



Course: CYB301 Security Defense and
Response (Canadian Context)

Lab 5: Firewall Rules, GPO, and Threat Analysis

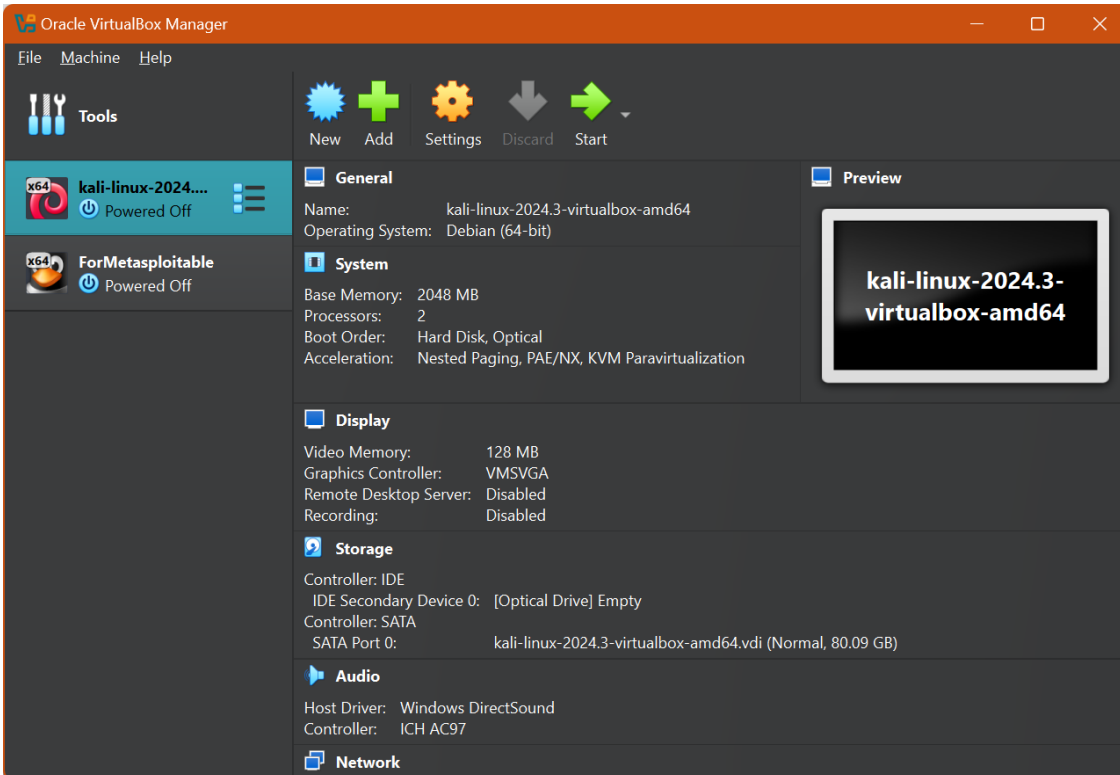
Coordinator and Instructor: Muhammad
Siddiqui

Student: Saiprasad Raman – 23074624
Preetika
Komal

Setting Up a Kali and Metasploitable Learning Environment Using VirtualBox

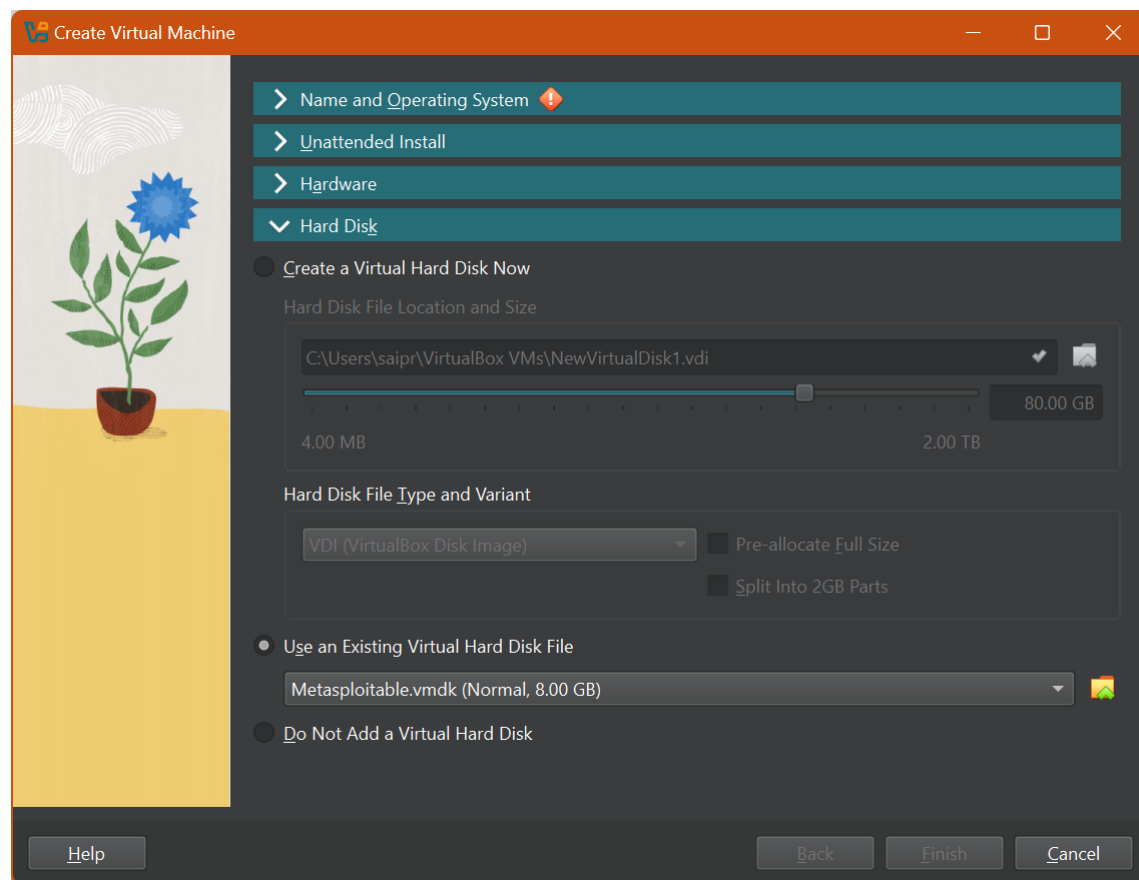
To add the Kali Linux virtual machine:

- Choose **File**, then **Import Appliance**. Navigate to the directory where you downloaded the Kali VM and import the virtual machine. Follow the wizard as it guides you through the import process, and when it is complete, you can continue with these instructions.



