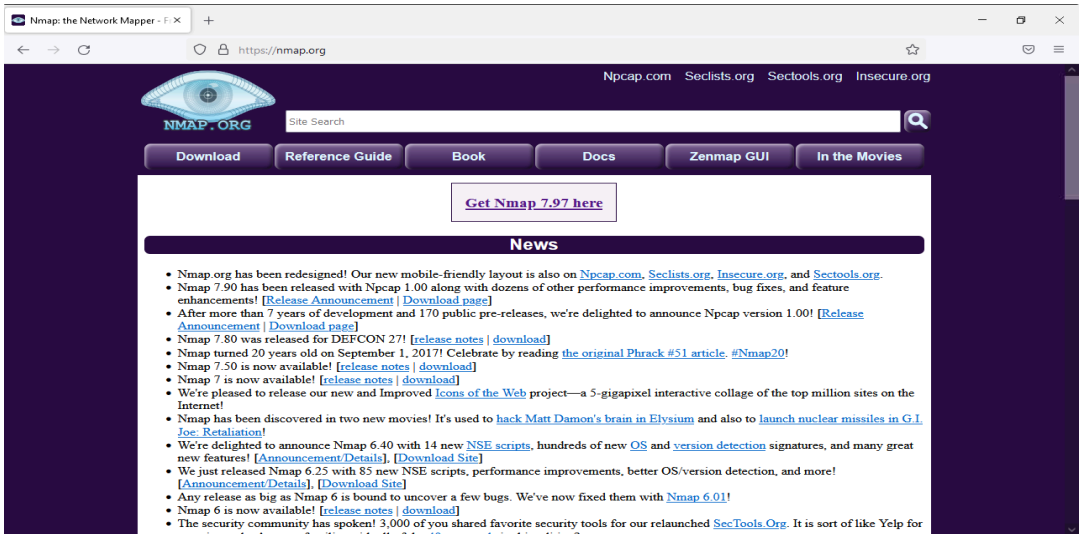
Vulnerability Assessment and Penetration Testing

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.

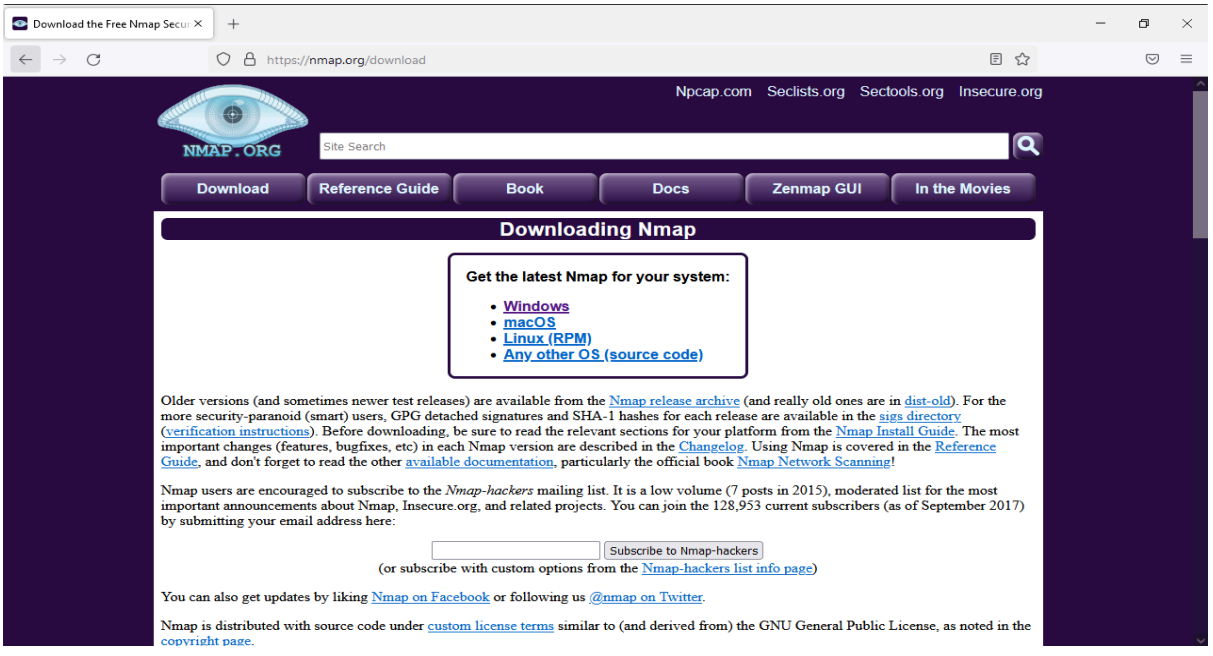
Steps to be followed:

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

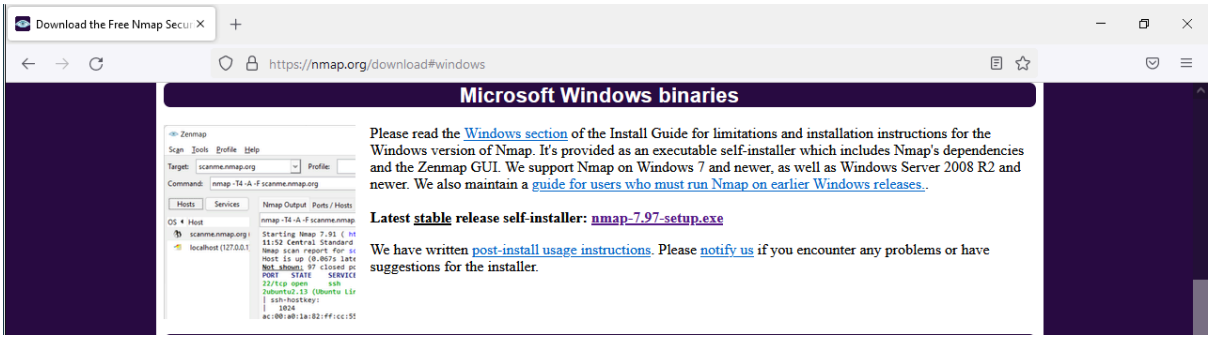
1. Open Windows 10 and download Zenmap.
   URL - https://nmap.org/
   Once the link opens, you will get this interface.



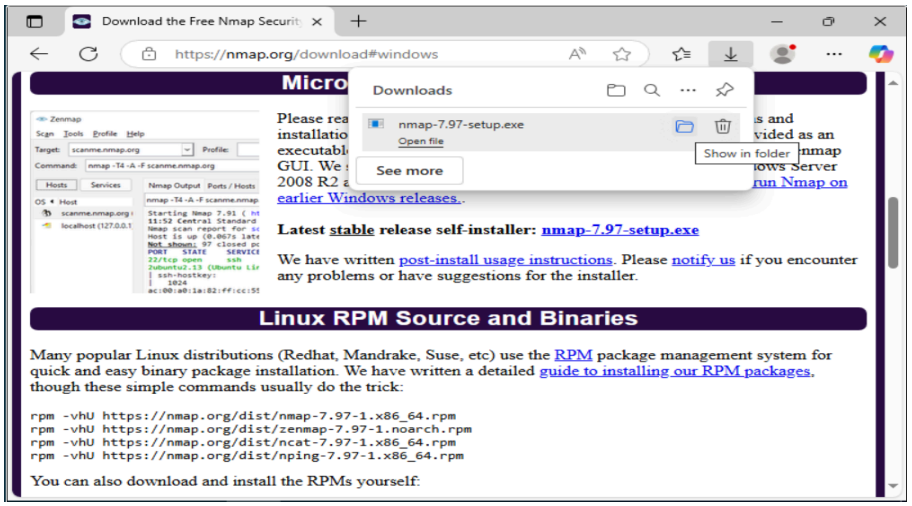
2. Click on “Get Namp 7.97 here”
3. Click on the “Windows” option.

