Hochschule Wismar
University of Applied Sciences Technology, Business and Design
Fakultät für Ingenieurwissenschaften

Master-Thesis

Strategie und Anwendung von Open Source Intelligence zur vorbeugenden Aufklärung von Angriffsflächen im Bereich der IT-Sicherheit

von: A.I.S.

Aufgabenstellung

Die Master-Thesis soll verschiedene Quellen, Softwares und Tools, die ihren Einsatz im Bereich OSINT finden können, identifizieren, anhand von festgelegten Kriterien bewerten und miteinander vergleichen. Weiterhin sollen die analysierten Quellen, Softwares und Tools in eine Strategie integriert werden. Sie soll auf dem Konzept des Intelligence Cycles aufgebaut werden, sodass die untersuchten Objekte (Softwares und Tools) mindestens einer Phase des Intelligence Cycles zugeordnet werden können. Die Strategie soll dem Leser eine Übersicht über eine strukturierte Vorgehensweise bei der passiven Informationssammlung anbieten. Mit Hilfe der Strategie soll die Angriffsfläche, die in der Reconnaissance-Phase der Cyber Kill Chain erkundet wird, strukturiert analysiert werden können. Weiterhin sollen die Vorgehensweise und die festgelegten Kriterien bei der Bewertung und Klassifizierung von neuen Softwares und Tools als Grundlage dienen können.

Kurzfassung

Die vorliegende Thesis beschäftigt sich mit der passiven Informationsbeschaffung mittels Open Source Intelligence und deren Einsatz zur vorbeugenden Aufklärung von Angriffsflächen im Bereich der IT-Sicherheit. Zuerst werden die Grundlagen zur Open Source Intelligence und IT-Sicherheit vermittelt. Als Nächstes werden die klassischen Strategien (Intelligence Cycle, F3EAD und OODA Loop) zur Gewinnung von Informationen näher betrachtet. Auf Basis des MITRE ATT&CK-Frameworks werden Kriterien zur Erstellung eines Bewertungsschemas ermittelt. Auf der Grundlage des Bewertungsschemas werden die Tools *SpiderFoot*, *Maltego*, *Recon-ng* und *theHarvester* analysiert, miteinander verglichen und den Phasen des Intelligence Cycles zugeordnet. Das Schema kann zur Evaluation weiterer Softwares und Tools verwendet werden. Im nächsten Schritt stellt die Arbeit eine Strategie dar, die auf dem Intelligence Cycle aufbaut und als Grundlage zur Aufklärung von Angriffsflächen dienen kann. Mithilfe dieser Strategie sollen Elemente der Reconnaissance-Phase der Cyber Kill Chain erkannt werden, um dem Anwender eine Übersicht der Angriffsfläche einer IT-Landschaft zu liefern. Die Anwendung der Strategie wird anhand von praktischen Beispielen überprüft.

Abstract

This thesis covers open source intelligence as a preventive method of passively gathering information on the attack surface of informatical systems. At first, the basics of open source intelligence and IT security are being presented. Next, three classical strategies for gathering information, the *intelligence cycle*, *F3EAD* and the *OODA loop*, are being examined in detail to determine if one of the last two could be an alternative to the intelligence cycle. Afterwards an evaluation scheme containing criteria extracted from the *MITRE ATT&CK framework* is being used to analyze and compare the tools *SpiderFoot*, *Maltego*, *Recon-ng* and *theHarvester*. At the same time, every one of these tools are being assigned to the phases of the intelligence cycle. The created scheme can be used to evaluate further software and tools which are not part of this thesis. Furthermore, a strategy built on the intelligence cycle will be presented. This strategy can be used as a foundation to conduct reconnaissance of attack surfaces of IT systems and it will provide the reader with an overview of the gathered elements from the targeted IT landscape. The use of the strategy will be proved by verifying it through practical examples.

Inhaltsverzeichnis

1 Einleitung

1.1 Ausgangslage und Forschungsstand

Durch die zunehmende Digitalisierung in allen Lebensbereichen wächst auch die Bedrohung durch Angriffe auf IT-Infrastrukturen. Ziel von Cyberangriffen können sowohl kleine, einfache Infrastrukturen, z.B. die Netzwerke kleiner Firmen, als auch hochkomplexe IT-Landschaften sein, beispielsweise im Bereich der kritischen Infrastrukturen. Dies kann erhebliche Konsequenzen für die Gesellschaft haben. Bei Cyberangriffen, seien es einfache, automatisierte Angriffe oder hochkomplexe, gut vorbereitete und gezielte Angriffe durch sogenannte APTs, können als Startpunkt öffentlich zugängliche Informationen genutzt werden. Die Daten, die im Rahmen der Digitalisierung entstehen, können zu einer Erhöhung der Angriffsfläche führen. Um die mögliche Angriffsfläche minimieren zu können, ist die rechtzeitige Erkennung der Elemente dieser Angriffsfläche nötig.
Gemäß einem Bericht des IT-Sicherheitsunternehmens ESET, zählen zu öffentlich verfügbaren Informationen technische Systemdaten über offene Ports, unsichere vernetzte Geräte, ungepatchte Softwares, Informationen zu eingesetzten Geräten und Softwares oder auf GitHub oder Pastebin unwissend veröffentlichte Sourcecodes [1]. Weiterhin können dazu Daten, die im Bereich von Social Media erworben werden können, gehören. Somit lassen sich diverse Angriffsszenarien, wie z.B. Spear-Phishing-Angriffe, realisieren[1]. Ein Beispiel für Informationen, die ausgekundschaftet werden können, sind RDP-Dienste. Laut einer Studie aus dem Jahr 2020 der IT-Sicherheitsfirma Palo Alto Networks waren im Jahr 2019 offene und nicht gut gesicherte RDP-Dienste für 50% der Angriffe mit Ransomware verantwortlich[2, S. 12].
NATO beschreibt den Prozess der Erzeugung von Erkenntnissen aus öffentlichen Quellen (eng. open sources) als Open Source Intelligence oder kurz OSINT[3, S. 17]. Im Bereich der IT-Sicherheit hat sich Open Source Intelligence als Mittel zur Informationssammlung aus öffentlichen Quellen etabliert. Oft wird der Begriff im Zusammenhang mit der von Lockheed Martin entwickelten Cyber Kill Chain gebracht. Bei

der Cyber Kill Chain handelt es sich um ein Modell zur Beschreibung von Cyberangriffen. Das Modell besteht aus sieben Phasen: Reconnaissance (dt. Aufklärung), Weaponization (dt. Bewaffnung), Delivery (dt. Zustellung), Exploitation (dt. Ausnutzung), Installation (dt. Installation), Command & Control (C2) (dt. Führung) und actions on objectives (Zielerreichung)[4]. Open Source Intelligence findet vor allem während der Reconnaissance-Phase Anwendung. Hierzu kommen verschiedene Tools und Methoden zum Einsatz, mit denen wiederum Informationen aus verschiedenen Quellenarten gewonnen werden können[5, o.S.]. Zu den Quellen können das Clear, Deep oder Dark Web gehören. Die gewonnenen Informationen können anhand des Intelligence Cycles abgearbeitet werden. Bei dem Intelligence Cycle handelt es sich um eine in fünf Phasen strukturierte Vorgehensweise zur Abarbeitung von Daten, sodass zum Schluss ein Produkt entsteht, das einem ursprünglich geplanten Zweck dient[6, S. 1 ff.]. Das Thema OSINT ist in der Vergangenheit oft Thema verschiedener Analysen, Bücher und akademischer Arbeiten gewesen.

1.2 Forschungsfrage

Die vorliegende Masterarbeit soll eine strukturierte, wissenschaftlich aufgearbeitete Antwort auf die folgende Frage liefern:

Können Quellen, Softwares und Tools in eine auf dem Intelligence Cycle basierende Strategie integriert werden, sodass eine strukturierte Vorgehensweise mittels Open Source Intelligence bei der Erkennung der Angriffsflächen einer IT-Infrastruktur möglich wird?

1.3 Zielgruppe

Das Ergebnis der Masterarbeit soll IT-Fachleute, IT-Sicherheitsexperten und Systemadministratoren bei der passiven Erkundung von Angriffsflächen der untersuchten IT-Infrastruktur mit einer Strategie unter Anwendung von OSINT-Quellen, -Tools und -Softwares unterstützen.

1.4 Abgrenzung

In dieser Studie wird hauptsächlich das Thema Open Source Intelligence mit Bezug auf die IT-Sicherheit behandelt. Es werden Softwares, Tools und Quellen, die nur im

Bereich der passiven Informationssammlung genutzt werden können, untersucht. Es werden keine aktiven Techniken (z.B. Port-Scanning) angewandt. Weitere Themen, wie z.B. die Nutzung von OSINT zur Personen-Suche oder Sammlung von öffentlich zugänglichen Firmeninformationen (z.B. Bilanzen etc.) sind nicht Bestandteile dieser Arbeit.

1.5 Methodik

Die Aufbereitung und Strukturierung der benötigten Informationen werden mittels Literaturrecherche, unter Betrachtung von akademischen Arbeiten, Büchern, Handbüchern, Katalogen, Statistiken sowie Online-Quellen erfolgen. Die Quellen, Tools und Softwares, die von besonderem Interesse für Open Source Intelligence sind, werden in dieser Arbeit anhand festgelegter Kriterien in einer Testumgebung mithilfe von Testdaten bewertet und miteinander verglichen.

2 Grundlage

2.1 Definition Intelligence

„Intelligence means Knowledge“ - so beschreibt Sherman Kent in seinem Buch ‚Strategic Intelligence for American World Policy‘ den Begriff *Intelligence*[7, S. 3]. Das Wissen entsteht in Folge eines mehrphasigen Prozesses, der Informationen sammelt, analysiert und in einen Kontext bringt. Das Ergebnis sagt ein Verhalten voraus und enthält Handlungsempfehlungen [8]. Der Begriff *Intelligence* wird mit Nachrichtendiensten in Verbindung gebracht. Der Bundesnachrichtendienst gewinnt Informationen aus unterschiedlichen Quellen, auch All-Source-Intelligence genannt, um der Bundesregierung einen Wissensvorsprung zu sichern[9]. Die Quellen können in mehreren klassischen Aufkommensarten klassifiziert werden. Beispielsweise gibt es die folgenden Arten[9][10, S. B-2]:

- GEOINT - Geospatial Intelligence: Informationsbeschaffung aus Satelliten (Satellitenbilder, Geodaten etc.)[10, S. B-2].
- HUMINT - Human Intelligence: Informationsbeschaffung aus menschlichen Quellen, Ausschöpfung von Gesprächen etc.[10, S. B-2].
- SIGINT - Signals Intelligence: Beschaffung durch Auswertung von elektronischen Signalen (z.B. Radar, Funksignale etc.)[9][10, S. B-2].
- MASINT - Measurement and Signature Intelligence: Informationen werden aus elektromagnetischen Daten, Radardaten, Funksignalen etc. beschafft[10, S. B-2].
- TECHINT - Technical Intelligence: Informationen werden beispielsweise aus wissenschaftlicher Forschung gesammelt[10, S. B-2].
- OSINT - Open Source Intelligence: Informationen werden aus öffentlichen Quellen beschafft[9][10, S. B-2].

2.1.1 Stufen der Intelligence

Abhängig vom Ziel der Gewinnung von Informationen aus öffentlichen Quellen kann zwischen drei grundlegenden Stufen der Intelligence unterschieden werden[8][11, S. 24 f.].

Taktische Intelligence

Die taktische Intelligence unterstützt operationale Gruppen. Dazu gehören beispielsweise die Analysten eines Security Operation Centers oder die Spezialisten eines Incident-Response-Teams. Ein Beispiel für taktische Intelligence ist im Bereich der IT-Sicherheit der IoC, der Indicator of Compromise. Der IoC kann eine IP-Adresse, eine Domäne oder hostbasierte Artefakte wie Hashwerte enthalten.Vergleichsweise wird die taktische Intelligence im militärischen Bereich von kleinen Einheiten eingesetzt[11, S. 24].

Operationale Intelligence

Die operationale Intelligence erweitert die gewonnenen Erkenntnisse aus der taktischen Intelligence. Im Bereich der IT-Sicherheit fließen dahin Informationen über angehende Kampagnen, die Attributionen von Angriffen einem spezifischen Akteur oder Tactics, Techniques and Procedures (TTPs). Vergleichsweise werden in dem militärischen Bereich Informationen über die Logistik eines Gegners eingegliedert [8] [11, S. 24].

Strategische Intelligence

Die strategische Intelligence unterstützt die Entscheidungsträger auf der höchsten Ebene, beispielsweise den Chief Information Security Officer oder den CTO. Im militärischen Bereich dient sie zur Benachrichtigung der Führungsebene auf nationalem Niveau. Es geht dabei um Informationen, die eine Übersicht über die aktuelle Lage und das Geschehen verschaffen[8][11, S. 25].

2.1.2 Grade der Zuverlässigkeit von Informationen

Um die Zuverlässigkeit von Informationen zu bewerten, muss zwischen der Bewertung der Quelle und der Bewertung des Ergebnisses eines Analysten unterschieden werden. Dazu kann eine Skala mit statistischen Methoden berechnet werden oder basierend auf der Interpretation eines Analysten verwendet werden[11, S. 25]. Die Bewertungsskala nach Sherman Kent ist wie folgt aufgebaut:

Tabelle 1: Abschätzungswahrscheinlichkeit nach Sherman Kent

100% certainty			
The General Area of Possibility	93%	Give or take almost 6%	Almost certain
	75%	Give or take about 12%	Probable
	50%	Give or take about 10%	Chances about even
	30%	Give or take about 10%	Probably not
	7%	Give or take about 5%	Almost certainly not
0% Impossibility			

Quelle: in Anlehnung an der Abschätzungswahrscheinlichkeit nach Sherman Kent[12, o.S.]

2.2 Von Open Source Data über Information bis zur Intelligence

In diesem Kapitel werden die Begrifflichkeiten Open Source Data, Open Source Information und Open Source Intelligence vorgestellt. Die Erläuterung soll dem Leser die Unterschiede sowie den Zusammenhang der Begriffe präsentieren.

2.2.1 Open Source Data

Das NATO Open Source Intelligence Handbook bezeichnet als Open Source Data (OSD) die öffentlichen Rohdaten, die in sämtlichen Formen (gedruckt, mündlich, etc.) in einer Primärquelle vorliegen. Gute Beispiele dafür sind Bilder, Tonbandaufnahmen oder Satellitenbilder [13, S. 2]. Bei den Rohdaten handelt es sich um Daten, die keinen Kontext oder keine Bedeutung haben. In der Informationstechnologie könnten als Rohdaten beispielsweise eine Port-Nummer (z.B. Portnummer 80) oder eine IP-Adresse (192.168.1.2) betrachtet werden. Wenn von diesen Arten von Daten keine Analyse vorgenommen wird, haben sie an sich keine Bedeutung, sie repräsentieren eine Zahlenfolge. Erst im nächsten Schritt könnten die Daten in

Informationen prozessiert werden[14, S. 6].
Es wird zwischen unstrukturierten, teil-strukturierten und strukturierten Daten unterschieden. Während eines OSINT-Prozesses haben die gesammelten Daten überwiegend ein unstrukturiertes Format. Bei diesem Typ kann es sich um Daten, die aus Büchern, Videos, Webseiten stammen, oder andere von Maschinen schwer verarbeitete Daten handeln. Zu den teil-strukturierten Daten können RSS-Feeds, XML/JSON-Dateien oder Daten, die via APIs beschafft werden, gehören. Zu den strukturierten Daten zählen Datenmodelle oder Datenbanken[15, S. 73 - 74].

2.2.2 Open Source Information

Als Open Source Information (OSIF) werden öffentlich verfügbare komprimierte Daten bezeichnet, die durch einen redaktionellen Prozess zusammengesetzt, gefiltert und validiert werden, sodass sie für den Abnehmer eine Bedeutung haben. Beispiele dafür sind Zeitungsartikel, Bücher oder im Bereich der Informationstechnologie eine IP-Port-Kombination[13, S. 2]. Die Zusammensetzung einer Port-Nummer (192.168.1.2:80) zu einer IP-Adresse, also die Zusammensetzung zweier Rohdaten, wird als Socket bezeichnet und liefert eine Information[16, S. 52]. Als vertiefende Erklärung dafür kann das Beispiel des Betriebssystems Linux dienen. Ein Dämonprozess hat die Aufgabe, auf dem assoziierten Port auf eingehende Nachrichten zu lauschen, um diese nachträglich dem zugeordneten Dienst zuzuweisen[17, S. 113]. Somit würde eine IP-Port-Kombination unmittelbar Auskunft über die Dienste, die auf dem betroffenen Rechner laufen, liefern. Sind diese Informationen aus dem Internet aufrufbar, handelt es sich per Definition um Open Source Information.

2.2.3 Open Source Intelligence

Unter dem Begriff Open Source Intelligence (OSINT) wird eine Ansammlung von Informationen verstanden, die zur Beantwortung einer spezifischen Frage gezielt gesammelt, validiert, analysiert und in einem Intelligence-Produkt zusammengefasst werden. Sie basiert somit auf offenen Informationsquellen und schafft Erkenntnisse[13, S. 2]. Das Produkt muss für eine bestimmte Zielgruppe umgesetzt werden können[14, S. 7]. Wird das Beispiel Socket weiterverfolgt, ist festzustellen, dass, nach einer Analyse des Sockets, die Portnummer 80 zu den Well-Known Ports gehört und von einem HTTP-Dienst verwendet wird[17, S. 114]. Mit dem HTTP-Protokoll können Inhalte auf einem Webserver aufgerufen werden. Es ist also die Erkenntnis gewonnen, dass auf dem betroffenen Rechner ein Webserver läuft. Außerdem ist

klar, dass es sich bei HTTP nicht um eine sichere, verschlüsselte Verbindung handelt, sondern dass die Kommunikation abgehört werden kann[17, S. 151 ff.]. Wenn die Zielgruppe aus IT-Administratoren besteht, würden sie die nötigen Maßnahmen treffen, um den Webserver abzusichern. Das Intelligence-Produkt hat somit seine Zielgruppe erreicht und wurde von dieser umgesetzt.

2.2.4 Bestätigte Open Source Intelligence

Das NATO Handbook beschreibt einen weiteren Intelligence-Typ, die bestätigte Intelligence (OSINT-V). Es handelt sich dabei um eine Intelligence, die einen hohen Grad an Gewissheit hat. Um OSINT zu validieren, kann auf All-Source-Intelligence zurückgegriffen werden, also eine Sammlung von Erkenntnissen, die aus mehreren Intelligence-Typen stammen und übereinstimmende Resultate liefern[13, S. 3].

2.3 Einsatzgebiete

2.3.1 Staatliche Stellen

Open Source Intelligence kommt ursprünglich aus der Welt der Nachrichtendienste, wird heutzutage aber branchenübergreifend eingesetzt. Der Bundesnachrichtendienst wertet offene Informationen mittels spezieller Recherche-Tools aus, um aus einer Informationsflut relevante Inhalte für das Aufgabenspektrum des BND zu extrahieren. Die Auswertung von Informationen aus öffentlichen Quellen steht am Anfang der nachrichtendienstlichen Arbeit und beträgt 80-90% der Gesamtmenge der Informationen[9][18, S. 175]. Im Rahmen des Forschungsprojektes SENTINEL untersucht die Deutsche Hochschule der Polizei in einer Kooperation mit verschiedenen Polizeidirektionen und weiteren Partnern den Einsatz von Open Source Intelligence zur Erhöhung des Schutzes der Einsatzkräfte und der Bevölkerung und zur Unterstützung bei der Aufgabenbewältigung. Dazu werden sogenannte Intel Officer eingesetzt, die einsatzbegleitend OSINT-Recherchen in beispielsweise sozialen Netzwerken durchführen[19].

2.3.2 Privater Einsatzbereich

OSINT kann auch von privaten Personen verwendet werden. Offene Quellen wurden von der Online-Community bei der Überwachung von militärischen Bewegungen im

Zuge des Ukraine-Konflikts Anfang 2022 verwendet[20]. Ein weiteres Beispiel für den Einsatz von OSINT ist das Recherchekollektiv Bellingcat, das aus Rechercheuren, Investigativ- und Bürgerjournalisten/innen besteht und zu verschiedenen Themen OSINT-Recherchen durchführt[21].

2.4 IT-Sicherheit

2.4.1 Defintion

Opplinger beschreibt in seinem Buch die IT-Sicherheit als „das Fachgebiet, das sich mit der Sicherheit in der IT, d.h. mit der sicheren Speicherung, Verarbeitung und Übertragung von informationstragenden Daten, befasst“[22, S. 2].

2.4.2 Technische Begriffe

In diesem Unterkapitel werden einige Begriffe erklärt, die oft in der IT-Sicherheit vorkommen oder eine Verbindung zur OSINT haben können.

Indicator of Compromise

Bautista bezeichnet einen *Indicator of Compromise* oder kurz IoC als eine technische Erkenntnis, die in Folge der Analyse von Honeypots, Malware, Open Source, HUMINT, Scanning oder Crawling entstanden ist. Seiner Erklärung nach gehören folgende Daten dazu[23, S. 97]:

- IP-Adressen
- Schädliche Domains oder URLs
- Hashwerte
- Dateigrößen
- Informationen über ein Betriebssystem

Cyber Threat Intelligence

Unter dem Begriff *Cyber Threat Intelligence* wird nach Bautista die Analyse der Absicht, der Gelegenheit und der Fähigkeit eines Angreifers verstanden, Schaden im Bereich der Informationssicherheit anzurichten[23, S. 8].

Spear-Phishing

Bei *Spear-Phishing* handelt es sich um eine gezielte Angriffsmethode durch den Versand von detaillierten E-Mail-Nachrichten an einen bestimmten Empfänger oder eine bestimmte Gruppe. Bei den Standard-Phishing-Angriffen wird versucht, so viele Empfänger wie möglich zu erreichen[24].

Domain Bruteforcing

Unter dem Begriff *Domain Bruteforcing* ist eine Methode zur Ermittlung von Subdomains zu verstehen. Dabei wird eine Liste mit bekannten Subdomains oder Hosts (z.B. *admin* wird der Domain *beispiel-domain.de* hinzugefügt) systematisch zu einer Domain eingefügt und eine forcierte DNS-Auflösung unternommen. Wenn die Auflösung erfolgreich ist, wird die Existenz der Subdomain oder des Hosts bestätigt. Die Methode gehört der Technik *Subdomain Enumeration*[25].

Google Dorking

Bei *Google Dorking* handelt es sich um eine Methode zur Auffindung von Schwachstellen unter Verwendung von speziellen Operatoren und deren Eingabe in die Suchmaschine *Google*[26].

2.4.3 Schutzziele

Die IT-Sicherheit wird durch die Erfüllung ihrer Sicherheitsziele erreicht. Die Hauptziele der IT-Sicherheit sind laut Gründer und Schrey die *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* von Informationen[27, S. 205]. Erst wenn diese Ziele erreicht werden, kann von einem sicheren Informationssystem gesprochen werden[28, S. 23].

Die *Vertraulichkeit* zielt auf eine Absicherung der Daten eines Systems ab, sodass nur autorisierte Informationsgewinnung möglich ist. Zu den schutzwürdigen Daten

gehören sowohl Nutzerdaten wie z.B. Dokumente, Datenbanken etc. als auch Systemkonfigurationen und Kennwörter[17, S. 10]. Mittels Open Source Intelligence können solche Informationen rechtzeitig aufgefunden werden, um die nötigen Gegenmaßnahmen zu ergreifen (z.B. die Löschung oder Einschränkung des Zugriffs).

Die *Integrität* eines Informationssystems wird erreicht, wenn eine unautorisierte und unbemerkte Manipulation der schutzwürdigen Daten nicht möglich ist. Dazu können erneut Daten wie z.B. Datenbanken gehören[17, S. 9]. Sollten Daten via OSINT rechtzeitig aufgefunden werden, können wieder die nötigen Gegenmaßnahmen ergriffen werden.

Weiterhin besagt die *Verfügbarkeit*, dass Systeme und Daten im Folge eines authentifizierten und autorisierten Zugriffs unabhängig von Zeit und Ort zugreifbar sein müssen[17, S. 12][28, S. 24].

Nach Eckert und Schoolmann gelten Informationssysteme als sicher, wenn zusätzlich zu den Hauptzielen *Authentizität* und *Verbindlichkeit* erreicht werden[17, S. 8][28, S. 25]. Die *Authentizität* besagt, dass Datenobjekte einen Erzeuger haben und deren Herkunft nicht bestreitet werden kann[28, S. 25]. Von einer *Verbindlichkeit* oder Nachvollziehbarkeit der Daten kann gesprochen werden, wenn die Fragen wann, warum und von wem bestimmte Daten geändert, gelöscht und erstellt worden sind, beantwortet werden können und sichergestellt ist, dass niemand die Vorgänge abstreiten kann[28, S. 25][17, S. 12].

2.5 Open Source Intelligence in der IT-Sicherheit

Da IT-Systeme sowohl im staatlichen als auch im privaten Sektor verwendet werden, kann die IT-Sicherheit als Schnittmenge für den Einsatz von OSINT betrachtet werden. Laut OWASP kann die Informationsbeschaffung aus öffentlichen Quellen sowohl für offensive als auch für defensive Zwecke verwendet werden[29, S. 7]. Demnach handelt es sich bei der offensiven Informationsbeschaffung um die Methode zur Sammlung von Informationen in der Vorbereitungsphase eines Angriffs. So kann OSINT im Bereich Penetration Testing (Abkürzung: Pentesting) verwendet werden, als Modalität, um die Angriffsfläche eines IT-Systems zu ermitteln. Außerdem kann es von Sicherheitsteams für die Suche nach öffentlich verfügbaren Informationen zu internen Ressourcen, z.B. Metadaten von Dokumenten oder Informationen zu IT-Systemen eines Unternehmens verwendet werden[1][30, o.S.].
Die defensive Informationsbeschaffung beschäftigt sich mit Aufklärungsarbeiten nach

einem Angriff[29, S. 7]. So können aus einer forensischen Festplattenanalyse die gewonnenen Indicators of Compromise, seien es IP-Adressen oder Hashwerte von Dateien, in öffentlich verfügbaren Quellen gesucht werden. Die gewonnenen Erkenntnisse können Auskunft über eine potenzielle Malware liefern, um nachträglich die Reduktion der entstandenen Schäden zu ermöglichen. Bei der Angabe des IoCs in einer OSINT-Plattform wie VirusTotal, wird das Datum in der Regel von der Plattform Nutzern zur Verfügung gestellt[31]. Da ein möglicher Bedrohungsakteur solche Plattformen in seinem eigenen Interesse verwenden kann, um beispielsweise das Incident Response und die Entwicklung des Angriffs zu beobachten, ist vorher eine Prüfung der Geheimhaltung der aus dem Angriff gewonnenen Daten nötig.

