunden. Ersichtlich ist, dass der User “Amup Karub” mit dem User “Kinimod Karub” verbunden ist, somit ist die Follow-Anfrage, welche akzeptiert wurde, ebenso erkennbar. Es ist auch der Tweet ersichtlich, welcher von dem User “Amup Karub” gepostet worden ist, siehe Abbildung 5 „*Maltego Twitter Scan 2*“.

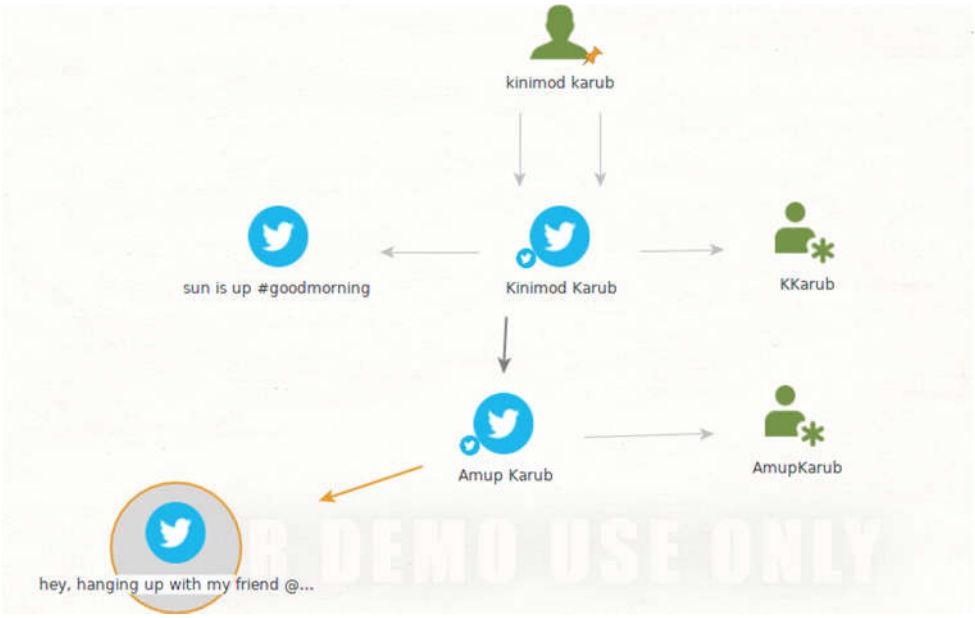


Abbildung 5 Maltego Twitter Scan 2

Anschließend wurde eine Überprüfung der Fachhochschule St. Pölten durchgeführt.
Diese Scan Übersicht gibt die gefundenen Einträge wieder, welche mit der Legende verglichen werden kann. In Abbildung 6 „*Maltego Big Picture*“ ist das “Big Picture” des Scans der Fachhochschule zu sehen und Abbildung 7 „*Maltego Big Picture Legende*“ zeigt die dazugehörigen Legenden.

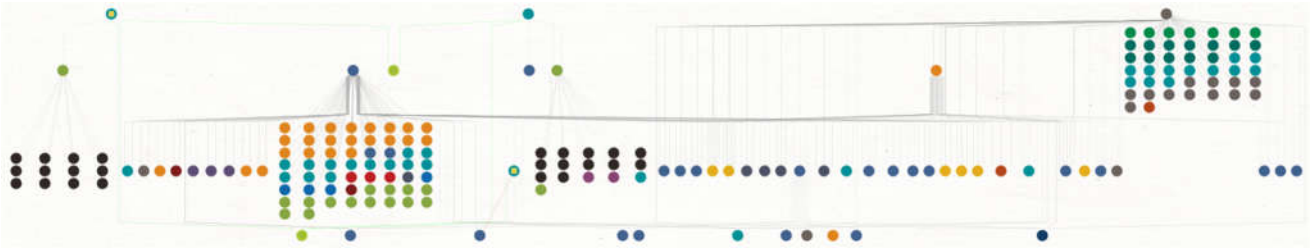


Abbildung 6 Maltego Big Picture

Abbildung 7 Maltego Big Picture Legende

Dieser Scan hat wie in der Legende erkennbar ist, verschiedene Informationen gefunden. Der Scan wurde zuerst mit einem “Webseiten” Scan begonnen. Anschließend wurde der Scan noch mit DNS und Domain erweitert, um mehr Ergebnisse zu bekommen. Hier ist ersichtlich, dass gewisse Informationen eine Verbindung miteinander herstellen können. Diese Zusammenhänge sind nach dem jeweiligen Scan automatisch verbunden worden.

Wie in Abbildung 8 „*Maltego DNS Scan*“ zu sehen ist, wurden beispielsweise folgende DNS-Einträge gefunden.

Abbildung 8 Maltego DNS Scan

Mit dem Tool können verschiedene Kategorien und deren enthaltene Informationen gefunden werden, welche in der oben gezeigten Abbildung 7 „*Maltego Big Picture Legende*“ ersichtlich ist, wie beispielsweise DNS, IP-Adressen, Locations oder Personen.

Weiters wurde getestet, welche Verbindungen das Tool mit einer E-Mail-Adresse herstellen kann. Für diesen Scan wurde ein beliebig ausgewählter Mitarbeiter der Fachhochschule herangezogen und dessen E-Mail-Adresse von der Webseite der Fachhochschule genommen. Dieser Scan wurde in dem bereits durchgeführten Scan der Fachhochschule durchgeführt. Das Tool stellt automatisch eine Verbindung zu dem Domain-Eintrag “fhstp.ac.at” her, ohne dass dies manuell durchgeführt werden muss. Dies ist möglich, da sich Maltego die Domain hinter dem “@” Zeichen automatisch nimmt.

Anschließend wurde überprüft welche Informationen gefunden werden können. Es sind weitere E-Mail-Adressen von Arbeitgebern ersichtlich, welche dazu verwendet werden können weitere Recherchen über den Mitarbeiter und den beruflichen Werdegang zu informieren, da ebenso Firmen E-Mail-Adressen gefunden worden sind. Grundsätzlich sollten diese Informationen aber gründlich überprüft werden, da es Personen mit demselben Namen gibt und somit eine Verzerrung der

Ergebnisse stattfinden kann. In Abbildung 9 „*Maltego Personen/E-Mail-Adresse Scan*“ wird gezeigt, wie es aussieht, wenn eine E-Mail-Adresse eines Mitarbeiters genauer überprüft wird und Rückschlüsse auf weitere Unternehmen geben kann. Das Tool überprüft zugleich, ob auf der Webseite “haveibeenpwned” Zugangsdaten zu dieser E-Mail-Adresse vorhanden sind und somit eine Bedrohung besteht, dass dieser Account übernommen werden kann. [112]

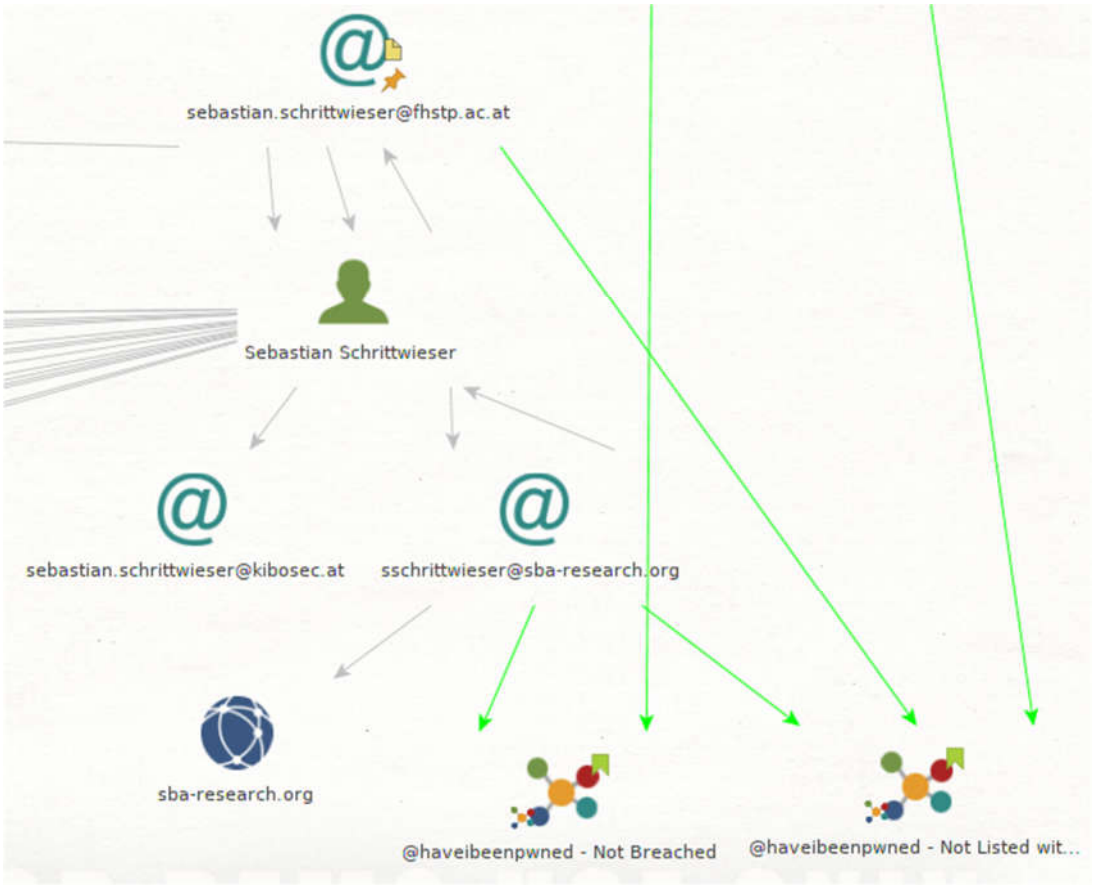


Abbildung 9 Maltego Personen/E-Mail-Adresse Scan

6.1.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests

Eine Auffälligkeit gab es bei dem Erstellen der Fake-Accounts auf Twitter. Es wurden für die verschiedenen Tests Fake User mit Fake E-Mail-Adressen auf Twitter registriert. Um die verschiedenen E-Mail-Adressen für die “Fake-Profile” zu erstellen wurde “GMX” und “GMAIL” verwendet.

Name	E-Mail-Adresse + Anbieter	Aktiv/Gesperrt
Kinimod Karub	GMAIL	Aktiv
Hubertus Osint	GMAIL	Aktiv
Hubert von OSINT	GMX	Gesperrt
Amup Karub	GMX	Gesperrt
Cat Karub	GMX	Gesperrt
Amanda dermichknutscht	GMX	Gesperrt

Tabelle 8 Erstellte Fake-E-Mail Adressen

Nach geraumer Zeit der Verwendung des Twitter-Accounts wurde bemerkt, dass der Account von “Hubert von OSINT” nicht völlig funktionsfähig ist und gesperrt wurde. Dieser wird erst nach Hinterlegung einer Telefonnummer wieder freigeschaltet. Dieser Twitter Account wurde gleichzeitig mit dem Account “Hubertus Osint” angelegt, bei diesem wurden hingegen keine Schwierigkeiten einer Autorisierung mit der Telefonnummer festgestellt. Nach weiteren Tests wurde ersichtlich, dass die Accounts welche mit einer “GMX” E-Mail-Adresse angelegt worden sind, nach kurzer Zeit gesperrt werden, außer es wird bei dem Account eine Telefonnummer hinterlegt. Hingegen sind die Accounts welche mit einer “GMAIL” E-Mail-Adresse angelegt worden sind nicht gesperrt worden. Daraus wurde die Erkenntnis gezogen, dass ein Account mit einer “GMAIL” Adresse als vertrauenswürdiger eingestuft wird.

6.1.6. Ergebnisse und Fazit

Über den Fake User “Kinimod Karub” ist anfangs, ohne dass etwas gepostet worden ist, nur der Name des Users auf Twitter ersichtlich. Darauffolgend wurde ein Tweet von dem User gepostet, welcher mit dem Tool ersichtlich war. Anschließend wurde von einem zweiten Fake-Account eine Follow-Anfrage gesendet und es wurde ein Tweet an “Kinimod Karub” gesendet. Mit dem Tool wurde geprüft ob dieser Tweet sowie das Folgen des Accounts ersichtlich ist. Die Informationen des Posts sowie dass der Person gefolgt wird, waren ersichtlich.
Ein weiteres interessantes Ergebnis lieferten die Accounts, welche mit einer Telefonnummer bestätigt werden müssen. Von diesen Accounts wurde bevor eine Telefonnummer Hinterlegung gewünscht worden ist, Tweets an “kinimod Karub” versendet. Diese Tweets sind zuvor gesehen worden, nachdem aber die Telefonnummer hinterlegt werden muss, sind diese Tweets nicht mehr mit dem Tool Maltego zu sehen.

Anschließend werden die positiven sowie die negativen Auffälligkeiten des Tools angeführt.

Positiv aufgefallen ist:

- Kann sich mit Social Media Plattformen verbinden z.B.: getestet mit Twitter
- Gefundene Informationen kann Maltego automatisch verknüpfen
- Grafische Darstellung der Scan Ergebnisse
- GUI
- Übersichtlichkeit
- Zeitersparnis, da viel automatisch durchgeführt wird (Verbindungen)

Negativ aufgefallen ist:

- Sehr umfangreich und komplex zu Beginn, da viele Funktionen nicht bekannt sind und erst erlernt und getestet werden müssen.

6.2. TheHarvester

6.2.1. Beschreibung

Das Tool “TheHarvester” (Ver. 3.0.6) ist auf der virtuellen Maschine von Kali-Linux standardmäßig installiert, daher wird eine manuelle Installation nicht benötigt. Für dieses Tool sind online verschiedene Dokumentationen sowie Videos verfügbar, dadurch wird einem neuen User eine schnellere Einführung in dieses Tool ermöglicht. Weiters wird direkt vom Tool eine Bedienungshilfe beim Ausführen des Tools geboten, da eine Liste erscheint, mit möglichen Eingabeparametern sowie Scan-Beispielen.

6.2.2. Allgemein

Mit diesem Tool ist es möglich Informationen über Personen und Unternehmen heraus zu finden. Weiters ist das Tool darauf ausgelegt nach E-Mail-Adressen von Personen oder Unternehmen zu suchen. Ebenso Sub-Domains und Hosts können mit dem Tool ausfindig gemacht werden.
Das Tool soll eine Unterstützung für beispielsweise Penetration-Tester sein, da verschiedene Informationen über ein Unternehmen gefunden werden können. Es können mit dem Tool noch weitere Informationen wie beispielsweise “offene Ports” von IT-Systemen, welche über das Internet erreichbar sind und “Banner” gefunden werden. Bei einem “Banner” handelt es sich beispielsweise um ein Bild oder eine Werbefläche, welches den Namen einer Webseite enthält. Diese Daten werden von verschiedenen öffentlichen Quellen gesammelt.

Es können sich Unternehmen selber scannen und somit selbst prüfen, welche Daten und Informationen öffentlich frei zugänglich und verfügbar sind. Diese Informationen sind jedoch auch für einen Angreifer ersichtlich, daher können präventive Maßnahmen gesetzt werden. Für die Verwendung des Tools ist keine Anmeldung oder Registrierung notwendig. Es werden jedoch für spezielle Plattformen wie beispielsweise LinkedIn oder Twitter ein API-Key benötigt.

Bei der ersten Inbetriebnahme war ersichtlich, dass es sich um ein CLI-Tool (Command Line Interface) handelt. Das Tool wurde mittels des Befehls “TheHarvester” auf der CLI gestartet. Nachdem der Befehl ausgeführt worden ist, wurden von dem Tool als Bedienungshilfe einige mögliche Befehle vorgeschlagen, um das Tool zu bedienen. Es kann beispielsweise nach “Domain” oder “Data Sources” gesucht werden. Alle Scans, welche mit dem Tool durchgeführt werden, können abgespeichert werden, um sie später im Detail zu analysieren. Es werden vier verschiedene Files gespeichert, hier handelt es sich um zwei html-Files, ein xml-File und ein sqlite-File. Bei einem sqlite File handelt es sich um ein Datenbankfile. Die HTML-Files können direkt in einem Internetbrowser geöffnet werden. Das “xml” File kann anschließend in Excel geöffnet werden.

6.2.3. Kriterien-Beschreibung

Das Kriterium “**Plattform**” ist das erste Kriterium, welches überprüft wird. Das Tool “TheHarvester” ist auf “Windows”, “Linux” sowie auf „iOS/MAC“ lauffähig, somit ist es auf allen gängigen Plattformen verfügbar.

Als nächstes Kriterium wurde “**GUI/CLI**” geprüft. Es wird von dem Tool “TheHarvester” nur eine CLI zur Verfügung gestellt, daher könnte es sein, dass Personen, welche zuvor noch keine CLI verwendet haben, eine Einlernphase benötigen.

Das nächste wichtige Kriterium, welches nachgeprüft wurde, ist der "**Import**" von Ergebnissen Daten oder Informationen. Es wird keine Import Funktion zur Verfügung gestellt, um bereits exportierte Ergebnisse von diversen anderen Scans zu importieren.

Darauffolgend wurde das Kriterium "**Export**" analysiert. Das Tool ermöglicht es von den durchgeführten Scans einen Export durchzuführen. Dies ist nützlich, wenn die gefundenen Informationen von einem Scan wiederverwendet werden wollen oder zu einem späteren Zeitpunkt analysiert werden möchten. Es können folgende Formate exportiert werden "html", "xml" und "sqlite".

Ebenso wurde das Kriterium "**Update**" betrachtet. Das Tool nimmt dieses Kriterium sehr ernst. Es ist auf GitHub [42] ersichtlich, dass in regelmäßigen Abschnitten von circa drei Monaten Änderungen und Verbesserungen sowie Bugfixes und Versionserneuerungen vorgenommen werden. [113]
GitHub wurde von Chris Wanstrath, PJ Hyett, Scott Chacon und Tom Preston-Werner entwickelt. Es handelt sich hier um einen Onlinedienst, welcher Software Entwicklungsprojekte auf deren Servern bereitstellt.

Das nächste Kriterium, welches analysiert wurde, ist "**Such- und Filtermöglichkeiten**". Es werden von dem Tool verschiedene Such- und Filtermöglichkeiten zur Verfügung gestellt. Das Tool ermöglicht vor dem Scan eine Filterung, indem bei dem Scanbefehl beispielsweise angegeben werden kann, auf welchen Social Media Plattformen gesucht werden soll. Es kann ebenso im Befehl mitgegeben werden, auf welchen Suchmaschinen gesucht werden soll und wie viele Einträge durchsucht werden sollen. Durch das Exportieren von "html", "xml" und "sqlite" können die gefundenen Daten anschließend in weiteren Tools gefiltert und durchsucht werden.

Anschließend wird das Kriterium "**Kosten**" analysiert. Es fallen bei diesem Tool keine Kosten an. Für Weiterbildungen gibt es verschiedene Dokumentationen, welche einige Bereiche des Tools abdecken und beschreiben. Da dieses Tool keine GUI anbietet und zu wenig komplex ist und auch nur eine beschränkte Anzahl an Funktionen anbietet, sind für dieses Tool Kurse zu aufwändig. Hier reicht ein Selbststudium/Einarbeitung, um diese Funktionen zu erlernen.

Das Kriterium "**Informationen**" wurde als nächstes überprüft. Es können folgende Informationen mit dem Tool gefunden werden:

- E-Mail-Adresse
- Sub-Domains
- Hosts
- Namen
- IP-Adressen
- Ports/Banner

Es wurde anschließend das Kriterium "**Korrektheit der Daten**" analysiert. Um dieses Kriterium zu überprüfen wurden die E-Mail-Adressen sowie die Hosts stichprobenmäßig überprüft. Um dies zu kontrollieren wurden gesammelte E-Mail-Adressen mit den auf der Webseite der Fachhochschule verfügbaren E-Mail-Adressen geprüft. Ebenso wurden die privaten "bekannten" E-Mail-Adressen überprüft und gegengeprüft. Bei der Korrektheit der Daten ist das Tool sehr gut aufgestellt und es sind nur einzelne Nacharbeiten nötig.

Folgend wird das Kriterium "**Berichtsverwaltung**" analysiert. Es ist möglich mit dem Tool Berichte zu erstellen. Diese Berichte können als "html" sowie "xls" Dateien erstellt werden und für weitere Analysen wiederverwendet werden.

Darauf wurde das Kriterium "**Darstellungsfunktionen**" überprüft. Die Files, die von dem Tool bereitgestellt werden, sind "xls" und "html". In dem "html" File wird zuerst grafisch ein Balkendiagramm

gezeigt, welches Scan-Ergebnisse übersichtlich darstellt, welches in Abbildung 10 „*Abbildung 10* TheHarvester Dashboard“ ersichtlich ist. Weiters wird ein “xls”-File erstellt, hier werden die gefundenen Informationen in einer Tabelle aufgezeigt.

Das Kriterium “**Rückverfolgbarkeit**” wurde anschließend überprüft. Es werden von dem Tool beispielsweise E-Mail-Adressen gefunden, welche Rückschlüsse auf den realen Namen einer Person geben können. Um die Rückverfolgbarkeit zu überprüfen, wurden stichprobenmäßig die gefundenen E-Mail-Adressen mit den E-Mail-Adressen der FH St. Pölten überprüft. Weiters sind verschiedene Hosts, welche mit dem Ziel in Verbindung gebracht werden, aufgelistet.

Für welche „Attacken“ können die gefundenen Informationen verwendet werden:
Durch die gefundenen Informationen können verschiedene Angriffsarten durchgeführt werde. Es ist möglich mittels der E-Mail-Adresse Phishing oder Ransomware-Angriffe durchzuführen sowie Würmer und Viren zu verteilen. Weiters kann durch die Information der Sub-Domains ein “Man-in-the-Middle" Angriff durchgeführt werden. Mittels der IP-Adresse können “DoS” und “IP-Spoofing” Angriffe durchgeführt werden.
Es besteht die Möglichkeit, dass mit den gefundenen E-Mail-Adressen Informationen über den “realen” Namen einer Person herausgefunden werden können. Damit können anschließend genauere Recherchen über eine Person stattfinden und beispielsweise Cyber Stalking durchgeführt werden. Diese Angriffsarten sind im Detail in Kapitel 4.8 „*Intelligence Collections und Angriffsarten*“ beschrieben.

6.2.4. Praktischer Test

Mit dem Tool „TheHarvester“ ist es möglich Unternehmensinformationen auszuforschen, daher wurde bei der Durchführung des praktischen Tests der Fokus auf die Fachhochschule St. Pölten gelegt. Es wird bei diesem Test überprüft, welche Daten und Informationen über die Fachhochschule gesammelt und gespeichert werden können.

Das Tool ermöglicht nach dem Abschluss des Scans eine automatische Speicherung des Ergebnisses. Da die Scans gespeichert und exportiert werden können, wird es einem User ermöglicht, den Scan im Detail zu begutachten und zu analysieren. Weiters werden dadurch eine Filterung und eine Suche der Ergebnisse ermöglicht.

Um das Tool optimaler zu verwenden und ein besseres Suchergebnis zu erzielen wird der API-Key von Hunter.io und Shodan hinzugefügt. Folgender Befehl wurde für das Suchen nach Daten verwendet:
”theharvester -d fhstp.ac.at -l 500 -b all -f Schreibtisch/theharvesterScan/fhstp5”

Anschließend können die Files, welche in dem Ordner “theharvesterScan” angelegt worden sind, analysiert werden. Es werden zwei Files angelegt, ein “html”-File und ein “xml”-File. Dadurch wird es einer Person ermöglicht, das Scan-Ergebnis im Detail zu filtern und zu analysieren. Eine Abbildung des html-File sowie des xml-File ist im Anhang „TheHarvester html-Scan-File“ und Anhang „TheHarvester xml-Scan-File“ zu sehen.

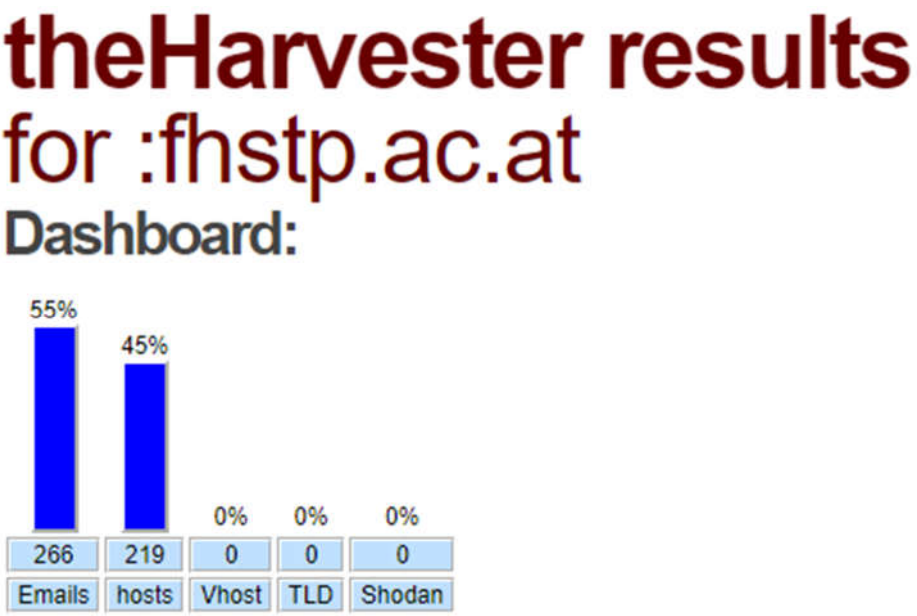


Abbildung 10 TheHarvester Dashboard

Ersichtlich ist, dass die Ergebnisse sehr übersichtlich in dem “html”-File dargestellt werden. Bei dem Öffnen des Files wird zuerst eine Gesamtanzahl der gefundenen Ergebnisse in einem Balkendiagramm gezeigt. Es wird hier die Anzahl der gefundenen Informationen gegeben von “E-Mails”, “Hosts”, “Vhost (Virtuelle-Host)”, “TLD (Top Level Domain)” und “Shodan” (Computer-Suchmaschine).

Aus dem durchgeführten Scan der “FH St. Pölten” ist bemerkbar, dass mit dem Tool viele E-Mail-Adressen gefunden werden können. Neben den E-Mail-Adressen sind verschiedene Hosts gefunden worden, welche einerseits mit Namen als auch mit IP-Adresse angezeigt werden. Unter dem Balkendiagramm werden die gefundenen Informationen übersichtlich in der jeweiligen Kategorie angezeigt, was in Abbildung 11 „*TheHarvester E-Mail Scan*“ sowie Abbildung 12 „*TheHarvester Host Scan*“ zu sehen ist. Ein Host, welcher beispielsweise ein Computer sein kann, kommuniziert mit anderen Hosts im Netzwerk. Es gibt verschiedene Arten von Hosts wie Web-Hosts, Cloud-Hosts, Virtueller-Host oder Remote-Host, diese werden in dieser Arbeit jedoch nicht weiter erklärt. Von einem Host werden Dienste für andere Computer bereitgestellt. [114]

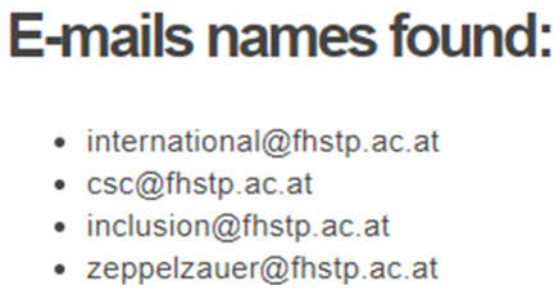


Abbildung 11 TheHarvester E-Mail Scan

Hosts found:

- *.fhstp.ac.at:empty
- .fhstp.ac.at:empty
- .liveweb.fhstp.ac.at:empty
- .mdh.fhstp.ac.at:empty
- .media.fhstp.ac.at:empty
- .nwt.fhstp.ac.at:empty
- .students.fhstp.ac.at:empty
- 25252Fsso.fhstp.ac.at:empty
- 2Fsso.fhstp.ac.at:empty
- Bewerbung.fhstp.ac.at:91.219.69.26

Abbildung 12 TheHarvester Host Scan

Weiters können von dem Tool offene Ports gefunden werden. Um dies mit dem Tool scannen zu können, wird der API-Key von Shodan [115] benötigt. Anschließend kann ein Scan auf das Ziel durchgeführt werden, welcher in der Abbildung 13 „*TheHarvester Scanergebnis Auszug*“ als kurzer Auszug des durchgeführten Portscans gegeben ist. Für eine bessere Ansicht wurde der Output in einen Texteditor kopiert.

IP address	Hostname	Org	Services:Ports	Technologies
91.2[redacted]	Not in Shodan	Not in Shodan	Not in Shodan	Not in Shodan
91.2[redacted]	Not in Shodan	Not in Shodan	Not in Shodan	Not in Shodan
91.2[redacted]	ris[redacted]	Fachhochschule St. Poelten GmbH	OpenSSH:22, OpenSSH:20000	
91.2[redacted]	ris[redacted]	Fachhochschule St. Poelten GmbH	None:30231, None:2021	
91.2[redacted]	Not in Shodan	Not in Shodan	Not in Shodan	Not in Shodan
91.2[redacted]	ris[redacted]	Fachhochschule St. Poelten GmbH	None:53, None:53	

Abbildung 13 TheHarvester Scanergebnis Auszug

6.2.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests

Das Tool ermöglicht einem Angreifer Informationen in kurzer Zeit über ein Ziel zu sammeln.
Es werden von dem Tool verschiedene API-Keys (Application Programming Interface) wie beispielsweise “hunter.io” und “Shodan” unterstützt, diese zwei API-Keys sind auch bei den Scans verwendet worden. Da nicht alle API-Keys verwendet worden sind, ist es nicht möglich gewesen das Tool in der völligen Funktionalität zu testen. Es werden die API-Keys dazu verwendet, um Zugriffe auf verschiedene Social Media Plattformen zu bekommen.

6.2.6. Ergebnisse und Fazit

Es werden diese Scans in zwei verschiedenen Formaten gespeichert, somit können diese Scans für einen weiteren Gebrauch verwendet werden. Es besteht ebenso die Möglichkeit eine Suche und Filterung durchzuführen.
Die Ergebnisse werden einer Person sehr übersichtlich wiedergegeben. Es wird ein “html” und ein “xls”-File erstellt, worin der durchgeführte Scan und dessen Ergebnisse gespeichert werden.

Anschließend werden die positiven sowie die negativen Auffälligkeiten des Tools angeführt.

Positiv aufgefallen ist:
- Automatische Erzeugung eines Scan-Bericht
- Übersichtlichkeit

Negativ aufgefallen ist:
- Kenntnisse von CLI sind gegeben (beispielsweise bei Updates des Tools)

6.3. Recon-ng

6.3.1. Beschreibung

Das Tool „Recon-ng“ wurde im Detail angeschaut. Dieses Tool ist standardmäßig auf der virtuellen Maschine „Kali Linux“ installiert, daher ist eine Installation des Tools nicht notwendig. Das Tool kann nur über die CLI bedient werden und es handelt sich um ein passives OSINT-Tool.
Dieses Tool wurde in der Programmiersprache „Python“ geschrieben und für Open Source Aufklärungen entwickelt. Das Tool generell ist kostenlos, hingegen können etliche kostenpflichtige, aber auch kostenlose API-Keys hinzugefügt werden. Es gibt verschiedene Dokumentationen und Lern-Videos über dieses Tool, welche bei der ersten Verwendung eine gute Einführung geben und als Nachschlagewerk genommen werden können. Das Tool wurde von „Tim Tomes“ entwickelt. [116]

6.3.2. Allgemein

Bei dem Tool „Recon-ng“ handelt es sich um ein „Reconnaissance“ Tool, welches in der Programmiersprache Python geschrieben wurde. Das Tool unterstützt einen User in der Information Gathering Phase, um die ersten “wichtigen” Informationen über ein Ziel zu sammeln.

Von dem Tool werden verschiedene Module angeboten um beispielsweise nach Attributen wie Hostname, IP-Adresse, Username und E-Mail-Adresse zu suchen. [117]
Es werden von dem Tool 76 Aufklärungsmodule, 8 Berichtsmodule, 2 Discovery, 2 Exploitation und 2 Import Module angeboten. Alle durchgeführten Scans werden in einer eigenen Datenbank gespeichert. Das Tool ist sehr flexibel, da es Interaktionen zwischen APIs und Web Scraping unterstützt. Mittels Web Scraping wird versucht, verschiedene Daten aus dem Internet zu erfassen.
Das Tool ist generell kostenlos zu verwenden, wenn hingegen detailliertere Scans durchgeführt werden möchten, ist es sehr von den 21 angebotenen API-Keys abhängig. [118]
Um die gesamte Funktionalität des Tools testen zu können ist es notwendig, diverse API-Keys hinzu zu fügen, welche teilweise mit Kosten verbunden sind.

6.3.3. Kriterien-Beschreibung

Das Kriterium „**Plattform**“ wurde zuerst überprüft, hier wurde festgestellt, dass das Tool nur auf „Linux“ und “Mac” verfügbar ist und es wird nicht auf Windows unterstützt.

Danach wurde das Kriterium "**GUI/CLI**" überprüft. Das Tool ist über die CLI zu bedienen, hier können die jeweiligen Scan-Abfragen durchgeführt werden. Es wird von dem Tool keine GUI zur Verfügung gestellt.

Ein wichtiges Kriterium, welches kontrolliert wurde, ist der "**Import**" von Dateien oder Listen. Es wird von dem Tool ermöglicht, dass verschiedene Wordlisten vor dem Scan importiert werden können. Die Wordlisten, die bei dem Scan hinzugefügt werden, enthalten eine Sammlung von Wörtern, um verschiedene Namen einer Domain zu prüfen. Somit kann ein Scan diese Wordliste, Zeile für Zeile durchgehen und mit verschiedenen Domains abgleichen.

Das nächste Kriterium, welches nachgeprüft wurde, ist der "**Export**". Das Tool ermöglicht den Anwendern einen Export der Scan-Ergebnisse durchzuführen. Es werden folgende Exportformate für den Scan zur Verfügung gestellt: "csv", "html", "xlsx" oder "xml". Weiters werden noch Formate wie "json", "list", "proxifier", "pushpin" als Exportformat angeboten.

Darauffolgend wurde das Kriterium "**Updates**" überprüft. Es ist auf "GitHub" ersichtlich, dass in regelmäßigen Abständen von circa drei Monaten Updates und Bug-Fixes der Programme durchgeführt werden.

Das Kriterium "**Such- und Filtermöglichkeiten**" wurde als nächstes überprüft. Das Tool ermöglicht einer Person, die gespeicherten Workspaces, welche separat für jeden Scan angelegt werden können, zu exportieren. Da von dem Tool wie beim Kriterium "Export-Formate" beschrieben, verschiedene Export-Formate zur Verfügung gestellt werden, wird es ermöglicht, dass diese exportierten Dateien mit weiteren Programmen durchsucht und gefiltert werden.

Als nächstes wurde das Kriterium "**Kosten**" überprüft. Das Tool selber ist kostenlos verwendbar.
Es werden jedoch von dem Tool verschiedene API-Keys unterstützt. Um die gesamte Vielfalt des Tools zu testen, müssten diverse API-Keys hinzugefügt werden, welche teilweise nicht kostenlos angeboten werden. Gegen geringe Gebühren werden online Tutorial-Videos angeboten, um sich ein besseres Verständnis über das Tool zu verschaffen.

Wichtig ist das Kriterium „**Informationen**", damit bekannt ist, welche Informationen mit dem Tool gesammelt werden können. Es können verschiedene "Informationen" gesammelt werden, wie beispielsweise:

- Telefonnummer
- E-Mail
- Standorte
- Webseiten
- Hosts
- IP-Adressen
- Personen/Unternehmen
- Username

Anschließend wurde das Kriterium "**Korrektheit der Daten**" geprüft. Es werden bei diesem Kriterium die gefundenen E-Mail-Adressen überprüft. Die Überprüfung erfolgt stichprobenmäßig, indem verschiedene E-Mail-Adressen online überprüft worden sind. Die Korrektheit der Informationen, welche mit dem Tool gefunden worden sind, waren sehr gut. Da der Scan direkt auf die Domain eingeschränkt werden hat können, waren keine Nacharbeitungen der Ergebnisse nötig.