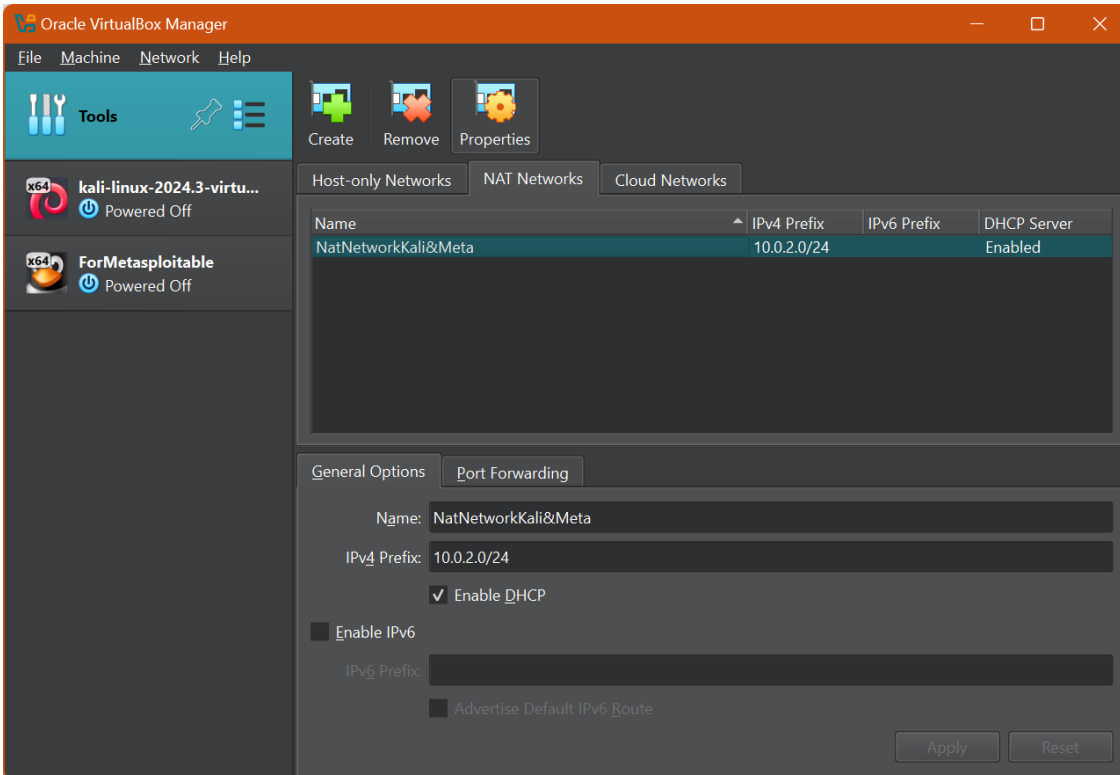
To add the Metasploitable virtual machine:

- The Metasploitable virtual machine comes as a zip file, so you will need to extract it first. Inside, you will see a VMDK instead of the OVA file that VirtualBox uses for its native virtual machines. This means you have to do a little more work.
 1. Click **New** in the VirtualBox main window.
 2. Click **Expert Mode** and name your system; then select Linux for the type. You can leave the default alone for Version, and you can leave the memory default alone as well.
 3. Select **Use An Existing Virtual Hard Disk File** and navigate to the location where you unzipped the Metasploitable.vmdk file to and select it. Then click **Create**.

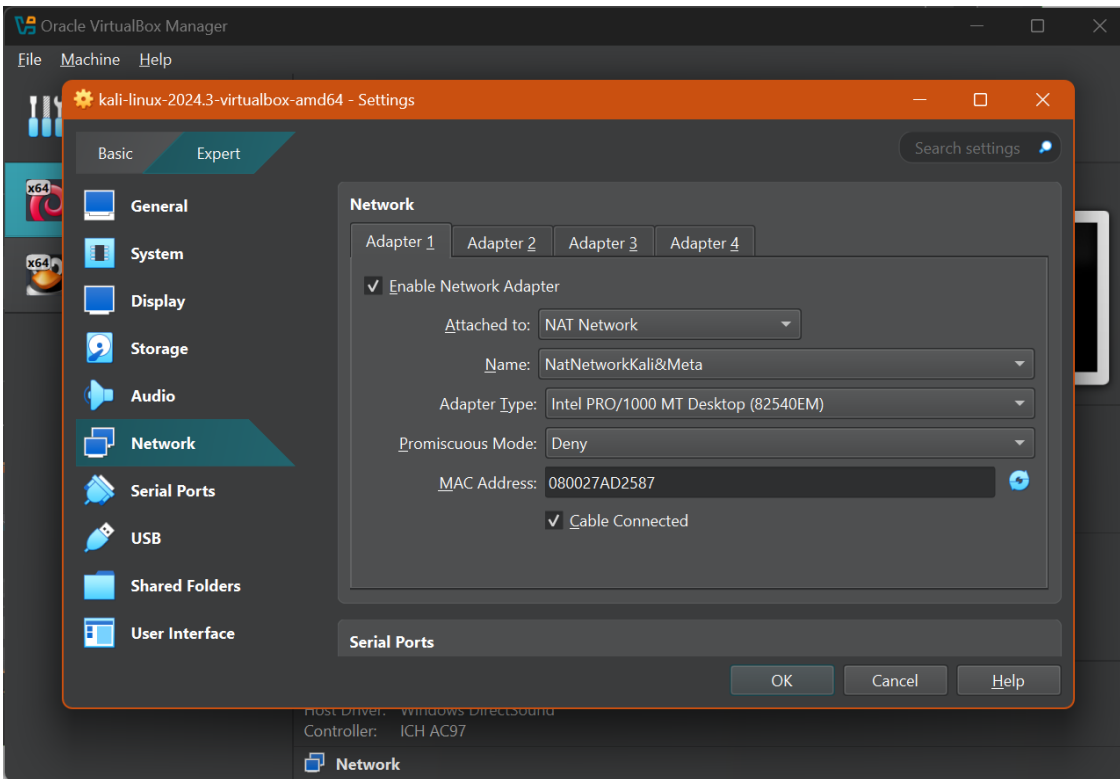


- Now that you have both virtual machines set up, you should verify their network settings. VirtualBox allows multiple types of networks.