Es können sich verschiedene Akteure OSINT zunutze machen. Nach Eckert gibt es mehrere Angreifer-Typen, die von verschiedenen Motivationen angetrieben werden. Demnach kann zwischen den folgenden Akteuren unterschieden werden[17, S. 21 ff.]:

- Hacker: versierter Angreifer, der Schwachstellen und Verwundbarkeiten in IT-Systemen aufdeckt und dafür Exploits entwickelt, die eine Ausnutzung der Systeme ermöglichen. Die Hacker verfolgen jedoch keine destruktiven Absichten, sondern wenden sich meistens an die Öffentlichkeit, um die Schwachstellen bekannt zu machen und diese beheben zu lassen[17, S. 21 ff.].
- Skript Kiddie: weniger technisch versierter Angreifer, der existente Exploits ausnutzt, um Angriffe auszuführen[17, S. 21 ff.].
- Spione: Akteure, die geheimdienstliche Tätigkeiten ausüben, um daraus strategische Vorteile zu gewinnen[17, S. 21 ff.].
- Kriminelle: nutzen IT-Systeme zur Durchführung von finanziell angetriebenen Angriffen. Ein gutes Beispiel dafür sind die Ransomware-Angriffe[17, S. 21 ff.].

Im Bereich der Cyberkriminalität bediente sich beispielsweise die Ransomware-Gruppe Conti an der Gewinnung von Informationen aus öffentlichen Quellen, um ihre Ziele auszukundschaften. Einem Bericht der israelischen Sicherheitsfirma Checkpoint zufolge verfügte die Gruppierung sogar über OSINT-Analysten, die gezielte Recherchen zu den Zielunternehmen durchführten[32]. Weiterhin nutzten die Kriminellen von Conti Crawlers und Scanners, um anfällige Server und Dienste wie Apache Tomcat, Remote Desktop Protocol, Outlook Web Access oder aus dem Internet erreichbare Drücker zu finden und sie anzugreifen[33]. Im Bereich der Cyberspionage sammelte laut einer Analyse von Azeria Labs die APT28-Gruppe, bekannt auch als Sofacy, öffentliche Informationen über mögliche Ziele[34].

2.6 Das Internet als OSINT-Quelle

Im Bereich der IT-Sicherheit ist das Internet die bedeutsamste Quelle zur Durchführung von OSINT-Analysen. Das BSI und das BKA unterscheiden zwischen drei Bereichen[35][36]:

Das Clear Web

Dazu werden Quellen gezählt, die via gewöhnlichem Browser und mit bekannten Suchmaschinen wie Google oder Startpage erreichet werden können[36]. Im Clear Web sind außerdem bekannte Social-Media-Dienste wie Facebook oder Instagram erreichbar[35].

Das Deep Web

Das Deep Web stellt ca. 90% des gesamten Internets dar. Darin befinden sich Firmendatenbanken, Streaming-Server und Online-Speicher[35]. Es handelt sich dabei um Inhalte, die von Suchmaschinen nicht indexiert werden. Auf das Deep Web kann grundsätzlich jeder zugreifen, jedoch sind Bereiche davon geschützt und können von einem normalen Nutzer ohne Zugriffsberechtigungen nicht eingesehen werden[36].

Das Dark Web

Bei dem Dark Web handelt es sich um einen kleinen Teil des Internets, auf den mit spezieller Software zugegriffen wird. Das Dark Web ist auf Anonymität und Sicherheit der Kommunikation ausgelegt. Darunter sind sowohl legale Inhalte, wie z.B. Wikis/Blogs, zu finden als auch illegale Inhalte, wie z.B. Handelsplattformen, über die Schadsoftware vertrieben wird[35][36].

2.7 Die Cyber Kill Chain

Um die IT-Sicherheit zu verbessern, werden Cyberangriffe von vielen Unternehmen, Behörden und privaten Sicherheitsforschern untersucht. Zur Beschreibung der Vorgehensweise eines Cyberangriffs hat das US-amerikanische Rüstungsunternehmen Lockheed Martin im Jahr 2011 die Cyber Kill Chain entwickelt, ein sieben stufiges Modell, das genau die Stufen einer Attacke darstellt[37]. Ziel der Chain ist, die

Aktionen eines Angreifers besser zu verstehen. Laut Lockheed Martin ist ein Cyberangriff nur dann erfolgreich, wenn die ersten sechs Stufen von einem Angreifer positiv abgeschlossen wurden und somit die letzte Stufe erreicht wird. Die Cyber Kill Chain kann als Framework sowohl aus der Sicht eines Angreifers als auch aus der Sicht eines Verteidigers betrachtet werden[5, o.S.].

2.7.1 Reconnaissance

In der ersten Phase eines Angriffs wird das potenzielle Ziel aufgeklärt. Mittels Open Source Intelligence werden Informationen über das Ziel gesammelt und die IT-Landschaft wird abgetastet[37] [5, o.S.]. Während der Durchführung dieser Phase kann eine große Anzahl von Forschern monatelang ein Ziel aufklären[38, S. 2]. Es wird zwischen drei Methoden zur Sammlung von Informationen unterschieden[39, S. 14 f.]:

Passive Beschaffung

Diese Methode basiert ausschließlich auf Sammlung von Informationen aus öffentlich verfügbaren Quellen. Es werden keine Systeme aktiv analysiert. Dadurch, dass keine Daten zu oder von den Zielsystemen übertragen werden, bekommt das Ziel keine Hinweise über eine laufende Aufklärung[39, S. 14]. Nicht selten werden dafür die Dienste dritter Anbieter verwendet. Dazu gehören Dienste, die beispielsweise DNS oder WHOIS-Daten anbieten[11, S. 38].

Semi-passive Beschaffung

Es werden dabei limitiert Daten an das Zielsystem gesendet, um darüber allgemeine Informationen zu sammeln. Es wird versucht, einen normalen Internetdatenverkehr zu generieren, sodass das Ziel keine Aufklärungsaktivitäten erkennt[39, S. 14].

Aktive Beschaffung

Bei dieser Methode werden Informationen über das Ziel aktiv gesammelt. Dazu gehört die Schwachstellenanalyse und das Scannen von Ports oder Serversystemen. Dadurch, dass Datenverkehr generiert wird, kann die Aufklärung von Intrusion

Detection- oder Intrusion Prevention Systemen erkannt und dem Ziel gemeldet werden. Zum aktiven Sammeln gehört außerdem auch Angriffe mittels Social Engineering[39, S. 14].

Die vorliegende Arbeit lässt die semi-passive und aktive Informationsbeschaffung aus und betrachtet nur die passive Informationsbeschaffung.

2.7.2 Weaponization

In dieser Phase bereitet der Angreifer Tools und Software zur Durchführung der Attacke vor. Dazu gehören beispielsweise die Entwicklung oder Beschaffung von Backdoor-Programmen, Payloads oder Schadcode[5, o.S.].

2.7.3 Delivery

Basierend auf den Informationen aus der ersten Phase liefert der Angreifer seinem Ziel die Malware oder andere präparierte Software. Die Zustellung kann hierzu via E-Mail, Drive-by-Downloads oder per Auslieferung von kompromittierten USB-Sticks erfolgen[5, o.S.].

2.7.4 Exploitation

Nach der erfolgreichen Zustellung der Tools beginnt die Ausnutzung einer Schwachstelle. Dazu können Sicherheitslücken in Hardware, Software, aber auch die Ausnutzung menschlicher Quellen, via Social Engineering gehören. Ein Beispiel für oft erfolgreiche Angriffe via Social Engineering ist das Anklicken schädlicher Anhänge in einer Phishing-Mail[5, o.S.].

2.7.5 Installation

Während dieser Phase werden auf dem kompromittierten System verschiedene Backdoors, Web Shells oder sonstige Implante zur Erstellung eines dauerhaften Zugangs eingeschleust[5, o.S.].

2.7.6 Command & Control (C&C)

Nachdem der Angreifer erfolgreich einen dauerhaften Zugang zum Zielsystem eingerichtet hat, beginnt er mit dessen Manipulation. Diese kann via sogenannter C2-Server erfolgen. Der Datentransfer kann via DNS, E-Mail-Protokollen oder Web-Protokollen (http/https) erfolgen[5, o.S.].

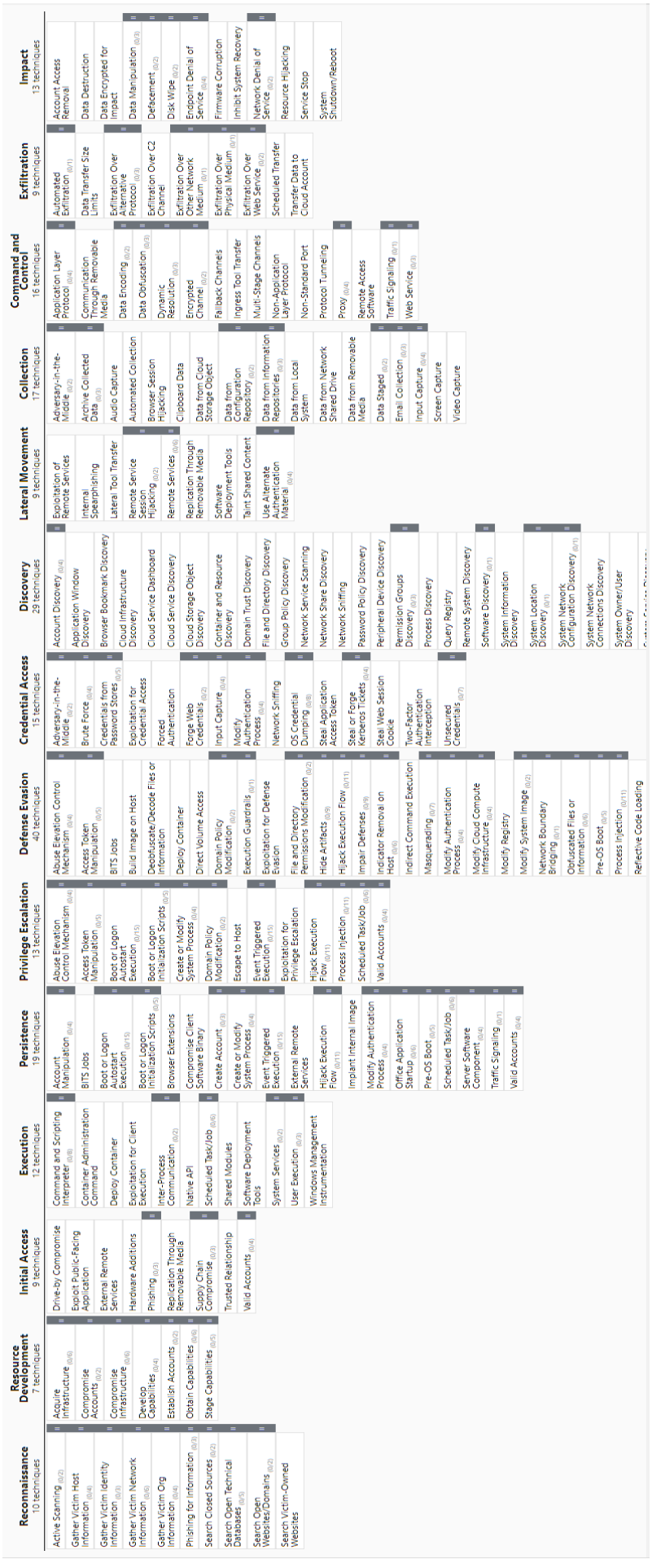
2.7.7 Actions on objectives

Sobald eine dauerhafte Verbindung besteht und die Kommunikation zur C2-Infrastruktur des Angreifers möglich ist, werden Aktionen wie z.B. die Sammlung von Informationen, Privilege Escalation, interne Aufklärung des Netzwerkes, Lateral movement, Zerstörung von Systemen oder Manipulation von Daten durchgeführt[5, o.S.].

2.8 MITRE ATT&CK-Framework

MITRE ATT&CK ist eine globale Wissensdatenbank mit einem Bezug zur IT-Sicherheit. Sie wurde 2013 von der Non-Profit-Organisation MITRE geschaffen, um bekannte Angriffstaktiken und -verfahren aus realen Beobachtungen zu dokumentieren[40]. Die neueste Version des Frameworks zum Zeitpunkt der Erstellung der vorliegenden Arbeit ist vom 03.11.2021. Die Wissensdatenbank besteht aus vierzehn Phasen. Jede Phase beinhaltet mehrere Techniken, die zur Erfüllung des jeweiligen Zweckes genutzt werden kann. Die vierzehn Phasen sind: *Reconnaissance, Resource Development, Initial Access, Execution, Persistance, Privilege Escalation, Defense Evasion, Credentials Access, Discovery, Lateral movement, Collection, Command and Control, Exfiltration, Impact.* Jedes Element der Matrix wird durch eine eindeutige ID gekennzeichnet (z.B. TA0043 für Reconnaissance-Phase) [41]. In der nächsten Abbildung ist eine Bildschirmkopie des Frameworks zu sehen.

Bild 1: MITRE ATT&CK Framework



Quelle: MITRE ATT&CK Framework[41]

Open Source Intelligence hat eine besondere Bedeutung für die erste Phase des Frameworks, *Reconnaissance*, die äquivalent zur Aufklärungsphase in der Cyber Kill Chain ist. Hier beschreibt MITRE die Ende 2020 erstellte Phase als ein Bündel aus zehn Techniken zur aktiven uns passiven Beschaffung von Informationen über Organisation, Infrastrukturen und Personal[42].

2.9 Rechtliche Aspekte

Dieses Kapitel beschreibt einige rechtliche Aspekte, die bei der Durchführung von OSINT-Recherchen zu beachten sind, stellt aber keine rechtlich sichere Beschreibung zur Durchführung von Investigationen dar. Dem IT-Sicherheitsunternehmen ESET zufolge ist OSINT in den meisten Ländern legal. Dabei muss allerdings das Datenschutzrecht berücksichtigt werden. Sollten Daten aus Social-Media-Netzwerken ausgelesen werden, könnte dadurch gegebenenfalls gegen Nutzungsbedingungen des Anbieters verstoßen werden[1]. Weiterhin müssen die Hackerparagrafen § 202a StGB – Ausspähen von Daten, §202b StGB – Abfangen von Daten, §202c StGB – Vorbereiten des Ausspähens und Abfangens von Daten (Hackerparagraf) aber auch §303a StGB - Datenveränderung und §303b StGB - Computersabotage berücksichtigt werden[43].

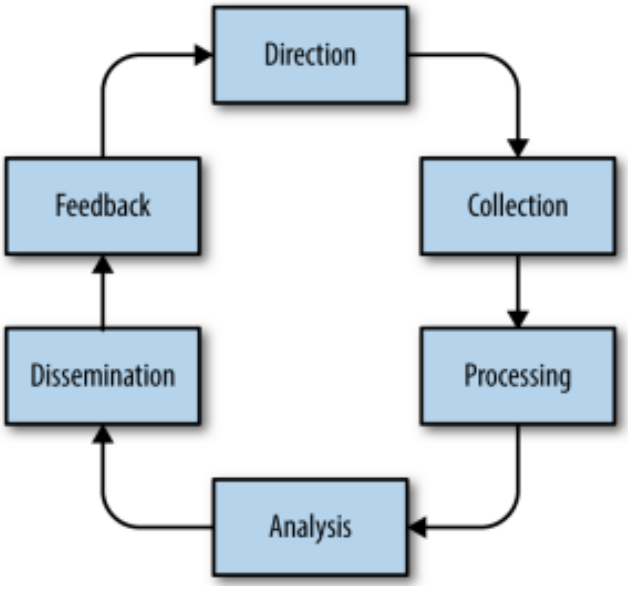
3 Klassische Strategien zur Gewinnung von Informationen

In diesem Kapitel werden drei der bekanntesten Ansätze zur Informationsgewinnung genauer analysiert. Die aus der Analyse gewonnenen Erkenntnisse dienen zur Auswahl der Strategie zur Integration in die Aufklärung von Angriffsflächen.

3.1 Der Intelligence Cycle

Der Erstellungsprozess von Intelligence basiert im Allgemeinen auf dem Intelligence Cycle. Der Intelligence Cycle oder übersetzt Intelligence-Zyklus wird in den Vereinigten Staaten von Amerika in der Intelligence Community als Standardprozess zur Gewinnung von Erkenntnissen verwendet[44]. Historisch betrachtet wurde der Begriff bereits 1948 von Robert Rigby Glass und Philip Buford Davidson in ihrem Werk ‚Intelligence is for Commanders' erwähnt[45, S. 5]. In der nächsten Abbildung ist eine grafische Darstellung des Intelligence Cycles zu sehen.

Bild 2: Der Intelligence Cycle



Quelle: Intelligence-Driver Incident Response: Outwitting the Adversary[11, S. 17]

Der Zyklus besteht grundsätzlich aus fünf Phasen[44]. Oft wird der Zyklus jedoch als ein sechsstufiges Modell beschrieben[11, S. 17]:

3.1.1 Planning/Direction

In der ersten Phase (eng. planning/direction, dt. Planung) werden von einer Zielgruppe die Absichten und die Anforderungen für die Informationsaufklärung festgelegt. Hierbei können Erkenntnisse aus vergangenen Intelligence-Zyklen analysiert werden, um gegebenenfalls auf einem bestehenden Intelligence-Produkt Wissen aufzubauen[44]. Die festgelegten Anforderungen sowie das Ziel der Informationsbeschaffung müssen so genau wie möglich definiert werden[13, S. 16]. Zur Erfüllung eines Auftrags sollen in erster ersten Linie die Erwartungen eines Auftragsgebers festgelegt werden. Sollten beispielsweise Informationen über die IT-Infrastruktur eines Unternehmens im Rahmen eines Pentests gesammelt werden, müssten spezifische Merkmale des betreffenden Unternehmens wie die statische IP-Adresse oder die Domäne festgelegt werden.

3.1.2 Collection

In der zweiten Phase (eng. collection, dt. Beschaffung) wird die Informationsbeschaffung durchgeführt. Im Bereich OSINT werden ausschließlich öffentlich verfügbare Informationen gesammelt. Zu den Informationen können IP-Adressen, Domains, Informationen über Sicherheitszertifikate, WHOIS-Informationen aber auch E-Mail-Adressen gehören[11, S. 17 f.].

3.1.3 Processing

In der dritten Phase (eng. processing, dt. Verarbeitung) werden die gesammelten Informationen gefiltert und organisiert, sodass nur die für den Auftrag relevanten Informationen in die nächste Phase übertragen werden. Die in der vorherigen Phase gesammelten Informationen befinden sich oft in einem schwer lesbaren Rohdatenformat und bedürfen einer erweiterten Verarbeitung. Dazu können die folgenden Prozesse verwendet werden[11, S. 19]:

Normalisierung der Daten

Die Rohdaten können in verschiedenen Formaten vorliegen, beispielsweise als JSON, XML, CSV oder als reiner Text. Aus diesem Grund sollen die Daten in einem einheitlichen Format, wie z.B. PDF normalisiert werden[11, S. 19].

Indexierung der Daten

Die Daten sollen so organisiert werden, dass sie schnell durchsuchbar sind[11, S. 19].

Übersetzung

Die Daten können in unterschiedlichen Sprachen vorliegen und müssen in eine Sprache übersetzt werden, die von den Analysten verstanden wird[11, S. 19].

Anreicherung der Daten

Zusätzlich zu den gesammelten Daten können mehr Kontextinformationen hinzugefügt werden. Beispielsweise können zu einer Domäne die auflösende IP-Adresse sowie der Domain-Name-Registrar hinzugefügt werden[11, S. 19].

Filterung der Daten

Unnötige Informationen sollen herausgefiltert werden [11, S. 19].

Priorisierung der Daten

Abhängig von der Relevanz soll eine Priorisierung der Daten anhand einer Skala erfolgen[11, S. 19].

Visualisierung der Daten

Für eine vereinfachte Verarbeitung sollen die gesammelten Daten visualisiert werden können[11, S. 19].

3.1.4 Analysis/Production

In der vierten Phase (eng. analysis/production, dt. Analyse/Erstellung) werden die gefilterten Informationen analysiert und miteinander verknüpft, sodass sie die Anforderungen der Planungsphase erfüllen. Dazu können verschiedene Methoden verwendet werden. Im Bereich der klassischen Informationsanalyse findet die *Analyse konkurrierender Hypothesen* (eng.: analysis of competing hypotheses) Anwendung[46, S. 95].

3.1.5 Dissemination

Die daraus gewonnenen Erkenntnisse werden in dieser Phase (eng. dissemination, dt. Verbreitung) der Zielgruppe vorgelegt. Wird das Intelligence-Produkt seiner Zielgruppe nicht vorgelegt, ist das Intelligence-Produkt nutzlos[11, S. 20 f.]. Die Verbreitung des Ergebnisses kann in verschiedenen Formaten erfolgen. Dazu gehören verbale Berichte, schriftliche Berichte, Präsentationen, Bilder oder Dashboards. Die

Ergebnisse können sowohl direkt von der Zielgruppe angefordert, als auch ohne Anforderung vom Analysten vorgelegt werden[23, S. 40].

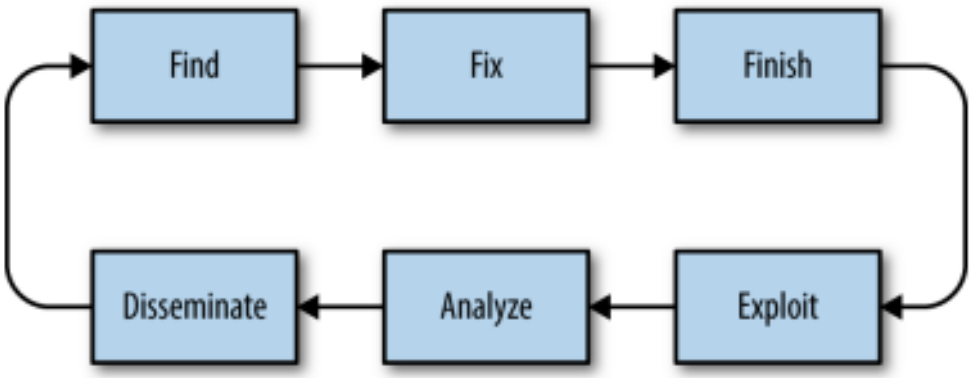
3.1.6 Feedback

Obwohl die Rückmeldung (eng. feedback) oft nicht als Phase des Intelligence Cycles genannt wird, ist sie laut Roberts und Brown für die Bewertung eines Produktes wesentlich. Das Ergebnis der Intelligence kann erfolgreich, aber auch erfolglos sein[11, S. 21]. Die Phase hat eine besondere Bedeutung für die Zielgruppe, denn sie beschreibt die Anwendung des Intelligence-Produktes. Bautista nennt diese Phase *Utilization* was **Anwendung** bedeutet[23, S. 43].

3.2 F3EAD

Der F3EAD-Zyklus steht für die englischen Begriffe *Find, Fix, Finish, Exploit, Analyze und Disseminate* und wird als Alternative zum klassischen Intelligence Cycle verwendet[47]. Laut dem US-amerikanischen Department of Army geht es dabei um einen Zyklus, der vom Militär zur Ausübung von Angriffen verwendet werden kann[48, FM 3-60]. Im Bereich der IT-Sicherheit wird der Zyklus von Roberts und Brown im Zusammenhang mit Incident-Response verwendet und besteht aus sechs Phasen[11, S. 52 - 53]. Eine grafische Darstellung des F3EAD-Zyklus ist in der nächsten Abbildung zu sehen.

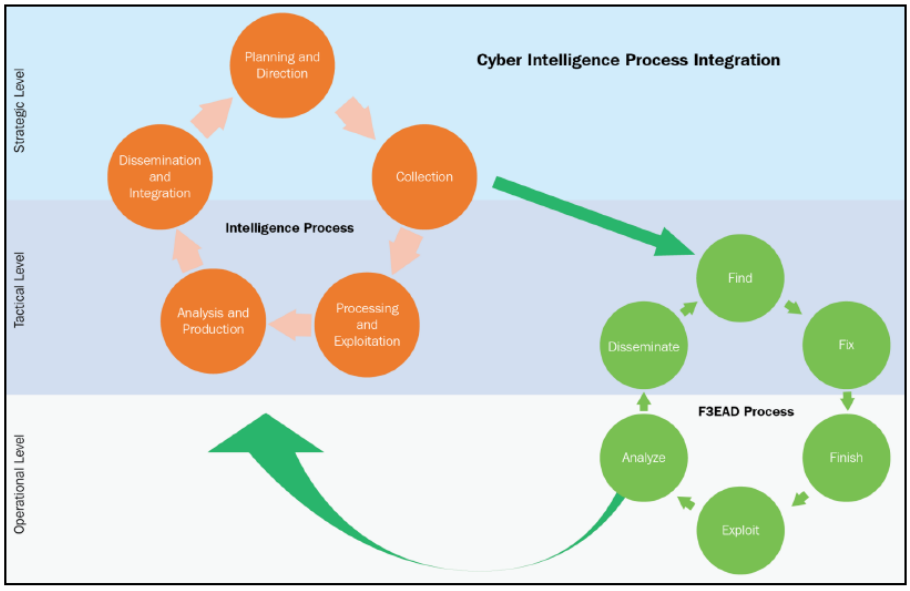
Bild 3: Der F3EAD Cycle



Quelle: Intelligence-Driver Incident Response: Outwitting the Adversary[11, S. 53]

Bautista beschreibt F3EAD als einen Unterprozess oder als einen ergänzenden Prozess zum klassischen Intelligence-Cycle, der operationale und taktische Intelligence erzeugt. Die ersten drei Phasen sind somit für die taktische Intelligence zuständig. Die nächsten drei finden bei der Erzeugung von operationaler Intelligence Anwendung[23, S. 80]. Eine Übersicht der Beziehung zwischen den beiden Zyklen kann in der nächsten Abbildung eingesehen werden.

Bild 4: Die Beziehung zwischen dem F3EAD und Intelligence Cycle



Quelle: Practical Cyber Intelligence [23, S. 80]

Sowohl Roberts und Brown als auch Bautista unterteilen die sechs Phasen des Zyklus in zwei Gruppen. Die ersten drei werden auf der operativen Ebene angewandt, also im Rahmen der eigentlichen Incident-Response[11, S. 61][23, S. 79]:

3.2.1 Find

Die erste Phase (eng. find, dt. finden) dient im militärischen Bereich der Identifikation eines möglichen Ziels[48, S. B-3]. Nach Roberts und Brown ist sie für die Erkennung eines Angreifers zur Reaktion auf einen eingehenden Cyberangriff zuständig. Die Phase kann als ein gesamter Prozess betrachtet werden[11, S. 61]. Als Anlaufstelle sind Informationen geeignet, die aus verschiedenen Quellen zusammen-

fließen können, darunter auch Open Source Intelligence[11, S. 53]. Zur Erfüllung dieser Phase können die folgenden Fragen beantwortet werden[47]:

- Wer?
- Was?
- Wo?
- Wann?
- Warum?