Danach wurde das Kriterium "**Berichtsverwaltung**" analysiert. Das Tool bietet verschiedene Export-Funktionen an, somit ist es möglich, die gesammelten Informationen auf mehrere Arten und in verschiedenen Tools wieder zu verwenden und es ist eine weitere Analyse der Informationen möglich.

Das Kriterium "**Darstellungsfunktionen**" wurde ebenfalls geprüft. Von dem Tool werden verschiedene Export-Formate angeboten. Durch die verschiedenen Export Möglichkeiten können die Berichte beispielsweise als Tabelle oder als Textfile dargestellt werden. Es wird damit eine übersichtliche Wiedergabe der Scan-Ergebnisse geboten.

Darauffolgend wurde das Kriterium "**Rückverfolgbarkeit**" analysiert. Es ist durch die gefundenen Informationen möglich, erste Vorbereitungen sowie Recherchen über eine Person zu starten. Das Tool schafft es, dass es einen vollständigen Namen mit der E-Mail-Adresse in Verbindung bringt und wenn angegeben, den "Spitznamen" einer Person in einer separaten Spalte namens "middle_name" hinzufügt, welche in Abbildung 17 „*Recon-NG Show Contacts*" zu sehen ist. Weiters sind die gefundenen Hosts mit einer IP-Adresse hinterlegt. Es können mit diesen Informationen genauere Recherchen über ein eingesetztes System oder ein Unternehmen stattfinden.
Da bei dem Scan direkt die Domain der Fachhochschule verwendet worden ist, sind die Ergebnisse des Scans eingegrenzt worden. Daher konnte sichergesellt werden, dass die gefundenen Informationen zu diesem Ziel gehören.

Für welche „Attacken" können die gefundenen Informationen verwendet werden:
Es wurden nicht alle Informationen gefunden, welche in dem Kriterium "Informationen" gelistet sind, da in der Arbeit keine "kostenpflichtige" API-Keys verwendet worden sind, sondern nur vorhandene API-Keys. Es sind die API-Keys von "Shodan" und "Buildwith" verwendet worden.
Mittels der gefundenen Informationen wie der E-Mail-Adresse können Phishing Attacken durchgeführt werden. Dadurch besteht auch die Möglichkeit, Ransomware sowie Würmer und Viren zu verteilen. Durch die IP-Adresse ist es möglich auf das Ziel einen "DoS" Angriff oder einen "IP-Spoofing" Angriff durchzuführen. Durch die genaue Namen-Zusammenstellung können detaillierte Nachforschungen zu einer Person durchgeführt werden. Da die E-Mail-Adresse mit dem Namen und dem Spitznamen in Verbindung gebracht wird, ist es möglich ein "realistisches" Personenprofil zu erstellen. Diese Angriffsarten sind im Detail in Kapitel 4.8 „*Intelligence Collections und Angriffsarten*" beschrieben.

6.3.4. Praktischer Test

Es wird von dem Tool durch den "help" Befehl eine Übersicht der bereitgestellten Funktionen gegeben. Somit erhält ein User eine Bedienungshilfe mit den jeweiligen Funktionen, welche von dem Tool ermöglicht werden. Mit dem Befehl "use" können die verschiedenen Module angezeigt und verwendet werden.

Bevor mit dem Tool eine Suche durchgeführt wird, sollte ein eigener Workspace erstellt werden z.B.: "workspace add fhstp1". Generell sollte für jedes Ziel ein eigener Workspace erstellt werden, somit vermischen sich die verschiedenen Daten der Ziele nicht und es ist ein getrenntes Arbeiten möglich. In dem Workspace können verschiedene Scans durchgeführt werden. Es wird zuerst eine Domain des Ziels hinzugefügt z.B.: "add domains <DOMAIN>". Nachdem die Domain hinzugefügt worden ist, können weitere Scans zu dieser Domain durchgeführt werden. Das Tool wurde mit dem API-Key von "Shodan" und "Buildwith" erweitert.

Mit dem Befehl "use bing_domain_web" wurden anschließend alle gefundenen Domains automatisch in eine Tabelle des Tools eingefügt, hier waren es insgesamt 80 neue Hosts. Anschließend wurde noch "use google_site_web" verwendet, hier wurden weitere 13 Hosts gefunden.

Diese Host-Liste wurde anschließend erweitert, dazu wurde mit dem Befehl "use_brute_hosts" ein neuer Scan durchgeführt. Bei diesem Scan wird ein hinterlegtes Textfile verwendet. Dieses Textfile hat verschiedene Einträge, welche bei dem Scan überprüft werden. Standardmäßig wird folgende

Wordliste verwendet "/usr/share/recon-ng/data/hostnames.txt." welche in Abbildung 14 „*Recon-NG Brute Hosts Einstellungen*" zu sehen ist.

Nach dem durchgeführten Scan mittels dem Standard-Textfile waren insgesamt 127 neue Hosts, die eingetragen wurden. Es wurde anschließend das Standard-Textfile verändert und mit einem umfangreicheren Textfile ersetzt, um mehr Hosts ausfindig zu machen. [119]

Folgende Textfiles wurden für den Scan verwendet, der Pfad wurde mittels "set WORDLIST <Pfad>" gewechselt:

- /usr/share/wordlist/dirbuster/directory-list-2.3-medium.txt
- /usr/share/wordlists/dirb/small.txt
- /usr/share/wordlists/dirb/big.txt
- /usr/share/wordlists/dirb/catala.txt

```
[recon-ng][fhstp1] > use recon/domains-hosts/brute_hosts
[recon-ng][fhstp1][brute_hosts] > set
Sets module options

Usage: set <option> <value>

  Name      Current Value                      Required  Description
  --------  -------------                      --------  -----------
  SOURCE    default                            yes       source of input (see 'show info' for details)
  WORDLIST  /usr/share/wordlists/dirb/common.txt  yes       path to hostname wordlist
```

Abbildung 14 Recon-NG Brute Hosts Einstellungen

Nachdem verschiedene Textfiles eingebundenen wurden, welche mittels den Scans durchlaufen worden sind, wurden insgesamt 357 Hosts und 140 Kontakte gefunden, sowie 8 Profile, auf welchen die FH St. Pölten vertreten ist, welches in Abbildung 15 „*Recon-NG Results Summary*" zu sehen ist.

```
+-----------------------------+
|      Results Summary        |
+-----------------------------+
|     Category     | Quantity |
+-----------------------------+
| Domains          | 1        |
| Companies        | 0        |
| Netblocks        | 4        |
| Locations        | 0        |
| Vulnerabilities  | 0        |
| Ports            | 0        |
| Hosts            | 357      |
| Contacts         | 140      |
| Credentials      | 0        |
| Leaks            | 0        |
| Pushpins         | 0        |
| Profiles         | 8        |
| Repositories     | 0        |
+-----------------------------+
```

Abbildung 15 Recon-NG Results Summary

Beschreibung der verwendeten Befehle:

- *use recon/domains-hosts/brute_hosts* = Mittels Wordlisten/Textfiles werden verschiedene Domain-Records getestet. Es wird damit die Existenz von Hosts überprüft.
- *use recon/domains-hosts/bing_domain_web* oder *use recon/domains-hosts/google_site_web* = Mittels diesen Befehlen können Hosts in der Domäne gefunden werden.

Nachdem die Scans durchgeführt worden sind, müssen die Informationen ausgewertet werden. Die Daten, welche gefunden worden sind, werden in der Datenbank zu dem jeweiligen Workspace hinterlegt, somit besteht die Möglichkeit getrennt die Informationen zu analysieren und zu überprüfen. Wenn in einem Workspace ein neuer Scan durchgeführt wird, werden die gefundenen Daten automatisch hinzugefügt. Bei der Überprüfung der Ergebnisse konnte sich ein Überblick verschaffen werden, über die Systeme, welche in Verwendung sind. Hier könnte ein Angreifer nach möglichen Schwachstellen der Systeme suchen und diese für einen Angriff verwenden.

Der Nachteil ist leider, dass von dem Tool keine Versionsnummern der verwendeten Programme angezeigt wird, dennoch kann man sich einen Überblick verschaffen, welche Systeme in einem Unternehmen verwendet werden. Durch die Hostnamen ist beispielsweise ersichtlich, dass das Monitoring Tool “Nagios” [120] [121] [122] verwendet wird. Weiters wurde herausgefunden, dass die Distribution “Fedora” [123] in Verwendung ist. Es ist ebenso “Mahara” [124], “Wordpress” [125], “Skype” [126], “Jabber” [127] und “Jira” [128] in Verwendung. Da wie oben erwähnt, keine Versionsnummern angegeben sind, können nur mutmaßliche Gefahren und CVEs [61] (Common Vulnerabilities and Exposures) angeführt werden.

6.3.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests

Das Tool ermöglicht das Wechseln der Wordliste, womit verschiedene Listen durchsucht werden können auf mögliche Hostnamen. Wenn bei einem Scan neue Einträge gefunden werden, werden diese automatisch in die Tabelle des jeweiligen Workspace hinzugefügt.
Einige der API-Keys sind kostenpflichtig welche sich in verschiedenen Preiskategorien befinden, oder es werden persönliche Informationen wie eine Telefonnummer für einen API-Key verlangt. Ohne den jeweiligen API-Keys ist es nicht möglich die gesamte Funktionalität des Tools zu untersuchen. Dennoch wurde trotz dessen, dass nicht alle angebotenen API-Keys verwendet worden sind, eine Vielzahl von Informationen über das Ziel gefunden.

6.3.6. Ergebnisse und Fazit

Das Tool bietet einer Person verschiedene Funktionalitäten der Scans. Die jeweiligen Scanvorgänge, die durchgeführt werden, können in einem eigenen Workspace durchgeführt werden. Somit können die Scanergebnisse nicht vermischt werden, welches in Abbildung 16 „*Recon-NG Show Workspaces*“ ersichtlich ist.

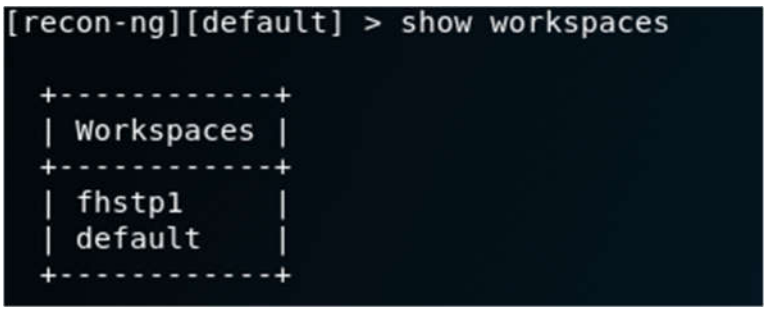


Abbildung 16 Recon-NG Show Workspaces

Optisch werden diese Suchergebnisse in einer übersichtlichen Liste dargestellt, in der die gefundenen Informationen des Scans zu sehen sind, siehe Abbildung 17 „*Recon-NG Show Contacts*“. Wenn bei einer Suche neue Einträge gefunden werden, werden diese automatisch in die jeweilige Liste eingetragen und können anschließend direkt geprüft werden.

```
[recon-ng][fhstp1] > show contacts

+-------+------------+-------------+-----------+-------+-----------------------+--------+---------+-------------+
| rowid | first_name | middle_name | last_name |       email           |       title           | region | country |   module    |
+-------+------------+-------------+-----------+-------+-----------------------+--------+---------+-------------+
| 1     | Re         |             |           | is    | PGP key association   |        |         | pgp_search  |
| 2     | Fl         |             | Hal       | fl    | PGP key association   |        |         | pgp_search  |
| 3     | Da         |             | Has       | da    | PGP key association   |        |         | pgp_search  |
| 4     | Le         |             | Hoc       | it    | PGP key association   |        |         | pgp_search  |
| 5     | Be         | R           | Fis       | be    | PGP key association   |        |         | pgp_search  |
| 6     | Re         |             | Fri       | is    | PGP key association   |        |         | pgp_search  |
| 7     | Fi         |             | Tho       | it    | PGP key association   |        |         | pgp_search  |
| 8     | Gi         |             | Rab       | is    | PGP key association   |        |         | pgp_search  |
```

Abbildung 17 Recon-NG Show Contacts

Es werden die gefundenen Hosts in einer übersichtlichen Form dargestellt und ebenso die dazu gefundenen IP-Adressen des jeweiligen Hosts vermerkt, welches in Abbildung 18 „*Recon-NG Hosts/IP-Adressen Auszug*“ zu sehen ist. Für eine bessere Ansicht des Ergebnisses wurde das Ergebnis in einem Texteditor wiedergegeben.

```
+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------------+
| rowid |              host             |   ip_address    | region | country | latitude | longitude |    module   |
+-------+-------------------------------+-----------------+--------+---------+----------+-----------+-------------+
| 81    | autodiscover.fhstp.ac.at      | 91.219.69.27    |        |         |          |           | brute_hosts |
| 82    | av.fhstp.ac.at                | 91.219.69.10    |        |         |          |           | brute_hosts |
| 83    | wwwneu2.fhstp.ac.at           |                 |        |         |          |           | brute_hosts |
| 84    | cdn.fhstp.ac.at               |                 |        |         |          |           | brute_hosts |
| 85    | cdn.fhstp.ac.at               | 91.219.69.47    |        |         |          |           | brute_hosts |
| 86    | community.fhstp.ac.at         | 195.202.144.40  |        |         |          |           | brute_hosts |
| 87    | conference.fhstp.ac.at        | 91.219.68.97    |        |         |          |           | brute_hosts |
```

Abbildung 18 Recon-NG Hosts/IP-Adressen Auszug

Es wird von dem Tool eine Vielfalt von Scan-Optionen bereitgestellt, welche Informationen über das Ziel finden können, insgesamt werden 77 verschiedene Scan Optionen zur Verfügung gestellt. Ebenso ist hier der erstellbare Workspace von großer Bedeutung, so kann man sich für jeden durchgeführten Scan eines Ziels einen Workspace erstellen.

Das Tool bietet eine gute Übersicht über die durchgeführten Scans und zeigt diese nummerisch in “Runs” in einer Tabelle mit dem Befehl “show dashbord” an, siehe Abbildung 19 „*Recon-NG Activity Summary*“.

```
+-------------------------------------------------------+
|                   Activity Summary                    |
+-------------------------------------------------------+
|                    Module                     | Runs  |
+-------------------------------------------------------+
| recon/companies-contacts/bing_linkedin_cache  | 2     |
| recon/companies-contacts/jigsaw/point_usage   | 1     |
| recon/companies-contacts/jigsaw/purchase_contact | 1  |
| recon/companies-contacts/jigsaw/search_contacts | 3   |
| recon/companies-multi/whois_miner             | 1     |
| recon/contacts-credentials/hibp_breach        | 1     |
| recon/contacts-profiles/fullcontact           | 1     |
| recon/domains-contacts/pgp_search             | 4     |
| recon/domains-contacts/whois_pocs             | 4     |
| recon/domains-hosts/bing_domain_web           | 2     |
| recon/domains-hosts/brute_hosts               | 9     |
| recon/domains-hosts/certificate_transparency  | 1     |
| recon/domains-hosts/google_site_web           | 2     |
| recon/domains-hosts/mx_spf_ip                 | 1     |
| recon/domains-hosts/ssl_san                   | 1     |
| recon/netblocks-companies/whois_orgs          | 1     |
| recon/netblocks-hosts/reverse_resolve         | 1     |
| recon/ports-hosts/migrate_ports               | 2     |
| recon/profiles-profiles/namechk               | 2     |
| recon/profiles-profiles/profiler              | 2     |
| recon/profiles-profiles/twitter_mentioned     | 1     |
| recon/profiles-profiles/twitter_mentions      | 1     |
| reporting/csv                                 | 2     |
| reporting/html                                | 1     |
| reporting/json                                | 1     |
| reporting/list                                | 1     |
| reporting/proxifier                           | 1     |
| reporting/pushpin                             | 1     |
| reporting/xlsx                                | 1     |
| reporting/xml                                 | 1     |
+-------------------------------------------------------+
```

Abbildung 19 Recon-NG Activity Summary

Es können mit dem Tool Informationen in kurzer Zeit über ein Ziel gefunden, gesammelt und gespeichert werden. Diese Informationen von beispielsweise verwendeten Systemen, kann ein Angreifer benutzen, um mögliche Schwachstellen für diese Systeme zu suchen.
Das Tool kann gefundene Namen und deren E-Mail-Adresse in einer Tabelle zusammenfassen und für eine weitere Analyse bereitstellen. Durch den Namen, den Spitznamen und der E-Mail-Adresse können Personen-Profile erstellt werden. Mit dem Spitznamen kann ein Fake User vertrauensvoller wirken.

Ein Nachteil des Tools ist, dass einige Scans nicht durchgeführt werden können, da das Tool sehr auf die API-Keys ausgelegt ist. Von dem Tool werden 21 verschiedene API-Keys unterstützt, davon wurden lediglich zwei API-Keys verwendet, da die restlichen meist mit Angaben von persönlichen Daten wie beispielsweise Telefonnummer oder Kosten verbunden sind. Es wurden für die Scans die API-Keys von “Shodan” und “Buildwith” verwendet.

Anschließend werden die positiven sowie die negativen Auffälligkeiten des Tools angeführt.

Positiv aufgefallen ist:

- Umfangreiches Angebot an Funktionen und Modulen
- Eigener Workspace für durchgeführtes Suchen
- Export Formate
    - reporting/csv
    - reporting/html
    - Reporting/json
    - Reporting/list
    - Reporting/proxifier
    - Reporting/pushpin
    - Reporting/xlsx
    - Reporting/xml

Negativ aufgefallen ist:

- Genauere Beschreibung der jeweiligen Funktionen
- Abhängigkeit von API-Keys [129]
- Funktionen nur “teilweise” verwendbar, da kostenpflichtige API-Keys benötigt werden

6.4. Spiderfoot

6.4.1. Beschreibung

Ein weiteres Tool, welches im Detail analysiert wurde, ist das Tool „Spiderfoot 3.0“. Das Tool wurde auf der virtuellen Maschine „Buscador2“ verwendet. Dieses Tool ist standardmäßig auf dieser virtuellen Maschine installiert, daher musste es nicht separat installiert werden. Das Tool wurde von Steve Micallef entwickelt. Mit dem Tool ist es möglich verschiedene Informationen wie beispielsweise “Webanwendungen”, “Netzwerke”, “DNS”, “E-Mail-Adressen" oder Informationen zu “Personen” zu sammeln. Das Tool ermöglicht noch weitere Informationen zu sammeln, welches in dem Kapitel 6.4.4 „*Praktischer Test*“ zu sehen ist. Um diese Informationen zu sammeln, werden mehr als 100 öffentliche Datenquellen verwendet. [130]
Es gibt verschiedene Versionen des Tools wie “Open Source”, „Hobby”, „Basic“, „Standard“, „Professional“ und „Enterprise“. In dieser Arbeit wurde für die Tests die Open Source Version gewählt.

6.4.2. Allgemein

Bei dem Tool “Spiderfoot” [131] handelt es sich um ein Reconnaissance Tool, das heißt es können aktive und passive Scans durchgeführt werden. Bei dem aktiven Information Gathering wird direkt mit dem Ziel kommuniziert, um über dieses Ziel Daten und Informationen zu sammeln. Aktives Information Gathering, wie beispielsweise Port-Scans, kann in vielen Ländern illegal sein [QUELLE], daher wird in dieser Arbeit kein aktiver Scan durchgeführt, sondern ein ”passiver” Scan.
Bei einem passiven Information Gathering Scan werden verschiedene Informationen über ein Ziel gesammelt, ohne mit dem Ziel direkt zu kommunizieren, dies können beispielsweise Informationen von Social Media Plattformen sein. [132]

Die Startseite des Tools ist strukturiert und übersichtlich gehalten welches in Abbildung 20 „*Spiderfoot Scans Übersicht*“ ersichtlich ist. Es gibt insgesamt 3 Reiter, welche zum Auswählen sind „New Scan“ hier kann ein neuer Scan durchgeführt werden. Der Reiter “Scan” enthält die durchgeführten Scans und bei dem Reiter “Einstellungen”, können verschiedene Scan-Einstellungen sowie API-Keys hinzugefügt werden, um auf bestimmten Seiten eine genauere Suche durchzuführen.

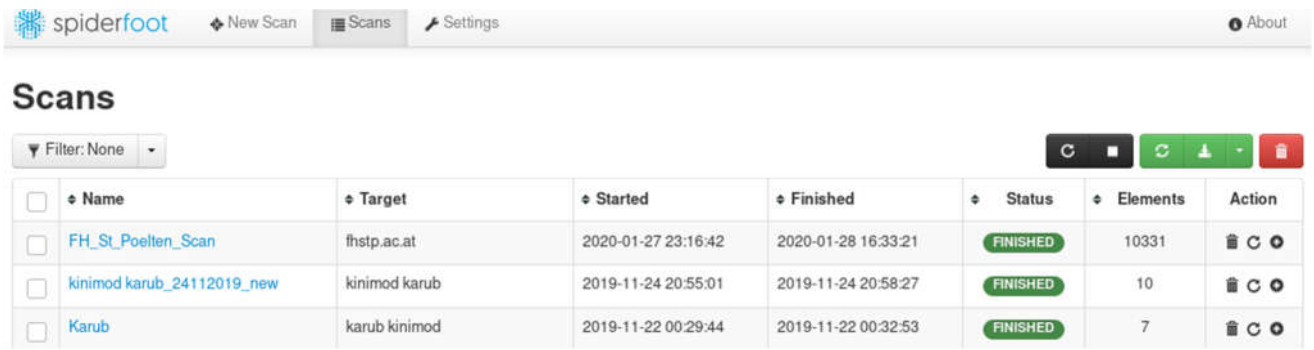


Abbildung 20 Spiderfoot Scans Übersicht

Es werden von dem Tool verschiedene Suchmöglichkeiten wie “All”, “Footprint”, “Investigate”, “Passive” angeboten. Abbildung 21 „*Spiderfoot New Scans*“ zeigt die verschiedenen Scan Methoden, welche anschließend erklärt werden.

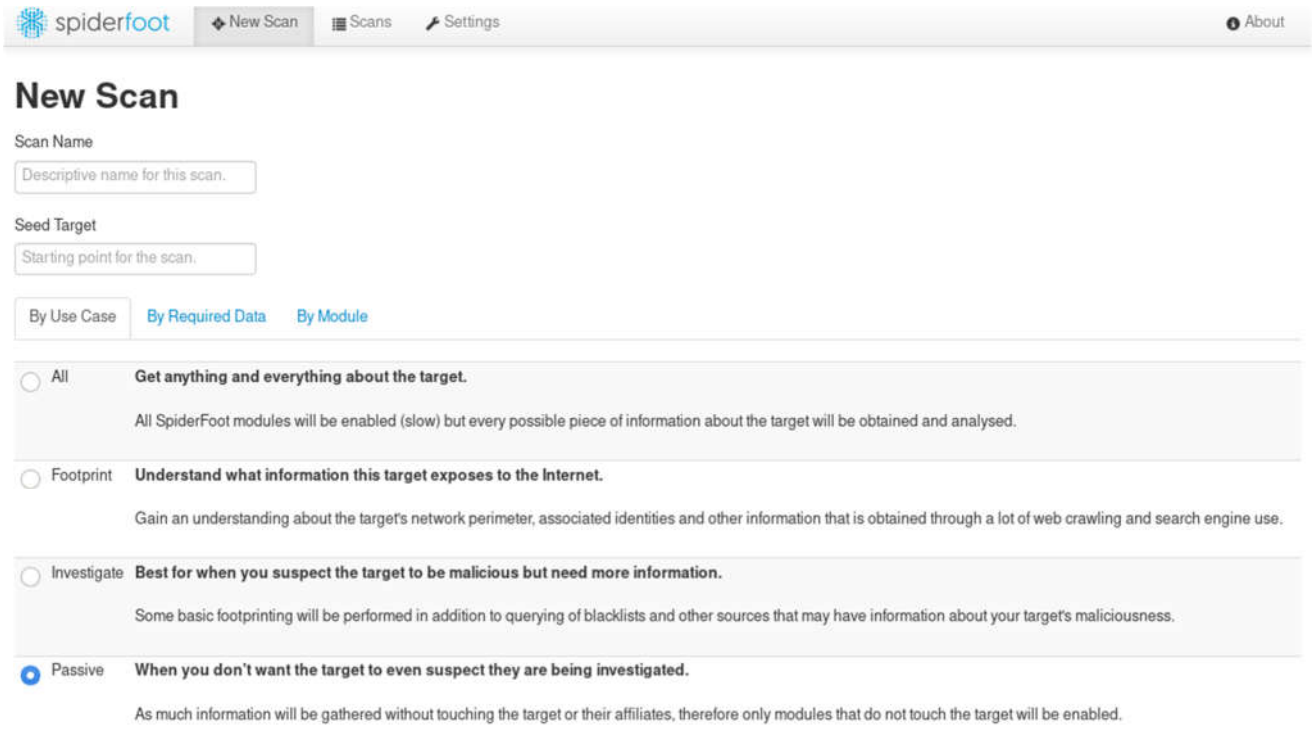


Abbildung 21 Spiderfoot New Scans

Bei “All” werden aktive und passive Scans durchgeführt, daher wurde diese Methode nicht für die Arbeit verwendet. Für diese Arbeit wurde nur der Scan “Passiv” verwendet.
“Footprint” dient dazu, um zu sehen welche, Informationen von einer Person beispielsweise im Internet auf Social Media Plattformen freigegeben worden sind.
“Investigate” wird verwendet, wenn der Verdacht besteht, dass ein Ziel nicht vertrauenswürdig ist und mehr Informationen benötigt werden.
”Passive” dient dazu, dass Daten und Informationen gesammelt werden ohne dass das Ziel etwas davon mitbekommt, welches auf eine mögliche Vorbereitung oder einen späteren Angriff deuten lässt.

Es können Scans auch anhand von benötigten Daten, was in Abbildung 22 „*Spiderfoot New Scan By Required Data*“ zu sehen ist, oder nur mit bestimmten Modulen, was in Abbildung 23 „*Spiderfoot New Scan By Module*“ zu sehen ist, durchgeführt werden, dazu wird auf der Plattform “By Required Data” oder “By Module” ausgewählt. Es wurden pro Abbildung nur kleine Ausschnitte der möglichen Auswahlen gezeigt.

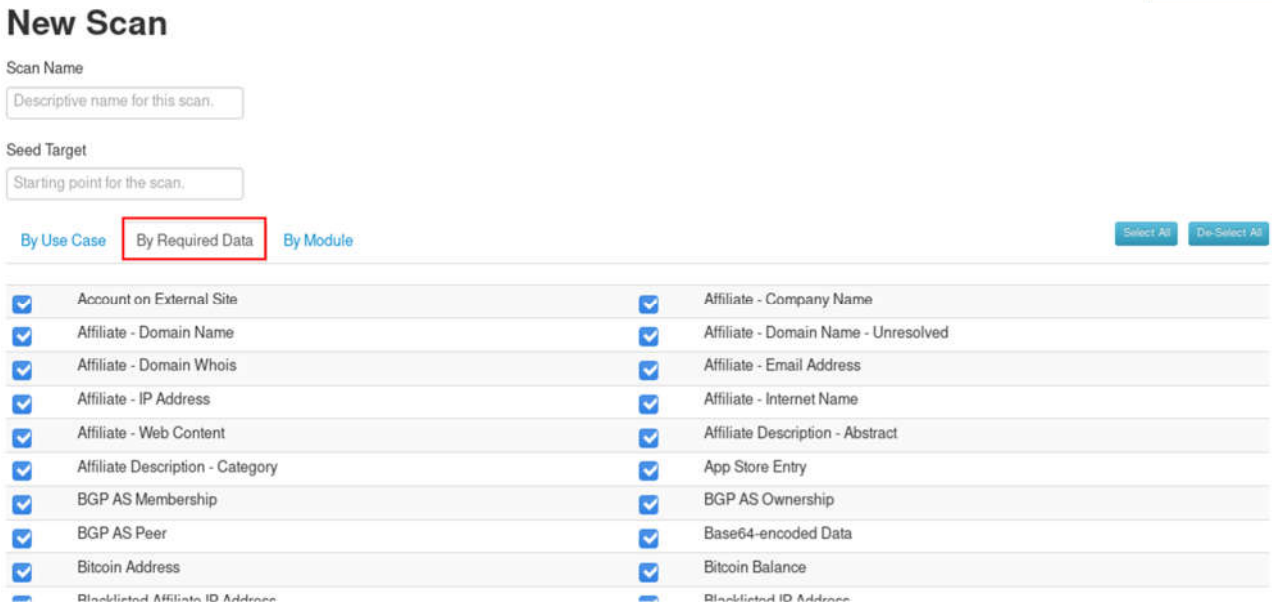


Abbildung 22 Spiderfoot New Scan By Required Data

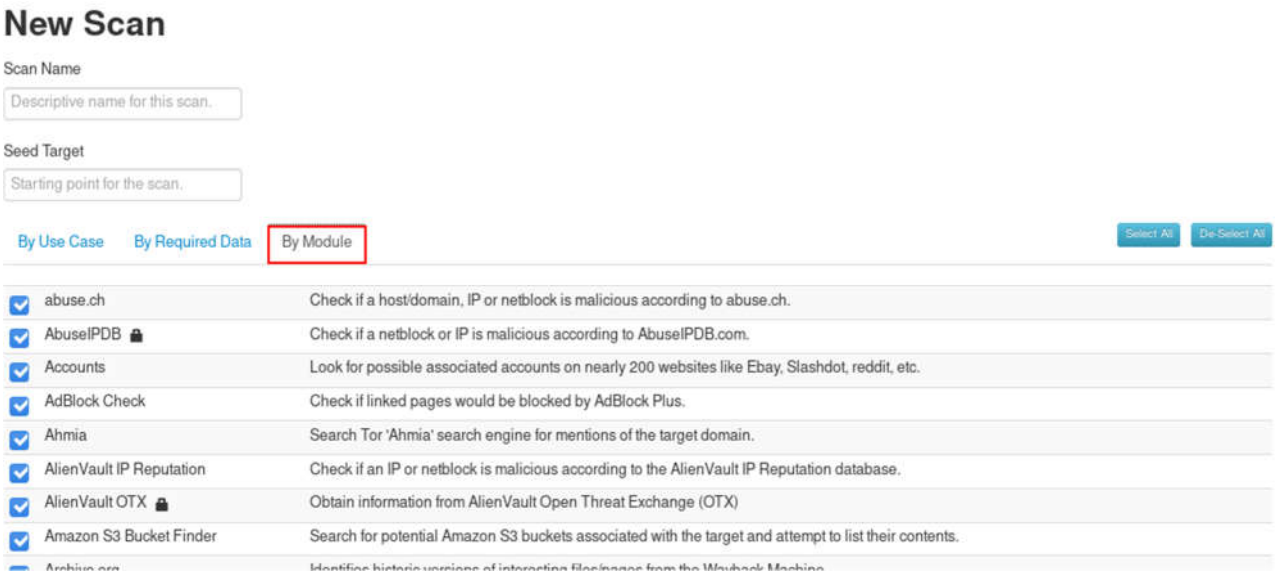


Abbildung 23 Spiderfoot New Scan By Module

Weiters ist eine Dokumentation von „Spiderfoot“ zur Verfügung gestellt worden. In dieser sind Abläufe zur Installation und dem Einfügen von API-Keys zu finden, weiters gibt es eine grundlegende Beschreibung zu dem Tool, um einen besseren Einstieg in das Tool zu finden. Dadurch werden auch für Personen, welche noch keine oder wenig Erfahrung mit dem Tool haben, eine Bedienbarkeit geschaffen.

Das Ergebnis eines Scans kann anschließend als Graph dargestellt werden, welches in Abbildung 24 „*Spiderfoot Graph*“ zu sehen ist. Somit können verschiedene Zusammenhänge der gefundenen Informationen ausfindig gemacht werden. Der Rote-Punkt in der Mitte stellt den Startpunkt “fhstp.ac.at” des Scans dar.

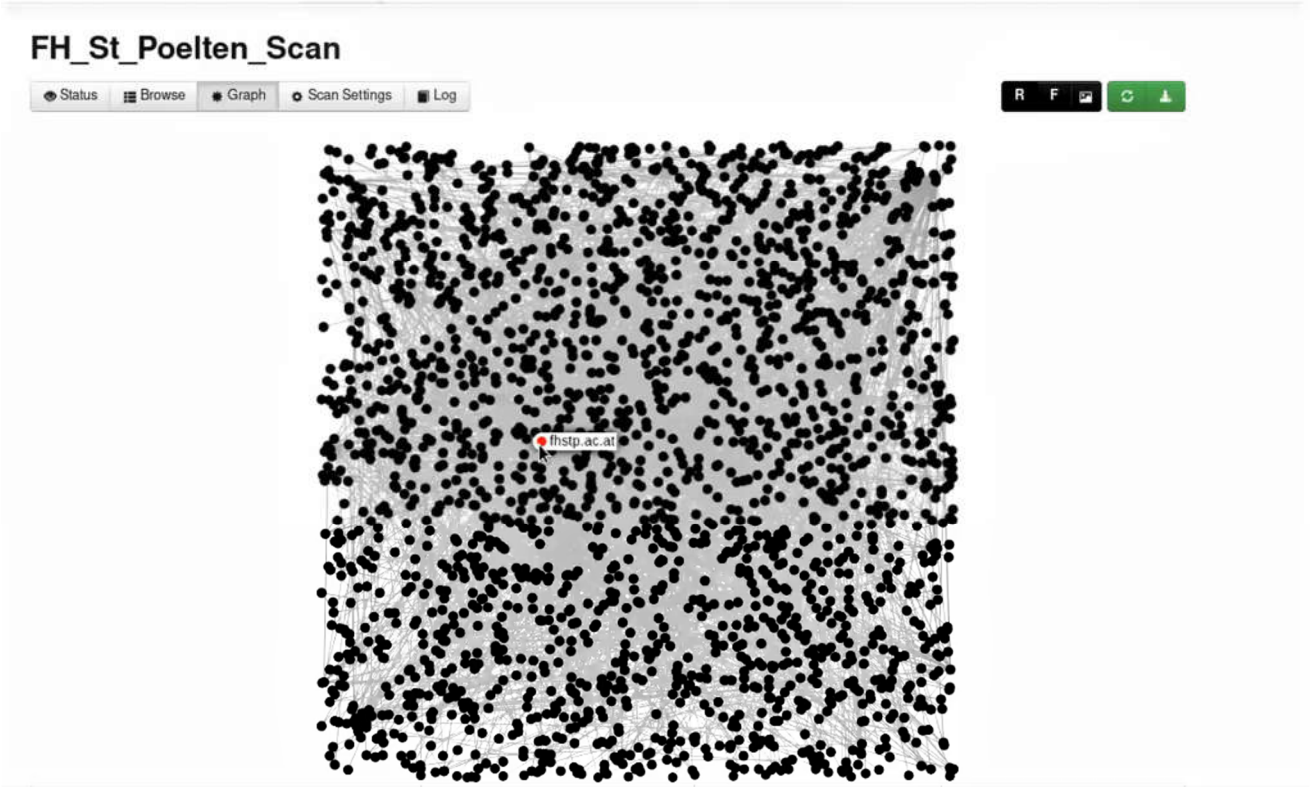


Abbildung 24 Spiderfoot Graph

6.4.3. Kriterien-Beschreibung

Das erste Kriterium, welches überprüft wird, ist die „**Plattform**“. Das Tool „Spiderfoot“ ist auf den Betriebssystemen „Windows“, „Linux“ und “iOS/Mac” verwendbar. Somit werden alle gängigen Plattformen von dem Tool unterstützt.

