HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

Bachelorarbeit

Herr
Alexander Gritzka

Konzeption einer Windows-Laborumgebung zur Untersuchung computerforensischer Artefakte

Mittweida, 2021

Fakultät Angewandte Computer- und Biowissen-
schaften

Bachelorarbeit

Konzeption einer Windows-Laborumgebung zur Untersuchung computerforensischer Artefakte

Autor:
Herr

Alexander Gritzka

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO17w4-B

Erstprüfer:
Prof. Dipl.-Ing. (BA) Ronny Bodach

Zweitprüfer:
BA Sc. Tobias Kasch

Einreichung:
Mittweida, 22.02.2021

Verteidigung/Bewertung:
Mittweida, 2021

Faculty Angewandte Computer- und Biowissen-
schaften

Bachelorthesis

Conception of a Windows laboratory environment for examining computer forensic artifacts

author:
Mr.

Alexander Gritzka

course of studies:
Allgemeine und Digitale Forensik

seminar group:
FO17w4-B

first examiner:
Prof. Dipl.-Ing. (BA) Ronny Bodach

second examiner:
BA Sc. Tobias Kasch

submission:
Mittweida, 22.02.2021

defence/ evaluation:
Mittweida, 2021

Bibliografische Beschreibung:

Gritzka, Alexander:

Konzeption einer Windows-Laborumgebung zur Untersuchung computerforensischer Artefakte. - 2021. - VI, 50, 0 S.

Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2021

Referat:

In dieser Bachelorarbeit wird die theoretische Planung einer digitalen Windows-Laborumgebung beschrieben, welche zur Untersuchung von Schadsoftware genutzt werden soll. Mithilfe von virtuellen Maschinen wird ein Modell eines Firmennetzwerkes konzipiert. Es wird sich unter anderem mit den Themen Virtualisierung, Microsoft Active Directory, Microsoft Exchange Server und Malwareanalyse befasst.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AD	Active Directory
AD DS	Active Directory-Domänendienste
DNS	Domain Name Service
EAC	Exchange Admin Center
IoC(s)	Indicator(s) of Compromise
PE-Datei	Portable Executable Datei
ProcMon	Process Monitor
T-Systems MMS	T-Systems Multimedia Solutions GmbH
VM(s)	virtuelle Maschine(n)

1 Einleitung

1.1 Motivation

Jeden Tag werden mehr als 300.000 unbekannte Varianten von Schadsoftware geschaffen, die als Waffen gegen die Daten von Unternehmen und Privatleuten genutzt werden [1]. Der ständige Zuwachs und Wandel, sowie die Entwicklung neuer Technologien der Cyberkriminalität ist eine Herausforderung für die IT-Sicherheit. Doch wie die Bedrohung der Cyberkriminalität wächst, so wächst auch der Wissensstand und Fortschritt derer, die diese Angriffe verhindern und untersuchen. So besteht ein ewiges Katz-und-Maus-Spiel zwischen Schadsoftwareattacken und der IT-Sicherheit. Auch in der Abteilung für IT-Forensik der T-Systems Multimedia Solutions GmbH (T-Systems MMS) treffen die IT-Forensiker immer wieder auf Schadsoftware, auch Malware genannt, die nach eigener Aussage möglicherweise nur wenige Tage oder Stunden alt ist. Die Untersuchung dieser unbekannten Malware ist extrem gefährlich, da immer das Risiko besteht, das eigene System zu infizieren oder zu beschädigen.

Um die computerforensische Untersuchung von Malware sicherer zu gestalten und mehr Möglichkeiten zur Untersuchung zu bieten, soll für die IT-Forensiker der T-Systems MMS eine virtuelle Windows Laborumgebung entwickelt werden. Diese Laborumgebung wird ein Modell eines Firmennetzwerkes darstellen. In dem Labor soll Malware abgeschottet in einer geschlossenen Umgebung untersucht werden können, was die Sicherheit des zuständigen IT-Forensikers und der Firma erhöht und die Möglichkeiten zur Untersuchung verbessert. Durch das Ausführen von Malware in der abgeschlossenen, überwachten Umgebung kann das Verhalten der Malware näher und sicherer studiert und analysiert werden.

1.2 Zielsetzung

Die Installation der gesamten Windows-Laborumgebung ist ein komplexes Projekt, welches unmöglich in einer einzigen wissenschaftlichen Bachelorarbeit allumfassend behandelt werden kann. Deshalb wird sich in dieser Arbeit ausschließlich auf den Theorie- und Planungsteil des Projekts konzentriert. Ziel ist es, ein Grundgerüst für die spätere Weiterentwicklung zum forensischen Labor auszuarbeiten. Dies umfasst die Planung zum Aufbau der Laborumgebung, welche Hard- und Software für die wichtigsten Komponenten benutzt und wie diese konfiguriert werden soll.

In Bezug auf das Gesamtprojekt wird eine Testumgebung in Form eines virtualisierten Netzwerkes entwickelt, welche unter hohen Sicherheitsvorkehrungen zur Analyse von Malware genutzt werden soll. Dieses virtuelle Netzwerk wird aus einem Server bestehen, der mithilfe eines Active Directory (siehe 2.2) mindestens zwei Nutzer verwalten soll, welche die Angestellten im Firmennetzwerk darstellen. Außerdem soll das Netzwerk über ein Microsoft Exchange Service (siehe 2.3) verfügen, mit dem die Nutzer über E-Mail-Verkehr miteinander vernetzt sind und kommunizieren können. Die virtuellen Server und Nutzer werden mithilfe von virtuellen Maschinen dargestellt (siehe 2.1). Die Mitglieder des virtuellen Netzwerkes werden mit Werkzeugen zur forensischen Untersuchung und Überwachung des Dateisystems und des Netzwerkverkehrs ausgestattet, um computerforensische Artefakte zu analysieren.

Ein Ziel bei dem Projekt der Laborumgebung ist die Einsparung von Hardware Ressourcen. Da das Labor mithilfe von Virtualisierung auf einem einzigen Computer installiert wird, werden so wenige Geräte wie möglich genutzt. Dies spart Anschaffungskosten und den Aufwand, der die Wartung der Geräte mit sich bringt. Des Weiteren ist es ein Ziel, die Administration des Servers sehr gering zu halten, da er nicht, wie bei herkömmlichen Firmennetzwerken, im Dauerbetrieb läuft und keine hohe Ausfallsicherheit gewährleisten muss.

Eine weitere Kernfunktion des Labors soll die Zurücksetzbarkeit auf einen unversehrten Grundzustand der Umgebung sein. Malware kann möglichweise die virtuellen Netzwerkteilnehmer unbrauchbar machen, indem sie beispielsweise die Daten eines Nutzers verschlüsselt. Solche Szenarien können mithilfe dieser Funktionen beabsichtigt provoziert werden, ohne große Schäden in Kauf nehmen zu müssen (siehe 2.1).

Außerdem soll die Laborumgebung über einen steuerbaren Internetzugang verfügen. Einige Arten von Malware benötigen Internetzugriff, um korrekt zu funktionieren. Das bedeutet, dass der Zugriff zum Internet flexibel an- und ausschaltbar sein muss.

1.3 Aufbau der Arbeit

Es werden zunächst die inhaltlichen Grundlagen erklärt und Fachbegriffe definiert, die für den Aufbau der Laborumgebung benötigt werden.

Im Punkt „Aufbau der Laborumgebung“ wird diskutiert, welche Hardware und Software genutzt werden soll. Dabei wird jede Schicht einzeln durchgegangen, angefangen beim Host Computer bis hin zu den einzelnen virtuellen Maschinen. Es wird erklärt, wie viele und welche Komponenten das Labor beinhalten muss, um ein kompaktes aber dennoch möglichst realistisches Firmennetzwerk zu modellieren. Dabei wird auf die Konfiguration der Komponenten für den Arbeitszweck der Laborumgebung eingegangen. Des Weiteren wird beschrieben, inwiefern die Laborumgebung auf einen älteren Arbeitsstand zurückgesetzt werden kann.

Im Kapitel „Vorbereitung zur Malwareanalyse“ wird vorerst das Grundverständnis zur Arbeit mit Schadsoftware vermittelt und worauf dabei zu achten ist. Außerdem werden Werkzeuge und Anwendungen beschrieben, die für die Malwareanalyse eingesetzt werden sollen. Dieses Kapitel ist in Werkzeuge für die statische Malwareanalyse und in Werkzeuge für die dynamische Malwareanalyse eingeteilt.

Erweiterungen, die die Sicherheit des Nutzers und des Netzwerkes erhöhen, werden in dieser Arbeit nicht behandelt. Das Labor muss bei der Benutzung eine erhöhte Sicherheit verfügen, um effektiv mit gefährlicher Malware arbeiten zu können. Dazu gehören beispielsweise der Aufbau einer Firewall und die Verschleierungsmaßnahmen des Labors, um nicht von der Malware als virtuelle Umgebung erkannt zu werden. Diese Maßnahmen können unter dem Begriff Containment zusammengefasst werden. Das Implementieren des steuerbaren Internetzugangs wird ebenfalls in dieser Arbeit nicht behandelt. Diese und weitere Punkte für die weitergehende Vorgehensweise des Projektes werden im abschließenden Kapitel „Fazit und Ausblick“ besprochen.

2 Grundlagen

2.1 Virtualisierung

Die Virtualisierung beschreibt ein Konzept der Informationstechnik, bei dem zwischen der Hardware eines Computers und einer Anwendung eine zusätzliche Abstraktionsschicht eingefügt wird [2]. Durch die Abstraktion der Hardwareressourcen des Wirtsystems – auch Hostsystem oder Host genannt – können mehrere Gastsysteme unabhängig voneinander darauf zugreifen. Die Ressourcen werden somit aufgeteilt und effizienter nutzbar. Es können Anwendungen, Speicherkomponenten, Betriebssysteme und auch ganze Netzwerke und Server virtualisiert werden [2]. Die Virtualisierung von Betriebssystemen, sowie Netzwerk- und Serverkomponenten wird einen Großteil dieser Arbeit umfassen.

Es gibt grundsätzlich drei Arten der Virtualisierung: Containerisierung, Hardware Emulation und Paravirtualisierung. Mithilfe von Containerisierung können üblicherweise keine ganzen Betriebssysteme simuliert werden. Diese Virtualisierung läuft auf einem Hostsystem und stellt bestimmten Anwendungen vordefinierte Bibliotheken zur Verfügung, wodurch nur diese Anwendungen Zugriff auf den Container haben. Beispielsweise Webserver können diese Möglichkeit nutzen, um den verschiedenen gehosteten Webseiten individuelle Bibliotheken und Anwendungen zur Verfügung zu stellen, ohne dass andere Klienten Zugriff darauf haben. Docker ist ein Beispiel für Containerisierungs-Software. Hardware Emulation hingegen nutzt einen Hypervisor, um eine komplexe virtuelle Hardwareumgebung für die virtuellen Betriebssysteme zu emulieren. Diese Hardwareumgebung wird auch Virtual Machine Monitor (VMM) genannt. Die virtuellen Betriebssysteme werden in Form von virtuellen Maschinen (VMs) dargestellt, welche jeweils streng voneinander getrennt sind. Sie kommunizieren mit dem VMM, anstatt direkt mit der physikalischen Hardware. Mithilfe des Hypervisoren können die virtuellen Maschinen erstellt, konfiguriert, gesteuert und gelöscht werden. Grundsätzlich funktionieren die VMs alle unabhängig voneinander und unabhängig vom Hostsystem, als wären sie eigenständige Betriebssysteme, zumindest aus ihrer Sicht. Mehrere VMs können in einem virtuellen Netzwerk verbunden werden, um miteinander kommunizieren zu können. Des Weiteren besteht durch den Hypervisor die Möglichkeit, unterschiedliche Betriebssysteme verschiedener Hersteller gleichzeitig zu betreiben. Es gibt zahlreiche Hypervisoren, die mit Hardware Emulation arbeiten, da dieser Typ der Virtualisierung am meisten Verwendung findet. Zum Beispiel lassen sich VMware Workstation

Pro oder Microsoft Hyper-V (siehe 3.2.2) darunter zählen. Bei der Paravirtualisierung hingegen gilt das Konzept, dass die Gast-Betriebssysteme direkt mit dem Hypervisor kommunizieren können [3]. Hier koordiniert der Hypervisor den Zugriff der einzelnen Gastbetriebssysteme auf die physikalischen Hardwarekomponenten und stellt sicher, dass kein anderes Betriebssystem gleichzeitig darauf zugreift. Dies soll eine bessere Performance des Systems ermöglichen, vor allem beim Betrieb mehrerer VMs. Um diese Art der Virtualisierung zu ermöglichen, müssen grundlegende Änderungen am Betriebssystem erfolgen, um direkt Kontakt mit dem Hypervisor aufzunehmen. Die Maßnahme kann von Rechteinhabern der Betriebssysteme, also beispielsweise Microsoft, abgelehnt werden [4]. Deshalb ist Paravirtualisierung, vor allem bei den großen Anbietern von Betriebssystemen, eher unpopulär. Diese Änderung wird auch Portierung oder Migration genannt [5]. Ein Beispiel für einen Hypervisor, der Paravirtualisierung unterstützt, ist Xen. Zu beachten ist außerdem, dass für ein virtualisiertes Betriebssystem nach wie vor eine gültige Lizenz benötigt wird. [6]

Hypervisoren werden in zwei verschiedene Arten unterteilt. Typ-1-Hypervisoren werden auch als „Bare-Metal“-Hypervisoren bezeichnet [6]. Diese Hypervisoren haben direkten Zugriff auf die Hardware, ohne das Host-Betriebssystem zu belasten. So werden Ressourcen für VMs direkt von der Hardware abgerufen [7]. Sie sitzen also im übertragenen Sinne auf dem „blanken Metall“. Aus diesem Grund unterstützen Typ-1-Hypervisoren meistens auch Hardware Virtualisierung [8]. Ein Beispiel für einen Typ-1-Hypervisor ist die Reihe der VMware ESXi Hypervisoren (siehe 3.2.1). Typ-2-Hypervisoren werden auch gehostete Hypervisoren genannt, da sie als Softwareanwendung auf einem bestehenden Host-Betriebssystem installiert werden [7]. Die virtuellen Maschinen kommunizieren mit dem Hypervisor, welcher die Hardware Ressourcen auf die virtuellen Maschinen aufteilt. Dadurch ergibt sich im Vergleich zu Typ-1-Hypervisoren eine geringere Performance, da das Host-Betriebssystem eine weitere Schicht zwischen der Hardware und den VMs darstellt. Oracle VirtualBox ist ein Beispiel für Typ-2-Hypervisoren.

Die Technik der Virtualisierung stellt die Möglichkeit zur Verfügung, dass virtualisierte Betriebssysteme auf einen früheren, gespeicherten Zustand zurückgesetzt werden können. Diese Funktion wird Snapshot Funktion genannt. Dabei wird ein virtuelles Abbild der Festplatte zu dem Zeitpunkt der Snapshot Aufnahme erzeugt. So können Snapshots erstellt werden, bevor Maßnahmen ausgeführt werden, die eventuell Schäden am System anrichten können. Falls es zu irreparablen Schäden kommt, kann die VM auf einen beliebigen, zuvor erstellten Snapshot zurückgesetzt werden. Beim Erstellen eines Snapshots wird eine Kopie der virtuellen Festplatte erstellt, sowie eine Delta Datei, welche alle Änderungen am Dateisystem der VM abspeichert. Die Festplattenabbilder können dementsprechend nur so

groß wie die eigentliche virtuelle Festplatte werden. Wird eine VM von einem Snapshot wieder hergestellt, so werden die Dateien mit der virtuellen Festplatte zusammengeführt. [9, 10]

2.2 Active Directory

Active Directory (AD) ist ein Verzeichnisdienst von Microsoft, welcher erstmals für Windows 2000 verfügbar war [11]. Active Directory wird auch als das Netzwerk Betriebssystem von Microsoft bezeichnet [11]. Es wird beispielsweise in Firmen-Intranets genutzt, um zentralisiert die gesamten Informationen über die Nutzer und Gruppen, Computer und Geräte, sowie Anwendungen und weitere Dienste abzuspeichern [11, 12]. Diese Informationen werden genutzt, um die einzelnen Mitglieder des Netzwerks zu authentifizieren und zu autorisieren [13]. Dafür wird das Sicherheitsprotokoll Kerberos verwendet [14]. Durch das Abspeichern der gesamten Informationen an einem Ort wird der Administrationsaufwand drastisch verringert, da neben dem Abrufen der Informationen auch die Verwaltung und Organisation des Netzwerkes erleichtert und zentralisiert wird. Des Weiteren kann der Administrator den Nutzern bestimmte Zugriffsrechte verteilen [12]. Dabei wird zwischen Computerrechten und Nutzerrechten unterschieden. Computerrechte sind an einen Computer gebunden, egal welcher Nutzer den Computer benutzt. Außerdem sind Computerrechte den Nutzerrechten übergestellt, falls es zu Konflikten kommt [15].

AD arbeitet objektorientiert. Das bedeutet, dass alle Daten im Netzwerk als Objekte angesehen werden, welche bestimmte Attribute aufweisen [14]. Sie können auch als Container und Non-Container oder Leaf nodes bezeichnet werden [11]. Active Directory bildet den Aufbau des Firmennetzwerks hierarchisch ab, wie es auch in einem Dateisystem praktiziert wird. Nutzer und andere Objekte in dem Netzwerk mit den gleichen Berechtigungen und Beziehungen werden vom Administrator in Gruppen eingeteilt, welche auch als Domänen bezeichnet werden [12]. Außerdem werden sogenannte Organisationseinheiten (OUs) genutzt, um Objekte und weitere OUs zu gruppieren. Das Erstellen von OUs bringt den Vorteil mit sich, dass das Verwalten nicht so aufwendig ist, als es bei neu erstellten Domänen der Fall ist [12]. Dabei bildet sich eine Baum- beziehungsweise Foreststruktur, welche sich aus dem Zusammenschluss von mindestens einer Domäne, OUs und weiteren Objekten bildet [14]. Der Server, auf dem die Administration der Domäne von statten geht, wird als Domain Controller, auf Deutsch Domänencontroller, bezeichnet [11, 12].