3.2.2 Fix

Die zweite Phase (eng. fix, dt. fixieren/anvisieren) nimmt das in der ersten Phase identifizierte Ziel ins Visier. Im Bereich der Incident Response kann sie zur Identifikation von Systemen verwendet werden, die Akteure kompromittierten können[11, S. 54]. Übertragen auf eine Informationsbeschaffung mittels OSINT, kann diese Phase mit der Aufklärungsphase der Cyber Kill Chain gleichgesetzt werden. Nachdem das Ziel anvisiert wurde, kann mit der Informationsbeschaffung begonnen werden.

3.2.3 Finish

Nachdem in der zweiten Phase ausreichend Informationen gesammelt wurden, wird in der dritten Phase (eng. finish, dt. beenden) mit der Aktion begonnen. Diese kann defensiv, wie die Reaktion auf einen Sicherheitsvorfall, oder offensiv sein, wie der Beginn eines Penetrationstests auf eine IT-Infrastruktur[11, S. 54].

Die nächsten drei Phasen sind der Gewinnung von Informationen von der operativen Ebene, beispielsweise nach der Entschärfung (engl. mitigation) eines Cyberangriffs oder nach einem erfolgreichen Pentest, zugeteilt[11, S. 61][23, S. 79].

3.2.4 Exploit

Nach Roberts und Brown kann die vierte Phase (eng. exploit, dt. ausnutzen) mit der Phase zwei des klassischen Intelligence Cycles, der Beschaffung, gleichgesetzt werden. Allerdings werden Informationen nur aus dem Sicherheitsereignis beschafft[11, S. 54].

3.2.5 Analyze

Roberts und Brown sehen für die fünfte Phase (eng. analyze, dt. analysieren) Parallenen zur dritten Phase des klassischen Zyklus. Somit werden an dieser Stelle die Informationen aus der vorherigen Phase analysiert[11, S. 55].

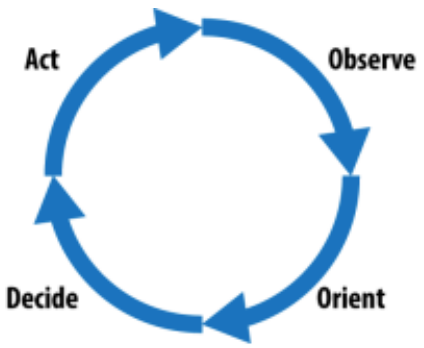
3.2.6 Disseminate

In der letzten Phase (eng. disseminate, dt. verbreiten) des F3EAD-Zyklus wird die aus der Phase fünf gewonnene Intelligence an eine Zielgruppe verteilt. Hier muss angemerkt werden, dass diese Phase nicht der gleich genannten Phase des klassischen Intelligence Cycles entspricht[11, S. 56][47].

3.3 OODA Loop

Die OODA Loop (dt. Entscheidungsschleife) wurde in den 60er Jahren vom Kampfjetpiloten, militärischen Forscher und Strategen John Boyd entworfen. Die Abkürzung OODA steht für *observe, orient, decide, act* und wird vom Militär dazu verwendet, schnelle Entscheidungen zu treffen. Im Bereich der IT-Sicherheit wird die OODA Loop zur Reaktion auf Sicherheitsvorfälle verwendet. In der nächsten Abbildung ist eine grafische Darstellung der OODA-Entscheidungsschleife zu sehen.

Bild 5: Die OODA-Entscheidungsschleife



Quelle: Intelligence-Driver Incident Response: Outwitting the Adversary[11, S. 14]

Die Entscheidungsschleife besteht aus vier Stufen[11, S. 14]:

3.3.1 Observe

In der ersten Phase (eng. observe, dt. beobachten) werden Informationen über ein potenzielles Ziel gesammelt. Aus einer defensiven Perspektive betrachtet, würde ein Verteidiger die IT-Systeme überwachen, um einen möglichen Angreifer aufzuspüren[11, S. 15]. Im Bereich von OSINT zur Aufklärung von Angriffsflächen, könnte der Analyst alle auffindbaren Informationen über sein Ziel beschaffen. Dazu gehört die Anwendung von Tools zur Aufklärung eines Zieles[23, S. 25].

3.3.2 Orient

Die gesammelten Informationen werden in einen Kontext gesetzt. Dazu können bereits bekannte Erkenntnisse addiert werden. Der Verteidiger eines IT-Systems kann in dieser Phase (eng. orient, dt. orientieren) Log-Dateien sichten und diese mit Informationen über die eigene Infrastruktur und Angriffsgruppen vergleichen, um einen möglichen Angriff zu identifizieren[11, S. 15].

3.3.3 Decide

Aufbauend hierauf werden in der dritten Phase (eng. decide, dt. entscheiden) die Entscheidungen getroffen. Sollte ein Angriff identifiziert werden, kann entschieden werden, ob der Incident-Response-Plan initiiert wird[11, S. 15].

3.3.4 Act

Die letzte Phase (eng. act, dt. handeln) beschäftigt sich mit dem Vorgang, der nach einer Entscheidung gestartet werden kann[11, S. 15].

3.4 Auswahl der Strategie

Im Bereich der Aufklärung der Angriffsflächen von IT-Systemen wird eine Strategie zur Erzeugung von Erkenntnissen und Intelligence auf Basis der gesammelten Daten benötigt. Aus der vergangenen Analyse kann festgestellt werden, dass F3EAD und OOAD nicht angewandt werden können, da die Aufklärung und Beschaffung von Informationen überwiegend in den ersten Phasen der beiden Strategien stattfinden. Als geeignetes Modell zum Aufbau der Strategie eignet sich daher der Intelligence

Cycle. Dieser beschreibt die notwendigen Schritte zur Gewinnung von Erkenntnissen über mögliche Angriffsflächen.

4 Auswertung von Softwares und Tools

4.1 Bestimmung der Kriterien

4.1.1 Technische Kriterien

Um die Strategie zur Aufklärung von Angriffsflächen zu entwickeln, müssten vorerst die Daten, die eine Bedeutung für einen Cyberangriff haben, identifiziert werden. Solche Daten konnten anhand des *MITRE ATT&CK-Frameworks* erkannt werden. Wie bereits im Kapitel MITRE ATT&CK-Framework erläutert, kann die Open Source Intelligence während der ersten Phase, *Reconnaissance*, angewandt werden. Anhand der Techniken und Methoden, die von MITRE im Rahmen der ersten Phase beschrieben werden, wurden nachfolgend die relevanten Daten zur Erstellung der Kriterien extrahiert.

Active Scanning - T1595

Die Technik T1595 besteht aus zwei Methoden, T1595.001 *Scanning IP Blocks* und T1595.002 *Vulnerability Scanning*. Daraus konnte das Datenelement **IP** gewonnen werden[49][50][51].

Gather Victim Host Information - T1592

Die Technik T1592 besteht aus den Methoden T1592.001 *Hardware*, T1592.002 *Software*, T1592.003 *Firmware* und T1592.004 *Client Configurations*. Daraus kann der Datensatz **Systeminformationen** extrahiert werden[52][53][54][55][56].

Gather Victim Identity - T1589

Die Technik T1589 besteht aus den Methoden T1589.001 *Credentials*, T1589.002 *Email Addresses* und T1589.003 *Employees Names*. Daraus konnten die Daten **Zugangsdaten**, **E-Mail-Adresse** und **Namen** gewonnen werden. Das Datenelement **Namen** wird aufgrund der Abgrenzung nicht weiter verwendet[57][58][59][60].

Gather Victim Network Information - T1590

Die Technik T1590 besteht aus den Methoden T1590.001 *Domain Properties*, T1590.002 *DNS*, T1590.003 *Network Trust Dependencies*, T1590.004 *Network Topology*, T1590.005 *IP-Addresses* und T1590.006 *Network Security Appliances*. Daraus konnten die Daten **Registrar**, **Domäne**, **Netzwerkroute** und erneut **IP-Adresse** gewonnen werden[61][62][63][64][65][66][67].

Gather Victim Org Information - T1591

Die Technik T1591 besteht aus den Methoden T1591.001 *Determine Physical Locations*, T1591.002 *Business Relationships*, T1591.003 *Identify Business Temp* und T1591.004 *Identify Roles*. Daraus konnten die Daten **Adresse der Organisation**, **Geschäftsbeziehungen** und **Öffnungszeiten** erhalten werden[68][69][70][71]. Wie bereits im Kapitel Abgrenzung erwähnt, werden in dieser Arbeit keine Methoden zur Sammlung von Informationen über Firmen behandelt. Aus diesem Grund werden die o.g. Daten nicht weiterverwendet.

Phishing for Information - T1598

Die Technik T1598 besteht aus den Methoden T1598.001 *Spearphishing Service*, T1598.002 *Spearphishing Attachment* und T1598.003 *Spearphishing Link*. Es konnten daraus die folgenden Daten extrahiert werden: **Zugangsdaten** und **Konten**. Aufgrund der ähnlichen Bedeutung wurden die beiden Daten zu einem einzigen zusammengefasst: **Zugangsdaten**[72][73][74][75].

Search Closed Sources - T1597

Die Technik T1597 besteht aus den Methoden T1597.001 *Threat Intel Vendors* und T1597.002 *Purchase Technical Data*. Es konnten daraus die folgenden Daten gewonnen werden: **Zugangsdaten** und **Domänen**[76][77][78].

Search Open Technical Databases - T1596

Die Technik T1596 besteht aus den Methoden T1596.001 *DNS/Passive DNS*, T1596.002 *WHOIS*, T1596.003 *Digital Certificates*, T1596.004 *CDNs* und T1596.005 *Scan Databases*. Daraus konnten die Daten **DNS**, **pDNS**, **WHOIS**, **Digitales Zertifikat**, **CDN**, **Server-Banner** und **Port** erhalten werden. **DNS** und **pDNS** wurden zum Datum **Domäne** (eng. domain) zusammengefasst[79][80][81][82][83][84].

Search Open Websites/Domains - T1593

Die Technik T1593 besteht aus den Methoden T1593.001 *Social Media* und *Search Engines*. Die daraus gewonnenen Daten sind **Firmeninformationen** und **Dateityp**. Die Daten **Firmeninformationen** wurden aufgrund der Abgrenzung nicht weiter verwendet[85][86][87].

Search Victim-Owned Websites - T1594

Die Technik enthält keine weiteren Methoden. Die daraus gewonnen Daten sind: **Personennamen** und **E-Mail-Adresse**. Das Datenelement **Personennamen** wird aufgrund der Abgrenzung im Kapitel Abgrenzung nicht weiter verwendet[88].

Zusammenfassung

Nach der Auffindung von mehreren Daten, die von Bedeutung für einen Angriff sein können, wurden daraus die technischen Kriterien für die Bewertung der Softwares und Tools tabellarisch erstellt (siehe Tabelle Übersicht der technischen Kriterien).

Tabelle 2: Übersicht der technischen Kriterien

Kriterium	Anmerkung
E-Mail	E-Mail-Adresse
Domain	Domain und/oder Subdomain
IP	IP-Adresse
Credentials	Kann ein Benutzername, Passwort oder ein Hashwert sein
Dateityp	Liefert Informationen über ein Dateityp (z.B. .txt)
SSL-Zertifikat	Liefert Informationen über das eingesetzte SSL-Zertifikat
Port	Liefert eine Portnummer
Systeminformationen	Liefert Informationen über ein System (z.B. Software, Version Operating System, etc.)

Die Kriterien konnten sowohl für die Eingabe als auch für die Ausgabe von Daten im Rahmen der Teststellung verwendet werden.

4.1.2 Zugehörigkeit im Intelligence Cycle

Um das analysierte Tool mindestens einer Phase des Intelligence Cycles zuordnen zu können, wurden weitere Kriterien festgelegt:

Tabelle 3: Übersicht der Daten für die Eingliederung im Intelligence Cycle

Phase	Abkürzung	Kriterien
1. Planning/Direction	(P)	Ermöglicht die Sammlung von Ideen, Brainstorming, etc.
2. Collection	(B)	Ermöglicht die Sammlung von Daten
3. Processing	(V)	Ermöglicht die Filterung und Sortierung von Informationen
4. Analysis/Production	(A)	Ermöglicht die Analyse (z.B. Daten verknüpfen) von Informationen
5. Dissemination	(D)	Ermöglicht die Erstellung von Berichten oder Präsentationen
6. Feedback	(R)	Ermöglicht Notizen

4.2 Beschreibung der Testbedingungen

4.2.1 Testdaten

Für eine gleichförmige Analyse der Tools wurden anhand der technischen Kriterien die folgenden Testdaten festgelegt:

- Domain: hs-wismar.de
- IP: 141.53.15.120 (Auflösung der Domäne hs-wismar.de)

4.2.2 Testsystem

Zur Durchführung der Tests wurde eine virtualisierte Umgebung verwendet. Auf einem Windows 10 Betriebssystem wurde der Hypervisor *Oracle VirtualBox* in der Version 6.1.28 verwendet. Es wurde darauf eine virtuelle Maschine mit dem Betriebssystem *Ubuntu Desktop*, Version 20.04.4. installiert. Folgende Ressourcen wurden der Maschine zugeteilt:

- Hauptspeicher: 4096 MB
- Prozessoren: 2
- Grafikspeicher: 128 MB
- Massenspeicher: 1 VDI, 20 GB

4.2.3 Laufzeit pro Testvorgang

Pro Testvorgang wurde eine maximale Laufzeit von 10 Minuten festgelegt. Der Grund dafür ist die Fähigkeit der Software, umfangreiche Scans durchzuführen, die unter Umständen viel Zeit benötigen.

4.2.4 Bewertung eines Testvorgangs

Die Bewertung erfolgte pro Testvorgang in vier Schritten.

Eingabeparameter

Im ersten Schritt wurde überprüft, welche der technischen Kriterien sich als Eingabeparameter eignen. Es wurde an der Stelle keine Gewichtung festgelegt, alle Kriterien wurden mit 1x bewertet. Dazu wurde die folgende Tabelle erstellt:

Tabelle 4: Bewertungsmatrix für die Eingabeparameter

Eingabe	
Phase	erfüllt
E-Mail	
Domain	
IP	
Credentials	
Dateityp	
SSL-Zertifikat	
Port	
Systeminformationen	
Anzahl erfüllter Kriterien	

Ausgabeparameter

Im zweiten Schritt wurden die Ausgabeparameter analysiert und anhand der folgenden Tabelle bewertet. Die Gewichtung pro Kriterium betrug 1x.

Tabelle 5: Bewertungsmatrix für die Ausgabeparameter

Ausgabe	
Phase	erfüllt
E-Mail	
Domain	
IP	
Credentials	
Dateityp	
SSL-Zertifikat	
Port	
Systeminformationen	
Anzahl erfüllter Kriterien	

Nutzbarkeit im Intelligence Cycle

Nachdem die Ausgabeparameter ausgewertet wurden, wurde analysiert, ob das Tool/-die Software Funktionen anbietet, die einer der fünf Phasen des Intelligence Cycles zugeordnet werden können. Die Phase *Feedback* wurde bei der Bewertung nicht betrachtet. Die Gewichtung pro Kriterium betrug 1x.

Tabelle 6: Bewertungsmatrix für die Zuweisung innerhalb des Intelligence Cycles

Intelligence Cycle	
Phase	erfüllt
Planning/Direction	
Collection	
Processing	
Analysis/Production	
Dissemination	
Anzahl erfüllter Phasen	

Gesamtergebnis

Das Gesamtergebnis eines Testvorgangs wurde mit der folgenden Formel berechnet:

$$Gesamtergebnis = (\sum_{n=1}^{m1} 1 + \sum_{n=1}^{m2} 1) * \sum_{n=1}^{m3} 1$$

m1 = Anzahl erfüllter eingegeben Kriterien
m2 = Anzahl erfüllter ausgegeben Kriterien
m3 = Anzahl erfüllter Phasen des Intelligence Cycles

Die Multiplikation der Summe (Σ) der Eingabe- und Ausgabeparameter mit der Anzahl der erfüllten Kriterien hat eine besondere Rolle für die Berechnung des Gesamtergebnisses. Die Möglichkeit der Abarbeitung des gesamten Intelligence Cycles innerhalb eines Tools bedeutet eine Vereinfachung des gesamten Rechercheprozesses und sinkt den Aufwand bei der Einarbeitung der Analysten, der Verwaltung von möglichen Lizenzen oder die möglichen anfallenden Lizenzkosten für mehrere Tools und steigert die Übersichtlichkeit im Rahmen der Softwareadministration.

4.3 Bewertung

In diesem Abschnitt wurden die Tools ausgewertet. Es wurden Linux-spezifische, lokal installierte Tools bewertet. Es wurden nur öffentliche APIs verwendet, die keine gesonderte Anmeldung benötigen. Die allgemeine Analyse der jeweiligen Software oder des Tools wurde bei der Berechnung des Gesamtergebnisses berücksichtigt.

4.3.1 SpiderFoot

SpiderFoot ist ein im Jahr 2005 entwickeltes OSINT-Tool. Das Tool greift auf mehr als 100 Open Source Quellen zurück, um Informationen über IP-Adressen, Domainnamen, E-Mail-Adressen, Namen zu sammeln. Die Verwendungszwecke sind laut dem Hersteller verschieden. So kann das Tool sowohl im Bereich Cyber Threat Intelligence als auch im Bereich der Erkennung der Angriffsflächen eingesetzt werden. Der Source Code ist Open source und in zwei Varianten erhältlich. Die self-hosted Version ist frei nutzbar. SpiderFoot wurde in der Programmiersprache Python 3 entwickelt und der Quellcode ist Open Source. Die Software nutzt sowohl öffentliche APIs als auch private APIs [89]. Die Installationsanleitung kann unter `https://www.spiderfoot.net/documentation` eingesehen werden.

Allgemeine Analyse

Das Tool ermöglicht die Suche nach den folgenden Daten: Domain Name, IPv4 Address, IPv6 Address, Hostname/Sub-Domain, Subnet, Bitcoin Address, E-Mail Address, Phone Number, Human Name, Username und Network ASN.

Bild 6: Eingabefeld SpiderFoot

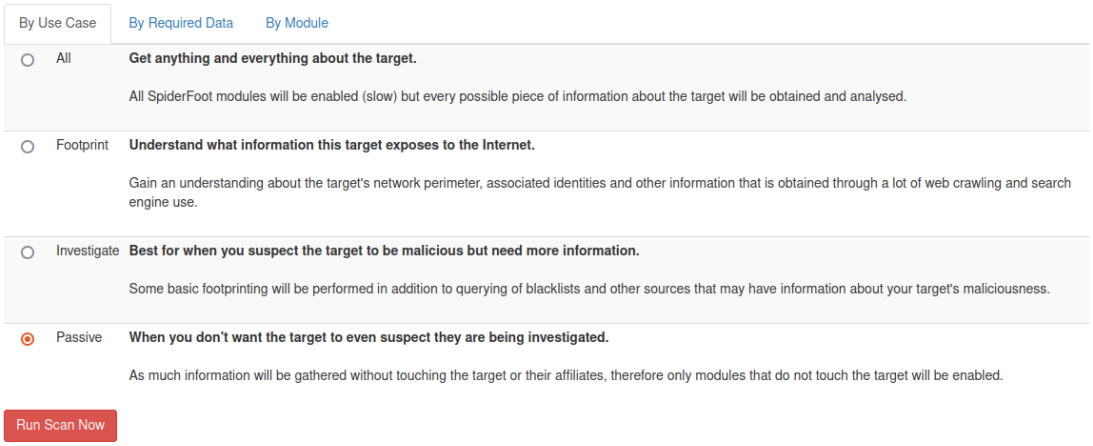
Quelle: eigene Darstellung, Screenshot der Softwareoberfläche

Vor dem Start eines Scans kann die Beschaffungsart ausgewählt werden (siehe Abbildung Auswahl Modi in SpiderFoot). Somit sind vier anwendungsbasierte Modi verfügbar:

- All: Es werden sowohl aktive als auch passives Scans unter Verwendung aller Module durchgeführt.
- Footprint: untersucht Informationen, die im Internet veröffentlicht wurden.
- Investigate: untersucht ein mögliches maliziöses Ziel, beispielsweise wenn eine Domäne auf Phishing verdächtigt wird.
- Passive: Es werden ausschließlich passive Scans durchgeführt.

Es besteht weiterhin die Möglichkeit, die Beschaffungsart anhand der benötigten Daten anzupassen. Somit kann aus mehr als 150 Kriterien ausgewählt werden. Dazu gehören beispielsweise IP-Adressen, BGP AS Ownership, Bitcoin Adressen, Country Name oder Geburtsdatum. Außerdem steht eine gezielte Auswahl der Module zur Verfügung, die im Scan eingebunden werden können. Demnach kann beispielsweise nur die API-Schnittstelle der Suchmaschine Shodan verwendet werden.

Bild 7: Auswahl Modi in SpiderFoot



Quelle: eigene Darstellung, Screenshot der Softwareoberfläche

Weiterhin kann die Beschaffungsart anhand der benötigten Daten angepasst werden.

Soweit im Rahmen des Tests bekannt wurde, bietet SpiderFoot in der Open Source-Version keine Möglichkeit, Daten zu analysieren. Aus diesem Grund handelt es sich um ein Tool, das der Phase *Beschaffung* des Intelligence Cycle zuzuordnen ist.

Durchführung der Bewertung

Zur Auswertung der Funktionalität wurde als Testdatum die Domäne **hs-wismar.de** eingetragen. Die Laufzeit des Testvorgangs betrug 10 Minuten. Wie in der Abgrenzung vermerkt, wurde die passive Informationsbeschaffung ausgewählt.

Nach dem Ablauf der Testzeit wurden unter anderem folgende Ergebnisse erhalten:

- Domain Name: 1
- Email Address: 57
- IP Address: 2
- SSL Certificate - Raw Data: 56
- Username: 1
- Web Server: 3

Somit wurden sechs Ausgabeparameter erfüllt. Das Gesamtergebnis beträgt 10 Punkte. Das Bewertungsschema und das Gesamtergebnis können anhand der Anlage Bewertung SpiderFoot nachvollzogen werden.

4.3.2 Maltego

Maltego ist eine proprietäre Software für die grafische Linkanalyse im Bereich Data-Mining, mit der Daten im Internet gesucht und nach der Beschaffung analysiert werden können[90]. Nach Whisperlab wurde Maltego von der Firma Paterva Ltd in der Programmiersprache Java entwickelt und benötigt eine Java Laufzeitumgebung der Version 8 oder höher für die Funktion[91]. Die Software ist in verschiedenen Versionen erhältlich[92]:

- Maltego One: eine kommerzielle Version, für komplexe Investigationen
- Maltego CaseFile: eine kostenlose Version, die nur offline Investigationen bietet
- Maltego XL: eine kommerzielle Version, für komplexe Investigationen, die die Anwendung von großen Graphen zulässt
- Maltego Community Edition (CE): eine kostenlose Version, die im Kali Linux-Betriebssystem integriert ist. Die Nutzung der Software kann mit einer kostenlosen Anmeldung ermöglicht werden.

Die Software ermöglicht sogenannte *Transforms*, in der Programmiersprache Python entwickelte Schnittstellen innerhalb der Software, die den Zugriff auf externe Ressourcen ermöglichen. Bei den externen Ressourcen handelt es sich um externe Server (Transform Servers), die Anfragen des Maltego-Clients verarbeiten und benötigte Informationen liefert[93]. Es gibt weitere Transforms, die auf die API-Schnittstelle von Drittanbietern (z.B. Shodan) zugreifen. Dazu wird ein API-Key benötigt, was oft mit einer Registrierung verbunden ist[94]. Aufgrund der Kommunikation mit dem externen Server von Maltego, muss vor dem Einsatz der Software geprüft werden, ob die verarbeiteten Daten innerhalb von Maltego nach außen kommuniziert werden dürfen[91]. Der Datenschutzerklärung von Maltego zufolge, werden beim Ausführen eines Transform Information wie Zeitstempel der Anfrage, Quell-IP-Adresse der Anfrage, die Suchanfrage als Parameter oder der User-Agent übermittelt[95]. Für sensible Informationen bietet Maltego eine self-hosted Lösung für das Betreiben von Transformsservern[93].

Laut dem Entwickler eignet sich das Tool für die Anwendung im Bereich Strafverfolgung, Cyber Threat Intelligence aber auch Penetration-Testing. Im Bereich der Strafverfolgung wird das Tool laut der Homepage von Maltego vom Bundeskriminalamt verwendet[96].

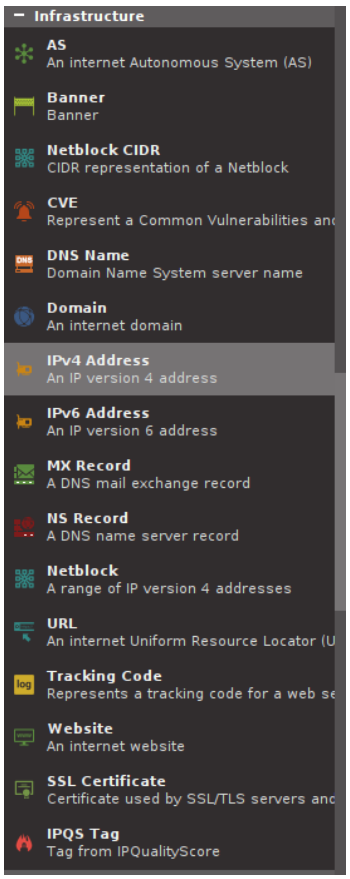
Für die Analyse und Bewertung in der vorliegenden Arbeit wurde die *Version Maltego Community Edition (CE)* für Linux verwendet.

Die Software kann von der offiziellen Seite bezogen werden: `https://www.maltego.com/downloads/`.

Allgemeine Analyse

Das Tool bietet im Bereich der Aufklärung von IT-Infrastrukturen die Eingabe folgender Daten an: IP-Adresse, Domain, Internet Autonomous System, SSL-Zertifikat, Port, ein Dokument, E-Mail-Adressen oder Namen von Personen. Sie sind als sogenannte *Entities* dargestellt (siehe Abbildung Screenshot Maltego Entities). Alle *Entities* erlauben das Ausführen von Transforms, womit weitere Informationen wie Zugehörigkeiten zu IP-Adressen beschaffen werden.