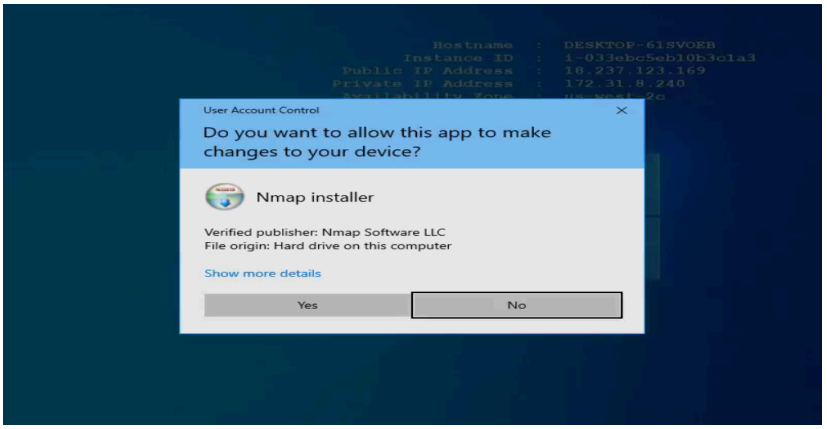


4. Click on the Link listed as “nmap 7.97 setup.exe”

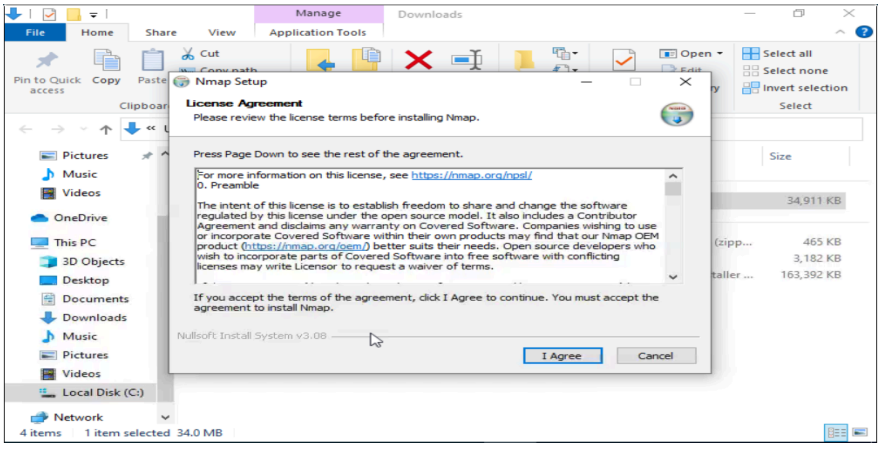


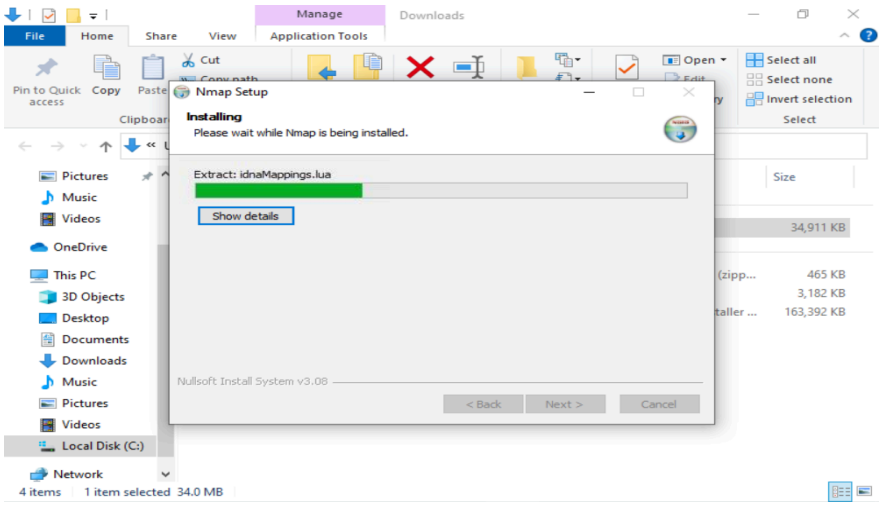
5. Open the downloaded folder and start installing.

