

## 3

## Setting Up for Advanced Penetration Testing Techniques

Learning the methodology and techniques of performing penetration testing is always exciting. While many professionals may focus on specific types of penetration testing, such as internal or external network penetration testing, social engineering penetration testing, or even web application security testing, it's always beneficial to understand how to perform wireless penetration testing and how to compromise a Microsoft Windows domain in an enterprise environment.

In this chapter, you will learn how to set up an Active Directory domain environment that will enable you to perform advanced penetration testing exercises such as red teaming techniques to discover security vulnerabilities and compromise the Domain Controller, taking over the domain of the organization. Red teaming focuses on a very comprehensive security assessment of an organization's cyber defenses, physical security controls, technologies, processes, and people, such as the employees. Red teaming is designed to simulate real-world cyber-attacks to test an organization's ability to detect, respond to, and mitigate cybersecurity incidents.

In addition, you will set up a **Remote Authentication Dial-In User Service (RADIUS)** access server to provide **Authentication, Authorization, and Accounting (AAA)** services to our enterprise wireless network.

In this chapter, we will cover the following topics:

- Building an Active Directory red team lab
- Setting up a wireless penetration testing lab

Let's dive in!

## Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following hardware and software requirements:


- Oracle VM VirtualBox: <https://www.virtualbox.org/>
- Windows 10 Enterprise: <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>
- Windows Server 2019: <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019>
- Ubuntu Server 22.04 LTS: <https://releases.ubuntu.com/jammy/>
- Wireless router that supports WPA2 and WPA3

## Building an Active Directory red team lab

**Active Directory** is a role within the Microsoft Windows Server operating system that enables IT administrators to centrally manage all users, devices, and policies within a Windows environment. Active Directory ensures that centralized management is available for user accounts across an entire Windows domain and that policies can be created and assigned to various user groups to ensure people have the necessary access rights to perform actions that are related to their job duties.

Active Directory is commonly found within many organizations around the world. Therefore, as an aspiring ethical hacker and penetration tester, it's important to understand how to discover various security vulnerabilities within a Microsoft Windows domain and leverage those security flaws to compromise an organization's **Domain Controller** and its systems, services, and shared resources.

Active Directory provides centralized identity management for user accounts, groups, and computer accounts within an organization that's using Microsoft Windows Server. By understanding Active Directory, ethical hackers and penetration testers can target and determine the security posture of this system. Since Active Directory is commonly used by organizations as their central hub for configuring access controls on user accounts and device accounts, this can be a prime targeted system for real threat actors. Therefore, it's essential for penetration testers to understand how Active Directory is integrated with other systems and the services it provides to better identify potential attack vectors and how it can be compromised. To put it simply, if an attacker can compromise and take over Active Directory within an organization, that's the end game as the attacker can control the Windows domain environment in the network.



To learn more about the role and importance of a Domain Controller, please see <https://www.techtarget.com/searchwindowsserver/definition/domain-controller>.

This section will teach you how to create a Microsoft Windows lab environment with Microsoft Windows Server 2019 and two Windows 10 Enterprise clients as virtual machines. This lab environment will allow you to practice advanced penetration testing techniques such as red teaming exercises in a Windows domain and exploit security flaws in Active Directory environments.

The following diagram shows the RedTeamLab environment:

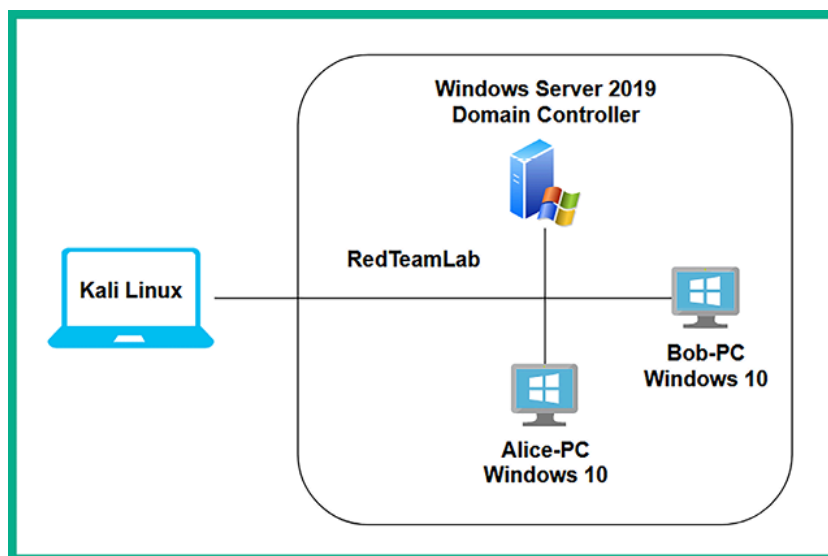


Figure 3.1: Red teaming topology

As we can see, our Kali Linux virtual machine is directly connected to the *RedTeamLab* environment, which has a Windows Server machine and two Windows 10 client machines. In later sections of this book, you will learn how to perform exploitation and post-exploitation techniques on targets, so when you're exploiting the systems within the Windows domain, we will assume you have already broken into the network and have compromised at least one system that's

connected to Active Directory. For now, we will focus on setting up our environment for security testing later.

The following table shows the user accounts that we will be setting up in the *RedTeamLab* environment:

Group	Username	Password	Device
Local user	Administrator	P@ssword1	Windows Server
Local user	bob	P@ssword2	Bob-PC
Local user	alice	P@ssword2	Alice-PC
Domain user	gambit	Password1	Domain user accounts (stored within Active Directory)
Domain user	rogue	Password1	
Domain administrator	wolverine	Password123	
Service account	sqladmin	Password45	

Figure 3.2: User accounts

As shown in the preceding table, we will create two domain users (*gambit* and *rogue*), an additional domain administrator (*wolverine*), and a service account with domain administrative privileges (*sqladmin*).

To get started setting up the red team section of our lab, please use the instructions in the following sections.

## Part 1 – Setting up Windows Server

In this section, you will learn how to set up Microsoft Windows Server 2019 as a virtual machine. To get started with this exercise, please use the following instructions:

1. On your host computer, go to <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019> and click on **Download the VHD**. Ensure you complete the registration form to access the download links for the **Virtual Hard Disk (VHD) 64-bit edition** file as shown below:

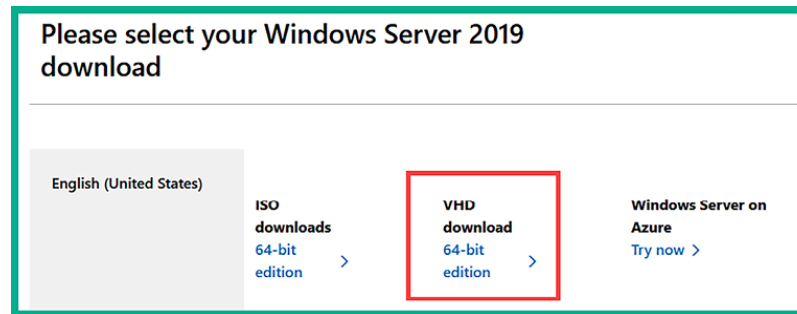
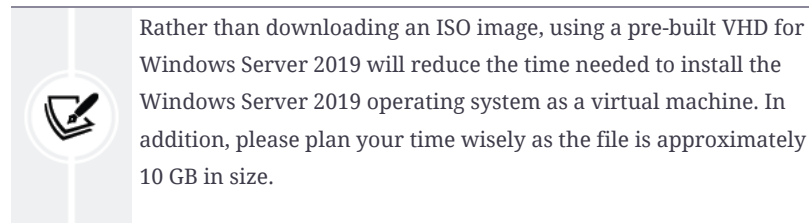