Als nächstes wurde das Kriterium „**GUI/CLI**“ geprüft. Zuerst muss das Tool über die CLI gestartet werden, danach ist es möglich das Tool mit der IP-Adresse über den Browser zu starten und mit der GUI des Webbrowsers zu bedienen. [133]

Darauffolgend wurde das Kriterium „**Import**“ überprüft. Das Tool bietet keine Möglichkeit bereits exportierte Daten, Informationen oder Listen von einem Scan zu importieren. Es wird ermöglicht API-Keys zu importieren, welche dafür verwendet werden können, um bestimmte Seiten zu durchsuchen. Für den Import eines API-Keys muss in der Weboberfläche unter dem Reiter “Settings” der jeweilige API-Key eingetragen werden.

Anschließend wurde das Kriterium „**Export**“ analysiert. Das Tool ermöglicht einer Person auf der Weboberfläche die verschiedenen Scans als “CVE”, “GEXF” oder “JSON” zu exportieren.

Das Kriterium „**Updates**“ ist „vollkommen erfüllt“, da auf GitHub [134] ersichtlich ist, dass monatlich Änderungen oder Verbesserungen sowie Bugfixes für das Programm durchgeführt werden (Stand 01.03.2020). Durch die ständigen Updates sowie Erweiterungen ist ersichtlich, dass dieses Kriterium sehr hoch angesetzt ist bei diesem Tool. [135]

Anschließend wurde das Kriterium "**Such- und Filtermöglichkeiten**" analysiert. Es wird von dem Tool angeboten, direkt auf der Weboberfläche nach durchgeführten Scans zu suchen. Dazu gibt es ein eigenes "Suchfeld", in welchem die Suchbefehle eingegeben werden können.
Bei den jeweiligen Scan Einträgen wird ein Link hinterlegt, welcher in Abbildung 26 „*Spiderfoot Kinimod Karub Account on External Site*" zu sehen ist. Dieser Link kann von einem User per Mausklick ausgeführt werden, somit kann per Mausklick beispielsweise das Social Media Profil des Ziels geöffnet werden. Eine Filterung ist leider nur nach dem Status eines Scans möglich. Hier kann nach "Running", "Finished" oder "Failed/Aborted" gefiltert werden.

Das Kriterium "**Kosten**" [136] wurde anschließend im Detail überprüft. Es ist möglich mit der kostenlosen Version "SpiderFoot 3.0", welche standardmäßig auf Buscador2 installiert ist, Scans durchzuführen und die Informationen von dem durchgeführten Scan zu speichern. Es sind keine Limitierungen ersichtlich, da ebenso eine weitere Verarbeitung und das Verschicken der Scans möglich ist. Es sind keine Kurse oder Schulungen zu diesem Tool verfügbar, dennoch gibt es verschiedene Dokumente und Videos, welche unterschiedliche Thematiken des Tools erklären und gratis zur Verfügung stehen. Die Tabelle 9 „Spiderfoot Kosten" zeigt die verschiedenen Versionen des Tools und die damit verbundenen Kosten.

	Open Source	**Hobby**	**Basis**	**Standard**	**Professional**	**Enterprise**
Kosten	gratis	gratis	19€	59€	179€	599€
Scans pro Monat	Unlimitiert	3	5	10	50	200
Benutzer-Accounts	N/A	1	1	2	5	Keine Limitierung
Scan-Dauer-Limits	Unlimitiert	15 Min	4 Std	24 Std	72 Std	120 Std

Tabelle 9 Spiderfoot Kosten

Das Kriterium „**Informationen**" wurde als nächstes analysiert. Folgende Informationen können mittels Spiderfoot gesammelt werden:

- Domain Name
- IP-Adressen
- Hostname/Sub-domain
- Subnetz
- ASN (Autonomous System Number)
- E-Mail-Adressen
- Telefonnummer
- Namen von Personen

Anschließend wurde das Kriterium "**Korrektheit der Daten**" geprüft. Nach dem Scan mit dem Tool sind etliche "falsche" Einträge vorhanden. Die falschen Einträge können direkt in dem Tool aussortiert werden, damit ein "saubereres" Ergebnis zustanden kommt. Durch das direkte Aussortieren in dem Tool, können die Scans bereinigt exportiert werden. Im Gegensatz zu den anderen analysierten Tools sind hier etliche falsche Ergebnisse vorhanden. Es wurden beispielsweise gefundene E-Mail-Adressen mit der Fachhochschule verglichen, hier waren einige nicht vorhanden.

Im Anschluss daran wurde das Kriterium "**Berichtsverwaltung**" analysiert. Das Tool ermöglicht eine Exportierung von drei verschiedenen Formaten. So können Personen ihre gewünschten Formate ("CVE", "GEXF", "JSON") für die weiteren Analysen verwenden.

Darauffolgend wurde das Kriterium “**Darstellungsfunktionen**” kontrolliert. Es werden von dem Tool verschiedene Export Formate angeboten, daher wird einer Person ermöglicht den Scan in unterschiedlichen Darstellungsformen wie beispielsweise Tabellen, Grafiken oder Textfiles zu generieren.

Anschließend wurde das Kriterium “**Rückverfolgbarkeit**” geprüft. Es sind durch den durchgeführten Scan viele verschiedene Ergebnisse gefunden worden. Wie bereits erwähnt waren etliche “falsche” Ergebnisse bei dem Scan enthalten. Dennoch ist es mit den gefundenen Ergebnissen möglich, im Detail Recherchen über ein Unternehmen oder eine Person durchzuführen.

Für welche „Attacken“ können die gefundenen Informationen verwendet werden:
Durch die gefundenen Informationen wird es einer Person ermöglicht, verschiedene Angriffe durchzuführen. Mittels dem Domain-Namen können Domain-Hijacking oder DNS-Flood Angriffe durchgeführt werden. Mit der IP-Adresse können “DoS” oder “IP-Spoofing” Angriffe stattfinden. Weiters können mit den Hostnamen und den Sub-Domains Angriffe wie “DNS-Tunneling” und “Man-in-the-Middle" durchgeführt werden. Durch die E-Mail-Adresse sowie der Telefonnummer und dem Namen einer Person können Cyber Stalking Attacken durchgeführt werden. Weiters werden mögliche Schwachstellen von einem Unternehmen mit dem Tool aufgezeigt wie beispielsweise “gehackte E-Mail-Adressen" oder “offene Ports”. Diese Angriffsarten sind im Detail in Kapitel „*Intelligence Collections und Angriffsarten*“ beschrieben.

6.4.4. Praktischer Test

Es wurde “SpiderFoot 3.0” für die Tests in dieser Arbeit verwendet. Die erste Inbetriebnahme für den Start erfolgt über die CLI, anschließend kann es über die Weboberfläche im Browser bedient werden, indem in Browser die IP-Adresse und der Port 5001 eingegeben wird. (Befehl: “python3 sf.py -l 127.0.0.1:5001”)

Beim ersten Scan der durchgeführt worden ist, war der User Name auf Twitter noch @KKarub und nicht @kinimodkarub. Der Username bei Reddit und Instagram war hingegen “kinimod karub”, daher wurden diese beim ersten Scan gefunden, siehe Abbildung 26 „*Spiderfoot Kinimod Karub Account on External Site*“. Abbildung 27 „*Kinimod Karub Instagram Account*“ und Abbildung 28 „*Kinimod Karub Reddit Account*“ zeigen die beiden Profile von Reddit und Instagram. Da der Twitter User Name nicht übereingestimmt hat, wurde dieser anfangs nicht gefunden. Daher wurde vor dem zweiten Scan der Twitter User Name in den Einstellungen der Social Media Plattform Twitter von “KKarub” auf “kinimod karub” geändert. Somit wurde der Twitter Account auch gefunden, siehe Abbildung 29 „*Spiderfoot Kinimod Karub Scan Ergebnis*“ sowie Abbildung 30 „*Spiderfoot Twitter Kinimod Karub*“.

Abbildung 25 Spiderfoot fertiger Scan Karub Kinimod

Browse > Account on External Site

	Data Element	Source Data Element	Source Module	Identified
☐	Instagram (Category: social) https://www.instagram.com/kinimodkarub/	Kinimod Karub	sfp_accounts	2019-11-19 23:41:33
☐	Minecraft (Category: gaming) https://namemc.com/name/kinimod.karub	Kinimod Karub	sfp_accounts	2019-11-19 23:42:13
☐	reddit (Category: news) https://www.reddit.com/user/kinimodkarub	Kinimod Karub	sfp_accounts	2019-11-19 23:41:33

Abbildung 26 Spiderfoot Kinimod Karub Account on External Site

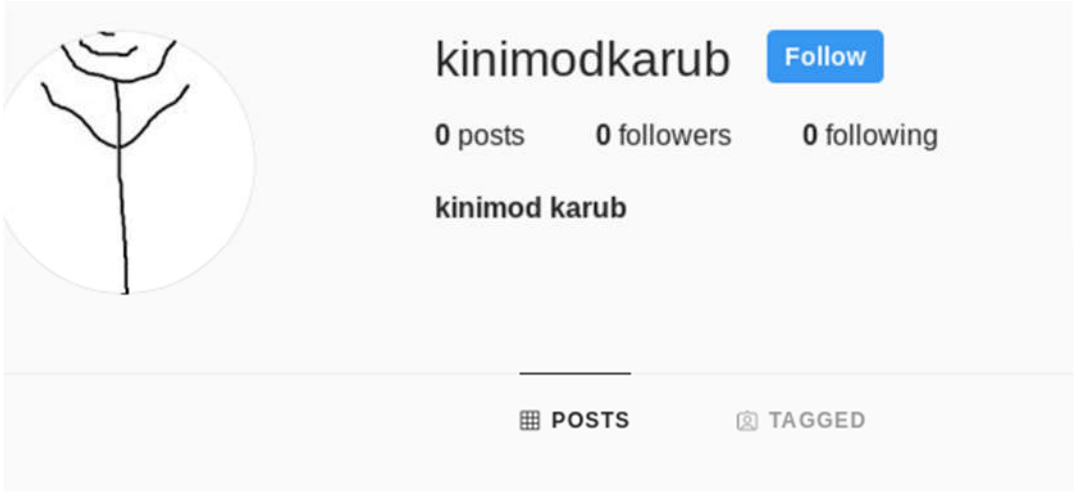


Abbildung 27 Kinimod Karub Instagram Account

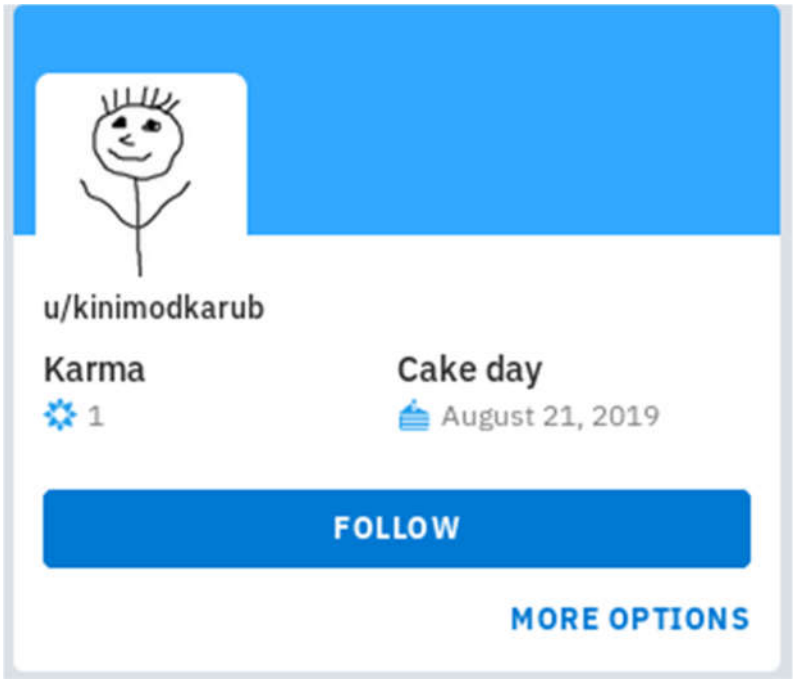


Abbildung 28 Kinimod Karub Reddit Account

Data Element	Source Data Element	Source Module	Identified
Instagram (Category: social) https://www.instagram.com/kinimodkarub/	kinimod karub	sfp_accounts	2019-11-20 00:18:48
Minecraft (Category: gaming) https://namemc.com/name/kinimod.karub	kinimod karub	sfp_accounts	2019-11-20 00:19:26
Twitter (Category: social) https://twitter.com/kinimodkarub	kinimod karub	sfp_accounts	2019-11-20 00:18:48
reddit (Category: news) https://www.reddit.com/user/kinimodkarub	kinimod karub	sfp_accounts	2019-11-20 00:18:48

Abbildung 29 Spiderfoot Kinimod Karub Scan Ergebnis

Abbildung 30 Spiderfoot Twitter Kinimod Karub

Dieses Tool eignet sich gut, um die Fachhochschule St. Pölten auf deren öffentliche Informationen zu durchsuchen. Es wurde daher ein passiver Scan durchgeführt, welcher eine Scandauer von ca. 17 Stunden hatte.
Bei diesem Scan wurden verschiedene Informationen gefunden, jedoch beinhaltet das Scan-Ergebnis einige “falsche” Informationen, welche aussortiert werden müssen. In Abbildung 35 „*Spiderfoot False Positive Flag*“ ist zu sehen, wie falsche Informationen entfernt werden können. Um sicher zu stellen, dass es sich um falsche oder richtige Informationen handelt, wurden die Scanergebnisse stichprobenmäßig mit Suchmaschinen und der Webseite der FH St. Pölten verglichen. Wenn keine Bezugspersonen gefunden wurden, war die Annahme, dass es sich um falsche Informationen handelt, welche aussortiert wurden. Es wurden beispielsweise gefundene E-Mail-Adressen mit der Fachhochschule verglichen, hier war ersichtlich, dass etliche E-Mail-Adressen nicht übereingestimmt haben. Die Abbildung 31 „*Spiderfoot Gesamtscan-Übersicht*“ zeigt den durchgeführten Scan der Fachhochschule St. Pölten.

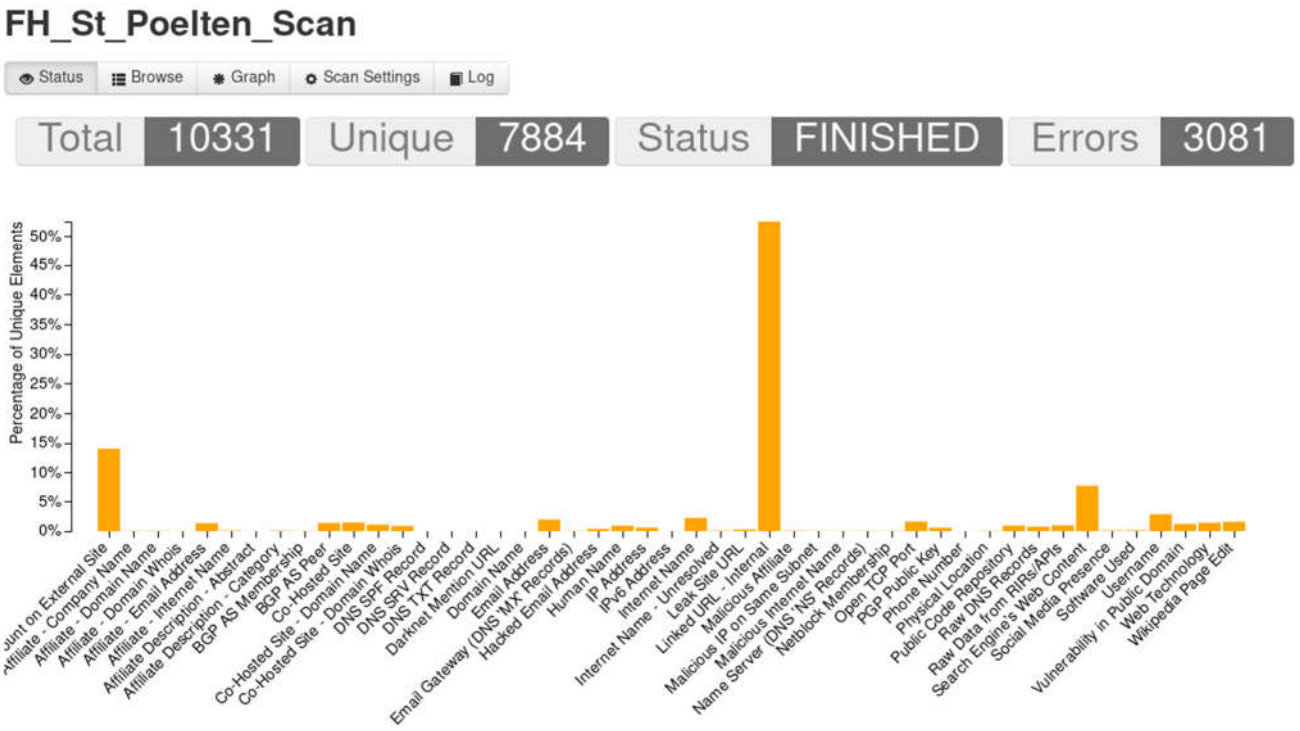


Abbildung 31 Spiderfoot Gesamtscan-Übersicht

6.4.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests

Eine Herausforderung stellten die verschiedenen API-Keys dar, da von dem Tool viele API-Keys unterstützt werden. [137]
Einige dieser API-Keys sind kostenpflichtig, daher konnte das Tool nicht in der vollständigen Vielfalt überprüft werden.

6.4.6. Ergebnisse und Fazit

Es wurden mit dem Tool verschiedene Tests und Scans durchgeführt.
Zuerst wurden Scans zu dem Fake-User der Social Media Profile durchgeführt. Hier wurde bemerkt, dass das Tool den exakten Usernamen “kinimod karub” benötigt, da ansonsten das Ergebnis erfolglos ist und den User nicht finden kann.
Wie in Abbildung 32 „*Spiderfoot Scans Kinimod Karub vs. Karub Kinimod*“ zu sehen ist, wurde der Scan zwei Mal durchgeführt. In der Spalte “Target” ist ersichtlich nach welchem Namen gesucht worden ist.
Beim ersten Scan von Abbildung 33 „*Spiderfoot Scan Karub Kinimod*“ wurde der Name nicht gemäß dem Twitter-Usernamen geschrieben, da der Vorname und Nachname vertauscht waren. Hier war das Ergebnis des Scans erfolglos, da es nur "falsche” Scan-Ergebnisse waren.
Bei dem zweiten Scan sind Vorname und Nachname umgedreht worden, so wie er auch auf Twitter, Instagram und Reddit angegeben war. Bei diesem Scan Ergebnis von Abbildung 34 „*Spiderfoot Scan Kinimod Karub*“ hingegen, war nur ein “falscher” Eintrag vorhanden, welcher “Minecraft” war. Daher ist es wichtig, dass die richtige Schreibweise der Person bekannt ist.

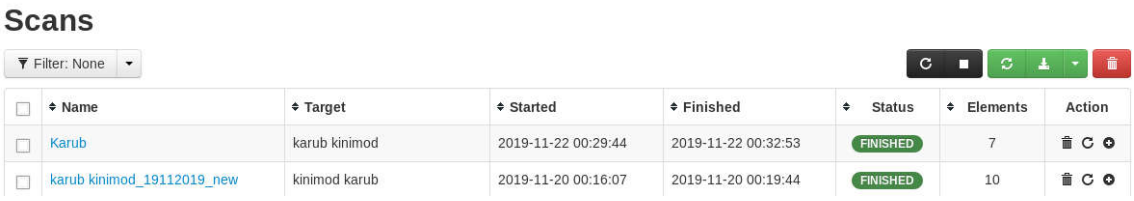


Abbildung 32 Spiderfoot Scans Kinimod Karub vs. Karub Kinimod

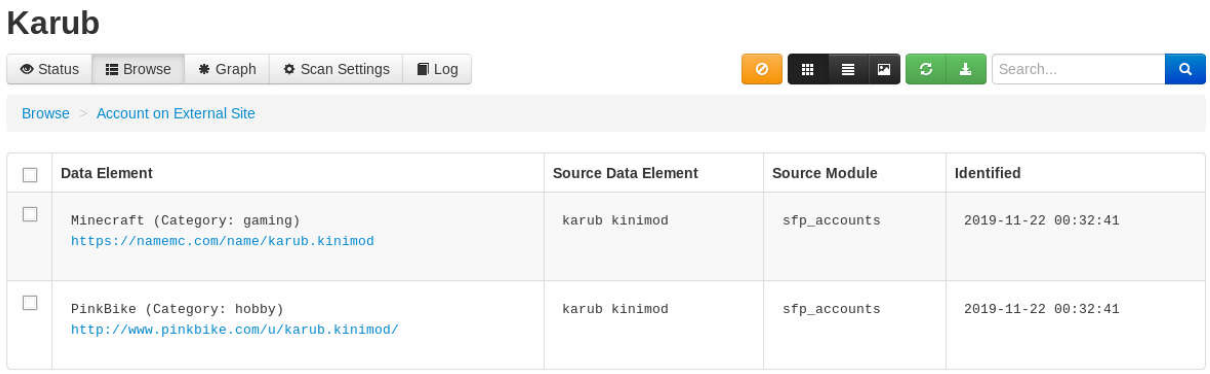


Abbildung 33 Spiderfoot Scan Karub Kinimod

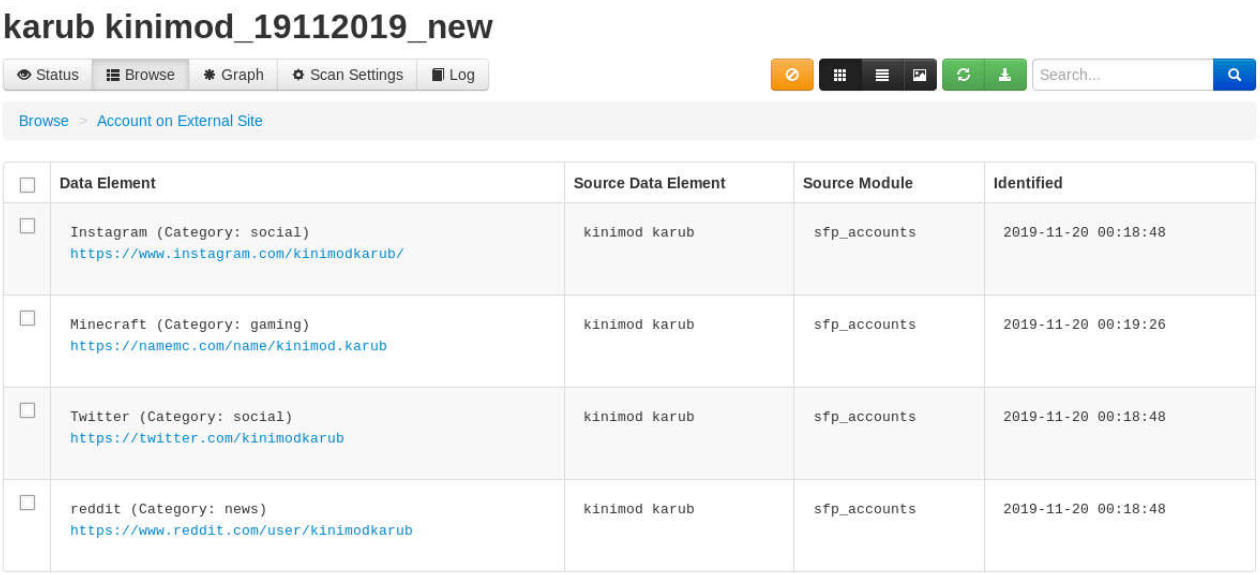


Abbildung 34 Spiderfoot Scan Kinimod Karub

Nachdem der Scan des Fake-Users durchgeführt worden ist, wurde ein Scan der FH St. Pölten durchgeführt. Es konnte leider nicht die vollständige Funktionalität der verschiedenen Module des Tools getestet werden, da diverse API-Keys benötigt werden, welche kostenpflichtig sind. Dennoch wurde ein Scan der Fachhochschule St. Pölten durchgeführt. Bei diesem Scan wurden einige "falsche" Informationen gefunden, welche zuerst aussortiert werden mussten. Um die "falschen" Einträge zu bereinigen, müssen die Checkboxen neben dem jeweiligen "falschen" Eintrag ausgewählt werden. Anschließend können diese mittels dem "gelben"-Button als "falsch" gekennzeichnet werden. Anhand der Abbildung 35 „*Spiderfoot False Positive Flag*" ist zu sehen, wie der falsche Eintrag "Minecraft" direkt in dem Tool als falsch ausgewählt werden kann.

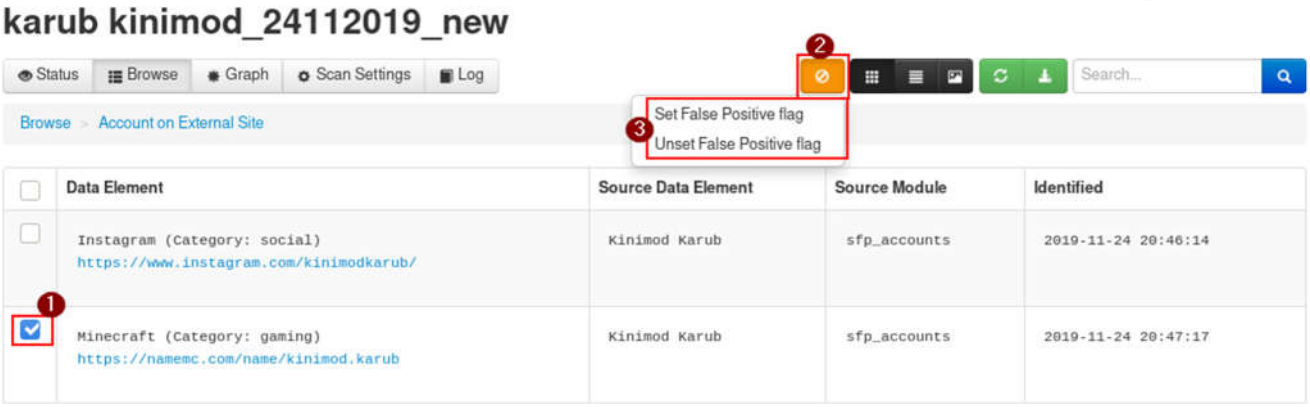


Abbildung 35 Spiderfoot False Positive Flag

Trotz dessen, dass nicht alle API-Keys verwendet worden sind, wurden wichtige Informationen über das Ziel gefunden. Bei der genaueren Analyse der Ergebnisse war ersichtlich, dass beispielsweise verschiedene E-Mail-Adressen, IP-Adressen, Ports, DNS-Einträge sowie offene Ports welche in Abbildung 39 „*Spiderfoot offene Ports*“ zu sehen sind und noch weitere Ergebnisse gefunden worden sind. Ebenso wurden auch mögliche Usernamen von Mitarbeitern gefunden. Anhand den Abbildungen 36 „*Spiderfoot Gesamtergebnis 1*“ bis Abbildung 38 „*Spiderfoot Gesamtergebnis 3*“, sind die verschiedenen Scanergebnisse zu sehen.

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	1110	1113	2020-01-28 16:23:10
Affiliate - Company Name	4	4	2020-01-28 12:22:19
Affiliate - Domain Name	5	7	2020-01-28 12:22:19
Affiliate - Domain Whois	2	4	2020-01-28 12:22:19
Affiliate - Email Address	106	373	2020-01-28 16:27:58
Affiliate - Internet Name	7	13	2020-01-28 12:22:16
Affiliate Description - Abstract	1	1	2020-01-28 12:22:20
Affiliate Description - Category	6	6	2020-01-28 12:22:20
BGP AS Membership	3	133	2020-01-28 16:27:58
BGP AS Peer	110	118	2020-01-28 11:52:32
Co-Hosted Site	115	141	2020-01-28 12:21:22
Co-Hosted Site - Domain Name	86	115	2020-01-28 12:21:25
Co-Hosted Site - Domain Whois	69	82	2020-01-28 11:53:41
DNS SPF Record	1	1	2020-01-28 12:22:36
DNS SRV Record	1	1	2020-01-28 12:22:14
DNS TXT Record	1	1	2020-01-28 12:22:36
Darknet Mention URL	1	1	2020-01-28 00:14:25
Domain Name	1	1	2020-01-27 23:23:05

Abbildung 36 Spiderfoot Gesamtergebnis 1

Email Address	154	199	2020-01-28 16:31:23
Email Gateway (DNS 'MX' Records)	4	4	2020-01-28 12:22:16
Hacked Email Address	29	29	2020-01-28 15:12:15
Human Name	73	125	2020-01-28 16:27:58
IP Address	48	329	2020-01-28 16:33:13
IPv6 Address	1	1	2020-01-28 09:56:51
Internet Name	176	938	2020-01-28 16:33:05
Internet Name - Unresolved	6	23	2020-01-28 12:23:54
Leak Site URL	21	21	2020-01-28 15:14:27
Linked URL - Internal	4139	4226	2020-01-28 16:33:05
Malicious Affiliate	6	6	2020-01-28 11:00:38
Malicious IP on Same Subnet	4	4	2020-01-28 11:52:28
Malicious Internet Name	3	3	2020-01-28 04:59:38
Name Server (DNS 'NS' Records)	4	10	2020-01-28 12:22:15
Netblock Membership	4	42	2020-01-28 16:27:56
Open TCP Port	127	129	2020-01-28 16:27:58
PGP Public Key	47	55	2020-01-28 15:01:57
Phone Number	1	1	2020-01-28 15:40:16
Physical Location	4	35	2020-01-28 16:27:58

Abbildung 37 Spiderfoot Gesamtergebnis 2

Public Code Repository	74	78	2020-01-28 15:24:57
Raw DNS Records	59	59	2020-01-28 16:32:28
Raw Data from RIRs/APIs	77	80	2020-01-28 16:27:58
Search Engine's Web Content	617	617	2020-01-28 16:33:05
Social Media Presence	8	8	2020-01-28 15:44:04
Software Used	10	64	2020-01-28 16:27:58
Username	226	230	2020-01-28 16:24:45
Vulnerability in Public Domain	96	483	2020-01-28 16:27:58
Web Technology	112	292	2020-01-28 12:19:55
Wikipedia Page Edit	125	125	2020-01-28 14:36:40

Abbildung 38 Spiderfoot Gesamtergebnis 3

```
Updated,Type,Module,Source,F/P,Data
2020-01-28 11:13:58,TCP_PORT_OPEN,sfp_shodan,131.130.4.9,0,131.130.4.9:443
2020-01-28 11:13:58,TCP_PORT_OPEN,sfp_shodan,131.130.4.9,0,131.130.4.9:80
2020-01-28 12:23:28,TCP_PORT_OPEN,sfp_shodan,195.202.144.2,0,195.202.144.2:25
2020-01-28 12:23:28,TCP_PORT_OPEN,sfp_shodan,195.202.144.2,0,195.202.144.2:587
2020-01-28 15:56:06,TCP_PORT_OPEN,sfp_shodan,195.202.144.53,0,195.202.144.53:22
2020-01-27 23:31:59,TCP_PORT_OPEN,sfp_shodan,91.219.68.10,0,91.219.68.10:53
2020-01-28 12:03:27,TCP_PORT_OPEN,sfp_shodan,91.219.68.189,0,91.219.68.189:8080
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:110
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:12345
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:1604
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:17000
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:18245
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:1883
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:20000
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:23
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:2323
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:2345
2020-01-28 12:08:17,TCP_PORT_OPEN,sfp_shodan,91.219.68.94,0,91.219.68.94:2375
```

Abbildung 39 Spiderfoot offene Ports

Anschließend werden die positiven sowie die negativen Auffälligkeiten des Tools angeführt.

Positiv aufgefallen ist:

- Verschiedene Scanfunktionen werden bereitgestellt und es werden verschiedene Bereiche gescannt
- Intuitive GUI
- Einträge können direkt in dem Tool entfernt werden

Negativ aufgefallen ist:

- Das Tool basiert auf API-Key, somit werden diese für diverse Plattformen benötigt. Wenn diese nicht verwendet werden, ist keine Suche auf dieser Plattform möglich.
- Genaue Eingabe des Usernamens – ansonsten ist die Suche erfolglos
- Im Vergleich zu Recon-NG waren mehrere falsche Einträge vorhanden

6.5. Tinfoleak

6.5.1. Beschreibung

Das Tool “Tinfoleak” ist standardmäßig auf der virtuellen Maschine von Buscador2 installiert. Es besteht ebenso die Möglichkeit das Tool webbasiert zu verwenden, somit kann das Tool auch ohne einer virtuellen Maschine verwendet werden. [138]
Hingegen können bei der webbasierten Version keine Scaneigenschaften durchgeführt werden. Das Tool wurde von Vicente Aguilera Diaz erstellt.

6.5.2. Allgemein

Das Tool und dessen Arbeitsweise ist simple. Es wird lediglich der Twitter Username des Ziels benötigt, welcher auf der Twitter Seite des Users ersichtlich ist. Anschließend werden von dem Tool die verschiedenen öffentlich freigegebenen Daten auf dem Twitter Profil abgefragt und abgespeichert. Nachdem der Scan abgeschlossen ist, wird das Ergebnis automatisch gespeichert. Wenn die webbasierte Variante verwendet wird, wird der Bericht an die angegebene E-Mail-Adresse gesendet, welche angegeben werden muss, damit der Scan durchgeführt werden kann.

Mit dem Tool können verschiedene Informationen über einen Twitter User gesammelt werden, wie beispielsweise Hashtags, Followers, Bilder/Videos, verwendete Geräte mit denen Posts erstellt wurden und auch welche Wörter am meisten verwendet worden sind. Ebenso ist es möglich, dass von Bildern, die hochgeladen wurden, die Geolocation Daten ausgelesen werden.
Das Tool ermöglicht weiters, dass eine Verbindung zwischen zwei unterschiedlichen Twitter Usern hergestellt wird. Somit können diese anschließend auf deren Gemeinsamkeiten verglichen werden.

6.5.3. Kriterien-Beschreibung

Das Kriterium “**Plattformen**” stellt für das Tool keine Schwierigkeiten dar. Dadurch, dass das Tool auch webbasiert unterstützt wird, werden alle möglichen Plattformen von dem Tool unterstützt.

Anschließend wird das Kriterium “**GUI/CLI**” geprüft. Das Tool bietet in der virtuellen Maschine sowie auf der webbasierten Version eine übersichtliche GUI an. Weiters ist es möglich das Tool mittels der CLI zu bedienen.

Das Kriterium “**Import**” wird als nächstes analysiert. Wenn das Tool in der virtuellen Maschine verwendet wird, ist es möglich ein File für eine Suche zu importieren. Bei der Webbrowser-Version ist kein Import möglich.

Nachdem das Importieren überprüft wurde, wird das Kriterium “**Exportieren**” überprüft. Dieses Tool bietet zwei verschiedene Export Möglichkeiten. Wenn der Scan mit dem Tool auf der virtuellen Maschine durchgeführt wird, wird der Scan automatisch nach Beendung als “html”-File abgespeichert. Es gibt auch die Möglichkeit den Scan über den Webbrowser durchzuführen, hier wird eine E-Mail-Adresse verlangt, um das Scan-Ergebnis an die Adresse zu senden. Das Ergebnis wird in einem “html”-File zu gesendet.

Anschließend wird das Kriterium “**Update**” geprüft. Das Kriterium Updates ist bei diesem Tool nicht möglich zu bewerten. Auf GitHub wurden die letzten Änderungen vor 2 Jahren durchgeführt (Stand von 06.02.2020).

Das Kriterium “**Such- und Filtermöglichkeit**” wurde anschließend überprüft. Nachdem der Scan durchgeführt wurde, wird automatisch eine “html”-Datei gespeichert. Dieses File kann anschließend geöffnet und durchsucht werden.