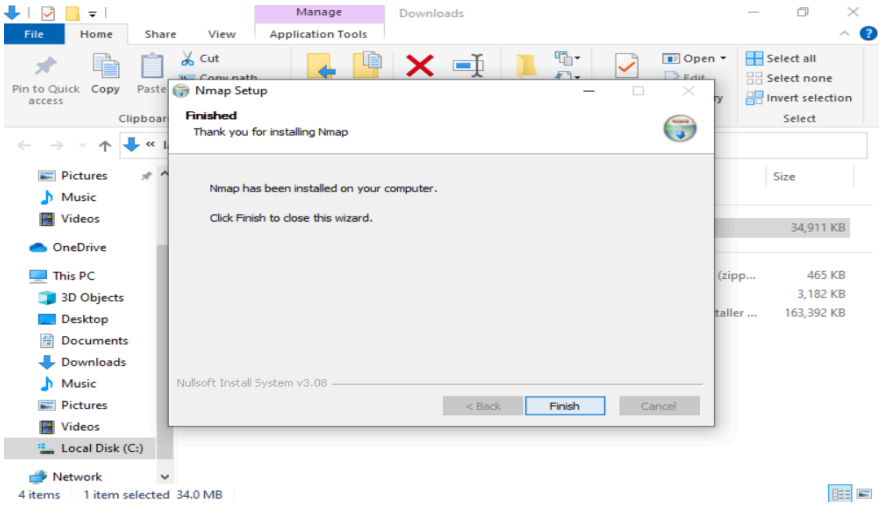




6. Click on yes and follow all the steps to install the nmap and agree all the T&Cs and finish the download.

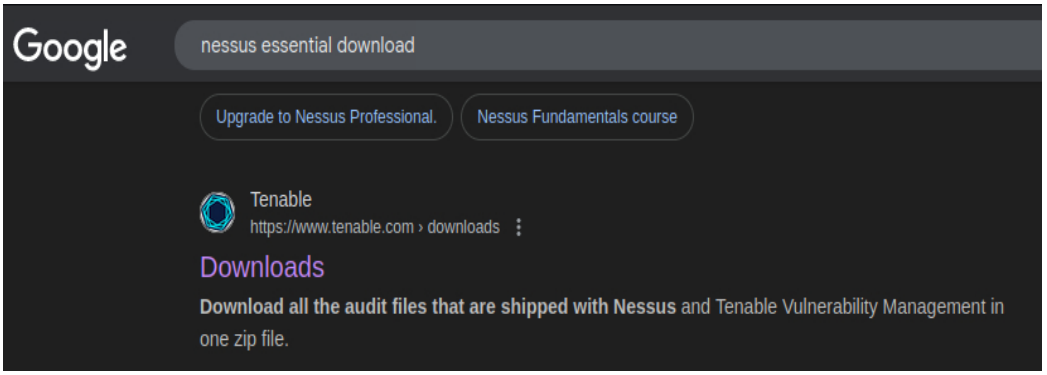




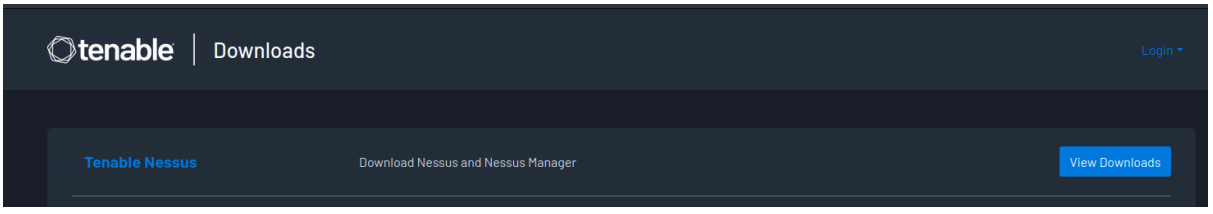


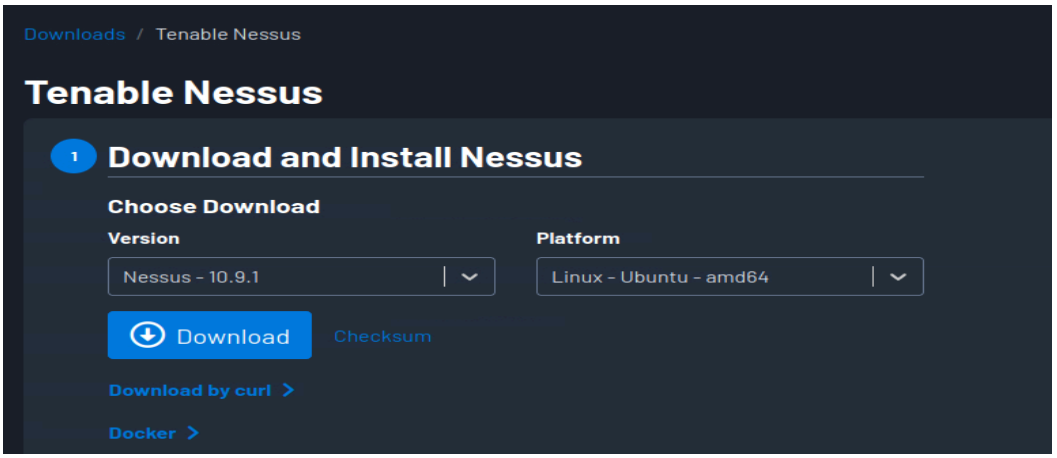
Now we'll download Nessus on Kali.

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

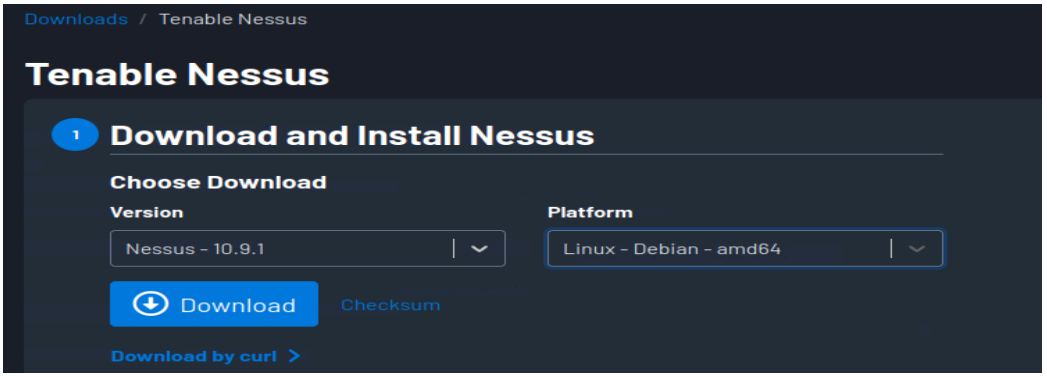


2. Click on "Download".
3. Click on the first option "Download Nessus and Nessus Manager"

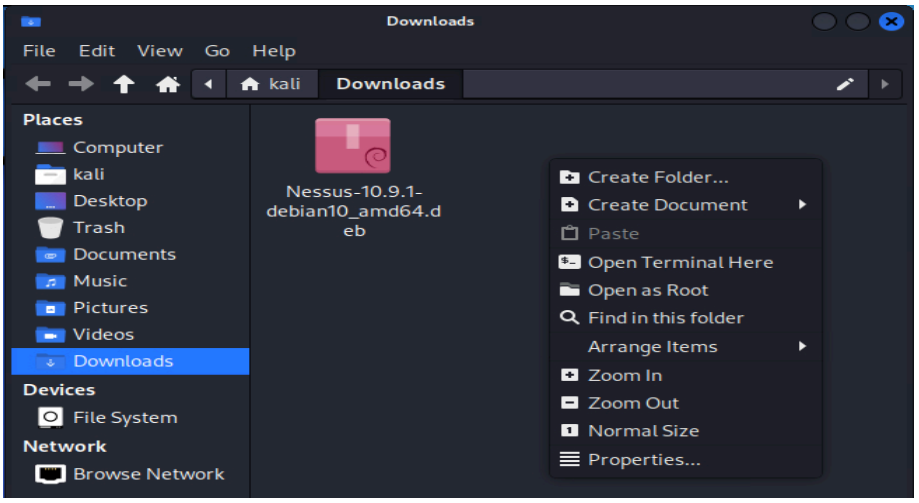




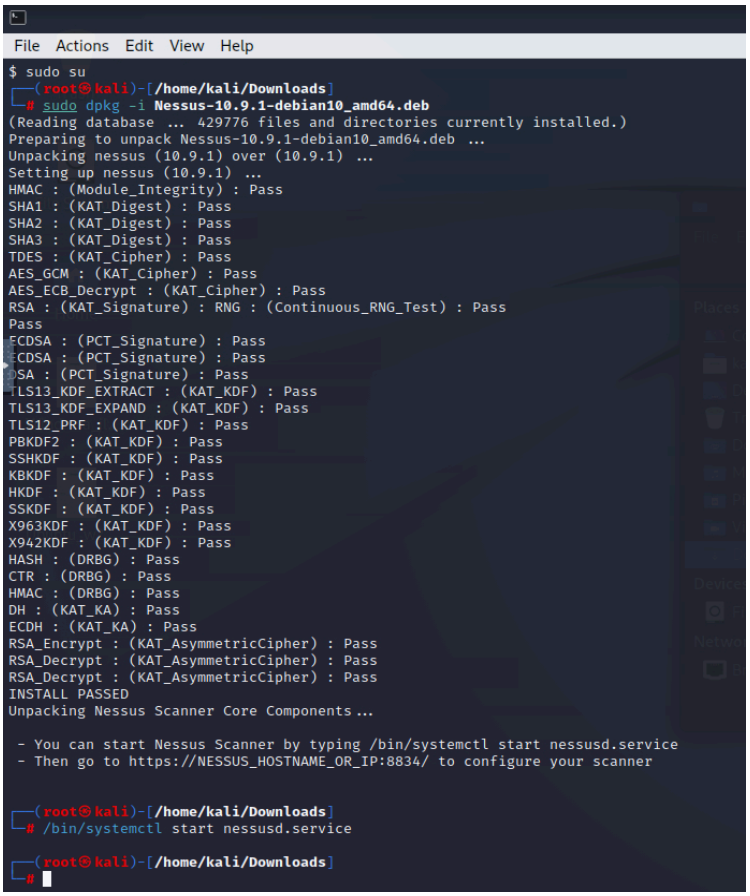
4. Change platform option to “Linux - Debian - amd64”.