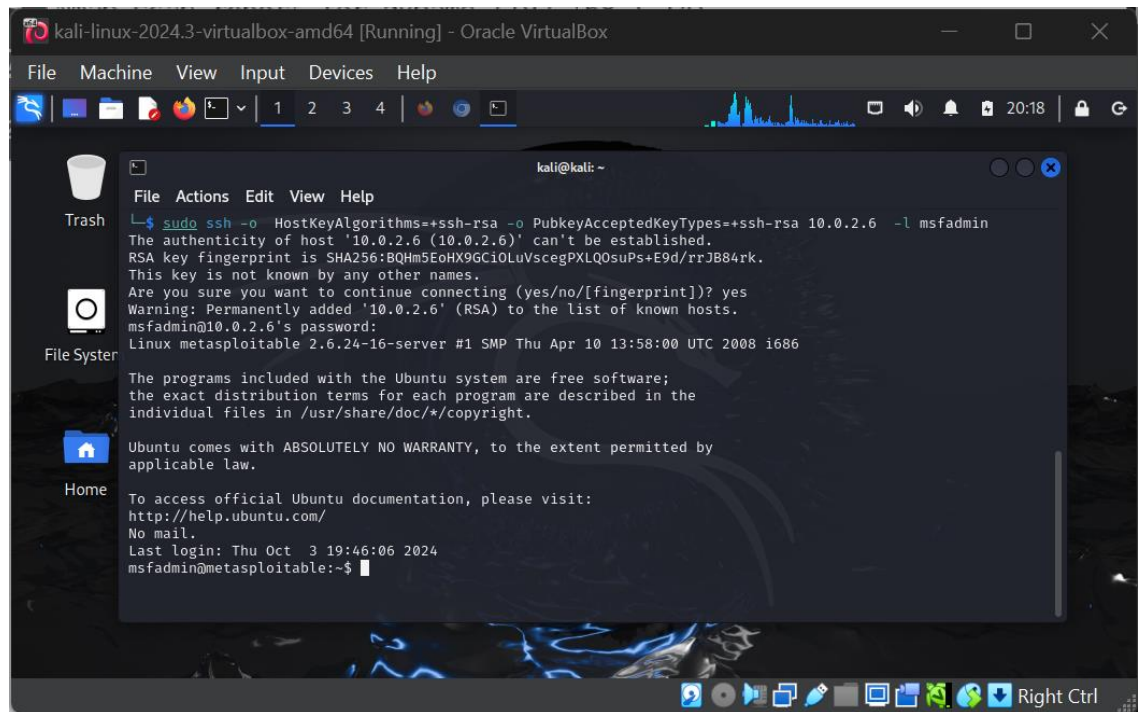
You may want to have internet connectivity for some exercises, or to update software packages. If you are reasonably certain you know what you are doing, using a NAT Network can be very helpful. To do so, you will need to click the **File > Preferences** menu of VirtualBox; then select **Network** and set up a NAT network, by clicking the network card with a + icon.



- Once your NAT network exists, you can set both machines to use it by clicking on them, then clicking the **Settings** gear icon in the VirtualBox interface. From there, click **Network**, and set the network adapter to be attached to the NAT network you just set up.



6. Now you are all set! You can start both machines and test that they can see each other. To do this, simply log in to the Metasploitable box and run **ifconfig** to find its IP address. Use SSH to connect from the Kali Linux system to the Metasploitable system using **ssh [ip address] -l msfadmin**. If you connect and can log in, you are ready to run exercises between the two systems!



The screenshot shows a Kali Linux terminal window titled "kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox". The terminal displays the output of the command `sudo ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa 10.0.2.6 -l msfadmin`. The output shows the SSH connection process, including the host key fingerprint and the user login prompt. The user `msfadmin` is successfully logged in to the `metasploitable` machine. The terminal also shows the Ubuntu system's default messages, including the warranty disclaimer and the official Ubuntu documentation link.