Figure 3.3: Download page for Windows Server 2019



2. Once the Windows Server 2019 VHD file is downloaded on your host computer, open **Oracle VM VirtualBox Manager** and click on **New** to create a new virtual machine environment.
  3. When the **Create Virtual Machine** window appears, click on **Expert Mode** and use the following configurations:
    1. **Name:** Windows Server 2019
    2. **Type:** Microsoft Windows
    3. **Version:** Windows 2019 (64-bit)
    4. **Hard Disk:** Use an existing virtual hard disk file (click on the folder icon and then **Add**, and select the **Windows Server 2019 VHD** file)
    5. Click on **Finish** to save the virtual machine
  4. Once the **Windows Server 2019 virtual machine** is created and saved on **Oracle VM VirtualBox Manager**, select it and click on **Settings**.
  5. In the **Settings** window, select the **Network** category and use the following settings for **Adapter 1**:
    1. **Adapter 1:** Enable network Adapter
    2. **Attached to:** Internal Network
    3. **Name:** RedTeamLab (manually type it in the field)
    4. **Promiscuous Mode:** Allow All
- The following screenshot shows the preceding configurations for **Adapter 1**:

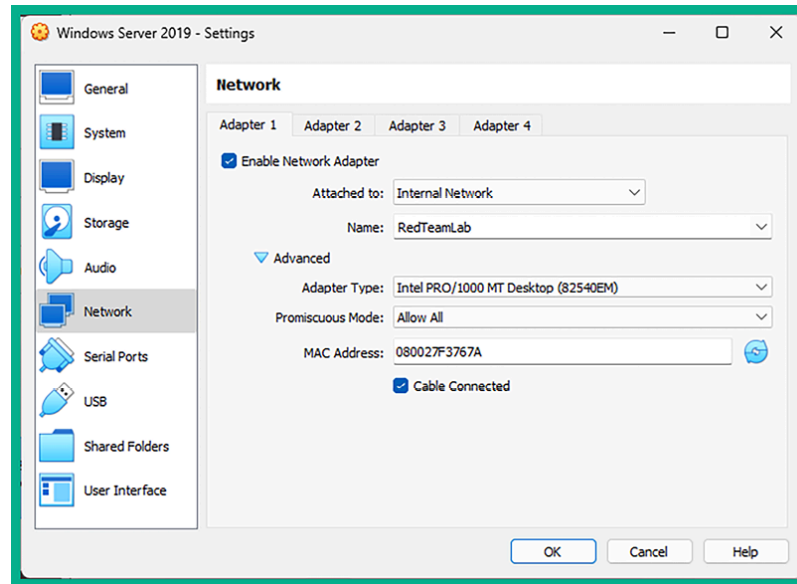


Figure 3.4: Network Adapter 1 settings

6. Next, select the **Windows Server 2019 virtual machine** and click on **Start** to power it on.
7. Once the virtual machine is running, you will be prompted to select your home country/region, preferred app language, and keyboard layout. Click on **Next**.
8. Next, you will need to read the **License terms** and click on **Accept**.
9. Next, create a password for the built-in **Administrator** account, use **P@ssword1** as the password, and click on **Finish**.
10. Next, log in to the Windows Server 2019 virtual machine. On the virtual machine menu bar, select **Input | Keyboard | Insert Ctrl-Alt-Del** to view the login window:

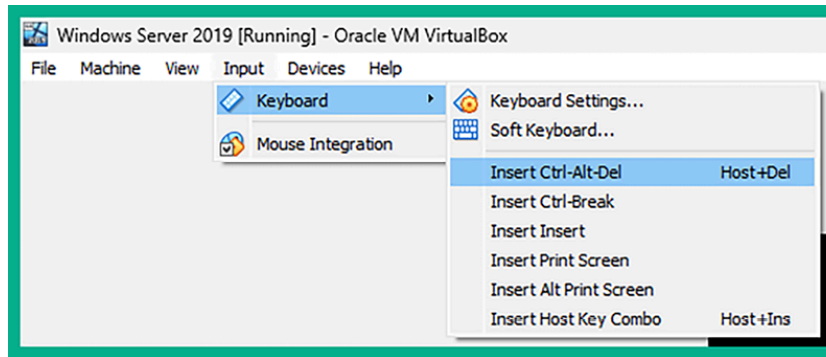


Figure 3.5: Soft keyboard menu

11. Log in using username: Administrator and password: P@ssword1.

## Part 2 – Configuring virtual machine additional features

In this section, you will configure additional virtual machine settings to ensure there's a smooth experience between your host operating system and the guest operating system:

1. Ensure the Windows Server 2019 virtual machine is running and you're logged in.

To scale the virtual machine's desktop resolution to fit your host computer's monitor, on the virtual machine menu bar, select **Devices** | **Insert Guest Additions CD image** as shown here:

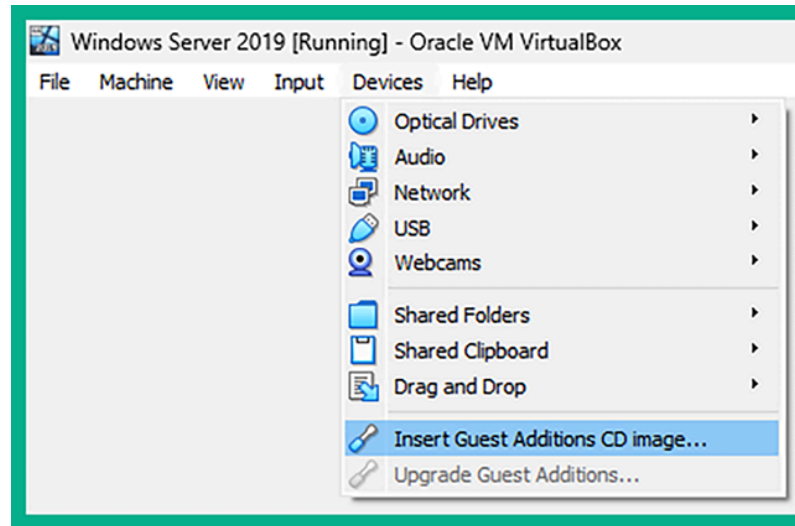
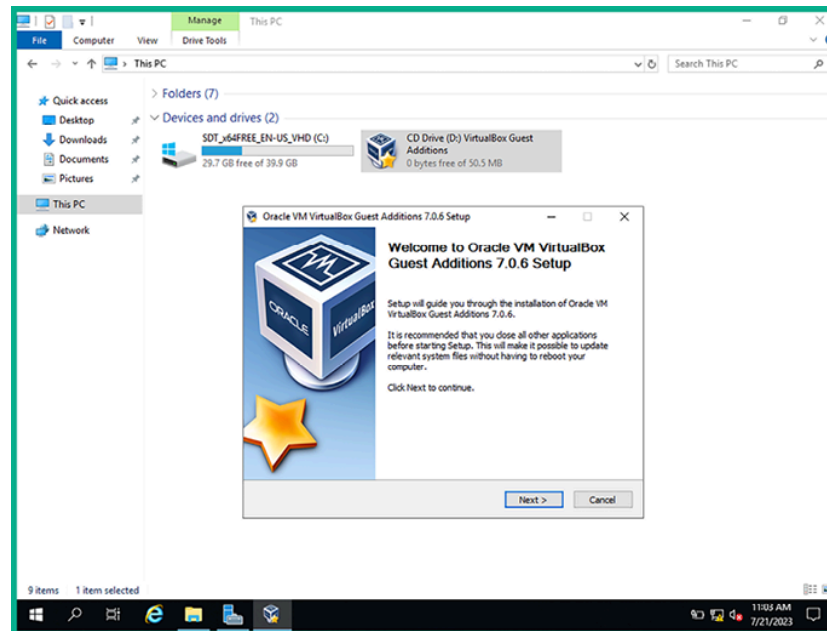


Figure 3.6: Guest additions image

2. Next, open **Windows Explorer** within Windows Server 2019, navigate to **This PC**, and double-click on the **VirtualBox Guest Additions** virtual disk:





*Figure 3.7: Guest Additions installer*

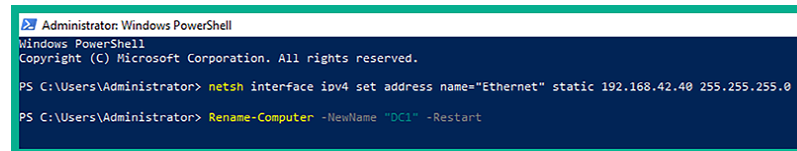
3. When the installation window appears, click on **Next** and ensure that you use the default settings during the installation process. When it's complete, do not reboot.
4. Next, within Windows Server 2019, click on the **Start** button (bottom-left corner) and open **Windows PowerShell**. Use the following commands to static assign an IP address and subnet mask to the Ethernet network adapter:

```
PS C:\Users\Administrator> netsh interface ipv4 set address name="Ethernet" static 192.168.42.40 255.255.255.0
```

5. Next, change the default hostname to **DC1** and reboot the server with the following commands:

```
PS C:\Users\Administrator> Rename-Computer -NewName "DC1" -Restart
```

The following screenshot shows the execution of the preceding commands:

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The window shows the following text: "Windows PowerShell", "Copyright (C) Microsoft Corporation. All rights reserved.", "PS C:\Users\Administrator> netsh interface ipv4 set address name='Ethernet' static 192.168.42.40 255.255.255.0", and "PS C:\Users\Administrator> Rename-Computer -NewName 'DC1' -Restart".