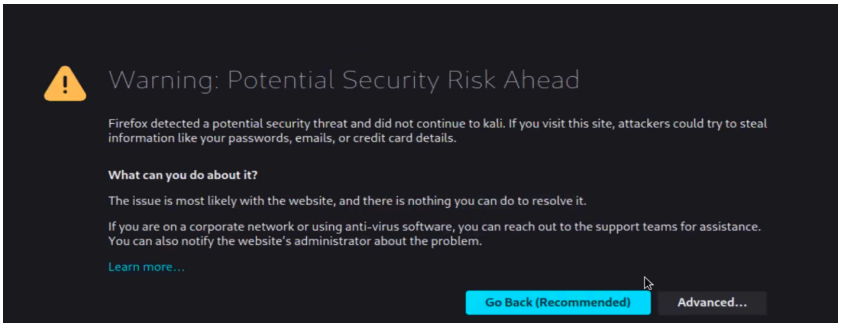
5. Click on download and agree with the licence agreement. Once downloaded, open the file location and click right and select “Open terminal here”.



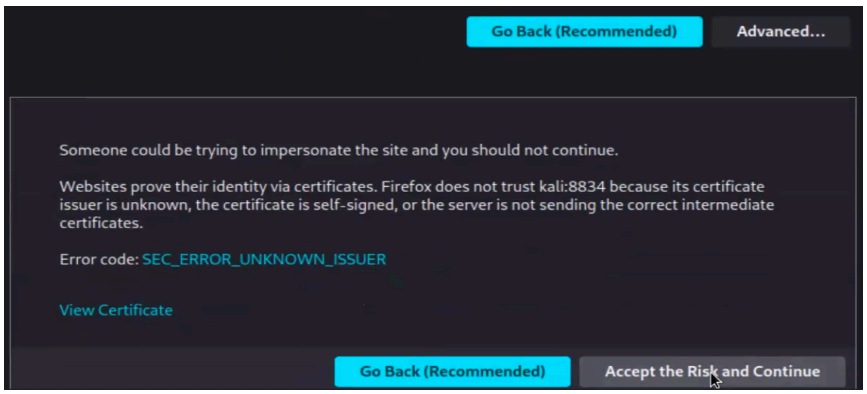
6. Once the terminal opens then type the command “sudo su” to enter root mode. Then typer the command “sudo dpkg -i Nessus-10.9.1-debian10_amd64.deb” to install the Nessus in the Kali system. Once all the processing is done, type “/bin/systemctl start nessusd.service” to start the software. And then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



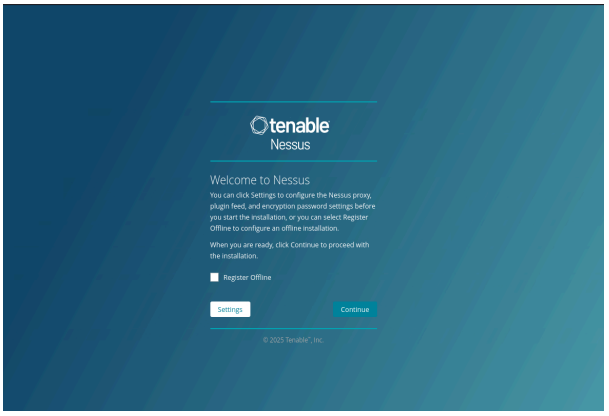
7. Once the link opens, you'll get the error page.



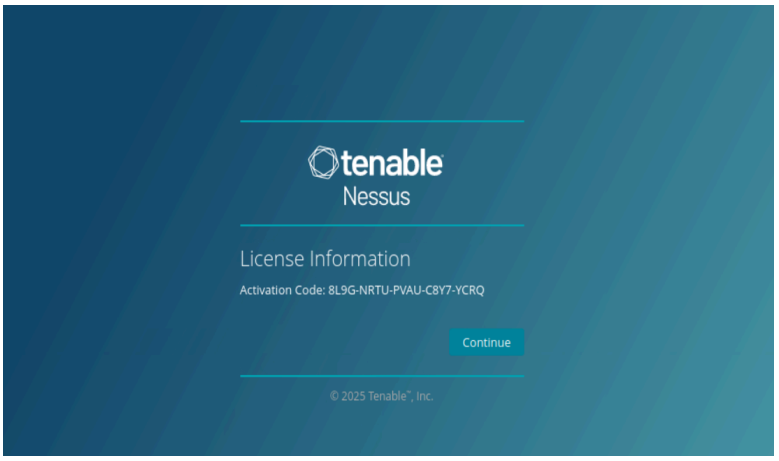
8. Click on the advance option and click on "Accept the risk and continue".



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



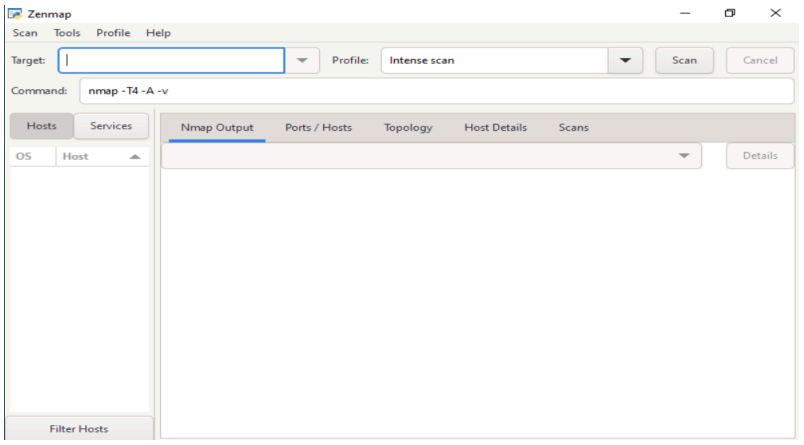
10. Click on continue and follow all the registration process and create your account.



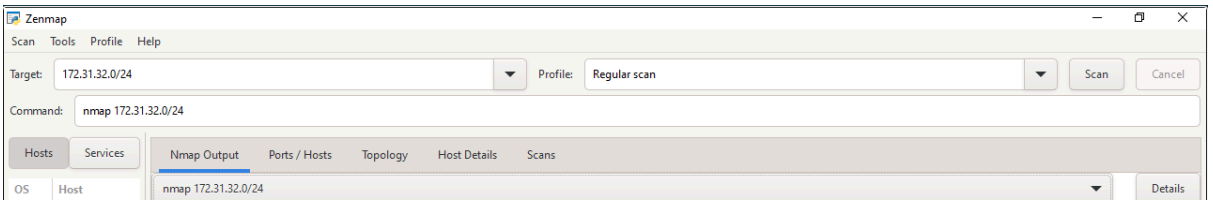
Now all the required software is downloaded.