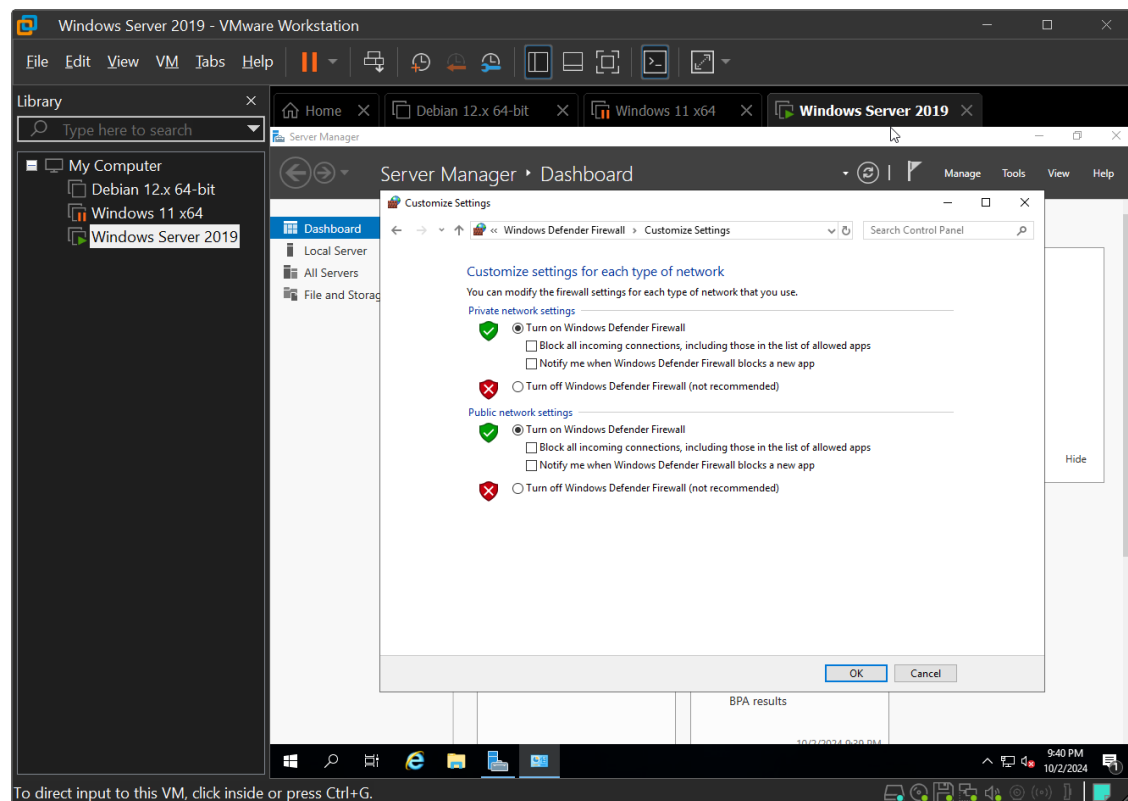
```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa 10.0.2.6 -l msfadmin  
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.  
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.2.6' (RSA) to the list of known hosts.  
msfadmin@10.0.2.6's password:  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
Last login: Thu Oct 3 19:46:06 2024  
msfadmin@metasploitable:~$
```

Activity 1: Create an Inbound Firewall Rule

In this lab, you will verify that the Windows Defender Firewall is enabled on a server and then create an inbound firewall rule that blocks file and printer sharing.

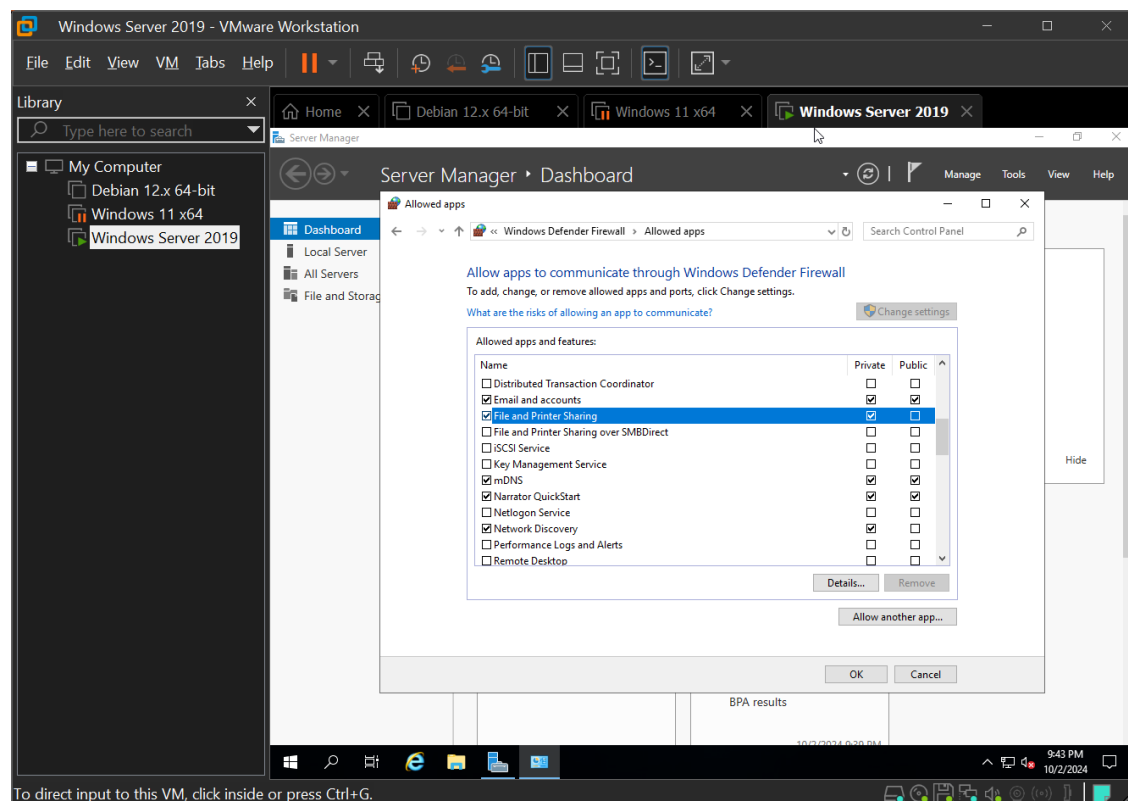
Part 1: Verify that Windows Defender Firewall is enabled.

1. Open the Control Panel for your Windows Server.
2. Choose **System and Security**.
3. Under Windows Defender Firewall, click **Check Firewall Status**.
4. Verify that the Windows Defender Firewall state is set to On for Private networks. If it is not on, enable the firewall by using the “Turn Windows Defender Firewall on or off” link on the left side of the window. **Take the screenshot.**



Part 2: Create an inbound firewall rule that allows file and printer sharing.