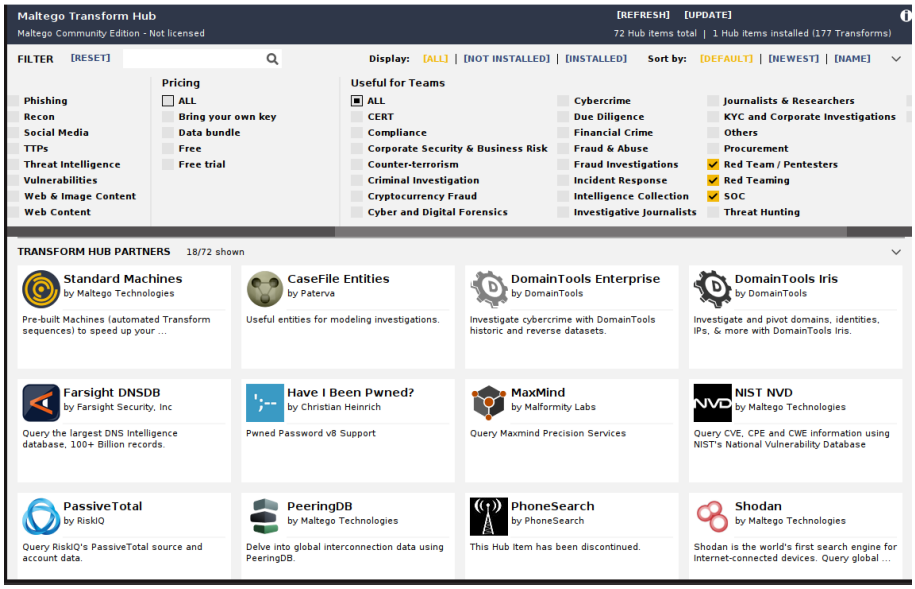
Bild 8: Screenshot Maltego Entities



Quelle: eigene Darstellung, Screenshot der Softwareoberfläche

Die Transforms können alle gleichzeitig ausgeführt werden oder vereinzelt nach persönlichem Bedarf. Es lassen sich über den Transformation-Hub alle Transforms sichten und installieren (siehe Abbildung Screenshot Maltego-Hub). Die Filterung der Transforms für die Bereiche Red Team / Pentesters und SOC hat beispielsweise ergeben, dass Tools wie DomainTools, Shodan, Have I Been Pwned? oder ThreatMiner eingebunden werden können.

Bild 9: Screenshot Maltego-Hub



Quelle: eigene Darstellung, Screenshot der Softwareoberfläche

Durchführung der Bewertung

Zur Auswertung der Funktionalität wurde als Testdatum die Domäne **hs-wismar.de** in der Entität **Domain** eingetragen. Die Laufzeit des Testvorgangs betrug 10 Minuten. Die ausgeführten Transforms werden laut der offiziellen Dokumentation der passiven Beschaffung zugeordnet und entsprechen der Abgrenzung[93]. Des Weiteren wurden die Transforms für die Quellen *Maltego Wayback Machine CE Transforms* und *Maltego Wikipedia-EN CE Transforms* entfernt.

Nach dem Ablauf der Testzeit wurden folgende Ergebnisse erzielt:

- DNS Names: 38
- Documents: 20
- Domains: 6
- MX Records: 4
- NS Records: 5
- Netblocks: 5
- People: 12

- Phone Numbers: 12
- Websites: 17

Das Tool bietet Funktionen zur Vorbereitung der Investigation, Beschaffung von Informationen, Sortierung und Filterung sowie die Möglichkeit einen Bericht zu generieren. Aus diesem Grund erfüllt die Software alle Phasen des Intelligence Cycles. Das Gesamtergebnis liegt somit bei 55 Punkten. Eine detaillierte Bewertung sowie der Screenshot der Ausgabe von Maltego (siehe Screenshot Maltego Ergebnisse) befindet sich im Anhang unter Bewertung Maltego.

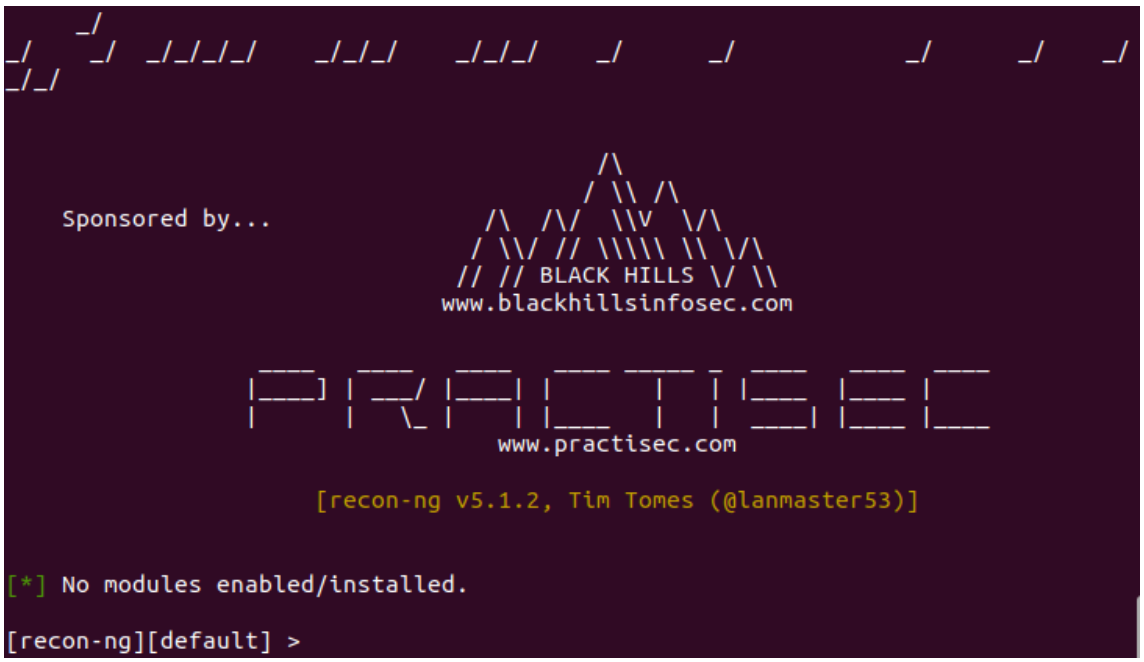
4.3.3 Recon-ng

Ein weiteres bekanntes Tool zur Aufklärung ist Recon-ng. Die Software wurde in der Programmiersprache Python entwickelt und ist frei erhältlich[97]. DiMaggio setzt das Tool dem Pentesting-Framework *Metasploit* gleich. Demnach können damit offene Infrastrukturen, bestehende Subdomains, E-Mail-Adressen, Protokolle, offene Ports, Systeminformationen und weitere Ressourcen gesammelt werden[98, S. 177]. Das Framework ist modularisch aufgebaut und kann mit API-Key externer Dienstleister wie Shodan ergänzt werden.

Allgemeine Analyse

Es wurde die Version 5.1.2 analysiert. Standardmäßig werden nach der Installation keine Module geladen, sie können aber aus dem sogenannten Marketplace installiert werden. Eine erste Sichtung des Github-Repository hat ergeben, dass Recon-ng sowohl passive Aufklärung durch die Nutzung externer Dienste wie VIEWDNS oder Shodan als auch aktive Aufklärung, durch die Nutzung von Tools wie NMAP, ermöglicht[99]. Gemäß der Abgrenzung wurde der passive Modus verwendet. Die Bedienung erfolgt ausschließlich über das Terminal und verfügt über keine grafische Oberfläche. Eine Installationsanleitung kann unter `https://github.com/lanmaster53/Recon-ng/wiki/Getting-Started#installation` eingesehen werden.

Bild 10: Screenshot Recon-ng



Quelle: eigene Darstellung, Screenshot der Ausgabe im Terminal

Durchführung der Bewertung

Die Verwendung von Recon-ng benötigt das Anlegen eines Workspace. Dafür wurde das Workspace ‚Test' angelegt. Zum Zeitpunkt der Analyse waren 98 Module im Bereich *recon* verfügbar, davon benötigten 56 eine API-Key für den Zugriff auf externe Ressourcen wie z.B. die Suchmaschinen Shodan oder Censys. Die restlichen 48 Module, die keine API-Key benötigt haben, sind in der nächsten Abbildung zu sehen. Bei dem Modul *brute_hosts* handelt es sich um eine Funktion, die aktive Aufklärung mittels DNS Brute Force von Host ermöglicht[100]. Weiterhin führt das Modul *Brute_suffix* eine ähnliche Funktion. Es verwendet die Methode Brute Force für Top-Level-Domains und Second Level Domains[101]. Die beiden Methoden gehören zur aktiven Aufklärung und wurden aus diesem Grund gemäß der Abgrenzung nicht in der Analyse betrachtet. Außer diesen beiden wurden alle in der nächsten Abbildung dargestellten Module in das Framework für den Test installiert. Die Testzeit betrug 10 Minuten.

Bild 11: Screenshot Recon-ng: freie Module

```
  | recon/companies-contacts/pen                          | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/pen                           | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/viewdns_reverse_whois         | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-multi/whois_miner                     | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/contacts-contacts/mailtester                    | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/contacts-contacts/mangle                        | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/contacts-contacts/unmangle                      | 1.1     | not installed | 2019-10-27 |   |   |
  | recon/contacts-domains/migrate_contacts               | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/credentials-credentials/adobe                   | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/credentials-credentials/bozocrack               | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-companies/pen                           | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-contacts/pen                            | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/domains-contacts/pgp_search                     | 1.4     | not installed | 2019-10-16 |   |   |
  | recon/domains-contacts/whois_pocs                     | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-contacts/wikileaker                     | 1.0     | not installed | 2020-04-08 |   |   |
  | recon/domains-credentials/pwnedlist/leak_lookup       | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-domains/brute_suffix                    | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/domains-hosts/bing_domain_web                   | 1.1     | not installed | 2019-07-04 |   |   |
  | recon/domains-hosts/brute_hosts                       | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/certificate_transparency          | 1.2     | not installed | 2019-09-16 |   |   |
  | recon/domains-hosts/google_site_web                   | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/hackertarget                      | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/domains-hosts/mx_spf_ip                         | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/netcraft                          | 1.1     | not installed | 2020-02-05 |   |   |
  | recon/domains-hosts/ssl_san                           | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/threatcrowd                       | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/threatminer                       | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-vulnerabilities/ghdb                    | 1.1     | not installed | 2019-06-26 |   |   |
  | recon/domains-vulnerabilities/xssed                   | 1.1     | not installed | 2020-10-18 |   |   |
  | recon/hosts-domains/migrate_hosts                     | 1.1     | not installed | 2020-05-17 |   |   |
  | recon/hosts-hosts/resolve                             | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/hosts-hosts/reverse_resolve                     | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/hosts-hosts/ssltools                            | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/hosts-locations/migrate_hosts                   | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-companies/whois_orgs                  | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-hosts/reverse_resolve                 | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-ports/census_2012                     | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/ports-hosts/migrate_ports                       | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/ports-hosts/ssl_scan                            | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/profiles-contacts/dev_diver                     | 1.1     | not installed | 2020-05-15 |   |   |
  | recon/profiles-profiles/profiler                      | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/repositories-vulnerabilities/gists_search       | 1.0     | not installed | 2019-06-24 |   |   |
```

Quelle: eigene Darstellung, Screenshot der Ausgabe im Terminal

Das Framework bietet keine Möglichkeit, alle installierte Module gleichzeitig auszuführen. Aus diesem Grund wurde eine angepasste Version des Shell-Skriptes *automated-Recon-ng* zur automatisierten Recherche verwendet. Das Skript wurde vom Github-Nutzer *SamShanks1* entwickelt[102]. Das angepasste Skript befindet sich im Anhang unter Bewertung Recon-ng. Im Rahmen der Analyse konnte der Eingabeparameter *Domain* verwendet werden. Der Eingabeparameter war die Domäne **hs-wismar.de**. Die Nutzung der API-freien Module hat ergeben, dass als Ausgabeparameter Domains oder IPs bestätigt werden können, obwohl die verschiedenen Module Auskunft über weitere Parameter wie E-Mail-Adressen geben sollten. Die Bewertung basiert ausschließlich auf der Ausgabe des Tools in Folge des Tests. Von den 48 Modulen, die in die Analyse einbezogen wurden, haben 12 positive Ergebnisse geliefert. Bei den Ergebnissen handelte es sich um Hosts, Domains, IP-Adressen und E-Mail-Adressen.

- Hosts: 892 (nach Entfernung der doppelten Einträge)
- Domains: 53 (nach Entfernung der doppelten Einträge)
- IP: 486 (nach Entfernung der doppelten Einträge)
- E-Mail: 16 (nach Entfernung der doppelten Einträge)

Das Tool bietet Funktionen zur Beschaffung von Informationen über IT-Infrastrukturen. Recon-ng bietet keine Möglichkeiten, die Daten zu filtern, zu sortieren oder zu analysieren. Aus diesem Grund eignet sich das Tool für die erste Phase des Intelligence-Cycles. Das Gesamtergebnis liegt somit bei 4 Punkten. Eine detaillierte Bewertung sowie die Ausgabe von Recon-ng befindet sich im Anhang unter Bewertung Recon-ng.

4.3.4 theHarvester

theHarvester ist ein in der Programmiersprache Python entwickeltes Tool. Die Software wurde von der Firma Edge-Security entwickelt und ist auf Github frei erhältlich[103]. Gemäß der Beschreibung des Tools greift es sowohl auf passives als auch auf aktives Scanning zu. Die aktive Methode verwendet beispielsweise die DNS Brute Force alt Methode[104]. Eine Installationsanleitung kann unter `https://github.com/laramies/theHarvester/wiki/Installation` eingesehen werden.

Allgemeine Analyse

theHarvester kann via Terminal verwendet werden und verfügt nicht über eine GUI-Oberfläche. Es nutzt sowohl API-freie Ressourcen wie RapidDNS als auch Dienste wie die Suchmaschine Shodan, die einen API-Zugang verwenden. Für diesen Test wurden die API-freien Ressourcen verwendet.

Bild 12: Screenshot theHarvester

Quelle: eigene Darstellung, Screenshot der Ausgabe im Terminal

Durchführung der Bewertung

Es wurde die Version 4.0.3 in der Laborumgebung installiert. Nach einer Sichtung der Ressourcen, wurden wie im Abschnitt Abgrenzung erwähnt, diejenigen Tools ausgeschlossen, die aktive OSINT-Methoden wie DNS Enumeration unterstützen oder eine API benötigen. Aus diesem Grund wurden die folgenden Module in die Analyse einbezogen:

- anubis-DB
- baidu
- bufferoverun
- dnsdumpster
- duckduckgo
- hackertarget
- omnisint
- otx
- qwant
- rapiddns

- threatcrowd
- threatminer
- urlscan
- yahoo

Das Tool unterstützt die Eingabe von Domains. Als Eingabeparameter wurde die Domäne **hs-wismar.de** verwendet. Nach einer manuellen Analyse wurden die doppelten Resultate entfernt. Folgende Ausgabeparameter wurden erhalten:

- E-Mail-Adressen: 14 (nach Entfernung der doppelten Einträge)
- ASNs: 2
- IP-Adressen. 719 (nach Entfernung der doppelten Einträge)
- Hosts: 918 (nach Entfernung der doppelten Einträge)

theHarvester erfüllte die Voraussetzung zur passiven und aktiven Aufklärung von IT-Infrastrukturen. Funktionen zur Filterung, Sortierung, Analyse von Daten und Erzeugung von Berichten wurden nicht erfüllt. Eine detaillierte Bewertung befindet sich im Anhang. Die Testzeit betrug 10 Minuten.

4.4 Ergebnis der Bewertung

Im nächsten Abschnitt werden die Ergebnisse der Analyse der einzelnen Tools tabellarisch gegenübergestellt. Weiterhin werden die Quellen, auf die jedes Tool zugreift, dargestellt und eine Schnittmenge der gemeinsamen Quellen präsentiert.

4.4.1 Integration im Intelligence Cycle

Die folgende Tabelle zeigt eine Übersicht der Bewertung der Tools zur Integration im Intelligence Cycle.

Tabelle 7: Integration der Tools im Intelligence Cycle

Intelligence Cycle				
Phase	SpiderFoot	Maltego	Recon-ng	theHarvester
Planning/Direction		x		
Collection	x	x	x	x
Processing		x		
Analysis/Production		x		
Dissemination		x		
Gesamt	1	5	1	1

Maltego erfüllte alle Kriterien, um den gesamten Intelligence Cycle zu durchlaufen.

4.4.2 Vergleich der Eingabe- und Ausgabeparameter

Die folgenden Tabellen zeigen eine Übersicht des Vergleichs der Eingabe- und Ausgabeparameter.

Tabelle 8: Vergleich der Eingabeparameter

Eingabeparameter				
Parameter	SpiderFoot	Maltego	Recon-ng	theHarvester
E-Mail	x	x	-	-
Domain	x	x	x	x
IP	x	x	-	-
Credentials	x	x	-	-
Dateityp	-	x	-	-
SSL-Zertifikat	-	x	-	-
Port	-	x	-	-
Systeminformationen	-	x	-	-
Gesamt	4	8	1	1

Tabelle 9: Vergleich der Ausgabeparameter

Ausgabeparameter				
Parameter	SpiderFoot	Maltego	Recon-ng	theHarvester
E-Mail	x	x	x	x
Domain	x	x	x	x
IP	x	x	x	x
Credentials	x	-	-	-
Dateityp	-	-	-	-
SSL-Zertifikat	x	-	-	-
Port	-	-	-	-
Systeminformationen	x	-	-	-
Gesamt	6	3	3	3

Anhand der Formel zur Berechnung des Gesamtergebnisses wurden folgende Resultate erzielt:

- SpiderFoot: 10 Punkte
- Maltego: 55 Punkte
- Recon-ng: 4 Punkte
- theHarvester: 4 Punkte

4.4.3 Schnittmenge der Quellen

Im Rahmen der Analyse des jeweiligen Tools wurden die Daten- und Informationsquellen zusammengefasst, sodass deren Schnittmenge und deren Verwendung innerhalb der getesteten Software erstellt wurde. Das Ergebnis ist in der folgenden Tabelle sichtbar.

Tabelle 10: Schnittmenge der Quellen

Quellen				
Quelle	SpiderFoot	Maltego	Recon-ng	theHarvester
Anubis-DB				x
Baidu				x
Bing	x		x	x
Bufferoverrun				x
Certs Spotter	x			x
Certificate Search				x
DNSdumpster				x
DuckDuckGo	x			x
Github	x		x	x
Google	x		x	x
Hacker Target	x		x	x
n45ht				x
Omnisint				x
OTX (AlienVault)	x	x		x
Qwant				x
RapidDNS				x
ThreatCrowd	x	x	x	x
ThreatMiner	x	x	x	x
Trello				x
URLScan	x			x
ViewDNS	x		x	
Whoxy	x		x	
Whois ARIN			x	
Have I been pwned	x	x	x	
Hashes.org			x	
PGP Key Owner	x		x	
Open Passive DNS Database	x			

Der Vergleich der verwendeten Ressourcen hat ergeben, dass die folgenden Dienste von allen vier Tools verwendet werden, unabhängig davon, ob die freie API oder eine kostenpflichtige verwenden wird:

- ThreatCrowd
- ThreatMiner

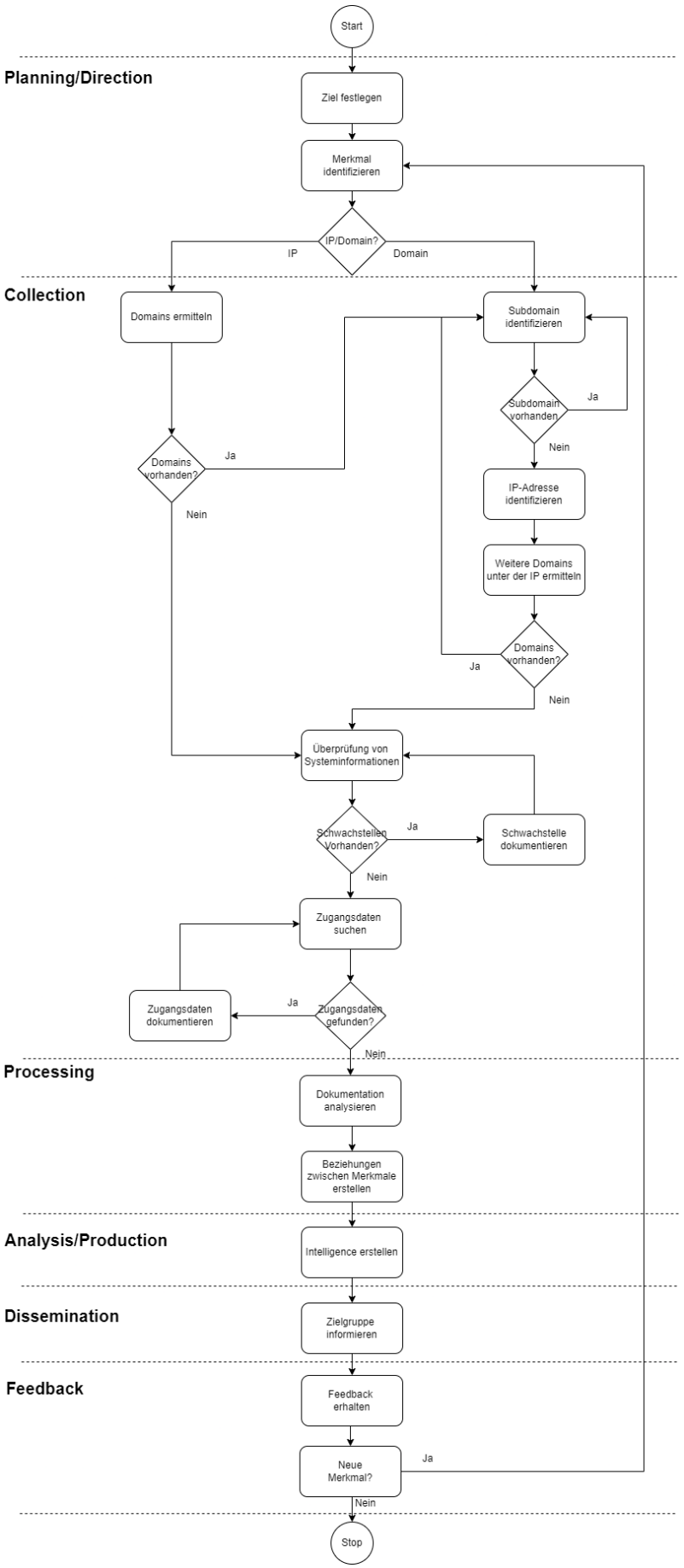
Es konnte festgestellt werden, dass mehrere Ressourcen von mindestens drei der Tools verwendet werden:

- ThreatCrowd
- ThreatMiner
- Bing
- Github
- Google
- Hacker Target
- OTX (AlienVault)
- Have I been pwned

5 Strategie zur passiven Informationsbeschaffung

In diesem Kapitel wird eine Strategie präsentiert, die die Zielgruppe bei der passiven Aufklärung der Angriffsflächen von IT-Infrastrukturen unterstützen soll. Sie basiert auf den Phasen des Intelligence Cycles und zeigt eine mögliche strukturierte Vorgehensweise zur Identifizierung von relevanten Indikatoren unter der Benutzung verschiedener Tools. Für die Erstellung der Strategie wurde auch die Phase *Feedback* berücksichtigt. In der folgenden Abbildung wird eine beispielhafte Vorgehensweise präsentiert, die sich um weitere Vorgänge erweitern lässt.

Bild 13: Ablaufdiagramm OSINT



Quelle: eigene Darstellung

5.1 Anforderungen festlegen

5.1.1 Allgemeinheiten

Am Anfang der Aufklärungstätigkeit müssen die Anforderungen festgelegt werden. Fehlende Anforderungen können den gesamten Ablauf einer OSINT-Aufklärung stören. Als Anforderung kann beispielsweise die Domäne oder die feste IP-Adresse eines Aufklärungszieles betrachtet werden. Des Weiteren ist eine Zielsetzung notwendig. Somit muss festgelegt werden, welche Informationen gesammelt werden und welchem Zweck die OSINT-Recherche dienen soll. Weiterhin müssen die Quellen und die Tools zur Beschaffung der Informationen bekannt sein und festgelegt werden. Um die Festlegung der Anforderungen zu dokumentieren, kann auf ein Collection Management Framework (CMF) zugegriffen werden. Das IT-Sicherheitsunternehmen Dragos fertigte ein Collection Management Framework zur Vorbereitung von Reaktionen auf Cyberangriffe im Bereich der Industrial Control Systems (ICS) an[105, S. 8]. Darauf basierend, kann ein Framework zur Aufklärung von Angriffsflächen entwickelt werden. Ein beispielhaftes Modell ist in der folgenden Tabelle dargestellt. Dazu können Tools wie LibreOffice Calc verwendet werden.

Tabelle 11: Beispiel eines Collection Management Frameworks

	IP-Adresse	Domain	Subdomain	Schwachstelle	Zugangsdaten
ViewDNS					
DNS Dumpster					
WHOIS DomainTools					

Quelle: angelehnt an der Tabelle aus Dragos [105, S. 8]

5.1.2 Beispiel

Im folgenden Beispiel wurde zur Initiierung des Intelligence Cycles die Domain **hs-wismar.de** ausgewählt. Darauf soll die dahinterstehende Infrastruktur passiv mittels OSINT-Tools aufgeklärt werden. Im Gegensatz zu den im Kapitel Bewertung ausgewerteten Tools sollen in diesem Fall einzelne Softwarepakete (auch diejenigen, die eine Anmeldung bedürfen) gezielt eingesetzt werden. Die nächste Abbildung zeigt die Festlegung der Tools und der aufzuklärenden Merkmale für das analysierte Beispiel.

Tabelle 12: Liste der Tools und der aufzuklärenden Merkmale

	IP-Adresse	Domain	Subdomain	Schwachstelle	Zugangsdaten	Phase
ViewDNS	x	x	x	-	-	B
DNS Dumpster	x	x	x	x	-	B
WHOIS DomainTools	x	x	x	-	-	B
Google	x	x	x	x	x	B
Shodan	x	x	x	x	-	B
Censys	x	x	x	x	-	B
Intelligence X	-	-	-	-	x	B
Haveibeenpwned	-	-	-	-	x	B
Maltego	x	x	x	x	x	A
LibreOffice Calc	x	x	x	x	x	V

Legende:
P = Anforderungen festlegen (Phase I im Intelligence Cycle)
B = Aufklärung/Beschaffung (Phase II im Intelligence Cycle)
V = Verarbeitung (Phase III im Intelligence Cycle
A = Analyse (Phase IV im Intelligence Cycle)
D = Verbreitung (Phase V im Intelligence Cycle)
R = Rückmeldung (Phase VI im Intelligence Cycle)

5.2 Aufklärung

Nachdem in der ersten Phase die Anforderungen festgelegt wurden, wird in der zweiten Phase mit der eigentlichen Sammlung von Informationen begonnen. Hierzu können sowohl automatisierte Tools, wie die im Kapitel Abgrenzung beschriebenen, die auf mehrere Softwarepakete oder Quellen zugreifen als auch einzelne Softwares wie z.B. die Suchmaschine Shodan, DNS Dumpster, ViewDNS, WHOIS-Tools, externe Datenbanken etc., verwendet werden.