Ebenso wurde das Kriterium “**Kosten**” betrachtet. Das Tool kann kostenlos verwendet werden, ohne hinzufügen von API-Keys. Zu diesem Tool sind keine Kurse oder Schulungen gefunden worden.

Das Kriterium “**Informationen**” wurde anschließend analysiert. Mit dem Tool können folgende Informationen gesammelt werden:

- Follower
- Tweets
- Bilder
- Hashtags (meistverwendete)
- Geolocation
- Verwendete Wörter
- Metadaten

Unter einem Hashtag ist beispielsweise “#fhstp” zu verstehen. Das heißt, es wird ein Schlagwort nach einer Raute hinzugefügt. Somit können Themen in sozialen Netzwerken verbunden werden.

Als nächstes wurde das Kriterium “**Korrektheit der Daten**” analysiert. Es werden von dem Tool nur online geteilte Informationen von einem User gesammelt. Daher haben die Daten und Informationen, die gesammelt werden können, eine ausgesprochen hohe Korrektheit. Die Korrektheit besteht darin, da direkt die Twitter Seite des Users abgefragt wird und somit nur Informationen gesammelt werden, welche direkt von dem User freigegeben worden sind.

Anschließend wurde das Kriterium “**Berichtsverwaltung**” geprüft. Wenn der Scan anhand der Webbrowser-Version durchgeführt worden ist, wird in einem E-Mail ein Link mitgesendet. Durch das Anklicken des Links, öffnet sich eine Webseite, auf dieser die Scan-Ergebnisse zu sehen sind. Somit können die Ergebnisse der Scans über den Webbrowser eingesehen werden. Auf der virtuellen Maschine kann das automatisch abgespeicherte “html”-File geöffnet werden, um die Ergebnisse zu sehen.

Danach wurde das Kriterium “**Darstellungsfunktionen**” kontrolliert. Es wird von dem Tool ein html-File bereitgestellt, somit kann das Ergebnis des Scans übersichtlich in einem Webbrowser wiedergegeben werden und ist in verschiedene Kategorien gegliedert.

Darauffolgend wurde das Kriterium “**Rückverfolgbarkeit**” geprüft. Es werden in dem Bericht verschiedene Daten über eine Person zusammengefasst und aufbereitet. Dadurch ist es möglich individuelle Vorlieben einer Person herauszufinden. Weiters kann das Profil eines Opfers nachgestellt werden und von einem Angreifer auf weiteren Plattformen angelegt werden. Dies wird ermöglicht, da mit dem Tool “Freunde” und “Follower” gefunden werden können. Weiters können die Posts und das Wording einer Person festgestellt werden. Somit ist es möglich, die im Scan gefundenen Freunde auf einer weiteren Social Media Plattform, bei einem erstellten Fake User hinzuzufügen.
Weiters ermöglicht das Tool, das Herausfinden der Geolocations von Bildern, welche von Usern hochgeladen worden sind. Dadurch können Personen und deren Standorte herausgefunden werden.

Für welche „Attacken“ können die gefundenen Informationen verwendet werden:
Durch die gesammelten Informationen wird einem Angreifer die Möglichkeit gegeben Cyber Stalking zu betreiben. Es können aber ebenso “Fake Profile” von einem Unternehmen oder einer Person erstellt werden, somit können beispielsweise kriminelle Aktivitäten im Namen anderer durchgeführt werden. Durch die Auflistung der “meist verwendeten Wörtern” sowie “Hashtags” können Angreifer die “Firmensprache” lernen und diese beispielsweise für Spam-Mails oder Fake-Profile verwenden. Es wird weiters ermöglicht, gepostete Bilder herunterzuladen. Hier können die Geolocation-Daten

herausgefunden werden, damit können Opfer und deren Standorte ausgeforscht werden. Ebenso können die Tweets für eine genaue Analyse und "versteckte" Informationen überprüft werden.
Diese Angriffsarten sind im Detail in Kapitel 4.8 „*Intelligence Collections und Angriffsarten*" beschrieben.

6.5.4. Praktischer Test

Das Tool ist userfreundlich zu starten, dazu muss lediglich auf der linken Seite der Social Media Button (ähnlich wie das Twitter Zeichen) gedrückt werden, hier muss anschließend das Tool "Tinfoleak" ausgewählt werden. Danach können noch verschiedene Einstellungen durchgeführt werden, wie beispielsweise das Datum der Zeitspanne des gewünschten Suchergebnisses. Abbildung 40 „*Tinfoleak starten*" zeigt, wie das Tool gestartet werden kann. In der Abbildung 41 „*Tinfoleak Tool Dashboard*" ist zu sehen wie das Programm nach dem Starten für einen User zu sehen ist und welche Einstellungen durchgeführt werden können. In dem Feld "User" wird der Twitter User Name des Ziels eingegeben. Anschließend können noch Sucheinstellungen vorgenommen werden, welche bei "Operations" ersichtlich sind. Bei dem Punkt "Filter" können Start und End Datum angegeben werden, damit können zeitliche Abgrenzungen gebildet werden für eine Suche.

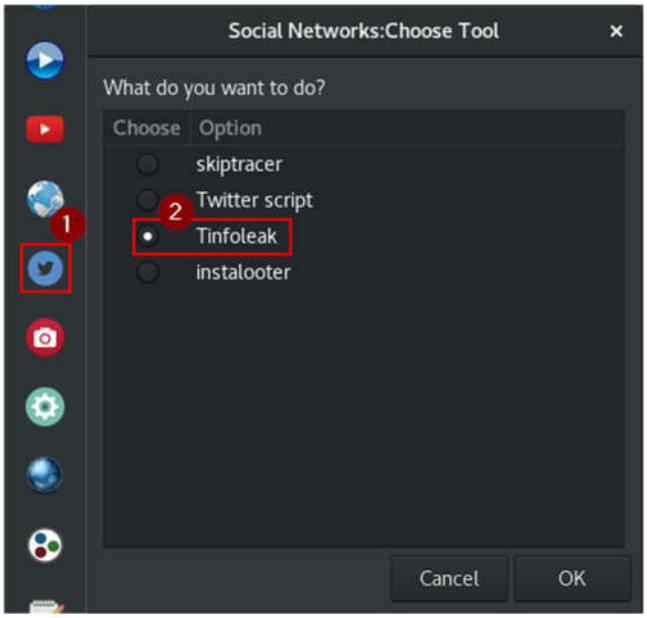


Abbildung 40 Tinfoleak starten

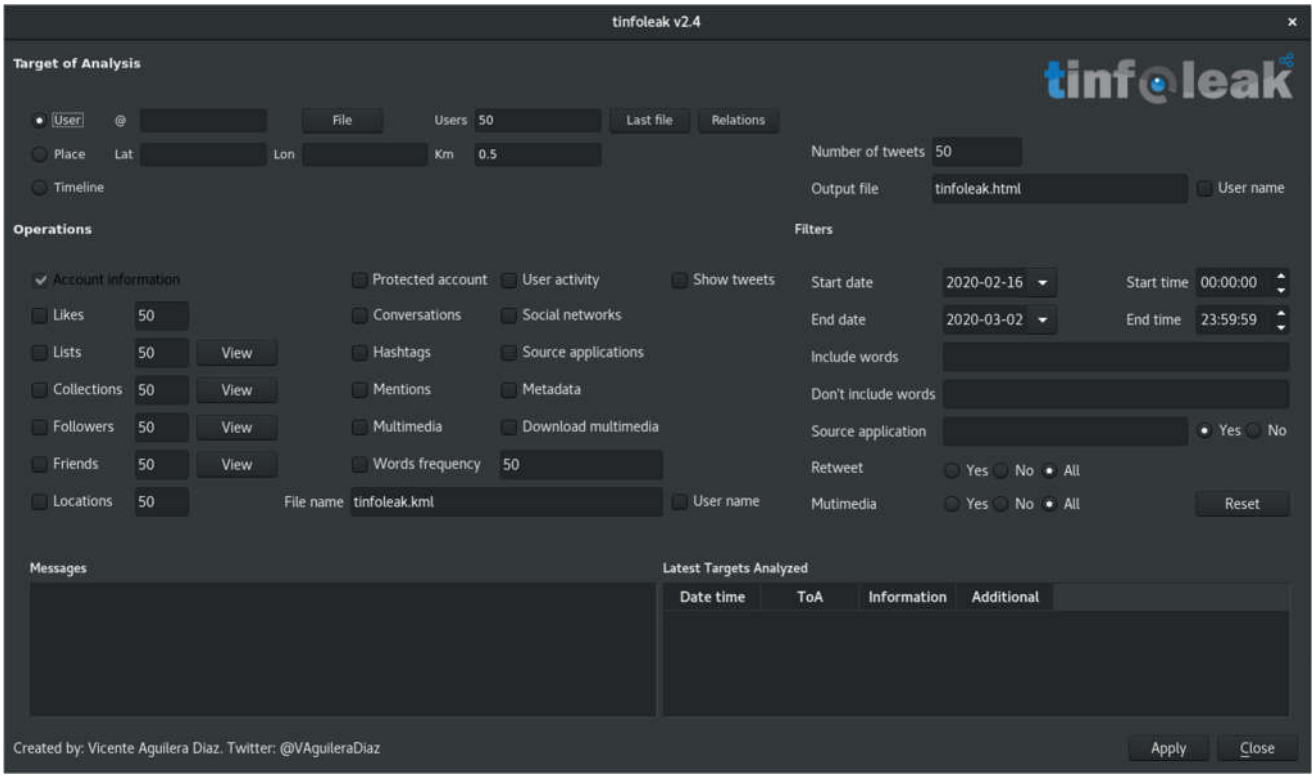


Abbildung 41 Tinfoleak Tool Dashboard

Anschließend wir in der Abbildung 42 „*Tinfoleak Webbrowser*“ die Webbrowser Version des Tools gezeigt. Hier ist lediglich der Twitter User Name erforderlich und eine E-Mail-Adresse, an welche der Bericht gesendet wird.

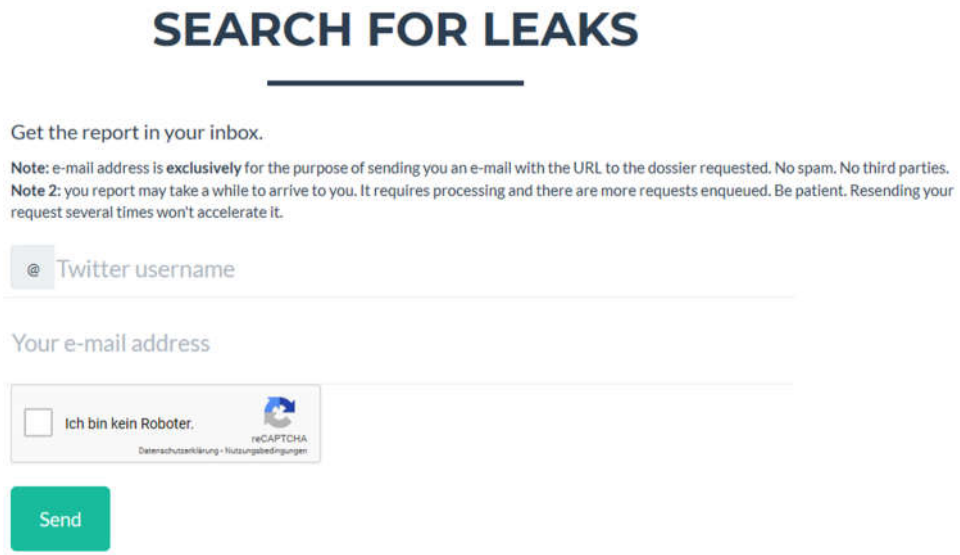


Abbildung 42 Tinfoleak Webbrowser

Bei diesem Tool wurde der Fokus auf die Twitter Seite der Fachhochschule gesetzt. Damit ein Scan durchgeführt werden kann, muss zuerst der Username des Ziels bekannt sein. Dazu wird mittels

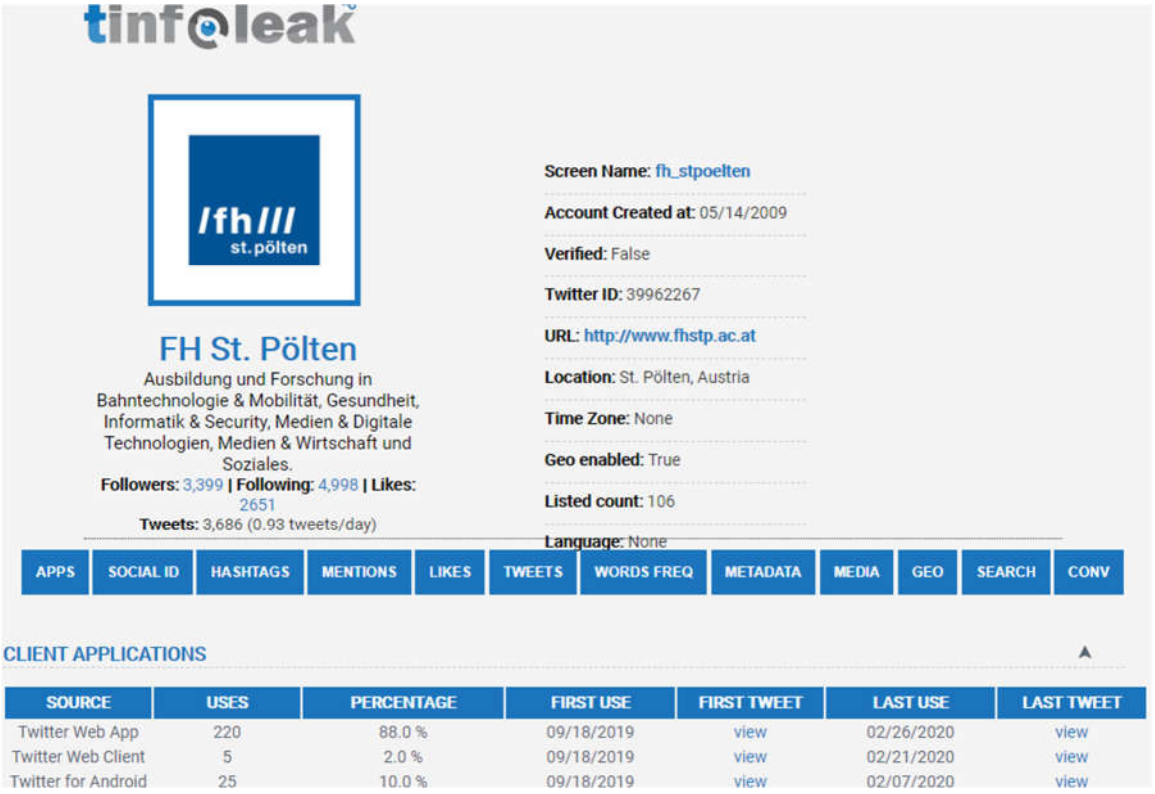
Suchmaschinen das Ziel und dessen Username ermittelt. Der Twitter User Name kann weiters, direkt von der Twitter Seite des Ziels genommen werden, was in Abbildung 43 „*Twitter FH Username*“ ersichtlich ist.

Abbildung 43 Twitter FH Username

Nachdem der Username bekannt ist, kann dieser in dem Tool eingegeben werden und der Scan kann durchgeführt werden. Der Scan ist auf der virtuellen Maschine “Buscador2” sowie auf der Webbrowser Version durchgeführt worden. Nachdem der Scan erfolgreich abgeschlossen ist, wird automatisch ein “html”-File mit den gesammelten Informationen über das Profil des Ziels generiert. Bei der Webbrowser Version wird ein E-Mail mit dem Scanergebnis an die Person gesendet. Dadurch wird es ermöglicht, das Ergebnis des Scans wiederzuverwenden.

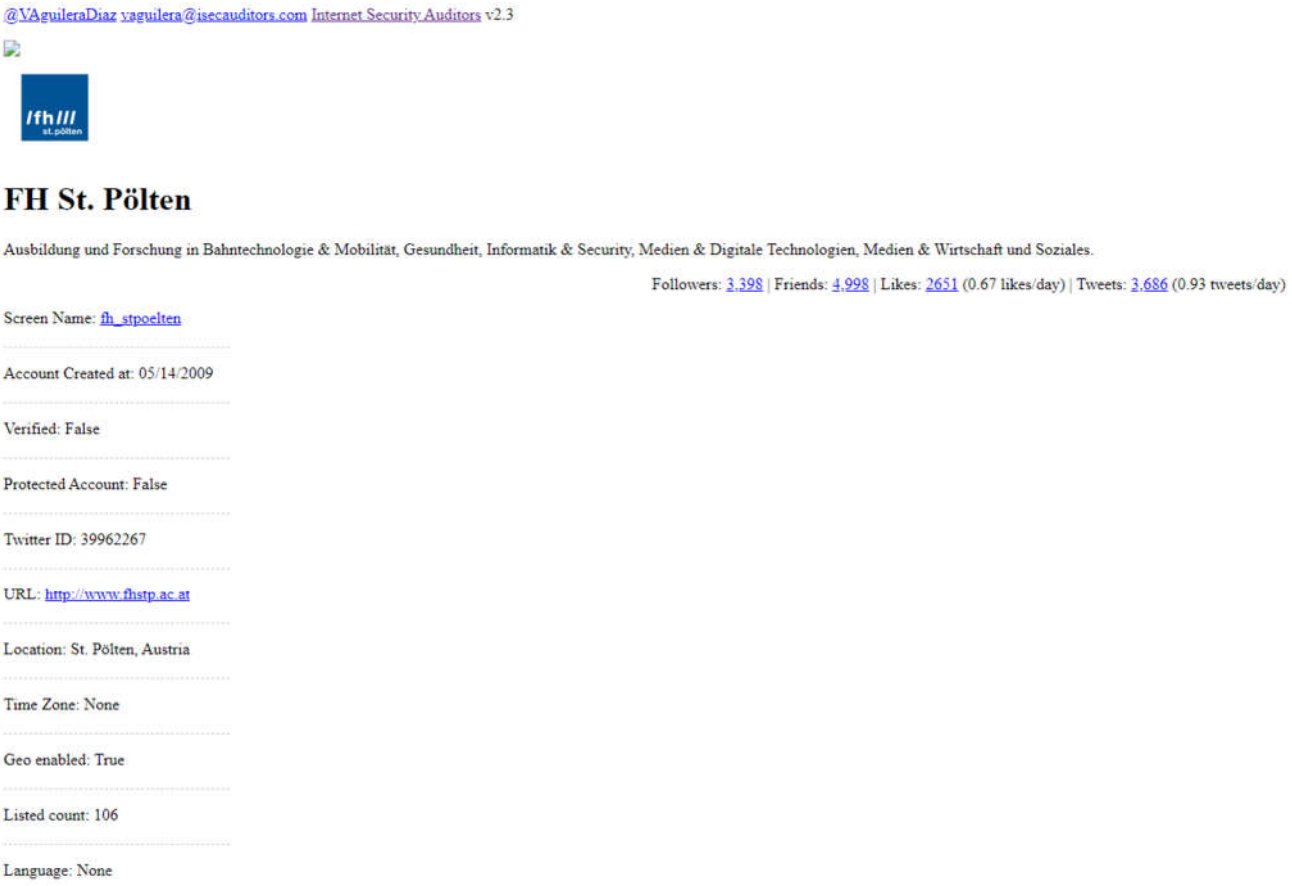
Dieses File kann anschließend im Detail analysiert werden. Dieser Bericht enthält verschiedene Informationen wie verwendete Hashtags, Followers, Bilder/Videos, verwendete Geräte mit denen Posts erstellt wurden, Geolocation und auch welche Wörter am meisten verwendet worden sind.

Anschließend wurde der Bericht von der virtuellen Maschine mit dem des Webbrowsers verglichen. Es wurde festgestellt, dass die Darstellung von dem Bericht des Webbrowsers übersichtlicher aufgebaut ist. Der Vergleich der beiden durchgeführten Scans ist in Abbildung 44 „*Tinfoleak Webbrowser-Scanergebnis*“ (Webbrowser) sowie Abbildung 45 „*Tinfoleak Tool-Scanergebnis*“ (Tool) zu sehen.



SOURCE	USES	PERCENTAGE	FIRST USE	FIRST TWEET	LAST USE	LAST TWEET
Twitter Web App	220	88.0 %	09/18/2019	view	02/26/2020	view
Twitter Web Client	5	2.0 %	09/18/2019	view	02/21/2020	view
Twitter for Android	25	10.0 %	09/18/2019	view	02/07/2020	view

Abbildung 44 Tinfoleak Webbrowser-Scanergebnis



@VAguileraDiaz vaguilera@isecauditors.com Internet Security Auditors v2.3

FH St. Pölten

Ausbildung und Forschung in Bahntechnologie & Mobilität, Gesundheit, Informatik & Security, Medien & Digitale Technologien, Medien & Wirtschaft und Soziales.

Followers: 3,398 | Friends: 4,998 | Likes: 2651 (0.67 likes/day) | Tweets: 3,686 (0.93 tweets/day)

Screen Name: fh_stpoelten

Account Created at: 05/14/2009

Verified: False

Protected Account: False

Twitter ID: 39962267

URL: http://www.fhstp.ac.at

Location: St. Pölten, Austria

Time Zone: None

Geo enabled: True

Listed count: 106

Language: None

Abbildung 45 Tinfoleak Tool-Scanergebnis

Zu Beginn werden allgemeine Informationen bereitgestellt, wie beispielsweise das Erstellungsdatum des Accounts, die Twitter-ID sowie eine Ortsangabe. Ebenso wird angezeigt wie viele Follower der User hat und wie vielen Personen der User selber folgt. Es wird auch angezeigt, wie viele Likes vergeben worden sind und wie viele Tweets gesendet worden sind, daraus wird berechnet wie viele Tweets am Tag von dem User veröffentlicht werden, welches in Abbildung 44 „*Tinfoleak Webbrowser-Scanergebnis*“ zu sehen ist.

Eine interessante Information, welche in Abbildung 46 „*Tinfoleak Client Applications 1*“ zu sehen ist, wird von dem Tool zur Verfügung gestellt, indem angezeigt wird, von welchem Endgerät, Web-App oder Operation-System die meisten Tweets gesendet werden. Seitens der Fachhochschule wird zumeist die Twitter Web App verwendet. Weiters ist bei dem Vergleich der Abbildung 46 „*Tinfoleak Client Applications 1*“ (Scan am 06-02-2020) mit der Abbildung 47 „*Tinfoleak Client Application 2*“ (Scan am 01-03-2020) zu sehen, dass in der Zeit zwischen dem ersten Scan und dem zweiten Scan vermehrt der Web Client verwendet worden ist (Anstieg um 0,4%). Die Abbildungen der Berichte und Ergebnisse sind von der Webbrowser Version aufgenommen worden – da die Ergebnisse besser dargestellt werden.

APPS | SOCIAL ID | HASHTAGS | MENTIONS | LIKES | TWEETS | WORDS FREQ | METADATA | MEDIA | GEO | SEARCH | CONV

CLIENT APPLICATIONS

SOURCE	USES	PERCENTAGE	FIRST USE	FIRST TWEET	LAST USE	LAST TWEET
Twitter Web App	221	88.4 %	08/21/2019	view	02/05/2020	view
Twitter for Android	25	10.0 %	08/26/2019	view	12/05/2019	view
Twitter Web Client	4	1.6 %	08/21/2019	view	12/05/2019	view

Abbildung 46 Tinfoleak Client Applications 1

APPS | SOCIAL ID | HASHTAGS | MENTIONS | LIKES | TWEETS | WORDS FREQ | METADATA | MEDIA | GEO | SEARCH | CONV

CLIENT APPLICATIONS

SOURCE	USES	PERCENTAGE	FIRST USE	FIRST TWEET	LAST USE	LAST TWEET
Twitter Web App	220	88.0 %	09/18/2019	view	02/26/2020	view
Twitter Web Client	5	2.0 %	09/18/2019	view	02/21/2020	view
Twitter for Android	25	10.0 %	09/18/2019	view	02/07/2020	view

Abbildung 47 Tinfoleak Client Application 2

Es kann zudem eine Statistik über die meist verwendeten Hashtags gegeben werden, welche in Abbildung 48 „*Tinfoleak Top Hashtags*“ zu sehen sind. Hier werden die meisten “Top 5” verwendeten Hashtags gezeigt.

TOP HASHTAGS

DATE (SINCE)	DATE (UNTIL)	RT	LIKE	COUNT	#HASHTAG
09/18/2019	02/20/2020	64	180	40	#fhstp
09/27/2019	10/08/2019	9	56	14	#Forschungsfest
11/12/2019	12/05/2019	3	9	10	#wissenvorsprung
11/07/2019	11/07/2019	22	54	8	#ForschungsChillOut
10/02/2019	02/20/2020	22	38	8	#Blockchain

Abbildung 48 Tinfoleak Top Hashtags

Weiters ist durch den Scan ersichtlich, welche Wörter der User am häufigsten verwendet. Dies kann nützlich sein, wenn man die Firmensprache lernen möchte.

In dem Bericht wird bei jedem gefundenen Usernamen, ein Link hinterlegt. Somit ist es möglich, dass direkt per Mausklick auf das Profil eines Users gesurft werden kann, ohne diesen separat in Twitter einzugeben.

Generell sollten die Sicherheitsmaßnahmen bei den jeweiligen Twitter-Profilen überprüft werden.
Es sollte die geografische Position deaktiviert werden, ansonsten besteht die Möglichkeit, dass die Geolocation-Daten von einem User anhand des Bildes oder des Tweets herausgefunden werden können. [139]
Weiters sollten auch die Tweets-Einstellungen überarbeitet werden. Standardmäßig können die Tweets von jedem gelesen werden, daher sollte diese Einstellung geändert werden. [140]

6.5.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests

Das Tool ist selbsterklärend und daher sind keine Herausforderungen festgestellt worden.

6.5.6. Ergebnisse und Fazit

Das Tool ist für das Analysieren von Twitter-Usern sehr gut geeignet. Der Bericht der Scans ist übersichtlich und kann für weitere Untersuchungen und Angriffsvorbereitungen gespeichert werden.
Die persönliche Empfindung ist, dass die Berichte und Ergebnisse von der Webbrowser Version übersichtlicher dargestellt werden, im Gegensatz zu dem Bericht des Tools.

Anschließend werden die positiven sowie die negativen Auffälligkeiten des Tools angeführt.

Positiv aufgefallen ist:
- Kein API-Key für eine Suche benötigt
- Verbindungen können zwischen Usern hergestellt werden

Negativ aufgefallen ist:
- Wenig Dokumentation vorhanden
- Wenige Berichte verfügbar

6.6. Twitter-Script/Twitter-Exporter

6.6.1. Beschreibung

Das Tool “Twitter-Script/Twitter-Exporter” ist standardmäßig auf der virtuellen Maschine “Buscador2” enthalten, daher ist eine manuelle Installation nicht notwendig gewesen. Das Tool benötigt keine weiteren Einstellungen, denn es wird nachdem das Tool gestartet wird, lediglich nach dem Twitter-Usernamen gefragt, welcher von der Twitter Seite entnommen werden kann. Nachdem dieser eingegeben wurde, beginnt das Programm die Twitter Posts sowie Bilder des Ziels herunterzuladen. Weiters sind noch die Freunde und Follower sowie die User-ID mit den Usernamen verbunden worden. Das Tool bietet nur eine Version, diese ist kostenlos verfügbar. Das Tool wurde von Michael Bazzle entwickelt.

6.6.2. Allgemein

Nachdem das Tool gestartet worden ist, öffnet sich ein Fenster, welches lediglich die Eingabe des Twitter-Username erwartet.
Nachdem der Twitter Username eingegeben worden ist, startet das Tool automatisch den Scan Vorgang und sucht nach verschiedenen Daten, Bildern und Informationen auf der Twitter Seite.
Es ist sehr leicht mit dem Tool einen Scan über ein Ziel durchzuführen, da lediglich der Username eines Twitter-User benötigt wird. Nachdem dieser eingegeben worden ist, werden die gesamten öffentlichen Daten der Twitter-Seite gesammelt und gespeichert. Weiters müssen bei dem Tool keine weiteren Einstellungen durchgeführt werden und es wird kein API-Key benötigt.

6.6.3. Kriterien-Beschreibung

Anfangs wurde das Kriterium “**Plattform**” analysiert. Das Tool ist auf der virtuellen Maschine “Buscador2” verfügbar.

Das Kriterium “**GUI/CLI**” wurde anschließend überprüft. Nachdem das Tool gestartet worden ist, wird lediglich in einem kleinen GUI Fenster nach dem Usernamen gefragt.

Danach wurde das Kriterium "**Import**" kontrolliert. Das Tool stellt keine Möglichkeit dar, um Informationen zu importieren und diese in einem Scan vom Tool "Twitter-Exporter" weiter zu verwenden.

Das Kriterium "**Export**" wurde als nächstes analysiert. Nachdem ein Scan durchgeführt worden ist, wird automatisch ein "csv"-File erzeugt.

Das Kriterium "**Updates**" wurde trotz Recherchen bei diesem Tool nicht gefunden.

Ein wichtiges Kriterium "**Such- und Filtermöglichkeiten**" wurde danach überprüft. Das Tool speichert automatisch nach dem Beenden des Scans das Ergebnis als "csv"-File ab. Dieses File kann in anderen Tools geöffnet werden und durchsucht werden, sowie verschiedene Filter darauf angewendet werden. Weiters werden gefundene Bilder von der Twitter-Seite des Users heruntergeladen und in einem separaten Ordner gespeichert.

Anschließend wurde das Kriterium "**Kosten**" überprüft. Das Tool ist kostenlos zu verwenden und es werden keine kostenpflichtigen Versionen angeboten. Ebenso werden keine Schulungen zu diesem Tool angeboten.

Das Kriterium "**Informationen**" stellt eine sehr wichtige Analyse dar. Es ist möglich von dem Tool folgende Informationen zu bekommen:

- Bilder des Twitter-Users
- Twitter-Usernamen
- Namen von Personen
- Freunde die auf Twitter folgen
- Tweets/Retweets mit Zeitstempel

Das nächste Kriterium, welches überprüft wird, ist "**Korrektheit der Daten**". Das Tool analysiert und speichert Informationen, welche direkt auf der Twitter-Seite des Ziels gefunden werden können. Daher sind die Informationen für eine weitere Verwendung wie beispielsweise einer Personenüberprüfung zu verwenden.

Anschließend wurde das Kriterium "**Berichtsverwaltung**" im Detail geprüft. Nachdem das Tool mit dem Scan fertig ist, werden automatisch drei "csv" Dateien abgespeichert. Diese sind für eine Wiederverwendung geeignet. In dem Bericht befinden sich Namen von Personen und Textabschnitte von Tweets, welches in Abbildung 53 „*Twitter-Script erstellter Ordner mit* " ersichtlich ist.

Das Kriterium "**Darstellungsfunktionen**" wurde darauffolgend überprüft. Die gespeicherten Informationen werden als Tabellenformat abgespeichert, des Weiteren werden Bilder gespeichert, welche analysiert werden können.

Ein wichtiges Kriterium stellt die "**Rückverfolgbarkeit**" dar. Durch die Informationen, welche mit diesem Tool gefunden werden, können weitere Recherchen durchgeführt werden. Mit den gefundenen Informationen wie beispielsweise dem Namen einer Person, können erste Suchanfragen auf diversen Social Media Plattformen gestartet werden. Die Ergebnisse, welche in einer Tabelle wiedergegeben werden, können damit analysiert werden. Somit können ebenso über die Freunde des Ziels Nachforschungen durchgeführt werden.

Für welche „Attacken" können die gefundenen Informationen verwendet werden:
Mittels den Informationen, welche mit dem Tool gesammelt werden können, ist es möglich verschiedene Angriffe zu planen. Durch die Bilder, die heruntergeladen werden mit dem Tool können

Überprüfungen zu den hinterlegten Geolocation-Daten durchgeführt werden. Es werden die gesamten Freunde aufgelistet, somit besteht die Möglichkeit, die Freunde in das “Fake Profil” hinzuzufügen.
=> Facebook Attacke 2020 - "Romance-Scamming"

Es können dadurch Aktivitäten unter einem anderen Namen durchgeführt werden. Weiters wird der Twitter Username von den “Freunden” in einer Tabelle gespeichert, somit können weitere Personen ausgeforscht und Fake Profile angelegt werden. Diese Angriffsarten sind im Detail in Kapitel 4.8 „*Intelligence Collections und Angriffsarten*“ beschrieben.

6.6.4. Praktischer Test

Nachdem das Tool gestartet worden ist, wird nach dem Usernamen des Ziels (Twitter-User) gefragt. Sobald die Eingabe erfolgt ist, wird keine weitere Interaktion des Users benötigt, da das Tool automatisch nach einem Suchvorgang startet. Das Starten sowie die User-Name-Eingabe wird in Abbildung 49 „*Twitter-Script starten*“ und 50 „*Twitter-Script Twittername-Eingabe*“ gezeigt.

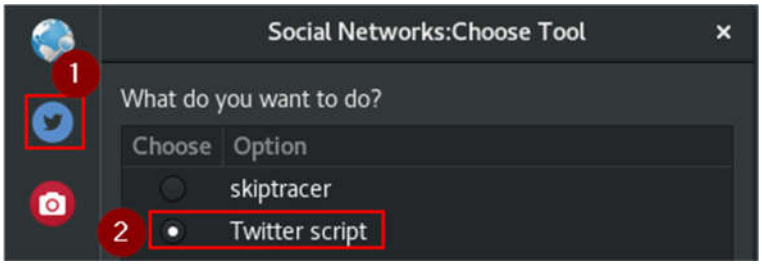


Abbildung 49 Twitter-Script starten

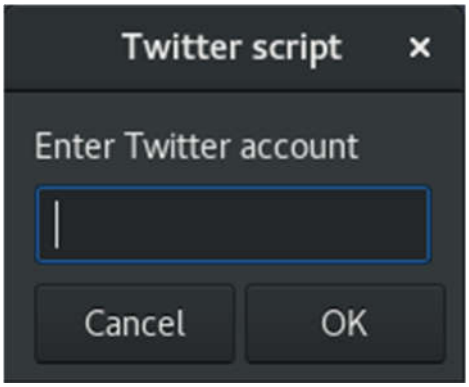


Abbildung 50 Twitter-Script Twittername-Eingabe

Im Terminal werden die aktuellen Suchen angezeigt, weiters wird gezeigt, ob gerade beispielsweise Bilder heruntergeladen werden von dem Programm. Abbildung 51 „*Twitter-Script Tweets sammeln*“ zeigt die Suche nach den Tweets eines Users. In Abbildung 52 „*Twitter-Script Photos sammeln*“ ist ersichtlich, dass von dem Tool verschiedene öffentliche Bilder eines Twitter Users heruntergeladen werden.

