

Vulnerability Assessment and Penetration Testing

Project agenda: 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.

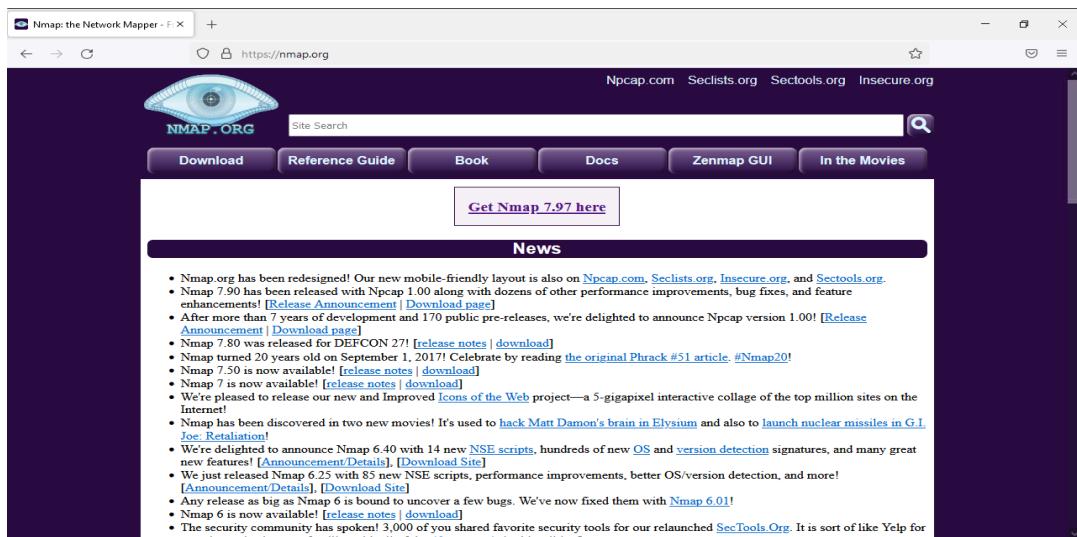
Steps to be followed:

First we have to install Zenmap in windows and Nessus in Kali. So, first:

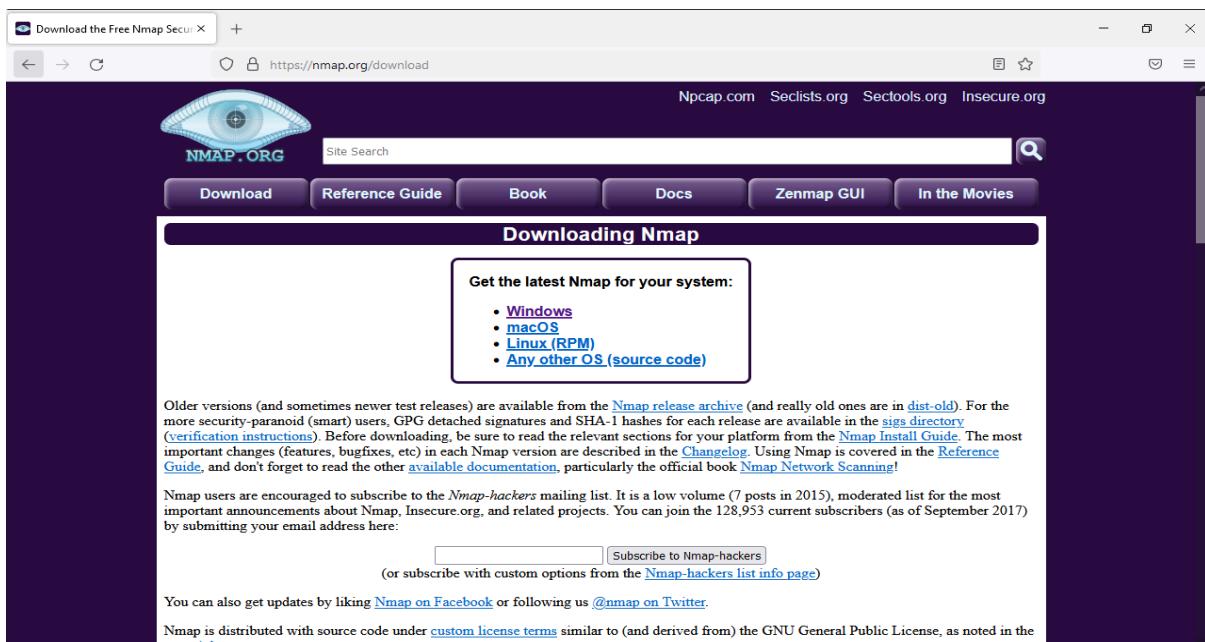
1. Open Windows 10 and download Zenmap.

URL - <https://nmap.org/>

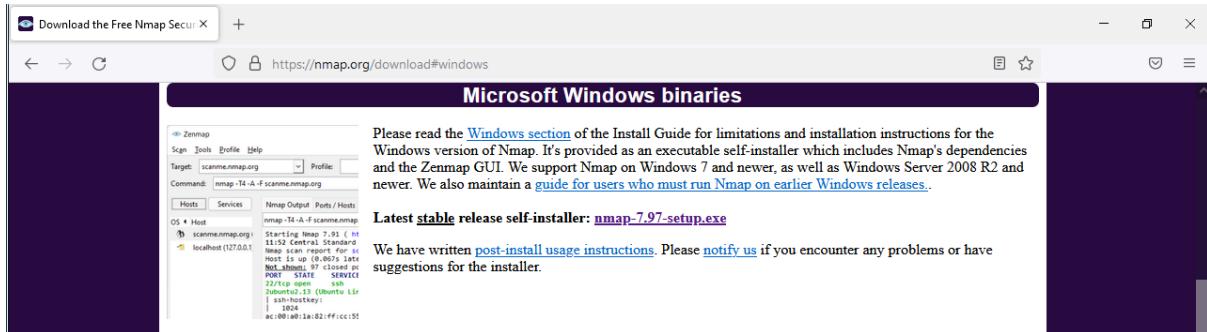
Once the link opens, you will get this interface.