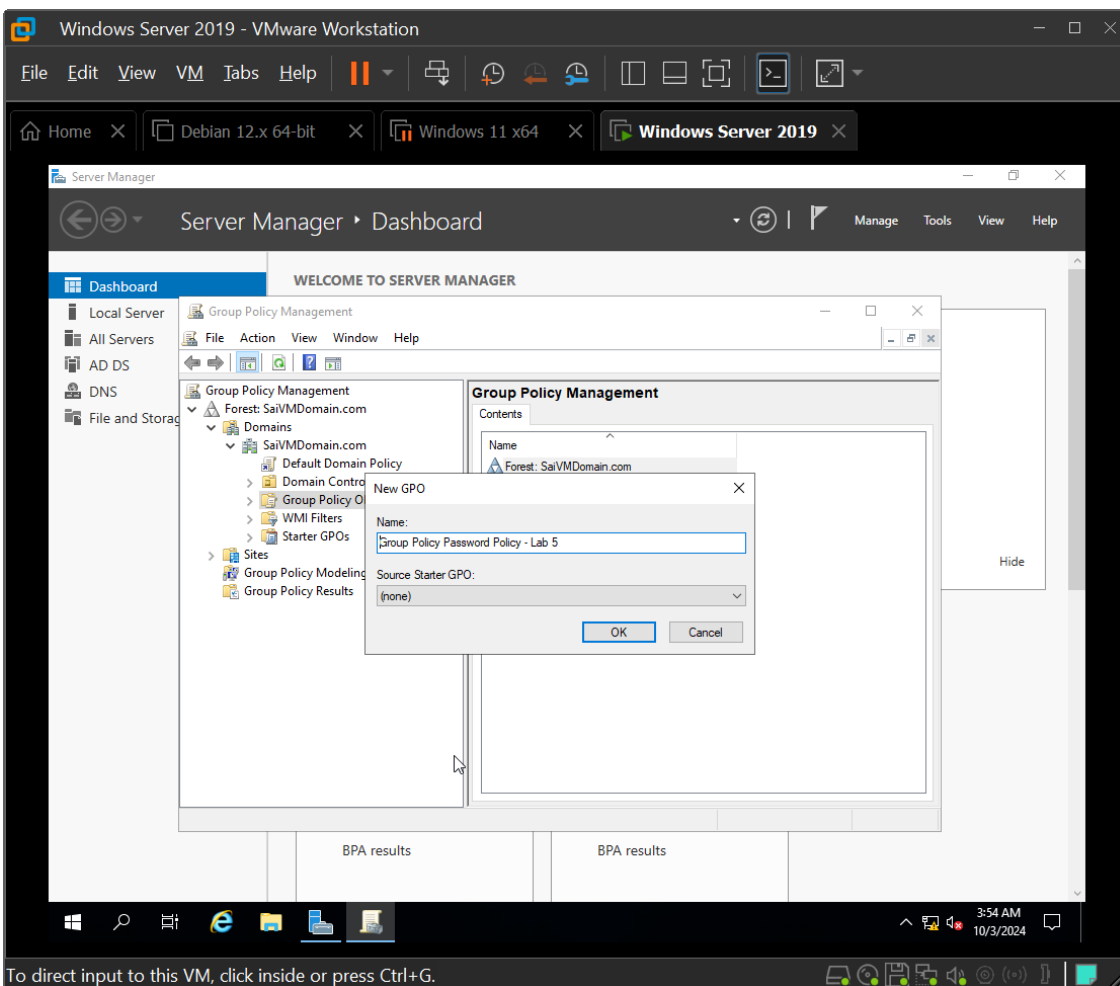
1. On the left side of the Windows Defender Firewall control panel, click **Allow an app or feature through Windows Defender Firewall**.
2. Scroll down the list of applications and find File and Printer Sharing.
3. Check the box to the left of that entry to block connections related to File and Printer Sharing.
4. Notice that the Private box to the right of that option was automatically selected. This allows File and Printer Sharing only for other systems on the same local network. The box for public access should be unchecked, specifying that remote systems are not able to access this feature. **Take the screenshot.**
5. Click **OK** to apply the setting.



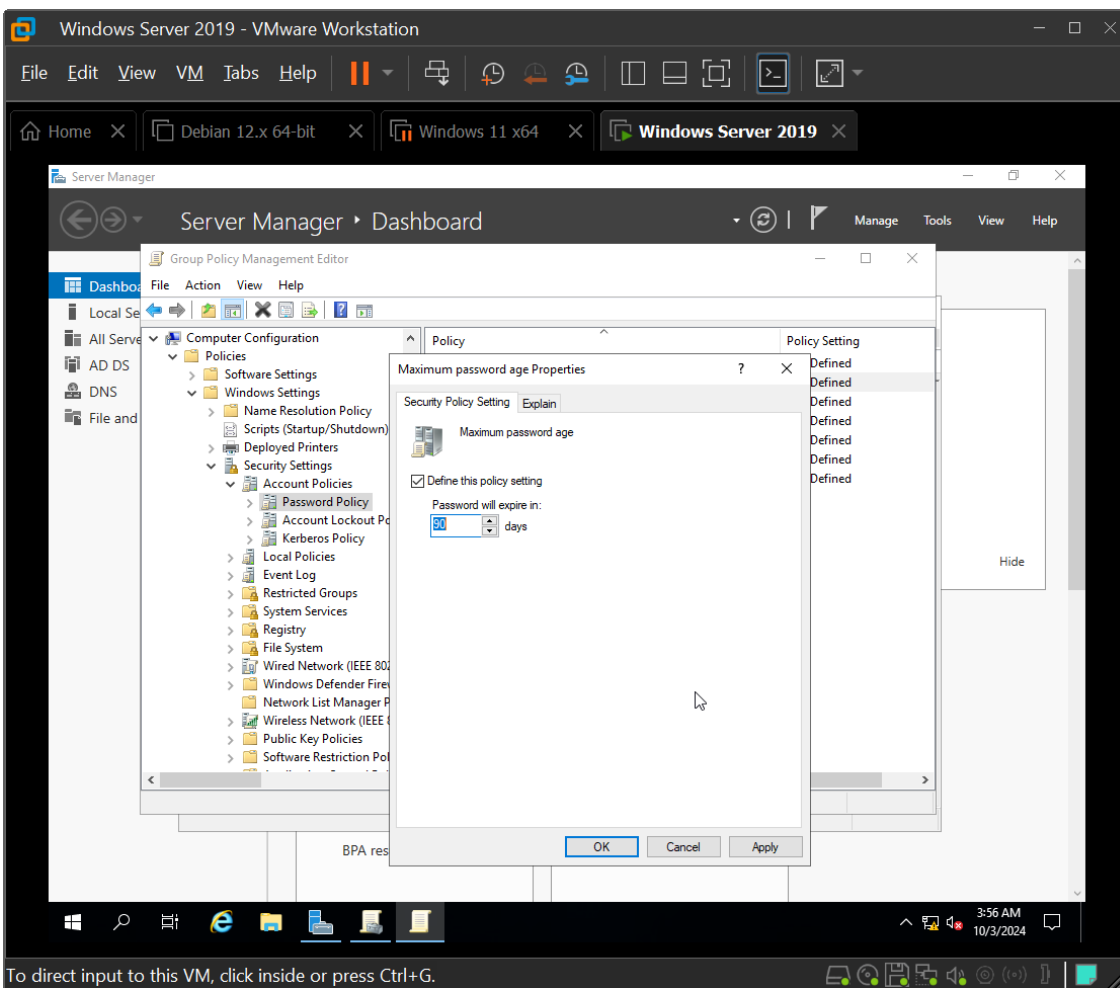
Activity 2: Create a Group Policy Object (GPO)