2.3 Domain Name Service

Der Domain Name Service (DNS) ist eng mit Active Directory verbunden. DNS ist ein standardisiertes Verfahren, um die Zuordnung von Namen zu numerischen Internetadressen - und andersherum - zu ermöglichen. Domänen-Namen, welche einen Computer bezeichnen, haben dementsprechend stets eine IP-Adresse als Gegenstück. Die Domänennamen dienen letztendlich nur zur besseren Identifizierung durch den Menschen, da sich Namen besser als lange Zahlenketten merken lassen. Außerdem sind Domänen hierarchisch aufgebaut. An der Spitze eines Domain-Namespace, oder Domänen-Namensraums, steht die Stammdomäne. Darunter teilt sich der Domain-Namespace in mehrere Server auf, welchen sich wiederum mehrere Server untergeordnet haben. Alle Domänennamen, deren übergeordnete Domäne einem Server zugeordnet wurde, können in einer DNS-Zone eingeordnet werden [11]. Diese Zonen stellen Verwaltungsbereiche im Domain-Namespace dar, welche auch Subdomänen beinhalten können. Um einen DNS-Namen eindeutig zu identifizieren und um seine zugehörige IP-Adresse zu erfahren, wird der Fully Qualified Domain Name (FQDN) genutzt. Dieser für jeden Computer einzigartige DNS-Name besteht aus mehreren Segmenten, welche durch Punkte getrennt sind. Jedes Segment stellt eine Domain in der Hierarchie dar. Um den Namen aufzulösen, muss er von rechts nach links gelesen werden. Ganz rechts steht meistens die sogenannte Top-Level-Domain (TLD), beispielsweise „.de“ oder „.com“. Danach folgen die Subdomänen. Bei Active Directory muss die Stammdomäne des Root-Servers aus einem Präfix und einem Suffix bestehen, in der Schreibweise „Präfix.Suffix“. Diese Domäne sollte möglichst kurz und prägnant sein. Clients einer Domäne können mithilfe von DNS Domänencontroller suchen, damit sie für die Clients bestimmte Aufgaben ausführen [16]. In einem Active Directory ist also ein DNS-Server essenziell. [17, 18, 19]

2.4 Microsoft Exchange Server

Microsoft Exchange Server ist unter anderem ein E-Mail-Dienst, der in einem Netzwerk die Kommunikation über E-Mails, sowie weitere Funktionen zur effizienten Arbeit in Arbeitsgruppen bereitstellt. Exchange Server ist dabei für die Verwaltung und Ablage von E-Mails in einem Netzwerk zuständig. Für die Konfiguration von Exchange Servern und für das Speichern von Informationen wird Active Directory verwendet [20]. Außerdem wird sichergestellt, dass die Kommunikation überprüft wird und sicher vonstattengeht. Genauer gesagt werden mit Viren infizierte E-Mails und Spam von dem Server herausgefiltert, bevor die Nachrichten beim Empfänger ankommen. Der Administrator des Exchange Servers ist in

der Lage, Änderungen an dem Viren- und Spamschutz nach seinen Präferenzen vorzunehmen, sowie die Nutzer in der Exchange Organisation zu verwalten. In Unternehmensumgebungen findet Exchange Server oft Anwendung. Zur Installation eines Microsoft Exchange Servers ist ein Betriebssystem der Windows Server Reihe vonnöten. Nutzer des E-Mail-Dienstes benötigen beispielsweise die Software Microsoft Outlook oder den Web-Browser Klienten von Microsoft Outlook, um mit anderen Teilnehmern im Netzwerk kommunizieren zu können. E-Mail-Verkehr ist für Malware ein sehr häufig vorkommender Angriffsvektor. Außerdem verbreiten sich vor allem Computerviren oft über E-Mail-Verkehr. Aus diesem Grund ist die Installation eines Exchange Servers in der Laborumgebung sinnvoll, um solche Angriffsszenarien zu simulieren und zu untersuchen. [21, 22]

2.5 Malware und Malwareanalyse

Malware setzt sich aus dem englischen malicious, wie bösartig und ware, angelehnt aus dem Wort Software, zusammen. Dementsprechend kann Malware auch als Schadsoftware übersetzt werden. Zu beachten ist, dass Malware dazu programmiert wurde, um beabsichtigt Schaden am Zielsystem zuzufügen. Software, die ungewollt schädliche Funktionen ausführt, zählt demnach nicht unter Malware. Abhängig von dem Typ der Malware kann es durch dessen Einsatz zum Verlust der Datenintegrität, zum Verlust der Vertraulichkeit von Daten oder zu direkter Beschädigung von Informationen und IT-Systemen kommen. [23, 24]

Es gibt zahlreiche Arten von Malware, die sich in drei Hauptcharakteristiken unterscheiden. Der Angriffsvektor beschreibt die Art, auf welche Weise eine Malware das Wirtssystem infiziert. Außerdem kann Malware in ihrem Verhalten im Wirtssystem unterschieden werden. Die dritte Eigenschaft beschreibt, auf welche Art und Weise die Malware sich verbreitet. In Abbildung 1 sind die häufigsten Verhaltensweisen beziehungsweise Varianten von Malware dargestellt und nach ihrem Grad der Bedrohung aufgereiht. Dabei sind sie in Laufrichtung des Pfeils von niedriger zu hoher Bedrohung sortiert. Die geringste Bedrohung stellen Exploits dar. Exploits sind Werkzeuge für Angreifer, die Sicherheitslücken von Software identifizieren und ausnutzen [25]. Rootkits hingegen sind meist Sammlungen von Softwaretools, die primär dazu dienen, dem Angreifer Administrator- oder Root-Rechte zu gewähren und seine Präsenz zu verschleiern [26]. Eine weit verbreitete Art von Malware sind Trojanische Pferde, oder Trojaner genannt. Diese geben sich als nützliche, harmlose Programme aus und führen im Hintergrund unentdeckt einen schädlichen Code aus, der beispielsweise weitere Schadsoftware herunterlädt oder eine Backdoor installiert [27]. Die Malware mit der nächsthöheren Bedrohungsstufe sind Backdoors. Backdoor bedeutet übersetzt Hintertür.

Dieser Typ von Malware ist „ein alternativer Zugang zu einer Software oder einem Hardwaresystem, der den normalen Zugriffsschutz umgeht.“ [28]. Die wahrscheinlich bekannteste Malware-Art ist der Virus. Computerviren infizieren mehrere Dateien auf dem Zielrechner und verbreiten sich durch Duplizieren und Versenden von infizierten Dateien, beispielsweise über E-Mail-Verkehr. Viren sind also auf die Hilfe des Nutzers angewiesen. Würmer hingegen können sich selbstständig in Netzwerken verbreiten, ohne Hilfe des Menschen, wodurch die Verbreitung weitaus schneller geschieht. Häufig bestehen Malwareprogramme aus mehreren Arten von Malware gleichzeitig oder sie laden weitere Schadsoftware nach, um die Erfolgschance der Entdeckung zu minimieren und die Chance der Kompromittierung des Zielsystems zu maximieren. So könnte ein komplexes Malwareprogramm potenziell alle dieser sechs beschriebenen Malwarearten beinhalten. Kompromittieren bedeutet „unberechtigt in ein Computersystem ein[zu]dringen und dort gespeicherte Daten aus[zu]spähen oder [zu] manipulieren“ [29]. [23, 24]

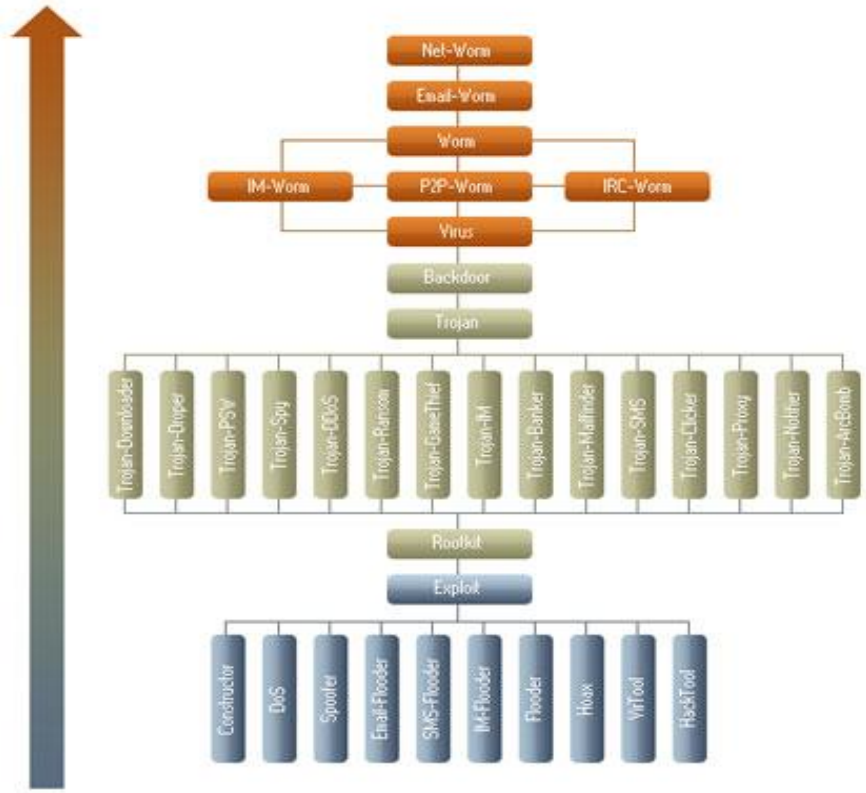

Abbildung 1: Malware Arten und Klassifikation ihrer Bedrohung

Quelle: [30]

Die Malwareanalyse beschäftigt sich mit der Untersuchung von Schadsoftware, um so viele nützliche Informationen wie möglich über die Malware zu erhalten. Die Hauptziele der Malwareanalyse sind zum einen, Informationen über den Angreifer zu erhalten. Zum anderen soll herausgefunden werden, was das Ziel der Malware ist. Außerdem wird die Malware auf spezifische forensisch relevante Artefakte untersucht, die zur Wiedererkennung beitragen. Solche Merkmale werden Indicators of Compromise (IoCs) genannt. Diese Kompromittierungsindikatoren sind „Hinweise auf die Aktivitäten der Schadsoftware“, welche benutzt werden, um Angriffe ähnlicher Art zu erkennen und zu verhindern. Die Artefakte beziehungsweise IoCs sind unter anderem Log-Dateien, Hashwerte, Konfigurationsdateien, Cachedaten, IP-Adressen, Hostnamen, Prozessnamen und Schlüssel der Windows-Registry [31, 32]. Hashwerte sind numerische Werte, welche aus mathematischen Hashfunktionen errechnet werden. Diese Funktionen sind Einwegfunktionen, das bedeutet, dass sie nicht zurückrechenbar sind und vom Hashwert nicht auf den Originalinhalt geschlossen werden kann. Die Windows-Registry wird auch Windows-Registrierungsdatenbank genannt. Darin werden sämtliche Konfigurationsinformationen vom Betriebssystem und von Programmen gespeichert. Sie besteht aus zahlreichen Schlüsseln, worin die Informationen gespeichert werden. Einige Arten von Malware versuchen, eigene Registry-Schlüssel zu erstellen, um beispielsweise nach einem Neustart des Wirt-Computers direkt ausgeführt zu werden [33]. Um die forensischen Artefakte zu finden und zu untersuchen, werden zahlreiche Tools genutzt, die jeweils auf spezifische Aufgaben spezialisiert sind. Die Malwareanalyse kann in zwei Vorgehensweisen unterteilt werden. Bei der statischen Analyse wird sich die Malware im Detail angeschaut ohne sie auszuführen. Die zweite Methode der Malwareanalyse ist die dynamische Analyse, welche erst nach der statischen durchgeführt werden sollte. Dabei wird die Malware in einer abgesicherten Umgebung unter Beobachtung ausgeführt. Beide Arten der Malwareanalyse werden in der zu entwickelnden Laborumgebung möglich sein. [34, 35]

3 Aufbau der Laborumgebung

Das virtuelle Labor zur Malwareanalyse soll ein möglichst realistisches Modell eines Firmennetzwerks darstellen. Bevor die eigentliche Umgebung konzipiert wird, muss sich mit dem Host Computer und der Hypervisor-Software auseinandergesetzt werden, auf denen die Laborumgebung installiert wird. Die Komponenten der Umgebung werden mithilfe von VMs realisiert. Eine VM stellt den Server dar, der die Daten- und Nutzerverwaltung sicherstellt. Auf dem Server wird ein Active Directory installiert, der diese Aufgabe als Domänencontroller ausführt. Des Weiteren muss diese VM als DNS-Server konfiguriert werden. Eine zweite VM ist für den Microsoft Exchange Server zuständig. Weiterhin gibt es zwei VMs, die die Nutzer beziehungsweise Angestellten des Firmennetzwerks darstellen. Im Anschluss geht es um die Zurücksetzbarkeit der gesamten Laborumgebung mithilfe der Snapshot-Technologie.

3.1 Der Host Computer

Der Computer, auf dem das virtuelle Labor installiert werden soll, stellt die notwendige Hardware zur Verfügung. Außerdem ist auf dem Host Computer der Hypervisor installiert, der die Schnittstelle zwischen der Hardware und den VMs darstellt. Die Systemanforderungen mehrerer virtueller Betriebssysteme und Server müssen von diesem einen Computer übertroffen werden. Deshalb muss der Host Computer über einen leistungsstarken Prozessor und ausreichend Arbeits- sowie Datenspeicher verfügen. Konkret wird ein Prozessor der 64-Bit-Architektur benötigt, bestenfalls mit einer Spezialisierung für den Zweck der Virtualisierung. Hier kommen beispielsweise ein VT-x Prozessor von Intel oder ein AMD-V Prozessor von Advanced Micro Devices (AMD) infrage [36]. Im BIOS muss außerdem die Möglichkeit zur Virtualisierung des Prozessors eingeschaltet sein, wenn diese Funktion nicht automatisch aktiviert ist.

Die benötigte Kapazität des Festplattenspeichers, der die Datenträgerabbilder der VMs speichert, ist schwer zu definieren. Aufgrund der Zielstellung, Snapshots aller VMs zu erstellen (siehe 3.5), muss der Festplattenspeicher über eine ausreichend große Reserve für die Snapshots verfügen, da diese Dateien sehr groß werden können. Snapshot Dateien können höchstens so groß werden, wie die entsprechenden virtuellen Festplatten selbst

[37]. Wird davon ausgegangen, dass vier VMs mit jeweils 60 Gigabyte (GB) Festplattenspeicher installiert werden und für jede VM zwei Snapshots erstellt werden können. Dann würden pro VM mindestens 180 GB Festplattenspeicher benötigt werden. Aufsummiert sind das für vier VMs 720 GB. Zusätzlich muss ausreichend Puffer eingeplant werden. Eine SSD Festplatte mit einem Terrabyte (TB) Speicherkapazität sollte für den Anfang also völlig ausreichen.

Was den Arbeitsspeicher betrifft, müssen die Systemanforderungen der einzelnen Betriebssysteme und Anwendungen akkumuliert werden. In Tabelle 1 sind die Mindestanforderungen für den Arbeitsspeicher angegeben, die für die zu benutzenden Betriebssysteme und Grundanwendungen benötigt werden. Damit die Betriebssysteme Windows Server 2019 und Windows 10 betrieben werden können, werden mindestens 2 GB Arbeitsspeicher benötigt. Um einen Domänencontroller mit Active Directory flüssig zu betreiben, werden 12 GB empfohlen. Die Arbeitsspeicherbelastung zum Betrieb des DNS Servers ist so gering (weniger als 5 Megabyte (MB)), dass ihr keine Beachtung geschenkt werden muss. Um einen Microsoft Exchange Server zu betreiben, werden in der virtuellen Umgebung 16 GB empfohlen. So ergeben sich bei der Domaincontroller VM mindestens 14 GB, bei der Exchange Server VM mindestens 18 GB und bei den Client VMs jeweils mindestens 2 GB. Zusätzlich zu den Anforderungen der VMs kommt noch die Mindestanforderung des Host Betriebssystems beziehungsweise des Typ-1-Hypervisors dazu. Aufsummiert sind dies also mehr als 36 GB minimal benötigter Arbeitsspeicher. Um eine flüssige Arbeit mit der Laborumgebung zu gewährleisten, muss der eingebaute Arbeitsspeicher diese Mindestangabe stark überschreiten. Üblicherweise werden in Computern Arbeitsspeicher eingebaut, dessen Größe einem Potenzwert von zwei in GB entsprechen. Aus diesem Grund wird der Host Computer mindestens 64 GB verfügen. [38, 39, 40, 41]

Abhängig vom Hypervisor, benötigt der Host Computer ein Betriebssystem, auf dem der Hypervisor installiert wird. Bei der Arbeit mit unbekannter Malware besteht die Gefahr, dass diese in der Lage ist, aus einer VM auszubrechen und das Host System anzugreifen. Nach Absprache mit den Mitarbeitern der T-Systems MMS sollte das Host-Betriebssystem von einem anderen Hersteller sein, als die Betriebssysteme der VMs. Diese Maßnahme erschwert es der Malware, das Host-Betriebssystem als solches zu erkennen und es anzugreifen. Die zu installierenden VMs haben Betriebssysteme von Microsoft Windows, weshalb das Host-Betriebssystem zum Beispiel eine Linux-Distribution sein sollte.

Ein Vorteil bei der Planung bezüglich der Hardwareressourcen ist, dass weitere Hardware nachträglich in den Host Computer verbaut werden kann. Vor allem der Festplatten- und Arbeitsspeicher kann ohne große Probleme erweitert werden. Sollten also die Kapazitäten während der Nutzung der Laborumgebung auf ihre Grenzen stoßen, kann die Laborumgebung im Nachhinein mit mehr Leistung ausgestattet werden.

Tabelle 1: Mindestanforderungen für den Arbeitsspeicher der verwendeten Betriebssysteme und Anwendungen

Name des Computers / Name der VM	Betriebssystem /Anwendung	Minimal benötigter Arbeitsspeicher
Domänencontroller VM	Microsoft Windows Server 2019	2 GB
	Active Directory Domain Controller Services	12 GB
	DNS Server	< 5 MB
		14 GB
Exchange Server VM	Microsoft Windows Server 2019	2 GB
	Microsoft Exchange Server 2019	16 GB
		18 GB
Client VM 1	Microsoft Windows 10	2 GB
Client VM 2	Microsoft Windows 10	2 GB

Quelle: eigene Darstellung, [38, 39, 40, 41]

3.2 Wahl des Hypervisoren

Der Hypervisor ist der Knotenpunkt zwischen der Hardware des Host Computers und den VMs. Aus diesem Grund ist es wichtig, die richtige Entscheidung zu treffen, welche Art der Virtualisierung und welche Hypervisor Software am besten für das Projekt geeignet ist. Da es sich bei den VMs um komplexe Betriebssysteme handelt, kommt der Virtualisierungstyp der Containerisierung nicht infrage, da mit dieser Art der Virtualisierung keine ganzen Betriebssysteme virtualisiert werden sollten. Die Paravirtualisierung ist ebenfalls ungeeignet, da durch die Portierung Kompatibilitätsprobleme mit dem Betriebssystem auftreten könnten. Außerdem wird Paravirtualisierung nicht von Microsoft unterstützt und bietet dementsprechend auch wenig Dokumentation [3]. Die Hardware Emulation als Virtualisierungstyp ist in diesem Szenario weitaus geeigneter. Sie ist zum Virtualisieren von mehreren Betriebssystemen ausgelegt und bietet das höchste Maß an Dokumentation, da sie auch der am meisten genutzte Virtualisierungstyp ist.

Ob ein Typ-1- oder Typ-2-Hypervisor die bessere Wahl ist, muss an bestimmten Anforderungen der Laborkomponenten, sowie an Vor- und Nachteilen der Hypervisor-Typen erschlossen werden. Der Hypervisor muss eine hohe Sicherheit gegen Malwareangriffe bieten. Vor allem das Host System sollte vor Übergriffen aus einer infizierten VM geschützt sein. Außerdem muss der Hypervisor eine Snapshot Funktion beinhalten, mit der die VMs der Laborumgebung einheitlich auf einen unversehrten Zustand zurückgesetzt werden können. Typ-1-Hypervisoren liefern aufgrund der dünneren Schicht zwischen Hardware und VMs eine bessere Leistungsfähigkeit als Typ-2-Hypervisoren. Da mehrere Betriebssysteme gleichzeitig flüssig betrieben werden müssen, kann die Reduzierung der Performance bei einem Typ-2-Hypervisor ein Problem darstellen. Ein Vorteil von Typ-2-Hypervisoren sind hingegen die Kosten. Die meisten Typ-1-Hypervisoren sind für den Betrieb einer komplexen Produktivumgebung konzipiert, potenziell mit mehreren Servern und vielen Clients. Deshalb werden für diese Hypervisoren auch höhere Kosten verlangt. Typ-2-Hypervisoren sollten nicht für Firmennetzwerke und ähnliche komplexere Projekte genutzt werden, sondern eher für Testszenarien und privaten Gebrauch [8]. Dementsprechend kosten Typ-2-Hypervisoren weitaus weniger und bieten oft sogar kostenfreie Versionen an.

Die forensische Laborumgebung soll zwar ein Firmennetzwerk simulieren, aber in einer minimalisierten Form. Aus diesem Grund kommen beide Hypervisor-Typen potenziell infrage. Zwei der bekanntesten Hypervisoren sind VMware ESXi und VMware Workstation Pro. Welcher dieser Hypervisoren für das Projekt am besten geeignet ist, soll in diesem Kapitel erschlossen werden.