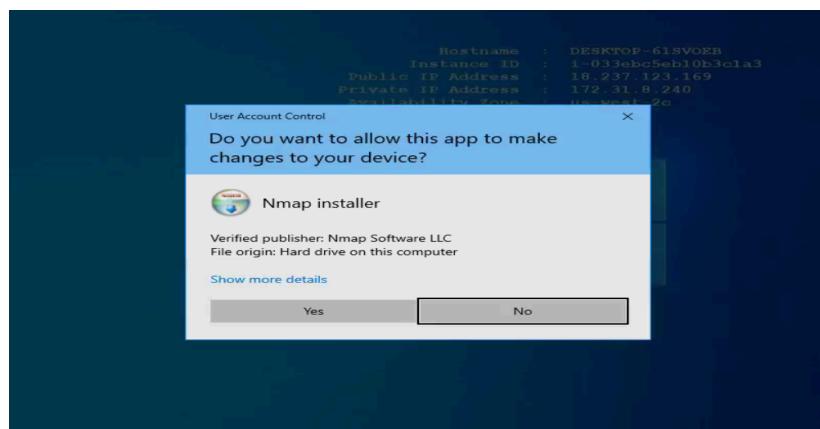
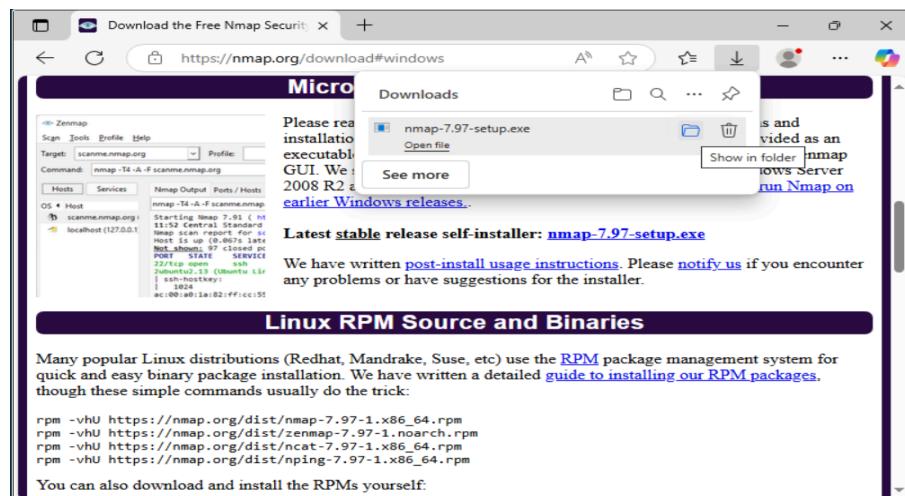
2. Click on “Get Namp 7.97 here”
3. Click on the “Windows” option.



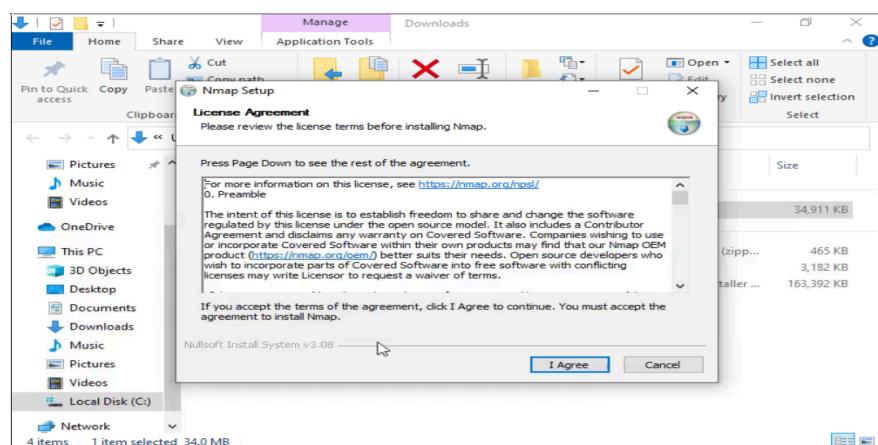
4. Click on the Link listed as “nmap 7.97 setup.exe”

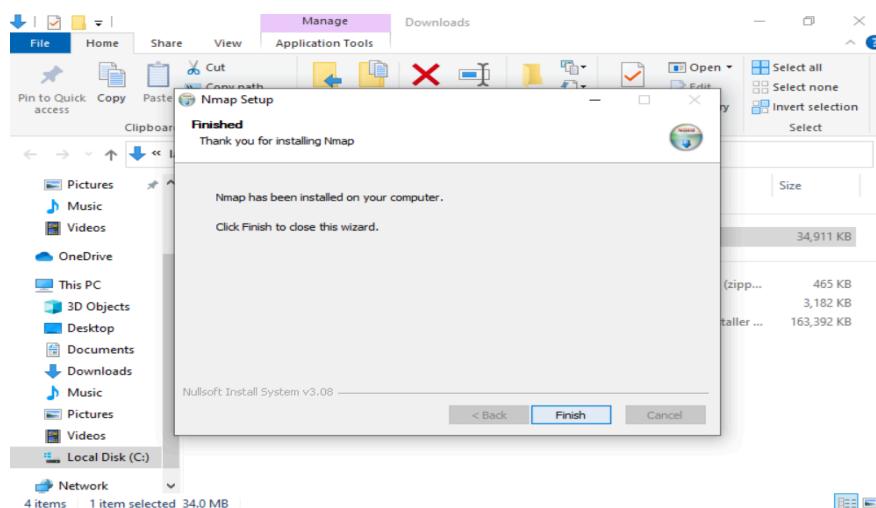
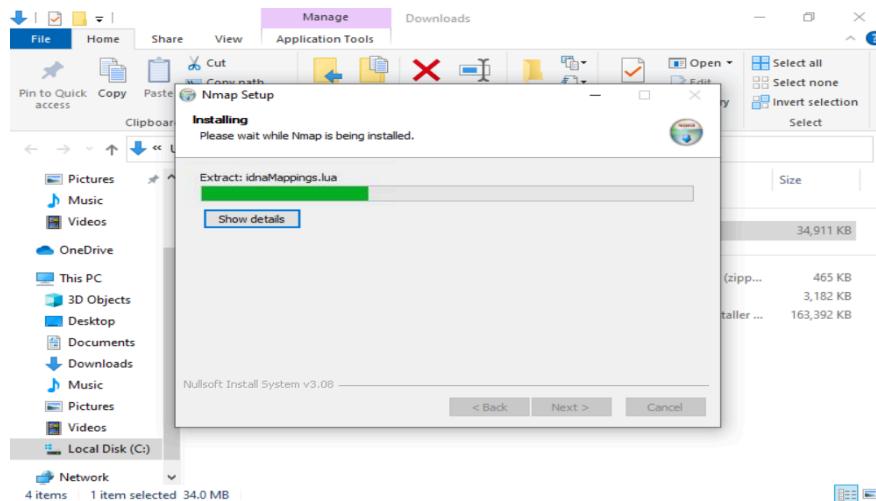