In this activity, you will create a Group Policy Object and edit its contents to enforce an organization's password policy.

1. Open the Group Policy Management Console. (If you do not find this console on your Windows Server, it is likely that it is not configured as a domain controller.)
2. Expand the folder corresponding to your Active Directory forest.
3. Expand the Domains folder.
4. Expand the folder corresponding to your domain.
5. Right-click the **Group Policy Objects** folder and click **New** on the pop-up menu.
6. Name your new GPO Password Policy. **Take the screenshot** and click **OK**.

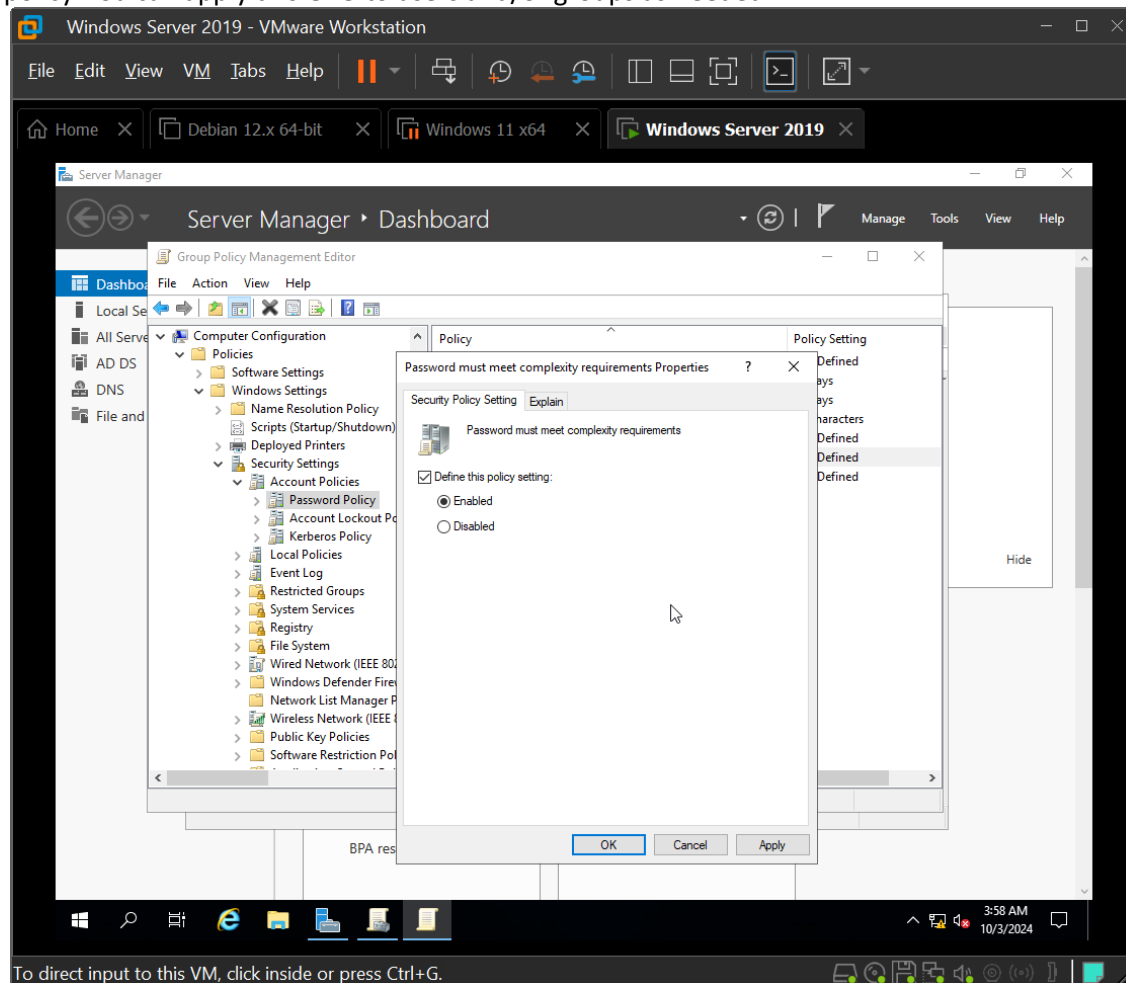


7. Click on the **Group Policy Objects** folder.
8. Right-click the new **Password Policy GPO** and choose **Edit** from the pop-up menu.
9. When Group Policy Editor opens, expand the Computer Configuration folder.
10. Expand the Policies folder.
11. Expand the Windows Settings folder.
12. Expand the Security Settings folder.
13. Expand the Account Policies folder.
14. Click **Password Policy**.
15. Double-click **Maximum Password Age**.
16. In the pop-up window, select the **Define This Policy Setting** checkbox and set the expiration value to 90 days. **Take the screenshot.**



17. Click **OK** to close the window.
18. Click **OK** to accept the suggested change to the minimum password age.
19. Double-click the **Minimum Password Length** option.
20. As in the prior step, click the box to define the policy setting and set the minimum password length to 12 characters.
21. Click **OK** to close the window.
22. Double-click the **Password Must Meet Complexity Requirements** option.
23. Click the box to define the policy setting and change the value to Enabled. **Take the screenshot.**
24. Click **OK** to close the window.
25. Click the **X** to exit Group Policy Editor.