Step 1: Performing Information gathering and Recon

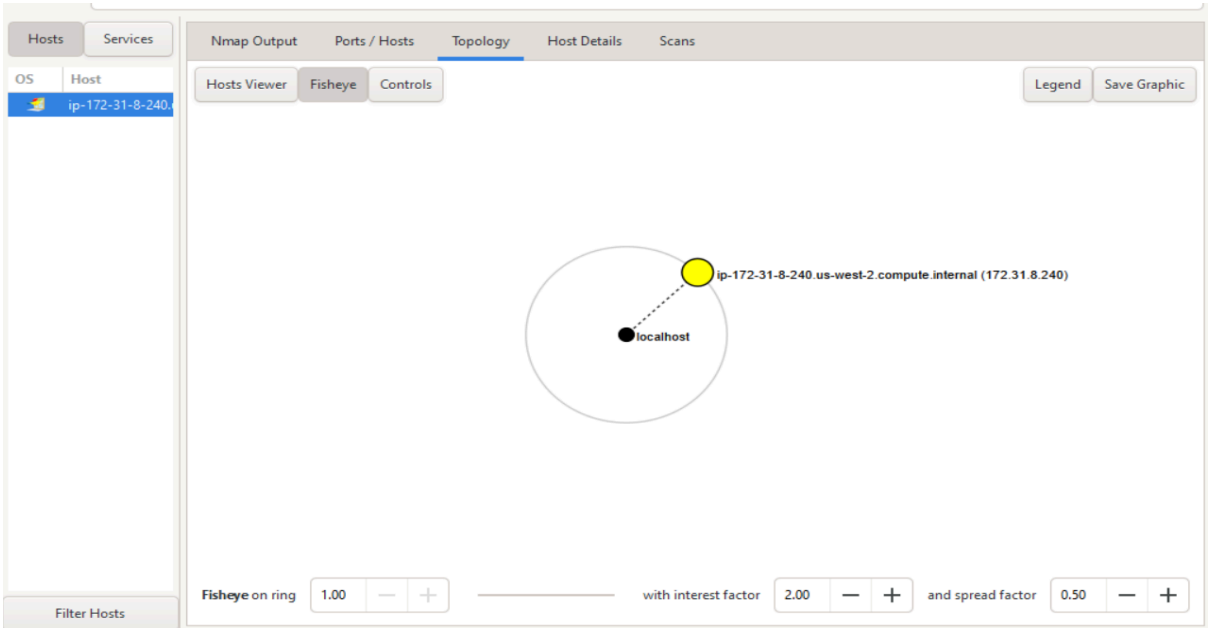
1. Open the Zenmap tool in the windows 10 server.



1. 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.



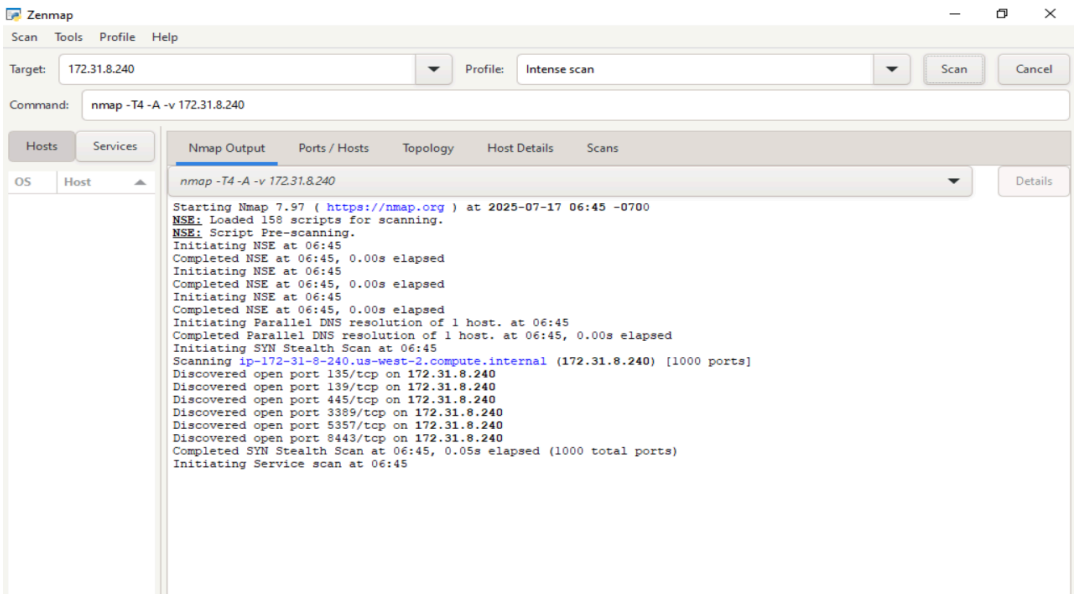
2. Check for the active systems and initial information of the network using the **Topology** tab in the tool as shown in the following screenshot:



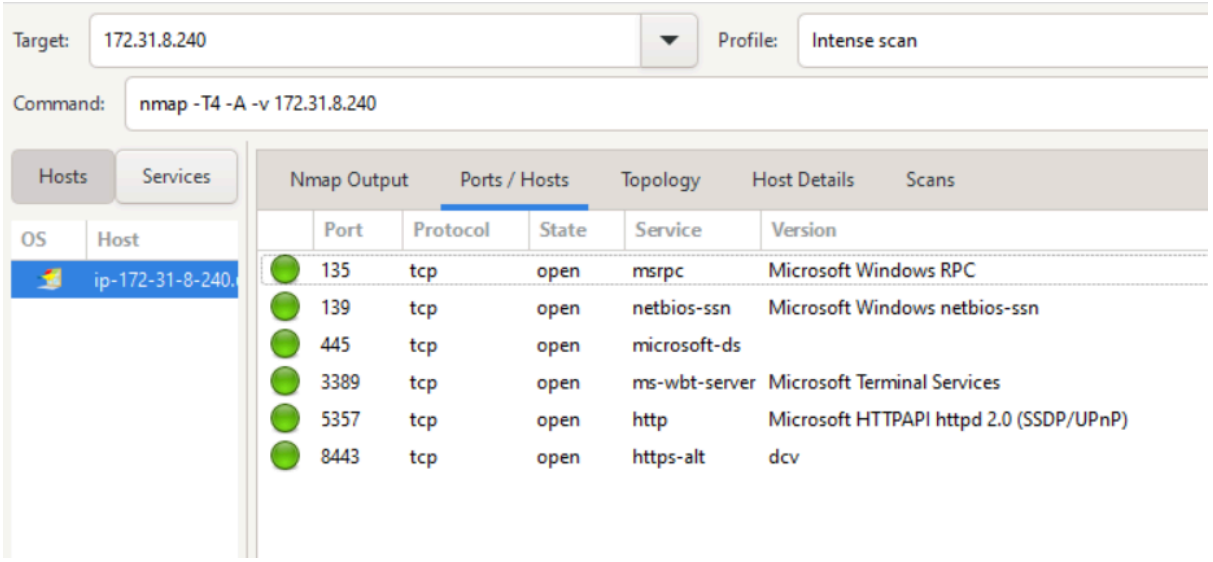
Step 2: Performing enumeration and service scanning

1. Check the IP address of the Windows and Debian System

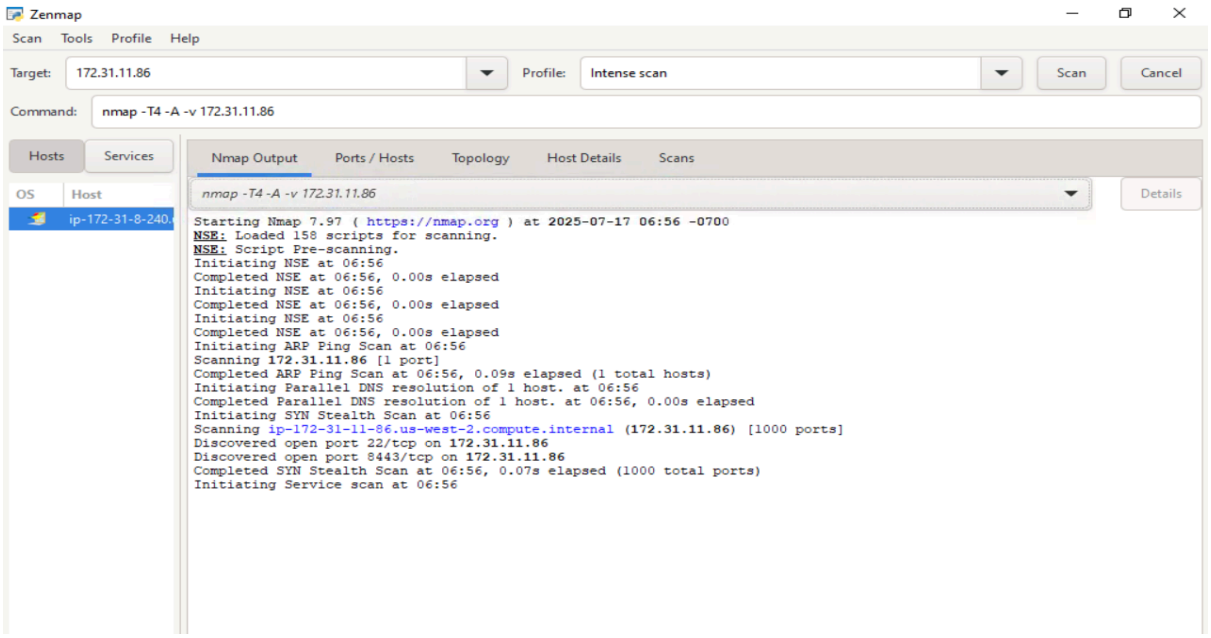
2. Now perform a focused **Intense scan** on **Windows System (172.31.8.240)**