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> netsh interface ipv4 set address name="Ethernet" static 192.168.42.40 255.255.255.0

PS C:\Users\Administrator> Rename-Computer -NewName "DC1" -Restart
```

*Figure 3.8: Setting a static address and custom name on Windows Server*

6. Next, after the server reboots, log in using the Administrator credentials. The Windows Server desktop interface will automatically scale to fit your monitor's resolution. If it doesn't, simply toggle this with the **VirtualBox menu bar** and go to the **View | Auto-resize Guest Display** option as shown here:

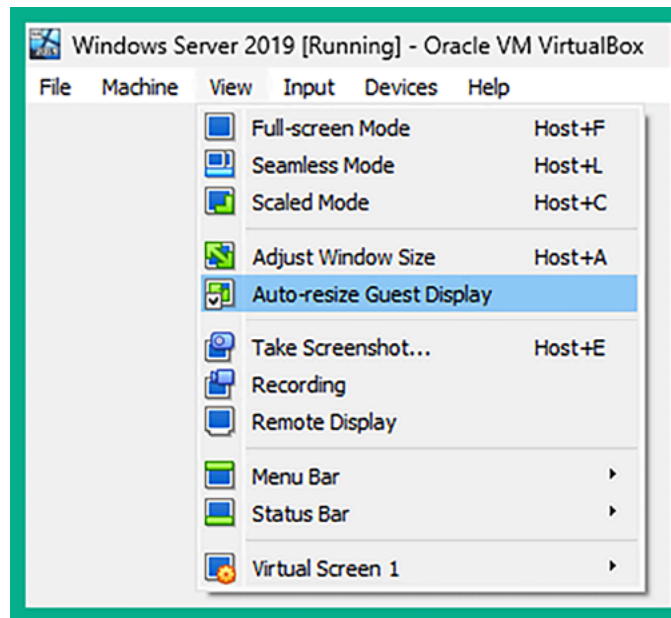


Figure 3.9: Resizing display

### Part 3 – Setting Active Directory Domain Services

Active Directory is a very important and popular role within Microsoft Windows Server as it allows IT professionals to centrally manage all users, devices, and policies within a Windows environment. To set up Active Directory within our lab, please use the following instructions:

1. Open the **Windows PowerShell** application within the Windows Server 2019 virtual machine.
2. Install **Active Directory Domain Services** and its management tools using the following commands:

```
PS C:\Users\Administrator> Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools
```

3. Next, configure a new Active Directory forest and domain with the name `redteamlab.local` using the following commands:

```
PS C:\Users\Administrator> Install-ADDSForest -DomainName redteamlab.local -skipprerechecks
```

You'll be prompted to enter a **Safe Mode Administrator Password**; use `P@ssword1`. When prompted to continue the operation, type `Y` and hit `Enter` to continue, as shown in the following screenshot:



```
PS C:\Users\Administrator> Install-ADDSForest -DomainName redteamlab.local -skipprerechecks
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****
The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

Figure 3.10: Joining a domain using PowerShell

The setup process takes a few minutes to complete, then Windows Server will automatically reboot.

After the server reboots, log in using the Administrator credentials. This time, you'll be logging in as a domain administrator on the server.

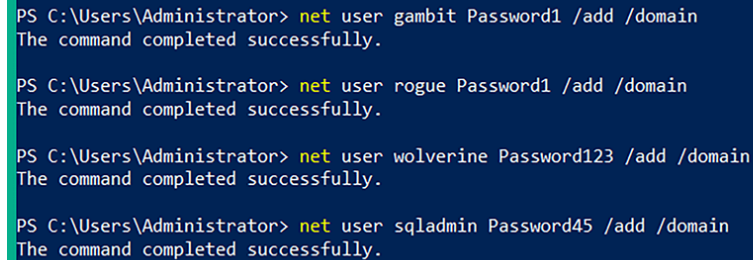
## Part 4 – Creating domain users and administrator accounts

The following steps will carefully guide you through the process of creating domain users and domain administrators and assigning the user to various security groups. To ensure these steps are simple and concise, we will be using Windows PowerShell on Windows Server:

1. On the Windows Server 2019 virtual machine, open the **Windows PowerShell** application and use the following commands to create four domain user accounts:

```
PS C:\Users\Administrator> net user gambit Password1 /add /domain
PS C:\Users\Administrator> net user rogue Password1 /add /domain
PS C:\Users\Administrator> net user wolverine Password123 /add /domain
PS C:\Users\Administrator> net user sqladmin Password45 /add /domain
```

The following screenshot shows the execution of the preceding commands:



```
PS C:\Users\Administrator> net user gambit Password1 /add /domain
The command completed successfully.

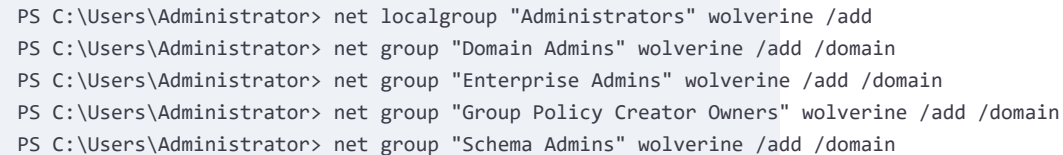
PS C:\Users\Administrator> net user rogue Password1 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user wolverine Password123 /add /domain
The command completed successfully.

PS C:\Users\Administrator> net user sqladmin Password45 /add /domain
The command completed successfully.
```

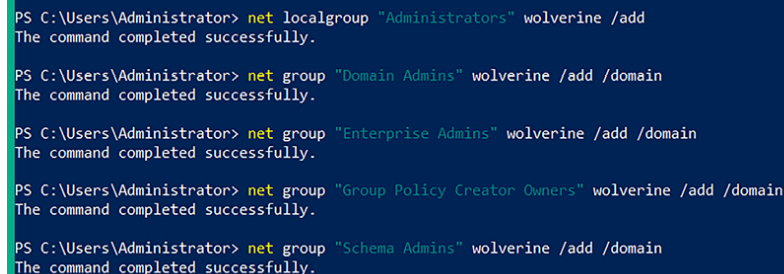
Figure 3.11: Creating user accounts

2. Next, let's make the `wolverine` account a high-privilege user account that has the same privileges as the administrator by using the following commands:



```
PS C:\Users\Administrator> net localgroup "Administrators" wolverine /add
PS C:\Users\Administrator> net group "Domain Admins" wolverine /add /domain
PS C:\Users\Administrator> net group "Enterprise Admins" wolverine /add /domain
PS C:\Users\Administrator> net group "Group Policy Creator Owners" wolverine /add /domain
PS C:\Users\Administrator> net group "Schema Admins" wolverine /add /domain
```

The following screenshot shows the execution of the preceding commands:



```
PS C:\Users\Administrator> net localgroup "Administrators" wolverine /add
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Admins" wolverine /add /domain
The command completed successfully.

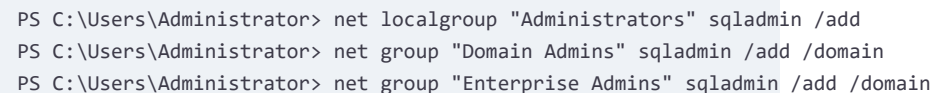
PS C:\Users\Administrator> net group "Enterprise Admins" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Group Policy Creator Owners" wolverine /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Schema Admins" wolverine /add /domain
The command completed successfully.
```