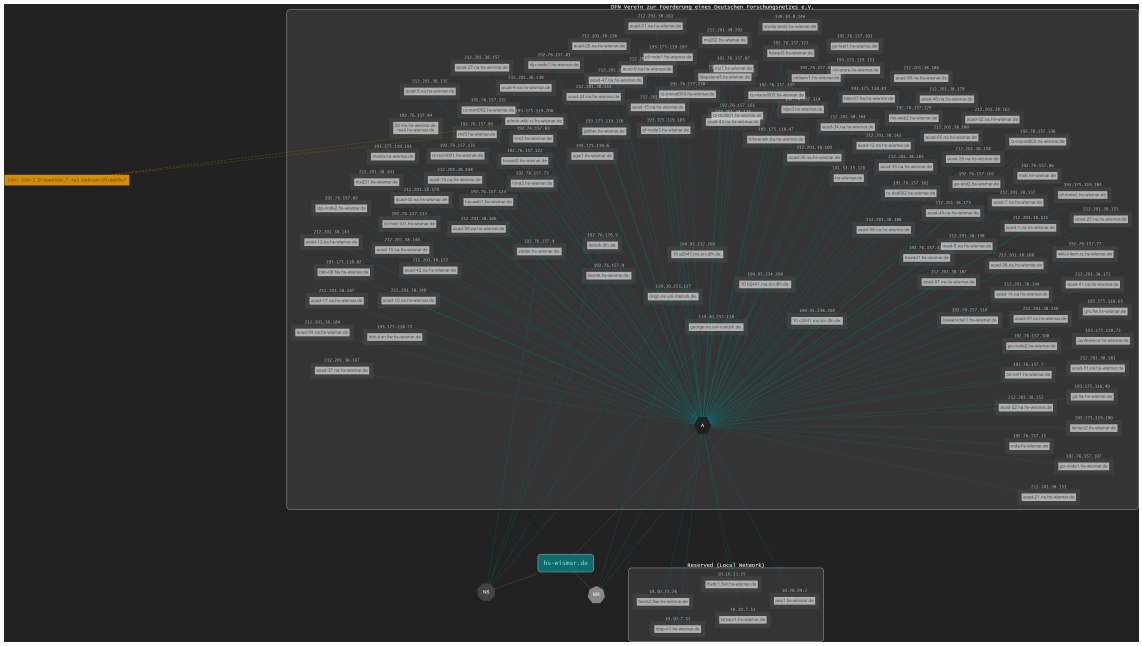
5.2.1 Aufklärung von Domains

Sollte der Startpunkt eine Domäne sein, kann beispielsweise auf DNS Dumpster gesetzet werden und damit eine Übersicht der Subdomains, der zugehörigen IP-Adressen und der einzelnen Systeme hinter den Merkmalen geschaffen werden. Sollte jedoch die IP-Adresse einer Domäne ermittelt werden, ist es möglich, eine WHOIS-Anfrage an einen Dienst wie z.B. WHOIS `https://whois.domaintools.com/` zu senden. Dadurch werden die aktuelle IP-Adresse sowie weitere Informationen wie das Land, in dem die Domäne gehostet wird, ermittelt.

Beispiel - DNS Dumpster

Hierzu wurde der Dienst `https://DNSDumpster.com/` verwendet. Die Eingabe des Merkmals **hs-wismar.de** hat ergeben, dass 110 Subdomains vorhanden sind. Zu den einzelnen Subdomains wurden die zugehörige IP-Adresse, der Netblock-Owner, das zugehörige Land sowie einzelne Informationen über laufende Systeme identifiziert (siehe Abbildung Ausgabe DNS Dumpster zu *hs-wismar.de*).

Bild 14: Ausgabe DNS Dumpster zu *hs-wismar.de*



Quelle: Export DNS Dumpster

5.2.2 Aufklärung von IP-Adressen

Wird eine IP-Adresse als Startpunkt verwendet, kann im ersten Schritt eine Ermittlung der Domains, die auf der IP-Adresse gehostet sind, erfolgen. Dazu kann beispielsweise das Tool ViewDNS `https://viewdns.info/` verwendet werden.

Beispiel

Nach der Eingabe der IP-Adresse **141.43.15.120** im Dienst ViewDNS ergab sich die Existenz von 17 Domains, die auf dem Server mit der IP gehostet waren (siehe Abbildung Ausgabe ViewDNS zu *141.43.15.120*). Dazu wurde außerdem das Datum der letzten DNS-Auflösung ermittelt.

Bild 15: Ausgabe ViewDNS zu *141.43.15.120*

Domain	Last Resolved Date
fh-stralsund.de	2022-04-16
fh-wismar.de	2022-04-16
hmt-rostock.de	2022-04-16
hochschule-neubrandenburg.de	2022-04-16
hochschule-neubrandenburg.eu	2022-04-12
hochschule-stralsund.de	2022-04-16
hs-nb.de	2022-04-16
hs-neubrandenburg.de	2022-04-16
hs-neubrandenburg.eu	2022-04-12
hs-wismar.de	2022-04-18
ieeg-greifswald.de	2022-04-16
iib-ev.de	2022-04-16
mathe-mv.de	2022-04-16
spp-antarktisforschung.de	2018-10-04
uni-greifswald.de	2022-04-16
wiko-greifswald.de	2022-04-16
young-academy-rostock.de	2022-04-16

Quelle: eigener Screenshot ViewDNS

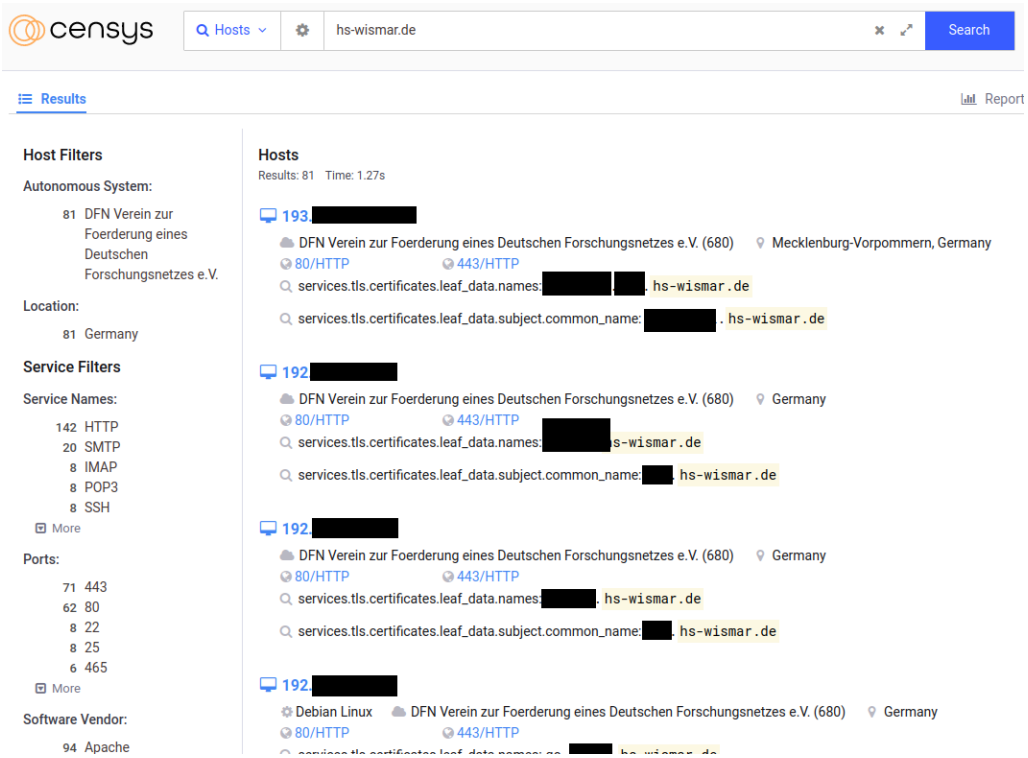
5.2.3 Aufklärung von Systeminformationen

Um Informationen der laufenden Dienste eines Systems passiv zu sammeln, kann der Einsatz der Suchmaschinen *Shodan, ZoomEye* oder *Censys* erfolgen. Hiermit können Informationen über offene Ports, laufende Dienste oder über die Version der eingesetzten Software gesammelt werden. Solche Informationen können unter Umständen Auskunft über die ausnutzbaren Schwachstellen geben. Weiterhin können Google-Suchanfragen (eng. dorks) verwendet werden. Dazu stehen verschiedene Operatoren zur Auswahl. Beispiele dafür können auf der Webseite `https://www.exploit-db.com/google-hacking-database` eingesehen werden.

Beispiel - Censys

Die Eingabe des Merkmals **hs-wismar.de** in der Suchmaschine *Censys* lieferte Auskunft über 20 offene Ports, den Einsatz von Produkten wie den Webserver Apache, VMware, Ubuntu, etc. oder über 7 unterschiedliche laufende Dienste wie LDAP, SMTP, oder SSH (siehe Abbildung Auszug der Ausgabe in Censys zu *hs-wismar.de*).

Bild 16: Auszug der Ausgabe in Censys zu *hs-wismar.de*

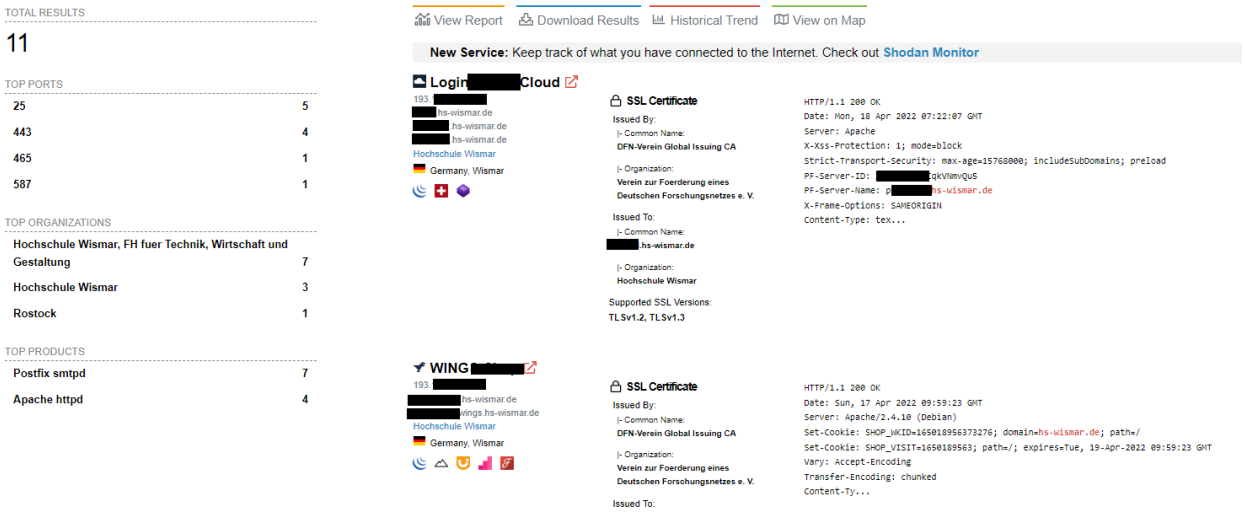


Quelle: eigener Screenshot Censys

Beispiel - Shodan

Die Eingabe des Merkmals **hs-wismar.de** in der Suchmaschine *Shodan* lieferte Auskunft über 4 offene Ports oder den Einsatz von Produkten wie Apache (siehe Abbildung Auszug der Ausgabe in Shodan zu *hs-wismar.de*).

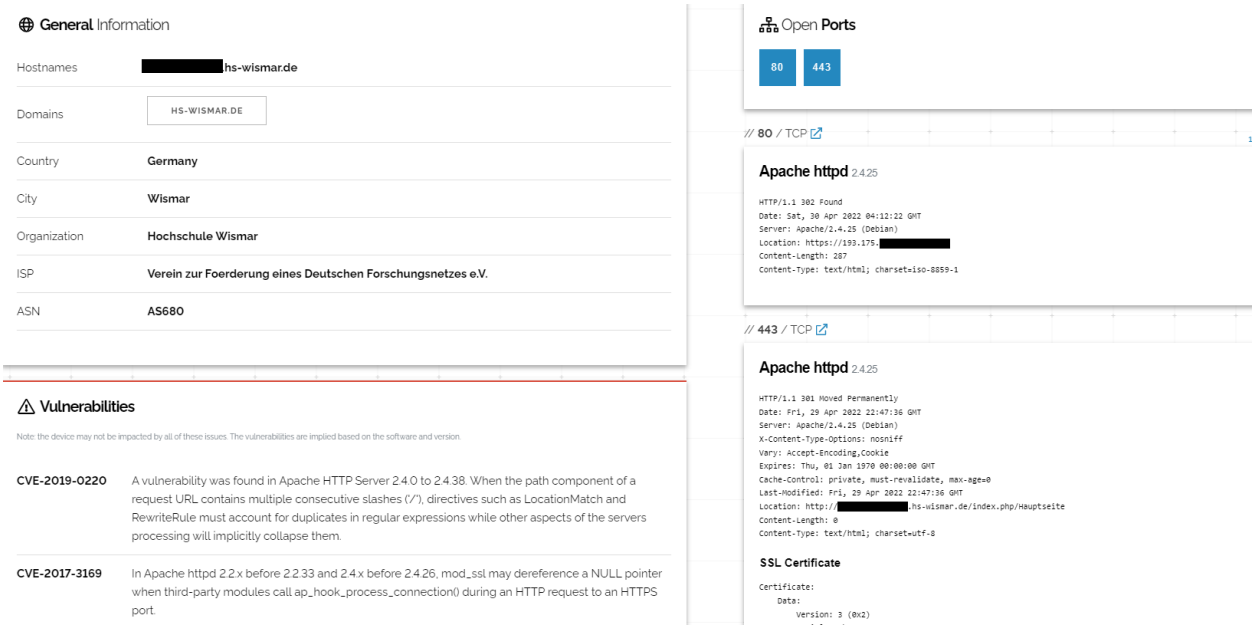
Bild 17: Auszug der Ausgabe in Shodan zu *hs-wismar.de*



Quelle: eigener Screenshot Shodan

Im Rahmen der Analyse wurden mehrere Server identifiziert, die laut Shodan über anfällige Apache-Versionen verfügten. Nach einem Informationsaustausch mit dem zuständigen Administrator an der Hochschule Wismar über die mutmaßlich anfälligen Server hat sich herausgestellt, dass es sich dabei um eine falsch-positive Erkennung der Suchmaschine handelte. Die gemeldeten Server waren auf dem aktuellsten Stand, jedoch meldete Shodan die veraltete Version des Servers aufgrund eines Backports eines Security-Patches für eine ältere Version des Betriebssystems. Die dankenswerterweise erfolgte Rückmeldung des Administrators ist der Beweis, dass der Einsatz von OSINT-Tools nicht zu 100% zuverlässig ist und Platz für falsch-positive Ergebnisse lässt. Die Ausgabe zu einem der mutmaßlich anfälligen Server ist in der nächsten Abbildung zu sehen.

Bild 18: Auszug der Ausgabe in Shodan zum mutmaßlich anfälligen Server



Quelle: eigener Screenshot Shodan

5.2.4 Aufklärung von abgeflossenen Zugangsdaten

Geleakte Zugangsdaten können dazu verwendet werden, um Zugriff auf Systeme zu erlangen, die zur Anmeldung gedient haben. Weiterhin kann eine Leak-Quelle auch ein Zeichen für eine Infektion mit Schadcode sein. Der Dienst *Have I been pwned? (`https://haveibeenpwned.com/`)* bietet die Möglichkeit eine E-Mail-Adresse auf Betroffenheit im Rahmen eines Leaks zu überprüfen. Weiterhin kann der OSINT-Dienst *Intelligence X (`https://intelx.io/`)* zur Suche nach abgeflossenen Zugangsdaten verwendet werden. In der Regel wird allerdings dazu ein kostenpflichtiger Zugang benötigt. Die freie Version bietet jedoch auch Auskunft über mögliche geleakte Daten[106].

Beispiel - Intelligence X

Die Eingabe der Domäne **hs-wismar.de** in die kostenfreie Variante des Dienstes hat die Existenz zweier E-Mail-Adressen ergeben. Aus Sicherheitsgründen werden diese in der vorliegenden Arbeit unkenntlich gemacht.

- m*****d.a*n@hs-wismar.de:z****d
- h**s-e**er*t.r*****s@hs-wismar.de:p***x

Beispiel - Haveibeenpwned

Die Eingabe beider E-Mail-Adressen lieferte Auskunft über die mögliche Quelle des Datenleaks. Somit konnten die folgenden Datenlecks ermittelt werden:

- m*****d.a*n@hs-wismar.de: Anti Public Combo List, Collection #1, Onliner Spambot, Verifications.io, LinkedIn, MySpace, Trik Spam Botnet, You've Been Scraped Data Enrichment Exposure From PDL Customer
- h**s-e**er*t.r*****s@hs-wismar.de: Anti Public Combo List, Collection #1, MDPI, Onliner Spambot, Verifications.io;

5.3 Verarbeitung von Daten

Während der OSINT-Analyse können Daten gesammelt werden, die für den Auftrag nicht benötigt werden. Wie im Kapitel Processing erläutert, werden in dieser Phase die gesammelten Daten so verarbeitet und organisiert, dass nur die benötigten Daten erhalten bleiben. Aus diesem Grund sind eine Sichtung und eine Filterung nötig. Am Beispiel der IP-Adresse 141.43.15.120 kann in der Abbildung Ausgabe ViewDNS zu *141.43.15.120* erkannt werden, dass neben der Domäne der Hochschule Wismar auch weitere Domänen vorhanden sind, die mutmaßlich anderen Institutionen gehören. Ein Teil dieser Daten wird allerdings nicht weiter benötigt und muss daher in dieser Phase ausgeschlossen werden. Um die Vereinfachung der Recherche zu ermöglichen, müssen die Daten in einem standardisierten Format gespeichert werden (siehe Kapitel Processing). Weiterhin gehört auch eine mögliche Übersetzung von Daten dieser Phase an. Hierzu kann auf verschiedene Tools zugegriffen werden, z.B. auf die Übersetzungsmaschinen **DeepL** oder **Google Übersetzer**.

Beispiel - XLSX als Standardformat für Dateien

Die Daten wurde aus DNS Dumpster als XLSX-Datei exportiert, sodass sie in Maltego zur Analyse importiert werden können. Zur Betrachtung und Entfernung von Duplikaten wurde die Software LibreOffice Calc verwendet (siehe Abbildung Processing: Auszug aus LibreOffice Calc).

Bild 19: Processing: Auszug aus LibreOffice Calc

Hostname	IP Address	Type	Reverse DNS	Netblock Owner	Country
[redacted]mar.de	141.[redacted]	A	[redacted]-greifswald.de	DFN Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.	Germany
[redacted].hs-wismar.de	212.[redacted]	A	[redacted].hs-wismar.de	DFN Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.	Germany
[redacted]-wismar.de	10.[redacted]	A		Reserved (Local Network)	unknown

Quelle: eigener Screenshot LibreOffice Calc

5.4 Analyse von Informationen

Wie im Buch ‚OSSTMM 3 – The Open Source Security Testing Methodology Manual' beschrieben, ist die Analyse fähig, Informationen in Intelligence umzuwandeln[107, S. 54]. Herzog beschreibt in seinem Buch sechs Schritte, um Informationen zu analysieren:

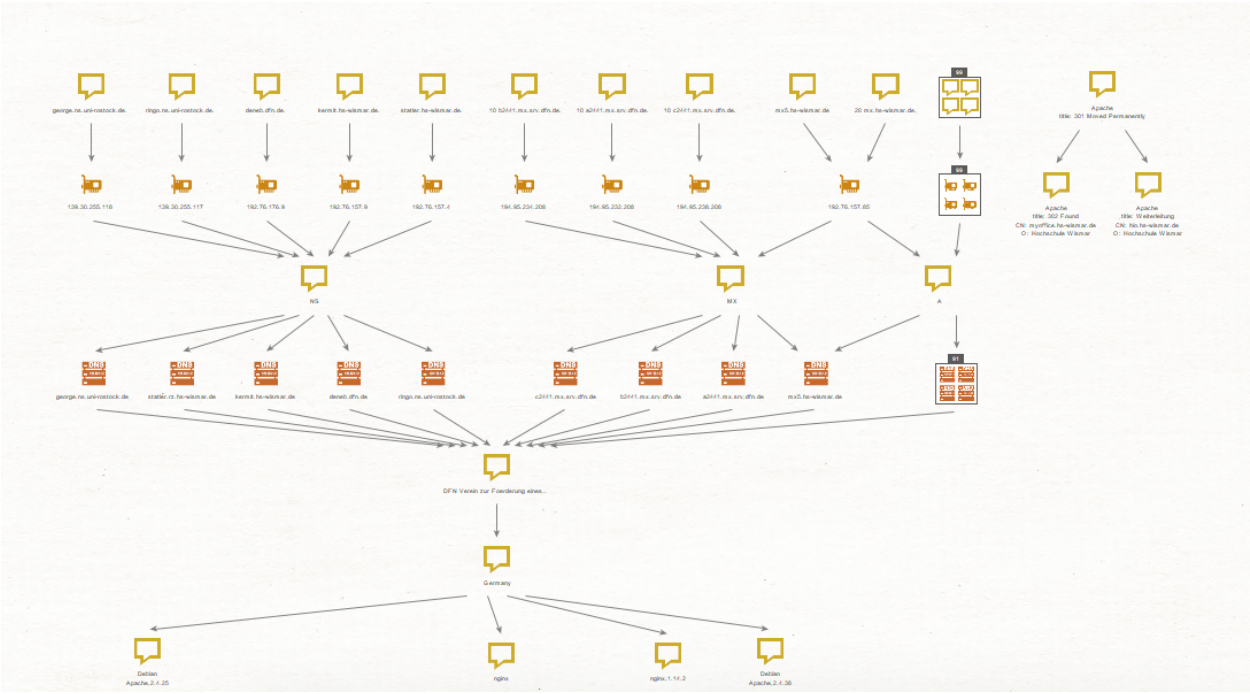
1. „Bauen Sie Ihr Wissen über das Ziel aus einer Vielzahl aktueller, sachlicher Quellen auf und vermeiden Sie kommerziell voreingenommene und spekulative Informationen"[107, S. 54].
2. „Bestimmen Sie den globalen Erfahrungsstand für die Art des Ziels und den Umfang der Informationen, die darüber bekannt sein könnten"[107, S. 54].
3. „Ermitteln Sie etwaige Voreingenommenheit oder Hintergedanken der Informationsquellen"[107, S. 54].
4. „Übersetzen Sie den Fachjargon der Informationsquellen zum Vergleich in ähnliche oder bekannte Wörter, denn was neu oder kompliziert klingt, ist vielleicht nur ein Trick, um etwas Gewöhnliches zu unterscheiden"[107, S. 54].
5. „Sich vergewissern, dass die Testgeräte richtig kalibriert sind und die Testumgebung überprüft wurde, um sicherzustellen, dass die Ergebnisse nicht durch den Test selbst verunreinigt werden"[107, S. 54].
6. „Sicherstellen, dass der Übersetzungszustand von Werkzeugen oder Prüfverfahren so weit wie möglich entfernt wurde, damit die Ergebnisse nicht von den indirekten Quellen in einem Prozess oder der Voranalyse einiger Werkzeuge stammen"[107, S. 54].

Ein gutes Beispiel zur Analyse von Informationen ist das Schwachstellenmanagement. Nach Recorder Future geht es bei der Analyse von Schwachstellen nicht um die Beseitigung der meisten Schwachstellen, sondern um die Schließung derjenigen, die für eine Organisation das höchste Exploit-Risiko haben[14, S. 55]. Die besonders gefährlichen Schwachstellen können durch die Schnittmenge zwischen Sicherheitslücken in der untersuchten Umgebung und denjenigen, die tatsächlich ausgenutzt werden, bestimmt werden[14, S. 56]. Informationen über aktuelle Schwachstellen können beispielsweise auf der Homepage der CERT-Bund unter `https://www.cert-bund.de/overview/AdvisoryShort` eingesehen werden.
Es werden jährlich ca. 8 000 Schwachstellen entdeckt[14, S. 54]. Die Anzahl der neuen Schwachstellen in Kombination mit einer großen IT-Infrastruktur führt rasch zu einem Verlust des Überblicks und erzeugt einen enormen Aufwand bei der Analyse der Angriffsflächen. Aus diesem Grund sollen so viele automatisierte Tools wie möglich eingesetzt werden, die die Daten analysieren.

Beispiel - Maltego

Als Beispiel wurde die Analysefunktion von Maltego verwendet. Es wurden zur Analyse die Ergebnisse des Tools DNS Dumpster aus dem Kapitel Beispiel - DNS Dumpster importiert. Die Daten wurden in Maltego hierarchisch dargestellt, sodass die Zusammenhänge zwischen den einzelnen Objekten sichtbar waren. Maltego ermöglichte die automatische Erstellung von Verlinkungen und Beziehungen zwischen den einzelnen Entitäten (z.B. eine Beziehung zwischen einer Domäne und der dazugehörigen IP-Adresse, siehe dazu die Abbildung Auszug der Link-Analyse in Maltego).

Bild 20: Auszug der Link-Analyse in Maltego



Quelle: eigener Screenshot Maltego

5.5 Verteilung des Intelligence-Produktes

In dieser Phase wird das Ergebnis der Analyse dem Empfängerkreis übermittelt. Dem Handbuch des Department of the Army zufolge kann die Weitergabe der Informationen auf drei Wegen erfolgen: schriftlich, grafisch und mündlich[108, S. 4-11]. Die vorliegende Arbeit behandelt die schriftliche Weitergabe von Informationen.
Nach dem NATO OSINT Handbuch müssen die Berichte eine analytische Zusammenfassung beinhalten. Weiterhin sollen dem Handbuch nach auf der ersten Seite Angaben über die Zeit, in der die OSINT-Recherche durchgeführt wurde, gemacht werden[13, S. 30]. Im Rahmen von Penetrationstest ist laut dem BSI der Bericht das letzte Arbeitspaket des Prozesses. Aufgrund der möglichen Inhalte soll der Bericht nur einem ausgewähltem Kreis angeboten werden. Zur Einschränkung der Weitergabe des Dokuments kann der Einsatz von Vertraulichkeitskennzeichnungen erfolgen[109, S. 24]. Zum sicheren Informationsaustausch von nicht öffentlichen und vertraulichen Informationen kann auf das Traffic Light Protocol (TLP) zurückgegriffen werden. Der Einsatz der TLP-Einstufung bedarf der Zustimmung durch

Unterschrift der TLP-Erklärung durch an dem Informationsaustausch beteiligten natürlichen und juristischen Personen. Das BSI stellt dazu ein ‚Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), TLP-Version 17-11'. Zum Zeitpunkt der Erstellung dieser Arbeit wurde die TLP-Version 17-11 berücksichtigt[110, S. 1]. Es gibt vier TLP-Stufen:

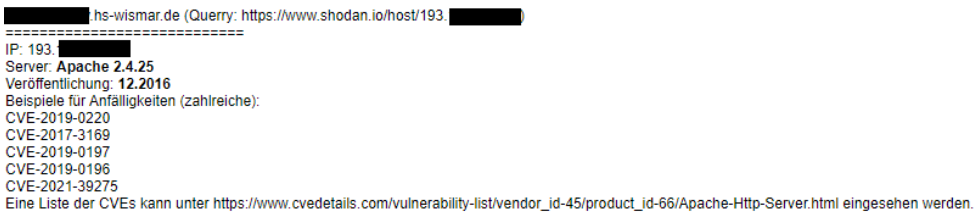
1. TLP:WHITE: Die Informationen dürfen ohne Einschränkungen weitergegeben werden[110, S. 2];
2. TLP:GREEN: Die Informationen dürfen innerhalb der Organisation und an den Partner weitergegeben, aber nicht veröffentlicht werden[110, S. 2];
3. TLP:AMBER: Die Informationen dürfen vom Empfänger innerhalb seiner Organisation nach dem Prinzip „Kenntnis nur, wenn nötig“ weitergegeben werden. Die Weitergabe auch an Dritte darf nur geschehen, wenn es dem Schutz des Empfängers oder der Schadensreduktion beim Empfänger dient[110, S. 2];
4. TLP:RED: Die Informationsweitergabe ist auf einen engen Kreis beschränkt und kann z.B. im Rahmen einer Besprechung, einer Video-/Audiokonferenz oder einer schriftlichen Korrespondenz erfolgen. Eine Weitergabe ist untersagt[110, S. 2].