Bei der Wahl des Hypervisors stand außerdem die Virtualisierungssoftware Vagrant zur Diskussion, da dieses Programm in der Firmenumgebung schon genutzt wird und die IT-Forensiker Erfahrung damit haben. Vagrant wurde von der Firma Hashicorp entwickelt und ist an sich kein Hypervisor. Die Software dient als sogenannter Wrapper, der mithilfe eines Hypervisors virtuelle Maschinen konfigurieren kann [42]. Dabei kann auf schon erstellte, vorkonfigurierte VMs zurückgegriffen werden, welche als Vagrantboxen bezeichnet werden. Die Konfiguration der VMs geschieht über die sogenannte Vagrant File. Diese Textdatei ist ein Ruby Skript, bei dem unter anderem die Hardwareressourcen, der Hypervisor und die Netzwerkeinstellungen definiert werden. Außerdem können Shell Befehlszeilen in der Vagrant File geschrieben werden, die beim Start der VM ausgeführt werden sollen. Die Nutzung von Vagrant wurde zwar in Betracht gezogen, jedoch ist die gesamte Konfiguration des Labors über eine Skript Datei, aus eigener Erfahrung, zu umständlich und aufwendig. [35]

3.2.1 VMware ESXi

VMware ESXi ist ein Typ-1-Hypervisor, welcher ohne ein Host-Betriebssystem installiert wird. VMware ESXi gehört zu der VMware vSphere Suite, einer Sammlung von Software, die zur Verwaltung und zum Ressourcenmanagement bei Virtualisierung entwickelt wurde. Dabei wird der Hypervisor ESXi als Hauptkomponente der vSphere Suite gesehen. In der T-Systems MMS sind einige ESXi Hosts in Betrieb. VMware ESXi 7.0 ist die neueste Version dieses Hypervisors, welche im April 2020 erstmals veröffentlicht wurde [43]. [44]

Um VMware ESXi zu installieren, muss die Software beispielsweise von einem USB-Stick gebootet werden, wie es auch bei einer Installation eines Betriebssystems üblich ist. Es werden lediglich 144 MB Festplattenspeicher belegt. Dadurch wird die Sicherheit erhöht, da der Hypervisor schwerer als solcher zu identifizieren ist. Die Konfiguration des Hypervisors und der Netzwerkeinstellungen wird über das Direct Console User Interface (DCUI) gesteuert, welches in Abbildung 2 zu sehen ist. Das Erstellen von VMs und deren Konfiguration, aber auch Maßnahmen während des Betriebs der VMs müssen von einem anderen Computer über einen Browser mit dem vSphere (HTML5 Web) Host Client durchgeführt werden [45]. Dafür muss sich dieser externe Computer selbstverständlich im gleichen Netzwerk wie der ESXi Host befinden. Daraus lässt sich schließen, dass der Host Computer mit dem Firmennetzwerk der T-Systems MMS verbunden sein muss, wenn die VMs genutzt werden sollen. Der Web Client von VMware hat nur Zugriff auf den ESXi Host über eine zusätzliche Anwendung namens vCenter Server. vCenter Server dient zur zentralisierten Verwaltung eines oder auch mehrerer Server in einer Unternehmensumgebung. Mithilfe

von vCenter Server kann ein Datacenter, oder auch Rechenzentrum, erstellt werden, mit dem der ESXi Host anschließend verbunden wird. Das Datacenter stellt in dem Sinne eine abgeschlossene Umgebung für den ESXi Host dar. [44]

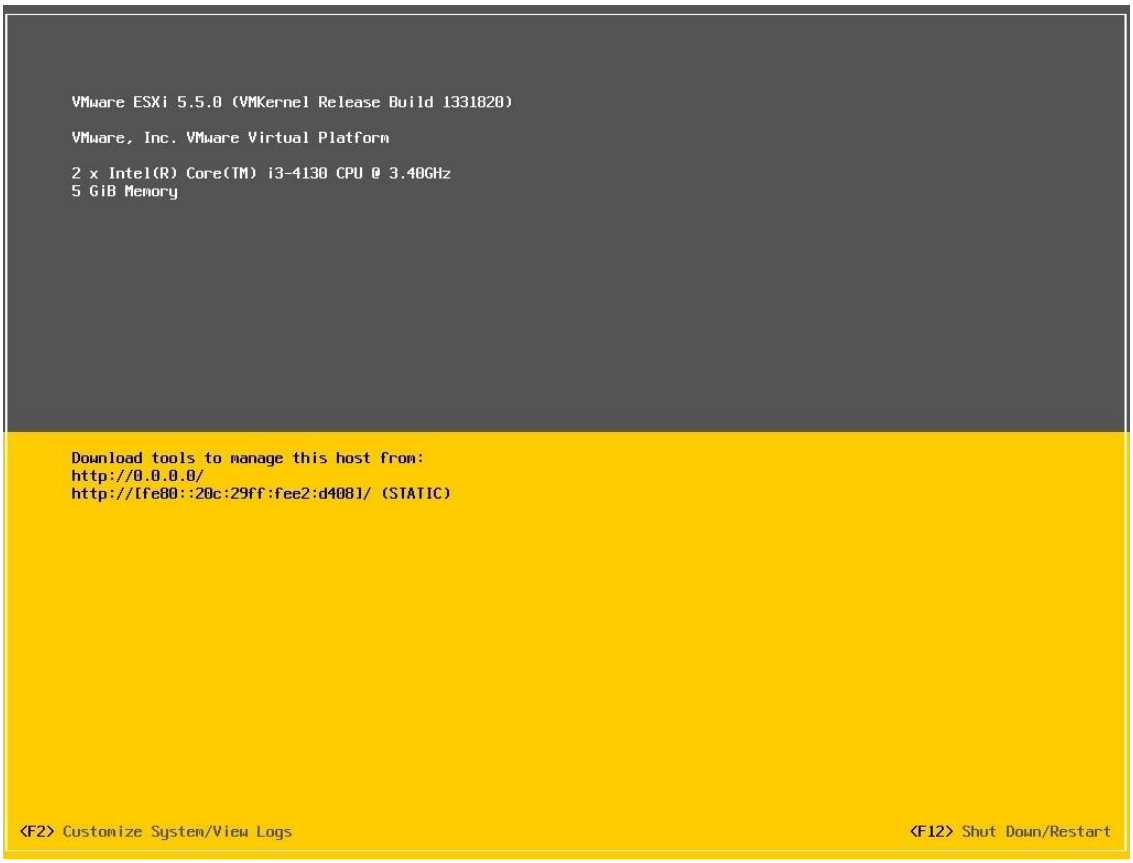

Abbildung 2: Direct Console User Interface (DCUI) eines VMware ESXi 5.5.0 Hosts

Quelle: [44]

VMware ESXi arbeitet mit einer Technologie namens CPU-Virtualisierung. Dabei wird der Prozessor des Hosts virtualisiert, um ihn als mehrere separate Prozessoren zu behandeln. Dadurch wird die Performance beim Betrieb mehrerer unterschiedlicher VMs beschleunigt. CPUs zu virtualisieren bietet bessere Leistung, als sie zu emulieren. Beim Emulieren des Prozessors werden die verschiedenen Operationen der VMs durch die Hypervisor Software ausgeführt, welche die nötigen Ressourcen vom Host-Prozessor gestellt bekommt. Des Weiteren ist in ESXi ein eigenes Dateisystem implementiert, das Virtual Machine File System (VMFS). Es bietet ein für virtuelle Umgebungen spezialisiertes Cluster-Dateisystem, wodurch hohe Leistung versprochen wird. Um virtuelle Vernetzung zu ermöglichen, bietet ESXi die Erstellung mehrerer virtueller Ethernet Adapter, sowie virtueller Switches. Ethernet Adapter sind die benötigten Schnittstellen, um einem externen Ethernet Netzwerk beitreten

zu können [46]. Mit einem virtuellen Switch können die VMs auf dem gleichen ESXi Host miteinander kommunizieren. [44]

Beim Erstellen einer neuen VM über den vSphere Client können der Name und Speicherort, die Kompatibilität mit älteren ESXi Versionen, sowie die Hardware Einstellungen definiert werden. Da keine anderen ESXi Hosts in der Laborumgebung Verwendung finden werden, ist die Kompatibilität auf der höchsten Version von ESXi zu belassen. Bei den Hardware Einstellungen sind die wichtigsten Punkte der Prozessor, der Arbeitsspeicher, die Festplatte und die Netzwerkeinstellungen sowie die Netzwerkschnittstellen. Die virtuelle Festplatte kann in ESXi auf drei verschiedene Arten beschrieben werden (siehe Tabelle 2). Thick Provision Lazy Zeroed beschreibt den gesamten angegebenen Speicherplatz bei der ersten Schreiboperation der VM. Im Unterschied dazu wird bei Thick Provision Eager Zeroed die Festplatte direkt beim Erstellen der VM angelegt. Der reservierte Speicherplatz wird mit Nullen vollgeschrieben, weshalb dieser Vorgang auch Zeroing genannt wird. Thin Provision beschreibt erst die Fesplattenblöcke, wenn diese auch benötigt werden. Das bedeutet, wenn der beschriebene Speicherplatz nicht mehr benötigt wird, wird dessen Inhalt auch wieder gelöscht. In Bezug auf die forensische Analyse der Datenträger, sollte die Festplatte im Vornherein vollständig erstellt werden, um einer physischen Festplatte am meisten zu ähneln. Aus diesem Grund sollte hier Thick Provision Eager Zeroed verwendet werden.

Tabelle 2: Festplatten Typen in VMware ESXi

Festplatten Typ	Erstelldauer	Block Vorbelegung	Zeroing
Thick Provision Lazy Zeroed	schnell	vollständig vorbelegt	tritt auf, wenn jeder Block zum ersten Mal beschrieben wird
Thick Provision Eager Zeroed	langsam	vollständig vorbelegt	tritt auf, wenn die Festplatte erstellt wird
Thin Provision	am schnellsten	auf Abruf	tritt auf, wenn Blöcke zugewiesen werden

Quelle: übersetzt nach [44]

Die Snapshot Funktion von VMware ESXi speichert die Zustände der Einstellungen, den Leistungszustand, die Zustände aller Festplatten und den Inhalt des Arbeitsspeichers. Mit Leistungszustand ist die Information gemeint, ob die VM zum Zeitpunkt des Snapshots an- oder ausgeschalten ist oder im Zustand suspended ist. [44]

In Bezug auf Sicherheit kann mithilfe von vCenter Server eine Firewall zwischen dem Netzwerk und der ESXi Host Verwaltung eingerichtet werden. Dabei können sämtliche Ports gesperrt werden, welche nicht von verwaltungsrelevanten Protokollen genutzt werden. [44]

Ein weiteres Programm, welches auf dem Host installiert werden sollte, ist VMware Tools. Bei VMware Tools handelt es sich um eine Sammlung von Features und Werkzeugen, die die Arbeit mit VMs verbessern. Unter anderem werden Werkzeuge zur Zeitsynchronisation, Gerätetreiber, Verbesserung der graphischen Darstellung und Verbesserungen der Performance hinzugefügt. [44]

3.2.2 VMware Workstation Pro

VMware Workstation Pro gehört zu den Typ-2-Hypervisoren. Die Software kann auf vielen Linux und Windows Betriebssystemen installiert werden. Die neuste Version von VMware Workstation ist 16.1.0 Pro, welches im November 2020 veröffentlicht wurde [47]. Es existiert eine kostenfreie Testversion, welche für 30 Tage nutzbar ist. Workstation Pro ist in der Lage, mehrere VMs mit unterschiedlichen Betriebssystemen zu erstellen und zu verwalten. Außerdem können virtuelle Netzwerke erstellt und verwaltet werden. Dafür ist die Konfiguration mehrerer virtueller Switches möglich. Außerdem kann Workstation Pro auch mit der in Abschnitt 3.2.1 beschriebenen vSphere Suite verbunden werden. Die gesamte Verwaltung der VMs wird zentral über das Workstation Pro Fenster gesteuert (siehe Abbildung 3). Das Programm ist so strukturiert, dass die einzelnen VMs in Registerkarten betrieben werden. Sie können zusätzlich in einzelne Fenster getrennt werden, um mehrere VMs gleichzeitig einsehen zu können. VMware Workstation 15 Pro wird aktiv von dem IT-Forensikern der T-Systems MMS genutzt. Aus diesem Grund wird im Folgenden diese Version zur Betrachtung herangezogen. [48]

Da die gesamte Verwaltung und Steuerung der VMs auf dem Host Computer abläuft, kann der Host Computer beispielsweise beim Ausführen von unbekannter Malware vollständig vom Firmennetzwerk getrennt werden. Dadurch wird die Gefährdung, dass die Malware aus der VM ausbricht und das Netzwerk des Host Computers befällt, nicht riskiert. In VMware Workstation ist ebenfalls die Technologie der CPU Virtualisierung vorhanden [49].

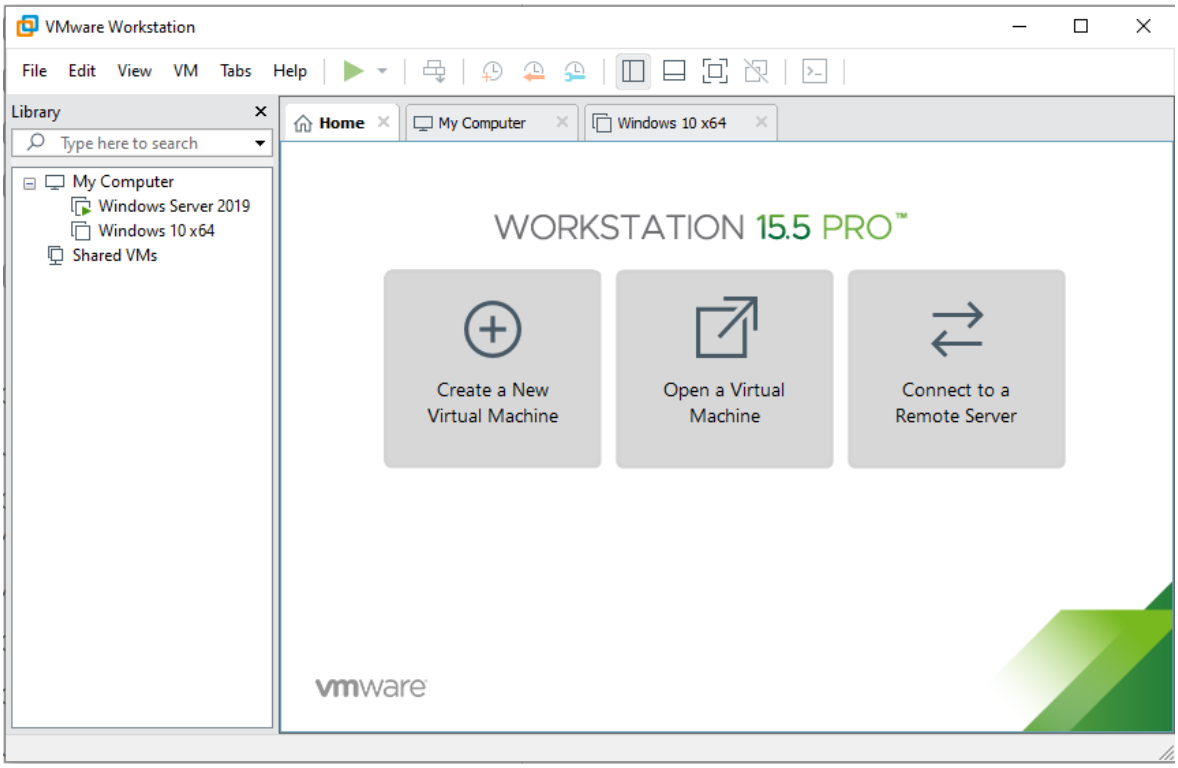

Abbildung 3: VMware Workstation 15.5 Pro Software, Home Registerkarte

Quelle: eigene Abbildung

Bei dem erweiterten Setup zum Erstellen einer VM mit VMware Workstation Pro muss ausgewählt werden, mit welcher Version von Workstation Pro die VM kompatibel sein soll. Da eine Kompatibilität mit älteren Versionen bei der Laborumgebung nicht notwendig ist, sollte die neueste Version gewählt werden. Wurde ein Name für die VM, ein Speicherort auf dem Host Computer, sowie das Installationsmedium gewählt, müssen die Hardware Einstellungen definiert werden. Bei Workstation Pro gibt es die Möglichkeit, die Firmware zu konfigurieren, dabei steht die Wahl zwischen BIOS und UEFI mit oder ohne Secure Boot. UEFI ist zwar moderner und bietet dem Nutzer mehr Komfort, durch eine grafische Oberfläche. Mit mehr Vereinfachung der grundlegenden Konfiguration kommt auch ein Abfall der Sicherheit zustande. Das BIOS schließt direkt an die Hardware an. Das UEFI hat andererseits die Möglichkeit, beispielsweise Treiberupdates über das Internet herunterzuladen. Dadurch ist das UEFI jedoch angreifbarer als das BIOS, da eine Netzwerkschnittstelle über TCP/IP besteht. Da bei der Laborumgebung auf die Bequemlichkeit eines UEFI verzichtet werden kann und das BIOS eine sicherere Hardwareschnittstelle darstellt, wird bei der Konfiguration der virtuellen Maschinen nur mit BIOS gearbeitet. [50]

Danach folgt die Zuweisung von CPUs und Prozessorkernen, Arbeitsspeicher, sowie die Wahl, welchen Netzwerk Typ die VM nutzen soll. Diese Einstellungen sind nach der Installation der VM änderbar. Falls also beim Betrieb Performance Einbuße registriert werden, können die zugewiesenen Ressourcen auch im Nachhinein erhöht werden. Bei VMware Workstation werden standardmäßig zwei Prozessoren mit jeweils einem Kern, zwei GB Arbeitsspeicher und eine Festplattengröße von 60 GB zugewiesen.

Des Weiteren kann, abhängig vom zu installierenden Betriebssystem, ausgewählt werden, welchen I/O-Controller Typ die VM emulieren soll. Bei der Wahl des Input/Output Controller Typs gibt es nur die Möglichkeit zwischen LSI Logic SAS und einem paravirtualisiertem SCSI Controller (PVSCSI). Laut VMware ist PVSCSI eher für Storage Area Networks (SAN) geeignet, die sich auf das Speichern von großen Mengen an Daten konzentrieren. Demnach ist der LSI Logic SAS Controller die geeignetere Wahl, da er über eine bessere Leistung verfügt. [51]

Der nächste Schritt besteht darin, den virtuellen Disktyp auszuwählen. Dabei kann zwischen IDE, SCSI, SATA und NVMe, gewählt werden, wobei der NVMe Typ empfohlen wird. NVMe (NVM Express) ist eine Softwareschnittstelle für SSD Festplatten. Sie wurde im Jahr 2011 erstmals veröffentlicht und stellt somit die modernste Möglichkeit für die Schnittstellentechnologie zwischen Speicher und Software dar [52]. Außerdem kann der Disk Typ nach der Installation der virtuellen Maschine verändert werden [53].

Beim Definieren der Festplatte muss die maximale Größe und die Art der Speicherbelegung ausgewählt werden (siehe Abbildung 4). Die Festplatte wächst beim Nutzen der VM und belegt nicht sofort den gesamten angegebenen Speicher. Um die Performance der VM zu steigern, kann der Haken bei „Allocate all disk space now“ gesetzt werden, wodurch die gesamte virtuelle Disk bei der Installation erstellt wird. Dies entspricht der Entscheidung, ob Thick Provision oder Thin Provision genutzt werden soll. Um die forensische Untersuchung der Festplatte zu erleichtern und möglichst nah am Abbild einer physikalischen Festplatte zu bleiben, sollte die virtuelle Festplatte als einzelne Datei gespeichert sein und nicht in mehrere Dateien aufgeteilt werden. Außerdem erhöht sich damit die Leistung der VM. [54]

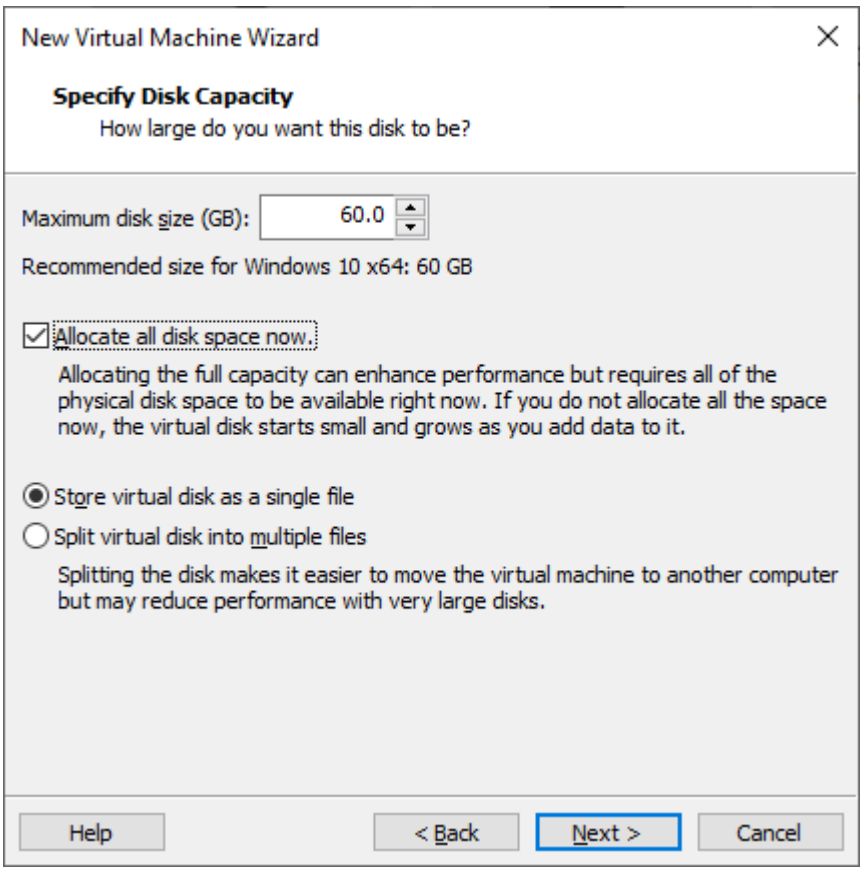

Abbildung 4: Einstellungen zum Festplattenspeicher einer neuen VM bei Workstation Pro
Quelle: eigene Abbildung

VMware Workstation bietet einige Einstellungen zur Snapshot Funktion. Die Konfiguration stellt die Möglichkeiten zu Verfügung, ob beim Herunterfahren der VM ein Snapshot erstellt werden soll, oder ob zum letzten Snapshot nach dem Herunterfahren zurückgekehrt werden soll. Des Weiteren können mit der AutoProtect Funktion automatische Snapshots in einem definierten Zeitintervall erstellt werden. Im Snapshot Manager können übersichtlich die einzelnen Snapshots in zeitlicher Abfolge eingesehen, geklont, gelöscht, sowie die VM von dem Snapshot aus hochgefahren werden. Um die Sicherheit der VMs zu erhöhen, können die virtuellen Festplatten verschlüsselt werden. Um auf eine verschlüsselte Festplatte zugreifen zu können, wird das vergebene Passwort benötigt. [54]

3.2.3 Diskussion und Fazit

Um die Auswahl des geeigneteren Hypervisors abzuschließen, werden Vor- und Nachteile der beiden Hypervisoren im folgenden Fazit ausgewertet.