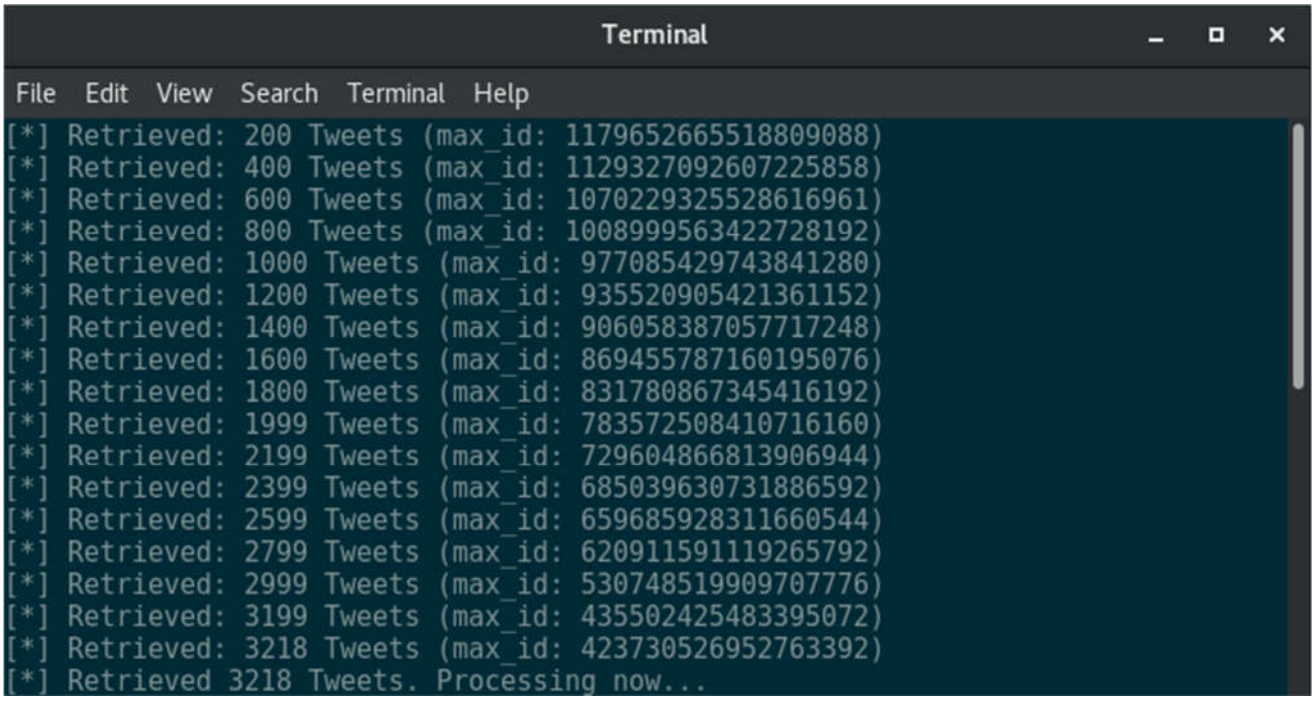


Abbildung 51 Twitter-Script Tweets sammeln

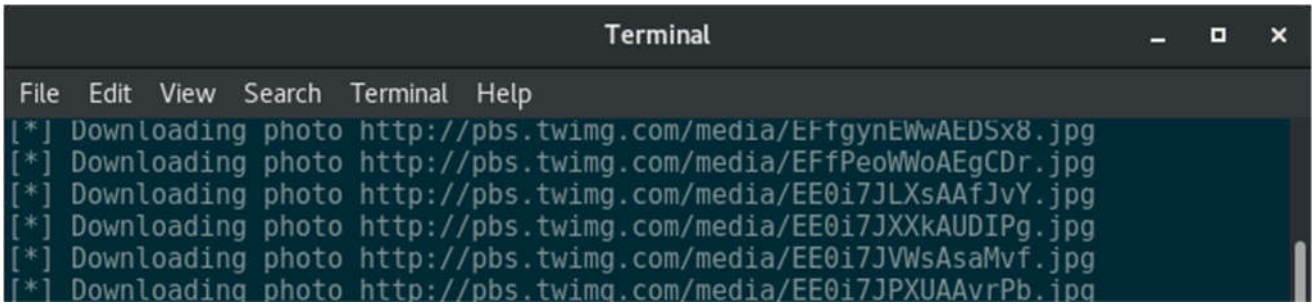


Abbildung 52 Twitter-Script Photos sammeln

Nach dem Abschluss des Scans, werden diese automatisch in dem Default-Ordner des Tools gespeichert. Es wurden insgesamt drei verschiedene csv-Dateien erstellt. Eine Datei enthält die “Followers” des Ziels, eine weitere enthält “Freunde” und die letzte “Twitter” enthält die verschiedenen Tweets, welche gespeichert wurden. Ein Tweet ist eine Statusmeldung von 140 Zeichen, welche von einem User geschrieben werden, worin verschiedene Situationen oder Lebenslagen beschrieben werden können.
In der “Followers”-Liste sind alle Followers des Twitter-Users angeführt. Die “Freunde”-Liste enthält alle Freunde des Users und die “Tweets”-Liste beinhaltet die Tweets des Users. In der “Followers” und “Friends” Liste sind einerseits die Twitter-Usernamen der Personen enthalten aber ebenso auch die realen Namen von Personen (wenn dieser auf Twitter angegeben worden sind).
Weiters wurde ein Ordner erstellt, in diesem sind diverse öffentliche Fotos vom Format “jpg” und “png” gespeichert worden. Dies sind Fotos, welche auf der Twitter-Seite des Ziels verfügbar waren. Diese Dateien, welche angelegt werden, sind in der Abbildung 53 „*Twitter-Script erstellter Ordner mit* “ zu sehen.

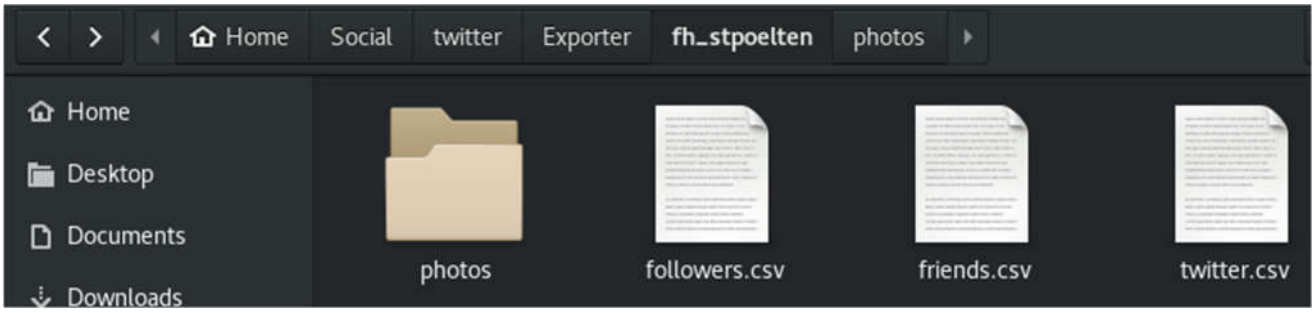


Abbildung 53 Twitter-Script erstellter Ordner mit Dateien

6.6.5. Herausforderungen und Erkenntnisse während den Vorbereitungen auf die Tests

Es gibt leider sehr wenige Informationen und Dokumentationen über dieses Tool. Dies war eine Herausforderung, da keine Beschreibung des Speicherortes angegeben wurde.

6.6.6. Ergebnisse und Fazit

Das Tool ist sehr leicht zu bedienen, da lediglich der Username eingegeben werden muss und anschließend der Scan automatisch durchgeführt wird. Die Speicherung des Scans und der Ergebnisse erfolgt ebenso automatisch. [141]

Anschließend werden die positiven sowie die negativen Auffälligkeiten des Tools angeführt.

Positiv aufgefallen ist:
- Sehr leicht zu bedienen
- Kein API-Key für die Suche erforderlich
- Automatische Speicherung von Ergebnissen

Negativ aufgefallen ist:
- Keine Dokumentation
- Sehr unbekannt das Tool

7. OSINT Use Case

In diesem Kapitel werden verschiedene Use Cases in Zusammenhang mit OSINT gebracht. Dadurch soll die Vielfältigkeit des Themenbereiches gezeigt werden. [4]
Es soll durch die Use Cases die Wichtigkeit des Themas demonstriert werden und es soll gezeigt werden, wie wichtig OSINT in den verschiedenen Bereichen ist. Die Use Cases werden anhand verschiedener Bereiche beschrieben, wie beispielsweise aus der Sicht von Unternehmen aber teilweise auch aus Sicht eines Angreifers. Weiters werden auch verschiedene Arten von Use Cases beschrieben, welche durch die vermehrten, verfügbaren Informationen möglich sind.

Tabelle 10 zeigt die Informationen, welche mit den jeweiligen Tools gesammelt werden können:

Tools	Informationen
Maltego	Personen/Namen/E-Mail-Adressen/Alias, Gruppen von Personen (Soziale Netzwerke), Unternehmen, Organisationen, Webseiten, DNS/Domains/Internet, Infrastrukturen, Verbindungen/Zugehörigkeiten, Dokumente/Files
TheHarvester	E-Mail-Adressen, Sub-Domains, Hosts, Namen, IP-Adressen, Ports/Banner
Recon-NG	Telefonnummern, E-Mail-Adressen, Standorte, Webseiten, Hosts, IP-Adressen, Personen/Unternehmen, Usernamen
Spiderfoot	Domain Name (DNS), IP-Adressen, Hostnamen/Sub-domains, Subnetze, ASN, E-Mail-Adressen, Telefonnummern, Namen von Personen
Tinfoleak	Follower, Tweets, Bilder, Hashtags (meistverwendete), Geolocations, verwendete Wörter, Metadaten
Twitter-Script	Bilder des Twitter-Users, Twitter-Usernamen, Namen von Personen, Freunde die auf Twitter folgen, Tweets/Retweets mit Zeitstempel

Tabelle 10 Welche Informationen können mit dem Tool gesammelt werden

Use Case der Arbeit:
Diese Arbeit zeigt einem Unternehmen verschiedene kostenlose Tools, um einerseits ihre Infrastruktur auf kritische Informationen zu überprüfen, andererseits kann auch der Social Media Account überprüft werden, auf kritische Informationen und Schwachstellen.

Anschließend sind drei verschiedene Use Cases beschrieben. Der erste Use Case beschreibt anhand der Tools das Finden von Schwachstellen. Der zweite Use Case beschreibt die Gefahren von Phishing. Der dritte Use Case beschreibt den Umgang mit firmeninternen Daten auf verschiedenen Share-Plattformen und Social Media Plattformen.

Use Case1: Finden von Schwachstellen (um Schwachstellen oder veraltete Versionen zu sehen):

Eine mögliche Schwachstelle könnte das Wissen sein, der verwendeten Software. Kritischer ist diese Information jedoch, wenn die Version der Software bekannt ist, somit können Schwachstellen der Version einer Software gesucht werden.
Hier könnte das Testing Framework Metasploit [142] verwendet werden. Dieses Framework listet eine Fülle von Attacken gegen eine bestimmte Software und dessen Version und es können alle Exploits getestet werden. Eine weitere Schwachstelle ist das Wissen von den offenen Ports.

Mit dem Tool “TheHarvester”, welches in Kapitel 6.2 „*TheHarvester*“ beschrieben ist, können passive Scans durchgeführt werden. Eines der interessanten Features von dem Tool ist das Suchen nach offenen Ports sowie E-Mail-Adressen. In das Tool kann ebenso das Online-Information-Gathering Tool

Shodan [115] eingebunden werden. Die Voraussetzung für die Verwendung von Shodan ist ein API-Key (Application Programming Interface-Key), welcher zuvor aus der Weboberfläche von Shodan kopiert und anschließend in "TheHarvester" importiert werden muss.

Nachdem der Scan abgeschlossen wurde, ist ersichtlich gewesen, dass das “TheHarvester” mit dem eingebundenen “Shodan”-API-Key nicht alle Informationen abholen konnte, wie dies direkt auf der Weboberfläche von Shodan der Fall war. Beispielsweise konnte die Softwareversion des Webservers nur auf der Shodan Weboberfläche eingesehen werden, da Shodan ein Banner-Grabbing anbietet und die derzeit eingesetzte Version eines Webservers anzeigt.
Angreifer können diese System-Banner (zeigt die Systemversion an) direkt dazu nutzen, um Penetration Tests mittels Penetration Frameworks z.B.: Metasploit Framework durchzuführen. Daher ist es für IT-Netzwerkpersonen wichtig, die Versionen zu kennen, die installiert wurden.

Eine Empfehlung für „TheHarvester“ wäre neben der Anzeige der Ports und der Apache-Software auch die Version anzuzeigen, damit lassen sich die Abfragen besser durch Scripting automatisieren. Eine weitere Einschränkung gibt es noch, denn ohne einem Abo bei Shodan können nur 3 Abfragen an einem Tag durchgeführt werden, welches bei größeren Unternehmen zu wenig sind und sich dadurch das passive Information-Gathering über mehrere Tage erstrecken kann.
Wie schon erwähnt, handelt es sich um passive Informationen. Die Informationen, welche bei einem passiven Scan gefunden werden, müssen nicht korrekt sein. Es kann sein, dass die Resultate, die gefunden worden sind, bereits vor einiger Zeit, von beispielsweise einem Netzwerkadministrator, behoben worden sind. Daher kommt es sehr stark auf das Aktualisierungsintervall der jeweiligen OSINT-Quellen an. Es sollten diese Informationen immer geprüft werden und kritisch hinterfragt werden.
Ersichtlich ist in dem Auszug eines Scans, welcher in Abbildung 13 „*TheHarvester Scanergebnis Auszug*“ ersichtlich ist, dass verschiedene offene Ports gefundenen worden sind. Die gefundenen Informationen über offene Ports können von Angreifern als auch von einem Netzwerkadministrator gefunden werden. Dieser muss anhand der Ergebnisse anschließend überprüfen, ob es einen legitimen Grund gibt, warum dieser Port offen ist oder ob dieser unverzüglich geschlossen werden muss, da ein Risiko dadurch gegeben ist und das Unternehmen damit angreifbar ist.

Nachdem beispielsweise ein Port geschlossen wurde, sollte diese Deaktivierung auch geprüft werden. Dazu kann ein Netzwerkadministrator einen aktiven Port Test von außen, dem Internet, starten.
Ein aktiver Scan, der vom eigenen Unternehmen durchgeführt wird, um die eingesetzten Systeme zu scannen, welche aus dem Internet erreichbar sind, ist ein nützlicher Schritt, den der Netzwerkadministrator durchführen und diesen mit einem passiven Scan ergänzen kann. Oftmals reicht ein passives Information Gathering aber nicht aus, da entweder falsche Informationen in den OSINT Informationen vorhanden sind oder nicht alle Schwachstellen (wie beispielsweise offene Ports, Applikationen und deren Versionen) gelistet werden. Der aktive Scan gibt schlussendlich die konkreten und aktuellen Informationen über die Schwachstellen und kann anschließend mit den Ergebnissen vom passiven Information Gathering verglichen werden.

Systeme aus dem Internet sind vielen Bedrohungen ausgesetzt, somit benötigen gerade diese, welche aus dem Internet erreichbar sind, eine hohe Aufmerksamkeit und Schutz.
Ein Unternehmen sollte daher auch in regelmäßigen Abständen einen geplanten aktiven Scan gegen die Systeme durchführen, welche aus dem Internet erreichbar sind.
Bei einem aktiven Scan muss das Management involviert sein und dies absegnen und somit einem IT-Mitarbeiter, welcher für die interne Sicherheit zuständig ist, die Erlaubnis erteilen, diesen Scan durchzuführen.

Der Netzwerkadministrator kann weitere grundlegende Basis-Vorkehrungen treffen, um Attacken zu verhindern oder einzudämmen, indem beispielsweise regelmäßig ein Patchmanagement und eine Aktualisierung der Software des Systems durchgeführt werden.
„TheHarvester“ und dessen Port Scan sollte immer in Verbindung mit “Shodan” [115] verwendet werden, eine detaillierte Begründung wird in dem Abschnitt “Vergleich der Tools“ gegeben. Damit kann das Scanergebnis genauer analysiert und die gefundenen Informationen validiert werden.

Das Tool “Recon-NG” welches im Kapitel 6.3 „*Recon-ng*“ beschrieben ist, bietet verschiedene Module für einen Scan an. Mit dem Modul “*use recon/domains-hosts/brute_hosts”* und *“use recon/domains-hosts/bing_domain_web”* oder “*use recon/domains-hosts/google_site_web”* können zu den gefundenen Hosts auch Rückschlüsse auf verwendete Systeme in einem Unternehmen gegeben werden, was in der Abbildung 18 „*Recon-NG Hosts/IP-Adressen Auszug*“ ersichtlich ist.
Wenn es ermöglicht wird die Versionsnummer einer Software oder einer Applikation herauszufinden, können Angreifer gezielt nach gelisteten CVE Schwachstellen suchen und diese durch Exploits, sogenannte Attacken, ausnutzen.
Von dem Tool werden keine Versionsnummern der verwendeten Software oder einer Applikation angeführt, daher dient dies nur als “potenzielles” Risiko, da dennoch auf der CVE Plattform nach möglichen Schwachstellen dieser Systeme gesucht werden kann. Der Nachteil ist, dass ein Angriff ohne einer Versionsnummer des Systems nicht gezielt auf eine Schwachstelle ausgelegt werden kann. Somit müssen mehrere Versionen getestet werden, was wiederum einen hohen zeitlichen Aufwand bedeutet, damit ein Angriff erfolgreich ist.

Bei den Scanergebnissen mit den Modulen “*brute_hosts”, “bing_domain_web”und “google_site_web”* sind teilweise, zu den gefundenen Hosts, die dazugehörigen IP-Adressen gelistet worden. Mit diesen Informationen können unterschiedliche (D)DoS-Attacken durchgeführt werden. Es gibt verschiedene Arten von (D)DoS Attacken. Eine (D)DoS Attacke kann beispielsweise ein ICMP (Internet Control Message Protocol) Angriff [143] sein. Dazu werden massenhaft ICMP-Echo Pakete an das Ziel gesendet, um diesen für den normalen Datenverkehr unzugänglich zu machen. Das Ergebnis eines solchen Angriffes ist es, dass das System für andere Clients nicht mehr verfügbar ist.
Ein weiterer Angriff könnte ein SYN-Angriff sein. Ein SYN (Synchronisation) Paket wird gesendet, um eine Verbindung zu einem Server herzustellen. Somit werden bei diesem Angriff wiederholt SYN-Pakete an das Ziel gesendet, damit kann der Angreifer alle verfügbaren Ports des Ziels überfordern und der Server kann nur auf wenig Datenverkehr reagieren. Somit kann dieser Server keine weiteren Anfragen von legitimen Quellen annehmen, da bereits alle verfügbaren Ressourcen durch die Attacke belegt sind. Bei diesem Angriff kommt meist der Service am System zum Stillstand oder es kommt zu erheblichen Verzögerungen oder Ausfällen.
Ebenso gibt es Amplification Attacks [144] (Verstärkungsangriffe). Eine Liste an IP-Adressen von einem Ziel-Unternehmen kann dazu genutzt werden, dass damit ein Angreifer diese IP-Adressen verwenden kann, um im Namen des Ziel-Unternehmens Anfragen zu tätigen. Die Verwendung von fremden IP-Adressen wird auch als “IP-Spoofing" verstanden, das heißt, dass sich ein Angreifer als das zu attackierende Ziel-Unternehmen ausgibt. Mit der IP-Adresse des Opfers können somit Anfragen an bestimmte Service im Internet geschickt werden. Anschließend wird versucht, dass dieser Service eine Menge an Daten zurücksendet. Da die IP-Adresse von dem Opfer für diese Anfragen verwendet wurde, werden die Antworten an diese IP-Adresse auch zurückgeschickt.
Hier wird erhofft, dass große Mengen an Daten zurückgesendet werden an den Zielserver des Opfers, damit dieser keine weiteren Anfragen verarbeiten kann. [145] [146]

Das Ziel in allen Fällen einer (D)DoS-Attacke ist es, ein Unternehmen und deren Services und Erreichbarkeit zu stören oder zum Erliegen zu bringen. Das wird durch das Senden von großen Mengen an Datenverkehr über die Leitungen des Opfers oder an den Server mit einem bestimmten Service erreicht.

Damit kann beispielsweise der Server in einer Art und Weise überlastet werden, dass dieser keine Ressourcen mehr zur Verfügung hat und die Applikation zum Ziel keine Verbindung mehr aufbauen kann. Dieser Angriff ist auch als “Application Attack” bekannt.
Eine weitere Angriffsart von (D)DoS ist die komplette Internetleitung durch “Bulk”-Traffic (also nutzlosen Traffic) zu belegen, damit die Ressourcen der Leitung so ausgelastet sind, dass keine Verbindung in das Internet von der Organisation mehr möglich ist. Diese (D)DoS Attacke wird auch als “Volumetric Attack” bezeichnet. [147]

Da sich die Angriffsmuster eines (D)DoS-Angriffes möglicherweise verändern, stellt dies eine Herausforderung dar, da somit ein Angriff nicht immer erkannt wird.
Es muss darauf geachtet werden, dass die Netzwerkinfrastruktur auf dem aktuellen Stand gehalten wird, dazu kann beispielsweise das Tool “TheHarvester” mit dem Zusatztool “Shodan” verwendet werden. Somit ist zu sehen, ob kritische Systeme aus dem Internet zugänglich sind und beispielsweise aktualisiert werden müssen. Ebenso können Firewalls, Monitoring-Tools sowie Antiviren-Softwares gegen einen solchen Angriff helfen. [148]
Eine weitere Maßnahme, um einen solchen Angriff zu verhindern, sind (D)DoS-Reaktionspläne. In einem solchen Plan muss eine umfassende Verteidigungsstrategie enthalten sein. Es müssen erste Schritte beschrieben werden, welche unternommen werden müssen, wenn ein solcher Angriff stattfindet. Ebenso muss ein Team dafür vorbereitet sein, indem jedes Mitglied wissen muss, wie es zu reagieren und welche Aufgabe es zu übernehmen hat. [149]

Es sollte im Vorhinein schon versucht werden, dass ein (D)DoS Angriff bereits bei einem ISP (Internet Service Provider) abgefangen wird. Somit kann ein Angreifer nicht das Unternehmensnetzwerk belasten. [150]

Die TIP (Threat Intelligence Plattformen) können gegen (D)DoS-Angriffe nur teilweise genutzt werden. Es muss hier beachtet werden, dass die Tools gegen die bereits signierten und heruntergeladenen Angriffe eine Hilfe darstellen. Neue Angriffe haben eine neue Signatur, womit die meisten Angriffe nicht erkannt werden können. Somit besteht eine Möglichkeit, dass TIP gegen (D)DoS Angriffe helfen, jedoch muss dies mit Bedacht verwendet werden.

Use Case 2: Phishing

Phishing ist eines der weitverbreitetsten und beliebtesten Angriffsarten. Dieser Angriff stellt eine der gefährlichsten Formen von Internetkriminalität dar, da diese meist von Antivirensoftwares nicht erkannt werden. [151]
Laut Statistik hat in der heutigen Zeit eine Person circa 2 E-Mail-Accounts (eine E-Mail-Adresse ist privat, die zweite ist geschäftlich). Da sich die Kommunikation immer mehr auf diese Technologie verlässt, werden hier auch immer wieder die Methoden von Phishing verändert, um besser auf ein Ziel einzugehen. [152]
Laut dem Bericht von Verizon welcher gratis zum Herunterladen verfügbar ist, wird gesehen, dass fast ein Drittel der Datenschutzverletzungen von Phishing ausgegangen ist. [153]

Auffällig sind die Gemeinsamkeiten von “Maltego”, “TheHarvester”, “Recon-NG” und “Spiderfoot”. Jedes dieser Tools bietet einem Angreifer die Möglichkeit, verschiedene E-Mail-Adressen eines Ziels zu sammeln. Wenn beispielsweise E-Mail-Adressen eines Unternehmens gesammelt werden, können somit Angriffe wie APT (Advanced Persistent Threat) geplant werden. Bei diesem Angriff versucht sich ein Angreifer für längere Zeit in einem Unternehmensnetzwerk aufzuhalten, um sensible Daten zu sammeln. Dafür könnte eine Spear-Phishing Attacke verwendet werden. Dieser Angriff weicht leicht von der Angriffsart “Phishing” ab, welcher in Kapitel 4.8 „*Intelligence Collections und Angriffsarten*“ erklärt wird. Bei Spear-Phishing ist der Angriff speziell auf ein Unternehmen oder eine Person gerichtet und nicht auf die Allgemeinheit.
Um Spam und Phishing-Angriffe auf das Netzwerk zu vermindern, kann eine Filterung von E-Mails durchgeführt werden. Ebenso sollte in regelmäßigen Abständen eine Überprüfung auf mögliche Updates und Schwachstellen in Netzwerken oder Betriebssystemen stattfinden. Weiters kann eine Vorsichtsmaßnahme an die Mitarbeiter ausgesprochen werden, damit diese nicht auf einen Link oder Anhänge von E-Mails klicken. Um ein besseres Verständnis dafür zu bekommen, können auch Schulungen angeboten werden.
Ebenso kann eine Whitelist eingepflegt werden, womit gesteuert werden kann, welche Domains und Anwendungen in einem Netzwerk Zugriff haben dürfen. Wenn somit eine Domain, welche nicht in dieser Liste gespeichert ist, versucht Zugriff auf das Netzwerk zu bekommen, ist dies nicht erlaubt. [154]

Eine weitere Unterstützung gegen Angriffe können hier ebenso die TIP (Thread Intelligence Plattform) sein, diese können in einem Unternehmen als zusätzlicher Schutz dienen.
Im Kapitel 2 „*Background*“ wurden bereits erste Beschreibungen zu den jeweiligen, verfügbaren TIPs gegeben, anschließend wird die TIP “MISP” im Praxistest beschrieben. Die TIPs dienen dazu, um ein Unternehmen gegen Angriffe und Bedrohungen zu schützen, wie beispielsweise gegen eine Phishing Attacke, indem die neuesten Cyber Attack Feeds von der Plattform “MIPS” heruntergeladen werden. Mit der TIP “MISP” wird somit dem Sicherheitsteam die Möglichkeit gegeben, in Echtzeit auf mögliche Bedrohungen oder Angriffe zu reagieren.
Es werden von MISP 40 verschiedene Feed Provider angeboten, welche einer Person einen kostenlosen Austausch von Feeds ermöglichen. Die ersten zwei kostenlosen Feeds Provider “CIRCL” und “Botvrij.eu” sind in Abbildung 54 „*MISP Feeds*“ ersichtlich. [21]
Es wird von dem Tool eine Weboberfläche angeboten, womit ermöglicht wird, übersichtlich die verschiedenen Events zu überprüfen und zu analysieren. Auf dieser Weboberfläche kann die Administration sowie die Verwaltung der Events durchgeführt werden. Es wird mit der Webansicht auch ermöglicht neue auftretende Bedrohungen zu sehen und diese zu “Editieren”, siehe Abbildung 55 „*MISP Events*“, dies wurde mit einem (1) gekennzeichnet. In Abbildung 56 „*MISP Edit Event*“ ist anschließend zu sehen, wie die Weboberfläche für das “Editieren” aussieht.
Dadurch wird einem IT-Mitarbeiter die Möglichkeit gegeben, direkt auf der Plattform, stichprobenmäßig Untersuchungen der neuen Events durchzuführen und diese auch zu “Editieren”

und mit dem “Threat Level” (Low, Medium, High, Undefined) neu zu evaluieren, siehe Abbildung 57 „*MISP Threat Level Einstellungen*“. Durch die Tools wird die Verarbeitung der Bedrohungsdaten erleichtert, dadurch müssen nur stichprobenmäßige Kontrollen durchgeführt werden, um mögliche falsche Bedrohungsinformationen zu löschen.

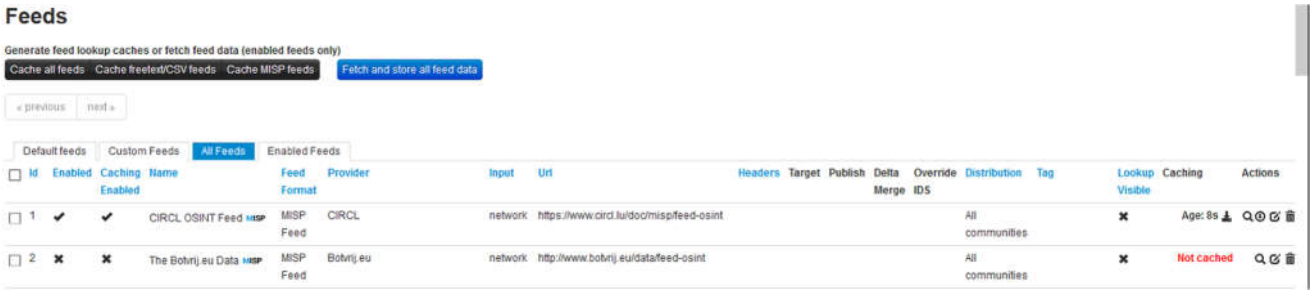


Abbildung 54 MISP Feeds

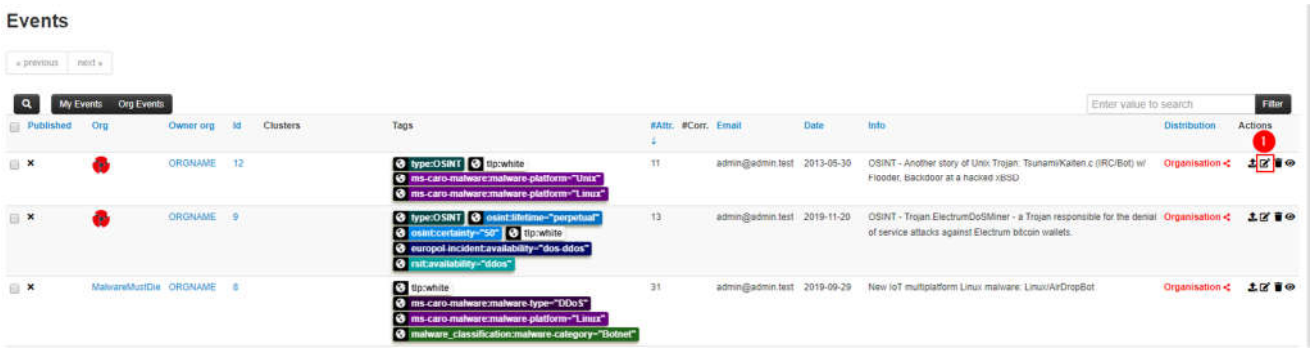


Abbildung 55 MISP Events

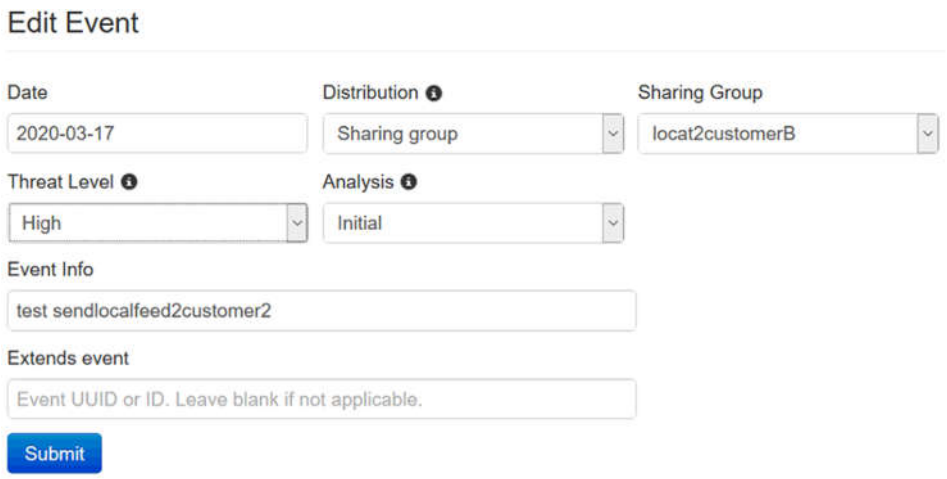


Abbildung 56 MISP Edit Event

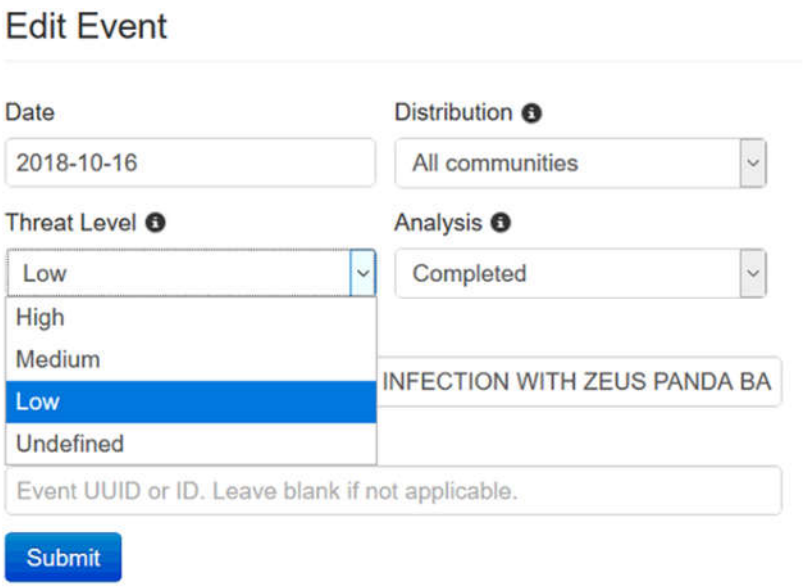


Abbildung 57 MISP Threat Level Einstellungen

Ebenso werden mit dem Tool auf dem "Dashboard" sehr übersichtlich die aktualisierten und veröffentlichten Events angezeigt, siehe Abbildung 58 „*MISP Dashboard*".

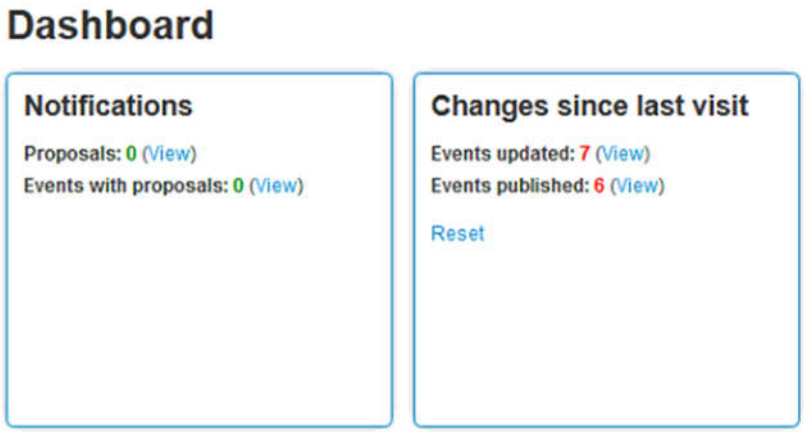


Abbildung 58 MISP Dashboard

Mit dem Tool wird die Möglichkeit gegeben, Bedrohungsinformationen rasch intern zwischen Abteilungen aber auch zwischen Kunden auszutauschen. Dazu muss zuerst eine "Sharing Group" erstellt werden, siehe 60 „*MISP Sharing Group*". Ebenso ist das Editieren der jeweiligen Sharing Groups möglich, siehe Abbildung 59 „*MISP Edit Sharing Group*"

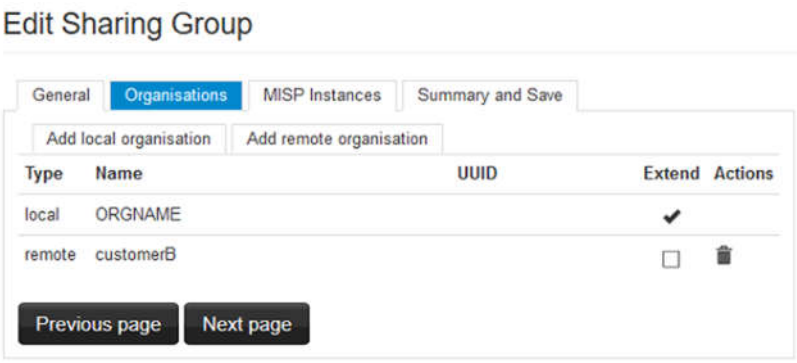


Abbildung 59 MISP Edit Sharing Group

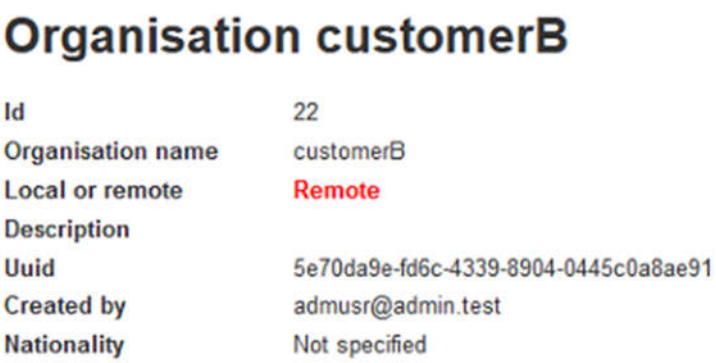


Abbildung 60 MISP Sharing Group

Nachdem die “Sharing Group” erstellt worden ist, muss die Gegenstelle eingerichtet werden, damit Events mit einem Kunden geteilt werden können, siehe Abbildung 61 „*MISP Add Server*“. In Abbildung 62 „*MISP Server*“ ist anschließend zu sehen, dass der zuvor erstellte Server auf “Run” gesetzt ist und somit aktiv ist. Abbildung 63 „*MISP Event mit Kunden teilen*“ zeigt, wie ein Event anschließend mit dem Kunden geteilt werden kann.