Die aus der OSINT-Analyse gewonnenen Erkenntnisse müssen im Bericht dargestellt werden. Im Falle von aufgefundenen Schwachstellen sollen Angaben über deren Kritikalität gemacht werden. Dazu können die Industriestandards CVSSv2 oder DREAD verwendet werden[109, S. 25].

Beispiel - Meldung von vermutlichen Schwachstellen

Wie bereits im Kapitel Aufklärung von Systeminformationen erwähnt, wurden IT-Systeme der Hochschule als potenziell anfällig gemeldet. Die Übermittlung der Erkenntnisse an die Hochschule erfolgte via E-Mail. Ein Beispiel für die Übermittlung der Erkenntnisse ist in der nächsten Abbildung zu sehen.

Bild 21: Auszug aus der Übermittlung der Anfälligkeiten per E-Mail



Quelle: eigene Darstellung, Auszug aus der Übermittlung der Anfälligkeiten per E-Mail

5.6 Rückmeldung

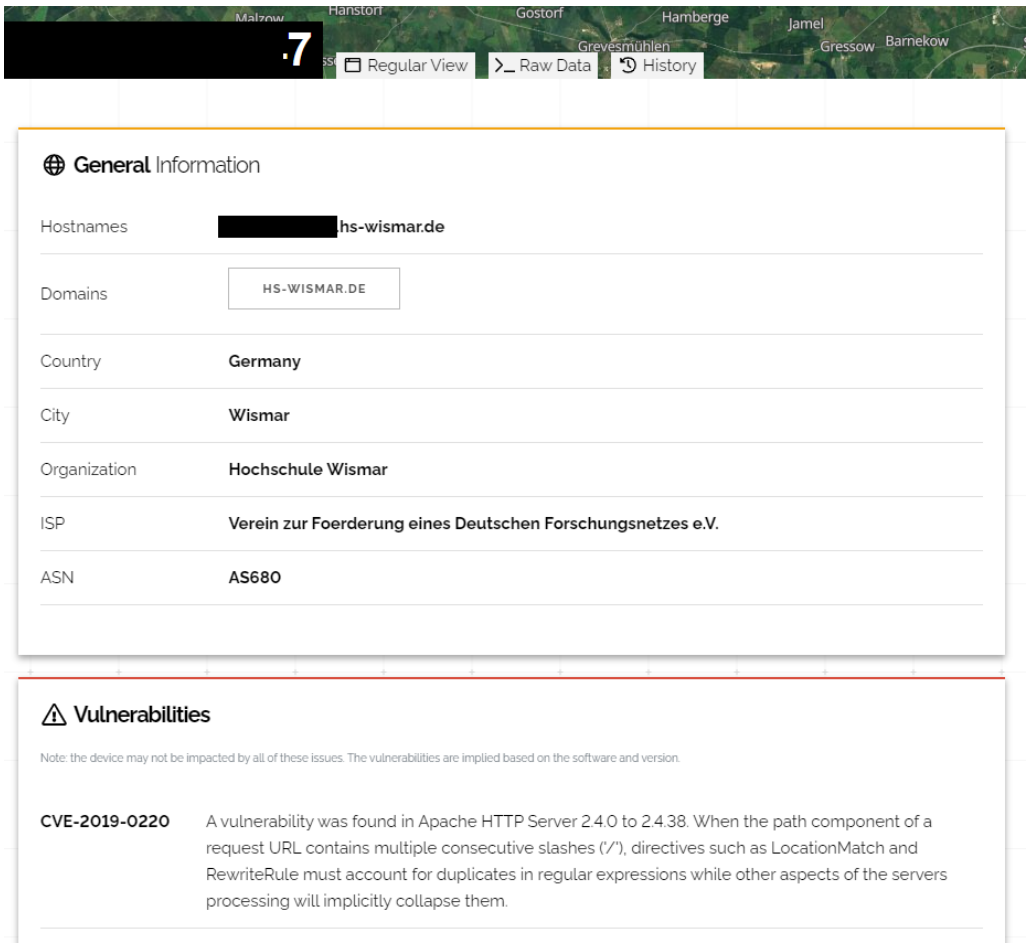
Obwohl die letzte Phase meistens vernachlässigt wird, hat sie für den Intelligence Cycle eine besondere Rolle. Durch sie können bei der Aufnahme einer OSINT-Recherche die Suchparameter oder die Kriterien verbessert werden, sodass das Intelligence-Produkt verbessert wird. Die Phase besteht nämlich aus der Rückmeldung der Zielgruppe. Roberts und Brown unterscheiden zwischen zwei Kategorien von Rückmeldungen[11, S. 200 - 201]:

- Technische Rückmeldung: Hierzu gibt die Zielgruppe Auskunft über die Informationen, die sie erhalten hat und darüber, ob diese den Anforderungen und Erwartungen entsprechen. Die OSINT-Recherche muss gegebenenfalls auf Basis von angepassten Kriterien erneut gestartet werden[11, S. 200].
- Formale Rückmeldung: Sie gibt Auskunft, ob das Ergebnis der Recherche nützlich für die Zielgruppe war[11, S. 201].

Beispiel - Rückmeldung von vermutlichen Schwachstellen

Im Rahmen der vorliegenden Masterarbeit wurden mithilfe der Suchmaschine Shodan mehrere vermeintlich anfällige Server im Netzbereich der Hochschule Wismar entdeckt (siehe Kapitel Aufklärung von Systeminformationen). Die vermeintlichen Schwachstellen wurden der zuständigen Stelle gemeldet. Die Rückmeldung des zuständigen IT-Administrators hat ergeben, dass die betroffenen Server auf dem neuesten Patchstand waren und somit nicht anfällig waren. Das ist ein Beispiel für die Bedeutsamkeit dieser Phase. Ein Beispiel für eine vermeintliche Schwachstelle ist in der nächsten Abbildung zu sehen.

Bild 22: Vermeintliche Schwachstelle



Quelle: eigener Screenshot Shodan

6 Zusammenfassung und Ausblick

6.1 Zusammenfassung

Innerhalb der Fragestellungen dieser Master-Thesis galt es, verschiedene Quellen, Softwares und Tools, die im Bereich Open Source Intelligence eingesetzt werden können, zu identifizieren, zu bewerten, miteinander zu vergleichen und sie mindestens einer Phase des Intelligence Cycles zuzuordnen. Weiterhin war der Aufbau einer Strategie zur Aufklärung von Angriffsflächen im Bereich der IT-Sicherheit auf Basis des Intelligence Cycles eine zentrale Aufgabe dieser Arbeit.
Im ersten Kapitel (siehe Kapitel Einleitung) wurden die wesentlichsten Begriffe und weitere Hintergrundinformationen aus dem Bereich Open Source Intelligence und IT-Sicherheit vermittelt. Als Nächstes wurden mehrere Strategien, die im Bereich *Intelligence* angewendet werden können, analysiert. Die Analyse begründete die Auswahl des *Intelligence Cycles* als grundlegenden Baustein für die Bewertung der OSINT-Tools und für den Aufbau der Strategie (siehe Kapitel Klassische Strategien zur Gewinnung von Informationen). Daraufhin wurden Tools uns Softwares anhand von Kriterien, die im Kapitel Bestimmung der Kriterien definiert wurden, bewertet und miteinander verglichen. Weiterhin wurden die Quellen, auf die diese Tools zugreifen, näher betrachtet (siehe Kapitel Schnittmenge der Quellen). Im Rahmen der Bewertung wurde außerdem die Zugehörigkeit des jeweiligen Tools im Intelligence Cycle ermittelt und ein Gesamtergebnis der Bewertung erstellt (siehe Kapitel Ergebnis der Bewertung). Das Bewertungsschema und die Vorgehensweise bei der Bewertung und Zuordnung im Intelligence Cycle von neuen Softwares und Tools kann als Grundlage verwendet werden. Somit wurde die erste Fragestellung dieser Master-Thesis beantwortet.
Des Weiteren wurde eine Strategie auf Basis des Intelligence Cycles zur passiven Informationsbeschaffung erstellt und angewandt (siehe Kapitel Strategie zur passiven Informationsbeschaffung). Die Strategie erwies sich anhand von praktischen Beispielen als tauglich, um die Angriffsfläche von IT-Systemen aufzuklären.

Die vorliegende Arbeit lieferte eine strukturierte, wissenschaftlich aufgearbeitete Antwort auf die Frage:

Können Quellen, Softwares und Tools in eine auf dem Intelligence Cycle basierende Strategie integriert werden, sodass eine strukturierte Vorgehensweise mittels Open Source Intelligence bei der Erkennung der Angriffsflächen einer IT-Infrastruktur möglich wird?

6.2 Ausblick

Anzumerken ist, dass OSINT nicht immer eine 100% sichere Auskunft über ein System liefert. Die Aussage wurde im Kapitel Aufklärung von Systeminformationen nachgewiesen. Die Rückmeldung der Zielgruppe ist trivial, um das Intelligence-Produkt zu verbessern und die angewandten Softwares und Tools besser kennenzulernen. Die Menge der Informationen, die aus öffentlichen Quellen gewonnen werden können, sind eine Herausforderung bei der Analyse und Gewinnung von Erkenntnissen. Die Lösung besteht in der automatisierten Auswertung der Informationen mittels beispielsweise künstlicher Intelligenz.

A Bewertung SpiderFoot

Tabelle 13: Bewertungsmatrix für die Eingabeparameter - SpiderFoot

Eingabe	
Phase	erfüllt
E-Mail	x
Domain	x
IP	x
Credentials	x
Dateityp	-
SSL-Zertifikat	-
Port	-
Systeminformationen	-
Anzahl erfüllter Kriterien	4

Tabelle 14: Bewertungsmatrix für die Ausgabeparameter - SpiderFoot

Ausgabe	
Phase	erfüllt
E-Mail	x
Domain	x
IP	x
Credentials	x
Dateityp	-
SSL-Zertifikat	x
Port	-
Systeminformationen	x
Anzahl erfüllter Kriterien	6

Tabelle 15: Bewertungsmatrix für die Zuweisung innerhalb des Intelligence-Zyklus - SpiderFoot

Intelligence-Zyklus	
Phase	erfüllt
Planning/Direction	-
Collection	x
Processing	-
Analysis/Production	-
Dissemination	-
Anzahl erfüllter Phasen	1

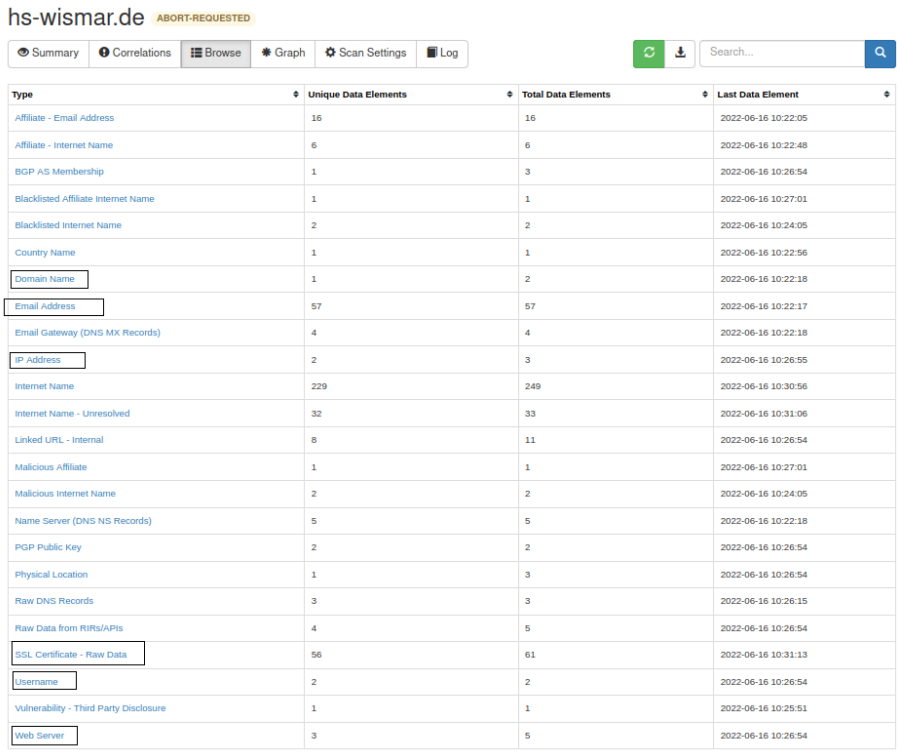
Gesamtergebnis

m1 = 4 (Anzahl erfüllter eingegeben Kriterien)
m2 = 6 (Anzahl erfüllter ausgegeben Kriterien)
m3 = 1 (Anzahl erfüllter Phasen des Intelligence-Zyklus)

$$Gesamtergebnis = (\sum_{n=1}^{m1} 1 + \sum_{n=1}^{m2} 1) * \sum_{n=1}^{m3} 1$$

Gesamtergebnis = 10

Bild 23: Screenshot SpiderFoot Ergebnisse



hs-wismar.de ABORT-REQUESTED

Summary | Correlations | Browse | Graph | Scan Settings | Log

Search...

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Email Address	16	16	2022-06-16 10:22:05
Affiliate - Internet Name	6	6	2022-06-16 10:22:48
BGP AS Membership	1	3	2022-06-16 10:26:54
Blacklisted Affiliate Internet Name	1	1	2022-06-16 10:27:01
Blacklisted Internet Name	2	2	2022-06-16 10:24:05
Country Name	1	1	2022-06-16 10:22:56
Domain Name	1	2	2022-06-16 10:22:18
Email Address	57	57	2022-06-16 10:22:17
Email Gateway (DNS MX Records)	4	4	2022-06-16 10:22:18
IP Address	2	3	2022-06-16 10:26:55
Internet Name	229	249	2022-06-16 10:30:56
Internet Name - Unresolved	32	33	2022-06-16 10:31:06
Linked URL - Internal	8	11	2022-06-16 10:26:54
Malicious Affiliate	1	1	2022-06-16 10:27:01
Malicious Internet Name	2	2	2022-06-16 10:24:05
Name Server (DNS NS Records)	5	5	2022-06-16 10:22:18
PGP Public Key	2	2	2022-06-16 10:26:54
Physical Location	1	3	2022-06-16 10:26:54
Raw DNS Records	3	3	2022-06-16 10:26:15
Raw Data from RIRs/APIs	4	5	2022-06-16 10:26:54
SSL Certificate - Raw Data	56	61	2022-06-16 10:31:13
Username	2	2	2022-06-16 10:26:54
Vulnerability - Third Party Disclosure	1	1	2022-06-16 10:25:51
Web Server	3	5	2022-06-16 10:26:54

Quelle: eigene Darstellung, Screenshot der Softwareoberfläche

Detailliere Beispiele für die Ergebnisse befinden sich auf dem beilegten Datenträger unter **Ergebnisse_Auswertung/Ergebnisse_Spiderfoot**.

B Bewertung Maltego

Tabelle 16: Bewertungsmatrix für die Eingabeparameter - Maltego

Eingabe	
Phase	erfüllt
E-Mail	x
Domain	x
IP	x
Credentials	x
Dateityp	x
SSL-Zertifikat	x
Port	x
Systeminformationen	x
Anzahl erfüllter Kriterien	8

Tabelle 17: Bewertungsmatrix für die Ausgabeparameter - Maltego

Ausgabe	
Phase	erfüllt
E-Mail	x
Domain	x
IP	x
Credentials	-
Dateityp	-
SSL-Zertifikat	-
Port	-
Systeminformationen	-
Anzahl erfüllter Kriterien	3

Tabelle 18: Bewertungsmatrix für die Zuweisung innerhalb des Intelligence Cycle - Maltego

Intelligence-Zyklus	
Phase	erfüllt
Planning/Direction	x
Collection	x
Processing	x
Analysis/Production	x
Dissemination	x
Anzahl erfüllter Phasen	5

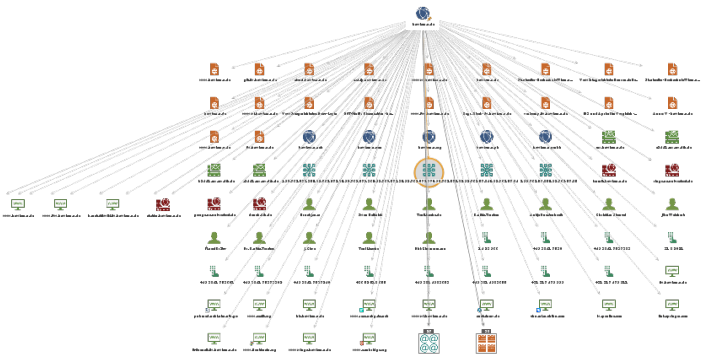
Gesamtergebnis

m1 = 8 (Anzahl erfüllter eingegeben Kriterien)
m2 = 3 (Anzahl erfüllter ausgegeben Kriterien)
m3 = 5 (Anzahl erfüllter Phasen des Intelligence-Zyklus)

$$Gesamtergebnis = (\sum_{n=1}^{m1} 1 + \sum_{n=1}^{m2} 1) * \sum_{n=1}^{m3} 1$$

Gesamtergebnis = 55

Bild 24: Screenshot Maltego Ergebnisse



Quelle: eigene Darstellung, Screenshot der Softwareoberfläche

C Bewertung Recon-ng

Tabelle 19: Bewertungsmatrix für die Eingabeparameter - Recon-ng

Eingabe	
Phase	erfüllt
E-Mail	-
Domain	x
IP	-
Credentials	-
Dateityp	-
SSL-Zertifikat	-
Port	-
Systeminformationen	-
Anzahl erfüllter Kriterien	1

Tabelle 20: Bewertungsmatrix für die Ausgabeparameter - Recon-ng

Ausgabe	
Phase	erfüllt
E-Mail	x
Domain	x
IP	x
Credentials	-
Dateityp	-
SSL-Zertifikat	-
Port	-
Systeminformationen	-
Anzahl erfüllter Kriterien	3

Tabelle 21: Bewertungsmatrix für die Zuweisung innerhalb des Intelligence Cycle - Recon-ng

Intelligence-Zyklus	
Phase	erfüllt
Planning/Direction	-
Collection	x
Processing	-
Analysis/Production	-
Dissemination	-
Anzahl erfüllter Phasen	1

Gesamtergebnis

m1 = 1 (Anzahl erfüllter eingegeben Kriterien)
m2 = 3 (Anzahl erfüllter ausgegeben Kriterien)
m3 = 1 (Anzahl erfüllter Phasen des Intelligence-Cycles)

$$Gesamtergebnis = (\sum_{n=1}^{m1} 1 + \sum_{n=1}^{m2} 1) * \sum_{n=1}^{m3} 1$$

Gesamtergebnis = 4

Auszug aus dem Ergebnis E-Mail-Adressen:

- a***.n******@hs-wismar.d
- t.l******@stud.hs-wismar.de
- sh********@hs-wismar.de
- hi******@hs-wismar.de
- e****.j****@hs-wismar.de

IP-Adressen:

- 212.xxx.37.xxx
- 212.xxx.38.xx
- 10.xx.23.xx

- 193.xxx.241.xx
- 192.xx.157.xxx

Hosts:

- it-forensik.fiw.hs-wismar.de
- vpn.hs-wismar.de
- hio.hs-wismar.de
- vdi-sec.fiw.hs-wismar.de
- ums.hs-wismar.de

Domains:

- wings-architecture.com
- wings-fernhochschule.com
- wings-fernhochschule.info
- wingsuniversity.com
- wings-fernstudium.at

Die Liste aller Ergebnisse befindet sich auf dem beigelegtem Datenträger unter **Ergebnisse_Auswertung/Ausgabe_recon_ng_full.txt**.

Angepasstes Shell-Skript

Das Originalskript ist unter `https://github.com/SamShanks1/automated-recon-ng` (Aufgerufen am 09.04.2022) vorhanden.

```
#!/bin/bash
domain=$1
# input from command-line becomes company to test
company=$2
#run as bash enum2all.sh Domain.com Company
#timestamp
stamp=$(date +"%m_%d_%Y")
path=$(pwd)
#create rc file with workspace.timestamp and start enumerating hosts
touch $company-$domain$stamp.resource
echo "spool start $domain$stamp.log" >> $domain$stamp.resource
echo "Domain:" $domain
echo "Company:" $company
echo "workspaces create $domain$stamp"
echo "workspaces load $domain$stamp" >> $domain$stamp.resource
echo "workspaces create $domain$stamp" >> $domain$stamp.resource
echo "workspaces load $domain$stamp" >> $domain$stamp.resource
echo "modules load recon/companies-contacts/pen" >> $domain$stamp.resource
```

```
19 echo "options set SOURCE $domain" >> $domain$stamp.resource
20 echo "run" >> $domain$stamp.resource
21 echo "modules load recon/companies-domains/pen" >> $domain$stamp.resource
22 echo "options set SOURCE $domain" >> $domain$stamp.resource
23 echo "run" >> $domain$stamp.resource
24 echo "modules load recon/companies-domains/viewdns_reverse_whois" >> $domain$stamp.
       resource
25 echo "options set SOURCE $domain" >> $domain$stamp.resource
26 echo "run" >> $domain$stamp.resource
27 echo "modules load recon/companies-multi/whois_miner" >> $domain$stamp.resource
28 echo "options set SOURCE $domain" >> $domain$stamp.resource
29 echo "run" >> $domain$stamp.resource
30 echo "modules load recon/contacts-contacts/mailtester" >> $domain$stamp.resource
31 echo "options set SOURCE $domain" >> $domain$stamp.resource
32 echo "run" >> $domain$stamp.resource
33 echo "modules load recon/contacts-contacts/mangle" >> $domain$stamp.resource
34 echo "options set SOURCE $domain" >> $domain$stamp.resource
35 echo "run" >> $domain$stamp.resource
36 echo "modules load recon/contacts-contacts/unmangle" >> $domain$stamp.resource
37 echo "options set SOURCE $domain" >> $domain$stamp.resource
38 echo "run" >> $domain$stamp.resource
39 echo "modules load recon/contacts-domains/migrate_contacts" >> $domain$stamp.
       resource
40 echo "options set SOURCE $domain" >> $domain$stamp.resource
41 echo "run" >> $domain$stamp.resource
42 echo "modules load recon/credentials-credentials/adobe" >> $domain$stamp.resource
43 echo "options set SOURCE $domain" >> $domain$stamp.resource
44 echo "run" >> $domain$stamp.resource
45 echo "modules load recon/credentials-credentials/bozocrack" >> $domain$stamp.
       resource
46 echo "options set SOURCE $domain" >> $domain$stamp.resource
47 echo "run" >> $domain$stamp.resource
48 echo "modules load recon/domains-companies/pen" >> $domain$stamp.resource
49 echo "options set SOURCE $domain" >> $domain$stamp.resource
50 echo "run" >> $domain$stamp.resource
51 echo "modules load recon/domains-contacts/pen" >> $domain$stamp.resource
52 echo "options set SOURCE $domain" >> $domain$stamp.resource
53 echo "run" >> $domain$stamp.resource
54 echo "modules load recon/domains-contacts/pgp_search" >> $domain$stamp.resource
55 echo "options set SOURCE $domain" >> $domain$stamp.resource
56 echo "run" >> $domain$stamp.resource
57 echo "modules load recon/domains-contacts/whois_pocs" >> $domain$stamp.resource
58 echo "options set SOURCE $domain" >> $domain$stamp.resource
59 echo "run" >> $domain$stamp.resource
60 echo "modules load recon/domains-contacts/wikileaker" >> $domain$stamp.resource
61 echo "options set SOURCE $domain" >> $domain$stamp.resource
62 echo "run" >> $domain$stamp.resource
63 echo "modules load recon/domains-credentials/pwnedlist/leak_lookup" >> $domain$stamp
       .resource
64 echo "options set SOURCE $domain" >> $domain$stamp.resource
65 echo "run" >> $domain$stamp.resource
66 echo "modules load recon/domains-hosts/bing_domain_web" >> $domain$stamp.resource
67 echo "options set SOURCE $domain" >> $domain$stamp.resource
68 echo "run" >> $domain$stamp.resource
69 echo "modules load recon/domains-hosts/certificate_transparency" >> $domain$stamp.
       resource
```

```
70 echo "options set SOURCE $domain" >> $domain$stamp.resource
71 echo "run" >> $domain$stamp.resource
72 echo "modules load recon/domains-hosts/google_site_web" >> $domain$stamp.resource
73 echo "options set SOURCE $domain" >> $domain$stamp.resource
74 echo "run" >> $domain$stamp.resource
75 echo "modules load recon/domains-hosts/hackertarget" >> $domain$stamp.resource
76 echo "options set SOURCE $domain" >> $domain$stamp.resource
77 echo "run" >> $domain$stamp.resource
78 echo "modules load recon/domains-hosts/mx_spf_ip" >> $domain$stamp.resource
79 echo "options set SOURCE $domain" >> $domain$stamp.resource
80 echo "run" >> $domain$stamp.resource
81 echo "modules load recon/domains-hosts/netcraft" >> $domain$stamp.resource
82 echo "options set SOURCE $domain" >> $domain$stamp.resource
83 echo "run" >> $domain$stamp.resource
84 echo "modules load recon/domains-hosts/ssl_san" >> $domain$stamp.resource
85 echo "options set SOURCE $domain" >> $domain$stamp.resource
86 echo "run" >> $domain$stamp.resource
87 echo "modules load recon/domains-hosts/threatcrowd" >> $domain$stamp.resource
88 echo "options set SOURCE $domain" >> $domain$stamp.resource
89 echo "run" >> $domain$stamp.resource
90 echo "modules load recon/domains-hosts/threatminer" >> $domain$stamp.resource
91 echo "options set SOURCE $domain" >> $domain$stamp.resource
92 echo "run" >> $domain$stamp.resource
93 echo "modules load recon/domains-vulnerabilities/ghdb" >> $domain$stamp.resource
94 echo "options set SOURCE $domain" >> $domain$stamp.resource
95 echo "run" >> $domain$stamp.resource
96 echo "modules load recon/domains-vulnerabilities/xssed" >> $domain$stamp.resource
97 echo "options set SOURCE $domain" >> $domain$stamp.resource
98 echo "run" >> $domain$stamp.resource
99 echo "modules load recon/hosts-domains/migrate_hosts" >> $domain$stamp.resource
100 echo "options set SOURCE $domain" >> $domain$stamp.resource
101 echo "run" >> $domain$stamp.resource
102 echo "modules load recon/hosts-hosts/resolve" >> $domain$stamp.resource
103 echo "options set SOURCE $domain" >> $domain$stamp.resource
104 echo "run" >> $domain$stamp.resource
105 echo "modules load recon/hosts-hosts/reverse_resolve" >> $domain$stamp.resource
106 echo "options set SOURCE $domain" >> $domain$stamp.resource
107 echo "run" >> $domain$stamp.resource
108 echo "modules load recon/hosts-hosts/ssltools" >> $domain$stamp.resource
109 echo "options set SOURCE $domain" >> $domain$stamp.resource
110 echo "run" >> $domain$stamp.resource
111 echo "modules load recon/hosts-locations/migrate_hosts" >> $domain$stamp.resource
112 echo "options set SOURCE $domain" >> $domain$stamp.resource
113 echo "run" >> $domain$stamp.resource
114 echo "modules load recon/netblocks-companies/whois_orgs" >> $domain$stamp.resource
115 echo "options set SOURCE $domain" >> $domain$stamp.resource
116 echo "run" >> $domain$stamp.resource
117 echo "modules load recon/netblocks-hosts/reverse_resolve" >> $domain$stamp.resource
118 echo "options set SOURCE $domain" >> $domain$stamp.resource
119 echo "run" >> $domain$stamp.resource
120 echo "modules load recon/netblocks-ports/census_2012" >> $domain$stamp.resource
121 echo "options set SOURCE $domain" >> $domain$stamp.resource
122 echo "run" >> $domain$stamp.resource
123 echo "modules load recon/ports-hosts/migrate_ports" >> $domain$stamp.resource
124 echo "options set SOURCE $domain" >> $domain$stamp.resource
125 echo "run" >> $domain$stamp.resource
```

```
126 echo "modules load recon/ports-hosts/ssl_scan" >> $domain$stamp.resource
127 echo "options set SOURCE $domain" >> $domain$stamp.resource
128 echo "run" >> $domain$stamp.resource
129 echo "modules load recon/profiles-contacts/dev_diver" >> $domain$stamp.resource
130 echo "options set SOURCE $domain" >> $domain$stamp.resource
131 echo "run" >> $domain$stamp.resource
132 echo "modules load recon/profiles-profiles/profiler" >> $domain$stamp.resource
133 echo "options set SOURCE $domain" >> $domain$stamp.resource
134 echo "run" >> $domain$stamp.resource
135 echo "modules load recon/repositories-vulnerabilities/gists_search" >> $domain$stamp
        .resource
136 echo "options set SOURCE $domain" >> $domain$stamp.resource
137 echo "run" >> $domain$stamp.resource
138 echo "modules load reporting/html" >> $domain$stamp.resource
139 echo "options set CREATOR Sam" >> $domain$stamp.resource
140 echo "options set CUSTOMER $domain" >> $domain$stamp.resource
141 echo "options set FILENAME $path/$domain.html" >> $domain$stamp.resource
142 echo "run" >> $domain$stamp.resource
143 echo "exit" >> $domain$stamp.resource
144 cd $HOME
145 cd recon-ng
146 ./recon-ng -r $path/$domain$stamp.resource
```