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

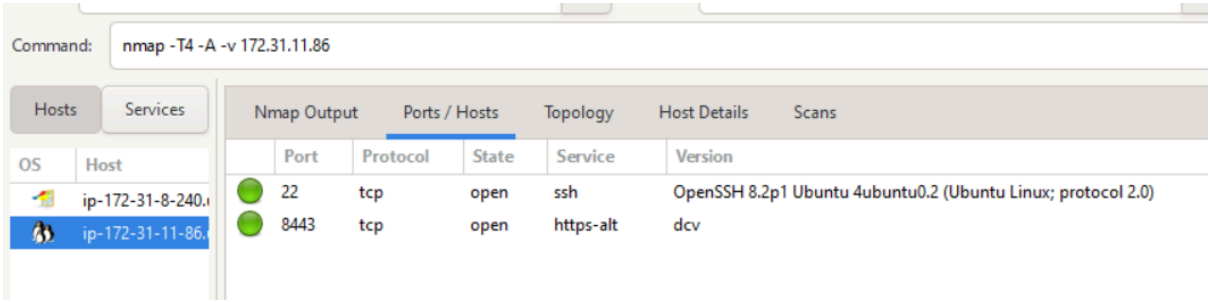


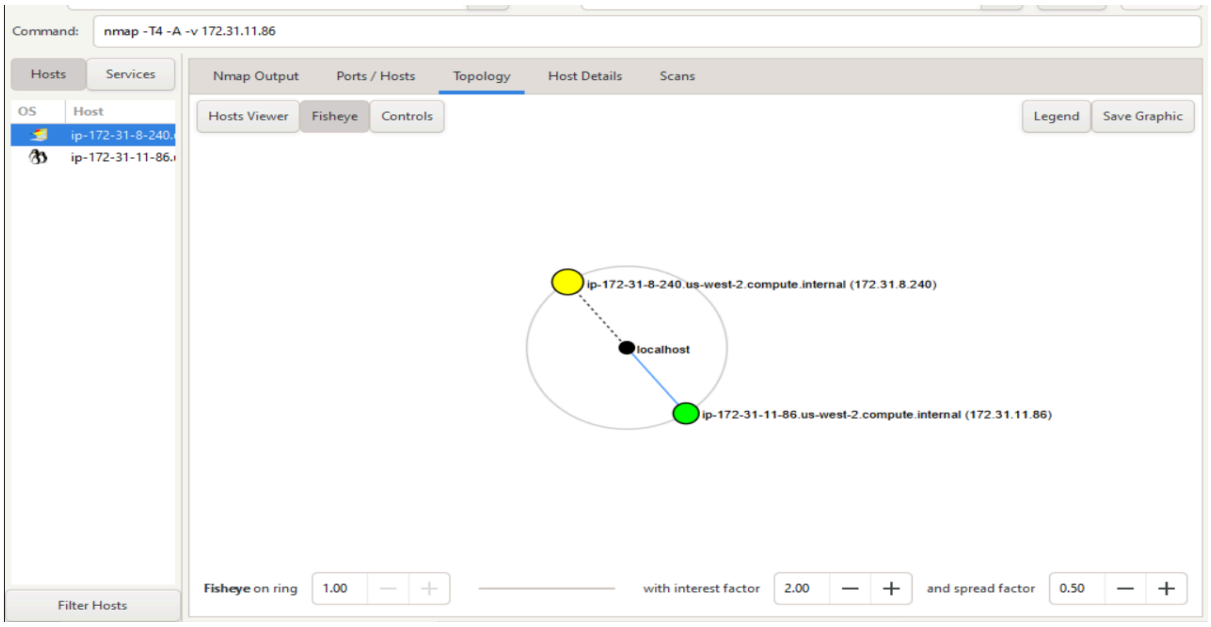
3. Now perform a focused **Intense scan** on **Debian Linux/Ubuntu (172.31.11.86).** Taking the IP from Ubuntu as Ubuntu and Debian is very much similar.