You have now successfully created a Group Policy Object that enforces the organization's password policy. You can apply this GPO to users and/or groups as needed.



Activity 3: Explore the ATT&CK Framework

In this exercise, you will use the ATT&CK framework to analyze a threat. You may want to select a recent compromise that you have seen in the news, or one that has impacted an organization that you have worked with. If nothing comes to mind, the 2019 Capital One data breach offers a useful example, and you can find details of the exploit in multiple places with a quick search.

Part 1: Build a threat profile.

1. List what you know about the compromise or exploit, including details about the threat actor, what occurred, what tools were used, and as many other details as you can find.

Ans.

An unauthorized access to Capital One's data was found on July 19, 2019 which involved access of personal information of over 100 million individuals.

Threat actor:

Performed by Paige Thompson a former AWS employee who had access to the AWS services of Capital One.

Tools Used:

AWS Services. Created a scanning tool to scan cloud infrastructure.

2. Review your list against the headings for the appropriate ATT&CK matrix. Do you have items that match the headings?

Ans.

ATT&CK Category	Details from the Breach
Initial Access	Misconfigured WAF called Modsecurity WAF being exploited
Execution	Created a scanning tool to scan cloud infrastructure and find misconfigured firewalls.
Persistence	N/A
Privilege Escalation	Access to discreet information without authorization
Defense Evasion	Exploited cloud service misconfigurations
Credential Access	Temporary credentials of the AWS platform were
Discovery	Discovered data stored in S3 buckets of AWS
Lateral Movement	N/A
Collection	30 GB of customer data across 700 different S3 buckets
Exfiltration	Transferred data from AWS to external site
Impact	Information leak of over 100 millions of individuals

Part 2: Analysis

Now that you have your basic profile, follow the detailed listings in the matrix to match up the threat to its ATT&CK techniques, threat actors, and other details.

1. Match each data point to the appropriate ATT&CK entry.

Ans.

Data Point	ATT&CK Technique	ATT&CK ID
Run commands on AWS CLI	Command-Line Interface	T1059
Access to personal information	Data from Information Repositories	T1213
Data collected from S3 buckets	Data Staged	T1074
Transferred data from to external site	Exfiltration over Command and Control Channel	T1041
Exploited misconfigured WAF	Exploitation of Public-Facing Application	T1190
Access to information without authorization	Access Token Manipulation	T1134

2. Review the details of each entry so that you become familiar with them.

Ans.

- T1059 – Command-Line interface: Used valid credentials to run commands on CLI.
- T1213 – Data from Information Repositories: Accessed information of over 100 million individuals.
- T1074 - Data Staged: Data were being collected from the S3 buckets of AWS
- T1041 – Exfiltration over Command and Control Channel: Data was copied to an different site.
- T1190 – Exploitation of Public-Facing Application: Misconfigured WAF which is a part of an AWS service.
- T1134 – Access Token Manipulation: Unauthorized access to credentials

3. Identify gaps in your knowledge. What information would you look for if you were researching this threat? What information do you think you could reasonably obtain, and what might you be unable to gather?

Ans.

Gaps in knowledge:

What specific policies were not put in place that led to this attack.

Information Obtained:

- High level knowledge of how the attack was carried out.
- Resolutions and fines on Capital One.

Information Unobtained:

- The commands used to exfiltrate the network.
- Precautions taken to avoid such attacks in the future.

4. Consider what your report on leadership would contain based on what you have found. What would you include for a technical group, and what would you include for senior leaders like a CIO or CEO?

Ans.

Technical Group:

- Future configurations of network and cloud services
- Security infrastructure and monitoring capabilities.

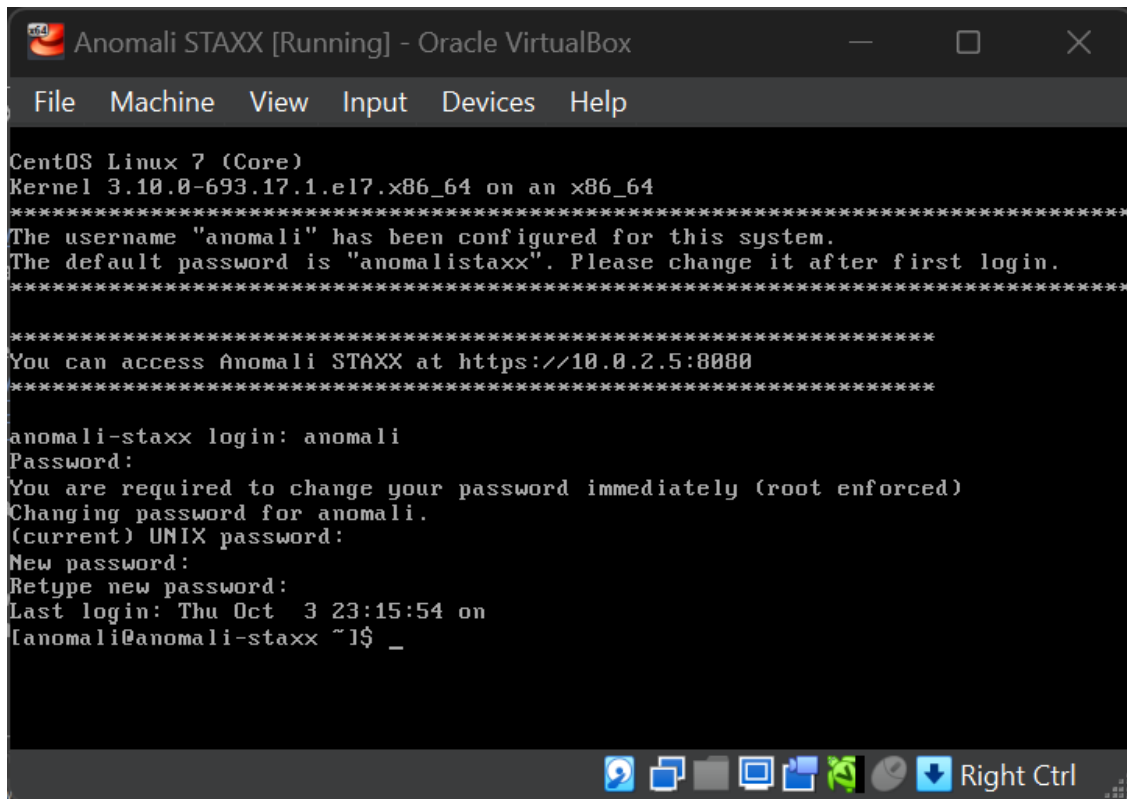
Senior Leaders:

- Invest in the technical teams to put proper security in place.
- Make sure GDPR or CCPA guidelines are met.

Activity 4: Set up a STIX/TAXII Feed

Anomali's STAXX community version provides an easy way to consume STIX feeds. In this exercise, you will download and install the STAXX client, and then review the data from one of the included feeds.

1. Visit www.anomali.com/community/staxx and download the STAXX Community edition software. STAXX is a 1 GB download and requires an email to get the download link.
2. Install the STAXX client. You will need a virtualization environment like VirtualBox or VMWare to open the OVA file. Follow the Anomali setup and installation guide at https://update.anomali.com/staxx/docs/Anomali_STAXX_Installation_&Administration_Guide.pdf



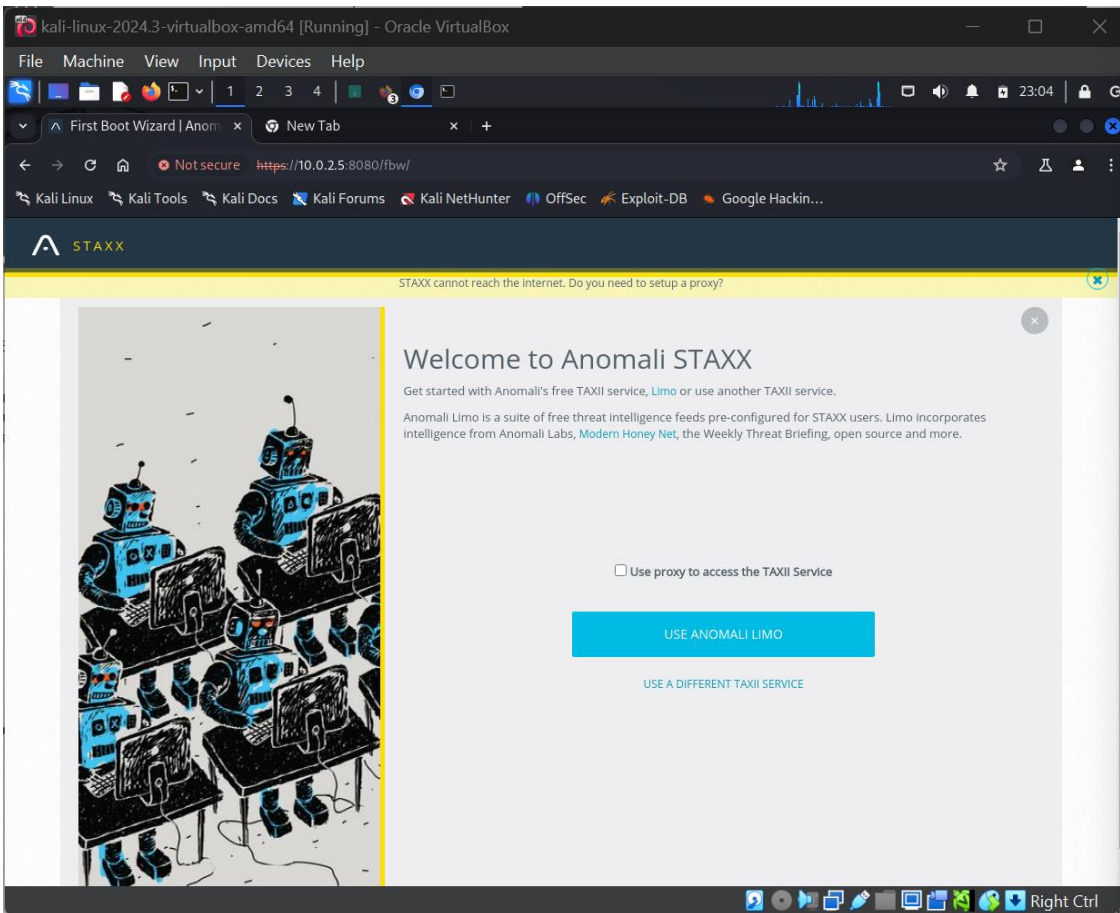
```
Anomali STAXX [Running] - Oracle VirtualBox
File Machine View Input Devices Help

CentOS Linux 7 (Core)
Kernel 3.10.0-693.17.1.el7.x86_64 on an x86_64
*****
The username "anomali" has been configured for this system.
The default password is "anomalistaxx". Please change it after first login.
*****

*****
You can access Anomali STAXX at https://10.0.2.5:8080
*****

anomali-staxx login: anomali
Password:
You are required to change your password immediately (root enforced)
Changing password for anomali.
(current) UNIX password:
New password:
Retype new password:
Last login: Thu Oct 3 23:15:54 on
[anomali@anomali-staxx ~]$_
```

3. This guide (Chapter 2) will help you get Anomali set up. When you connect to the web interface, you will need to accept the insecure connection on most major browsers.
4. When asked, use the Anomali Limo service to gather data for your first feeds.



5. Once you are in and Anomali has ingested its feeds, explore the dashboards. **Take the screenshot of Dashboard.**