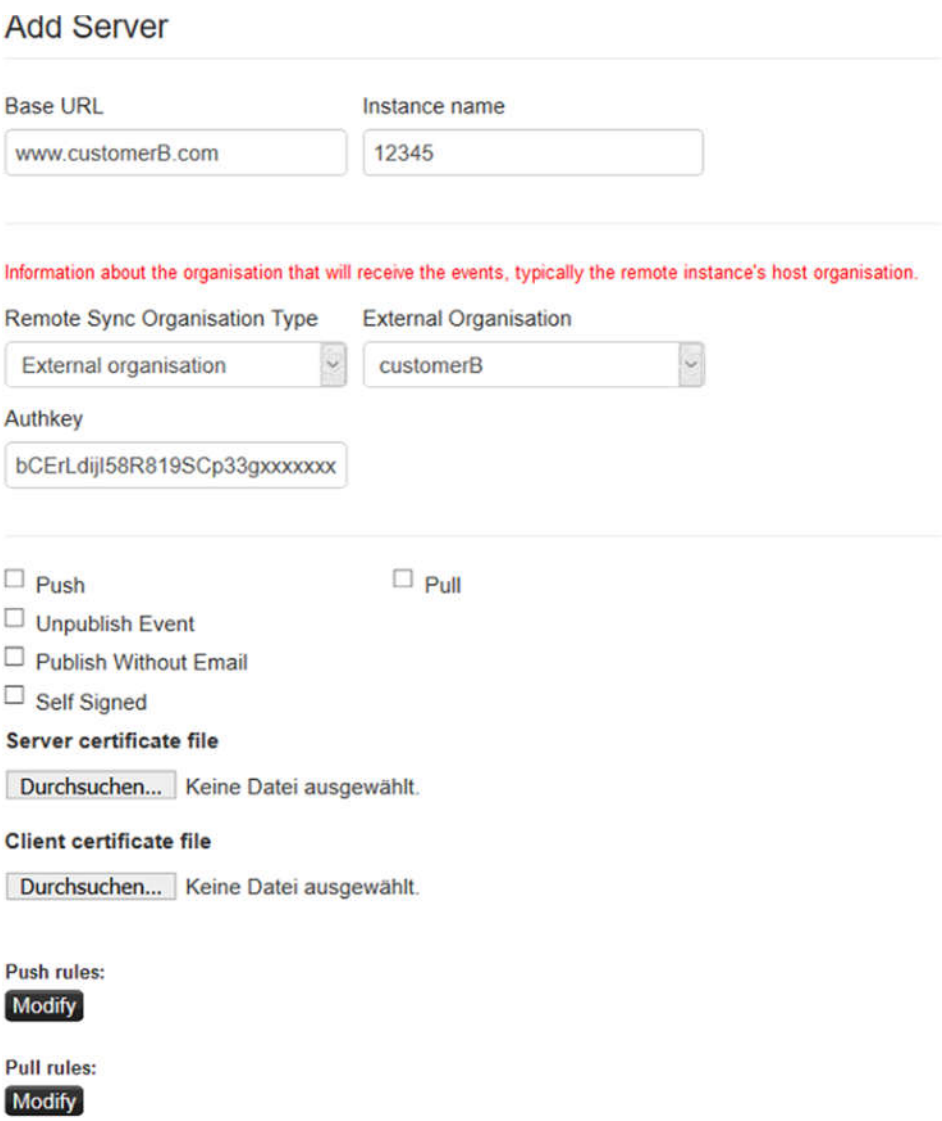


Abbildung 61 MISP Add Server

Abbildung 62 MISP Server

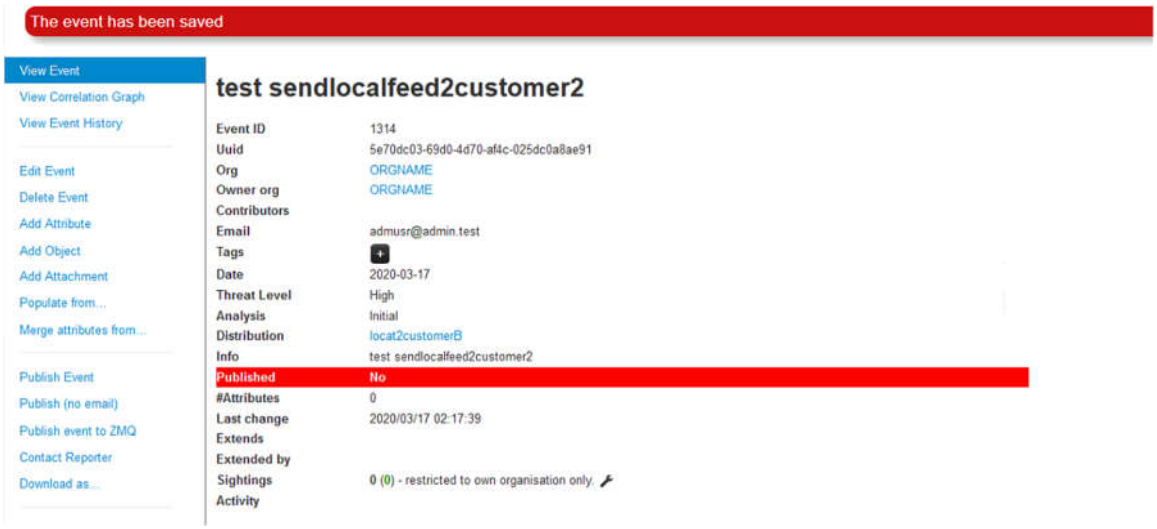


Abbildung 63 MISP Event mit Kunden teilen

Use Case 3: Social Media Plattform / Social Engineering - Was posten Mitarbeiter in den Sozialen-Medien

In der heutigen Zeit werden Social Media Plattformen immer populärer und stetig erhöht sich die Anzahl der Mitglieder auf den Plattformen. [155]
Dadurch steigt auch das potenzielle Risiko, dass von einem Mitarbeiter oder einer Person mögliche firmeninterne oder persönliche Informationen veröffentlicht werden. Es ist oft nicht bekannt, welche weiteren Personen diesen Post/Tweet sehen können, da es an der Kenntnis der benötigten Privacy-Einstellungen fehlt, damit diese Informationen nicht für jeden sichtbar sind. Oft besteht bei unerfahrenen Benutzern die Angst, dass sie sich durch Privacy-Einstellungen das Social Media Profil verstellen. [156]

In dieser Arbeit wurden verschiedene Tools verwendet, mit welchen es möglich ist, Informationen von Social Media Plattformen zu beziehen, welche anschließend beschrieben werden.
Es ist mit dem Tool “Maltego” möglich, über Social Media Plattformen Informationen über das Ziel zu bekommen.
Damit ein Scan zu einer Person durchgeführt werden kann, werden keine weiteren Informationen benötigt außer lediglich der Name einer Person, welcher in der Scan-Funktion “Person” eingegeben werden muss. Ein Beispiel wie ein solcher Scan aussehen kann, wird in Abbildung 4 „*Maltego Twitter Scan*“ gezeigt.
Nach dem Scan wird das Ergebnis sehr detailliert wiedergegeben, da es grafisch aufbereitet und Verbindungen mit dem jeweiligen User und dessen geposteten Tweets aufgebaut werden. Ein Unternehmen kann damit beispielsweise feststellen, ob ein Mitarbeiter firmeninterne Informationen nach draußen weitergegeben hat.

Ein weiteres Tool, um auf Social Media Plattformen Informationen über ein Ziel zu sammeln ist “Spiderfoot”. Hier wird ebenso wie im Tool “Maltego” lediglich der Name einer Person benötigt, um einen Scan durchzuführen. Bei diesem Tool wird lediglich angezeigt, auf welchen Plattformen eine Person einen Account angelegt hat und keine weiteren Informationen zu Tweets, Freunden oder Followern gegeben. Es werden ebenso keine Tweets gespeichert oder wiedergegeben, somit kann keine Analyse der preisgegebenen Informationen durchgeführt werden. Die Ergebnisse dienen daher lediglich dazu, um zu sehen, auf welchen Plattformen ein Ziel vertreten ist.

Die zwei Tools “Tinfoleak” und “Twitter-Script” sind ausschließlich für das Sammeln von Twitter Informationen geeignet.
Mit dem Tool “Tinfoleak” können verschiedene Informationen über ein Ziel auf dessen Twitter Seite gesammelt werden, siehe Tabelle 10 „Welche Informationen können mit dem Tool gesammelt werden“. Um Informationen über ein Ziel zu finden und den Scan durchführen zu können, wird hier lediglich der Username beispielsweise @fh_stpoelten benötigt. Das Ergebnis des Scans ist durch die genaue Speicherung der Tweets, Follower und Freunde von einem Ziel für ein Unternehmen von großem Nutzen. Damit können Untersuchungen durchgeführt werden, wie beispielsweise, welche Informationen in einem Tweet über das Unternehmen von einem Mitarbeiter preisgegeben worden sind. Ebenso können die geteilten Fotos eines Ziels angesehen werden. Diese Fotos werden im Gegensatz zu dem Tool “Twitter-Script” nur im Bericht angezeigt und nicht heruntergeladen. Dennoch können Überprüfungen zu den geposteten Fotos stattfinden, da möglicherweise firmeninterne Informationen auf Bildern ersichtlich sind (z.B.: Flipcharts oder auf dem Bild eines Arbeitsplatzes ein Passwort) und somit preisgegeben werden können.

Das Tool “Twitter-Script” ist ebenso ausschließlich für das Sammeln von Twitter Daten über ein Ziel geeignet. Es können hier ebenso verschiedene Daten über einen Twitter User gesammelt werden, Tabelle 10 „Welche Informationen können mit dem Tool gesammelt werden“. Es wird bei diesem Tool

ebenso lediglich der Twitter Username eines Ziels benötigt, um einen Scan zu starten. Bei diesem Tool werden alle gefundenen Informationen wie Follower, Freunde und Tweets in einem Ordner lokal abgespeichert. Ebenso werden die gesamten Bilder von einem User abgespeichert. Dadurch wird einem Unternehmen oder einer Person die Möglichkeit gegeben, alle geposteten Tweets eines Mitarbeiters auf firmeninterne Daten zu überprüfen. Aber auch die gespeicherten Bilder können auf mögliche Freigabe von Firmendaten kontrolliert werden.

Die oben beschriebenen Tools können ebenso von einem Unternehmen für andere Zwecke verwendet werden. Es können beispielsweise Personen vor einem Bewerbungsgespräch überprüft werden, damit wird ein Background-Check der Person ermöglicht. Aber auch bereits eingestellte Mitarbeiter/innen können von dem Unternehmen überprüft werden. Jedoch können auch Angreifer/innen geteilte firmeninterne oder persönliche Informationen von Mitarbeitern verwenden und gegen ein Unternehmen oder eine Person richten.

Es wird ebenso auf Plattformen wie GitHub [42] produktiver Code eines Unternehmens als Projekt gespeichert. Dieses Projekt wird auf einem Repository gespeichert, auf dessen anschließend mit einem URL (Uniform Resource Locator) zugegriffen werden kann. GitHub ist ein Versionskontrollsystem, in diesem können Entwickler zusammen an einem Code arbeiten und diesen überarbeiteten Code anschließend wieder für die weiteren Mitglieder zur Verfügung stellen. Es ist aber auch möglich, dass Personen, welche nichts mit der Entwicklung des Projekts zu tun haben, diesen Code herunterladen können. Wenn daher unbedacht oder aus Versehen vertrauliche Informationen preisgegeben werden, können diese von Personen eingesehen werden, welche in dem Projekt nicht involviert sind. Damit wird einem/einer Angreifer/in die Möglichkeit geboten, diese Informationen zu speichern und einen Angriff auf das Unternehmen vorzubereiten. Um dies zu verhindern gibt es verschiedene Tools, welche anschließend namentlich erwähnt werden, um zu überprüfen, ob das Repository sensible Informationen wie Kennwort, Benutzername oder E-Mail-Adressen enthält. Dazu können die Tools ”Gittyleaks”, ”Git Secrets” oder ”Repo Superviso” verwendet werden, diese werden auf der Seite von Geekflare [157] genauer beschrieben.
Laut dem Bericht von “Nakedsecurity” [158] sind ebenso Verschlüsselungsschlüssel auf GitHub enthalten. Es wird beschrieben, dass über 100.000 Code-Repository Zugriffsschlüssel enthalten sind, womit ein/e Angreifer/in einen privilegierten Zugriff auf das Repository oder auf diverse Onlinedienste erhalten.

Eine weitere mögliche Plattform hierbei wäre Stack Overflow. [41] Hier können beispielsweise von Mitarbeitern Code Snippets (Codeausschnitte von einem Programm) hochgeladen werden. Zu diesem Code Snippets können anschließend von der Community Verbesserungsvorschläge genannt werden. Diese Ausschnitte eines Codes können firmeninterne Informationen, oder geheime Daten (wie beispielsweise Passwörter) enthalten, weshalb diese Plattformen auch für Angreifer/innen interessant sind, da sie damit mögliche Systeme und Probleme eines Unternehmens feststellen können. Daher sollte bevor ein Code hochgeladen wird, dieser so bereinigt werden, dass keine Informationen über das Unternehmen oder eine Person enthalten sind. Ein Unternehmen kann beispielsweise Untersuchungen durchführen, ob wichtige und kritische Systeme oder IP-Adressen auf diesen Plattformen vorhanden sind. Es ist bei Stack Overflow oft schwer eine Frage zu löschen. Wenn jemand auf diese Frage geantwortet hat, dann ist diese Frage für die Community als wichtig eingestuft und kann nicht gelöscht werden. Wenn diese Frage dennoch gelöscht werden soll, muss die Frage zuvor von einem Moderator geprüft werden. [159]

GitHub und Stack Overflow sind nicht die einzigen Plattformen, welche kritische Informationen enthalten. Es werden ebenso auch auf Social Media Plattformen wie beispielsweise Twitter, firmeninterne Informationen preisgegeben. [160] [161]

Die Studie von “PewResearchCenter” [15] zeigt, dass Mitarbeiter/innen oft verschiedene Informationen oder Fragen, welche firmeninterne Inhalte aufweisen, auf Social Media Plattformen preisgeben. Beispielsweise zeigt der Report, dass auf verschiedenen Plattformen über firmeninterne Probleme gefragt wird oder mit externen Personen über die internen Probleme geredet wird. Aber auch die persönlichen Ansichten von Mitarbeitern zu einem Thema können einen schlechten Ruf auf das Unternehmen werfen, da die Personen leicht in Verbindung mit dem Unternehmen gebracht werden können. Dies ist für eine Firma ein großes Risiko, da diese Informationen dadurch öffentlich zugänglich sind. [160]
Ein weiteres Problem stellt das Vertrauen der Freunde dar, welchen gefolgt wird. Dementsprechend wird oft nicht überlegt, wenn dieser Freund einen neuen Post mit einem Link erstellt. Doch hier ist die Gefahr, dieser Link kann ein Malware-Risiko mit sich bringen und für das Unternehmen verheerende Auswirkungen haben. Um dies zu verhindern, kann beispielsweise eine Social Media Policy eingeführt werden, welche eine Regulierung für die Mitarbeiter festlegt. Auf diese Richtlinie muss bei der Verwendung von Social Media Plattformen in einem Unternehmen hingewiesen werden.

Vergleich der Tools:
In diesem Abschnitt wird auf die Eigenschaften und Fähigkeiten der Tools eingegangen. Damit kann ein kurzer Überblick über die jeweiligen Tools gegeben werden und dessen Auffälligkeiten beschrieben werden.

Maltego:
Das Tool “Maltego” war von den Tests eines der größeren Tools, welches auch in dem Bereich von Open Source Intelligence sehr bekannt ist. Das Tool stellt verschiedene Funktionen wie das Scannen nach “Domain”, “Webseite” oder “IP-Adressen” bereit. Weiters werden dessen bereitgestellte Funktionen regelmäßigen Updates unterzogen. Es ist möglich verschiedene Informationen wie beispielsweise “DNS”, “IP-Adressen” und “E-Mail-Adressen" zu sammeln, siehe Tabelle 10 „*Welche Informationen können mit dem Tool gesammelt werden*“.
Mit dem Tool kann weiters auch ein Twitter User und dessen Informationen sowie deren Follower und Tweets überprüft und dessen Informationen gespeichert werden.
Nachdem ein Scan durchgeführt worden ist, werden die Ergebnisse grafisch anhand einer Punkte-Grafik angezeigt, dies ist in Abbildung 6 „*Maltego Big Picture*“ zu sehen. Wenn anschließend ein neuer Scan durchgeführt wird, werden die neuen Informationen automatisch mit den bereits zuvor gefundenen Informationen, mit dem dazugehörigen Punkt auf der Grafik (Knoten) verbunden.

Mit dem Tool wird einem Unternehmen die Möglichkeit geboten, eine automatisierte grafische Aufbereitung der Ergebnisse nach einem Scan zu bekommen. Somit können diese Informationen von Mitarbeitern in einem Unternehmen verwendet werden, um mögliche kritische Informationen zu finden und diese zu beheben. Es kann ein Domain Scan durchgeführt werden, damit können verschiedene DNS-Einträge gefunden werden, womit Informationen über die eingesetzten Systeme in einem Unternehmen gewonnen werden können. Es werden jedoch keine Versionsnummern der Systeme angeführt, dafür müsste zusätzlich das Tool Shodan verwendet werden.
Mit dem Tool wird ebenso ermöglicht, dass verschiedene E-Mail-Adressen gefunden werden können. Wie in Abbildung 9 „*Maltego Personen/E-Mail-Adresse Scan*“ zu sehen ist, können von einer E-Mail-Adresse mehrere berufliche E-Mail-Adressen zu einer Person gefunden werden, somit ist der berufliche Werdegang überprüfbar.
Hingegen muss darauf aufmerksam gemacht werden, dass im Gegensatz zu den weiteren analysierten Tools, bei diesem Tool weniger DNS-Einträge gefunden worden sind.
Durch die grafische Aufbereitung der Ergebnisse und der automatischen Verknüpfung neuer Ergebnisse, ist dieses Tool für kleine aber auch für große Unternehmen zu verwenden. Weiters besteht die Möglichkeit die Grafik und die Punkte selber zu adaptieren. Das Tool befähigt weiters, dass Informationen über Social Media Profile gesammelt werden können. Somit können Mitarbeiter überprüft werden, ob von diesen möglicherweise firmeninterne Daten veröffentlicht worden sind. Aber

auch Bewerber können vor einem Bewerbungsgespräch überprüft werden und einem Background Check unterzogen werden. Anzumerken ist, dass für detailliertere Scans ein API-Key benötigt wird.

TheHarvester:
Das Tool "TheHarvester" (Ernten) ist ein Tool, welches seinem Namen gerecht wird. Das Tool unterstützt Person in der Phase des Information Gathering, da Informationen wie offene Ports, E-Mail-Adressen und IP-Adressen gesammelt werden können, siehe Tabelle 10 „*Welche Informationen können mit dem Tool gesammelt werden*". Die Ergebnisse eines Scans können von einer Person durch das vom Tool automatisch erstellten "html"-File in einem Browser analysiert werden. Eine detailliertere Veranschaulichung der Darstellung von Ergebnissen, sowie eine Beschreibung ist in Kapitel 6.2.4 „*Praktischer Test*" zu sehen.

Wie bereits erwähnt ist das Tool vor allem darauf ausgelegt, E-Mail-Adressen sowie Hosts und IP-Adressen zu sammeln. Mit dem Hostnamen können mögliche Rückschlüsse über die verwendeten Systeme in einem Unternehmen gezogen werden. Da jedoch keine Versionsnummer angeführt ist, können keine Angriffe direkt auf die Version durchgeführt werden. Daher besteht nur ein "potenzielles" Risiko, da nur mögliche Schwachstellen gesucht werden können, welche nicht direkt auf die Version ausgelegt sind. Ein Auszug von gefundenen Hosts wird in Abbildung 64 „*TheHarvester gefundene Hosts mit IP*" gezeigt.

Weiters kann mit dem Tool auch ein Scan auf offene Ports durchgeführt werden, dafür wird jedoch der API-Key von Shodan benötigt. Während dem Testen der Scans mit „Shodan" und „TheHarvester" wurde ersichtlich, dass von "TheHarvester" wichtige Informationen wie beispielsweise die Versionsnummern eines Systems, nicht in dem Scan-Bericht angeführt werden. Daher wurde auch bei Kapitel 7 „*OSINT Use Case*" auf dies hingewiesen, dass trotz dem Scan in „TheHarvester", „Shodan" als zusätzliche Kontrolle für weitere Informationen verwendet werden soll. In Abbildung 65 „*Shodan Portscan Ergebnis*" ist der „Shodan" Auszug zu sehen, welcher eine Versionsnummer enthält. Diese Information der Apache-Versionsnummer ist hingegen bei dem Scan mit „TheHarvester" zu dieser IP-Adresse nicht ersichtlich, welches in der Abbildung 66 „*TheHarvester Scanergebnis ohne Versionsnummer*" zu sehen ist.

Das Tool unterstützt ein Unternehmen, da mit dem Tool die gefundenen Hosts überprüft werden ob eine mögliche Schwachstelle besteht und diese einem Update unterzogen werden müssen. Weiters können wie zuvor beschrieben offene Ports gefunden werden. Hier sollte ein Unternehmen darauf achten, ob es einen legitimen Grund gibt, dass ein Port offen ist oder dieser unverzüglich geschlossen werden muss, da ein Risiko besteht. Wie zuvor erwähnt sollte, zu dem durchgeführten Scan auch „Shodan" zur Hilfe genommen werden.

```
Hosts found:
    jabber.fhstp.ac.at:91.219.68.14
    mahara.fhstp.ac.at:91.219.69.15
    mahara.mdh.fhstp.ac.at:91.219.68.90
    skype.fhstp.ac.at:91.219.69.12
    wordpress.fhstp.ac.at:91.219.69.17
    nextcloud.nwt.fhstp.ac.at:91.219.68.61
```

Abbildung 64 TheHarvester gefundene Hosts mit IP

Abbildung 65 Shodan Portscan Ergebnis

91.219.69.53	bilddb.fhstp.ac.at	Fachhochschule St. Poelten GmbH	Apache httpd:443, Apache httpd:80	Gravatar

Abbildung 66 TheHarvester Scanergebnis ohne Versionsnummer

Recon-NG:
Das Tool "Recon-NG" ist wie der Name schon sagt dafür ausgelegt, Personen in der "Reconnaissance" Phase zu unterstützen. Mit diesem Tool können Personen wichtige Informationen finden wie beispielsweise IP-Adressen, Hosts oder E-Mail-Adressen, siehe Tabelle 10 „*Welche Informationen können mit dem Tool gesammelt werden*". Die Informationen wie beispielsweise Hosts, geben sehr detaillierte Informationen über ein Ziel preis.

Das Tool sticht mit der Übersichtlichkeit und Strukturierung hervor. Da für jeden Scan ein eigener "Workspace" angelegt werden kann, was in Kapitel 6.3.4 „*Praktischer Test*" erklärt ist, vermischen sich dadurch nicht die gefundenen Ergebnisse eines Scans. Ein weiterer positiver Punkt ist die Menge von 78 Aufklärungsmodulen, welche von dem Tool angeboten werden. Anzumerken ist, dass für detailliertere Scans und einige Informationen ein API-Key benötigt wird. Wie zuvor erwähnt ist das Tool auf das Finden von Hosts, IP-Adressen sowie E-Mail-Adressen ausgelegt.

Mit dem Tool wird einem Unternehmen die Möglichkeit geboten, die gefundenen Informationen in dem jeweiligen dafür erstellten Workspace zu analysieren. Durch die Informationen wie Hostname und IP können beispielsweise die verwendeten Systeme in einem Unternehmen herausgefunden werden. Ein IT-Mitarbeiter kann diese Informationen für eine interne Überprüfung verwenden, um zu prüfen, ob ein gelistetes System eine Aktualisierung benötigt. Jedoch muss angemerkt werden, dass nicht die Versionsnummern der verwendeten Systeme in dem Scan-Bericht angezeigt werden. Daher können nur mögliche Schwachstellen gesucht werden, welche nicht direkt auf die Version ausgelegt sind, dies wird in Abbildung 67 „*Recon-NG Scanergebnis von Hosts und IP ohne Versionsnummern*" gezeigt. Um genaue Informationen über die Hosts und dessen Systemversion zu bekommen, kann hier ebenso wie beim Tool „TheHarvester", „Shodan" verwendet werden.

rowid	host	ip_address	region	country	latitude	longitude	module
8	mahara.fhstp.ac.at						bing_domain_web
51	phaidra-fedora.fhstp.ac.at						bing_domain_web
75	mahara.mdh.fhstp.ac.at						bing_domain_web
123	wordpress.fhstp.ac.at	91.219.69.17					brute_hosts
162	skype.fhstp.ac.at	91.219.69.13					brute_hosts
163	skype.fhstp.ac.at	91.219.69.12					brute_hosts
168	samba.fhstp.ac.at	91.219.69.17					brute_hosts
207	jabber.fhstp.ac.at	91.219.68.14					brute_hosts
276	WordPress.fhstp.ac.at	91.219.69.17					brute_hosts
348	git.nwt.fhstp.ac.at						google_site_web

Abbildung 67 Recon-NG Scanergebnis von Hosts und IP ohne Versionsnummern

Spiderfoot:
Das Tool “Spiderfoot” ist so wie die zuvor beschriebenen Tools für das Sammeln von Informationen zuständig, um Personen in der Information Gathering Phase zu unterstützen und verschiedene Informationen über ein Ziel zu sammeln. Mit “Spiderfoot” wird es ermöglicht, mit dem Namen eines Ziels, zu überprüfen, auf welchen Social Media Plattformen ein Ziel einen Account besitzt.
Von dem Tool werden lediglich die Plattformen angezeigt und keine weiteren Informationen, wie die Tweets oder Posts von einem User.
Einen wesentlich größeren Bereich deckt das Tool mit der Suche nach Informationen über Unternehmen ab. Es können mit einem Scan Informationen wie beispielsweise IP-Adressen, Hosts, offene Ports oder E-Mail-Adressen gefunden werden. In den Abbildungen 36 „*Spiderfoot Gesamtergebnis 1*“ bis Abbildung 38 „*Spiderfoot Gesamtergebnis 3*“ ist ersichtlich, wie breit der Scan des Tools ausgelegt ist und welche Informationen gefunden werden können. Anzumerken ist, dass für detailliertere Scans und einige Informationen ein API-Key benötigt wird.

Das Tool ist darauf ausgelegt E-Mail-Adressen, Hosts und IP-Adressen sowie offene Ports zu sammeln. Jedoch können mit dem Tool noch mehr Informationen wie beispielsweise “Hacked E-Mail Adress” oder “Physical Location” und “Accounts on External Site” gesammelt werden, während dies mit den anderen Tools nicht möglich ist. Beispielsweise werden bei dem “Accounts on External Site” verschiedene Webseiten überprüft, auf welchen die gefundenen Namen von Personen vorkommen.
Ein Vorteil von diesem Tool ist, dass falsche Informationen direkt in dem Tool entfernt werden können. Dies unterscheidet es wesentlich von den weitern analysierten Tools, siehe Abbildung 35 „*Spiderfoot False Positive Flag*“.

Mit dem Tool „Spiderfoot“ wird einem Unternehmen die Möglichkeit gegeben, die gefundenen Informationen auf der Weboberfläche des Tools zu analysieren. Es können verschiedene Informationen abgerufen werden, wie beispielsweise ist durch die Scan Funktion “Hacked Email Adress” ersichtlich, ob eine E-Mail-Adresse angreifbar ist. Wie bei den zuvor beschriebenen Tools können hier ebenfalls die Hosts und dessen IP-Adressen sowie E-Mail-Adressen über das Ziel gesammelt werden. Es können ebenso Informationen über die angelegten Profile auf Social Media Plattformen einer Person gefunden werden. Mit diesen Informationen können IT-Mitarbeiter beispielsweise weitere Tools verwenden, um einen Mitarbeiter auf den Social Media Plattformen im Detail zu analysieren, da mit dem Tool “Spiderfoot” keine geposteten Tweets oder Posts ersichtlich sind.
Ebenso ist es mit “Spiderfoot” möglich, mit den gefundenen Hosts, Informationen über die verwendeten Systeme in dem Unternehmen heraus zu finden. Jedoch wird hier ebenso keine Versionsnummer angegeben, womit es nur ein “potentielles” Risiko darstellt. Weiters ermöglicht das Tool das Sammeln von offenen Ports, dies ist in Abbildung 39 „*Spiderfoot offene Ports*“ zu sehen. Hier sollten die IT-Mitarbeiter/innen überprüfen, ob es einen legitimen Grund gibt, weshalb ein Port geöffnet ist, oder ob dieser geschlossen werden muss, da ein Risiko dadurch besteht. Für eine genaue Analyse der Port Informationen sollte das Tool „Shodan“ als Unterstützung verwendet werden. Hier werden ebenso die Versionsnummern der Systeme angezeigt.

Tinfoleak:
Das Tool “Tinfoleak” ist dazu entwickelt worden, um Informationen eines Twitter Users zu sammeln. Um einen Scan durchzuführen, wird lediglich der Username, beispielsweise “@fh_stpoelten”, benötigt. Nach dem Scan wird einem Unternehmen ermöglicht, die Ergebnisse durch das automatisch gespeicherte “html”-File im Browser zu analysieren.

Das Tool ist für ein Unternehmen ein einfaches, aber effizientes Tool, da es beim Auswerten der gefundenen Informationen selbstständig einige Analysen durchführt. Es kann beispielsweise herausgefunden werden, welche Endgeräte verwendet worden sind für einen Post/Tweet. Das Tool speichert ebenso Tweets ab, welche von einem Unternehmen oder einer Person auf möglicherweise firmeninterne Informationen überprüft werden können. Weiters werden in dem erstellten “html”-Bericht

gepostete Bilder eines Users angezeigt. Mit den Bildern können ebenso die Geolocations angezeigt werden, welche in einem Bild hinterlegt sind.
Dafür muss jedoch die Einstellung „Standort“ [162] in Twitter aktiv sein (diese ist standardmäßig inaktiv), damit diese Information hinzugefügt wird und analysierbar ist.
Das Tool ist weiters darauf ausgelegt, dass verschiedene Analysen wie “meistverwendete Wörter” oder “Top Hashtags” gesammelt werden können. Das Tool benötigt keinen Twitter API-Key, um die Informationen eines Users zu speichern.

Twitter-Script/Twitter-Exporter:
Das Tool “Twitter Script/Twitter-Exporter” ist dafür ausgelegt, dass Informationen über einen Twitter User auf der Twitter Seite gesammelt werden können. Das Scannen mit dem Tool ist ein einfaches Vorgehen, da lediglich der Username eines Twitter Users benötigt wird. Nach dem Scan werden von dem Tool automatisch “csv”-Files erstellt, mit den Followers und den Freunden sowie mit den gesamten Tweets. Weiters wird ein eigener “photos”-Ordner erstellt mit den gesamten Bildern eines Twitter Users, welche von dem Tool automatisch runtergeladen werden, welches in Abbildung 53 „Twitter-Script erstellter Ordner mit “ zu sehen.

Twitter Script ist für ein Unternehmen ein einfaches Tool, da für einen Scan keine weiteren Schritte benötigt werden, lediglich der Username eines Twitter Users. Das Auffällige an dem Tool ist, dass die gesamten Informationen wie Followers, Freunde und Tweets in einem analysierbaren csv-Format abgespeichert werden. Ebenso werden die Bilder automatisch in einem Ordner abgespeichert.
Es ist mit dem Tool möglich, sowohl die gesamten Tweets eines Mitarbeiters in dem dafür erstellten „csv“-File, als auch alle Followers und Freunde von einem Twitter User in den dafür je erstellten csv-Files zu analysieren. Mit diesen Informationen können Unternehmen eine/n Mitarbeiter/in überprüfen, ob diese/r firmeninternen Daten auf Social Media Plattformen verteilt. Ebenso können die geposteten Bilder eines Users überprüft werden und ob diese Bilder firmeninterne Informationen enthalten, wie beispielsweise von einem Flipchart oder einem Arbeitsplatz. Für die Durchführung der Scanvorgänge wird kein API-Key benötigt.

Nutzen der Arbeit
Durch die Gegenüberstellung der jeweiligen Tools, welche in Tabelle 11 „*Ergebnisse der Tool-Evaluierung 1*“ bis 15 „*Ergebnisse der Tool-Evaluierung 5*“ ersichtlich sind, soll einem Unternehmen die jeweiligen Funktionalitäten eines Tools aufgezeigt werden. Weiters wird eine Beschreibung zu den jeweiligen Tools gegeben, welche in Kapitel 6 „*Evaluierung von den Tools*“ durchgeführt wurde.

Durch die Gegenüberstellung und Beschreibung der Tools können Unternehmen ein geeignetes Tool auswählen, welches ihren Anforderungen entspricht. Anforderungen können beispielsweise die jeweiligen Informationen sein, die mit dem Tool gefunden werden können, aber auch das Betriebssystem auf welchem die Tools verfügbar sind. Weiters können Kriterien wie Import und Export-Formate als Anforderung gelten, da diese Ergebnisse möglicherweise in weiteren Programmen verarbeitet werden. Diese Arbeit soll KMUs unterstützen, aber auch IT-Mitarbeiter, welche sich in diesem Bereich mehr Wissen aneignen möchten. Es soll auf die Risiken aufmerksam gemacht werden, da diese Tools ebenso von Angreifern verwendet werden können. Diese Informationen, welche im Internet verfügbar sind, können daher auch gegen ein Unternehmen gerichtet werden.

Weiters soll diese Arbeit dazu dienen, dass Unternehmen dadurch präventive Schutzmaßnahmen bilden können, indem verschiedene Scans durchgeführt wurden, welche potenzielle Schwachstellen aufzeigen können. Durch die Beschreibung der einzelnen Tools wird ebenso der Aufwand abgenommen ein Tool von Anfang an neu kennenzulernen, was mit viel Zeit verbunden ist. Es soll somit ein Unternehmen entlastet werden und für Zeitersparnis sorgen.

Weiters soll durch die Beschreibung der TI-Plattformen gezeigt werden, dass es eine große Unterstützung gibt, damit ein Unternehmen auf mögliche Bedrohungen in Echtzeit reagieren kann und sich ebenso mit weitern Abteilungen und Unternehmen austauschen kann.

Ein weiterer Aspekt dieser Arbeit ist, dass die Gefahr aufgezeigt wird, dass ein/e Mitarbeiter/in firmeninterne Informationen auf Plattformen, wie GitHub, Stackover Flow oder Social Media Netzwerken preisgeben kann. Eine Sammlung sowie die Speicherung der Informationen ist ein einfacher Prozess, dies ist in Use Case 2 hervorgehoben.