Figure 3.12: Adding users to groups

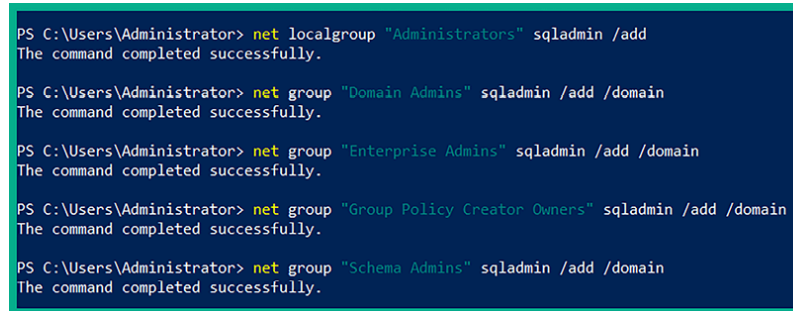
3. Next, we will do the same for the `sqladmin` account:



```
PS C:\Users\Administrator> net localgroup "Administrators" sqladmin /add
PS C:\Users\Administrator> net group "Domain Admins" sqladmin /add /domain
PS C:\Users\Administrator> net group "Enterprise Admins" sqladmin /add /domain
```

```
PS C:\Users\Administrator> net group "Group Policy Creator Owners" sqladmin /add /domain
PS C:\Users\Administrator> net group "Schema Admins" sqladmin /add /domain
```

The following screenshot shows the execution of the preceding commands:



```
PS C:\Users\Administrator> net localgroup "Administrators" sqladmin /add
The command completed successfully.

PS C:\Users\Administrator> net group "Domain Admins" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Enterprise Admins" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Group Policy Creator Owners" sqladmin /add /domain
The command completed successfully.

PS C:\Users\Administrator> net group "Schema Admins" sqladmin /add /domain
The command completed successfully.
```

Figure 3.13: Adding another user to groups

## Part 5 – Disabling antimalware protection and the domain firewall

Within our lab, we need to ensure the Windows Defender antimalware protection is disabled on the clients that are connected to the Windows domain. Some techniques are being used to bypass antiviruses that will work currently, but they might not work afterward due to the continuous advancement of malware protection and solutions.

The following steps will guide you through the process of ensuring Windows Defender and the host-based firewall is disabled on all systems by leveraging **Group Policy Objects (GPOs)**:

1. On the Windows Server 2019 virtual machine, open the **Windows PowerShell** application and use the following commands to create a new GPO called `DisableAVGPO` :

```
PS C:\Users\Administrator> New-GPO -Name DisableAVGPO -Comment "This GPO disables AV on the entire domain"
```

The following screenshot shows the expected results when executing the preceding commands:

```
PS C:\Users\Administrator> New-GPO -Name DisableAVGPO -Comment "This GPO disables AV on the entire domain"

DisplayName : DisableAVGPO
DomainName  : redteamlab.local
Owner       : REDTEAMLAB\Domain Admins
Id          : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus   : AllSettingsEnabled
Description : This GPO disables AV on the entire domain
CreationTime : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:20:06 AM
UserVersion : AD Version: 0, SysVol Version: 0
ComputerVersion : AD Version: 0, SysVol Version: 0
WmiFilter   :
```

Figure 3.14: Creating new GPO

2. Next, use the following commands to disable the antimalware service from always running:

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key "HKLM\Software\Policies\Microsoft\Windows Defen
```

As shown below, the preceding commands successfully updated the DisableAVGPO policy:

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key "HKLM\Software\Policies\Microsoft\Windows Defender" -ValueName "ServiceKeepAlive" -Type DWORD -Value 0

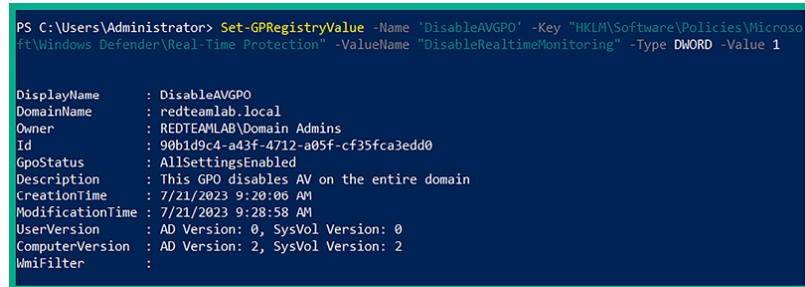
DisplayName : DisableAVGPO
DomainName  : redteamlab.local
Owner       : REDTEAMLAB\Domain Admins
Id          : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus   : AllSettingsEnabled
Description : This GPO disables AV on the entire domain
CreationTime : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:26:08 AM
UserVersion : AD Version: 0, SysVol Version: 0
ComputerVersion : AD Version: 1, SysVol Version: 1
WmiFilter   :
```

Figure 3.15: Disabling Windows Defender

3. Next, turn off the antimalware real-time protection using the following commands:

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key "HKLM\Software\Policies\Microsoft\Windows Defen
```

The following screenshot shows the preceding commands updated the policy:



```
PS C:\Users\Administrator> Set-GPRegistryValue -Name 'DisableAVGPO' -Key 'HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection' -ValueName 'DisableRealtimeMonitoring' -Type DWORD -Value 1

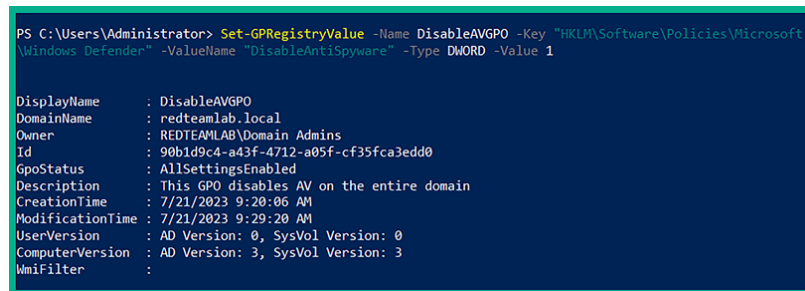
DisplayName : DisableAVGPO
DomainName  : redteamlab.local
Owner       : REDTEAMLAB\Domain Admins
Id          : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus   : AllSettingsEnabled
Description : This GPO disables AV on the entire domain
CreationTime : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:28:58 AM
UserVersion : AD Version: 0, SysVol Version: 0
ComputerVersion : AD Version: 2, SysVol Version: 2
Wmifilter   :
```

Figure 3.16: Disabling Windows real-time protection

4. Next, turn off Windows Defender Antivirus by using the following commands:

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\Windows Defende
```

The following screenshot shows the execution of the preceding commands:



```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\Windows Defender" -ValueName "DisableAntiSpyware" -Type DWORD -Value 1

DisplayName : DisableAVGPO
DomainName  : redteamlab.local
Owner       : REDTEAMLAB\Domain Admins
Id          : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus   : AllSettingsEnabled
Description : This GPO disables AV on the entire domain
CreationTime : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:29:20 AM
UserVersion : AD Version: 0, SysVol Version: 0
ComputerVersion : AD Version: 3, SysVol Version: 3
Wmifilter   :
```

Figure 3.17: Disabling anti-spyware protection

5. Next, turn off Windows Defender Firewall with the following commands:

```
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall
PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall
```

As shown in the following screenshot, the preceding commands executed successfully:

```

PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall\StandardProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0

DisplayName : DisableAVGPO
DomainName  : redteamlab.local
Owner       : REDTEAMLAB\Domain Admins
Id          : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus   : AllSettingsEnabled
Description  : This GPO disables AV on the entire domain
CreationTime : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:29:54 AM
UserVersion  : AD Version: 0, SysVol Version: 0
ComputerVersion : AD Version: 4, SysVol Version: 4
WmiFilter    :

PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0

DisplayName : DisableAVGPO
DomainName  : redteamlab.local
Owner       : REDTEAMLAB\Domain Admins
Id          : 90b1d9c4-a43f-4712-a05f-cf35fca3edd0
GpoStatus   : AllSettingsEnabled
Description  : This GPO disables AV on the entire domain
CreationTime : 7/21/2023 9:20:06 AM
ModificationTime : 7/21/2023 9:30:04 AM
UserVersion  : AD Version: 0, SysVol Version: 0
ComputerVersion : AD Version: 5, SysVol Version: 5
WmiFilter    :

PS C:\Users\Administrator> Set-GPRegistryValue -Name DisableAVGPO -Key "HKLM\Software\Policies\Microsoft\WindowsFirewall\PublicProfile" -ValueName "EnableFirewall" -Type DWORD -Value 0

DisplayName : DisableAVGPO
DomainName  : redteamlab.local
Owner       : REDTEAMLAB\Domain Admins

```

Figure 3.18: Disabling Windows Firewall

## Part 6 – Setting up for service authentication attacks

In this part of the book, you will learn how to discover file and network sharing resources in a Windows environment. This section demonstrates how to create a network file share on Windows Server 2019 to simulate a vulnerable service that can be exploited by a threat actor.