5. Open the downloaded folder and start installing.



6. Click on yes and follow all the steps to install the nmap and agree all the T&Cs and finish the download.





Now we'll download Nessus on Kali.

1. Open Kali in your system and open your browser. And write "Nessus essential download". You'll get this link.

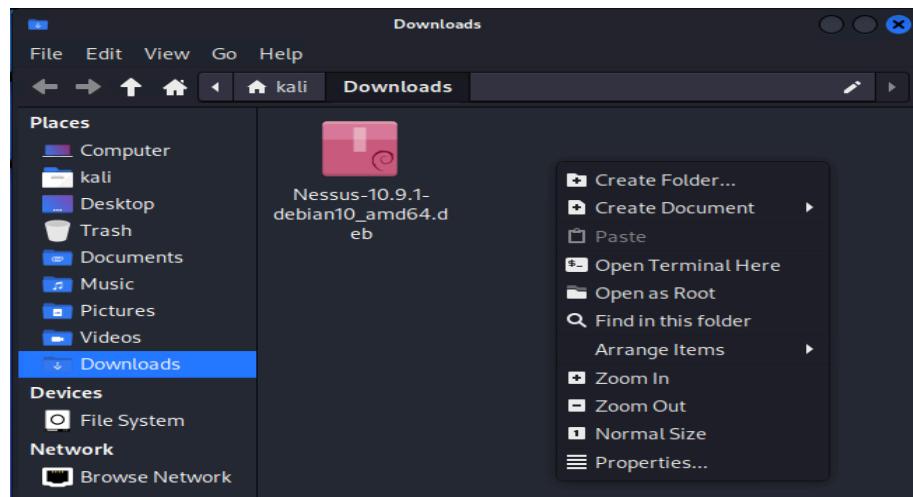
2. Click on "Download".
3. Click on the first option "Download Nessus and Nessus Manager"

The screenshot shows the 'Tenable Nessus' download page. In the 'Choose Download' section, the 'Version' dropdown is set to 'Nessus - 10.9.1' and the 'Platform' dropdown is set to 'Linux - Ubuntu - amd64'. Below these dropdowns are two buttons: a blue 'Download' button and a smaller 'Checksum' button.

4. Change platform option to “Linux - Debian - amd64”.

The screenshot shows the 'Tenable Nessus' download page. In the 'Choose Download' section, the 'Version' dropdown is set to 'Nessus - 10.9.1' and the 'Platform' dropdown is set to 'Linux - Debian - amd64'. Below these dropdowns are two buttons: a blue 'Download' button and a smaller 'Checksum' button.

5. Click on download and agree with the licence agreement. Once downloaded, open the file location and click right and select “Open terminal here”.



6. Once the terminal opens then type the command “sudo su” to enter root mode. Then type the command “sudo dpkg -i Nessus-10.9.1-debian10_amd64.deb” to install the Nessus in the Kali system. Once all the processing is done, type “/bin/systemctl start nessusd.service” to start the software. And then click on the Link given above “https://NESSUS_HOSTNAME_OR_IP:8834”

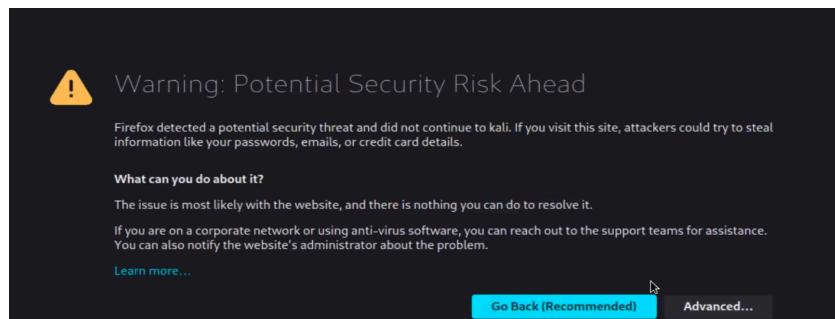
```

File Actions Edit View Help
$ sudo su
[~]# sudo dpkg -i Nessus-10.9.1-debian10_amd64.deb
(Reading database ... 429776 files and directories currently installed.)
Preparing to unpack Nessus-10.9.1-debian10_amd64.deb ...
Unpacking nessus (10.9.1) over (10.9.1) ...
Setting up nessus (10.9.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://NESSUS_HOSTNAME_OR_IP:8834/ to configure your scanner

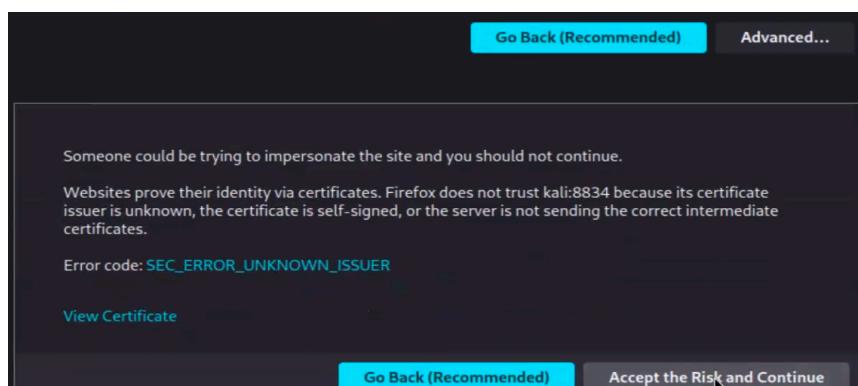
[~]# /bin/systemctl start nessusd.service
[~]# 