VMware ESXi ,als Vertreter für die Typ-1-Hypervisoren, verfügt über eine sehr große Palette an Funktionen zur Verwaltung der VMs, zur Netzwerkkonfiguration, zur komplexen Speicherverwaltung und zur Kommunikation zwischen VM Hosts, die in Produktivumgebungen ihre Aufgabe zuverlässig erfüllen können. VMware Workstation Pro, ein Typ-2-Hypervisor, bietet dahingegen nicht so viele Möglichkeiten zur Verwaltung und zum Hinzufügen weiterer spezieller Features. Doch ein Großteil der Einstellungen von ESXi ist für die Laborumgebung nicht notwendig, da sie zwar eine Firmenumgebung modellieren soll, aber in sehr stark reduzierter Form. Der Überfluss an Möglichkeiten dieses Hypervisors kann sich negativ auf die Konfiguration der VMs auswirken, da man durch die große Auswahl überfordert werden könnte und ein womöglich doch wichtiges Feature übersehen werden könnte. Im Vergleich dazu ist die Konfiguration bei VMware Workstation Pro überschaubar und reduzierter, dennoch sind die wichtigsten Features in der Software enthalten, sodass ohne erweiternde Programme eine Laborumgebung mit vier VMs installiert werden kann. Aus diesem Grund bringt VMware Workstation Pro einen weiteren Vorteil mit sich: die Kosten. Für VMware ESXi wird ein hoher Preis verlangt, der sich realistisch gesehen nur für weitaus größere Produktivumgebungen lohnt. Außerdem muss für VMware vCenter zusätzlich eine Lizenz erworben werden, welche in ähnlich hohen Preiskategorien zu finden ist. Für VMware ESXi ist eine kostenfreie Testversion verfügbar, die 60 Tage gültig ist, mit der der Hypervisor ausgiebig für das benötigte Verwendungsszenario erprobt werden kann. VMware Workstation Pro als alleinstehendes Programm ist bei weitem günstiger. Für VMware Workstation Pro ist eine kostenfreie, 30 Tage gültige Testversion verfügbar, also halb so kurz wie bei VMware ESXi. Die komplexe Konfiguration bei VMware ESXi bringt den Vorteil mit sich, die virtuelle Umgebung für jeden Verwendungszweck zu optimieren, eine Laborumgebung eingeschlossen. Doch der Hypervisor benötigt einen zusätzlichen externen Computer zur Verwaltung der VMs. Darunter leidet die Zielsetzung, die Laborumgebung so zentralisiert wie möglich zu konzipieren. Die IT-Forensiker bei der T-Systems MMS arbeiten aktiv mit VMware Workstation Pro. Dies ist ein Auswahlkriterium, das nicht zu vernachlässigen ist, denn die Mitarbeiter sind letztendlich diejenigen, die mit der Laborumgebung arbeiten werden. In der Firma existieren zwar auch ESXi Server, doch damit wird nicht aktiv in der Abteilung gearbeitet, wenn es um Virtualisierung und Malwareanalyse geht. Aufgrund der aufgeführten Gründe ist VMware Workstation Pro der geeignetere Hypervisor.

3.3 Erstellen der virtuellen Maschinen

Als erstes wird die Domänencontroller VM installiert und die Active Directory Verzeichnisdienste sowie der DNS Server konfiguriert. Anschließend wird der Exchange Server installiert und konfiguriert. Danach werden die beiden Klient VMs erstellt und mit den Serverdiensten verbunden. Da die virtuelle Laborumgebung ein virtuelles Netzwerk darstellt, benötigen die VMs einen gemeinsamen Netzwerkadapter, über den die VMs miteinander kommunizieren. In den VMware Workstation Einstellungen muss bei der Installation der VMs der Netzwerkadapter in einen Custom Adapter geändert werden, welcher noch nicht zugewiesen wurde. Für die Laborumgebung kann beispielsweise der Adapter „VMnet2“ gewählt werden. Alle VMs müssen einen eindeutigen Nutzernamen und ein ausreichend starkes Passwort haben. Die Passwörter sollten für jede VM einzigartig sein. Außerdem muss jeder VM eine feste IP-Adresse zugewiesen werden. Dabei dürfen sich die IP-Adressen nur im letzten Oktett unterscheiden, damit sie miteinander kommunizieren können. Beim Konfigurieren der Hardwareressourcen können zunächst die Standardeinstellungen beibehalten werden. Falls beim Betrieb Einbrüche der Performance auftreten, können die Hardwareressourcen später angepasst werden.

3.3.1 Domänencontroller VM

Die virtuelle Maschine, auf der das Active Directory, sowie der DNS-Server installiert werden soll, stellt den wichtigsten Teil der Windows-Laborumgebung dar. Diese VM muss zuerst installiert werden. Der erste Schritt ist stets, das Betriebssystem zu installieren, in diesem Falle muss ein Windows Server 2019 VM erstellt werden. Mithilfe des Server-Managers, der grundsätzlich bei Windows Server Betriebssystemen installiert ist, können sämtliche Einstellungen bezüglich des Servers und seinen Serverrollen konfiguriert werden (siehe Abbildung 5).

Zunächst sollte dem Server VM ein prägnanter PC Name und eine IP-Adresse zugewiesen werden. Um den Namen der VM zu ändern, muss im Suchfenster „Erweiterte Systemeinstellungen anzeigen“ eingegeben werden. Unter dem Reiter „Computername“ bei „Ändern…“ kann der Computername eingeben werden. Der Name des Domänencontrollers muss als solcher erkennbar sein und darf keinen zu langen Namen bekommen. In diesem Fenster kann auch der Domänenname eingegeben werden, zu welcher der Computer gehören soll. Da noch keine Domäne besteht, muss an dieser Stelle keine Änderung vorgenommen werden. Die IP-Adresse muss über die Adapteroptionen in den Netzwerkeinstellungen geändert werden. Dazu müssen die TCP/IPv4 Einstellungen des Netzwerkadapters

angepasst werden. Der bevorzugte DNS-Server erhält dieselbe IP-Adresse wie die VM selbst, da der Domänencontroller den DNS Server repräsentiert [55]. Es ist außerdem möglich, für die IP-Adresse des DNS Servers „127.0.0.1“ zu wählen. Diese IP-Adresse stellt als „localhost“ die lokale VM dar. [56]

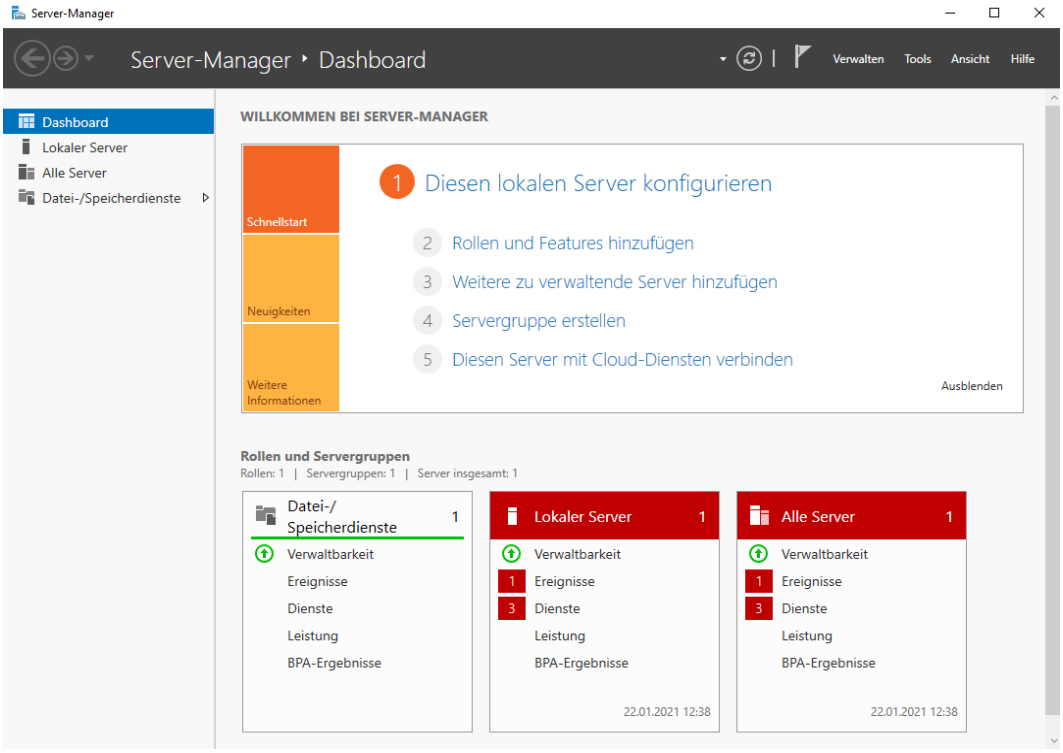

Abbildung 5: Server-Manager einer Windows Server 2019 VM

Quelle: eigene Abbildung

Bei der Konfiguration des Servers müssen die Serverrollen ausgewählt werden. Die Wahl der Serverrollen bestimmt, welche Dienste der Server beim Betrieb ausführen soll. Dementsprechend müssen die Active Directory-Domänendienste (AD DS) und die DNS-Serverrolle ausgewählt werden (siehe Abbildung 6). Die Features, welche zu den gewählten Serverrollen gehören, werden nach der Wahl der Serverrollen automatisch hinzugefügt. Damit werden die notwendigen Komponenten für ein Active Directory und einen DNS-Server installiert.

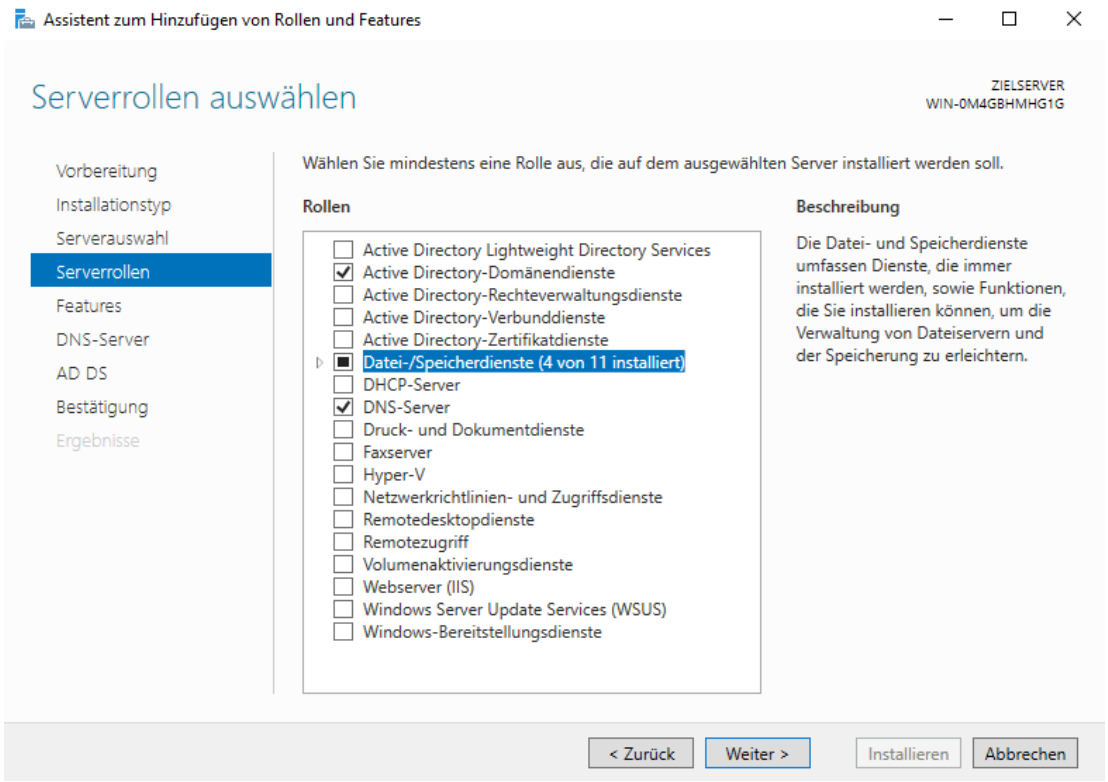

Abbildung 6: Auswahl der Serverrollen

Quelle: eigene Abbildung

Um die Windows Server VM als Domänencontroller und zugleich als DNS-Server nutzen zu können, muss der Server aufgestuft werden. Dies ist im Server-Manager sehr einfach möglich. Der erste Schritt, um den Server aufzuwerten, ist die Erstellung einer neuen Gesamtstruktur einer Domäne. Dazu wird zuerst ein Name für die Stammdomäne benötigt. Die einzigen Kriterien, die bei der Wahl des Domänennamens beachtet werden müssen, sind in Abschnitt 2.3 beschrieben. Bei der Wahl des Forest functional level und des Domain functional level sollten nur Änderungen vorgenommen, wenn ältere Server, als der Domänencontroller, in der Baumstruktur beziehungsweise Domäne vorhanden sind, also beispielsweise Windows Server 2008. Falls ältere Serverversionen eingesetzt werden, muss dies angegeben werden, da diese Versionen ältere Sicherheitskonfigurationen benutzen und die neueren Versionen möglicherweise nicht verstehen [56]. Des Weiteren muss dem Verzeichnisdienst ein Passwort vergeben werden. Dabei handelt es sich um ein Passwort für den Directory Services Restore Mode (DSRM), also dem Wiederherstellungsmodus des Active Directory, falls es zu einer Notfallwartung kommen sollte [57]. Im Anschluss müssen der NetBIOS Name, sowie die Speicherorte für die AD DS-Datenbank, für die Protokolldateien und für die .SYSVOL Datei definiert werden. Die standardmäßigen Eingaben können belassen werden und die Aufstufung ist nach einer erfolgreichen Voraussetzungsüberprüfung installierbar. Hierbei ist zu beachten, dass die Aufstufung zum Domänencontroller nur

durch das Administratorkonto durchgeführt werden kann. Das Hinzufügen der weiteren VMs zum Active Directory wird in den entsprechenden Unterpunkten beschrieben.

3.3.2 Exchange Server VM

Exchange Server 2019 muss auf einem Windows Server 2019 Betriebssystem installiert werden. Wie auch bei der Domänencontroller VM muss die Exchange Server VM einen PC-Namen und eine feste IP-Adresse zugewiesen bekommen. Die IP-Adresse darf sich nur im letzten Oktett zu der IP-Adresse des Domänencontrollers unterscheiden. Die IP-Adresse des DNS Servers muss wieder auf den Domänencontroller weisen. Damit die VM der Domäne beitreten kann, muss bei der Änderung des Computernamens auch die Domänenadresse angegeben werden. Nach einem Neustart der VM ist sie Mitglied der erstellten Domäne. Dies kann auch im Domänencontroller überprüft werden, indem in den AD DS das Fenster „Active Directory-Benutzer und -Computer“ geöffnet wird. Im Unterordner „Computers“ sind alle VMs zu sehen, die im Active Directory eingebunden sind. In diesem Fenster müssen dem Exchange Server VM Mitgliedschaften für die Gruppen „Organisations-Admins“, „Schema-Admins“ und „Organisation“ zugeteilt werden. Diese Gruppenzuweisung im Active Directory gibt der Exchange Server VM die erforderlichen Rechte, die zur Installation des Exchange Servers benötigt werden. Das Nutzerkonto, welches den Exchange Server verwalten soll, existiert noch nicht und muss vom Domänencontroller erstellt werden. Im Unterordner „Users“ im Fenster „Active Directory-Benutzer und -Computer“ muss dafür ein neuer Nutzer erstellt werden. Anschließend müssen diesem Nutzer die Rollen „Domänen-Admins“ und „Exchange Servers“ zugewiesen werden. Nach einer Neuanmeldung in der Exchange Server VM kann sich mit dem Nutzernamen „Domänenname\Exchange Admin Name“ angemeldet werden.

Damit Exchange Server installiert werden kann, wird zunächst Visual C++ 2013 benötigt. Außerdem muss .NET Framework 4.8 oder höher installiert werden. Diese Software ist kostenlos erhältlich und kann beispielsweise über einen USB-Stick auf der VM installiert werden. Des Weiteren wird Unified Communications Managed API 4.0 (UCMA 4) benötigt, was in der Exchange ISO mit inbegriffen ist. Diese ISO Datei muss über Workstation Pro in das CD/DVD Laufwerk eingebunden werden oder von einem für ISO-Dateien formatierten USB-Stick auf die VM kopiert werden. Bevor die Installation von Exchange beginnt, muss das Active Directory für die Installation vorbereitet werden. Dafür muss die Windows-Powershell als Administrator geöffnet werden. Folgende Befehle sind auszuführen: [58, 59]

Install-WindowsFeature RSAT-ADDS
Die Remote Server Administration Tools (RSAT) für Active Directory Domänendienste müssen installiert sein, um Exchange erfolgreich installieren zu können. [58, 59]

.\Setup.exe /IAcceptExchangeServerLicenseTerms /PrepareSchema
Mit diesem Befehl wird das Active Directory Schema für Exchange Server erweitert. [58, 59]

.\Setup.exe /IAcceptExchangeServerLicenseTerms /PrepareAD /OrganizationName: "Mail-Laborumgebung"
Dieser Befehl bereitet das Active Directory vor. Mit der Neuinstallation von Exchange Server wird eine neue Exchange-Organisation gegründet, der ein Name zugewiesen muss. In diesem Beispiel heißt die Exchange Organisation „Mail-Laborumgebung". [58, 59]

Nachdem die Einführung und die Lizenzbedingungen akzeptiert wurden, muss mit der Konfiguration fortgefahren werden. Es muss die Postfachrolle sowie die erforderlichen Server-Rollen und -Features installiert werden. Weiterhin kann entschieden werden, ob der integrierte Schutz vor Schadsoftware aktiviert werden soll. Dieser sollte zunächst aktiviert bleiben. Nachdem die Bereitschaftsüberprüfung erfolgreich ist, wird Exchange Server installiert. [60]

Die Konfiguration des Exchange Servers wird über das Exchange Admin Center (EAC) vorgenommen welches in Abbildung 7 zu sehen ist. EAC ist eine Internetbrowser-basierte Verwaltungskonsole. Zunächst kann sich nur über den Administrator im EAC angemeldet werden. Da der zusätzliche Exchange Administrator, der den Mail Server verwalten soll, noch keine Rechte dafür hat, müssen unter dem Reiter „Berechtigungen" die Administratorrollen angepasst werden. Da der Exchange Admin sich um alle Dienste kümmern soll, die mit dem Mail Server zu tun haben, sollten alle Administratorrollen dem Exchange Admin Nutzer zugewiesen werden. Im Anschluss sollte in den Einstellungen der Lizenzschlüssel eingegeben werden, um die Installation zu validieren. In dem Unterpunkt „Akzeptierte Domänen" im Reiter „Nachrichtenfluss" kann die Domäne der Laborumgebung hinzugefügt werden. Unter „E-Mail-Adressrichtlinie" muss definiert werden, wie die E-Mail-Adressen der Nutzer aufgebaut sind. Beispielsweise können mit dem Alias, welcher den Nutzernamen entsprechen, die E-Mail-Adressrichtlinie „Alias@Domainname" sein. Eine weitere nützliche Maßnahme ist es, die Exchange Datenbank umzubenennen und ihren Speicherort festzulegen. Dies kann unter „Server" im Reiter „Datenbanken" vorgenommen werden. [58, 61]