To get started with this exercise, please use the following instructions:

1. On Windows Server 2019, open the **Windows PowerShell** application with administrative privileges and execute the following commands to create a shared folder on the **C:** drive:

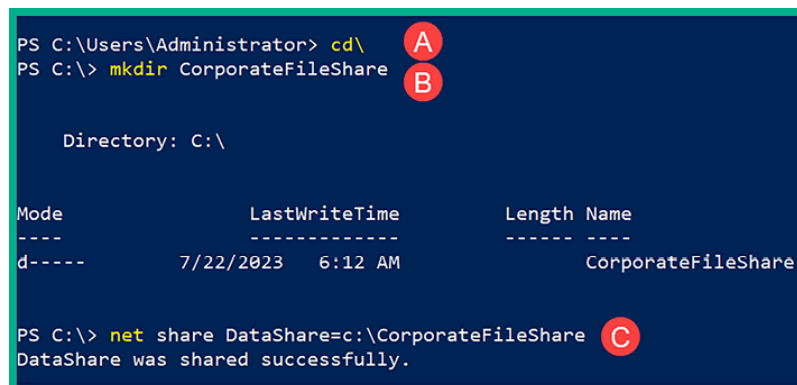
```

PS C:\Users\Administrator> cd \
PS C:\> mkdir CorporateFileShare
PS C:\> net share DataShare=c:\CorporateFileShare

```



The following screenshot shows the execution of the preceding commands:



```

PS C:\Users\Administrator> cd\
PS C:\> mkdir CorporateFileShare

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          7/22/2023   6:12 AM                CorporateFileShare

PS C:\> net share DataShare=c:\CorporateFileShare
DataShare was shared successfully.

```

Figure 3.19: Creating a file share

- Next, we can verify the shared folder by opening the **Server Manager** application and selecting **File and Storage Services** | **Shares**, as shown here:

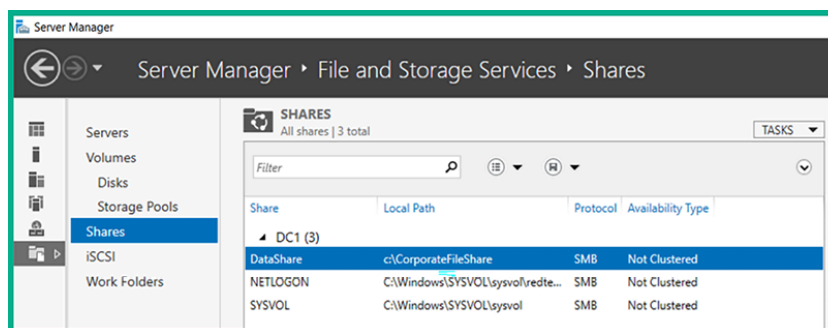


Figure 3.20: Verifying file share

- Next, to ensure we can simulate a cyber-attack to compromise the Kerberos feature on a Windows Server environment, we need to create a **Service Principal Name (SPN)** on our Domain Controller, which is our Windows Server. Open the **Windows PowerShell** application with administrative privileges and execute the following commands:

```
PS C:\> setspn -a DC1/sqladmin.REDTEAMLAB.local:64123 REDTEAMLAB\sqladmin
```

The following screenshot shows the execution of the preceding command to assign the `sqladmin` account as an SPN:

```
PS C:\> setspn -a DC1/sqladmin.REDEAMLAB.local:64123 REDTEAMLAB\sqladmin
Checking domain DC=redteamlab,DC=local

Registering ServicePrincipalNames for CN=sqladmin,CN=Users,DC=redteamlab,DC=local
DC1/sqladmin.REDEAMLAB.local:64123
Updated object
PS C:\>
```

Figure 3.21: Creating an SPN account



To learn more about service principle names on Windows Server, please see <https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names>.

4. Lastly, use the `slmgr /rearm` command on the Windows Server 2019 virtual machine to prevent it from automatically powering off as it's a trial version. Reboot the system to ensure the changes take effect, then power off the virtual machine until it's needed later.

## Part 7 – Installing Windows 10 Enterprise

In this section, you will learn how to set up two Microsoft Windows 10 client systems within the RedTeamLab topology. One virtual machine will be logged on as Bob, while the other user will be logged on as Alice.

To get started with this exercise, please use the following instructions:

1. On your host computer, to download the Windows 10 Enterprise ISO file, go to <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise> and click on **Download the ISO – Enterprise**.
2. Next, complete the registration form and click on the **Download** button, then select **ISO - Enterprise 64-bit edition** as shown below:

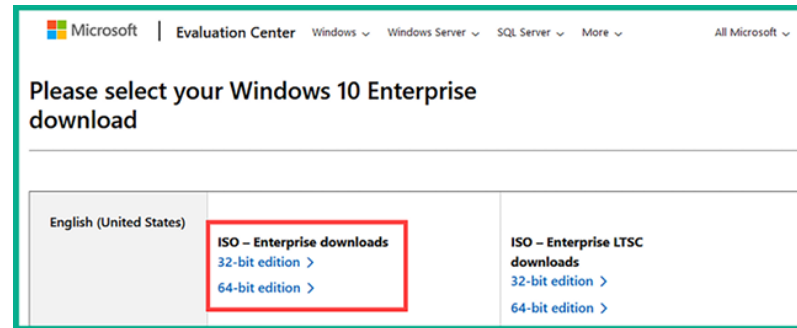


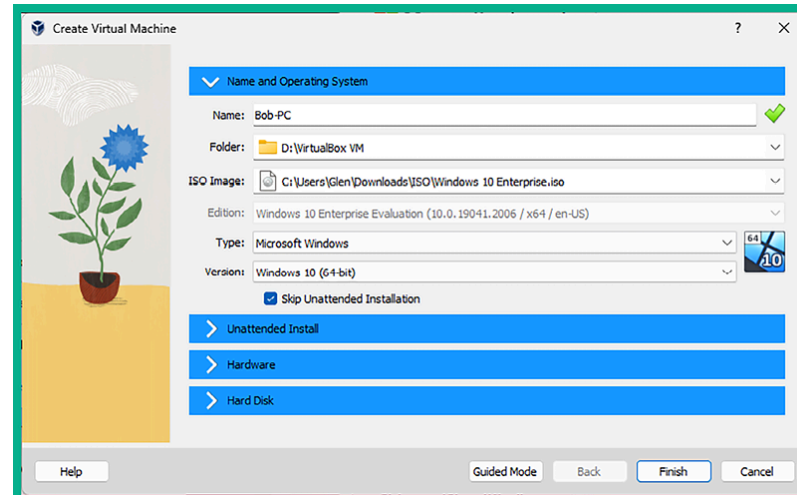
Figure 3.22: Download page for Windows 10

Once the Windows 10 Enterprise ISO file is downloaded onto your host computer, open **Oracle VM VirtualBox Manager** and click on **New** to create a new virtual machine.