```

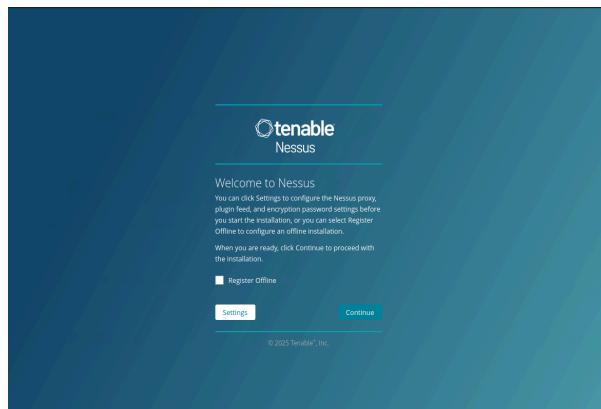
7. Once the link opens, you'll get the error page.



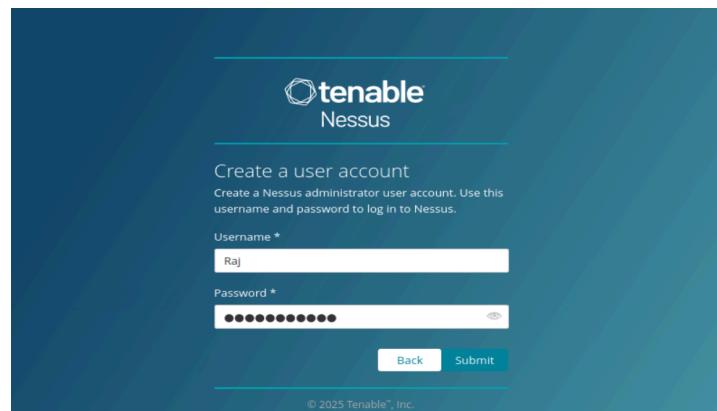
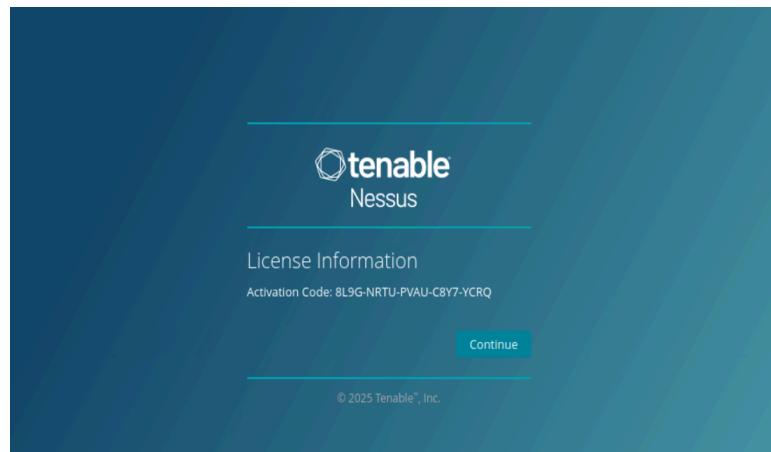
8. Click on the advance option and click on “Accept the risk and continue”.



9. You'll land on the Nessus set up page.



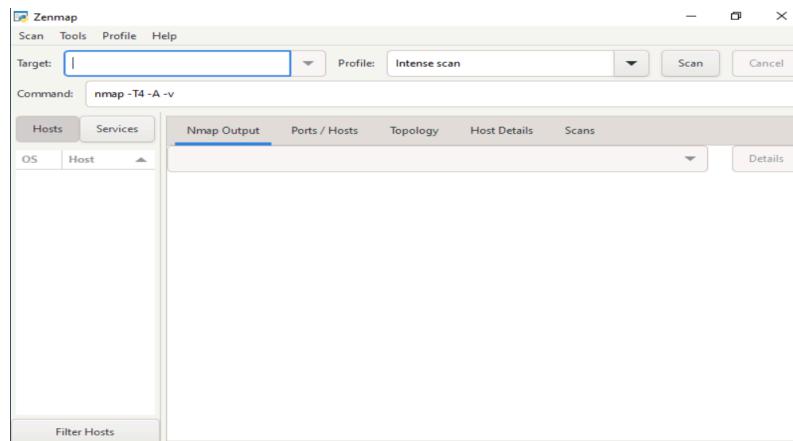
10. Click on continue and follow all the registration process and create your account.



Now all the required software is downloaded.

Step 1: Performing Information gathering and Recon

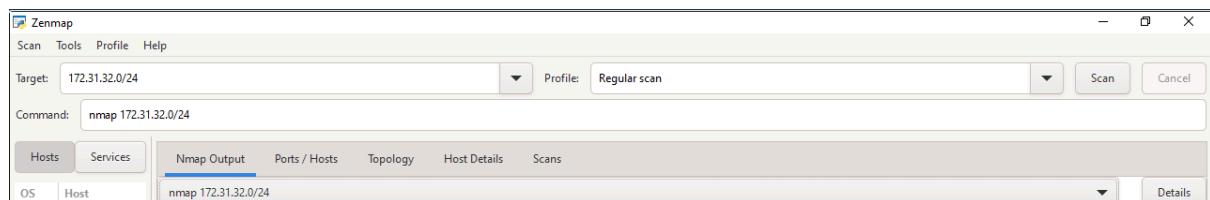
1. Open the Zenmap tool in the windows 10 server.