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

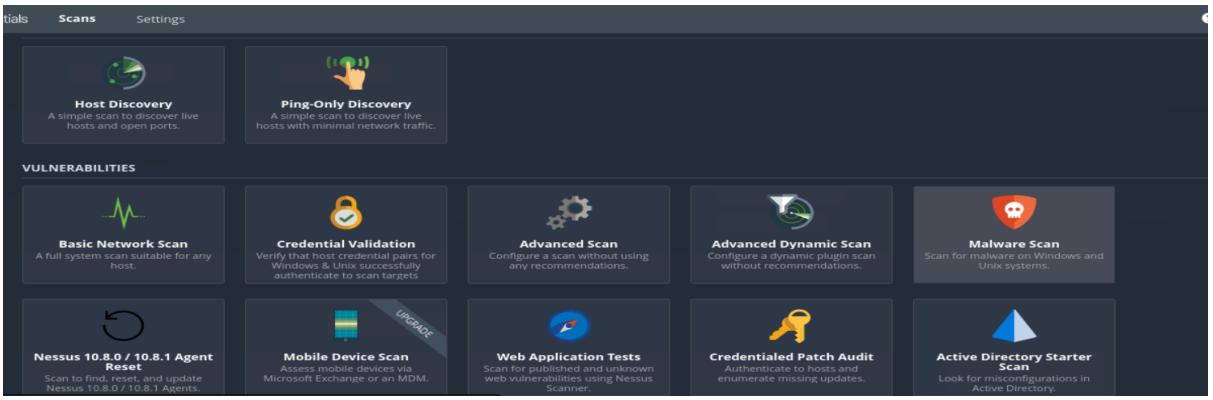


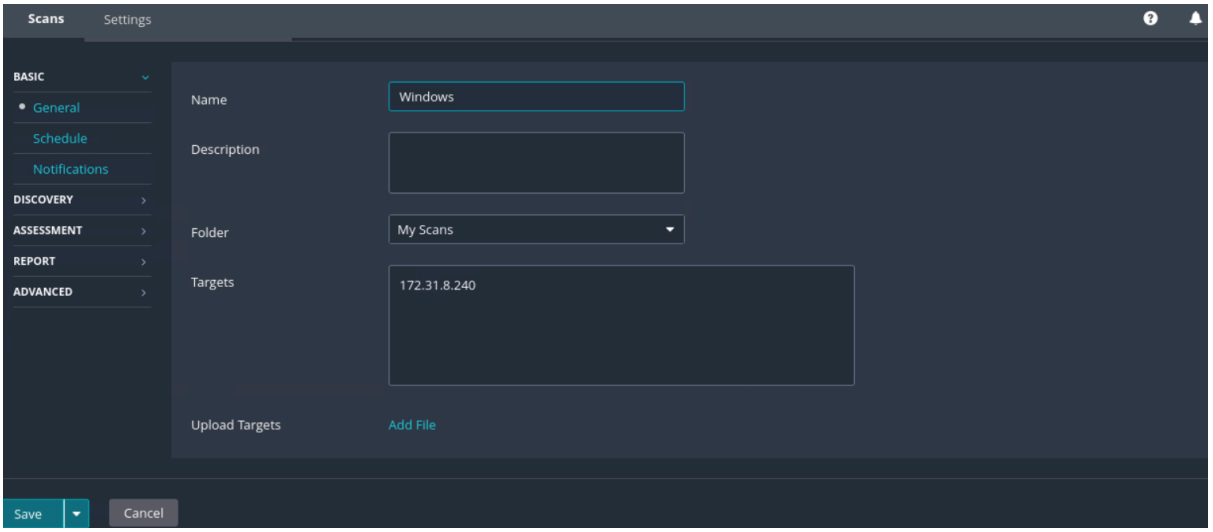


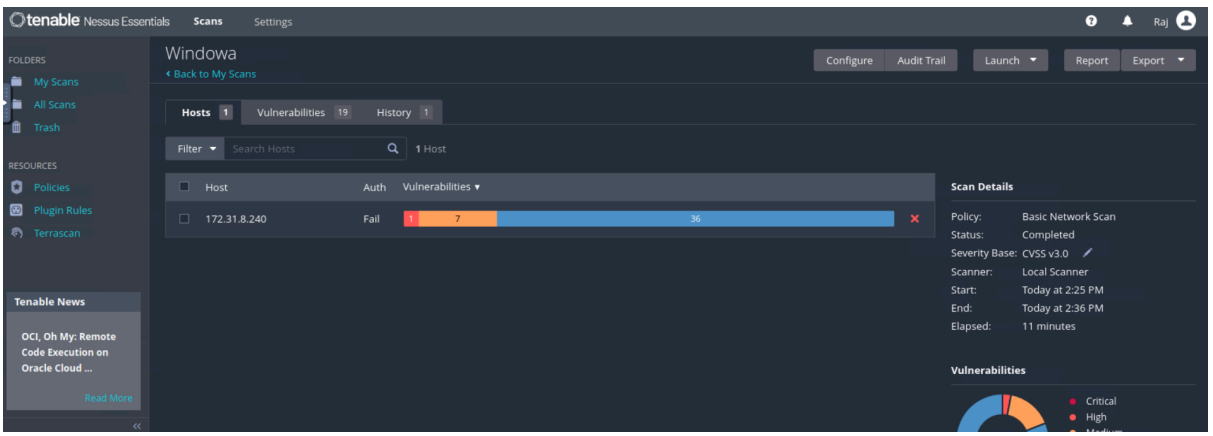
Step 3: Performing vulnerability assessment

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

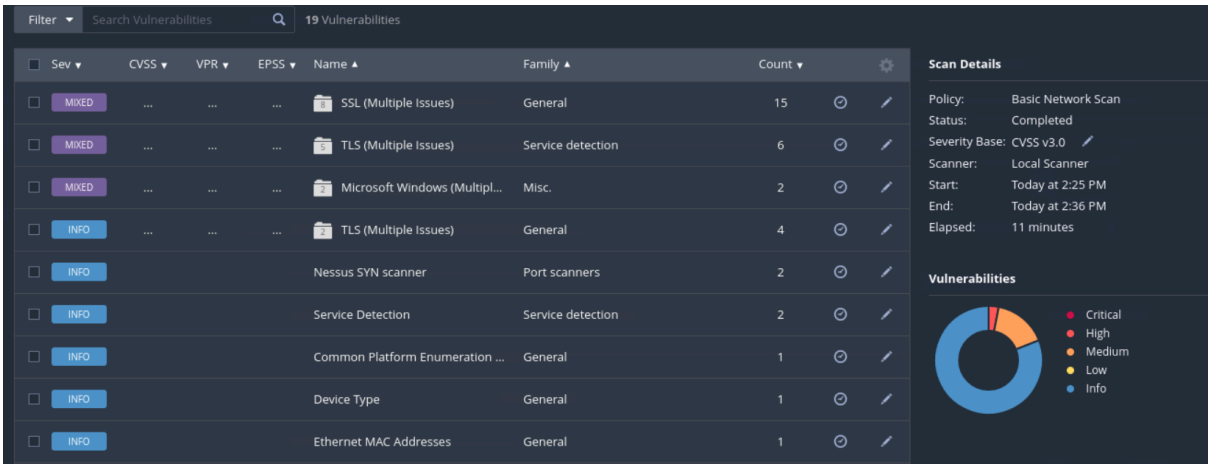
   And enter the **Windows System (IP address 172.31.8.240**) and click on **Submit.**



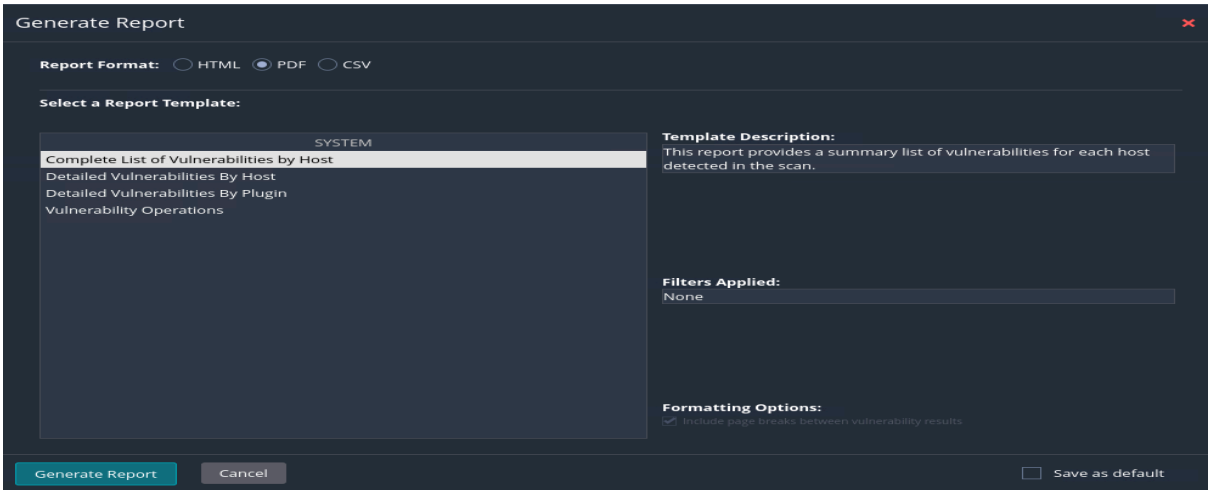




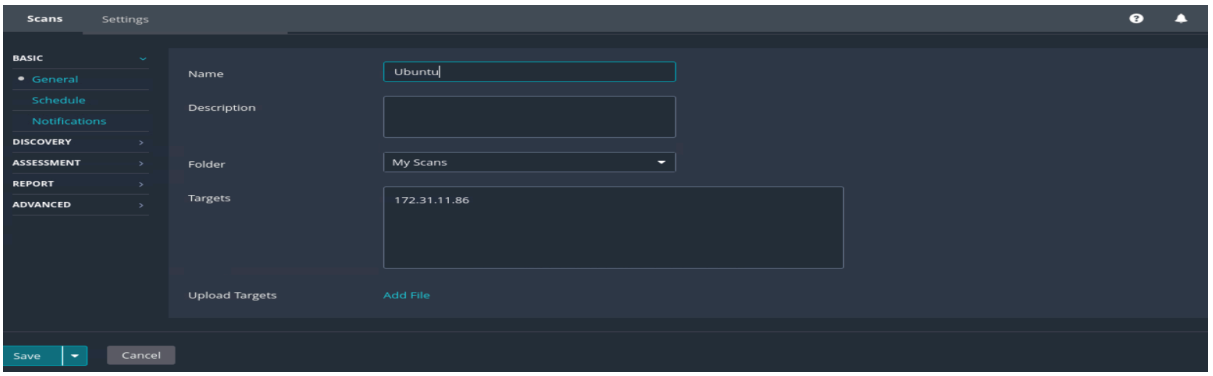
2. Click on the Vulnerabilities tab to see the issues that Nessus had found



