

Experiment 05

Learning Objective: Use of Networking tools like Advance IP Scanner, Nmap, Zenmap & Nessus Scanner to scan and enumerate Active Host, Open Ports, Services Running and Vulnerability Assessment using Nessus Scanner.

Tools: Advance IP Scanner, Nmap, Zenmap & Nessus Scanner.

Theory:

Scanning is a technique that allows for a deep dive into a system to seek out valuable data and services in an IP address range. Scanning techniques locate potential entry points on a system to exploit. This type of scanning is key to ethical hackers who are responsible for preventing attacks on an organization.

Scanning is more than just port scanning, but it is a very important part of this process. Scanning allows you to identify open ports on the target system and can be used for port mapping, performing an interactive session with the operating system via those ports, or even redirecting traffic from these open ports. There are many tasks that can be performed with a scanning tool.

Scanning techniques:

Network Scanning: Network scanning is used to identify the devices and services that are running on a target network, determine their operating systems and software versions, and identify any potential security risks or vulnerabilities. Network scanning can be performed manually or automated using software tools and can target specific systems or an entire network.

Network Mapping: Scanning attacks can be used to map out a target network, including its infrastructure, servers, and devices. This information can be used to plan and execute a more sophisticated attack, such as a DDoS attack or a data breach.

Vulnerability Scanning: Vulnerability scanning is a process of identifying, locating, and assessing the security vulnerabilities of a computer system, network, or application. This process is performed using automated software tools that scan for known vulnerabilities, as well as weaknesses in the configuration or implementation of the system being tested.

Implementation:

Using Advance IP Scanner

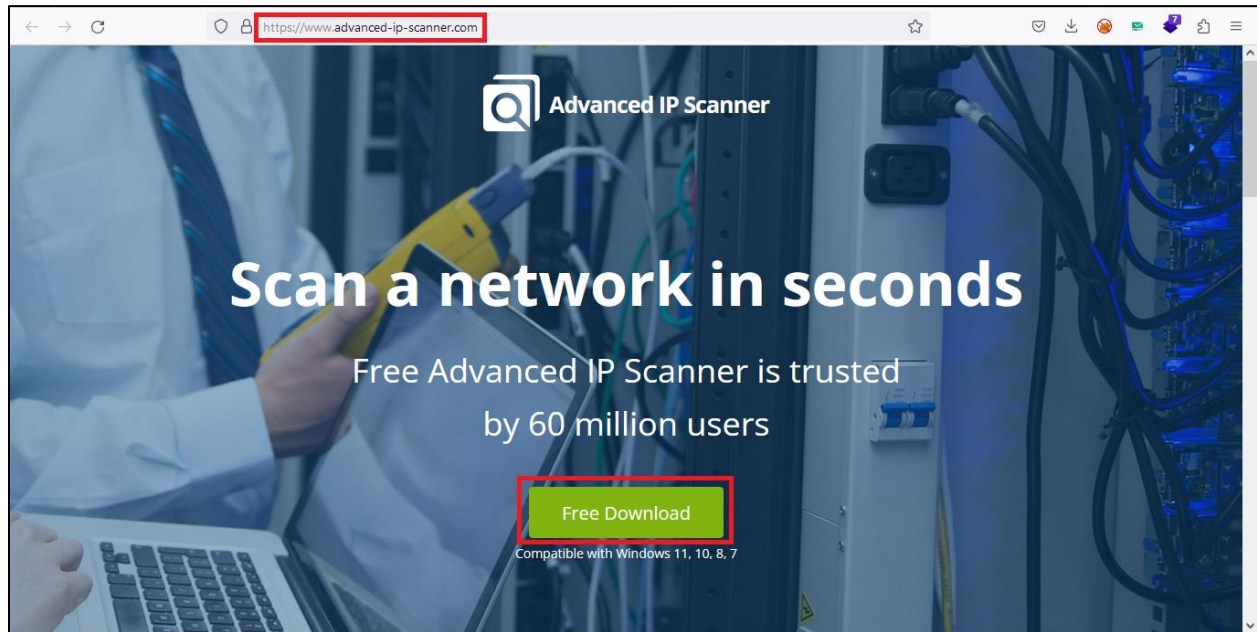
Reliable and free network scanner to analyze LAN. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off. It is easy to use and runs as a portable edition. It should be the first choice for every network admin.