Um Fehlermeldungen zu vermeiden, die Arbeit mit dem Exchange Server zu erleichtern und um eine zuverlässige Verbindung beim E-Mail Verkehr zu gewährleisten, muss ein digitales Zertifikat für die Kommunikation erstellt werden. Digitale Zertifikate dienen dazu, „um die Identität eines Benutzers oder eines Computers zu überprüfen“, damit eine verschlüsselte und vertrauenswürdige Verbindung zwischen zwei Kommunikationspartnern entstehen kann [62]. Es gibt mehrere Möglichkeiten, ein Zertifikat zu erstellen. Zum einen kann ein Zertifikat intern erstellt und selbst signiert werden. Dies bringt einen hohen Administrationsaufwand beim Hinzufügen des Zertifikats mit sich. Wenn die Laborumgebung mit dem Firmennetzwerk der T-Systems MMS verbunden ist, könnte auch beispielsweise mit den Active Directory Zertifikatdiensten in der Firma ein Zertifikat ausgestellt werden. Außerdem können digitale Zertifikate auch durch Drittanbieter erstellt und erworben werden. Inwiefern ein digitales Zertifikat erstellt werden muss, wird in dieser Arbeit nicht näher behandelt, da dafür ein höherer Administrationsaufwand vonnöten ist und davon abhängt, ob die Laborumgebung in das Firmennetzwerk eingebunden wird. [62]

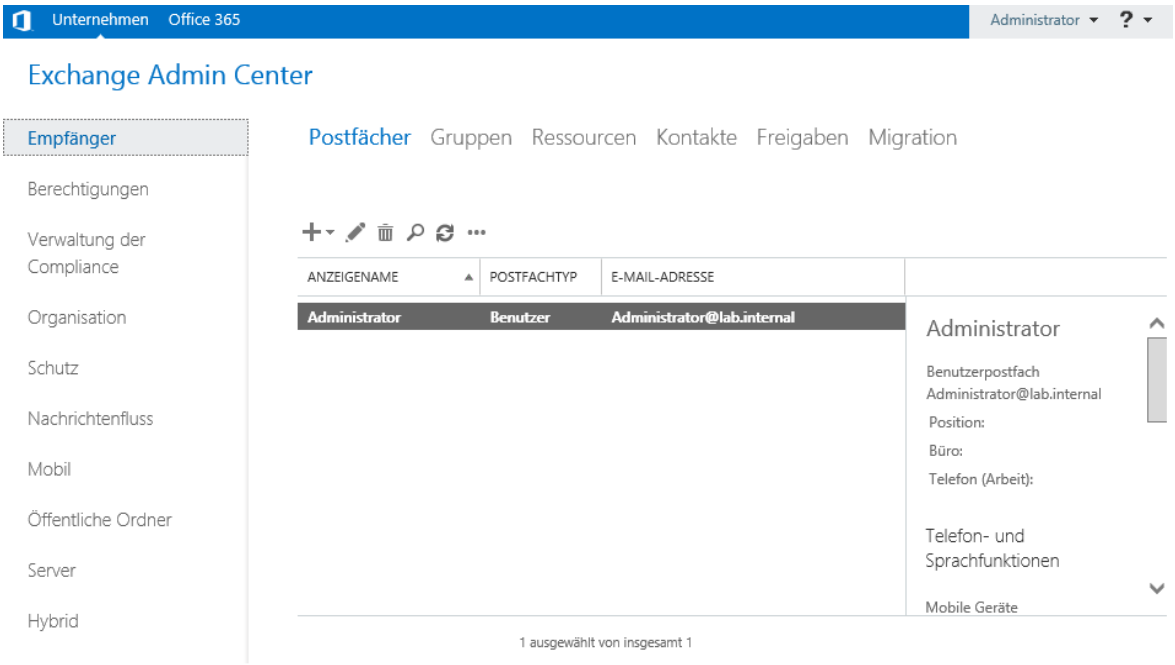

Abbildung 7: Exchange 2019 Admin Center (EAC) nach einer Neuinstallation

Quelle: eigene Abbildung

Um die E-Mail Kommunikation zwischen den Mitgliedern des Netzwerks zu ermöglichen, wird ein Programm zum E-Mail Austausch benötigt. Dafür wird Microsoft Outlook auf allen Netzwerkteilnehmern installiert und eingerichtet. Sind die Konten im Active Directory und im Exchange Server korrekt konfiguriert, so können beim Starten von Outlook die jeweiligen Konten der Nutzer hinzugefügt werden.

Außerdem muss die Konfiguration der virtuellen Verzeichnisse durchgeführt werden. Virtuelle Verzeichnisse werden von den Internet Information Services (IIS) genutzt, um den Nutzern Zugriff auf Web-Anwendungen zu erlauben. Es existieren zahlreiche virtuelle Verzeichnisse, zum Beispiel für Autodiscover, Outlook Web App und Active Sync. In der Konfiguration müssen die korrekten URLs über die Exchange Management Shell konfiguriert werden. Außerdem können Einstellungen bezüglich der Sicherheit, Authentifizierung und Berichterstellung vorgenommen werden. Diese Maßnahme wird in dieser Arbeit nicht näher behandelt, da dafür eine nutzbare Laborumgebung benötigt wird. [61, 63]

3.3.3 Windows Klienten

Die beiden Windows Klienten VMs werden mit dem Betriebssystem Windows 10 arbeiten. Die ersten Schritte nach der Installation der VMs sind wieder die Zuweisung der Computernamen und die Vergabe von IP-Adressen. Außerdem müssen die VMs der Active Directory Domäne hinzugefügt werden. Damit sind die VMs automatisch im Active Directory eingebunden. Im Domänencontroller müssen die beiden Nutzer Accounts erstellt werden. In der „Active Directory-Benutzer und -Computer“ Übersicht müssen dafür im Ordner „Users“ zwei neue Accounts erstellt werden. Es werden nur ein vollständiger Name und ein Benutzeranmeldename benötigt. Weiterhin müssen die Klienten in den Exchange Server eingebunden werden. Dazu müssen im EAC in der Exchange Server VM neue Exchange-Postfächer erstellt werden, welche den Active Directory-Konten zugeordnet werden. Über das Active Directory-Konto kann der Nutzer E-Mails verschicken und empfangen. Der Vorgang der Erstellung eines Postfaches für ein schon existierendes Active Directory-Konto wird Postfachaktivierung genannt [64]. Unter dem Reiter „Empfänger“ im EAC können neue Benutzerpostfächer angelegt werden.

3.4 Snapshots

Snapshot Abbilder der VMs zu erstellen hat mehrere Vorteile. Die offensichtlichste Anwendung der Snapshot Funktion ist wahrscheinlich bei einer Kompromittierung des Systems durch das Ausführen von Malware. Das Ausführen von Malware kann das Zielsystem – in dem Falle die VMs – komplett unbrauchbar machen, wo kaum andere Maßnahmen helfen, als die VMs auf einen unversehrten Zeitpunkt zurückzusetzen. Weiterhin kann die Snapshot Funktion genutzt werden, um bestimmte Abläufe bei der Malwareanalyse mehrfach auszuführen. Beispielsweise kann eine Maßnahme zur Malwareanalyse ausgeführt werden und Änderungen am Dateisystem und Reaktionen der eingeschleusten Malware beobachtet sowie dokumentiert werden. Anschließend müssen die VMs auf einen zuvor erstellten Snapshot zurückgesetzt werden. Dann kann genau dieselbe Maßnahme erneut durchgeführt werden, ohne Änderung jeglicher Parameter. Nun müssen die Beobachtungen verglichen werden, wodurch das Verhalten der Malware auf Einheitlichkeit geprüft werden kann. Durch die Snapshot Funktion kann dies beliebig oft wiederholt werden, um statistisch aussagekräftige Antworten zu erhalten. Zu beachten ist, dass die VMs in einem Active Directory miteinander verknüpft sind und dadurch Probleme der Synchronisation der VMs entstehen können. Die Active Directory Datenbank wird durch Änderungen und Handlungen der anderen VMs überschrieben. Aus diesem Grund müssen auf allen VMs gleichzeitig ein Snapshot erstellt werden und ebenso muss das Zurückkehren auf einen erstellten Snapshot bei allem VMs in der Laborumgebung gleichzeitig durchgeführt werden. [11]

Das Arbeiten mit Snapshots in einem Active Directory ist meist nicht empfehlenswert. Da es sich bei der Laborumgebung nur um eine minimalisierte Darstellung mit nur einem Domänencontroller handelt, sollte diese Funktion dennoch funktionieren. Größere Produktivumgebungen haben sehr oft mehr als einen Domänencontroller, welche sich gegenseitig synchronisieren. Bei diesem Szenario würde die Snapshot Technologie nicht gut funktionieren. Ähnlich verhält es sich bei Exchange Server. Laut Microsoft werden Momentaufnahmen virtueller Computer für Exchange VMs nicht unterstützt. Ihre Verwendung könne „zu nicht beabsichtigten und unerwarteten Folgen für eine Serveranwendung führen, die Zustandsdaten verwaltet“ [65]. Dabei wird jedoch von Produktivumgebungen mit Exchange Services ausgegangen, bei denen ein Mailserver hochverfügbar sein muss und nicht ausgeschalten wird. Wenn Snapshots bei abgeschalteten VMs erstellt werden, ist es wahrscheinlicher, dass keine Synchronisationsfehler auftreten. Ob die gleichzeitige Erstellung von Snapshots und das gleichzeitige Zurücksetzen der VMs in der Praxis reibungslos funktioniert, kann in dieser Bachelorarbeit nicht bewiesen werden. Dafür muss eine konfigurierte Laborumgebung aufgebaut sein. Das Testen mit Snapshots – vor allem in Zusammenhang

mit Domänencontroller und Exchange Server – muss dementsprechend in einem späteren Zeitpunkt des Gesamtprojektes durchgeführt werden.

Eine Alternative zu den Snapshots ist es, ein Backup der Laborumgebung zu erstellen. Es müsste die virtuelle Laborumgebung aufgebaut werden, sodass sie bereit für die Nutzung ist. Anschließend können die VMs geklont und die Referenz-VMs geschützt abgespeichert werden. An diesen Referenz-VMs dürfen dann keine Änderungen mehr vorgenommen werden. [66]

4 Vorbereitung zur Malwareanalyse

Dieses Kapitel umfasst die Vorbereitung der Laborumgebung, um computerforensische Artefakte finden und analysieren zu können. Zunächst wird ein besseres Grundverständnis zur Malwareanalyse und zur forensischen Arbeit vermittelt. Im Anschluss werden Werkzeuge vorgestellt, welche essenziell für die Malwareanalyse sind. Dies wird in Werkzeuge für die statische Analyse und Werkzeuge für die dynamische Analyse unterteilt.

4.1 Grundverständnis

Bevor sich mit der grundlegenden Thematik auseinandergesetzt werden kann, muss das Grundverständnis zum Arbeiten mit Malware vermittelt werden. Wenn eine potenziell schädliche Software untersucht werden soll, ist grundsätzlich ungewiss, wie gefährlich diese Software sein kann. Sehr oft ist Malware, welche beispielsweise ein Unternehmen angreift, nur wenige Stunden alt. Es entstehen tagtäglich neue, unbekannte Versionen von Malware, welche folglich selbst in großen Malware-Datenbanken nicht erfasst sind. Die Angreifer modifizieren meistens schon existierende Malwarearten, um noch versteckter agieren zu können und um nicht nachverfolgbar zu sein. Aufgrund dieser Verhaltensweise wurde der Begriff Malware Familien geprägt [67]. Die verschiedenen Malware Varianten einer Malware Familie weisen gleiche Attribute auf, wodurch auf neue Ableger von schon erforschter Malware geschlossen werden kann. Die Malware wird so konstruiert, um zum einen mehr Schaden am Zielsystem anzurichten und um sich schnellstmöglich zu verbreiten. Zum anderen werden auch Maßnahmen entwickelt und optimiert, um nicht entdeckt zu werden beziehungsweise nicht beseitigt werden zu können. Aus diesem Grund ist bei der Malwareanalyse ein hohes Maß an Vorsicht und Respekt gegenüber der Malware geboten. Malware sollte nie außerhalb einer geeigneten abgeschlossenen Umgebung untersucht werden. Selbst die statische Analyse sollte nicht im eigenen System geschehen, wenn ungewiss ist, um welche Art von Malware es sich handelt. Bei der Malwareanalyse ist davon auszugehen, dass Angreifer ihre Malware aus dem Grund verschleiern, um nicht von IT-Forensikern entdeckt zu werden. Es werden also zahlreiche Methoden von Angreifern genutzt, um den Malwareanalysten die Arbeit zu erschweren und zu verlangsamen. Absichtlich werden falsche Hinweise und fingierte Spuren im Code der Malware hinterlassen, um die Analysten auf falsche Fährten zu führen. Des Weiteren können manche Arten von Malware inaktiv bleiben, wenn sie merken, dass sie in virtuellen Maschinen ausgeführt werden.

Ein IT-Forensiker muss hartnäckig bleiben und davon ausgehen, dass die Malwareanalyse nicht bei dem ersten Versuch gelingt. Virtualisierung gewinnt hingegen in Produktivumgebung mehr und mehr an Bedeutung, beispielsweise werden ganze Domänen mithilfe von Hypervisoren wie VMware ESXi virtualisiert, wie in Punkt 3.2.1 beschrieben ist. Somit wird es für Malware schwieriger, eine Laborumgebung von einer Produktivumgebung zu unterscheiden. Wie die Entwicklung der Technologien voranschreitet, so entwickeln sich auch neue Angriffsvektoren und Methoden von Malware, sowie auch Maßnahmen, diese neuen Angriffsvektoren zu erkennen und unschädlich zu machen.

Wie auch in der naturwissenschaftlichen Forensik geht es in der IT-Forensik um das Sammeln von so vielen Spuren wie möglich und das Sammeln von kleinen Stücken an Informationen beziehungsweise forensisch relevanten Artefakten. Es muss Wissen kombiniert und Hypothesen aufgestellt werden. Oft muss von potenziell falschen Theorien ausgegangen werden, um Fortschritte in der Untersuchung zu erzielen [32]. Die Arbeitserfahrung eines Malwareanalysten und IT-Forensikers ist sehr wichtig für das Erkennen von Anomalien und Hinweisen, sie kann sich jedoch auch als negativ entpuppen. Umso mehr Arten von Malware bekannt sind, desto besser können Schlüsse gezogen und Hypothesen aufgestellt werden. Doch es muss stets an einen neuen Fall mit absoluter Objektivität herangegangen werden. Abgeschlossene Fälle, die ein ähnliches Spurenbild aufzeigen, können zwar zum Vergleich herangezogen, aber es dürfen auf dieser Grundlage keine Fälle bewertet werden. Es ist davon auszugehen, dass jede Malware einzigartig ist. Ein Großteil der Arbeit eines Malwareanalysten besteht darin, nach Auffälligkeiten und Anomalien in potenziell schädlichen Dateien zu suchen. Dabei wirkt sich die Arbeitserfahrung durch ein geschultes Auge positiv aus.

4.2 Statische Analyse

Die Statische Analyse sollte stets vor der dynamischen Analyse durchgeführt werden. Denn es ist möglich, genügend Informationen über die Datei zu gewinnen, ohne sie ausführen zu müssen. Der Quellcode des schädlichen Programmes kann zum Beispiel bestimmte Zeichenketten, oder Strings, beinhalten, die Informationen über die Verschlüsselung oder sogar auf den Angreifer preisgeben können. Zusätzlich können aus dem Code Hashwerte generiert werden, welche mit bekannter Malware abgeglichen werden können.

4.2.1 pestudio

pestudio wurde von Marc Ochsenmeier entwickelt und ist ein frei erhältliches Programm, das allgemeine, nützliche Informationen über Portable Executable (PE)-Dateien liefert, ohne sie auszuführen. Das PE-Dateiformat bezeichnet ausführbare Binärdateien in Windows, worunter unter anderen die Dateiendungen .exe, .dll und .sys zu zählen sind [68]. Um sich einen anfänglichen Überblick über die zu untersuchende Datei zu verschaffen, ist pestudio sehr aufschlussreich. Das Programm wurde zur statischen Malwareanalyse entwickelt. Das ist gut daran erkennbar, dass keine Installation der Software vonnöten ist. Dadurch wird kein Abdruck im Dateisystem in der Windows-Registry oder in Form von weiteren Dateien hinterlassen. In Abbildung 8 ist das Startfenster von pestudio in der Version 9.09 dargestellt, mit vmware.exe als untersuchte Beispieldatei. Die Software wird neben der kostenfreien Version auch als kostenpflichtige Version angeboten, welche mehr Features bietet. [69]

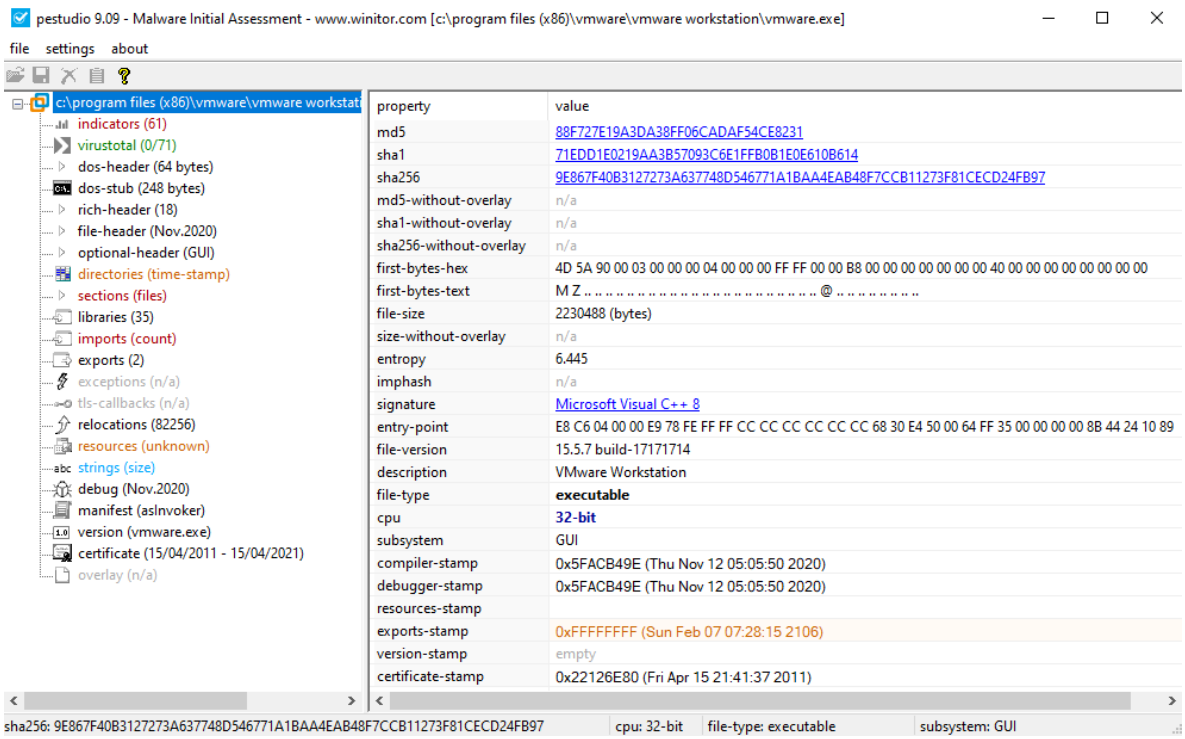

Abbildung 8: pestudio 9.09 - Übersicht zur Analyse von vmware.exe

Quelle: eigene Abbildung

pestudio bietet sehr viele Eigenschaften und Informationen über die untersuchte Datei. Darunter gehört die Auflistung jeglicher Strings in der Datei, also Zeichenketten im Code der PE-Datei. In den Strings können erste Hinweise auf Funktionsnamen, Befehle, Domänen und weitere Dateien, welche ausgeführt werden sollen, zu finden sein. Selbst, wenn auffällig viele unlesbare Strings erkannt wurden, kann dies ein nützlicher Hinweis sein, dass die Datei gepackt sein könnte. Malware im komprimierten, gepackten Format ist eine gängige Methode von Angreifern, ihre Dateien nicht von Antivirus Software entdecken zu lassen. Der Entropiewert in pestudio gibt einen Hinweis darauf, ob die Datei gepackt wurde [70]. Er kann Werte zwischen 0 und 8 annehmen, wobei 0 den geringsten Entropiewert angibt und 8 den höchsten Wert an Entropie [70]. Der Entropiewert von 6.445 in Abbildung 8 lässt demnach vermuten, dass vmware.exe auch gepackt sein könnte. Wenn eine PE-Datei gepackt ist, hilft meist das kostenfreie Kommandozeilen Tool UPX, um sie zu entpacken [71]. Des Weiteren kann pestudio verschiedene Hashwerte der Datei erstellen, um sie in Malwaredatenbanken zu suchen. Die am meisten genutzten Hashwerte sind der MD5-Hash oder der SHA256-Hash. Dateien können durch ihren Hashwert eindeutig identifiziert werden, jeder Hashwert muss einzigartig sein. Das bedeutet, wenn eine Malware Datei vorher schon identifiziert wurde, ist die Wahrscheinlichkeit hoch, dass sie in einer Datenbank für Malware aufgenommen wurde. Die bekannteste Datenbank ist VirusTotal [72]. In VirusTotal kann

nach URLs, IP-Adressen, Domänennamen und Datei-Hashes gesucht werden. Weitere Beispiele für Datenbanken zur Malwareanalyse sind Totalhash und URLVoid, welche auf Hashwerte und verdächtige URLs spezialisiert sind [73, 74]. Die Methode, in Datenbanken nach der entsprechenden Datei zu suchen, wird auch Open Source Intelligence gathering genannt. Weiterhin werden von pestudio die Windows Bibliotheken angezeigt, auf die die untersuchte Datei zugreifen will. Die Bibliotheken haben die Dateiendung .dll, was für Dynamic Link Library steht, und bestehen aus Daten, auf die ausführbare Dateien zugreifen können [75, 70]. Die Befehle, welche Funktionen aus den Bibliotheken laden, werden Imports genannt. Diese Schnittstelle zwischen .dll Dateien und der zu untersuchenden Datei kann von pestudio erfasst und angezeigt werden. Eine weitere Information, die pestudio liefert, ist der Zeitstempel, zu welcher Zeit die Datei kompiliert wurde. Pestudio bietet einen umfassenden ersten Einblick in die zu untersuchende Datei, auf dem die weitere Malwareanalyse gestützt werden kann. [32]

4.2.2 PEview

Mit PEview kann der Code einer PE-Datei strukturiert dargestellt werden. Das Programm wurde von Wayne J. Radburn veröffentlicht [76]. Es ist nützlich, wenn der Inhalt der einzelnen Sektoren der Datei und vor allem der PE Header genauer betrachtet werden soll. Der PE Header steht am Anfang einer PE-Datei und beinhaltet Grundinformationen über die Datei. Wenn die Malware durch ein unbekanntes Kompressionsverfahren gepackt wurde, kann mithilfe von PEview die Art der Kompression ermittelt werden [71]. Weitere wichtige Informationen werden von Programmen wie pestudio übersichtlicher zusammengefasst.