Informationskriege/Desinformation/Fake-News:
Das Phänomen von “Information Warfare” ist schon sehr lange bekannt. Durch den rasanten Anstieg an Informationen, welche frei zugänglich sind, ist dieses Thema ein immer wichtiger werdendes. Personen können durch einen “Informationskrieg” und “Fake-News” und den damit entstehenden “falschen Nachrichten” so manipuliert werden, dass sie den richtigen Nachrichten nicht mehr Glauben schenken. [163]

1993 wurde schon von einem RAND-Mitarbeiter verkündet: ”Cyberwar is coming”. [164]
Unter Fake News sind Informationen zu verstehen, welche als “wahrheitsgemäße”-Nachrichten sowie als Nachrichtenberichterstattung ausgegeben werden. [165]

Es wurde in den USA eine sehr bekannte Fake News Seite “Infowars” von “Alex Jones” geleitet, dieser wurde am 03.04.2019 durch eine Massenklage verurteilt. Laut diesem Bericht sind einige der Nachrichten, welche veröffentlicht wurden, anhand von Verschwörungstheorien entstanden. [166]
Alex Jones Webseite ”Infowars” wurde auch von diversen Unternehmen wie Twitter, Apple, Facebook und YouTube verbannt. [167]

Laut dem Bericht ist ersichtlich, dass Österreich von 38 überprüften Ländern die höchste Nutzung gedruckter Zeitungen hat, obwohl die Verkäufe von den Zeitungen jährlich sinken. Es ist zu merken, dass Nachrichten und den möglicherweise verbundenen ”Fake News” einen großen Bereich treffen würde. Auch das “Smart-Phone” wird weltweit ein immer wichtigeres Nachrichten-Medium. In Österreich gilt der “ORF” (Österreichische Rundfunk) als vertrauenswürdigster Nachrichtendienst. Dieser Bericht zeigt, wie viele Menschen den Medien vertrauen und wie viele Menschen mit potenziellen “Fake News” erreicht werden können. [168]

Falsche Nachrichtenübermittlung, dieses Problem gibt es schon seit ewigen Zeiten. Es wurde ein altes Problem mit einem neuen Namen und zwar “Fake-News” ausgestattet.
Unter Fake-News werden Nachrichten verstanden, welche erfunden sind und nicht der Wahrheit entsprechen. Diese Nachrichten sind aus dem Nichts entstanden und werden dazu verwendet, um Menschen zu täuschen. Es werden somit beispielsweise “echte”-Bilder verwendet, mit einem Text ausgeschmückt, welcher aber auf “Fake-News” Basis beruht. [169]
Solche falschen Nachrichten können massiv die Politik und somit Wahlen beeinflussen, daher wird rigoros von Unternehmen/Plattformen gegen solche Nachrichten durchgegriffen. [170]

Mittels OSINT ist es möglich solche Fake-News auf deren “Wirklichkeit” zu prüfen. Um das Ausmaß von “Fake-News” zu begrenzen sollten diese manipulierten Nachrichten so schnell wie möglich assimiliert werden. Dazu müssen diese Nachrichten zuerst einmal identifiziert werden. Es werden für OSINT-Experten auch Analysetechniken zur Verfügung gestellt, welches auf kritisches Denken beruhen. Es wird empfohlen, dass eine Analyse von cloudbasierten-Medien durchgeführt wird, sowie deren Quellen. [165]

OSINT im militärischen Bereich:
In der heutigen Zeit ist es relevant, dass man verschiedenste Daten, welche gesammelt werden können, auch verwalten kann. Somit können diese Daten auch zugeordnet werden und für Recherchen verwendet werden.
Das Militär kann OSINT ebenso für sich verwenden. OSINT hat ein hohes Potenzial in diesem Bereich, da es nachrichtendienstliche Unterstützung bietet und für Hinweise und Warnungen zuständig sein kann. Es kann dadurch beispielsweise der Waffenerwerb kontrolliert werden und dementsprechende Gegenmaßnahmen getroffen werden. Aber es können auch politische Entwicklungen erforscht, sowie Notfallplanungen und Sicherheitsunterstützungen erstellt werden. Daher dient OSINT als Grundlage in diesem Bereich.

Durch OSINT wird ermöglicht, dass Hinweise und Warnungen gegeben werden können. Somit kann eine mögliche Instabilität oder eine Gefahr schneller eingeschätzt werden. Es können dadurch ebenso wichtige Beschaffungs- und Konstruktions-Entscheidungen beeinflusst werden. Weiters können umklassifizierte Bedrohungsinformationen bereitgestellt werden. Diese können zur Aufklärung und Unterstützung von öffentlicher oder politischer Mobilität dienen. Im weiteren Verlauf können davon dann Strategien und Entwicklungen abgeleitet werden.

Es hilft ebenso regionalen Streitkräften bei der Planung zur Bereitstellung von Einsatzkräften. So kann herausgefunden werden, wo welche Luft/Land/See- Streitkräfte eingesetzt werden müssen. Weiters ist ein wichtiger Punkt, dass dadurch auch die Koordination von gemeinsamen Operationen verbessert werden kann. Ein weiterer Bereich wo OSINT Abhilfe schaffen kann ist, bei der Bekämpfung der Verbreitung von Massenvernichtungswaffen und der Terrorismusbekämpfung sowie der damit verbundenen friedenserhaltenden Maßnahmen. Durch OSINT können aktuelle Landkarten der Gebiete an einen Befehlsinhaber übermittelt werden, somit sind aktuelle geografische Informationen gegeben. [171] [172] [173]

Ethisches Hacking/Penetration Tests:
OSINT kann auch im Bereich von “ethischen Hacking” sowie bei Penetrations-Tests verwendet werden. Hier können verschiedene Sicherheitsexperten Überprüfungen durchführen, um potenzielle Schwachstellen in Netzwerken zu finden.

Von Unternehmen selber kann ein Penetration-Test in Auftrag gegeben werden. Das heißt, dass ein externes Unternehmen oder direkt die firmeninterne Abteilung einen Test durchführt und somit überprüft, ob Ports oder vertrauliche Informationen nach außen sichtbar sind. Weiters können Überprüfungen durchgeführt werden ob es nicht aktualisierte Software Versionen ersichtlich sind, welche Angreifbar sind.

Durch OSINT, welches in diesem Bereich schon eine kaum mehr wegzudenkende Technik ist, werden die einzelnen Arbeitsabläufe beschleunigt und vereinfacht. Normalerweise müssten Pentester manuell alle gesammelten Informationen sortieren, das nimmt im Allgemeinen viel Zeit sowie Ressourcen in Anspruch.
Um Ressourcen sowie Zeit zu sparen, können diverse Tools angewandt werden, welche es einem Anwender ermöglichen, die gesammelten Daten zu sortieren und in einem lesbaren Format darzustellen.

So können verschiedene Informationen, welche über das Unternehmen ausfindig gemacht werden konnten, zusammengefügt werden und helfen es zu schützen. Durch diese gefundenen Informationen über ein Unternehmen können dementsprechende präventive Maßnahmen gesetzt werden. Somit können Schwachstellen möglicherweise vor einem Angereifer gefunden werden, dadurch wird das Sicherheitsniveau einer Firma verbessert. [67]

8. Auswertung & Interpretation der Ergebnisse

Es wurden ausgewählte Tools anhand der jeweiligen Funktionen analysiert, dessen Kriterien verglichen und gegenübergesellt. Durch die Vielzahl der möglichen Tools war eine Eingrenzung unumgänglich. Es wurden daher nur Tools analysiert und bewertet, welche standardmäßig auf der virtuellen Maschine “Buscador2” und “Kali-Linux” vorhanden sind. In diesem Kapitel werden die verwendeten Kriterien in einer Matrix dargestellt sowie die Gegenüberstellung der Tools durchgeführt.

In dieser Arbeit wurde der Fokus und somit die Eingrenzung auf Tools gelegt, welche in den “Top 10” Rankings der meist verwendeten OSINT-Tools vertreten sind. [174] [175] [176] [177] [178]
Die Entscheidung dieser zwei virtuellen Maschinen „Kali-Linux“ sowie „Buscador2“ wurde aufgrund der Bekanntheit und der Empfehlungen in verschiedenen Foren gefällt.
Durch die weitere Eingrenzung, dass nur Tools verwendet werden, welche auf den beiden virtuellen Maschinen verfügbar sind, ergeben sich für den Anwender einige Vorteile. Mit den virtuellen Maschinen wird eine Person unterstützt, da keine manuellen Installationen von Tools durchgeführt werden müssen. Ebenso fällt das Aktualisieren von System- und Programmversionen nicht mehr an, da die virtuellen Maschinen mit den Versionen der Tool- und der Systemversionen übereinstimmen. Daher ist es möglich, nach dem Aufsetzen der virtuellen Maschine, die Tools zu verwenden, ohne manuelle Interaktionen durchführen zu müssen, somit ersparen sich Anwender/innen wesentliche Aufwände.

Grundlagen der Evaluierung:
Die Grundlage der Evaluierung sind die Tools, welche anhand der definierten Kriterien bewertet wurden. Anhand dieser Kriterien wurden die ausgewählten Tools verglichen.
Um ein besseres Scan-Ergebnis zu schaffen wurden für diese Arbeit sechs API-Keys verwendet, je nach Möglichkeit der Tools wurden folgende verwendet:

- Shodan
- AbuserIPDB
- Hunter.io
- Buildwith.com
- Botscout.com
- Zetalytics

Evaluierungsmodell:
Um einen Vergleich der Tools herstellen zu können, mussten zuerst verschiedene Kriterien definiert werden. Nach deren Definition, welche nötig war, um die Forschungsfragen zu beantworten, konnte zum nächsten Schritt übergegangen werden. Dieser beinhaltet das Überprüfen der einzelnen Tools sowie die Beschreibung der einzelnen Kriterien.

Um die Tools analysieren zu können, wurden zuerst die beiden virtuellen Maschinen “Kali-Linux” sowie “Buscador2” installiert. Nachdem dies durchgeführt wurde, konnten die verschiedenen Kriterien in der Praxis überprüft werden. Es wurde anschließend mit jedem Tool ein passiver Scan auf die Fachhochschule oder/und auf den Twitter-User der Fachhochschule oder den Fake User durchgeführt. Die durchgeführten Scans waren abhängig von der Spezialisierung der jeweiligen Tools.

Anschließend wurden die gesammelten Informationen überprüft und somit das Kriterium “Informationen” analysiert. Hier war es bei den Tools nicht möglich, die gesamten Funktionalitäten zu prüfen, da verschiedene API-Keys benötigt werden. Für diese Arbeit wurden keine kostenpflichtigen API-Keys verwendet, jedoch sind sechs kostenlose API-Keys verwendet worden. Diese Keys wurden, je nach Möglichkeit der Unterstützung des API-Keys, bei den Tools eingebunden.

Die Überprüfung der gesammelten Informationen durch den passiven Scan ist ein wichtiger Schritt in dieser Arbeit, dadurch soll gezeigt werden, welche Angriffsvektoren damit ausgenutzt werden können. Es soll gezeigt werden, mit welchen Informationen welche Angriffe durchgeführt werden können. Ebenso können Unternehmen durch diese Scans erkennen, welche Informationen nach außen ersichtlich sind und präventiv dagegenwirken.

Nachdem die Scans durchgeführt worden sind, werden die restlichen Kriterien analysiert. Einige dieser Kriterien konnten direkt in dem Tool getestet und herausgefunden werden wie beispielsweise "GUI/CLI" und das "Exportieren" sowie das "Importieren". Hier wurde überprüft ob von dem Tool eine CLI/GUI zur Verfügung gestellt wird. Anschließend wurde geprüft, welche Export- und Import-Formate unterstützt werden.
Bei dem Kriterium "Suche- und Filtermöglichkeit" wurde überprüft, ob dieses Kriterium direkt in dem Tool möglich ist. Ist dies nicht der Fall, wurde geprüft ob es mit der exportierten Datei in einem weiteren Tool gefiltert und durchsucht werden kann.
Das Kriterium "Plattformen" wurde überprüft, indem die Tools auf diesen getestet worden sind, sowie durch Berichts-Recherchen, welche Plattformen unterstützt werden von dem Tool.

Bei dem Kriterium "Updates" wurde überprüft, ob direkt auf der Webseite der Tools ein Change-Log der Versionen und Änderungen angeboten wird. Wenn dies nicht der Fall war und das Tool über GitHub bezogen werden konnte wurde hier geprüft, welche Änderungen, wann vorgenommen worden sind. Somit ist ersichtlich ob ein Tool gewartet und auf den neuesten Stand gebracht wird.

Ein weiteres Kriterium waren die "Kosten" eines Tools. In der Arbeit wurden jene Tools in der kostenlosen Version verwendet, dennoch ist dieses Kriterium wichtig, falls ein Unternehmen ein Tool produktiv in dem Unternehmen einsetzen möchte. Daher wurde geprüft, wie hoch die Anschaffung eines Tools ist. Weiters werden möglicherweise Weiterbildungen für einen Mitarbeiter benötigt, daher wurde überprüft, ob eine Schulung für das jeweilige Tool angeboten wird. Wenn dies der Fall ist, wird überprüft, wie hoch die Kosten einer Schulung sind.

Das Kriterium "Attacken" ist ein sehr wichtiges Kriterium in dieser Arbeit. Es ist sehr eng mit dem Kriterium "Informationen" verbunden, da hier die Attacken aufgelistet werden, welche mit den gesammelten Informationen der jeweiligen Tools durchgeführt werden können. Dadurch soll einem Unternehmen gezeigt werden, welche Daten öffentlich ersichtlich sind, somit können verschiedene präventive Maßnahmen gesetzt werden. Jedoch können ebenso Angreifer diese Informationen sammeln und diese gegen das Unternehmen verwenden.

Das Kriterium "Berichtsverwaltung" wurde mit dem Kriterium "Export" in Verbindung gebracht. Hier wird analysiert, welche Tools einen Bericht über einen Scan generieren können. Weiters wird überprüft, ob dieser Bericht für eine detailliertere Analyse wiederverwendet werden kann.

Es ist ebenso das Kriterium "Darstellungsfunktion" wichtig. Dieses Kriterium hängt mit dem Kriterium "Berichtsverwaltung" und "Export" zusammen. Hier wird überprüft, welche Darstellung von einem Bericht ermöglicht wird.

Bei dem Kriterium "Korrektheit der Daten" wurden Stichproben von den gefundenen Informationen genommen und gegengeprüft. Es werden beispielsweise die gefundenen E-Mail-Adressen von der FH St. Pölten mit den E-Mail-Adressen, welche auf der Webseite der Fachhochschule St. Pölten angegeben sind, verglichen. Weiters werden die gefundenen Daten anhand von Suchmaschinen auf deren Korrektheit geprüft.

Das Kriterium "Rückverfolgbarkeit" wurde einerseits mit den Fake Usern getestet und geprüft ob die gefundenen Informationen auf den Fake User hinweisen. Weiters wurden mit den gefundenen Informationen Suchanfragen auf Suchmaschinen oder Social Media Plattformen durchgeführt, um zu

überprüfen ob eine Person gefunden werden kann. Es wird auch geprüft ob die gefundenen Daten Rückschlüsse auf die verwendeten Systeme in einem Unternehmen geben.

Ergebnisse der Evaluierung:

Tools	Plattform	GUI/CLI	Import-Format	Export-Format	Updates
Maltego	Linux, Windows, iOS/Mac	GUI	csv, Entitäten	xls, xlsx, csv	regelmäßige Updates - letztes Update am 12-11-2019 (Stand 26.01.2020) - Bugfixes und Sicherheitsupdates
TheHarvester	Linux, Windows, iOS/Mac	CLI	nicht möglich	html, xml, sqlite	regelmäßige Updates - letztes Update am 14-10-2019 (Stand 26.01.2020) - Bugfixes und Verbesserungen allgemein (Versionserneuerungen)
Recon-NG	Linux, Mac/iOS	CLI	Es können vorhandene Textdateien als Suche verwendet werden	csv, html, xlsx, xml, json, list, proxifier, pushpin	regelmäßige Updates - letztes Update im Oktober 2019 (Stand 23.02.2020) - Bugfixes und kleine Änderungen und Versionierungen
Spiderfoot	Windows, Linux, Mac/iOS, Webbasiert	GUI	n.v.	cve, gexf, json	regelmäßige Updates - neue Release von Spiderfoot 3.0 am 26-01-2020 (Stand 26.01.2020)
Tinfoleak	Webbasiert, Linux, Windows, iOS/Mac	GUI, CLI	Bei der Webbrowser-Version ist kein Import möglich. Wenn das Tool in Buscador2 verwendet wird dann ist ein Import möglich.	html	Keine regelmäßigen Updates
Twitter-Script	Linux (Buscador2)	GUI (es erscheint ein Pop-Up Fenster)	Es ist kein Import möglich	csv, Bilddateien (z.B.: jpg)	Keine regelmäßigen Updates

Tabelle 11 Ergebnisse der Tool-Evaluierung 1

Tools	Such- und Filtermöglichkeiten	Kosten
Maltego	Ja - Durch das Exportieren der Dateien in verschiedene Formate und im Tool selber auch	Verschiedene Versionen sind verfügbar, der Preis liegt zwischen 899€ und 1799€, Schulungskosten kommen direkt bei Maltego auf 15.000€, es werden aber auch von externen Firmen Kurse angeboten, hier liegt die Preisspanne zwischen 390€ und 1999€.
TheHarvester	Ja - können direkt vor der Suche schon mitgegeben werden und durch die Exportmöglichkeiten in einem eigenen Tool	Es fallen keine Kosten an und es sind keine Kurse für dieses Tool vorhanden.
Recon-NG	Ja - Es können für jeden Scan eigene Workspaces erstellt werden, darin können verschiedene Suchaktionen und Filterungen durchgeführt werden. Ebenso können durch die unterschiedlichen Exportformate in verschiedenen Tools Filterungen und Suchen durchgeführt werden.	Es fallen bei dem Tool keine Kosten an. Online werden verschiedene Video-Kurse sowie Tutorial Videos angeboten, welche gegen eine geringe Gebühr eine weiterführende Bildung bieten können.
Spiderfoot	Eine Suche kann auf der Weboberfläche durchgeführt werden. Eine Filterung ist nur nach dem Status (running, finish, failed/aborted) eines Scans möglich. Es können jedoch die gesamten Export-Files durchsucht und gefiltert werden.	Es werden verschiedene Versionen angeboten, somit besteht eine Preisspanne zwischen 19€ bis 599€. Zu dem Tool sind keine Schulungen gefunden worden.
Tinfoleak	Eine Suche kann nur in dem html-File durchgeführt werden.	Das Tool ist kostenlos zu verwenden. Es sind keine Schulungen zu dem Tool gefunden worden.
Twitter-Script	Eine Suche sowie die Filterung können in den exportierten csv-Files durchgeführt werden.	Bei der Verwendung des Tools fallen keine Kosten an. Es sind keine Schulungen zu dem Tool gefunden worden.

Tabelle 12 Ergebnisse der Tool-Evaluierung 2

Tools	Informationen	Korrektheit der Daten	Berichtsverwaltung
Maltego	Personen/Namen/E-Mail-Adressen/Alias, Gruppen von Personen (Social Media Netzwerke), Unternehmen, Organisationen, Webseiten, DNS/Domains/Internet-Infrastrukturen, Verbindungen/Zugehörigkeiten, Dokumente/Files	hohe Korrektheit	Durch die Exportvielfalt können Berichte für weitere Untersuchungen verwendet werden
TheHarvester	E-Mail-Adressen, Sub-Domains, Hosts, Namen, IP-Adressen, Ports/Banner	hohe Korrektheit	Berichte können für weitere Analysen verwendet werden.
Recon-NG	Telefonnummern, E-Mail-Adressen, Standorte, Webseiten, Hosts, IP-Adresse, Personen/Unternehmen, Usernamen	sehr hohe Korrektheit	Es ist eine Vielzahl einer Berichtserzeugung möglich, da viele Exportformate unterstützt werden. Dies dient für weitere Analysen der Scan Ergebnisse
Spiderfoot	Domain Name (DNS), IP-Adressen, Hostnamen/Sub-domains, Subnetze, ASN, E-Mail-Adressen, Telefonnummern, Namen von Personen	teilweise Korrektheit (es wird eine manuelle Entfernung der falschen Einträge benötigt)	Es werden verschiedene Exportformate für eine weitere Analyse zur Verfügung gestellt.
Tinfoleak	Follower, Tweets, Bilder, Hashtags (meistverwendete), Geolocation, verwendete Wörter, Metadaten	sehr hohe Korrektheit (Daten werden direkt von der Twitter Seite des Users gespeichert)	Es wird ein html-File für die weitere Analyse bereitgestellt.
Twitter-Script	Bilder des Twitter-Users, Twitter-Usernamen, Namen von Personen, Freunde die auf Twitter folgen, Tweets/Retweets mit Zeitstempel	sehr hohe Korrektheit (Daten werden direkt von der Twitter Seite des Users gespeichert)	Es werden drei verschiedene csv-Files gespeichert und die Bilder von dem Konto extrahiert. Diese Daten können für weitere Analysen verwendet werden.

Tabelle 13 Ergebnisse der Tool-Evaluierung 3

Tools	Darstellungsfunktion	Rückverfolgbarkeit	Attacken
Maltego	Textfile, PDF, Tabelle	gute Rückverfolgbarkeit	Phishing-Angriffe, Ransomware, Malware, Virus und Würmer, Identity Theft, Cyber Stalking, IP-Spoofing
TheHarvester	Tabelle, Webbrowser-File	sehr gute Rückverfolgbarkeit	Man-in-the-Middle, DoS, IP-Spoofing, Phishing-Angriffe, Ransomware, Würmer und Viren, Cyber Stalking
Recon-NG	Tabelle, Textfile	sehr gute Rückverfolgbarkeit	IP-Spoofing, Phishing-Angriffe, DoS, Ransomware, Würmer und Viren, Cyber Stalking, Identity Theft
Spiderfoot	Tabelle, Textfile, Grafiken	gute Rückverfolgbarkeit	Domain-Hijacking, DNS-Flooding, DoS, IP-Spoofing, DNS-Tunneling, Man-in-the-Middle, Cyber Stalking
Tinfoleak	Webbrowser - html-File	sehr gute Personennachforschungen möglich	Cyber-Stalking
Twitter-Script	Tabelle, Bilder	ermöglicht eine sehr genaue Personennachforschung	Cyber-Stalking

Tabelle 14 Ergebnisse der Tool-Evaluierung 4

Tools	Funktionalitäten
Maltego	Das Tool ermöglicht es, ein Unternehmen auf diverse Arten zu überprüfen. Dazu kann beispielsweise für den ersten Scan die Webseite oder die Domain des Unternehmens verwendet werden. Anhand der gefundenen Informationen können weitere Scans durchgeführt werden. Ebenso können mit Maltego Social Media Profile beispielsweise auf Twitter überprüft werden und Tweets/Freunde und Follower eines Ziels anzeigen.
TheHarvester	Das Tool ermöglicht das Untersuchen eines Unternehmens. Dazu kann für den ersten Scan-Vorgang die Webseite eines Unternehmens verwendet werden, um Informationen zu sammeln.
Recon-NG	Mit dem Tool können Unternehmen untersucht werden. Es können weiters Twitter Profile gescannt werden, dazu wird aber der API-Key benötigt.
Spiderfoot	Es können mit dem Tool Unternehmen aber auch Sozial Media Profile untersucht und deren Daten gespeichert werden.
Tinfoleak	Das Tool ermöglicht eine Abbildung der gesamten Twitter Seite eines Ziels. Es können beispielsweise die verwendeten Endgeräte für das Posten eingesehen werden. Ebenso können beispielsweise Geolocations, Metadaten, Hashtags und die meist verwendeten Wörter gespeichert werden.
Twitter-Script	Mit dem Tool ist es möglich, den gesamten Inhalt einer Twitter Seite des Zieles zu speichern. Es werden sämtliche Tweets, Freunde und Follower sowie Bilder gespeichert.

Tabelle 15 Ergebnisse der Tool-Evaluierung 5

Prozessablauf für die Information Gathering Phase:

In diesem Abschnitt wird der Prozess für eine Durchführung von Information Gathering anhand des Open Source Intelligence Cycle von Kapitel 4.2 „*Open Source Intelligence Cycle*“ beschrieben. In diesem Beispiel wird als Ziel die FH St. Pölten verwendet.

Um Information Gathering durchführen zu können muss zuerst bekannt sein, auf welches Ziel der Fokus gelegt wird. Es müssen daher zuerst die Anforderungen und eine Planung durchgeführt werden, somit wird festgelegt, welche Informationen von einem Ziel benötigt werden. Für das Ziel in diesem Beispiel wird erwartet, dass grundlegende Informationen wie, “E-Mail-Adressen", “DNS”, “Hosts” sowie “Ports” gefunden werden und es soll der Social Media Account des Ziels überprüft werden. Weiters wird festgelegt, dass nur ein passiver Scan durchgeführt wird, damit die Fachhochschule das Sammeln der Daten nicht merkt.
Dieser Scan soll überprüfen, ob das Ziel von außen angreifbar ist oder Schwachstellen sowie Informationen nach außen preisgegeben werden.

Nachdem die benötigten Requirements (Anforderungen) über das Ziel sowie die Scan Art definiert worden sind, kann begonnen werden die Daten zu sammeln. Dafür können verschiedene Tools verwendet werden, in diesem Beispiel richtet sich der Fokus auf die Tools, welche in der Arbeit beschrieben wurden.
Es wurde zu Beginn überprüft welche der Tools die definierten Anforderungen erfüllen, aus diesem Grund wurden für das Beispiel die Tools “Recon-NG” sowie “TheHarvester” ausgesucht. Um die Social Media Daten zu sammeln wurde das Tool “Tinfoleak” verwendet. Es sollten für einen Scan zwei Tools verwendet werden können, da somit die Informationsmenge vergrößert wird. Zudem können die Ergebnisse der Scans auf deren gefundenen Informationen verglichen werden.

Um die ersten Informationen über das Ziel zu bekommen, wurde in diesem Beispiel zuerst das Tool “Recon-NG” verwendet. Dies hat den Grund, da für einen Scan lediglich die Domain des Ziels benötigt wird und das Tool die gefundenen Informationen sehr übersichtlich wiedergibt.
Um einen Scan mit diesem Tool zu starten wird anfangs nur die Domain des Ziels verwendet, in diesem Beispiel ist es “fhstp.ac.at”. Durch diesen Scan ist es möglich verschiedene Hosts, Ports, DNS, sowie E-Mail-Adressen zu finden. Dadurch können einige der zu Beginn definierten Requirements gesammelt werden.
Danach wurde das Tool “TheHarvester” verwendet. Dieses Tool ermöglicht ebenso das Sammeln von den benötigten Informationen.
Um die offenen Ports zu finden, wurde zusätzlich das Tool “Shodan” verwendet. Von den Tools werden die Ports aufgelistet, hingegen fehlt es an der Versionsnummer, welche mittels „Shodan“ angezeigt wird.
Um das Social Media Profil des Ziels zu überprüfen, wurde “Tinfoleak” verwendet. Dieses Tool bietet eine übersichtliche Darstellung der Posts, Freunde und der Follower. Hier können die verschiedenen Tweets von einem Ziel kontrolliert werden.

Die gefundenen Informationen der jeweiligen Tools werden in verschiedenen Exportformaten angeboten. Das Tool Recon-NG bietet “csv”, “html”, “xlsx” und “xml” an. Von dem Tool “TheHarvester” werden “html” und “xml” als Export Format angeboten. Die Informationen müssen analysiert und auf dessen Richtigkeit überprüft werden. In dieser Arbeit wurden die Informationen nur stichprobenmäßig überprüft, somit wurden gefundene E-Mail-Adressen mit den E-Mail-Adressen, welche auf der FH St. Pölten Webseite veröffentlicht sind, verglichen. Das Tool “Tinfoleal” bietet ein “html”-File als Export an.

Es ist ersichtlich, dass die Tools in diesem Beispiel alle das Exportformat “html” unterstützten. Durch dieses Format wird es für eine Person in einer gut lesbaren Form wiedergegeben.

Dadurch wird einem Sicherheitsteam in Unternehmen oder anderen Personen ermöglicht, diese exportierten Informationen in dem File zu analysieren und auf gefundene Schwachstellen zu reagieren und diese zu beheben.

Anhand der durchgeführten Scans der FH St. Pölten konnten verschiedene Hostsysteme gefunden werden wie Nagios, Fedora, Mahara, Wordpress, Jabber, Skype und Jira. Weiters wurde anhand von den Portscans und „Shodan“ ein Apache-Server mit der Version 2.4.29 gefunden. Mit dem Tool “Tinfoleak” wurde herausgefunden, dass für die Tweets vor allem die “Twitter Web App” verwendet wird.
Diese Findings können grundlegend einiges über die Systeme, welche in einem Unternehmen verwendet werden, aussagen. Um jedoch detailliertere und somit gezieltere Angriffe durchzuführen, benötigt man Versionsnummern von den Systemen. Es können mit den genauen Versionsnummern verschiedene CVEs gesucht werden, womit anschließend das Ziel angegriffen werden kann.

9. Beantwortung der Forschungsfragen

In dem folgenden Kapitel werden die definierten Forschungsfragen im Detail beschrieben und erklärt.

1. Wie kann die Reconnaissance Phase für Information Gathering bei den ausgewählten Tools eingesetzt werden?

Um die Forschungsfrage beantworten zu können, mussten die ausgewählten Tools im Detail überprüft werden. Hier muss zuerst überprüft werden, welche Informationen mit den jeweiligen Tools gefunden werden können. Es wurde dafür in Kapitel 8 „*Auswertung & Interpretation der Ergebnisse*“ in Tabelle 11 „*Ergebnisse der Tool-Evaluierung 1*“ bis 15 „*Ergebnisse der Tool-Evaluierung 5*“ die ausgewählten Tools im Detail analysiert und deren jeweiligen Funktionalitäten aufgelistet. Diese Tabellen geben eine detaillierte Übersicht über die verschiedenen Tools, womit einem Unternehmen oder einer Person ermöglicht wird, die Tools auf einen Blick zu vergleichen. Es ist in der Tabelle ersichtlich, dass jedes Tool einen wichtigen Beitrag in der Reconnaissance Phase leistet.
Jegliche Tools, welche in dieser Arbeit analysiert wurden, können für die Information Gathering Phase eingesetzt werden. Es ist zu beachten, dass bei den Tools trotz denselben Scan Methoden, unterschiedliche Informationen gesammelt werden können. Daher ist es ratsam, nicht nur eines der analysierten Tools zu verwenden, sondern eine Kombination der Tools. Somit können der Informationsgehalt und die Informationsmenge vergrößert werden.

   a. Welche Informationen können mit den analysierten kostenlosen OSINT Tools gesammelt werden?

Für die Beantwortung der Frage hat mit dem jeweiligen Tool ein Scan zu einer Person oder einem Unternehmen durchgeführt werden müssen. Nach dem Scan wurden die Ergebnisse im Detail überprüft und aufgelistet. Um diese Forschungsfrage zu beantworten wurde in Kapitel 8 „*Auswertung & Interpretation der Ergebnisse*“ eine Tabelle 13 „*Ergebnisse der Tool-Evaluierung 3*“ mit der Spalte “Informationen” erstellt. In dieser sind die jeweiligen Informationen aufgelistet, welche mit dem Tool gefunden werden können. Jedoch können nicht alle Informationen kostenlos bezogen werden, da möglicherweise kostenpflichtige API-Keys benötigt werden.

   b. Welche Angriffe können mit den gefundenen Informationen durchgeführt werden?

Es wurden nur “passive” Scans durchgeführt. Das heißt es sind keine “realen” und “bemerkbare” Angriffe durchgeführt worden, sondern öffentlich frei zugängliche Informationen gesammelt worden. Somit konnten die möglichen Angriffe nur anhand der Informationen, die gesammelt werden konnten, abgeleitet werden. Diese Forschungsfrage wurde in der Tabelle 14 „*Ergebnisse der Tool-Evaluierung 4*“ in der Spalte “Attacken” beantwortet.

   c. Wie kann die Information Gathering Phase durchgeführt werden?

Dies Forschungsfrage wurde in dem Kapitel 4.2 „*Open Source Intelligence Cycle*“ beschrieben. Bevor ein Scan durchgeführt wird, muss bekannt sein, welches Ziel angegriffen wird und welche Informationen davon benötigt werden. Nachdem dieser Punkt geklärt wurde, können die weiteren Schritte überlegt werden. Zuerst muss ein Scan durchgeführt werden. Nachdem dieser durchgeführt wurde, erhält man eine Menge an verschiedenen Rohdaten. Diese Rohdaten stammen von verschiedenen öffentlichen Quellen. Um diese Daten anschließend verarbeiten zu können müssen sie zuerst entschlüsselt oder übersetzt werden. Anschließend werden diese im Detail überprüft, da sich hier möglicherweise “falsche” Informationen befinden, welche das Ergebnis verfälschen. Nachdem diese Daten anhand ihrer Relevanz, sowie deren Gültigkeit geprüft wurden, können sie verarbeitet

werden. In dem letzten Schritt sind die Daten so aufbereitet, dass diese an Personen oder Unternehmen weitergeleitet werden können.

d. Inwiefern können die Open Source Tools für die Information Gathering Phase eingesetzt werden und wie unterscheiden sich die jeweiligen Tools in deren Funktionen?

Es wurden sechs unterschiedliche Tools analysiert. Jedes dieser Tools bietet einer Person die Möglichkeit, verschiedene Informationen über ein Ziel zu sammeln. Durch den Praxistest und den durchgeführten Scans der Tools wurde ersichtlich, welche Informationen für die Information Gathering Phase, mit den jeweiligen Tools gesammelt werden können, siehe Tabelle 13 „*Ergebnisse der Tool-Evaluierung 3*“ Spalte “Informationen”. Somit kann ein Unternehmen ein Tool anhand der benötigten Informationen auswählen.
Bei der Analyse der jeweiligen Tools wurden ebenso die gesamten Unterschiede der Tools bemerkt. Es ist in Kapitel 8 „*Auswertung & Interpretation der Ergebnisse*“ im Absatz “Vergleich der Tools” eine Beschreibung durchgeführt worden, in welcher die Tools und dessen Funktionen beschrieben wurden. Ebenso in Kapitel 6 „*Evaluierung von den Tools*“ ist eine Beschreibung zu den jeweiligen Tools gegeben.

2) Inwiefern entstehen durch die Verwendung von OSINT Vorteile und Nachteile und wie kann dies zum Schutz der Infrastruktur eines Unternehmens beitragen?

Durch diese Arbeit wurde ersichtlich, dass eine Vielzahl von kostenlosen OSINT Tools zur Verfügung stehen. Da den KMUs das Personal oder die finanziellen Mitteln fehlen, sind diese Tools eine kaum wegzudenkende Unterstützung. Es wird einem Unternehmen dadurch ermöglicht, das eigene Unternehmen zu überprüfen. Damit ist ersichtlich, welche Informationen frei verfügbar sind über das Unternehmen und welche möglicherweise kritisch und als gefährlich erscheinen. Es ist immer wichtig zu wissen, alle Informationen, die ein Unternehmen bei einem selbst durchgeführten Scan auf das eigene Unternehmen findet, können auch von einem Angreifer gefunden werden.
Durch den eigenen Scan auf das Unternehmen können auch präventive Maßnahmen durchgeführt werden. Wie vorhin schon erwähnt ist der größte Nachteil eines Unternehmens, dass ein Angreifer ebenso diese Tools verwenden kann. Somit besteht die Möglichkeit, dass verschiedene Informationen gesammelt und diese gegen das Unternehmen eingesetzt werden.
Das Problem bei KMUs ist jedoch oft, dass die Zeit sowie das Personal fehlen, um sich mit diesem Thema zu beschäftigen.

a. Wie können die ausgewählten Tools in einem Unternehmen eingesetzt werden?