Installation of Advance IP Scanner

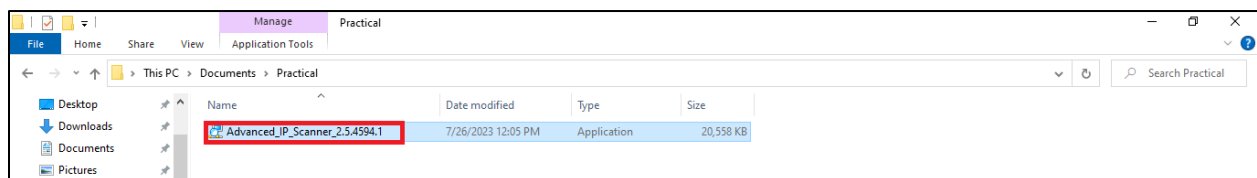
If we want to install the Advance IP Scanner in windows, we can use the following steps:

Step 1: First, we need to go to the Advance IP Scanner Website through the <https://www.advanced-ip-scanner.com> in the system's internet browser. It is the link where we will download the Advance IP Scanner setup file.

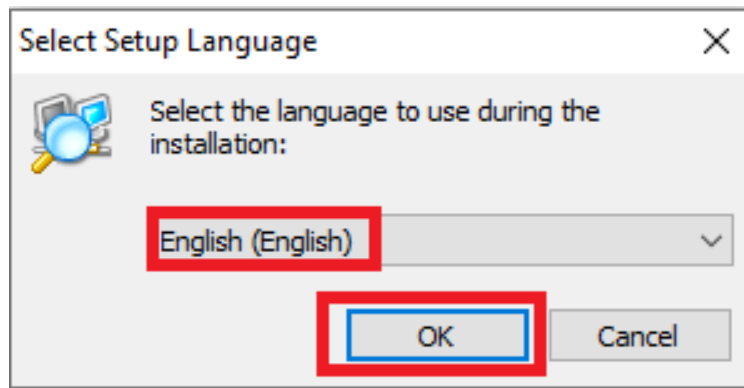
Step 2: Click on the Free Download button, which appears on a green button on the page.



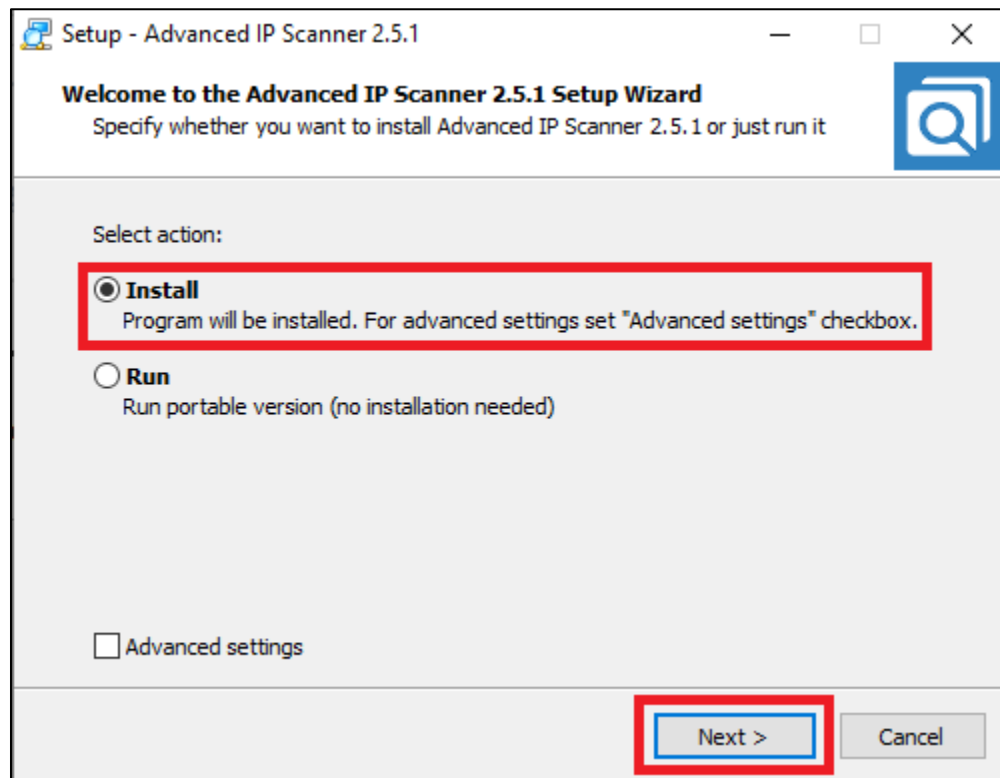
Step 3: Now, launch the Advance IP Scanner EXE file from where we have downloaded this file in the system. After that, the Advance IP Scanner installation window will open.