4.2.3 IDA Pro

IDA Pro ist ein Programm von Hex-Rays, welches als Disassembler und Debugger genutzt werden kann. Diese Art von Software wird unter den Werkzeugen für Reverse Engineering gezählt. Reverse Engineering bedeutet so viel wie rekonstruieren, es werden aus einem fertigen Programm die einzelnen Komponenten extrahiert und analysiert [77]. Ein Disassembler ist in der Lage, den Maschinencode eines Programms in der Assembler-Sprache darzustellen. Dabei werden alle binären Prozessorinstruktionen für den Menschen lesbar. So kann der Programmcode auf der tiefsten Ebene analysiert werden. Da die Assembler-Sprache dennoch sehr schwer zu lesen ist, bietet IDA Pro verschiedene Visualisierungsmöglichkeiten an, um sich einen besseren Überblick über die Ausführung eines Programms verschaffen zu können. Ziel ist es, den ursprünglichen Quellcode so originalgetreu wie mög-

lich abzubilden. „95% aller Viren kommen sofort nach dem Starten der Datei zur Ausführung“ [71]. Aus diesem Grund sollte vor allem der Anfang des Programmcodes untersucht werden. Als Debugger kann IDA Pro den Programmcode Schritt für Schritt ausführen. Dadurch können Veränderungen am System kontrolliert beobachtet und analysiert werden. Durch diese Technologie kann die Verschleierung des Codes umgangen werden, da der Code nicht direkt analysiert werden muss. Des Weiteren ist IDA Pro mit Plugins erweiterbar, mit anderen Analysetools. Zusätzlich bietet IDA Pro eine eigene Entwicklungsumgebung, eigene Programme und Funktionen zu schreiben, die beispielsweise Analyseaufgaben automatisieren. Der Nachteil von IDA Pro ist eindeutig der Preis. Eine Windows Lizenz kostet laut dem Hersteller 1879 US Dollar [78]. In Abbildung 9 ist die kostenfreie alternative Version IDA Free zu sehen, welche jedoch nicht zur kommerziellen Nutzung gestattet ist und weitaus weniger erweiterte Funktionen bietet, bezüglich Plugins und Programmierbarkeit [79]. In der Abbildung ist links die Visualisierung des Programmcodes als Graph zu sehen und rechts der Programmcode in Hexadezimal Schreibweise, sowie in ASCII-Text übersetzt. Der obere Streifen stellt die Art des Codeinhalts mithilfe der Legende farbig dar. Zusätzlich können unter anderem Imports und Exports angezeigt werden. Eine Alternative zum kostenintensiven IDA Pro bietet die Software Ghidra. [80]

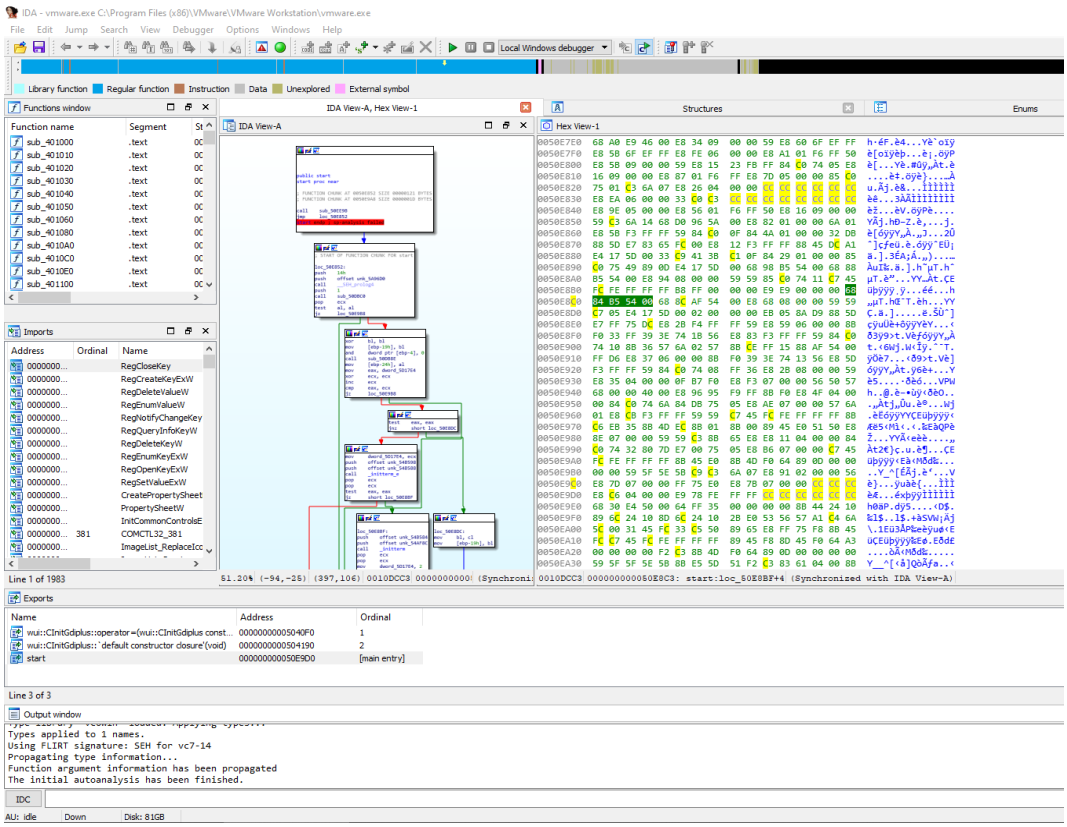

Abbildung 9: IDA Free 7.0 - Analyse von vmware.exe

Quelle: eigene Abbildung

4.2.4 Ghidra

Ghidra ist eine kostenfreie Software Suite, die von der amerikanischen National Security Agency (NSA) entwickelt wurde [70]. Um Ghidra nutzen zu können, muss Java 11 64-bit Runtime und Development Kit (JDK) installiert sein [81]. Wie auch IDA Pro, ist diese Software zum Reverse Engineering geeignet und stellt eine Sammlung von Software zur Analyse von kompiliertem Code zur Verfügung. Ghidra kann den dekompilierten Assembler Code direkt in C Code umwandeln. Dieser Code gleicht höchstwahrscheinlich nicht dem Originalcode, aber versucht diesem so sehr wie möglich zu ähneln [82].

Ob dieses Programm oder doch IDA Pro für die Laborumgebung genutzt wird, hängt zum einen davon ab, ob die T-Systems MMS über eine IDA Pro Lizenz verfügt. Außerdem sollte sich auch an der Expertise der Mitarbeiter orientiert werden. Wenn in der Firma beispielsweise mehr mit Ghidra gearbeitet wird, dann sollte diese Software auch installiert werden.

4.3 Dynamische Analyse

Die Werkzeuge für die Live Analyse stellen den deutlich wichtigeren Teil der Laborumgebung dar. Dabei spielen die vorher beschriebenen Active Directory-, Exchange- und Netzwerkkomponenten eine entscheidende Rolle. Es soll beobachtet werden, wie die zu untersuchende Datei mit dem Netzwerk interagiert und wie sie sich verbreitet. Zum einen muss beobachtet werden, ob und wie die einzelnen Domänenmitglieder auf die Ausführung der Malware reagieren. Welche Versuche zum Kommunikationsaufbau mit anderen IP-Adressen und Domänen gesendet werden, stellt ebenfalls einen wichtigen Teil der Dynamischen Analyse dar. Ein weiterer wichtiger Bestandteil der dynamischen Analyse ist das Mitschneiden sämtlicher Änderungen am Dateisystem, insbesondere an der Windows-Registry. Im Arbeitsspeicher befinden sich oft flüchtige Informationen, welche essenziell für die Malwareanalyse sein können. Deshalb muss die Laborumgebung auch über ein Werkzeug zur Arbeitsspeichersicherung verfügen. Durch die in der statischen Analyse gewonnenen Informationen können die Werkzeuge zur dynamischen Analyse effizienter genutzt werden, da gezielt nach schon gefundenen Strings, Funktionen und Imports gesucht werden kann. Nicht jedes Programm zur Malwareanalyse sollte auf jeder VM installiert werden, da Malware in der Lage sein kann, die Aktivität solcher Programme zu identifizieren.

4.3.1 Microsoft Sysinternals Suite

Diese Sammlung von zahlreichen „Dienstprogrammen zur Fehlerbehebung“ wurde von Mark Russinovich entwickelt und ist kostenfrei zum Download verfügbar [83]. Einige der Programme, die in Sysinternals enthalten sind, sind sehr gut zum Monitoring und Untersuchen von Prozessen geeignet.

4.3.1.1 Autoruns

Dieses Programm gibt dem Nutzer ausführliche Informationen darüber, welche Programme so konfiguriert sind, dass sie beim Systemstart oder beim Login eines Nutzers gestartet werden. Diese Funktion ist computerforensisch relevant, da Malware so konfiguriert sein kann, dass sie versucht, nach einem Neustart des Computers direkt ausgeführt zu werden. Dieses Vorgehen wird Persistancy mechanism genannt, was ins Deutsche als Hartnäckigkeits- oder Beständigkeitsmechanismus übersetzt werden kann. Autoruns kann außerdem über das Kommandozeilen-Tool Autorunsc genutzt werden. Dabei werden die Ergebnisse als CSV Dateien abgespeichert [84]. Da es sehr viele Prozesse gibt, die als Autostart konfiguriert sind, werden sie in Autoruns mithilfe von Registerkarten unterteilt und übersichtlich eingeordnet. Die Prozesse in Autoruns haben immer einen zugehörigen Eintrag in der Windows-Registry oder im Dateisystem, in denen die Autostart-Konfiguration gespeichert ist. Diese Informationen sind in Autoruns einsehbar. Mit einem direkten Link zum Eintrag im Registry Editor können schnell weitere Untersuchungen durchgeführt werden. Mit verschiedenen Einfärbungen der Einträge werden weitere Informationen vermittelt. So wird der Nutzer durch einen pink eingefärbten Eintrag gewarnt, wenn ein Eintrag keine Informationen über den Herausgeber des Prozesses verfügt oder wenn die digitale Signatur nicht verifiziert werden kann. Außerdem wird ein Beitrag in Gelb angezeigt, wenn zwar ein Autostart Eintrag existiert, aber die dazugehörige Datei nicht gefunden werden kann. Eine weitere Eigenschaft zur Malwareanalyse ist die direkte Verbindung mit der VirusTotal Datenbank. Wenn ein Eintrag in der Datenbank bekannt ist, wird dies in einer zusätzlichen Spalte im Programm angezeigt. Des Weiteren können Abbilder der Anzeige von Autoruns gespeichert werden und an einem späteren Zeitpunkt mit dem aktuelleren Abbild verglichen werden. Alle Änderungen der Einträge werden dann in Grün dargestellt. So kann beispielsweise ein Abbild vor dem Ausführen einer Malware gespeichert werden und dann nach der Kompromittierung verglichen werden. Wenn beim Ausführen einer Malware ein Autostart Eintrag erstellt wird, dann wird er in Autoruns angezeigt. [85]

4.3.1.2 Process Monitor

Process Monitor, oder auch ProcMon, ist in der Lage, sämtliche Interaktionen mit dem Dateisystem in Echtzeit zu dokumentieren. Dazu zählt zum einen, welche Dateien von welchem Prozess verändert, erstellt und gelöscht werden. Des Weiteren wird angezeigt, welche Prozesse die Windows-Registry verändern und welche Dateien auf welche Art auf die Windows-Registry zugreifen. Informationen über den Netzwerkverkehr sowie über die Erstellung von neuen Prozessen und Threads ist ebenfalls einsehbar. In Abbildung 10 ist das ProcMon zu sehen. Die blau eingefärbten Buttons stellen die beschriebenen Arten von Aktivitäten dar, welche per Mausklick herausgefiltert werden können. Ähnlich wie bei Autoruns kann auch bei ProcMon bei Einträgen, die mit der Windows-Registry in Verbindung stehen direkt zum Registry Editor gesprungen werden, um sich zusätzliche Informationen über Registry Schlüssel einzuholen.

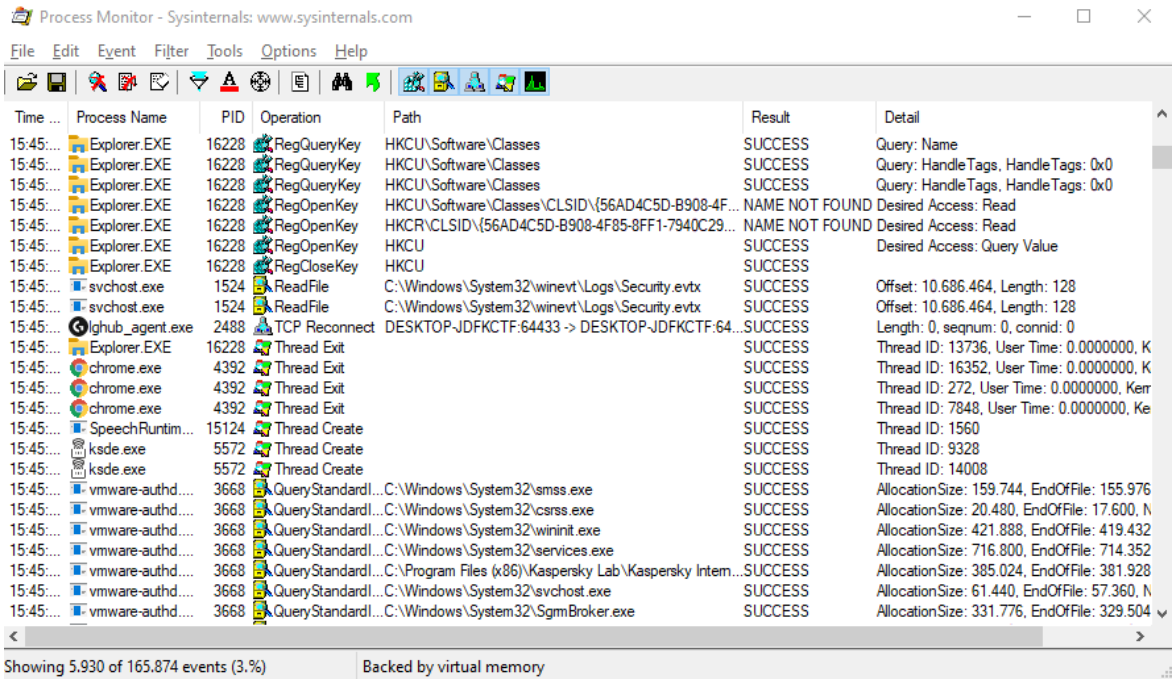

Abbildung 10: Process Monitor ohne Filter

Quelle: eigene Abbildung

Die Menge der aufgezeichneten Interaktionen in kürzester Zeit ist sehr hoch. Aus diesem Grund sollte ProcMon bei der dynamischen Analyse kurz vor der Ausführung der Malware gestartet werden. Außerdem können komplexe Filter erstellt oder importiert werden, welche lediglich die Anzeige der Ergebnisse filtert. Dies hilft vor allem, um nicht wichtige Daten, welche parallel im Hintergrund laufen, auszuschließen. Außerdem helfen Filter dabei, wenn

nach bestimmten Aktivitäten gesucht wird, worauf im vorherigen Verlauf der Analyse hingearbeitet wurde. Das Herausfiltern der irrelevanten Daten in ProcMon stellt die größte Herausforderung bei der Arbeit mit dem Programm dar. Es existieren vorgefertigte frei verfügbare Filter, welche heruntergeladen und importiert werden können. Das selbstständige Erstellen von Filtern ist dennoch zu empfehlen, da an jede Situation in der Malwareanalyse individuell herangegangen werden sollte. Ein weiteres Feature von ProcMon ist das Speichern des erzeugten Logs für die spätere Untersuchung. [86]

4.3.1.3 *Process Explorer*

Während der Nutzung von ProcMon kann Process Explorer parallel genutzt werden, um weitere Informationen über laufende Prozesse zu erlangen. Mit dieser Software kann nachvollzogen werden, welche Handles und Bibliotheken von bestimmten Prozessen geladen und geöffnet werden. Handles sind als Referenzwerte zu verstehen, die bestimmten Systemressourcen zugewiesen sind, welche von Prozessen verarbeitet werden [87]. So kann nachvollzogen werden, welcher Prozess eine .dll-Datei geladen hat und welcher Prozess momentan bestimmte Dateien nutzt. Unter den Handles gibt es den Handle-Typ names Mutant oder auch Mutex. Mutex Objekte werden genutzt, um den Zugriff zu einer geteilten Ressource zu synchronisieren, damit nicht zwei Prozesse gleichzeitig auf eine Ressource zugreifen können. In Hinsicht auf die Malwareanalyse sind Mutex Objekte sehr interessant, da Malware oft ein Mutex Objekt erstellt, um sich selbst zu signalisieren, dass das Hostsystem schon infiziert wurde. Es soll nicht erneut von derselben Malware befallen werden, da dadurch eventuell die Betriebsstabilität darunter leiden kann. Aus diesem Grund sind Mutex Handles, oder auch so genannte Infection Markers, sehr gute IOCs beziehungsweise forensische Artefakte. Die Ansicht der laufenden Prozesse in Process Explorer ist hierarchisch aufgebaut und eingefärbt, um einen besseren Überblick zu bekommen. Eine Hierarchie von Prozessen entsteht dann, wenn ein Prozess einen weiteren Prozess startet. Mithilfe von Process Explorer können ganze Prozessbäume angehalten beziehungsweise gänzlich gestoppt werden. Außerdem können detaillierte Statistiken zur Prozessorauslastung und Arbeitsspeichernutzung eingesehen werden. Auch hier wird die VirusTotal Datenbank mit einbezogen, um schnellstmöglich eine schädliche Aktivität zu erkennen. Process Explorer wird oft mit dem Task Manager von Windows verglichen, da viele Nutzungszwecke ähnlich sind. Process Explorer ist im Vergleich zum Task Manager weitaus detaillierter und geeignet, um Malwareanalyse zu betreiben. [32, 86, 88]

4.3.2 Process Hacker

Process Hacker observiert, ähnlich wie Process Explorer, laufende Prozesse. Es ist ebenfalls eine frei verfügbare Software. Das Besondere an Process Hacker ist, dass nachvollzogen werden kann, wie ein Prozess ausgeführt wird. Unter anderem wird der Speicherort angezeigt, von dem der Prozess gestartet wurde und welche Parameter dem ausgeführten Programm mitgegeben wurden. Des Weiteren können Strings während des laufenden Betriebs eines Programms extrahiert werden. Dies ist äußert nützlich, wenn dadurch flüchtige Informationen gespeichert werden können, die weder vor noch nach der Ausführung des Programms sichtbar gewesen wären. Darunter können dementsprechend auch computerforensische Artefakte sein, welche die Präsenz Malware-typischer Aktivität beweist. Wie auch Process Explorer ist Process Hacker in der Lage, Handles, inklusive Mutex Objekte, auszulesen. [32]