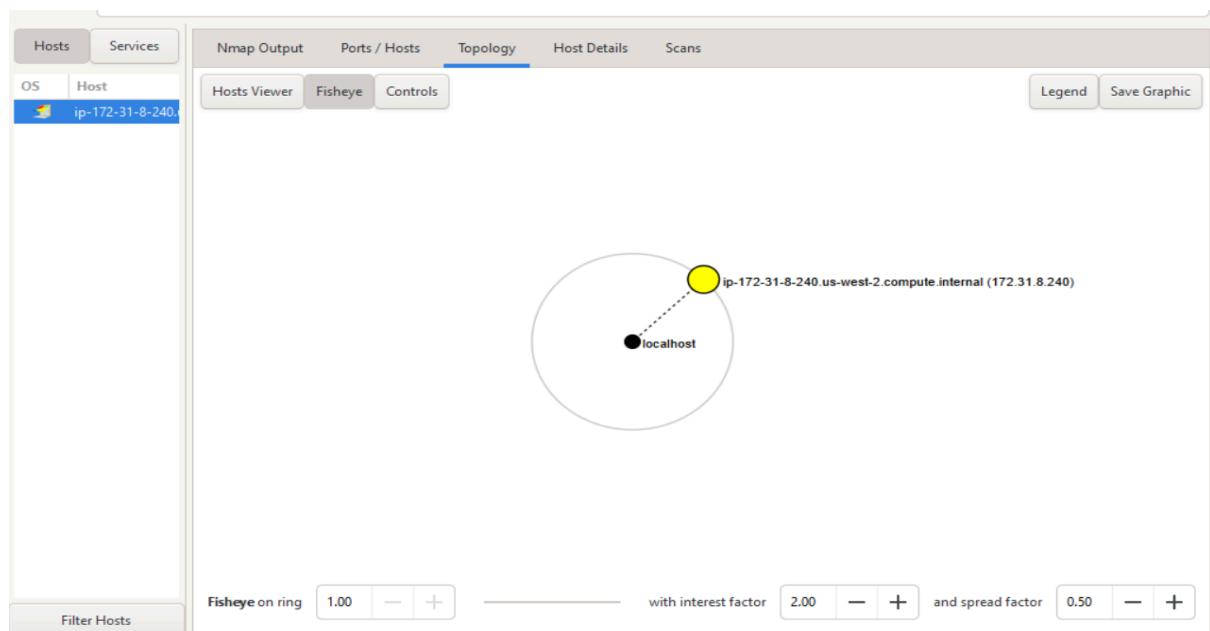
- Get the Windows 10's IP address by going to the command prompt and type "ipconfig/all".

Windows 10 IP address - 172.31.8.240

Now put this IP address on the target tab and run intense scan.



- Check for the active systems and initial information of the network using the **Topology** tab in the tool as shown in the following screenshot:



Step 2: Performing enumeration and service scanning

- Check the IP address of the Windows and Debian System

2. Now perform a focused Intense scan on Windows System (172.31.8.240)

The screenshot shows the Zenmap interface with the following details:

- Target:** 172.31.8.240
- Profile:** Intense scan
- Command:** nmap -T4 -A -v 172.31.8.240
- Output Tab:** Shows the Nmap command and its execution log, indicating it discovered several open ports (135, 139, 445, 3389, 5357, 8443) and their corresponding services.

Note: Click on Ports/Hosts under the Ports, Services, and Version of the service user details.

In the Windows system, we could notice system listening on TCP ports 3389, 5357 and 8443. As additional details, version information of the service is displayed

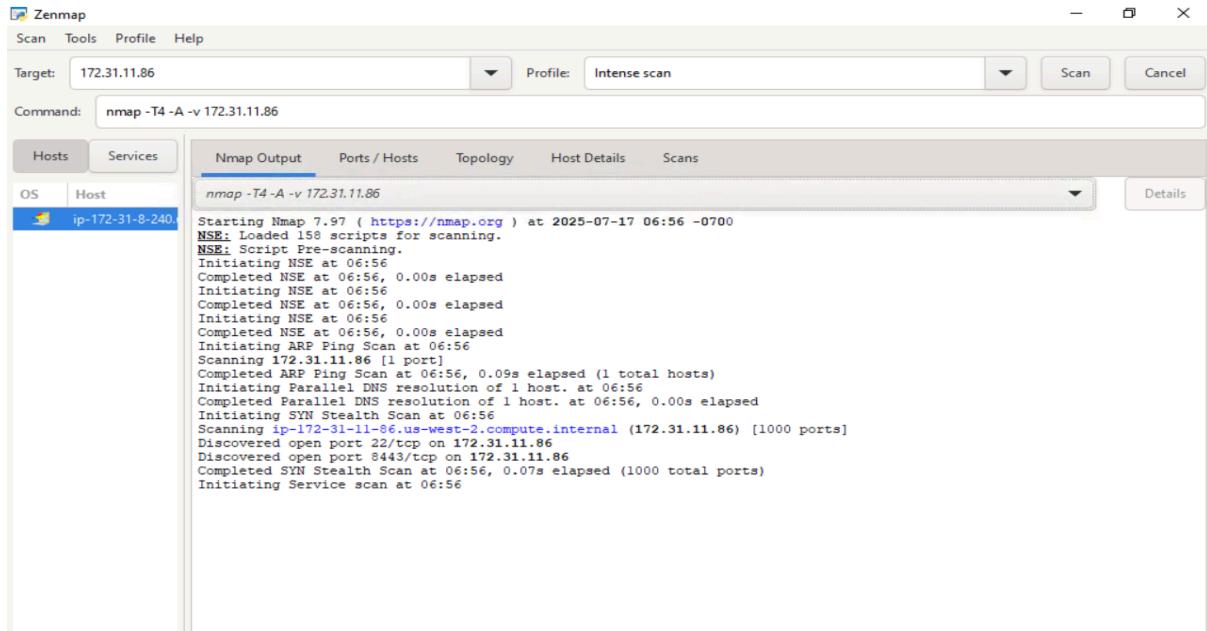
The screenshot shows the Zenmap interface with the following details:

- Target:** 172.31.8.240
- Profile:** Intense scan
- Command:** nmap -T4 -A -v 172.31.8.240
- Ports / Hosts Tab:** This tab is selected, showing a table of open ports and their details. The table includes columns for Port, Protocol, State, Service, and Version.
- Data in the Ports / Hosts Table:**

	Port	Protocol	State	Service	Version
ip-172-31-8-240.	135	tcp	open	msrpc	Microsoft Windows RPC
	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
	445	tcp	open	microsoft-ds	
	3389	tcp	open	ms-wbt-server	Microsoft Terminal Services
	5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
	8443	tcp	open	https-alt	dcv

3. Now perform a focused Intense scan on Debian Linux/Ubuntu (172.31.11.86).

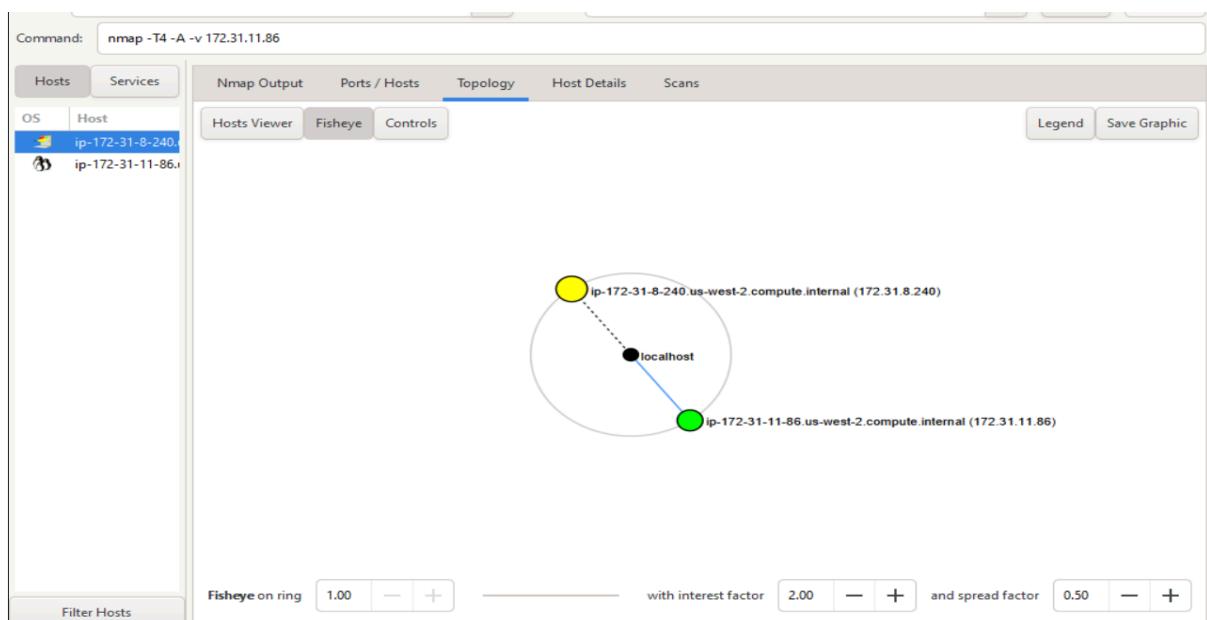
Taking the IP from Ubuntu as Ubuntu and Debian is very much similar.



Note: Click on **Ports/Hosts** under the Ports, Services, and Version of the service user details. In Debian Linux, we could notice system listening on TCP port 22, and 8443.