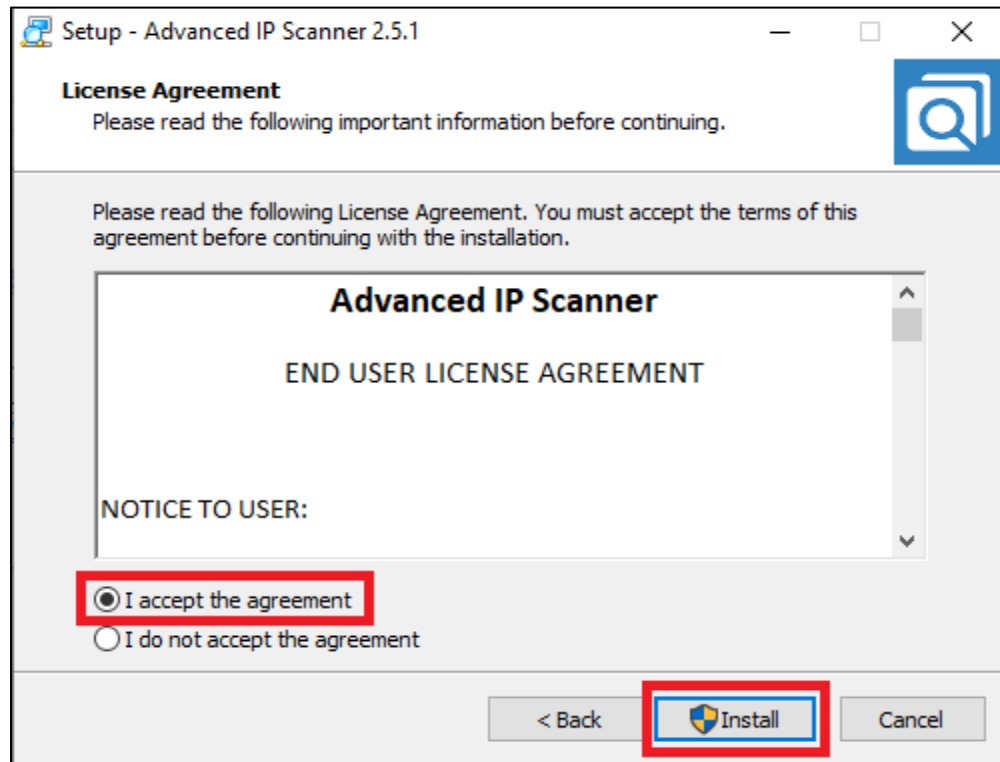
Step 4: Select the language and click on the OK button.



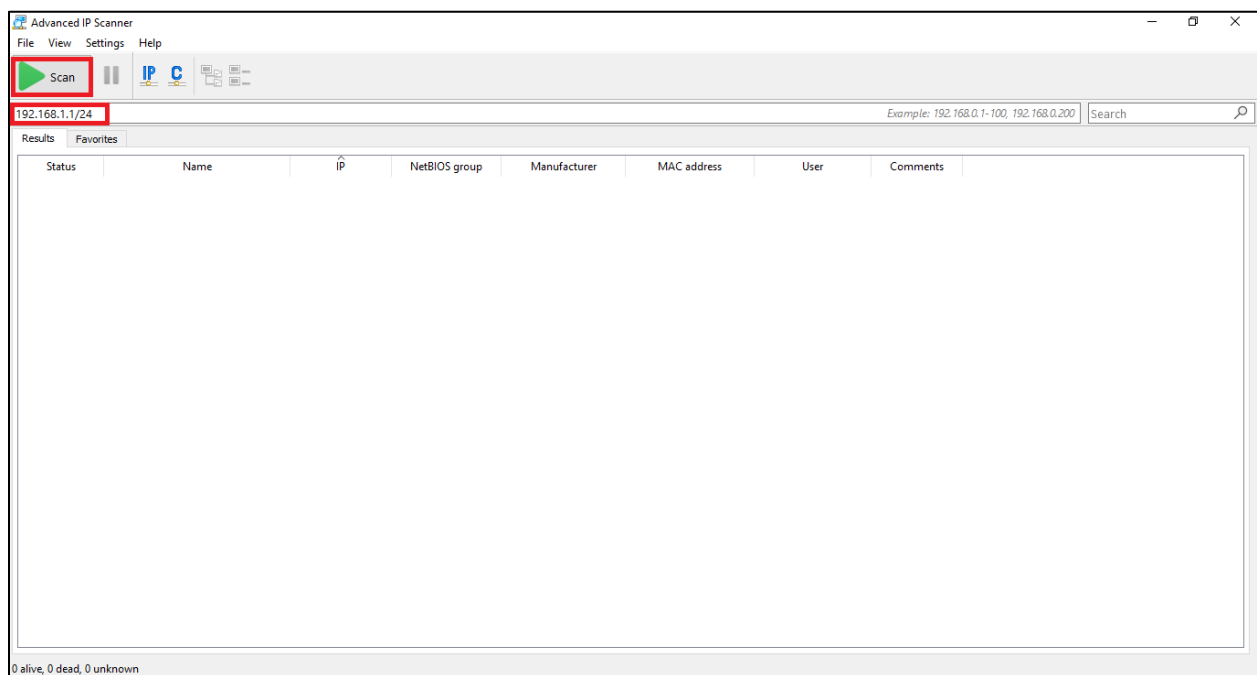
Step 5: Select the action Install and click on the Next button.