3. The **Create Virtual Machine** window will appear. Use the following configurations:

1. **Name:** Bob-PC
2. **ISO Image:** Use the drop-down menu, select **Other**, then select the **Windows 10 Enterprise ISO** file and click on **Open** to attach it
3. **Type:** Microsoft Windows
4. **Version:** Windows 10 (64-bit)
5. **Skip Unattended Installation:** Yes (check the box)

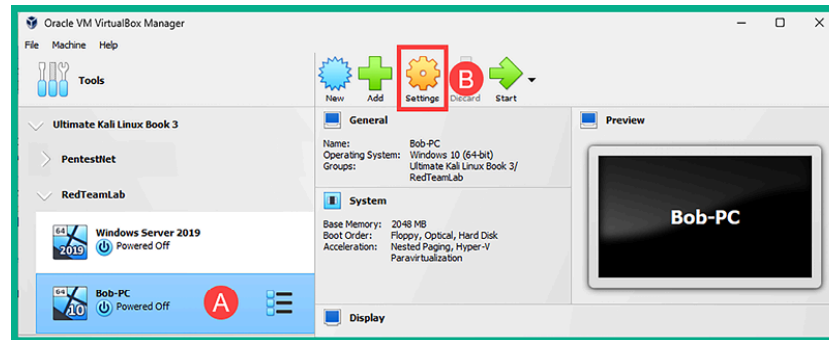
The following screenshot shows the preceding configurations:



*Figure 3.23: Creating a virtual machine*

Once you're all set, click on **Finish** to save the virtual environment.

4. Next, select the **Bob-PC** virtual machine and click on **Settings**, as shown below:

*Figure 3.24: Accessing the Settings menu*

5. Click on the **Network** category and apply the following settings to **Adapter 1**:

1. **Adapter 1: Enable Network Adapter**
2. **Attached to: Internal Network**
3. **Name:** RedTeamLab (manually type it in the field)
4. **Promiscuous Mode: Allow All**

The following screenshot shows the preceding configurations for **Adapter 1**:

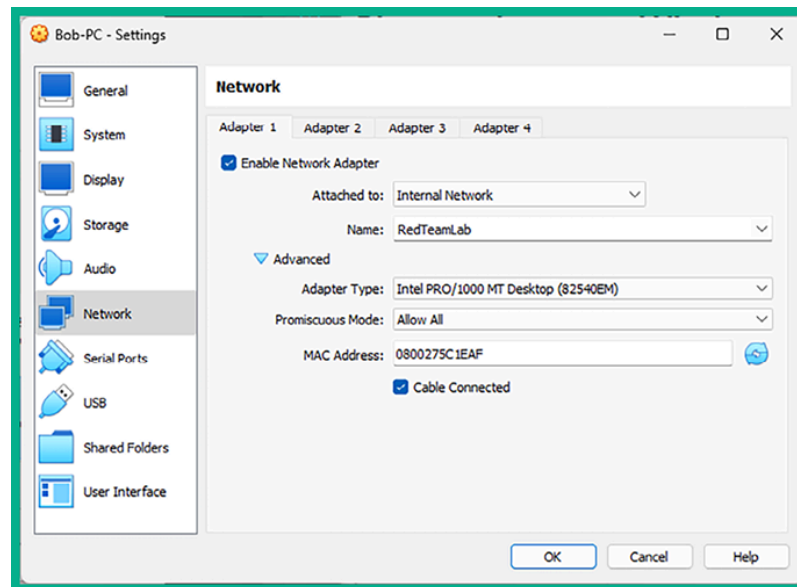


Figure 3.25: Network Adapter 1 configuration

6. Next, select the newly created virtual machine and click on **Start** to power on the system.
7. On the **Windows Setup** window, click on **Next**, then click on **Install now**.
8. Accept the **Applicable notices and license terms** and click on **Next**.
9. For the installation type, click on the **Custom: Install Windows only (advanced)** option.
10. Then, select **Dive 0: Unallocated Space** as it's the only destination storage media within the virtual machine and click on **Next** to start the installation. After the installation is complete, the virtual machine will automatically reboot twice.
11. After the second reboot, you'll be prompted to select your region. Then, click on **Yes**.  
Next, select your keyboard layout, and click on **Yes**. You can skip the option for adding a second keyboard layout.
12. During the setup process of Windows 10, you'll be asked to connect to a network. Select the **I don't have internet** option to continue, as shown below:

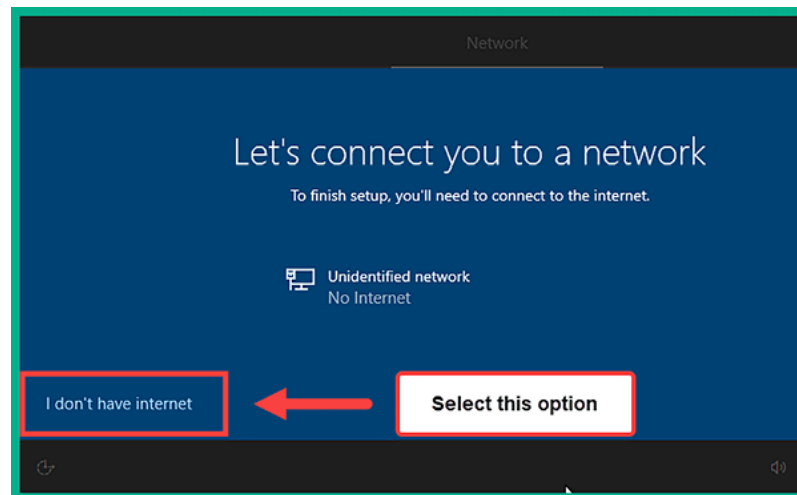


Figure 3.26: Network options

13. Next, click on **Continue with limited setup**.
14. Next, create the username: `bob` with the password: `P@ssword2`.
15. Disable any unnecessary services on the privacy window and disable Cortana. Afterward, the setup process continues and will log you in automatically to the Windows 10 desktop.
16. Install **VirtualBox Guest Additions** on the Windows 10 virtual machine. Please see *Part 2, steps 2–4*.
17. On Bob-PC, open the **Command Prompt** with administrative privileges and turn on network discovery and file sharing using the following commands:

```
C:\Windows\system32> netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes
C:\Windows\system32> netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
```

The following screenshot shows the execution of the preceding commands:

```
C:\Windows\system32> netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes
Updated 52 rule(s).
Ok.

C:\Windows\system32> netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
Updated 30 rule(s).
Ok.
```

*Figure 3.27: Enabling file and printer sharing*

18. Next, use the following commands to change the default hostname to **Bob-PC** :

```
C:\Windows\system32> powershell
PS C:\Windows\system32> Rename-Computer -NewName Bob-PC
PS C:\Windows\system32> Restart-Computer
```

Once this virtual machine is rebooted, the hostname will be Bob-PC, and Windows network and file sharing will be enabled. Power off Bob-PC for now.

19. Next, let's create another Windows 10 virtual machine and call it **Alice-PC**.

Repeat *steps 3 – 20* and ensure you set **Alice-PC** as both the name of the new virtual machine (*step 4*) and the hostname (*step 20*). Create the username **alice** with the password **P@ssword2** as the local user during the setup process.

## Part 8 – Adding the clients to the domain

Use the following instructions to join/add each Windows 10 virtual machine, Bob-PC and Alice-PC, to the Active Directory database on the Domain Controller and allow them to participate as domain members:

1. Power on the **Windows Server 2019** virtual machine, **Bob-PC**, and **Alice-PC**.
2. On **Bob-PC** and **Alice-PC**, open the Command Prompt with administrative privileges (**Run As Administrator**) and use the `ping 192.168.42.40` command to test network connectivity between each Windows 10 system and the Windows Server 2019 machine, as shown below:

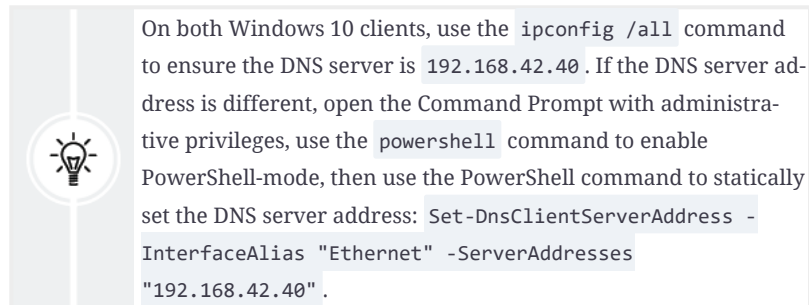
```
C:\Windows\system32> ping 192.168.42.40

Pinging 192.168.42.40 with 32 bytes of data:
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128
Reply from 192.168.42.40: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.42.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

*Figure 3.28: Testing connectivity to the Domain Controller*

As shown in the preceding screenshot, **Bob-PC** was able to communicate with the **Windows Server 2019** virtual machine successfully.



3. Next, use the following commands on **Bob-PC** and **Alice-PC** to join the `redteamlab.local` domain:

```
C:\Windows\system32> powershell
PS C:\Windows\system32> Add-Computer -DomainName RedTeamLab.local -Restart
```

4. Next, the **Windows PowerShell credentials request** window will appear. Simply enter the domain administrator account (`Administrator / P@ssword1`) to authenticate the request and click on **OK**, as shown below:



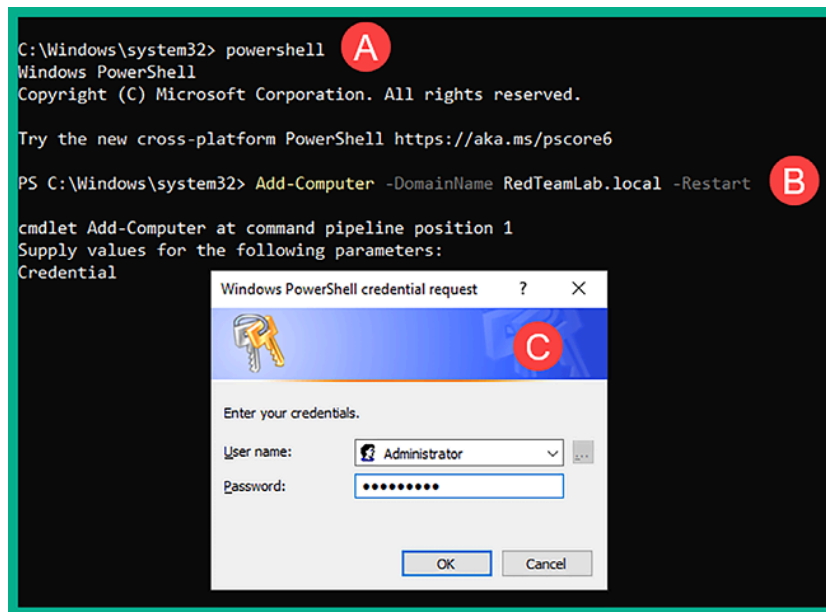


Figure 3.29: Joining a domain

5. Once the system has rebooted, click on **Other user** in the bottom-left corner of the login window and log in using a domain user account, such as username `gambit` or `rogue` with the password `Password1`, as shown below:

Figure 3.30: Log in as a domain user

## Part 9 – Setting up for account takeover and file sharing attacks

To ensure we can exploit file-sharing services and perform account takeover attacks on Windows clients that are connected to the domain, please use the following instructions:

1. Log in to **Bob-PC** and **Alice-PC** using a domain administrator account, such as username `redteamlab\Administrator` and password `P@ssword1`, as shown below:

*Figure 3.31: Log in as domain Administrator*

2. Open the **Command Prompt** with administrative privileges and use the following commands to make the domain user accounts, `gambit` and `rogue`, local administrators on **Bob-PC** and **Alice-PC**:

```
C:\Users\Administrator> net localgroup "Administrators" redteamlab\gambit /ADD  
C:\Users\Administrator> net localgroup "Administrators" redteamlab\rogue /ADD
```

The following screenshot shows the execution of the preceding commands:

*Figure 3.32: Adding users to local admin group*

3. Next, using the same **Command Prompt** window, use the following commands to create a local shared folder on each Windows 10 machine, **Bob-PC** and **Alice-PC**:

```
C:\Users\Administrator> cd\  
C:\> mkdir SharedData  
C:\> net share DataShare=c:\SharedData
```

The following screenshot shows the execution of the preceding commands:

*Figure 3.33: Creating a shared folder*

4. Lastly, power down your Windows 10 and Windows Server 2019 virtual machines until they are needed later on.

Having completed this section, you have built a Microsoft Windows lab environment containing the most common type of services and configurations found in many organizations. This environment will enable you to perform advanced exploitation techniques on Active Directory in later sections of this book that focus

on red team exercises. In the next section, you will learn how to set up a wireless penetration testing lab to practice wireless exploitation.

## Setting up a wireless penetration testing lab

Understanding how to perform wireless penetration testing helps organizations to determine how a real threat actor is able to discover and exploit security vulnerabilities in their company's wireless network infrastructure. Let's first have a quick overview of wireless networks and the associated security standards and access methods.

### Brief overview of wireless network security

Within many organizations, you will commonly find wireless networks that are implemented to support wireless mobility for their employees. Employees can connect their smartphones, **Internet of Things (IoT)** devices, tablets, and laptops to the corporate Wi-Fi network and access the resources on the wired network, such as printers and servers. In small and large organizations, the wireless router or access point is usually configured using one of the following wireless security standards:

- **Wired Equivalent Privacy (WEP)**
- **Wi-Fi Protected Access (WPA)**
- **Wi-Fi Protected Access 2 (WPA2)**
- **Wi-Fi Protected Access 3 (WPA3)**

Most modern wireless networks are usually configured with WPA2 and WPA3 standards. The preceding list of security standards is also designed for small networks and the regular consumer as they are simple to configure using a single shared password, known as a **Pre-Shared Key (PSK)**. Therefore, anyone who wants to access the wireless network will need the same PSK.

In large environments, it is necessary to improve the security and centralized management of users on the corporate wireless network. Security professionals typically implement an **Authentication, Authorization, and Accounting (AAA)** server such as **Remote Authentication Dial-In User Service (RADIUS)** on the network, which handles the centralized management of network users, accounts, and policies.

The following is a brief explanation of AAA:

- **Authentication:** Verifies the identity of users by requiring valid credentials before granting access to the network.
- **Authorization:** Determines user privileges or access levels after authentication, ensuring users only access resources appropriate to their roles.
- **Accounting:** Keeps track of user activities on the network, providing valuable information for auditing, billing, or reporting purposes.

The following are the access methods for wireless networks:

- **Pre-Shared Key (PSK)** – This method enables you to configure a password or passphrase on the wireless router or access point. Anyone with the PSK can access the network.
- **Enterprise** – This method leverages a centralized access server running RADIUS to handle AAA. Each user on the wireless network will require a unique user account to be created on the access server, with policies assigned to the account, and logs are generated for accountability.
- **Wi-Fi Protected Setup (WPS)** – This access method removes the need for using passwords and passphrases on the wireless network. It provides an easy method to authenticate to the wireless network using an 8-digit PIN. However, there are known security vulnerabilities and attacks on retrieving the WPS PIN.

Next, you will learn how to set up a wireless penetration testing lab environment that supports security testing for both personal and enterprise wireless networks.

## Setting up a RADIUS server

In this section, we will be leveraging the power of virtualization to set up a RADIUS server, such as FreeRadius, on our network to handle the AAA processes of the wireless router for testing WPA2-Enterprise. We will demonstrate how to set up RADIUS on top of an Ubuntu server as a virtual machine on your computer and associate it with a wireless router or access point.

You will need a wireless router or access point that supports WPA2-Personal for security testing on newer security standards, and WPA2-Enterprise for security testing of enterprise wireless networks. In addition, having a wireless router that supports WPA3 will be beneficial for learning how to compromise WPA3-targeted networks.

The following diagram shows the wireless penetration testing lab environment:

*Figure 3.34: Wireless network topology*

As shown in the preceding diagram, the RADIUS server (access server) and wireless router/access point are connected to an organization's internal network. Therefore, if an attacker is able to compromise the wireless network, the adversary will gain unauthorized access to the corporate network and perform lateral movement.

To get started with this exercise, please follow the instructions in the subsequent sections.

## Part 1 – Install a Ubuntu server

To get started with setting up an Ubuntu server for hosting our RADIUS service, please use the following instructions:

1. Firstly, you'll need to download and set up Ubuntu Server as a virtual machine. On your host machine, go to <https://ubuntu.com/download/server> to download the **Ubuntu Server 22.04 LTS** ISO image.
2. Next, open **Oracle VM VirtualBox Manager** and click on **New** to create a new virtual machine.
3. In the **Create Virtual Machine** window, ensure you use the following configurations:
  1. **Name: Radius Server**
  2. **ISO Image:** Use the drop-down menu, select **Other**, then select the **Ubuntu Server ISO file**
  3. **Type: Linux**
  4. **Version: Ubuntu (64-bit)**
  5. **Skip Unattended Installation:** Check the box

The following screenshot shows the preceding configurations:

*Figure 3.35: Creating a new virtual machine*

4. After clicking on **Finish** to save the new virtual machine, select the **Radius Server** virtual machine and click on **Settings**.

5. On the **Settings** windows, select the **Network** category and use the following configurations for **Adapter 1**:
  1. Enable the Network Adapter
  2. **Attached to: Bridged Adapter**
  3. **Name**: Use the drop-down menu to select your physical network adapter on your host machine that's connected to your physical network
6. Next, power on the **Radius Server** virtual machine to start the installation process of Ubuntu Server.
7. In the installation window, select the **Try or Install Ubuntu Server** option to start the installation process.
8. Next, select your preferred language and hit *Enter*.
9. Next, select your preferred keyboard configuration and select **Done**.
10. For **Choose type of install**, select **Ubuntu Server** and select **Done**.
11. Next, in the **Network connection** menu, an IP address will automatically be assigned to this Ubuntu Server from your network. Ensure you make a note of the address and select **Done**.
12. In the **Configure proxy** menu, leave it as the default and select **Done**.
13. In the **Configure Ubuntu archive mirror** menu, leave it as the default and select **Done**.
14. In the **Guided storage configuration** menu, leave it as the default and select **Done**.
15. In the **Storage configuration** menu, leave it as the default and select **Done**.
16. When the **Confirm destructive action** window appears, select **Continue**.
17. In the **Profile setup** menu, create a user account for yourself and select **Done**.
18. In the **Upgrade to Ubuntu Pro** menu, leave it as the default and select **Continue**.
19. In the **SSH Setup** menu, use the spacebar on your keyboard to select the **Install OpenSSH server** option, then select **Done**.
20. Next, the **Featured Server Snaps** menu will appear. Leave it as the default and select **Done**.

The installation process will take some time to complete as it will attempt to automatically download and install updates. After this process is complete, select **Reboot Now**.



After the reboot, if there's an error in automatically ejecting the ISO file from the CD-ROM drive, simply hit *Enter* on the console screen to continue.

## Part 2 – Setting up FreeRadius

In this section, you will learn how to set up FreeRadius on the Ubuntu server and create user accounts for users on the wireless network.

Please use the following instructions to get started with this exercise:

1. Ensure the **Radius Server** virtual machine is running in **Oracle VM VirtualBox Manager**.
2. Next, on your Windows host machine, open the Windows **Command Prompt** application and use the following commands to remotely connect to the virtual machine:

```
C:\Users\Glen> ssh <yourname>@<server-ip-address>
```

The following screenshot shows the expected output when executing the preceding commands:

*Figure 3.36: Remote access using SSH*



Keep in mind that passwords are invisible when you're entering them on a terminal interface for security reasons.

3. Next, use the following commands to update the local package repository list and install FreeRadius:

```
glen@radius:~$ sudo apt update
glen@radius:~$ sudo apt install freeradius
```

After executing the preceding commands, you'll be prompted to enter **Y/n**. Simply enter **Y** to continue. The following screenshot shows the execution of the preceding commands:

*Figure 3.37: Installing FreeRadius*

4. Next, use the following commands to verify the sub-directories of FreeRadius:

```
glen@radius:~$ sudo ls -l /etc/freeradius/3.0/
```

The following screenshot shows the list of files and directories within the `3.0` folder:

Figure 3.38: Listing files



The `users` file contains the user credentials, while the `clients.conf` file contains the AAA client accounts, such as the wireless router within our lab topology.

5. Next, let's use the Nano command-line text editor to modify the `users` file and create a user account:

```
glen@radius:~$ sudo nano /etc/freeradius/3.0/users
```

Using the directional keys on your keyboard, find the following line:

```
#bob    Cleartext-Password := "hello"
```

Then uncomment the line by removing the `#` symbol and change the password from `hello` to `password123`, as shown below:

Figure 3.39: Creating user account

6. Next, save the file by pressing `CTRL + X`, then `Y` and `Enter`.

7. Next, let's create a client account for the wireless router. Use the following commands to edit the `clients.conf` file:

```
glen@radius:~$ sudo nano /etc/freeradius/3.0/clients.conf
```



8. Using the directional keys, go to the **Defines a RADIUS client** section and insert the following code, which defines the RADIUS client (wireless router):

```
client 172.16.17.123 {  
    secret = radiusclientpassword1  
    shortname = corporate-ap  
}
```

The following screenshot shows the preceding code within the `clients.conf` file:

*Figure 3.40: Creating client account*

The client IP address ( 172.16.17.123 ) is the IP address of the wireless router. Please ensure you check the IP address of your wireless router and substitute the one in the preceding code. If the client IP address is not the same as your wireless router, the user (Bob) will not be able to authenticate to the RADIUS server.

Press `CTRL + X`, then `Y` and `Enter` to save the file.

9. Next, use the following commands to restart the FreeRadius service and verify its status:

```
glen@radius:~$ sudo systemctl restart freeradius  
glen@radius:~$ sudo systemctl status freeradius
```

The following screenshot shows the `freeradius` service is active and running:

*Figure 3.41: Restarting the FreeRadius service*

10. Additionally, use the `sudo lsof -i -P -n | grep freerad` command to verify ports 1812 and 1813 are open for the FreeRadius services, as shown below:

*Figure 3.42: Checking open ports*

## Part 3 – Setting the wireless router with RADIUS

This section will show you how to configure a wireless router to operate a RADIUS server on the network. For this section, you will need a physical wireless router that supports the WPA2-Personal and WPA-Enterprise security modes.

The following diagram shows the IP addresses of the RADIUS server and wireless router. Keep in mind the IP addresses may be different on your personal network:

*Figure 3.43: Wireless network topology*

To get started configuring the wireless router with RADIUS, please use the following guidelines:

1. Power on the wireless router and log in to the management dashboard.
2. Next, go to the **Wireless** tab and change the **Network Name (SSID)** to `Target_Net`, as shown below:

*Figure 3.44: Wireless router configurations*

3. Next, in the **Wireless Security** menu, use the following configuration to enable the wireless router to query the RADIUS server on the network:
  1. **Security Mode:** WPA2-Enterprise
  2. **Encryption:** AES
  3. **RADIUS Server:** Enter the IP address of the RADIUS server virtual machine
  4. **RADIUS Port:** 1812
  5. **Shared Secret:** radiusclientpassword1

The following screenshot shows the preceding configurations when applied to the wireless router:

Figure 3.45: Wireless router security configuration

Keep in mind that you need to ensure the IP address on your wireless router matches the IP address within the `clients.conf` file on the RADIUS server and that the IP address of the RADIUS server matches the IP address on the wireless security configuration on the wireless router.

Having completed this section, you have learned how to set up a wireless penetration testing lab environment to perform advanced penetration testing techniques.

## Summary

In this chapter, you have gained the hands-on skills to build a Windows environment that simulates a typical enterprise organization with domain users, various service accounts, administrators, and shared network resources. Additionally, you have learned how to create a wireless network lab that contains a RADIUS server to provide AAA services, which help replicate an enterprise wireless network within a large organization. These lab environments will be utilized later in this book when you learn about advanced penetration testing techniques such as red team exercises.

I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path toward becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Chapter 3, Setting Up for Advanced Penetration Testing Techniques*, you will learn how to perform **Open Source Intelligence (OSINT)** to passively collect sensitive information on a target.

## Further reading

- Active Directory Domain Services: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100->
- Wireless security standards: <https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2>
- Understanding FreeRadius: <https://www.techtarget.com/searchsecurity/definition/RADIUS>

## Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

<https://packt.link/SecNet>