Listing 1: Angepasstes Shell-Skript

D Bewertung theHarvester

Tabelle 22: Bewertungsmatrix für die Eingabeparameter - theHarvester

Eingabe	
Phase	erfüllt
E-Mail	-
Domain	x
IP	-
Credentials	-
Dateityp	-
SSL-Zertifikat	-
Port	-
Systeminformationen	-
Anzahl erfüllter Kriterien	1

Tabelle 23: Bewertungsmatrix für die Ausgabeparameter - theHarvester

Ausgabe	
Phase	erfüllt
E-Mail	x
Domain	x
IP	x
Credentials	-
Dateityp	-
SSL-Zertifikat	-
Port	-
Systeminformationen	-
Anzahl erfüllter Kriterien	3

Tabelle 24: Bewertungsmatrix für die Zuweisung innerhalb des Intelligence-Zyklus - theHarvester

Intelligence-Zyklus	
Phase	erfüllt
Planning/Direction	-
Collection	x
Processing	-
Analysis/Production	-
Dissemination	-
Anzahl erfüllter Phasen	1

Gesamtergebnis

m1 = 1 (Anzahl erfüllter eingegeben Kriterien)
m2 = 3 (Anzahl erfüllter ausgegeben Kriterien)
m3 = 1 (Anzahl erfüllter Phasen des Intelligence-Zyklus)

$$Gesamtergebnis = (\sum_{n=1}^{m1} 1 + \sum_{n=1}^{m2} 1) * \sum_{n=1}^{m3} 1$$

Gesamtergebnis = 4

Auszug aus dem Ergebnis

E-Mail-Adressen:

- c*****n.b***k@hs-wismar.d
- f**k.s******r@hs-wismar.de

IP-Adressen:

- 212.xxx.128.xxx
- 212.xxx.36.xx
- 10.xx.23.xx
- 193.xxx.118.xx
- 192.xx.157.xxx

Hosts:

- it-forensik.fiw.hs-wismar.de
- webs2.rz.hs-wismar.de
- watt.wi.hs-wismar.de

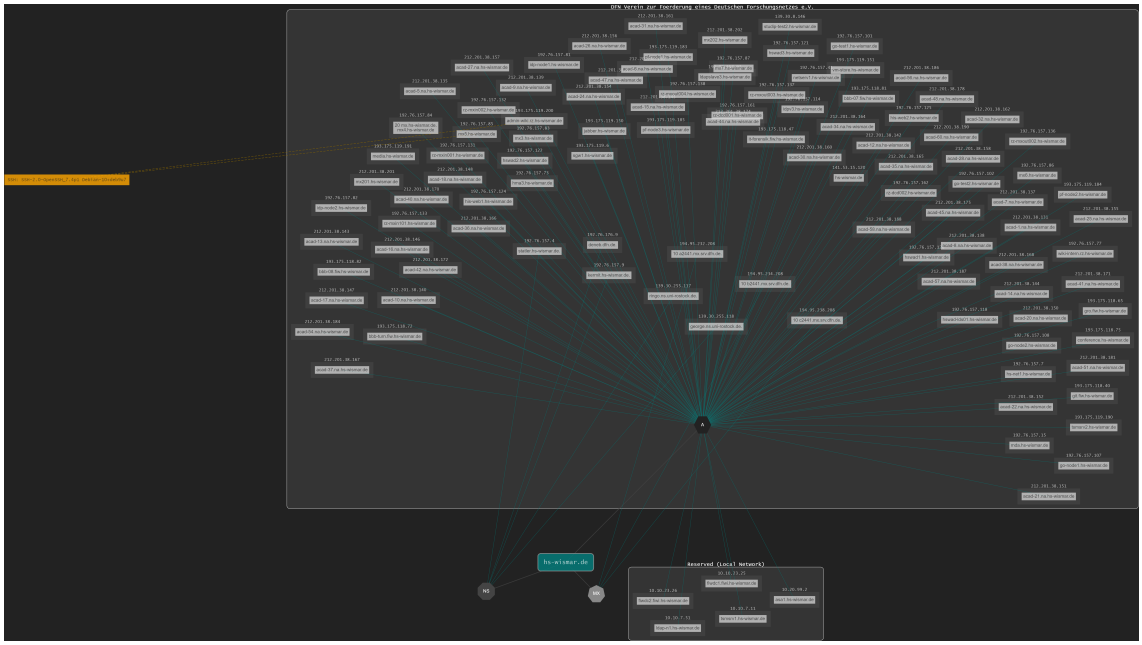
Die Liste aller Ergebnissen befindet sich auf dem beigelegtem Datenträger unter **Ergebnisse_Auswertung/Ausgabe_TheHarvester_full.txt**.

E Zusammenfassung der Beispiele aus dem Kapitel Strategie zur passiven Informationsbeschaffung

Aufklärung der Domains mit DNSDumpster

Hierzu wurde der Dienst `https://DNSDumpster.com/` verwendet. Die Eingabe des Merkmals **hs-wismar.de** hat ergeben, dass 110 Subdomains vorhanden sind. Zu den einzelnen Subdomains wurden die zugehörige IP-Adresse, der Netblock-Owner, das zugehörige Land sowie einzelne Informationen über laufende Systeme identifiziert (siehe Abbildung Ausgabe DNS Dumpster zu *hs-wismar.de*).

Bild 25: Ausgabe DNS Dumpster zu *hs-wismar.de*



Quelle: Export DNS Dumpster

Aufklärung von IP-Adressen mit ViewDNS

Nach der Eingabe der IP-Adresse **141.43.15.120** im Dienst ViewDNS ergab sich die Existenz von 17 Domains, die auf dem Server mit der IP gehostet waren (siehe

Abbildung Ausgabe ViewDNS zu *141.43.15.120*). Dazu wurde außerdem das Datum der letzten DNS-Auflösung ermittelt.

Bild 26: Ausgabe ViewDNS zu *141.43.15.120*

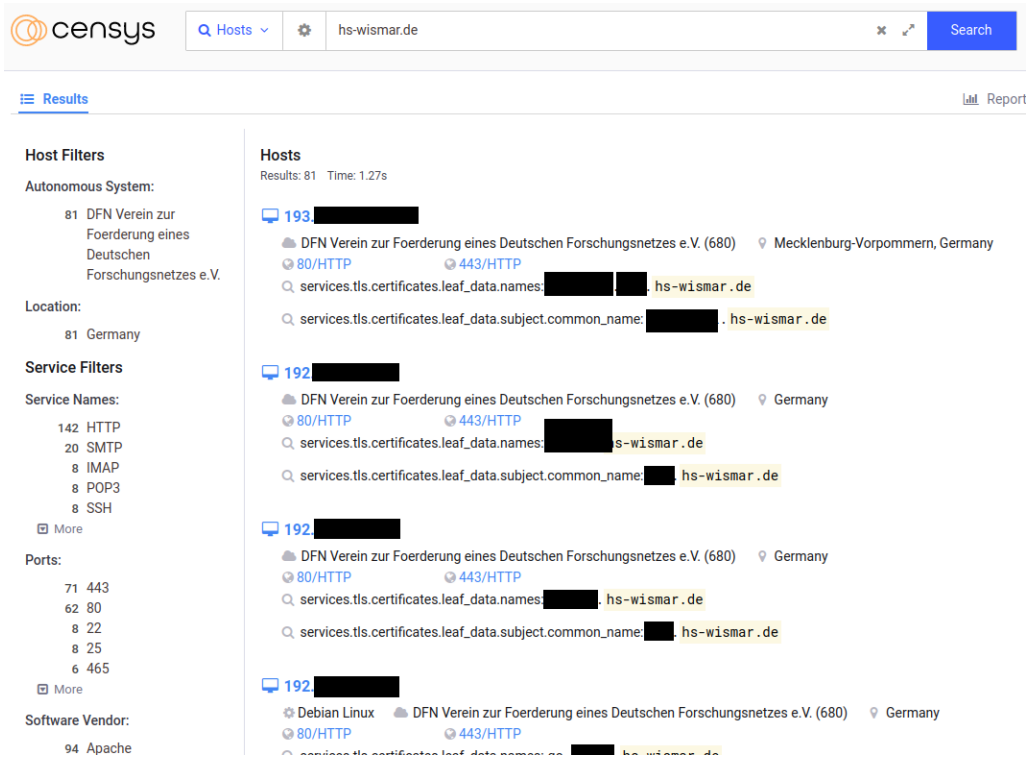
Domain	Last Resolved Date
fh-stralsund.de	2022-04-16
fh-wismar.de	2022-04-16
hmt-rostock.de	2022-04-16
hochschule-neubrandenburg.de	2022-04-16
hochschule-neubrandenburg.eu	2022-04-12
hochschule-stralsund.de	2022-04-16
hs-nb.de	2022-04-16
hs-neubrandenburg.de	2022-04-16
hs-neubrandenburg.eu	2022-04-12
hs-wismar.de	2022-04-18
ieeg-greifswald.de	2022-04-16
iib-ev.de	2022-04-16
mathe-mv.de	2022-04-16
spp-antarktisforschung.de	2018-10-04
uni-greifswald.de	2022-04-16
wiko-greifswald.de	2022-04-16
young-academy-rostock.de	2022-04-16

Quelle: eigener Screenshot ViewDNS

Aufklärung von Systeminformationen mit Censys

Die Eingabe des Merkmals **hs-wismar.de** in der Suchmaschine *Censys* lieferte Auskunft über 20 offene Ports, den Einsatz von Produkten wie den Webserver Apache, VMware, Ubuntu, etc. oder über 7 unterschiedliche laufende Dienste wie LDAP, SMTP, oder SSH (siehe Abbildung Auszug der Ausgabe in Censys zu *hs-wismar.de*).

Bild 27: Auszug der Ausgabe in Censys zu *hs-wismar.de*

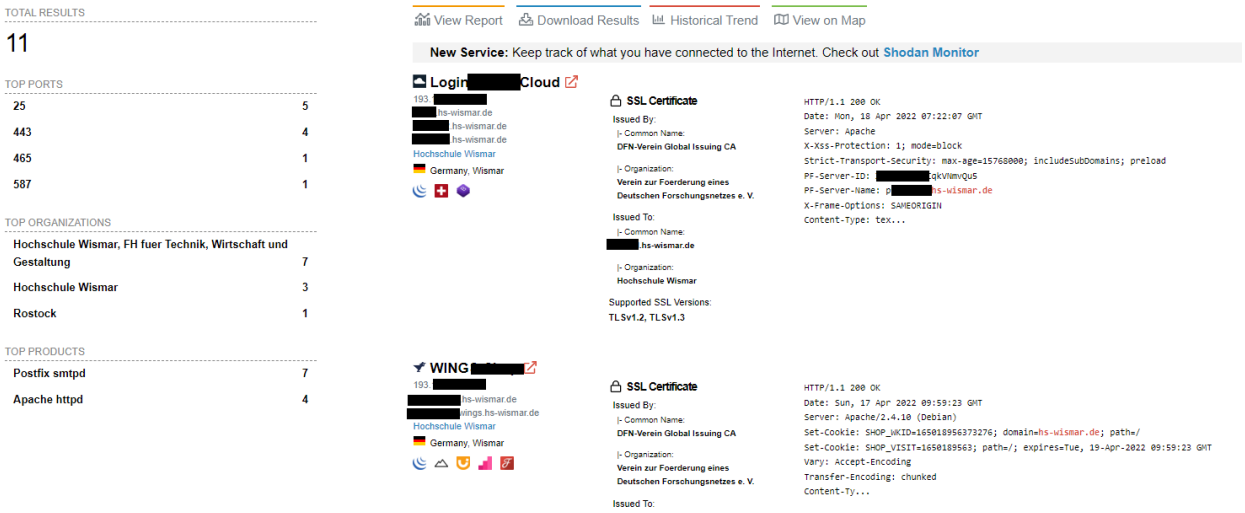


Quelle: eigener Screenshot Censys

Aufklärung von Systeminformationen mit Shodan

Die Eingabe des Merkmals **hs-wismar.de** in der Suchmaschine *Shodan* lieferte Auskunft über 4 offene Ports oder den Einsatz von Produkten wie Apache (siehe Abbildung Auszug der Ausgabe in Shodan zu *hs-wismar.de*).

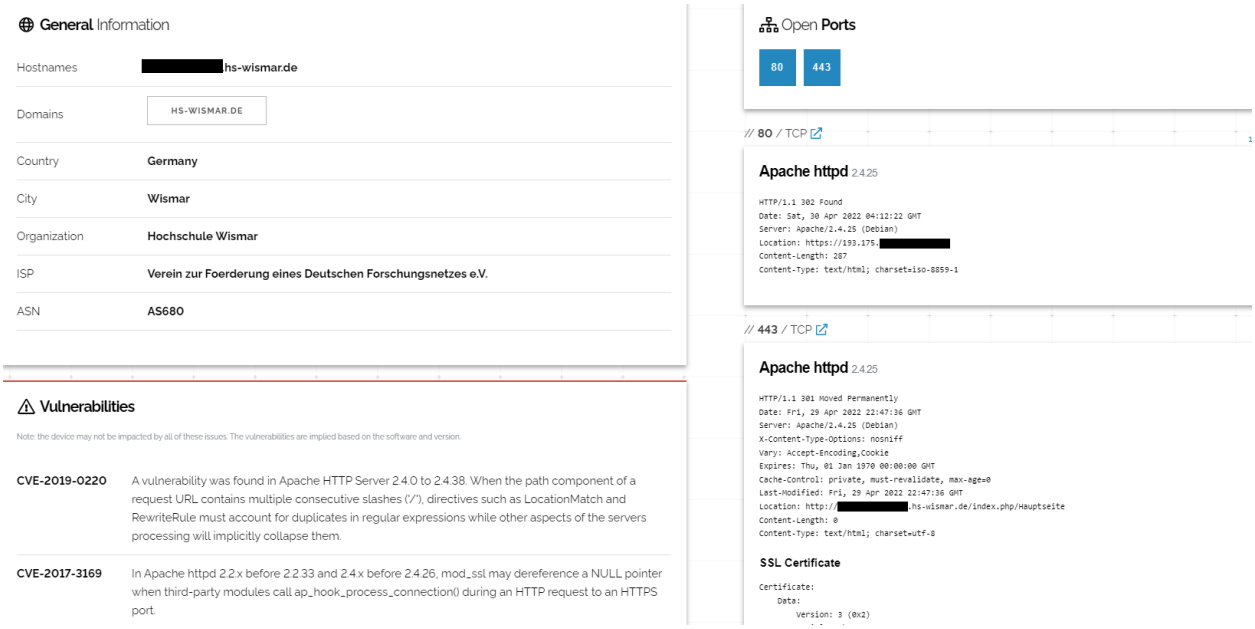
Bild 28: Auszug der Ausgabe in Shodan zu *hs-wismar.de*



Quelle: eigener Screenshot Shodan

Im Rahmen der Analyse wurden mehrere Server identifiziert, die laut Shodan über anfällige Apache-Versionen verfügten. Nach einem Informationsaustausch mit dem zuständigen Administrator an der Hochschule Wismar über die mutmaßlich anfälligen Server hat sich herausgestellt, dass es sich dabei um eine falsch-positive Erkennung der Suchmaschine handelte. Die gemeldeten Server waren auf dem aktuellsten Stand, jedoch meldete Shodan die veraltete Version des Servers aufgrund eines Backports eines Security-Patches für eine ältere Version des Betriebssystems. Die dankenswerterweise erfolgte Rückmeldung des Administrators ist der Beweis, dass der Einsatz von OSINT-Tools nicht zu 100% zuverlässig ist und Platz für falsch-positive Ergebnisse lässt. Die Ausgabe zu einem der mutmaßlich anfälligen Server ist in der nächsten Abbildung zu sehen.

Bild 29: Auszug der Ausgabe in Shodan zum mutmaßlich anfälligen Server



Quelle: eigener Screenshot Shodan

Aufklärung von abgeflossenen Zugangsdaten mit Intelligence X

Die Eingabe der Domäne **hs-wismar.de** in die kostenfreie Variante des Dienstes hat die Existenz zweier E-Mail-Adressen ergeben. Aus Sicherheitsgründen werden diese in der vorliegenden Arbeit unkenntlich gemacht.

- m*****d.a*n@hs-wismar.de:z****d
- h**s-e**er*t.r*****s@hs-wismar.de:p***x

Aufklärung von abgeflossenen Zugangsdaten mit Haveibeenpwned

Die Eingabe beider E-Mail-Adressen lieferte Auskunft über die mögliche Quelle des Datenleaks. Somit konnten die folgenden Datenlecks ermittelt werden:

- m*****d.a*n@hs-wismar.de: Anti Public Combo List, Collection #1, Onliner Spambot, Verifications.io, LinkedIn, MySpace, Trik Spam Botnet, You've Been Scraped Data Enrichment Exposure From PDL Customer
- h**s-e**er*t.r*****s@hs-wismar.de: Anti Public Combo List, Collection #1, MDPI, Onliner Spambot, Verifications.io;

Beispiel - XLSX als Standardformat für Dateien

Die Daten wurde aus DNS Dumpster als XLSX-Datei exportiert, sodass sie in Maltego zur Analyse importiert werden können. Zur Betrachtung und Entfernung von Duplikaten wurde die Software LibreOffice Calc verwendet (siehe Abbildung Processing: Auszug aus LibreOffice Calc).

Bild 30: Processing: Auszug aus LibreOffice Calc

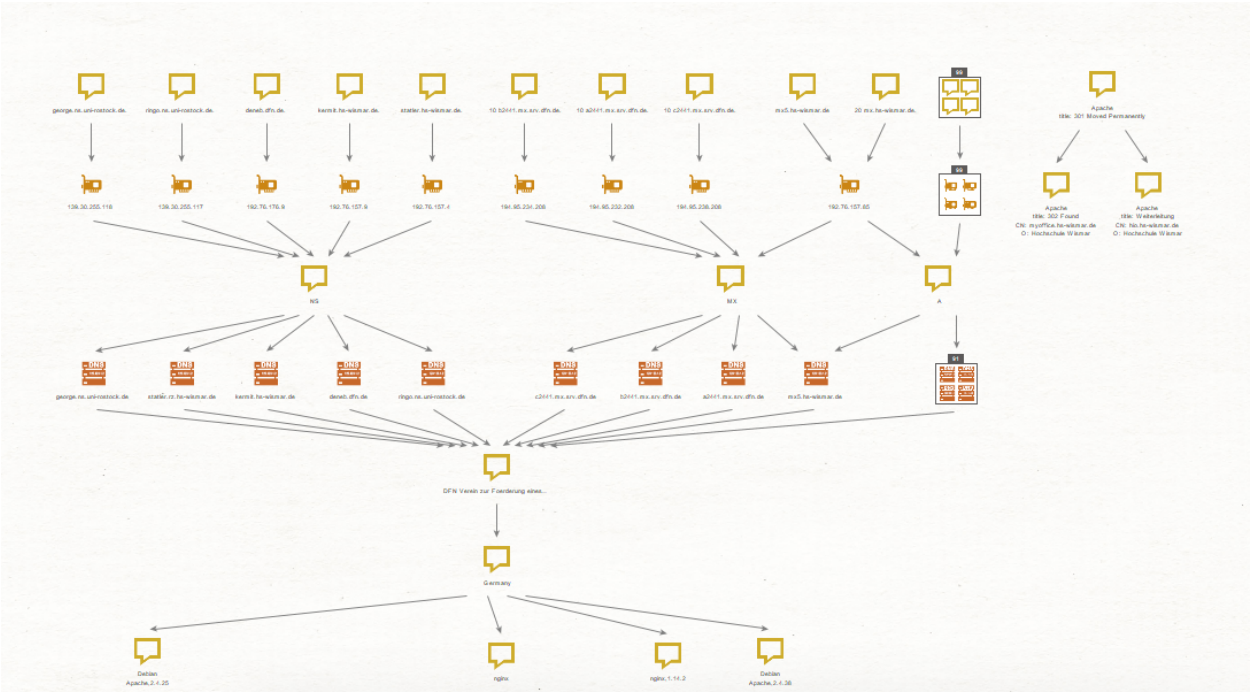
Hostname	IP Address	Type	Reverse DNS	Netblock Owner	Country
[redacted]mar.de	141.[redacted]	A	[redacted]-greifswald.de	DFN Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.	Germany
[redacted].hs-wismar.de	212.[redacted]	A	[redacted].hs-wismar.de	DFN Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.	Germany
[redacted].wismar.de	10.[redacted]	A		Reserved (Local Network)	unknown

Quelle: eigener Screenshot LibreOffice Calc

Analyse von Informationen mit Maltego

Als Beispiel wurde die Analysefunktion von Maltego verwendet. Es wurden zur Analyse die Ergebnisse des Tools DNS Dumpster aus dem Kapitel Beispiel - DNS Dumpster importiert. Die Daten wurden in Maltego hierarchisch dargestellt, sodass die Zusammenhänge zwischen den einzelnen Objekten sichtbar waren. Maltego ermöglichte die automatische Erstellung von Verlinkungen und Beziehungen zwischen den einzelnen Entitäten (z.B. eine Beziehung zwischen einer Domäne und der dazugehörigen IP-Adresse, siehe dazu die Abbildung Auszug der Link-Analyse in Maltego).

Bild 31: Auszug der Link-Analyse in Maltego



Quelle: eigener Screenshot Maltego

Beispiel - Meldung von vermutlichen Schwachstellen

Wie bereits im Kapitel Aufklärung von Systeminformationen erwähnt, wurden IT-Systeme der Hochschule als potenziell anfällig gemeldet. Die Übermittlung der Erkenntnisse an die Hochschule erfolgte via E-Mail. Ein Beispiel für die Übermittlung der Erkenntnisse ist in der nächsten Abbildung zu sehen.

Bild 32: Auszug aus der Übermittlung der Anfälligkeiten per E-Mail

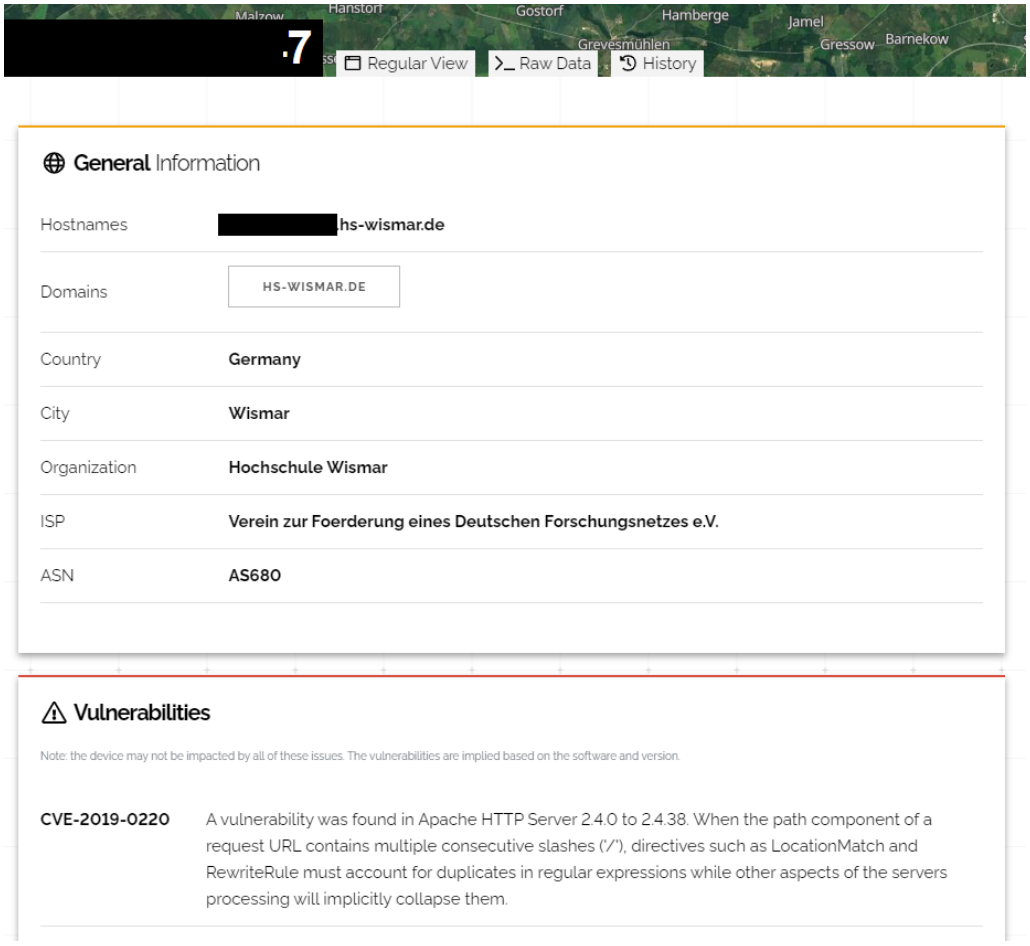
[redacted]:hs-wismar.de (Querry: https://www.shodan.io/host/193.[redacted])
==========
IP: 193.[redacted]
Server: **Apache 2.4.25**
Veröffentlichung: **12.2016**
Beispiele für Anfälligkeiten (zahlreiche):
CVE-2019-0220
CVE-2017-3169
CVE-2019-0197
CVE-2019-0196
CVE-2021-39275
Eine Liste der CVEs kann unter https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/Apache-Http-Server.html eingesehen werden.