4. As additional details, version information of the service is displayed

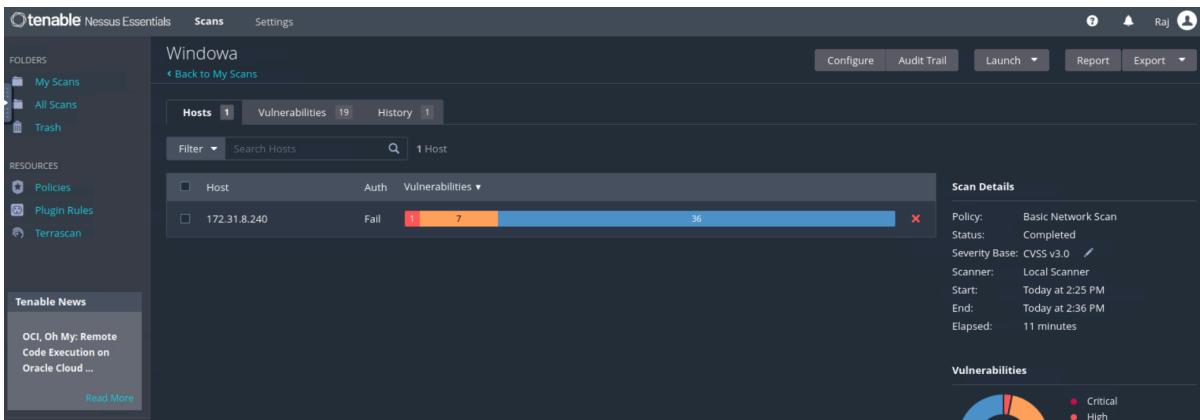
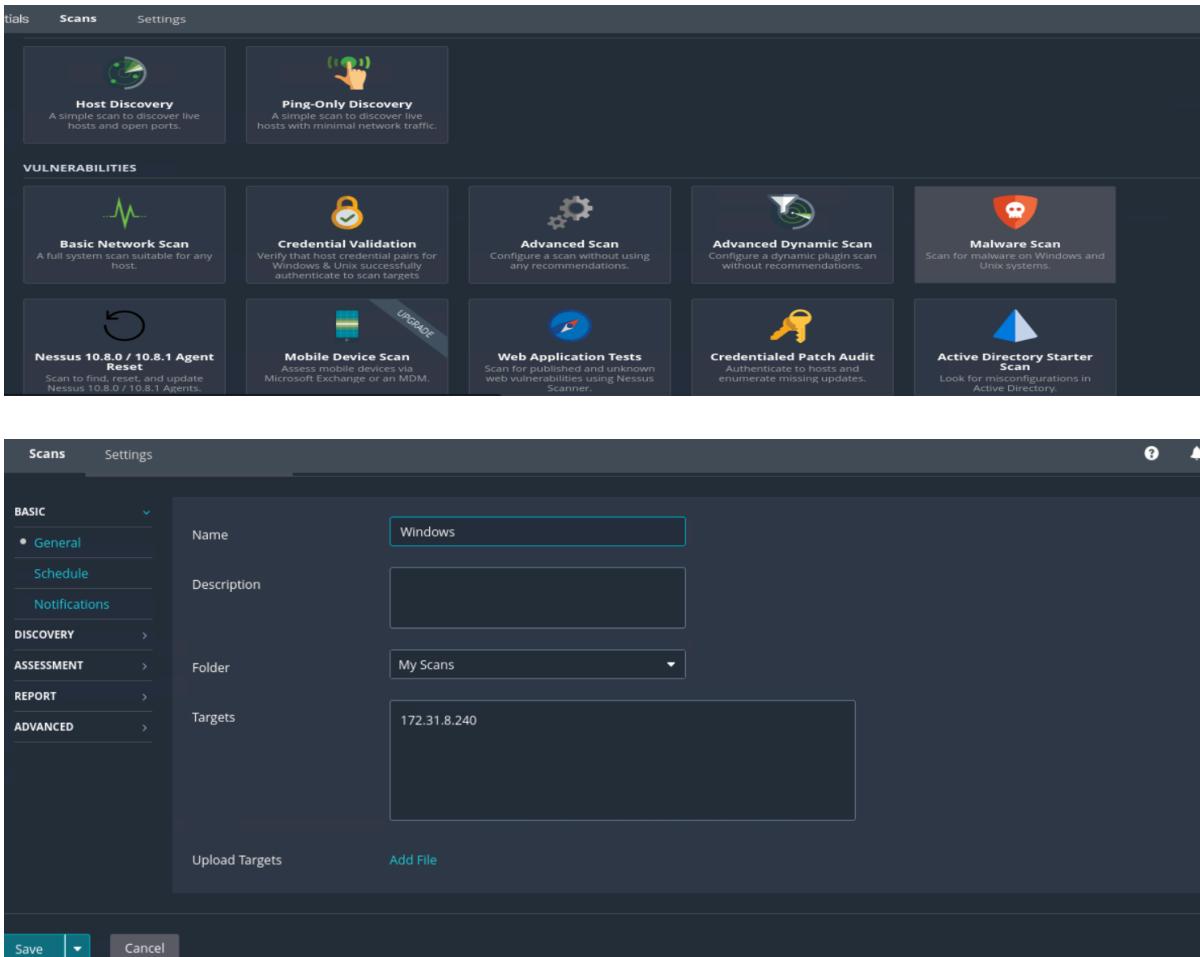
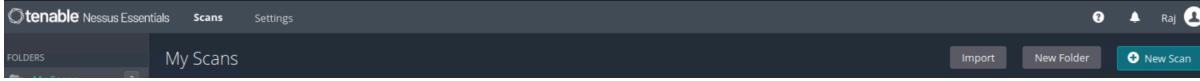
	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
●	8443	tcp	open	https-alt	dcv



Step 3: Performing vulnerability assessment

1. **Note:** Use the Nessus tool to perform a basic network scan by clicking on a new scan option.

And enter the **Windows System (IP address 172.31.8.240)** and click on **Submit**.



- Click on the Vulnerabilities tab to see the issues that Nessus had found

Sev	CVSS	VPR	EPSS	Name	Family	Count	Action
MIXED	SSL (Multiple Issues)	General	15	<input type="radio"/> <input type="radio"/> <input type="radio"/>
MIXED	TLS (Multiple Issues)	Service detection	6	<input type="radio"/> <input type="radio"/> <input type="radio"/>
MIXED	Microsoft Windows (Multiple Issues)	Misc.	2	<input type="radio"/> <input type="radio"/> <input type="radio"/>
INFO	TLS (Multiple Issues)	General	4	<input type="radio"/> <input type="radio"/> <input type="radio"/>
INFO				Nessus SYN scanner	Port scanners	2	<input type="radio"/> <input type="radio"/> <input type="radio"/>
INFO				Service Detection	Service detection	2	<input type="radio"/> <input type="radio"/> <input type="radio"/>
INFO				Common Platform Enumeration ...	General	1	<input type="radio"/> <input type="radio"/> <input type="radio"/>
INFO				Device Type	General	1	<input type="radio"/> <input type="radio"/> <input type="radio"/>
INFO				Ethernet MAC Addresses	General	1	<input type="radio"/> <input type="radio"/> <input type="radio"/>

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 2:25 PM
- End: Today at 2:36 PM
- Elapsed: 11 minutes

Vulnerabilities

- Click on the report and generate the report. Choose the report format (PDF, HTML, or CSV) and click on **Generate Report**.

Generate Report

Report Format: HTML PDF CSV

Select a Report Template:

SYSTEM

Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
 Include page breaks between vulnerability results

Buttons: Generate Report, Cancel, Save as default

- Check the **Debian Linux System/Ubuntu** (IP address **172.31.11.86***) and click on **Submit**.

Scans

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Fields:

- Name: Ubuntu
- Description:
- Folder: My Scans
- Targets: 172.31.11.86

Buttons: Save, Cancel

- Click on the Vulnerabilities tab to see the issues that Nessus had found.

Ubuntu

[Back to My Scans](#)

Hosts 1 Vulnerabilities 28 History 1

Filter Search Hosts 1 Host

Host	Auth	Vulnerabilities
172.31.11.86	Fail	5 1 36

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 2:26 PM
 End: Today at 2:32 PM
 Elapsed: 6 minutes

Vulnerabilities

Filter Search Vulnerabilities 28 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
MEDIUM	5.3	3.9	0.9169	CUPS cups-browsed Remote Un...	CGI abuses	1	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
MIXED	SSL (Multiple Issues)	General	8	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
MIXED	Openbsd Openssh (Multipl...	Misc.	2	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remo...	General	1	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
INFO	SSH (Multiple Issues)	General	2	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
INFO	SSH (Multiple Issues)	Misc.	2	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
INFO	TLS (Multiple Issues)	General	2	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
INFO	TLS (Multiple Issues)	Service detection	2	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>
INFO				Nessus SYN scanner	Port scanners	2	<input type="radio"/> <input type="checkbox"/> <input type="pen"/>

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 2:26 PM
 End: Today at 2:32 PM
 Elapsed: 6 minutes

Vulnerabilities

- Click on the report and generate the report. Choose the report format (PDF, HTML, or CSV) and click on **Generate Report**.