Es wurden in dieser Arbeit ausschließlich kostenlose Open Source Tools verwendet. Je nach Einsatzgebiet kann das geeignete Tool aus den Tabelle 11 „*Ergebnisse der Tool-Evaluierung 1*“ bis 15 „*Ergebnisse der Tool-Evaluierung 5*“ gewählt werden. Nach dem gewünschten Einsatzgebiet und den Anforderungen, können Unternehmen sich auf verschiedene der analysierten Tools konzentrieren. Die Entscheidung, welches der analysierten Tools in einem Unternehmen eingesetzt werden soll, kann mit dieser Arbeit nicht abgenommen werden, da jedes Unternehmen andere Informationen sucht oder benötigt. Daher wurde in der Tabelle 11 bis 15 ein Überblick für Unternehmen geschaffen, um ein Tool für ihre Bedürfnisse auszuwählen.
Da alle getesteten Tools auf den zwei virtuellen Maschinen „Kali-Linux“ sowie „Buscador2“ verfügbar sind, können die Tools nach dem Installieren der virtuellen Maschine verwendet werden und diverse Scans durchgeführt werden, da diese bereits von den Entwicklern getestet worden sind. Somit müssen keine Versionen oder Updates von den Tools nachgezogen werden, damit diese funktionstüchtig sind.

3) Wie können Use-Cases dabei helfen, um mit Open Source Intelligence Schwachstellen zu finden und wie kann dadurch das Unternehmen abgesichert werden?

Um das Thema und dessen Bedeutung anhand eines Beispiels wiederzugeben, wurden in Kapitel 7 „*OSINT Use Case*“ verschiedene Use Case gebildet. In dem Kapitel 7, sind drei unterschiedliche Szenarien beschrieben worden, in welcher die Verwendung von OSINT eine Hilfe große Rolle spielt. Diese Beispiele sollen einem Unternehmen zeigen, welche Möglichkeiten durch die Verwendung von OSINT bestehen und wie dadurch ein Unternehmen geschützt und besser abgesichert werden kann.

10. Conclusion

Durch diese Arbeit soll ein Überblick für Unternehmen gegeben werden, welche Tools welche Funktionalitäten bieten. Somit können Unternehmen schnell eine Tendenz zu einem Tool finden, da diese mit den benötigten Kriterien verglichen werden können.
Diese Übersicht wird durch eine Tabelle und der beschriebenen und hervorgehobenen Funktionalitäten gegeben. Ebenso wurden Kriterien definiert und im Detail beschrieben, um dem Unternehmen oder einer Person eine noch genauere Erklärung der Tools zu bereitstellen. Weiters wurden die ausgewählten Tools auf deren Praxis-Tauglichkeit geprüft.

Der Bereich von OSINT wird immer größer, weshalb eine Abgrenzung bei diesem Thema eine wichtige Rolle spielt.
In dieser Arbeit wurde der Fokus auf die verschiedenen Tools sowie dem “passiven” Scan gelegt. Es wurde anschließend ein Vergleich und eine Beschreibung der jeweiligen Tools durchgeführt.
Für weitere Arbeiten kann der Fokus auf andere Tools gelegt werden. Es könnten die analysierten Tools ebenso auf neue Zusatzfeatures analysiert werden, da die meisten Tools eine ständige Weiterentwicklung erleben.

Diese Arbeit hat den Fokus auf die Reconnaissance Phase der Cyber Kill Chain gelegt. Daher wurde mit verschiedenen Tools getestet, welche sammelbaren Informationen mit den jeweiligen Tools gefunden werden können, ohne dass das Ziel davon etwas bemerkt. Weitere Arbeiten können auf dieser aufbauen und sich auf die restlichen Phasen des Cyber-Kill-Chain konzentrieren.

Da in dieser Arbeit der Fokus auf dem “passiven” Scan liegt, können sich weitere Arbeiten diese als Vergleich nehmen und einen “activen” Scan durchführen. Dieser Scan muss im Vorhinein mit dem Ziel vereinbart werden und darf nur für Sicherheitszwecke verwendet werden.

Eine herausfordernde Forschungsaufgabe wäre das Ändern von verschiedenen Privacy-Einstellungen der Social Media Plattformen. Somit kann erforscht werden, welche Informationen nach Änderungen dieser Einstellungen sichtbar und sammelbar sind.

Weitere Arbeiten können sich ebenso mit anderen Social Media Plattformen als Ausgangslage befassen, somit könnte hier die Nachverfolgbarkeit von öffentlichen Informationen begutachtet werden sowie mit zusätzlichen Use Cases befassen und diese hervorheben welche für OSINT relevant sind.

Ebenso können sich Arbeiten damit befassen, dass der Fokus auf die TI-Plattformen gelegt wird und in Verbindung mit OSINT-Tools gebracht werden.

Damit können in nachfolgenden Arbeiten die Tools auf Änderungen und Unterschiede in deren Anwendbarkeit, sowie auch deren Analyse und Sammlung von frei zugänglichen Informationen in der Zukunft untersucht werden.

Es können ebenso OSINT Informationen in SIEM (Security Information and Event Management) Lösungen integriert werden und dieses genauer erforscht werden.

Literaturverzeichnis

[1] BSI, „BSI,“ [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf;jsessionid=BE1B42FB04867DA7CD27C94D20DBBAA8.2_cid351?__blob=publicationFile&v=3. [Zugriff am 20 April 2020].

[2] D. Mitchell, „SAS,“ [Online]. Available: https://www.sas.com/de_at/insights/big-data/internet-of-things.html. [Zugriff am 20 April 2020].

[3] K. Gyarmathy, „vxchnge,“ 26 März 2020. [Online]. Available: https://www.vxchnge.com/blog/iot-statistics. [Zugriff am 20 April 2020].

[4] T. R. F. Team, „recordedfuture,“ 19 Februar 2019. [Online]. Available: https://www.recordedfuture.com/open-source-intelligence-definition/. [Zugriff am 20 April 2020].

[5] T. E. Team, „echosec,“ 31 Mai 2019. [Online]. Available: https://www.echosec.net/blog/-5-reasons-why-every-organization-needs-an-osint-team. [Zugriff am 20 April 2020].

[6] „wordstream,“ [Online]. Available: https://www.wordstream.com/articles/google-privacy-internet-privacy. [Zugriff am 20 April 2020].

[7] D. Standard, „derstandard,“ 14 September 2010. [Online]. Available: https://www.derstandard.at/story/1282979677101/usa-einbrecher-spionieren-opfer-ueber-facebook-aus. [Zugriff am 20 April 2020].

[8] krone, „krone,“ 30 Juni 2010. [Online]. Available: https://www.krone.at/207531. [Zugriff am 20 April 2020].

[9] J. Nordine, „osintframework,“ [Online]. Available: https://osintframework.com/. [Zugriff am 20 April 2020].

[10] S. Simon, „bayern3,“ 30 Oktober 2018. [Online]. Available: https://www.bayern3.de/osint-funktion-spionage-tool-inteltechniques. [Zugriff am 20 April 2020].

[11] o.V., „fas,“ [Online]. Available: https://fas.org/irp/nsa/ioss/threat96/part02.htm. [Zugriff am 20 April 2020].

[12] RFSID, „recordedfuture,“ 8 März 2017. [Online]. Available: https://www.recordedfuture.com/threat-intelligence-data/. [Zugriff am 20 April 2020].

[13] J. &. A. C. Richard A. Best, „fas,“ 05 Dezember 2007. [Online]. Available: https://fas.org/sgp/crs/intel/RL34270.pdf. [Zugriff am 20 April 2020].

[14] C. FLEISHER, „phibetaiota,“ 2008. [Online]. Available: https://phibetaiota.net/wp-content/uploads/2013/02/2008-Fleisher-on-OSINT-English-and-Spanish.pdf. [Zugriff am 20 April 2020].

[15] C. L. N. B. E. Kenneth Olmstead, „pewresearch,“ 22 Juni 2015. [Online]. Available: http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/06/PI_2016.06.22_Social-Media-and-Work_FINAL.pdf. [Zugriff am 20 April 2020].

[16] M. Czumak, „securitysift,“ 05 Februar 2014. [Online]. Available: https://www.securitysift.com/passive-reconnaissance/. [Zugriff am 20 April 2020].

[17] R. v. d. Meulen, „gartner,“ 07 Februar 2017. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. [Zugriff am 20 April 2020].

[18] A. J. Weissberger, 09 März 2916. [Online]. Available: https://techblog.comsoc.org/2016/03/09/idc-directions-2016-iot-internet-of-things-outlook-vs-current-market-assessment/. [Zugriff am 20 April 2020].

[19] o.V., „misp-project,“ [Online]. Available: https://www.misp-project.org/index.html. [Zugriff am 20 April 2020].

[20] o.V., „securitymadein," [Online]. Available: https://securitymadein.lu/tools/malware-information-sharing-platform/. [Zugriff am 20 April 2020].

[21] „misp-project feeds," [Online]. Available: https://www.misp-project.org/feeds/. [Zugriff am 20 April 2020].

[22] o.V., „cybersecurity," [Online]. Available: https://cybersecurity.att.com/documentation/usm-appliance/otx/about-otx.htm. [Zugriff am 20 April 2020].

[23] D. Robb, „esecurityplanet," 18 Juli 2017. [Online]. Available: https://www.esecurityplanet.com/products/ibm-x-force-exchange.html. [Zugriff am 20 April 2020].

[24] K. Tietjen, „permalink," 10 Juni 2011. [Online]. Available: https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-11-05782. [Zugriff am 20 April 2020].

[25] M. K. A, „cyware," 17 Juni 2019. [Online]. Available: https://cyware.com/educational-guides/cyber-threat-intelligence/what-is-open-indicators-of-compromise-openioc-framework-ed9d. [Zugriff am 20 April 2020].

[26] P. S. Stefan Luber, „security-insider," 22 Mai 2019. [Online]. Available: https://www.security-insider.de/was-ist-stix-a-830518/. [Zugriff am 20 April 2020].

[27] S. Barnum, „stixproject," 20 Februar 2014. [Online]. Available: https://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf. [Zugriff am 20 April 2020].

[28] „anomali," [Online]. Available: https://www.anomali.com/resources/what-are-stix-taxii. [Zugriff am 20 April 2020].

[29] Y. Demchenko, „ietf," Dezember 2007. [Online]. Available: https://tools.ietf.org/html/rfc5070. [Zugriff am 20 April 2020].

[30] R. Waldner, „cert," 13 März 2019. [Online]. Available: https://cert.at/de/ueber-uns/rfc2350/. [Zugriff am 20 April 2020].

[31] o.V., „circl," [Online]. Available: https://www.circl.lu/mission/. [Zugriff am 20 April 2020].

[32] o.V., „cssa," [Online]. Available: https://www.cssa.de/. [Zugriff am 20 April 2020].

[33] J. Hendricksen, „ru," 26 März 2013. [Online]. Available: https://www.ru.nl/publish/pages/769526/j_hendricksen-profiler-final.pdf. [Zugriff am 20 April 2020].

[34] M. K. V. S. D. G. Lilian Mitrou, „semanticscholar," 2014. [Online]. Available: https://pdfs.semanticscholar.org/4fe7/dde0066940748f3822d88db05014546e8d49.pdf. [Zugriff am 20 April 2020].

[35] P. P. Alexander Pak, „nectec," 2010. [Online]. Available: https://lexitron.nectec.or.th/public/LREC-2010_Malta/pdf/385_Paper.pdf. [Zugriff am 20 April 2020].

[36] M. M. G. F. S. Mariam Adedoyin-Olowe, „arxiv," 2014. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1312/1312.4617.pdf. [Zugriff am 20 April 2020].

[37] P. K. D. V. M. A. J. T. F. Sudip Mittal, „ieee," 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7752338. [Zugriff am 20 April 2020].

[38] E. S. Team, „expertsystem," 24 Februar 2017. [Online]. Available: https://expertsystem.com/advantages-disadvantages-open-source-intelligence/. [Zugriff am 20 April 2020].

[39] M. Colón, „misti," 20 Dezember 2017. [Online]. Available: https://misti.com/infosec-insider/the-pros-and-cons-of-leveraging-osint-tools. [Zugriff am 20 April 2020].

[40] K. Smith, „brandwatch," 03 Januar 2020. [Online]. Available: https://www.brandwatch.com/de/blog/twitter-statistiken/. [Zugriff am 20 April 2020].

[41] „stackoverflow," [Online]. Available: https://stackoverflow.com/. [Zugriff am 20 April 2020].

[42] „github," [Online]. Available: https://github.com/. [Zugriff am 20 April 2020].

[43] D. W. Quirine Eijkman, „cyberwar," 2013. [Online]. Available: https://cyberwar.nl/d/03_Eijkman_Weggemans_v2%5B1%5D_1367418023.pdf. [Zugriff am 20 April 2020].

[44] o.V., „infosecinstitute," 11 Mai 2016. [Online]. Available: https://resources.infosecinstitute.com/the-art-of-searching-for-open-source-intelligence/. [Zugriff am 20 April 2020].

[45] B. Hayes, „cilip," 18 Dezember 2010. [Online]. Available: https://www.cilip.de/2010/12/18/in-einer-durchsichtigen-welt-die-open-source-intelligence-industrie/. [Zugriff am 20 April 2020].

[46] N. A. H. R. Hassan, Open Source Intelligence Methods and Tools, Springer, 2018.

[47] o.V., „e-education," [Online]. Available: https://www.e-education.psu.edu/sgam/node/15. [Zugriff am 20 April 2020].

[48] o.V., „fas," [Online]. Available: https://fas.org/irp/nsa/ioss/threat96/part02.htm#targetText=Intelligence%20Collection%20Disciplines,-Several%20intelligence%20disciplines&targetText=These%20disciplines%20include%20human%20intelligence,open%20source%20intelligence%20(OSINT).. [Zugriff am 20 April 2020].

[49] o.V., „fas," [Online]. Available: https://fas.org/irp/cia/product/facttell/intcycle.htm. [Zugriff am 20 April 2020].

[50] z3roTrust, „medium," 05 November 2018. [Online]. Available: https://medium.com/@z3roTrust/open-source-intelligence-osint-reconnaissance-75edd7f7dada. [Zugriff am 20 April 2020].

[51] D. W. Fahimeh Tabatabaei, OSINT in the Context of Cyber-Security, Springer, 2017.

[52] A. Nurudini, „owasp," 21 Juni 2019. [Online]. Available: https://owasp.org/www-chapter-ghana/assets/slides/OWASP_OSINT_Presentation.pdf. [Zugriff am 21 April 2020].

[53] M. Rouse, „techtarget," 2018. [Online]. Available: https://whatis.techtarget.com/de/definition/Indicator-of-Compromise-IOC. [Zugriff am 21 April 2020].

[54] S. B. Vasileios Mavroeidis, „uio," 2017. [Online]. Available: https://www.duo.uio.no/bitstream/handle/10852/58492/CTI_Mavroeidis%25282017%2529.pdf?sequence=1. [Zugriff am 21 April 2020].

[55] P. S. Stefan Luber, „security-insider," 06 September 2019. [Online]. Available: https://www.security-insider.de/was-ist-ein-indicator-of-attack-a-860141/. [Zugriff am 21 April 2020].

[56] J. DeCianno, „crowdstrike," 09 Dezember 2014. [Online]. Available: https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/. [Zugriff am 21 April 2020].

[57] R. A. M. Tarun Yadav, „arxiv," 10 Juni 2016. [Online]. Available: https://arxiv.org/pdf/1606.03184.pdf. [Zugriff am 21 April 2020].

[58] A. D. K.-K. R. C. J. S. Dennis Kiwia, „arxiv," 2017. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1807/1807.10446.pdf. [Zugriff am 21 April 2020].

[59] S. Mason, „darkreading," 12 Februar 2014. [Online]. Available: https://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810. [Zugriff am 21 April 2020].

[60] P. S. Oliver Schonschek, „security-insider," 19 Mai 2017. [Online]. Available: https://www.security-insider.de/cyber-kill-chain-grundlagen-anwendung-und-entwicklung-a-608017/. [Zugriff am 21 April 2020].

[61] o.V., „mitre," [Online]. Available: https://cve.mitre.org/. [Zugriff am 21 April 2020].

[62] D. Ivan, „infosecinstitute," [Online]. Available: https://resources.infosecinstitute.com/information-gathering/. [Zugriff am 21 April 2020].

[63] o.V., „paloaltonetworks," [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan. [Zugriff am 21 April 2020].

[64] T. Bandos, „digitalguardian," 27 Juli 2017. [Online]. Available: https://digitalguardian.com/blog/building-your-incident-response-team-key-roles-and-responsibilities. [Zugriff am 21 April 2020].

[65] r. i. services, „ecompass," 09 Mai 2013. [Online]. Available: https://list.ecompass.nl/listserv/cgi-bin/wa?A3=ind1512&L=NEDBIB-L&E=base64&P=1518719&B=--001a113fd744a456bd052808a958&T=application%252Fpdf;%2520name=%2522SIGNIFICANCE%2520OF%2520OSINT%2520(1).pdf%2522&N=SIGNIFICANCE%2520OF%2520OSINT%2520(1).pdf&attachme. [Zugriff am 21 April 2020].

[66] T. Praescient, „praescientanalytics," 16 März 2018. [Online]. Available: https://praescientanalytics.com/why-osint-matters-to-the-intelligence-community/. [Zugriff am 21 April 2020].

[67] H. Velez, „secjuice," 03 November 2019. [Online]. Available: https://www.secjuice.com/osint-in-penetration-testing/. [Zugriff am 21 April 2020].

[68] o.V., „libguides," 05 März 2020. [Online]. Available: https://usnwc.libguides.com/c.php?g=494120&p=3381426. [Zugriff am 21 April 2020].

[69] P. Cherkasets, „medium," 07 Mai 2019. [Online]. Available: https://medium.com/the-first-digit/osint-how-to-find-information-on-anyone-5029a3c7fd56. [Zugriff am 21 April 2020].

[70] o.V., „cia," 30 April 2013. [Online]. Available: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html. [Zugriff am 21 April 2020].

[71] J. Pike, „fas," 08 Mai 2000. [Online]. Available: https://fas.org/irp/program/masint.htm. [Zugriff am 21 April 2020].

[72] J. Pike, „fas," 09 März 1997. [Online]. Available: https://fas.org/spp/military/program/sigint/overview.htm. [Zugriff am 21 April 2020].

[73] o.V., „nsa," [Online]. Available: https://www.nsa.gov/what-we-do/signals-intelligence/. [Zugriff am 21 April 2020].

[74] L. K. Donohue, „scholarship," 2015. [Online]. Available: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2540&context=facpub. [Zugriff am 21 April 2020].

[75] M. SA, „monitorulapararii," Mediafax SA, 01 Oktober 2019. [Online]. Available: https://en.monitorulapararii.ro/from-osint-to-socint-how-social-media-is-turning-into-a-battlefield-between-intelligence-agencies-and-society-1-23365. [Zugriff am 21 April 2020].

[76] o.V., „techopedia," 1 Februar 2017. [Online]. Available: https://www.techopedia.com/definition/76/targeted-attack. [Zugriff am 21 April 2020].

[77] „techopedia," 27 März 2020. [Online]. Available: https://www.techopedia.com/definition/26361/hacking. [Zugriff am 21 April 2020].

[78] J. Kagan, „investopedia," 11 August 2019. [Online]. Available: https://www.investopedia.com/terms/i/identitytheft.asp. [Zugriff am 21 April 2020].

[79] o.V., „flashcardmachine," 01 Januar 2014. [Online]. Available: https://www.flashcardmachine.com/cissp-attacktypes.html. [Zugriff am 21 April 2020].

[80] o.V., „techopedia," [Online]. Available: https://www.techopedia.com/definition/6712/cyberterrorism. [Zugriff am 21 April 2020].

[81] K. Kiener-Manu, „unodc," [Online]. Available: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html. [Zugriff am 21 April 2020].

[82] R. Joseph, „avg," 11 Juli 2019. [Online]. Available: https://www.avg.com/en/signal/what-is-malware. [Zugriff am 21 April 2020].

[83] NortonLifeLock, „norton," [Online]. Available: https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html. [Zugriff am 21 April 2020].

[84] A. G. Johansen, „norton," [Online]. Available: https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html. [Zugriff am 21 April 2020].

[85] M. Rouse, „computerweekly," Dezember 2016. [Online]. Available: https://www.computerweekly.com/de/definition/Scareware. [Zugriff am 21 April 2020].

[86] M. Landesman, „lifewire," 17 Juni 2019. [Online]. Available: https://www.lifewire.com/what-are-adware-and-spyware-153403. [Zugriff am 21 April 2020].

[87] NortonLifeLock, „norton," [Online]. Available: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html. [Zugriff am 21 April 2020].

[88] o.V., „techopedia," 28 September 2012. [Online]. Available: https://www.techopedia.com/definition/4157/virus. [Zugriff am 21 April 2020].

[89] F.-S. Deutschland, „f-secure," 11 Jänner 2017. [Online]. Available: https://blog.f-secure.com/de/wie-findet-man-die-grundlegenden-probleme-bei-attacken/. [Zugriff am 21 April 2020].

[90] G. Jacquart, „medium," 06 April 2018. [Online]. Available: https://medium.com/@guillaumejacquart/targeted-and-opportunistic-attacks-292e6db587b9. [Zugriff am 21 April 2020].

[91] B. Hendricks, „study," 18 Juli 2018. [Online]. Available: https://study.com/academy/lesson/vandalism-in-digital-crime-types-evidence.html#lesson. [Zugriff am 21 April 2020].

[92] o.V., „techopedia," 28 Mai 2012. [Online]. Available: https://www.techopedia.com/definition/14326/cyberstalking. [Zugriff am 21 April 2020].

[93] G. H. Brian H. Spitzberg, „semanticscholar," 2002 . [Online]. Available: https://www.semanticscholar.org/paper/Cyberstalking-and-the-technologies-of-interpersonal-Spitzberg-Hoobler/84272e9ade137f5886debe4cd7cd39998fc7cf9c. [Zugriff am 21 April 2020].

[94] P. S. Stefan Luber, „security-insider," 02 April 2018. [Online]. Available: https://www.security-insider.de/was-ist-spam-a-700767/. [Zugriff am 21 April 2020].

[95] I. Location, „iplocation," 18 November 2018. [Online]. Available: https://www.iplocation.net/arp-spoofing. [Zugriff am 21 April 2020].

[96] S. Augsten, „security-insider," 15 März 2012. [Online]. Available: https://www.security-insider.de/domain-hijacking-verhindern-verisign-gibt-tipps-a-356667/. [Zugriff am 21 April 2020].

[97] o.V., „imperva," [Online]. Available: https://www.imperva.com/learn/application-security/dns-flood/. [Zugriff am 21 April 2020].

[98] o.V., „itwissen," 05 Juli 2016. [Online]. Available: https://www.itwissen.info/DRDoS-distributed-reflective-denial-of-service-DRDoS-Attacke.html. [Zugriff am 21 April 2020].

[99] M. t. Robot, „kaspersky," 31 Juli 2015. [Online]. Available: https://www.kaspersky.de/blog/exploits-problem-explanation/5905/. [Zugriff am 21 April 2020].

[100] S. Carruthers, „mindpointgroup," [Online]. Available: https://www.mindpointgroup.com/wp-content/uploads/2018/04/Social-Engineering-Part-Two-OSINT.pdf. [Zugriff am 21 April 2020].

[101] G. Gilead, „incentive-il," 14 November 2018. [Online]. Available: https://www.incentive-il.com/single-post/2018/11/14/Tips-and-Trends-in-Open-Source-Intelligence. [Zugriff am 21 April 2020].

[102] Datorama, „onlinemarketing," 30 Juli 2018. [Online]. Available: https://onlinemarketing.de/unternehmensnews/was-versteht-man-unter-marketing-intelligence. [Zugriff am 21 April 2020].

[103] A. Ng, „cnet," 21 Dezember 2019. [Online]. Available: https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk/. [Zugriff am 21 April 2020].

[104] M. Tanjim, „itsfoss," 01 Jänner 2020. [Online]. Available: https://itsfoss.com/linux-hacking-penetration-testing/. [Zugriff am 21 April 2020].

[105] M. Bazzell, „inteltechniques," [Online]. Available: https://inteltechniques.com/buscador/. [Zugriff am 21 April 2020].

[106] M. Bazzell, „inteltechniques," [Online]. Available: https://inteltechniques.com/book1.html. [Zugriff am 21 April 2020].

[107] wondersmith_rae, „medium," 07 August 2019. [Online]. Available: https://medium.com/@raebaker/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc. [Zugriff am 21 April 2020].

[108] V. Kumar, „cyberpratibha," 16 Jänner 2020. [Online]. Available: https://www.cyberpratibha.com/information-gathering-with-maltego/. [Zugriff am 21 April 2020].

[109] J. Weber, „corma," 01 Februar 2020. [Online]. Available: https://corma.de/serie-3-unentbehrliche-maltego-transformationen-fuer-osint-und-ermittlungen/. [Zugriff am 21 April 2020].

[110] o.V., „maltego," 30 Jänner 2020. [Online]. Available: https://www.maltego.com/changelog/?utm_source=paterva.com&utm_medium=referral&utm_campaign=301. [Zugriff am 21 April 2020].

[111] o.V., „maltego," 2019. [Online]. Available: https://buy.maltego.com/shop/page/adaf0f4e-d531-45a1-8645-d63e9ea60fcc. [Zugriff am 21 April 2020].

[112] „haveibeenpwned," [Online]. Available: https://haveibeenpwned.com/. [Zugriff am 21 April 2020].

[113] C. Martorella, „github," 2020. [Online]. Available: https://github.com/laramies/theHarvester. [Zugriff am 21 April 2020].

[114] M. Rouse, „searchnetworking," Februar 2017. [Online]. Available: https://searchnetworking.techtarget.com/definition/host. [Zugriff am 21 April 2020].

[115] o.V., „shodan," 2020. [Online]. Available: https://www.shodan.io/. [Zugriff am 21 April 2020].

[116] o.V., „kali," [Online]. Available: https://tools.kali.org/information-gathering/recon-ng. [Zugriff am 21 April 2020].

[117] J. Turla, „infosecinstitute," [Online]. Available: https://resources.infosecinstitute.com/awesome-modules-of-recon-ng-used-for-web-recon-testing/. [Zugriff am 21 April 2020].

[118] D. S. Ishan Girdhar, „packtpub," April 2017. [Online]. Available: https://subscription.packtpub.com/book/networking_and_servers/9781783982165/5/ch05lvl1sec45/setting-up-api-keys-for-recon-ng. [Zugriff am 21 April 2020].

[119] o.V., „goblinsecurity," 08 September 2017. [Online]. Available: https://goblinsecurity.blogspot.com/2017/09/domain-discovery-techniques-and-recon.html. [Zugriff am 21 April 2020].

[120] „nagios," [Online]. Available: https://www.nagios.org/. [Zugriff am 21 April 2020].

[121] C. Lyne, „exploit-db," 22 Jänner 2019. [Online]. Available: https://www.exploit-db.com/exploits/46221. [Zugriff am 21 April 2020].

[122] „cvedetails," [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-1424/Nagios.html. [Zugriff am 21 April 2020].

[123] „fedoraproject," [Online]. Available: https://docs.fedoraproject.org/en-US/Fedora/11/html/Security_Guide/sect-Security_Guide-Common_Exploits_and_Attacks.html. [Zugriff am 21 April 2020].

[124] o.V., „cvedetails," [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-7696/Mahara.html. [Zugriff am 21 April 2020].

[125] o.V., „exploitalert," 2020. [Online]. Available: https://www.exploitalert.com/search-results.html?search=wordpress. [Zugriff am 21 April 2020].

[126] o.V., „cvedetails," 2019. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-35646/Microsoft-Skype.html. [Zugriff am 21 April 2020].

[127] o.V., „cvedetails," 2019. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-25412/Cisco-Jabber.html. [Zugriff am 21 April 2020].

[128] o.V., „cvedetails," 2019. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-3578/product_id-8170/Atlassian-Jira.html. [Zugriff am 21 April 2020].

[129] Jason, „stuffjasondoes," 17 November 2018. [Online]. Available: http://stuffjasondoes.com/2018/07/18/information-gathering-part-ii-recon-ng/. [Zugriff am 21 April 2020].

[130] HackingLoops, „hackingloops," 2020. [Online]. Available: https://www.hackingloops.com/spiderfoot/. [Zugriff am 21 April 2020].

[131] S. Micallef, „spiderfoot," [Online]. Available: https://www.spiderfoot.net/. [Zugriff am 21 April 2020].

[132] o.V., „greycampus," [Online]. Available: https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking. [Zugriff am 21 April 2020].

[133] o.V., „spiderfoot," [Online]. Available: https://www.spiderfoot.net/documentation/. [Zugriff am 21 April 2020].

[134] S. Micallef, „github," 2020. [Online]. Available: https://github.com/smicallef/spiderfoot. [Zugriff am 21 April 2020].

[135] S. Micallef, „spiderfoot," 26 Jänner 2020. [Online]. Available: https://www.spiderfoot.net/spiderfoot-3-0-open-source-release/. [Zugriff am 21 April 2020].

[136] S. Micallef, „spiderfoot," 2020. [Online]. Available: https://www.spiderfoot.net/hx/. [Zugriff am 21 April 2020].

[137] o.V., „n0where," [Online]. Available: https://n0where.net/open-source-intelligence-automation-spiderfoot. [Zugriff am 21 April 2020].

[138] V. A. Diaz, „tinfoleak," 2020. [Online]. Available: https://tinfoleak.com/. [Zugriff am 21 April 2020].

[139] moc9, „moc9," [Online]. Available: https://moc9.com/tinfoleak-lets-you-gather-personal-details-twitter-account. [Zugriff am 21 April 2020].

[140] Twitter, „twitter," [Online]. Available: https://help.twitter.com/de/safety-and-security/how-to-make-twitter-private-and-public. [Zugriff am 21 April 2020].

[141] M. Bazzell, „inteltechniques," [Online]. Available: https://inteltechniques.com/books.html. [Zugriff am 21 April 2020].

[142] Metasploit, „metasploit," [Online]. Available: https://www.metasploit.com/. [Zugriff am 21 April 2020].

[143] Cloudflare, „cloudflare," [Online]. Available: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/. [Zugriff am 21 April 2020].

[144] Radware, „radware," 2019. [Online]. Available: https://security.radware.com/ddos-knowledge-center/ddospedia/amplification-attack/. [Zugriff am 21 April 2020].

[145] Imperva, „imperva," [Online]. Available: https://www.imperva.com/learn/application-security/dns-amplification/. [Zugriff am 21 April 2020].

[146] Cloudflare, „cloudflare," [Online]. Available: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/. [Zugriff am 21 April 2020].

[147] A. Kesavan, „thousandeyes," 15 November 2016. [Online]. Available: https://blog.thousandeyes.com/three-types-ddos-attacks/. [Zugriff am 21 April 2020].

[148] o.V., „dnsstuff," 17 September 2019. [Online]. Available: https://www.dnsstuff.com/prevent-ddos-attack. [Zugriff am 21 April 2020].

[149] B. Dobran, „phoenixnap," 10 September 2018. [Online]. Available: https://phoenixnap.com/blog/prevent-ddos-attacks. [Zugriff am 21 April 2020].

[150] Reply, „reply," [Online]. Available: https://www.reply.com/Documents/10943_img_SYTR12_Prevent_DDoS_attacks.pdf. [Zugriff am 21 April 2020].

[151] G. Team, „globallearningsystems," 14 Jänner 2014. [Online]. Available: https://www.globallearningsystems.com/the-dangers-of-phishing-scams-and-how-to-protect-yourself/. [Zugriff am 21 April 2020].

[152] 9. Firms, „99firms," 2020. [Online]. Available: https://99firms.com/blog/how-many-email-users-are-there/. [Zugriff am 21 April 2020].

[153] Verizon, „verizon," 2019. [Online]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. [Zugriff am 21 April 2020].

[154] Imperva, „imperva," [Online]. Available: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/. [Zugriff am 21 April 2020].

[155] Brandwatch, „brandwatch," 02 Jänner 2020. [Online]. Available: https://www.brandwatch.com/blog/twitter-stats-and-statistics/. [Zugriff am 21 April 2020].

[156] S. khan, „hackernoon," 22 März 2019. [Online]. Available: https://hackernoon.com/the-default-settings-on-your-social-media-ffdd5fc8d6a5. [Zugriff am 21 April 2020].

[157] C. Kumar, „geekflare," 27 September 2019. [Online]. Available: https://geekflare.com/github-credentials-scanner/. [Zugriff am 21 April 2020].

[158] D. Bradbury, „sophos," 25 März 2019. [Online]. Available: https://nakedsecurity.sophos.com/2019/03/25/thousands-of-coders-are-leaving-their-crown-jewels-exposed-on-github/. [Zugriff am 21 April 2020].

[159] D. Johnson, „bleepingworld," 22 Mai 2018. [Online]. Available: https://www.bleepingworld.com/delete-question-on-stack-overflow/. [Zugriff am 21 April 2020].

[160] S. Mills, „microfocus," 05 Juni 2014. [Online]. Available: https://blog.microfocus.com/social-media-in-the-workplace-the-risks/. [Zugriff am 21 April 2020].

[161] S. Mills, „microfocus," 23 Jänner 2017. [Online]. Available: https://blog.microfocus.com/social-media-in-the-workplace-benefits-and-growth/. [Zugriff am 21 April 2020].

[162] Twitter, „twitter," [Online]. Available: https://help.twitter.com/de/safety-and-security/tweet-location-settings. [Zugriff am 21 April 2020].

[163] M. C. Libicki, „dtic," August 1995. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a367662.pdf. [Zugriff am 21 April 2020].

[164] S. Zeitung, „vsp-vernetzt," 31 August 2000. [Online]. Available: http://www.vsp-vernetzt.de/soz/001803.htm. [Zugriff am 21 April 2020].

[165] T. S. Gherghina OLARU, „afahc," 17 Mai 2018. [Online]. Available: http://www.afahc.ro/ro/rcic/2018/rcic'18/volum_2018/391-396%20Olaru%20Stefan.pdf. [Zugriff am 21 April 2020].

[166] D. Polman, „whyy," 03 April 2019. [Online]. Available: https://whyy.org/articles/fake-news-fraud-alex-jones-suffers-his-day-of-reckoning/. [Zugriff am 21 April 2020].

[167] S. Salinas, „cnbc," 06 September 2018. [Online]. Available: https://www.cnbc.com/2018/09/06/twitter-permanently-bans-alex-jones-and-infowars-accounts.html. [Zugriff am 21 April 2020].

[168] R. F. A. K. R. K. N. Nic Newman, „reutersinstitute," 2019. [Online]. Available: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/inline-files/DNR_2019_FINAL.pdf. [Zugriff am 21 April 2020].

[169] o.V., „30secondes," [Online]. Available: https://30secondes.org/en/module/what-is-fake-news/. [Zugriff am 21 April 2020].

[170] A. E. Waldman, „scholarship," März 2018. [Online]. Available: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1661&context=jcl. [Zugriff am 21 April 2020].

[171] H. G. Douglas Wells, „shu,“ 2017. [Online]. Available: http://shura.shu.ac.uk/17412/2/OSINT_EASS.pdf. [Zugriff am 21 April 2020].

[172] M. Abadicio, „emerj,“ 08 Mai 2019. [Online]. Available: https://emerj.com/ai-sector-overviews/big-data-military/. [Zugriff am 21 April 2020].

[173] R. D. Steele, „oss,“ 2004. [Online]. Available: http://www.oss.net/dynamaster/file_archive/090709/20c7eb99750563642ebee2b6d545eb1c/STRATINT%20OSINT%20MIL.pdf. [Zugriff am 21 April 2020].

[174] A. NAINI, „geekflare,“ 06 September 2019. [Online]. Available: https://geekflare.com/osint-tools/. [Zugriff am 21 April 2020].

[175] H. Passi, „greycampus,“ 24 September 2018. [Online]. Available: https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools. [Zugriff am 21 April 2020].

[176] M. Foster, „mustips,“ 08 September 2019. [Online]. Available: https://www.mustips.com/10-extremely-useful-open-source-intelligence-osint-tools/. [Zugriff am 21 April 2020].

[177] o.V., „latesthackingnews,“ 18 November 2019. [Online]. Available: https://latesthackingnews.com/2019/11/18/6-osint-tools-that-make-a-pentesters-life-easier/. [Zugriff am 21 April 2020].

[178] o.V., „infosecinstitute,“ 17 Februar 2018. [Online]. Available: https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/. [Zugriff am 21 April 2020].