4.3.3 Wireshark

Wireshark ist ein Werkzeug zur umfassenden Netzwerk Protokoll Analyse. Diese Art von Programm kann auch Sniffer oder PCAP genannt werden [89]. Es ist eine kostenlose Software, welche als Community Projekt seit 1998 existiert. Das Projekt wurde initial von Gerald Combs gegründet. Die neuste Version 3.4.3 wurde am 29. Januar 2021 veröffentlicht. Wireshark ist in der Lage den Netzwerkverkehr von hunderten verschiedenen Protokollen in Echtzeit zu erfassen und graphisch darzustellen. Um Wireshark installieren zu können, wird zusätzlich Npcap oder WinPcap benötigt. Dies sind Windows Bibliotheken, die auf der Windows Bibliothek libpcap basieren. Die Namen dieser Bibliotheken stehen für Network-, Windows-, und Library Packet Capture. Sie sind erforderlich, um Datenpakete im Netzwerkverkehr überwachen, oder sniffen, zu können. WinPcap ist die veraltete, nicht mehr unterstützte Version dieser Bibliotheken, weshalb die Installation von Npcap empfohlen wird. [90, 91]

In Abbildung 11 ist Wireshark während der Aufzeichnung eines Ethernet Netzwerkverkehrs zu sehen. Im oberen Fenster sind die einzelnen empfangenen und gesendeten Datenpakete in Echtzeit angezeigt. Die Pakete sind entsprechend des Netzwerkprotokolls eingefärbt, um einen besseren Überblick über den Datenverkehr zu behalten. Die Farbeinstellungen können in den Einstellungen auch nach Belieben geändert werden. In dem mittleren Fenster werden detaillierte Informationen über das markierte Datenpaket angezeigt. Sie sind in die einzelnen Schichten sortiert, auf denen Netzwerkdaten vermittelt werden. Es werden dementsprechend auch Informationen über die physische Schicht und über die ver-

wendeten Netzwerkadapter von dem Absender und von dem Empfänger überwacht. Weiterhin werden dann Informationen angezeigt, welches Protokoll verwendet wird und welche Daten über dieses Protokoll vermittelt werden. Es werden beispielsweise die Quell- und Zielports und Quell- und Ziel-IP-Adressen und das dazugehörige Netzwerkprotokoll angezeigt. Die aktivierten Flags und Zeitstempel können ebenfalls eingesehen werden. Welche Daten eingesehen werden können, hängt von der Art des Datenpakets und dem dazugehörigen Protokoll ab. Der tatsächliche Inhalt der Datenpakete wird im unteren Teil des Programms in Hexadezimal-Code und übersetzt in besser lesbaren ASCII-Code angezeigt. [92, 93]

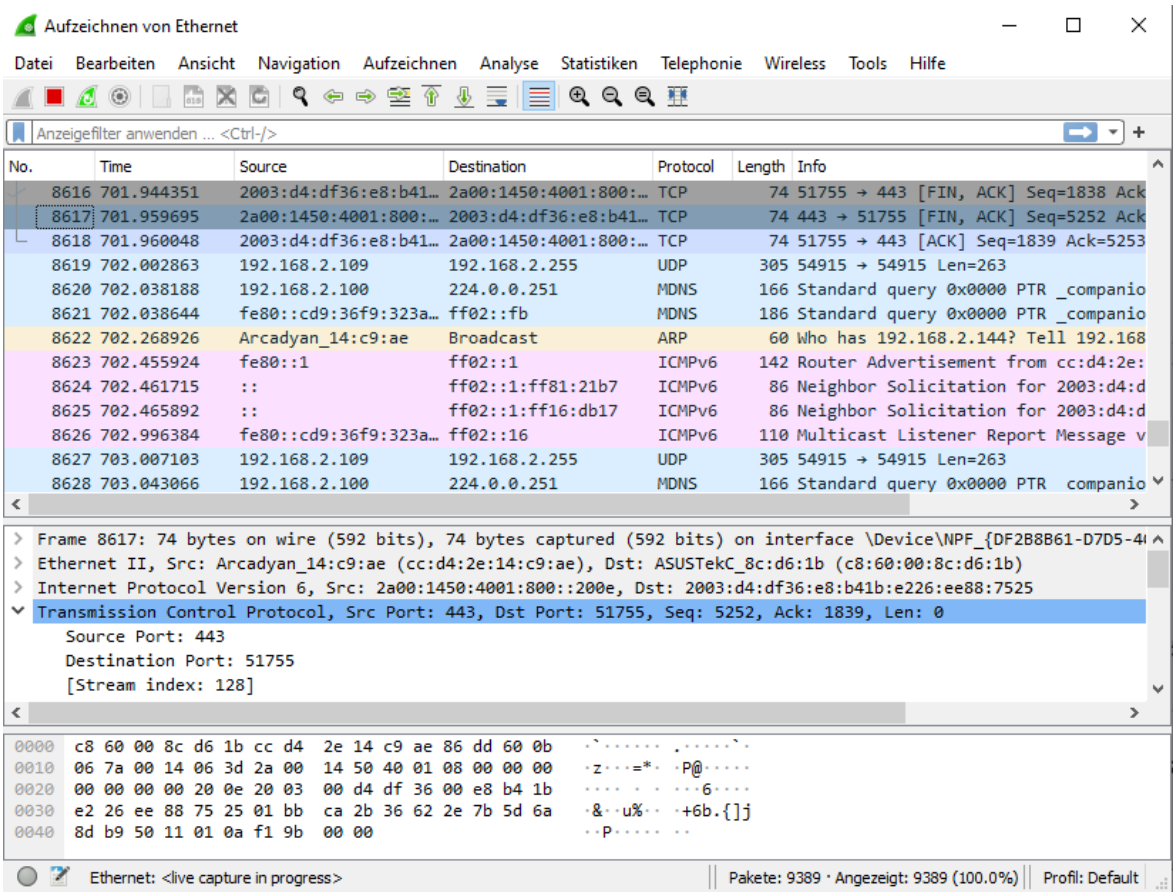

Abbildung 11: Wireshark - während der Live-Überwachung

Quelle: eigene Abbildung

Wie auch bei anderen Monitoring-Tools ist es äußerst wichtig, die unerwünschten Daten in der Anzeige herauszufiltern. Das Filtersystem von Wireshark ist sehr umfangreich. Es können vorgefertigte Filtereingaben genutzt werden oder auch eigene Filter, die mit einer komplexen Eingabesyntax zahlreiche Möglichkeiten zum Kombinieren verschiedener Filtereinstellungen bieten. Des Weiteren kann Wireshark die aufgezeichneten Daten in Exportdateien abspeichern. Denn neben der Live Analyse können auch aufgezeichnete Daten in

Wireshark geladen und analysiert werden. Beim Exportieren können ganze Aufzeichnungsprotokolle und auch einzelne Pakete und spezifizierte Objekte gespeichert werden. Die Aufzeichnungen können auch von anderen Sniffern stammen. [93]

Da in der Laborumgebung alle VMs im selben virtuellen Netzwerk sind, kann der gesamte Datenverkehr im Netzwerk von der Domänencontroller VM aus beobachtet werden. Wireshark muss nicht auf jeder VM installiert sein, da damit das Risiko steigen würde, dass die Malware die Aktivität eines Sniffers wie Wireshark erkennt. Im Zusammenhang mit der Malwareanalyse können verschiedene Netzwerkaktivitäten Hinweise auf die Aktivität von Malware geben. Beispielweise könnten unerwartete Verbindungsversuche mit fremden IP-Adressen beobachtet werden. Wenn diese Verbindungsversuche gehäuft vorkommen, ist es wahrscheinlich, dass die Malware eine Netzwerk Scan durchführt, bei dem offene Ports zur Kommunikation gesucht werden [93].

4.3.4 DumpIt

Mithilfe dieses Tools können Abbilder des Arbeitsspeichers erstellt werden. Das Werkzeug wird über die Eingabekonsole genutzt und wurde von Matthieu Suiche entwickelt. Wird das Programm ausgeführt, wird ein Abbild des Arbeitsspeichers des gesamten Systems zum Zeitpunkt der Aufnahme erstellt. Dafür muss die Konsole mit Administratorrechten geöffnet werden. Diese Dump Datei kann dann mit Tools zur Arbeitsspeicheranalyse, wie zum Beispiel mithilfe des Programms Mimikatz oder mit Python Skripts des Volatility Framework, weiter untersucht werden. Genauer gesagt können im Arbeitsspeicher sehr viele nützliche Daten gefunden werden, welche zum Zeitpunkt der Aufnahme vom System genutzt wurden. Darunter zählen zum Beispiel aktive Dienste und Prozesse, sowie offene Netzwerkverbindungen. Weiterhin können im Arbeitsspeicher dechiffrierte Passwörter und Informationen zu finden sein. Verschlüsselte Malware muss sich erst selbst entschlüsseln, wenn sie ausgeführt wird. Die entschlüsselten Daten können offen im Arbeitsspeicher liegen. Mithilfe des Arbeitsspeichers können Aussagen über die ausgeführten Aktivitäten der Malware getroffen werden. So können beispielsweise ausgeführte Skripts lesbar sein. [71, 94]

4.3.5 ProcDOT

Diese Software ist ein Werkzeug, welches die Ergebnisse verschiedener Analysewerkzeuge verbinden kann. ProcDOT dient dazu, aufgezeichnete Daten zur Malwareanalyse visuell und qualitativ aufzuwerten. Genauer gesagt ist das kostenlose Programm in der Lage, die Aufzeichnungen von Process Monitor und die Aufzeichnungen von Wireshark

oder einer ähnlichen Sniffer Anwendung zu kombinieren und darzustellen. Es werden die Korrelationen zwischen Netzwerkaktivitäten und den dafür zuständigen Prozessen erschlossen. Die Daten werden in einem Graphen visualisiert, welcher interaktiv analysiert werden kann. Ein Beispiel für einen solchen Graph ist in Abbildung 12 zu sehen. Die relevanten Prozesse und Dateien sind mit Pfeilen verbunden, welche Zugriffe aufeinander darstellen. [32, 95]

Sowohl die aufgezeichneten Daten von ProcMon, als auch von Wireshark können sehr große Ausmaße mit vielen irrelevanten Hintergrunddaten annehmen. Aus diesem Grund verfügt ProcDOT über Algorithmen, die lernen, welche Daten relevant sind und welche nicht. Darüber hinaus können eigene Filter angewendet werden. Der zeitliche Ablauf der Prozesse und Netzwerkaktivitäten kann in einem Animationsmodus nachvollzogen werden. [95]

ProcDOT selbst deckt zwar keine computerforensisch relevanten Daten auf, doch mithilfe dieses Programms können besser und schneller die Zusammenhänge verschiedener digitaler Spuren erkannt werden. Es dient also in gewisser Weise als forensisches Hilfsmittel zur Malwareanalyse. [95]

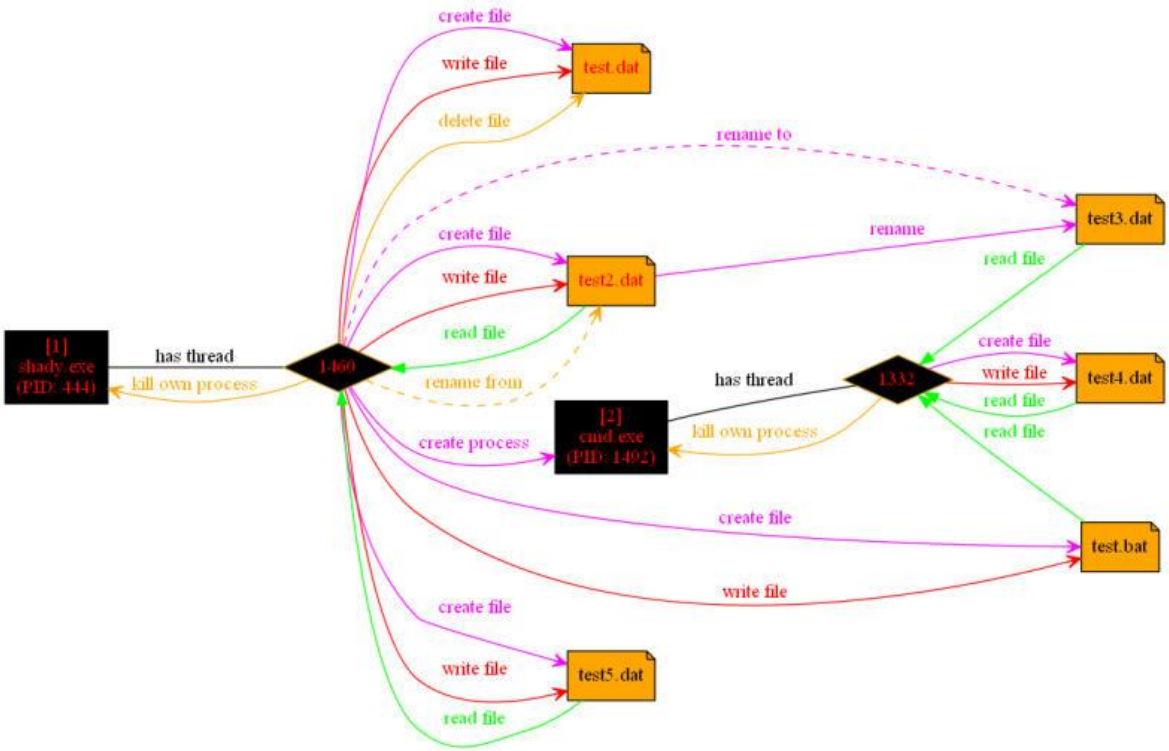

Abbildung 12: ProcDOT Beispiel eines Graphen

Quelle: [96]

5 Fazit und Ausblick

In dieser Bachelorarbeit wurde der Grundstein für das Projekt der Windows-Laborumgebung zur Malwareanalyse für die T-Systems MMS gelegt. Ziel der Arbeit war es, die Planung und das Konzept auszuarbeiten, wie die Laborumgebung aufgebaut werden muss und welche grundlegenden Komponenten sie enthalten muss. So wurde definiert, dass die Laborumgebung auf einem einzigen Computer installiert werden soll, auf dem mithilfe von virtuellen Maschinen das Modell eines Firmennetzwerks dargestellt wird. Aufgrund der komplexen Systemanforderungen der virtuellen Maschinen ist ein Plan entwickelt worden, über welche Hardware Ressourcen der Host Computer verfügen muss. Durch die Tatsache, dass die Laborumgebung zentral auf einem Computer installiert werden soll, wird an Kosten und Administrationsaufwand gespart.

Des Weiteren wurde ausdiskutiert, dass der Hypervisor VMware Workstation Pro als Schnittstelle zwischen der Hardware des Host Computers und den virtuellen Maschinen die geeignete Software für diesen Verwendungszweck ist. Die virtuellen Maschinen selbst wurden umfassend bezüglich ihrer Installation und Konfiguration erklärt. Der virtuelle Domänencontroller, auf dem das Active Directory sowie die DNS Serverrolle installiert ist, verwaltet den virtuellen Microsoft Exchange Server und die zwei virtuellen Klienten, welche über E-Mail Verkehr miteinander in einem privaten, abgeschlossenen Netzwerk kommunizieren können. Es wurde ein kompaktes, abgeschottetes Labor konzipiert, welches zentral verwaltet werden kann.

Weiterhin wurde besprochen, inwiefern die Laborumgebung mithilfe von Snapshots zurückgesetzt werden kann. Um die Laborumgebung für die forensische Arbeit vorzubereiten, wurden einige der wichtigsten Werkzeuge und Programme zur Malwareanalyse und zum Finden computerforensischer Artefakte erklärt. Die Laborumgebung wird sowohl über Werkzeuge zur Statischen Analyse als auch zur interaktiven dynamischen Analyse verfügen.

Diese Bachelorarbeit und das Gesamtprojekt vereinigen mehrere Inhalte des Studiengangs Allgemeine und Digitale Forensik in einem komplexen Modell. Sowohl die Lehren über Windows Betriebssysteme und Netzwerkadministration, als auch die Netzwerkforensik, Malwareanalyse und forensische Methoden sind Kerninhalte dieser Arbeit. Es handelt sich

hierbei um einen Anwendungsfall, bei dem die theoretischen Inhalte dieser Module in einem praktischen Projekt miteinander verbunden werden.

Der nächste Schritt, bezogen auf das Gesamtprojekt, wird das Installieren und Testen der provisorischen Laborumgebung sein. Für den praktischen Gebrauch ist dieses Modell noch nicht geeignet. Zum einen muss getestet werden, ob das Zurücksetzen der Laborumgebung durch Snapshots im Ganzen funktioniert. Außerdem muss geprüft werden, ob der Exchange Server mit der erklärten Konfiguration funktionsfähig ist. Im Rahmen dieser Arbeit wurden lediglich das Active Directory und das private Netzwerk auf Funktionalität geprüft. Das Erstellen und Testen von mehreren Snapshots und die vollständige Installation des Exchange Servers war aufgrund mangelnder Hardwareressourcen nicht möglich.

Das Konzept der Laborumgebung muss außerdem um weitere Funktionen und Komponenten erweitert werden. Zum einen muss ein steuerbarer Zugriff zum Internet konfiguriert werden. Beispielsweise könnte eine weitere VM als Router konfiguriert werden, welcher einen Internetzugang ermöglichen könnte. Diesbezüglich müssten die Funktionen des Exchange Servers erweitert werden, um E-Mails aus dem Internet zu empfangen.

Eine weitere sehr wichtige Funktion, welche in dieser Bachelorarbeit nicht besprochen wurde, ist die Sicherheit des Nutzers der Laborumgebung. Bevor die Laborumgebung zur Malwareanalyse genutzt werden kann, muss sichergestellt werden, dass sie über ein hohes Containment verfügt. Containment bedeutet auf Deutsch Eindämmung und beschreibt, wie gut die Laborumgebung von dem Hostrechner und anderen äußeren Einflüssen geschützt ist. Weiterhin zählt unter Containment die Absicherung nach außen. Wenn eine schädliche Software in der Laborumgebung ausgeführt wird, dürfen keine Auswirkungen außerhalb der Umgebung registriert werden. Dazu gehören auch Hinweise in der virtuellen Umgebung, dass es sich nicht um einen tatsächlichen Computer handelt. Dateien und Prozesse, welche beispielsweise auf die Präsenz eines Hypervisors hinweisen, können von Malware erkannt werden. Diesbezüglich muss die Laborumgebung in Zukunft vorbereitet werden.

Eine weitere Möglichkeit, die Laborumgebung zu erweitern, wäre das Implementieren von älteren Windows Versionen, wie zum Beispiel einem Windows XP Klienten. Diese Maßnahme könnte nützlich sein, um etwaige unterschiedliche Reaktionen der Betriebssysteme auf Malware nachvollziehen zu können. Wenn die Laborumgebung umfassend konfiguriert und bereit für die Nutzung ist, könnte sie auch in anderen Abteilungen der T-Systems MMS Verwendung finden.

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2020," 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2. [Zugriff am 27. 12. 2020].

[2] S. Luber und F. Karlstetter, „Was ist Virtualisierung?," Cloudcomputing Insider, 2018. [Online]. Available: https://www.cloudcomputing-insider.de/was-ist-virtualisierung-a-756279/. [Zugriff am 28. 12. 2020].

[3] S. J. Bigelow, „Paravirtualisierung vs. Virtualisierung: Die Unterschiede," 2018. [Online]. Available: https://www.computerweekly.com/de/feature/Paravirtualisierung-vs-Virtualisierung-Die-Unterschiede. [Zugriff am 14. 01. 2021].

[4] Wikipedia, „Paravirtualisierung," 2019. [Online]. Available: https://de.wikipedia.org/wiki/Paravirtualisierung. [Zugriff am 04. 01. 2021].

[5] Bundesstelle für Informationstechnik, „ Migrationsleitfaden, Leitfaden für die Migration von Software (Version 4.0)," 2012. [Online]. Available: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/migrationsleitfaden_4_0_download.pdf?__blob=publicationFile. [Zugriff am 04. 01. 2021].

[6] B. Golden, Virtualization for Dummies, Hoboken, NJ, USA: Wiley Publishing, 2008.

[7] Red Hat, „Virtualisierung; Was ist ein Hypervisor?,“ Red Hat, [Online]. Available: https://www.redhat.com/de/topics/virtualization/what-is-a-hypervisor. [Zugriff am 07. 01. 2021].

[8] N. Ruest, „Vergleich zwischen Typ 1 und Typ 2: Den richtigen Hypervisor auswählen,“ Computerweekly, 2014. [Online]. Available: https://www.computerweekly.com/de/tipp/Vergleich-zwischen-Typ-1-und-Typ-2-Den-richtigen-Hypervisor-auswaehlen. [Zugriff am 06. 01. 2021].