Generate Report

Report Format: HTML PDF CSV

Select a Report Template:

SYSTEM	Template Description:
Complete List of Vulnerabilities by Host Detailed Vulnerabilities By Host Detailed Vulnerabilities By Plugin Vulnerability Operations	This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied: None

Formatting Options:
 Include page breaks between vulnerability results

Save as default

Step 4: Performing vulnerability classification and ranking

1. Below document is the classification and ranking of the vulnerability.

■ Vulnerability Classification

Step 5: Generating report based on analysis

Executive Report

Project Summary:

A Vulnerability Assessment and Penetration Testing (VAPT) engagement was conducted on two systems: a Windows 10 machine (IP: 172.31.8.240) and a Debian-based Ubuntu machine (IP: 172.31.11.86). The goal was to detect, evaluate, and prioritize security weaknesses and to provide recommendations to mitigate the risks identified. The assessment was performed using Zenmap and Nessus.

Key Risk Findings:

System	Risk Level	Description
Windows 10	High	Use of weak SSL cipher (SWEET32) susceptible to cryptographic attacks.
Windows 10	Medium	TLS 1.0 and 1.1 are still enabled; considered insecure and deprecated.
Windows 10	Medium	Self-signed and untrusted SSL certificates in use.
Ubuntu	Medium	SSH implementation is vulnerable to Terrapin attack (CVE-2023-48795).
Ubuntu	Medium	CUPS service allows remote unauthenticated printer registration (CVE-2024-47176).
Ubuntu	Medium	Use of expired or self-signed SSL certificates.

Risk Summary by Severity:

Severity	Windows	Ubuntu
Critical	0	0
High	1	0
Medium	5	5
Low/Info	26	30+

Recommendations:

Windows 10:

- Disable 3DES-based ciphers to mitigate SWEET32 attacks.
- Enforce use of TLS 1.2 or higher; disable TLS 1.0/1.1.
- Replace self-signed SSL certificates with ones from trusted Certificate Authorities.
- Configure Remote Desktop Protocol (RDP) to require Network Level Authentication (NLA).

Ubuntu Linux:

- Patch OpenSSH to address CVE-2023-48795 (Terrapin).
 - Restrict or disable CUPS service or apply access controls.
 - Renew expired certificates and replace self-signed certs with CA-signed ones.
-

Conclusion:

Although no critical vulnerabilities were found, both systems contain medium-risk issues that can be exploited under certain circumstances. Timely remediation of these issues will improve the overall security posture and reduce potential attack surfaces.

Technical Report

Assessment Overview:

Two systems were tested as part of this VAPT project:

- **Windows 10** (IP: 172.31.8.240)
- **Ubuntu Linux** (IP: 172.31.11.86)

Scanning tools used:

- **Zenmap** (Nmap GUI) for network discovery and service enumeration
- **Nessus Essentials** for vulnerability scanning and analysis

1. Windows 10 (172.31.8.240)

Zenmap Results:

- Open Ports: 135, 139, 445, 3389, 5357, 8443
- OS Detected: Windows 10 (Build 19041)
- Observations: RDP exposed with potential lack of strong authentication.

Nessus Key Vulnerabilities:

CVE / Plugin ID	Name	Severity y	Exploitable ?	Recommendation		
				?	?	?
42873	SWEET32 - Strength Cipher	Medium	High	Yes	Disable 3DES cipher suites.	cipher suites.
51192	SSL Certificate Cannot Be Trusted	Cannot Be Trusted	Medium	No	Replace with CA-signed certificate.	certificate.
57582	SSL Certificate	Self-Signed	Medium	No	Use trusted certificates only.	only.

104743	TLS v1.0 Enabled	Medium	No	Disable TLS 1.0.	
157288	TLS v1.1 Enabled	Medium	No	Disable TLS 1.1.	
58453	Terminal Services NLA	No	Medium	Yes	Enable NLA in RDP settings.

2. Ubuntu Linux (172.31.11.86)

Zenmap Results:

- Open Ports: 22 (SSH), 631 (CUPS), 443
- OS Detected: Debian/Ubuntu Linux
- Observations: Several outdated services; CUPS and SSH exposed externally.

Nessus Key Vulnerabilities:

CVE / Plugin ID	Name	Severity	Exploitable	Recommendation
		?	?	
187315	SSH Terrapin Truncation Prefix (CVE-2023-48795)	Medium	Yes	Update OpenSSH to patched version.
207864	CUPS Remote Registration Printer (CVE-2024-47176)	Medium	Yes	Restrict or disable CUPS.
51192	SSL Certificate Cannot Be Trusted	Medium	No	Replace certs with valid CA-signed certs.
57582	SSL Self-Signed Certificate	Medium	No	Same as above.

15901	SSL Certificate Expiry	Medium	No	Renew certificates.	expired
-------	------------------------	--------	----	---------------------	---------

Remediation Summary:

- **Windows:** Focus on hardening TLS, enforcing RDP NLA, and eliminating weak certificates.
- **Ubuntu:** Patch vulnerable services, restrict exposed interfaces, and fix SSL configurations.

Suggested Tools for Fixes:

- **openssl** for cert management
- Group Policy Editor for RDP policies
- **apt** for patching Linux services (e.g., **sudo apt update && apt upgrade openssh-server**)

Screenshots & Attachments:

- Screenshots from Zenmap topology and scan results
- Nessus exported reports with full vulnerability listings

Conclusion:

Both systems exhibit medium-risk vulnerabilities that are exploitable in the right conditions. Remediation efforts should prioritize encryption protocols, authentication configurations, and certificate hygiene to significantly enhance security.