Quelle: eigene Darstellung, Auszug aus der Übermittlung der Anfälligkeiten per E-Mail

Rückmeldung: Beispiel

Im Rahmen der vorliegenden Masterarbeit wurden mithilfe der Suchmaschine Shodan mehrere vermeintlich anfällige Server im Netzbereich der Hochschule Wismar entdeckt (siehe Kapitel Aufklärung von Systeminformationen). Die vermeintlichen Schwachstellen wurden der zuständigen Stelle gemeldet. Die Rückmeldung des zuständigen IT-Administrators hat ergeben, dass die betroffenen Server auf dem neuesten Patchstand waren und somit nicht anfällig waren. Das ist ein Beispiel für die Bedeutsamkeit dieser Phase. Ein Beispiel für eine vermeintliche Schwachstelle ist in der nächsten Abbildung zu sehen.

Bild 33: Vermeintliche Schwachstelle



Quelle: eigener Screenshot Shodan

Literaturverzeichnis

[1] Phil Muncaster. *OSINT – Was ist Open Source Intelligence und wie nutzt man sie?* 2021. URL: https://www.welivesecurity.com/deutsch/2021/06/16/osint-was-ist-open-source-intelligence-und-wie-nutzt-man-sie/ (besucht am 14. 03. 2022).

[2] Unit 42. *Incident Response & Data Breach Report 2020*. Palo Alto Networks, 2020. URL: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/2020-unit42-incident-response-and-data-breach-report (besucht am 14. 06. 2022).

[3] NATO. *NATO Open Source Intelligence Reader*. 2002.

[4] Hornetsecurity. *Cyber Kill Chain Schritt für Schritt die IT-Sicherheit im Unternehmen stärken*. o.J. URL: https://www.hornetsecurity.com/de/wissensdatenbank/cyber-kill-chain/?_adin=0896487498 (besucht am 12. 06. 2022).

[5] Lockheed Martin. „Gaining the advantage: Applying Cyber Kill Chain Methodolgy to Network Defense“. In: *Lockheed Martin* (2015), S. 2–13. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf (besucht am 22. 03. 2022).

[6] Mark Phythian, Hrsg. *Understanding the Intelligence Cycle*. 1. Auflage. Studies in Intelligence. Taylor & Francis, 2013. ISBN: 978-0-203-55847-8.

[7] Sherman Kent. *Strategic Intelligence for American World Policy*. Princeton University Press, 2015. ISBN: 9781400879151. Originales Veröffentlichungsjahr 1966.

[8] Recorded Future. *What Is Threat Intelligence?* o.J. URL: https://www.recordedfuture.com/threat-intelligence (besucht am 08. 06. 2022).

[9] BND. *Informationsgewinnung*. o.J. URL: https://www.bnd.bund.de/DE/Die_Arbeit/Informationsgewinnung/informationsgewinnung_node.html (besucht am 17. 03. 2022).

[10] Joint Chiefs of Staff. *Joint Intelligence*. Joint Chiefs of Staff, 2013. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf (besucht am 15. 03. 2022).

[11] Scott J. Roberts und Rebekah Brown. *Intelligence-Driven Incident Response: Outwitting the Adversary*. 1. Auflage. O'REILLY, 2017. ISBN: 978-1-491-93494-4.

[12] CIA. „Words of Estimative Probability“. In: (1993). URL: https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf (besucht am 27. 03. 2022).

[13] NATO. *NATO Open Source Intelligence Handbook*. 2001. URL: https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook (besucht am 14. 06. 2022).

[14] Recorded Future. *Das Handbuch zu Security Intelligence*. 3. Auflage. CyberEdge Group LLC, 2020. ISBN: 978-1-948939-15-7.

[15] Babak Akhgar, P.Saskia Bayerl und Fraser Sampson. *Open Source Intelligence Investigation: From Strategy to Implementation*. Advanced Sciences and Technologies for Security Applications. Springer, 2016. ISBN: ISBN 978-3-319-47670-4.

[16] W. Richard Stevens, Bill Fenner und Andrew M. Rudoff. *UNIX Network Programming: The sockets networking API*. Addison-Wesley professional computing series V. 1. Addison-Wesley, 2004. ISBN: 9780131411555.

[17] Claudia Eckert. *IT-Sicherheit Konzepte-Verfahren-Protokolle*. 10. Auflage. De Gruyter Oldenburg, 2012. ISBN: 978-3-11-055158-7.

[18] Thomas Jäger, Alexander Höse und Kai Oppermann. *Deutsche Außenpolitik*. VS Verlag für Sozialwissenschaften | Springer Fachmedien Wiesbaden GmbH 2011, 2011. ISBN: 978-3-531-93024-4.

[19] Deutsche Hochschule der Polizei. *SENTINEL Sicherheit im Einsatz durch Open-Source-Intelligence (OSINT) in Einsatzleitstellen*. o.J. URL: https://www.dhpol.de/departements/departement_II/FG_II.1/projekt-sentinel.php (besucht am 17. 03. 2022).

[20] Max Knieriemen. *Open Source Intelligence – Der „Geheimdienst der Öffentlichkeit“*. 11.03.2022. URL: https://www.swr.de/swr2/leben-und-gesellschaft/open-source-intelligence-der-geheimdienst-der-oeffentlichkeit-100.html (besucht am 15. 03. 2022).

[21] Bellingcat. *Bellingcat auf Deutsch*. o.J. URL: https://de.bellingcat.com/ (besucht am 15. 03. 2022).

[22] Rolf Opplinger. *IT-Sicherheit: Grundlagen und Umsetzung in der Praxis*. 1. Auflage. vieweg, 1997. ISBN: 978-3-528-05566-0.

[23] Wilson Jr. Bautista. *Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents*. Packt Publishing Ltd., 2018. ISBN: 978-1-78862-556-2.

[24] Rapid7. *Spear-Phishing-Angriffe: Verhindern und Erkennen von Spear-Phishing-Angriffen*. o.J. URL: https://www.rapid7.com/de/cybersecurity-grundlagen/spear-phishing-attacks/ (besucht am 18. 04. 2022).

[25] Siddhesh Parab. *Subdomain Enumeration Guide*. o.J. URL: https://sidxparab.gitbook.io/subdomain-enumeration-guide/active-enumeration/dns-bruteforcing (besucht am 18. 04. 2022).

[26] Esteban Borges. *Exploring Google Hacking Techniques*. o.J. URL: https://securitytrails.com/blog/google-hacking-techniques (besucht am 18. 04. 2022).

[27] Torsten Gründer und Joachim Schrey. *Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht*. 1. Auflage. Erich Schmidt Verlag, 2007. ISBN: 9783503100026.

[28] Jürgen Schoolmann und Achim von Berg. *Praxishandbuch IT-Sicherheit: Risiken, Prozesse, Standards*. 1. Auflage. Symposion Publishing GmbH, 2005. ISBN: 3-936608-94-6.

[29] Adam Nurudini. „OSINT - Open - Source Intelligence“. In: (o.J.). URL: https://owasp.org/www-chapter-ghana/assets/slides/OWASP_OSINT_Presentation.pdf (besucht am 27. 03. 2022).

[30] T Systems International GmbH. „Penetration Testing“. In: (o.J.). URL: https://www.telekom.com/resource/blob/578666/fe9a8b5df5e14dd67ce212ebbf4f2702/dl-190809-pentesting-flyer-data.pdf (besucht am 15. 03. 2022).

[31] VirusTotal. *Privacy Policy*. o.J. URL: https://support.virustotal.com/hc/en-us/articles/115002168385-Privacy-Policy (besucht am 18. 03. 2022).

[32] Checkpoint. *Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of*. 2022. URL: https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/ (besucht am 28. 03. 2022).

[33] Stiv Kupchik. *Conti's Hacker Manuals — Read, Reviewed & Analyzed*. 2022. URL: https://www.akamai.com/blog/security/conti (besucht am 06. 04. 2022).

[34] Azeria Labs. *RECONNAISSANCE*. o.J. URL: https://azeria-labs.com/reconnaissance/ (besucht am 28. 03. 2022).

[35] Bundesamt für Sicherheit in der Informationstechnik. *Darknet und Deep Web – wir bringen Licht ins Dunkle*. o.J. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deep-web_node.html (besucht am 22. 03. 2022).

[36] Sabine Vogt. „Das Darknet - Rauschgift, Waffen, Falschgeld, Ausweise - das digitale „Kaufhaus” der Kriminellen?“ In: *Die Kriminalpolizei* (2017), S. 4. URL: https://www.bka.de/SharedDocs/Reden/DE/vogtArtikelDarknet.pdf?__blob=publicationFile (besucht am 21. 03. 2022).

[37] Lockheed Martin. *The Cyber Kill Chain*. o.J. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (besucht am 22. 03. 2022).

[38] Symantec. *Advanced Persistent Threats: A Symantec Perspective*. 2017.

[39] Nihad A. Hassan und Rami Hijazi. *Open Source Intelligence Methods and Tools*. 1. Auflage. APRESS, 2018. ISBN: 978-1-4842-3213-2.

[40] Rapid7. *Was ist das MITRE ATT&CK Framework?* o.J. URL: https://www.rapid7.com/de/cybersecurity-grundlagen/mitre-attack/ (besucht am 28. 03. 2022).

[41] MITRE. *MITRE ATT&CK Framework*. o.J. URL: https://mitre-attack.github.io/attack-navigator/ (besucht am 30. 03. 2022).

[42] MITRE. *MITRE ATT&CK Framework*. o.J. URL: https://attack.mitre.org/versions/v10/tactics/TA0043/ (besucht am 30. 03. 2022).

[43] WILDE BEUGER SOLMECKE RECHTSANWÄLTE. *Penetrationstests*. o.J. URL: https://www.wbs-law.de/it-und-internet-recht/computerkriminalitaet/penetrationstests/ (besucht am 28. 03. 2022).

[44] U.S. Intelligence Community. *HOW INTELLIGENCE WORKS*. o.J. URL: https://www.intelligencecareers.gov/icintelligence.html (besucht am 18. 03. 2022).

[45] Robert Rigby Glass und Philip Buford Davidson. *Intelligence is for Commanders*. The military service publishing company, 1948. URL: https://bit.ly/3JsdK0X (besucht am 08. 06. 2022).

[46] Richards J. Jr. Heuer. *Psychology of Intelligence Analysis*. Center for the study of intelligence, Central Intelligence Agency, 1999. ISBN: 1 929667-00-0.

[47] Stewart K. Bertram. *F3EAD: Find, Fix, Finish, Exploit, Analyze And Disseminate – The Alternative Intelligence Cycle*. 2017. URL: https://www.digitalshadows.com/blog-and-research/f3ead-find-fix-finish-exploit-analyze-and-disseminate-the-alternative-intelligence-cycle/ (besucht am 28. 03. 2022).

[48] Department of the Army. „The Targeting Process“. In: (2010).

[49] MITRE. *Active Scanning*. o.J. URL: https://attack.mitre.org/techniques/T1595/ (besucht am 31. 03. 2022).

[50] MITRE. *Active Scanning: Scanning IP Blocks*. o.J. URL: https://attack.mitre.org/techniques/T1595/001/ (besucht am 31. 03. 2022).

[51] MITRE. *Active Scanning: Vulnerability Scanning*. o.J. URL: https://attack.mitre.org/techniques/T1595/002/ (besucht am 31. 03. 2022).

[52] MITRE. *Gather Victim Host Information*. o.J. URL: https://attack.mitre.org/techniques/T1592/ (besucht am 31. 03. 2022).

[53] MITRE. *Gather Victim Host Information: Hardware*. o.J. URL: https://attack.mitre.org/techniques/T1592/001/ (besucht am 31. 03. 2022).

[54] MITRE. *Gather Victim Host Information: Software*. o.J. URL: https://attack.mitre.org/techniques/T1592/002/ (besucht am 31. 03. 2022).

[55] MITRE. *Gather Victim Host Information: Firmware*. o.J. URL: https://attack.mitre.org/techniques/T1592/003/ (besucht am 31. 03. 2022).

[56] MITRE. *Gather Victim Host Information: Client Configurations*. o.J. URL: https://attack.mitre.org/techniques/T1592/004/ (besucht am 31. 03. 2022).

[57] MITRE. *Gather Victim Identity Information*. o.J. URL: https://attack.mitre.org/techniques/T1589/ (besucht am 31. 03. 2022).

[58] MITRE. *Gather Victim Identity Information: Credentials*. o.J. URL: https://attack.mitre.org/techniques/T1589/001/ (besucht am 31. 03. 2022).

[59] MITRE. *Gather Victim Identity Information: Email Addresses*. o.J. URL: https://attack.mitre.org/techniques/T1589/002/ (besucht am 31. 03. 2022).

[60] MITRE. *Gather Victim Identity Information: Employee Names*. o.J. URL: https://attack.mitre.org/techniques/T1589/003/ (besucht am 31. 03. 2022).

[61] MITRE. *Gather Victim Network Information*. o.J. URL: https://attack.mitre.org/techniques/T1590/ (besucht am 31. 03. 2022).

[62] MITRE. *Gather Victim Network Information: Domain Properties*. o.J. URL: https://attack.mitre.org/techniques/T1590/001/ (besucht am 31. 03. 2022).

[63] MITRE. *Gather Victim Network Information: DNS*. o.J. URL: https://attack.mitre.org/techniques/T1590/002/ (besucht am 31. 03. 2022).

[64] MITRE. *Gather Victim Network Information: Network Trust Dependencies*. o.J. URL: https://attack.mitre.org/techniques/T1590/003/ (besucht am 31. 03. 2022).

[65] MITRE. *Gather Victim Network Information: Network Topology*. o.J. URL: https://attack.mitre.org/techniques/T1590/004/ (besucht am 31. 03. 2022).

[66] MITRE. *Gather Victim Network Information: IP Addresses*. o.J. URL: https://attack.mitre.org/techniques/T1590/005/ (besucht am 31. 03. 2022).

[67] MITRE. *Gather Victim Network Information: Network Security Appliances*. o.J. URL: https://attack.mitre.org/techniques/T1590/006/ (besucht am 31. 03. 2022).

[68] MITRE. *Gather Victim Org Information*. o.J. URL: https://attack.mitre.org/techniques/T1591/ (besucht am 31. 03. 2022).

[69] MITRE. *Gather Victim Org Information: Business Relationships*. o.J. URL: https://attack.mitre.org/techniques/T1591/002/ (besucht am 31. 03. 2022).

[70] MITRE. *Gather Victim Org Information: Identify Business Tempo*. o.J. URL: https://attack.mitre.org/techniques/T1591/003/ (besucht am 31. 03. 2022).

[71] MITRE. *Gather Victim Org Information: Identify Roles*. o.J. URL: https://attack.mitre.org/techniques/T1591/004/ (besucht am 31. 03. 2022).

[72] MITRE. *Phishing for Information*. o.J. URL: https://attack.mitre.org/techniques/T1598/ (besucht am 31. 03. 2022).

[73] MITRE. *Phishing for Information: Spearphishing Service*. o.J. URL: https://attack.mitre.org/techniques/T1598/001/ (besucht am 31. 03. 2022).

[74] MITRE. *Phishing for Information: Spearphishing Attachment*. o.J. URL: https://attack.mitre.org/techniques/T1598/002/ (besucht am 31. 03. 2022).

[75] MITRE. *Phishing for Information: Spearphishing Link*. o.J. URL: https://attack.mitre.org/techniques/T1598/003/ (besucht am 31. 03. 2022).

[76] MITRE. *Search Closed Sources*. o.J. URL: https://attack.mitre.org/techniques/T1597/ (besucht am 31. 03. 2022).

[77] MITRE. *Search Closed Sources: Threat Intel Vendors*. o.J. URL: https://attack.mitre.org/techniques/T1597/001/ (besucht am 31. 03. 2022).

[78] MITRE. *Search Closed Sources: Purchase Technical Data*. o.J. URL: https://attack.mitre.org/techniques/T1597/002/ (besucht am 31. 03. 2022).

[79] MITRE. *Search Open Technical Databases*. o.J. URL: https://attack.mitre.org/techniques/T1596/ (besucht am 31. 03. 2022).

[80] MITRE. *Search Open Technical Databases: DNS/Passive DNS*. o.J. URL: https://attack.mitre.org/techniques/T1596/001/ (besucht am 31. 03. 2022).

[81] MITRE. *Search Open Technical Databases: WHOIS*. o.J. URL: https://attack.mitre.org/techniques/T1596/002/ (besucht am 31. 03. 2022).

[82] MITRE. *Search Open Technical Databases: Digital Certificates*. o.J. URL: https://attack.mitre.org/techniques/T1596/003/ (besucht am 31. 03. 2022).

[83] MITRE. *Search Open Technical Databases: CDNs*. o.J. URL: https://attack.mitre.org/techniques/T1596/004/ (besucht am 31. 03. 2022).

[84] MITRE. *Search Open Technical Databases: Scan Databases*. o.J. URL: https://attack.mitre.org/techniques/T1596/005/ (besucht am 31. 03. 2022).

[85] MITRE. *Search Open Websites/Domains*. o.J. URL: https://attack.mitre.org/techniques/T1593/ (besucht am 31. 03. 2022).

[86] MITRE. *Search Open Websites/Domains: Social Media*. o.J. URL: https://attack.mitre.org/techniques/T1593/001/ (besucht am 31. 03. 2022).

[87] MITRE. *Search Open Websites/Domains: Search Engines*. o.J. URL: https://attack.mitre.org/techniques/T1593/002/ (besucht am 31. 03. 2022).

[88] MITRE. *Search Victim-Owned Websites*. o.J. URL: https://attack.mitre.org/techniques/T1594/ (besucht am 31. 03. 2022).

[89] SpiderFoot. *SpiderFoot*. o.J. URL: https://www.spiderfoot.net/documentation/ (besucht am 31. 03. 2022).

[90] Maltego. *What is Maltego?* 2020. URL: https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego- (besucht am 02. 04. 2022).

[91] Duff Jones. *Open Source Intelligence (OSINT) with Maltego*. 2021. URL: https://whisperlab.org/introduction-to-hacking/notes/maltego (besucht am 02. 04. 2022).

[92] Maltego. *Which Maltego edition is right for me?* 2022. URL: https://docs.maltego.com/support/solutions/articles/15000030836-which-maltego-edition-is-right-for-me- (besucht am 13. 06. 2022).

[93] Maltego. *Introduction to Maltego Standard Transforms*. 2021. URL: https://docs.maltego.com/support/solutions/articles/15000041468-introduction-to-maltego-standard-transforms#overview-0-0 (besucht am 02. 04. 2022).

[94] Maltego Technologies. *Shodan*. 2020. URL: https://www.maltego.com/transform-hub/shodan/ (besucht am 02. 04. 2022).

[95] Maltego. *What gets logged when I run a Transform?* 2021. URL: https://docs.maltego.com/support/solutions/articles/15000011924-what-gets-logged-when-i-run-a-transform- (besucht am 02. 04. 2022).

[96] Maltego. *Maltego Homepage*. o.J. URL: https://www.maltego.com/ (besucht am 02. 04. 2022).

[97] lanmaster53. *The Recon-ng Framework*. 2020. URL: https://github.com/lanmaster53/recon-ng (besucht am 07. 04. 2022).

[98] Jon DiMaggio. *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*. No Starch Press, Inc., 2022. ISBN: 978-1-17185-0215-4.

[99] lanmaster53. *The Recon-ng Framework*. URL: https://github.com/lanmaster53/recon-ng-marketplace/tree/master/modules (besucht am 07. 04. 2022).

[100] Tim Tomes. *brute_hosts*. URL: https://github.com/lanmaster53/recon-ng-marketplace/blob/master/modules/recon/domains-hosts/brute_hosts.py (besucht am 09. 04. 2022).

[101] Marcus Watson. *brute_suffix*. URL: https://github.com/lanmaster53/recon-ng-marketplace/blob/master/modules/recon/domains-domains/brute_suffix.py (besucht am 09. 04. 2022).

[102] SamShanks1. *automated-recon-ng*. URL: https://github.com/SamShanks1/automated-recon-ng (besucht am 09. 04. 2022).

[103] Edge-Security. *theHarvester*. URL: http://www.edge-security.com/software.html (besucht am 09. 04. 2022).

[104] laramies. *theHarvester*. URL: https://github.com/laramies/theHarvester (besucht am 09. 04. 2022).

[105] Robert M. Lee, Ben Miller und Mark Stacey. „Collection Management Frameworks – Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats". In: (o.J.). URL: https://www.dragos.com/wp-content/uploads/CMF_For_ICS.pdf (besucht am 17. 04. 2022).

[106] Intelligence X. *Intelligence X*. o.J. URL: https://intelx.io/about (besucht am 13. 06. 2022).

[107] Pete Herzog. *OSSTMM3: The Open Source Security Testing Methodology Manual*. 3.0. ISECOM, 2010. URL: https://www.isecom.org/OSSTMM.3.pdf (besucht am 12. 06. 2022).

[108] Department of the Army. „Open-Source Intelligence“. In: (2012). URL: https://irp.fas.org/doddir/army/atp2-22-9.pdf (besucht am 13. 06. 2022).

[109] Bundesamt für Sicherheit in der Informationstechnik. *Ein Praxis-Leitfaden für IS-Penetrationstests*. 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html (besucht am 08. 06. 2022).

[110] Bundesamt für Sicherheit in der Informationstechnik. *Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), TLP-Version 17-11*. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/TLP/merkblatt-tlp.html (besucht am 08. 06. 2022).

[111] Tony Lambert und Greg Foss. *Defense evasion: why is it so prominent & how can you detect it?* 2019. URL: https://redcanary.com/blog/defense-evasion-why-is-it-so-prominent-how-can-you-detect-it/ (besucht am 29. 05. 2022).

[112] BSI. *Drive-by-Exploits / Drive-by-Download*. o.J. URL: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/D/Drive-by-Download.html (besucht am 29. 05. 2022).

[113] CROWDSTRIKE. *Lateral Movement*. 2022. URL: https://www.crowdstrike.de/cybersecurity-101/lateral-movement/ (besucht am 29. 05. 2022).

[114] RiskNET. *Privilege Escalation*. o.J. URL: https://www.risknet.de/wissen/glossar-eintrag/privilege-escalation/ (besucht am 29. 05. 2022).

[115] Imperva. *Web Shell*. o.J. URL: https://www.imperva.com/learn/application-security/web-shell/ (besucht am 29. 05. 2022).

Bildverzeichnis

Tabellenverzeichnis

Listingverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface. 14, 43, 44, 46, 50–54, 58
APT	Advanced Persitent Threat. 8, 19
ASN	autonomous system number. 44, 55
CDN	Content Delivery Network. 38
CSV	comma-separated-values. 28
CTO	Chief Technology Officer. 12
CVSSv2	Common Vulnerability Scoring System v.2. 74
DNS	Domain Name System. 37, 38, 49, 51, 54
JSON	JavaScript Object Notation. 14, 28
PDF	Portable Document Format. 28
pDNS	Passive Domain Name System. 38
RDP	Remote Desktop Protocol. 8
RSS	Really Simple Syndication. 14
USB	Universal Serial Bus. 22
XML	eXtensible Markup Language. 14, 28

Symbolverzeichnis

Σ Summenzeichen Sigma. 43

Glossar

Defense Evasion	Technik eines Angreifers zur Vermeidung einer Erkennung im Rahmen eines Angriffs [111]. 23
Drive-by-Download	„Drive-by-Exploits oder Drive-by-Downloads bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser, in Zusatzprogrammen des Browsers (Plugins) oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.“[112]. 22
Lateral movement	Technik eines Angreifers nach dem Eindringen in einem Netzwerk sich zu bewegen [113]. 23
Privilege Escalation	Rechteausweitung nach einem erfolgreichen Angriff [114]. 23
Web Shell	Schädliches Skript auf einem System [115]. 22

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.
Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Fassung entspricht der auf dem Medium gespeicherten Fassung.

Ort, Datum Unterschrift

Thesen

Master-Thesis
Strategie und Anwendung von Open Source Intelligence zur vorbeugenden Aufklärung von Angriffsflächen im Bereich der IT-Sicherheit

von: A.I.S.

- Open Source Intelligence wird erst nach Verarbeitung von Daten und Analyse der daraus gewonnen Informationen erzeugt.
- OSINT wird sowohl von staatlichen Stellen (z.B. von Nachrichtendiensten), als auch im privaten Bereich verwendet.
- Im Bereich der IT-Sicherheit kann auf OSINT zugegriffen werden, um Informationen über einen IT-Sicherheitsvorfall oder im Rahmen eines Penetrationstests zu sammeln.
- Das Internet ist eine grundlegende Quelle für die Durchführung von OSINT-Recherchen.
- Open Source Intelligence ist Bestandteil der Aufklärungsphase in der Cyber Kill Chain.
- Es gibt grundsätzlich mehrere Strategien zur Gewinnung von Informationen. Jedoch ist der Intelligence Cycle das passende Modell zum Aufbau einer Strategie für die Gewinnung von Erkenntnissen über mögliche Angriffsflächen.
- Softwares und Tools können anhand von festgelegten Kriterien analysiert, miteinander verglichen und mindestens einer Phase des Intelligence Cycles zugewiesen werden.
- Es gibt eine Schnittmenge von Diensten, worauf OSINT-Softwares und -Tools zugreifen.
- Die passive Informationsbeschaffung kann systematisch anhand einer festgelegten Strategie erfolgen. Die Strategie durchläuft die sechs Phasen des Intelligence Cycles.