[9] O. Geißler und U. Ostler, „Achtung Aufnahme!; Was ist ein Snapshot?,“ Datacenter-Insider, 2019. [Online]. Available: https://www.datacenter-insider.de/was-ist-ein-snapshot-a-784078/. [Zugriff am 12. 01. 2021].

[10] S. J. Bigelow, „How VMware snapshots work and how to use them,“ TechTarget, 2019. [Online]. Available: https://searchvmware.techtarget.com/tip/How-VMware-snapshots-work. [Zugriff am 29. 01. 2021].

[11] B. Desmond, J. Richards, R. Allen und A. G. Lowe-Norris, Active Directory, Sebastopol, CA, USA: O'Reilly Media, Inc., 2013.

[12] A. Czernik, „Active Directory und Domäne – einfach erklärt,“ Dr-Datenschutz.de, 2016. [Online]. Available: https://www.dr-datenschutz.de/active-directory-und-domaene-einfach-erklaert/. [Zugriff am 08. 01. 2021].

[13] ManageEngine ADSolutions, „What is Active Directory?,“ 2017. [Online]. Available: https://www.youtube.com/watch?v=i9I5poSokow&t=322s&ab_channel=ManageEngineADSolutions. [Zugriff am 12. 01. 2021].

[14] Wikipedia, „Active Directoy,“ 2020. [Online]. Available: https://de.wikipedia.org/wiki/Active_Directory. [Zugriff am 08. 01. 2021].

[15] www.free-online-training-courses.com, „User Configuration Group Policy,“ www.free-online-training-courses.com, 2021. [Online]. Available: https://www.free-online-training-courses.com/user-configuration/. [Zugriff am 03. 02. 2021].

[16] Microsoft, „Domänencontrollersuche,“ 2017. [Online]. Available: https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/domain-controller-location. [Zugriff am 11. 01. 2021].

[17] Cloudflare, Inc., „Was ist eine DNS-Zone?,“ 2021. [Online]. Available: https://www.cloudflare.com/de-de/learning/dns/glossary/dns-zone/. [Zugriff am 26. 01. 2021].

[18] SambaWiki, „Active Directory Naming FAQ,“ 2021. [Online]. Available: https://wiki.samba.org/index.php/Active_Directory_Naming_FAQ. [Zugriff am 26. 01. 2021].

[19] Microsoft, „Assigning the Forest Root Domain Name,“ 2011. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc738121(v=ws.10)?redirectedfrom=MSDN. [Zugriff am 26. 01. 2021].

[20] D. Maguire, „Vorbereitung von Active Directory und Domänen für Exchange Server,“ Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/de-de/Exchange/plan-and-deploy/prepare-ad-and-domains?view=exchserver-2019. [Zugriff am 29. 01. 2021].

[21] Wikipedia, „Microsoft Exchange Server,“ 2020. [Online]. Available: https://de.wikipedia.org/wiki/Microsoft_Exchange_Server. [Zugriff am 13. 01. 2021].

[22] J. Fischer, „Was ist ein Exchange Server?,“ Die media-company, 2020. [Online]. Available: https://www.media-company.eu/blog/allgemein/%EF%BB%BF-was-ist-ein-exchange-server/. [Zugriff am 01. 13. 2021].

[23] O. Schonschek und P. Schmitz, „Definition Malware, Was ist Malware?," 2017. [Online]. Available: https://www.security-insider.de/was-ist-malware-a-578417/. [Zugriff am 04. 01. 2021].

[24] H. Siller, „Malware, Definition: Was ist "Malware"?," 2018. [Online]. Available: https://wirtschaftslexikon.gabler.de/definition/malware-53410/version-276503. [Zugriff am 04. 01. 2021].

[25] S. Luber und P. Schmitz, „Definition Exploit(Ausnutzen von Schwachstellen); Was ist ein Exploit?," Security Insider, 2017. [Online]. Available: https://www.security-insider.de/was-ist-ein-exploit-a-618629/. [Zugriff am 04. 01. 2021].

[26] S. Malenkovich, „Was ist ein Rootkit?," Kaspersky Daily, 2013. [Online]. Available: https://www.kaspersky.de/blog/was-ist-ein-rootkit/853/. [Zugriff am 04. 01. 2021].

[27] P. Schmitz und S. Luber, „Definition Trojaner; Was ist ein Trojanisches Pferd?," Security Insider, 2019. [Online]. Available: https://www.security-insider.de/was-ist-ein-trojanisches-pferd-a-818987/. [Zugriff am 04. 01. 2021].

[28] S. Luber und P. Schmitz, „Definition Backdoor; Was ist eine Backdoor?," Security Insider, 2018. [Online]. Available: https://www.security-insider.de/was-ist-eine-backdoor-a-676126/. [Zugriff am 04. 01. 2021].

[29] Duden online, [Online]. Available: https://www.duden.de/rechtschreibung/kompromittieren. [Zugriff am 04. 01. 2021].

[30] AO Kaspersky Lab, „Verschiedene Arten und Klassifikation von Malware," 2021. [Online]. Available: https://www.kaspersky.de/resource-center/threats/malware-classifications. [Zugriff am 04. 01. 2021].

[31] HWZ Digital, „Digitale Forensik in a big Nutshell,“ HWZ Digital, 2020. [Online]. Available: https://www.hwzdigital.ch/digitale-forensik-in-a-big-nutshell/. [Zugriff am 05. 02. 2021].

[32] L. Zeltser, „Practical Malware Analysis Essentials for Incident Responders,“ in *RSA Conference 2019*, San Francisco, 2019.

[33] S. Follmer, „Was ist die Registry und wie funktioniert sie?,“ Chip.de, 2015. [Online]. Available: https://praxistipps.chip.de/was-ist-die-registry-und-wie-funktioniert-sie_43423. [Zugriff am 08. 02. 2021].

[34] C. Maler, „Malwareanalyse und Verteidigung,“ Hornetsecurity, 2018. [Online]. Available: https://www.hornetsecurity.com/de/services/malwareanalyse-und-verteidigung/. [Zugriff am 04. 01. 2021].

[35] A. Gritzka, „Praxisbericht, Praktikum bei der T-Systems Multimedia Solutions GmbH,“ Dresden, 2020.

[36] R. Burnett, „So wählen Sie die beste CPU für die Virtualisierung,“ ComputerWeekly.de, 2019. [Online]. Available: https://www.computerweekly.com/de/tipp/So-waehlen-Sie-die-beste-CPU-fuer-die-Virtualisierung. [Zugriff am 13. 01. 2021].

[37] rickardnobel, „Max size of snapshot,“ VMware, 2012. [Online]. Available: https://communities.vmware.com/t5/ESXi-Discussions/Snapshot-how-much-space-will-be-used/td-p/1330396. [Zugriff am 20. 01. 2021].

[38] S. Makbuloğlu, „Capacity Planning for Active Directory Domain Services,“ Microsoft TechNet, 2017. [Online]. Available: https://social.technet.microsoft.com/wiki/contents/articles/14355.capacity-planning-for-active-directory-domain-services.aspx#Calculation_Summary_Example. [Zugriff am 13. 01. 2021].

[39] Microsoft Docs, „Planning DNS Services," Microsoft, 2009. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732715(v=ws.11)?redirectedfrom=MSDN. [Zugriff am 13. 01. 2021].

[40] J. Gerend, olprod und N. Dolci, „Systemanforderungen," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/de-de/windows-server/get-started-19/sys-reqs-19. [Zugriff am 13. 01. 2021].

[41] Microsoft, „windows-10-specifications," Microsoft, 2020. [Online]. Available: https://www.microsoft.com/de-de/windows/windows-10-specifications. [Zugriff am 13. 01. 2021].

[42] Wikipedia, „Wrapper (Software)," 2020. [Online]. Available: https://de.wikipedia.org/wiki/Wrapper_(Software). [Zugriff am 22. 01. 2021].

[43] VMware, „Build numbers and versions of VMware ESXi/ESX (2143832)," My VMware, 2021. [Online]. Available: https://kb.vmware.com/s/article/2143832. [Zugriff am 20. 01. 2021].

[44] T. Peyo, „VCP5-DCV course," Geek-University.com, [Online]. Available: https://geek-university.com/course/vcp5-dcv-course/. [Zugriff am 2021].

[45] A. Hancock, „HOW TO: Connect to the VMware vSphere Hypervisor 7.0 (ESXi 7.0) using the vSphere (HTML5 Web) Host Client 7.0," Experts Exchange, 2020. [Online]. Available: https://www.experts-exchange.com/articles/34113/HOW-TO-Connect-to-the-VMware-vSphere-Hypervisor-7-0-ESXi-7-0-using-the-vSphere-HTML5-Web-Host-Client-7-0.html. [Zugriff am 16. 01. 2021].

[46] LoveToKnow, „Ethernet-adapter meaning," Your Dictionary, 2020. [Online]. Available: https://www.yourdictionary.com/ethernet-adapter. [Zugriff am 17. 01. 2021].

[47] mahabaleshwm, „VMware Workstation 16.1.0 Pro Release Notes,“ VMware, 2020. [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.1.0/rn/VMware-Workstation-1610-Pro-Release-Notes.html. [Zugriff am 20. 01. 2021].

[48] VMware, „VMware Workstation – Häufig gestellte Fragen,“ VMware, 2021. [Online]. Available: https://www.vmware.com/de/products/workstation-pro/faq.html. [Zugriff am 19. 01. 2021].

[49] Fhettenbach, „Virtualisierungstechnologien im Überblick,“ 2015. [Online]. Available: https://www.thomas-krenn.com/de/wiki/Virtualisierungstechnologien_im_%C3%9Cberblick. [Zugriff am 20. 01. 2021].

[50] R. Schanze, „UEFI & BIOS – die wichtigsten Unterschiede,“ GIGA, 2018. [Online]. Available: https://www.giga.de/extra/bios/specials/uefi-und-bios-wichtigsten-unterschiede/. [Zugriff am 20. 01. 2021].

[51] djohn, „Selecting the I/O Controller Type for a Virtual Machine,“ VMware, 2019. [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-A0438F6C-6651-4A38-853A-0A7A494E23DF.html. [Zugriff am 20. 01. 2021].

[52] Wikipedia, „NVM Express,“ 2020. [Online]. Available: https://de.wikipedia.org/wiki/NVM_Express. [Zugriff am 20. 01. 2021].

[53] VMware, „Selecting the Virtual Hard Disk Type for a Virtual Machine,“ VMware, 2019. [Online]. Available: https://docs.vmware.com/en/VMware-Workstation-Pro/16.0/com.vmware.ws.using.doc/GUID-4E8FB60D-350B-4158-B3DD-E4003B962296.html. [Zugriff am 20. 01. 2021].

[54] S. V. Vugt, VMware Workstation - No Experience Necessary, Brimingham, UK: Packt Publishing, 2013.

[55] R. McMillen, „Create an Active Directory lab using VMWare and Windows Server 2016," 2018. [Online]. Available: https://www.youtube.com/watch?v=1O0smx7F2yw&ab_channel=RobertMcMillen. [Zugriff am 25. 01. 2021].

[56] InformatikTube, „Server2012R2 Grundlagen und Active Directory," InformatikTube, 2016. [Online]. Available: https://www.youtube.com/watch?v=pbGIEWUo23w&ab_channel=InformatikTube. [Zugriff am 11. 01. 2021].

[57] M. Rouse, „Directory Services Restore Mode (DSRM)," TechTarget, 2012. [Online]. Available: https://searchwindowsserver.techtarget.com/definition/Directory-Services-Restore-Mode-DSRM. [Zugriff am 25. 01. 2021].

[58] R. J. Butt, „Install and Configure Exchange Server 2019 Part 1 - 10," MSExpertTalk, 2018. [Online]. Available: https://msexperttalk.com/install-and-configure-exchange-server-2019/. [Zugriff am 27. 01. 2021].

[59] V. Singh, „How to Install Exchange Server 2019 Step by Step full," Labs Hands On, 2020. [Online]. Available: https://www.youtube.com/watch?v=vU5WbNIShyE&ab_channel=LabsHandsOn. [Zugriff am 27. 01. 2021].

[60] F. Zöchling, „HowTo: Installation von Exchange 2019 auf Server 2019," Frankys Web, 2018. [Online]. Available: https://www.frankysweb.de/howto-installation-von-exchange-2019-auf-server-2019/. [Zugriff am 27. 01. 2021].

[61] F. Zöchling, „Exchange 2019: Die Basiskonfiguration," 2018. [Online]. Available: https://www.frankysweb.de/exchange-2019-die-basiskonfiguration/. [Zugriff am 27. 01. 2021].

[62] D. Maguire, „Digitale Zertifikate und Verschlüsselung in Exchange Server," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/de-de/exchange/architecture/client-access/certificates?view=exchserver-2019. [Zugriff am 02. 02. 2021].

[63] D. Maguire, M. Penna, C. Davis, A. Borys, A. M. Gorzelany und D. Strome, „Virtual directory management," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/en-us/exchange/virtual-directory-management-exchange-2013-help. [Zugriff am 03. 02. 2021].

[64] D. Maguire, „Erstellen von Benutzerpostfächern in Exchange Server," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/de-de/exchange/recipients/create-user-mailboxes?view=exchserver-2019. [Zugriff am 29. 01. 2021].

[65] D. Maguire, „Exchange Server-Virtualisierung," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/de-de/exchange/plan-and-deploy/virtualization?view=exchserver-2019. [Zugriff am 03. 02. 2021].

[66] C. Thorpe, „Restoring snapshot for Microsoft Exchange server," StackExchange, 2010. [Online]. Available: https://serverfault.com/questions/82625/restoring-snapshot-for-microsoft-exchange-server. [Zugriff am 29. 01. 2021].

[67] P. D. D. Pawlaszczyk, Virentechnoligie/Antivirensoftware 01, Mittweida: Hochschule Mittweida, University of Applied Sciences, 2018.

[68] K. Bridge, D. Batchelor, D. Coulter, J. Krell, R. Keldorph, Y. Zhu, j04n, C. Robertson, M. Kayser, J. Kennedy, C. Warrington, M. Satran und M. LeBLanc, „PE Format,"

Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/debug/pe-format. [Zugriff am 05. 02. 2021].

[69] R. Dombach, „PESTUDIO," secuteach, 2020. [Online]. Available: https://www.secuteach.de/pestudio.html. [Zugriff am 05. 02. 2021].

[70] N. Fox, „11 Best Malware Analysis Tools and Their Features," Varonis.com, 2021. [Online]. Available: https://www.varonis.com/blog/malware-analysis-tools/. [Zugriff am 06. 02. 2020].

[71] P. D. D. Pawlaszczyk, Virentechnologie/Antivirensoftware 05, Mittweida: Hochschule Mittweida, University of Applied Sciences, 2018.

[72] VirusTotal, „VirusTotal," VirusTotal, 2021. [Online]. Available: Virustotal.com. [Zugriff am 06. 02. 2021].

[73] Team Cymru, „#totalhash Malware Analysis Database," Team Cymru, 2021. [Online]. Available: https://totalhash.cymru.com/. [Zugriff am 06. 02. 2021].

[74] NoVirusThanks, „URLVoid Website Reputation Checker," NoVirusThanks, 2021. [Online]. Available: urlvoid.com. [Zugriff am 09. 02. 2021].

[75] C. Robertson, M. A. Tahan, M. Jones, G. Hogenson und S. Cai, „Create C/C++ DLLs in Visual Studio," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/en-us/cpp/build/dlls-in-visual-cpp?redirectedfrom=MSDN&view=msvc-160. [Zugriff am 05. 02. 2021].

[76] Wayne J. Radburn, „Wayne J. Radburn," Wayne J. Radburn, 2019. [Online]. Available: http://wjradburn.com/software/. [Zugriff am 06. 02. 2021].

[77] P. D. D. Markgraf, „Reverse Engineering," Gabler Wirtschaftslexikon, 2018. [Online]. Available: https://wirtschaftslexikon.gabler.de/definition/reverse-engineering-45260/version-268557. [Zugriff am 08. 02. 2021].

[78] Hex-Rays, „Hex-Rays Online Store," Hex-Rays, 2020. [Online]. Available: https://www.hex-rays.com/cgi-bin/quote.cgi/products. [Zugriff am 08. 02. 2021].

[79] Hex-Rays, „Main differences between IDA editions," Hex-Rays, 2020. [Online]. Available: https://www.hex-rays.com/products/ida/main-differences-between-ida-editions/. [Zugriff am 08. 02. 2021].

[80] Hex-Rays, „IDA Pro in a nutshell," Hex-Rays, 2020. [Online]. Available: https://www.hex-rays.com/products/ida/. [Zugriff am 08. 02. 2021].

[81] National Security Agency (NSA), „Ghidra Installation Guide," National Security Agency (NSA), 2020. [Online]. Available: https://ghidra-sre.org/InstallationGuide.html. [Zugriff am 08. 02. 2021].

[82] C. Mössner, „Reverse Engineering mit Ghidra Tutorial #2 - Eine einfache Aufgabe," The Morpheus Tutorials, 2020. [Online]. Available: https://www.youtube.com/watch?v=KwVAdKZieag&ab_channel=TheMorpheusTutorials. [Zugriff am 08. 02. 2021].

[83] M. Russinovich, foxmsft, L. Kim, analyze-v, Y. Steinmetz und L. Picking, „Sysinternals Suite," Microsoft, 2021. [Online]. Available: https://docs.microsoft.com/de-de/sysinternals/downloads/sysinternals-suite. [Zugriff am 08. 02. 2021].

[84] M. Russinovich, L. Kim, analyze-v, VSC-Service-Account und wesdawg, „Autoruns for Windows v13.98," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns. [Zugriff am 09. 02. 2021].

[85] L. Heddings, „Using Autoruns to Deal with Startup Processes and Malware,“ How-To Geek, 2019. [Online]. Available: https://www.howtogeek.com/school/sysinternals-pro/lesson6/. [Zugriff am 09. 02. 2021].

[86] P. B. Mundas, „DYNAMIC MALWARE ANALYSIS – PROCESS MONITOR AND EXPLORER | By Prasanna B Mundas,“ eForensics Magazine, 2019. [Online]. Available: https://eforensicsmag.com/dynamic-malware-analysis-process-monitor-and-explorer-by-prasanna-b-mundas/. [Zugriff am 09. 02. 2021].

[87] Informatik-Verstehen, „Lexikon - Handle,“ Informatik-Verstehen, 2021. [Online]. Available: https://www.informatik-verstehen.de/lexikon/handle/. [Zugriff am 09. 02. 2021].

[88] M. Russinovich, H. Mauerer, L. Kim, analyze-v und L. Tsarev, „Process Explorer v16.32,“ Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer. [Zugriff am 09. 02. 2021].

[89] Redaktion ComputerWeekly.de, „Sniffer,“ ComputerWeekly.de, 2016. [Online]. Available: https://www.computerweekly.com/de/definition/Sniffer. [Zugriff am 10. 02. 2021].

[90] Wireshark Community, „Wireshark. Go Deep.,“ Wireshark Community, 2021. [Online]. Available: https://www.wireshark.org/. [Zugriff am 10. 02. 2021].

[91] C. Craft, „WinPcap,“ GitLab, 2020. [Online]. Available: https://gitlab.com/wireshark/wireshark/-/wikis/WinPcap. [Zugriff am 10. 02. 2021].

[92] R. Teixeira, „Intro to Wireshark: Basics + Packet Analysis!,“ SinnohStarly - Ross Teixeira, 2016. [Online]. Available: https://www.youtube.com/watch?v=jvuiI1Leg6w&ab_channel=SinnohStarly-RossTeixeira. [Zugriff am 10. 02. 2021].

[93] A. Alexander, „Wireshark Tutorial for Beginners,“ Anson Alexander, 2015. [Online]. Available: https://www.youtube.com/watch?v=TkCSr30UojM&ab_channel=AnsonAlexander. [Zugriff am 10. 02. 2021].

[94] P. Januszkiewicz, „Memory Dump Analysis – Extracting Juicy Data,“ CQURE Academy, 2016. [Online]. Available: https://cqureacademy.com/blog/hacks/memory-dump-analysis. [Zugriff am 12. 02. 2021].

[95] C. Wojner, „ProcDOT,“ ProcDOT, 2017. [Online]. Available: https://www.procdot.com/. [Zugriff am 10. 02. 2021].

[96] C. Wojner, „[2015-06-28] Edge label modes.,“ ProcDOT, 2015. [Online]. Available: https://www.procdot.com/blog_20150628.htm. [Zugriff am 10. 02. 2021].

Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Ort, Datum	Vollständiger Name	Unterschrift

Nutzungs- und Verwertungsrechte

Ich übertrage zusätzliche Nutzungs- und Verwertungsrechte für die vorliegende Arbeit und allen damit in Zusammenhang stehenden Daten auf Grundlage der *Creative Commons Lizenz* "*CC0*" an alle genannten Betreuer dieser Arbeit.

Ort, Datum	Unterschrift