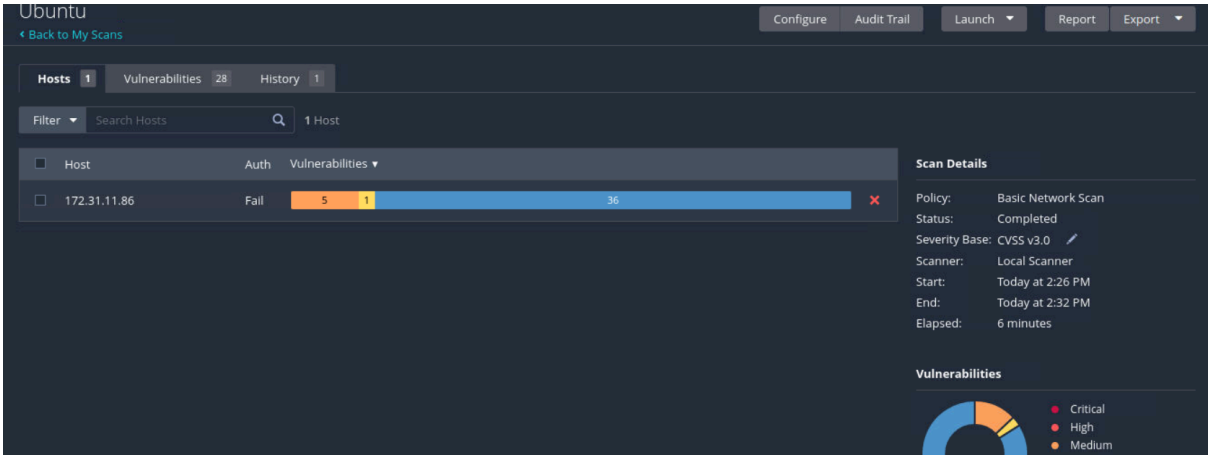
3. Click on the report and generate the report. Choose the report format (PDF, HTML, or CSV) and click on **Generate Report.**

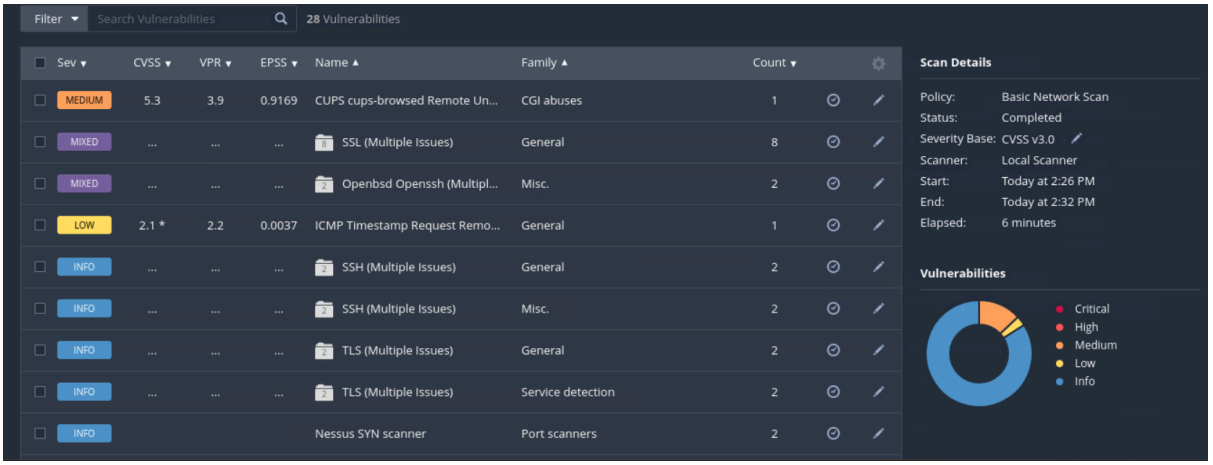


4. Check the **Debian Linux System/Ubuntu** (IP address **172.31.11.86***) and click on **Submit.**

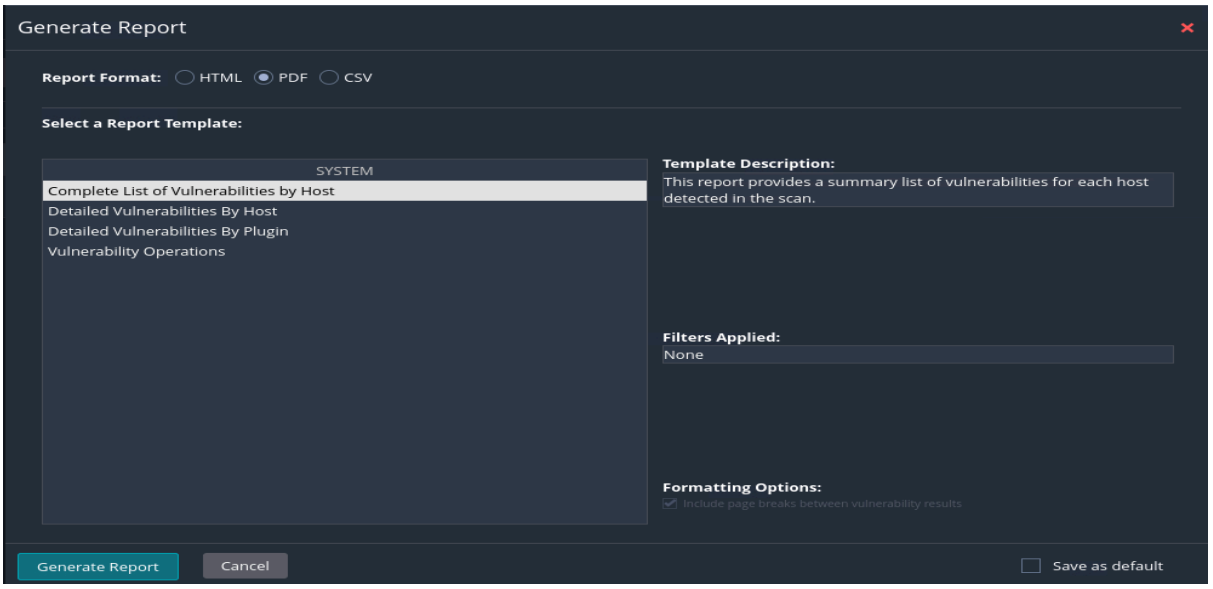


5. Click on the Vulnerabilities tab to see the issues that Nessus had found.





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



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	Exploitable?	Recommendation
42873	SWEET32 - Medium Strength Cipher	High	Yes	Disable 3DES cipher suites.
51192	SSL Certificate Cannot Be Trusted	Medium	No	Replace with CA-signed certificate.
57582	SSL Self-Signed Certificate	Medium	No	Use trusted certificates 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 No NLA	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 Prefix Truncation (CVE-2023-48795)	Medium	Yes	Update OpenSSH to patched version.
207864	CUPS Remote Printer Registration (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 expired certificates.

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.