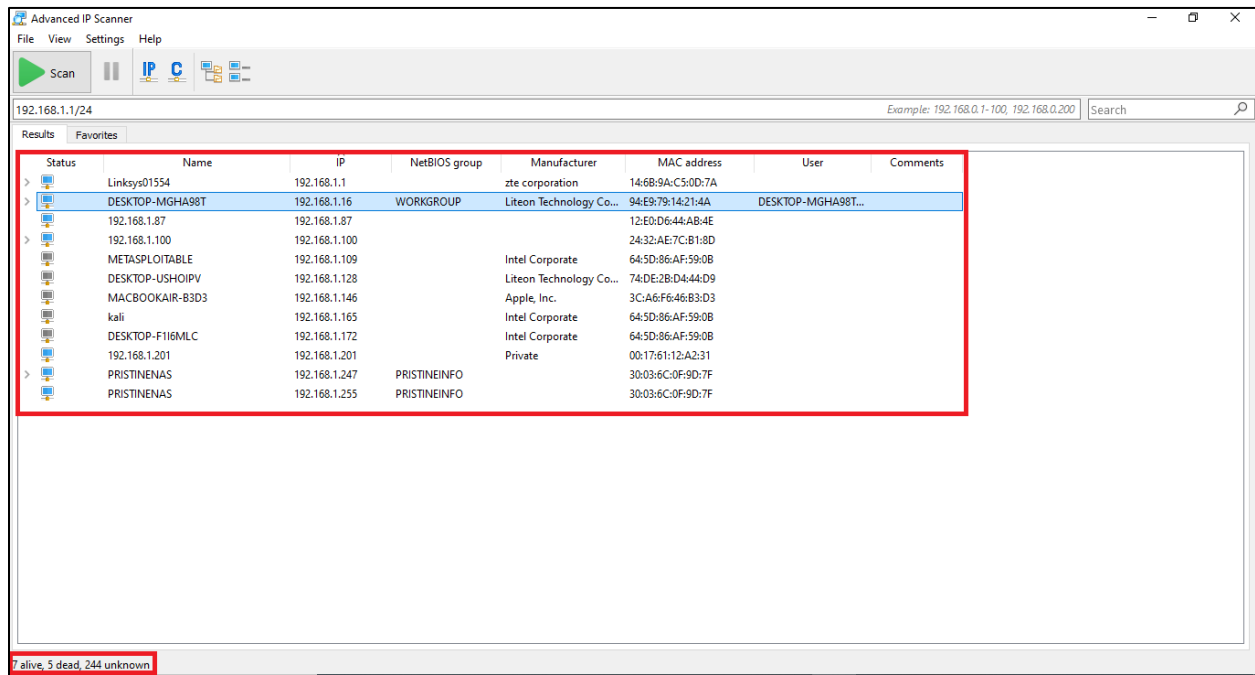
Step 6: Accept the User License Agreement and click on the Install button.



Step 7: Enter the Subnet Range and click on the Scan button.



Step 8: Once the scan is completed you will see the number of IP address which are live and host name.



Advanced IP Scanner

File View Settings Help

Scan

192.168.1.1/24

Example: 192.168.0.1-100, 192.168.0.200 Search

Status	Name	IP	NetBIOS group	Manufacturer	MAC address	User	Comments
>	Linksys01554	192.168.1.1		zte corporation	14:6B:9A:C5:0D:7A		
>	DESKTOP-MGHA98T	192.168.1.16	WORKGROUP	Liteon Technology Co...	94:E9:79:14:21:4A	DESKTOP-MGHA98T...	
>	192.168.1.87	192.168.1.87			12:E0:D6:44:AB:4E		
>	192.168.1.100	192.168.1.100			24:32:AE:7C:B1:8D		
>	METASPLOITABLE	192.168.1.109		Intel Corporate	64:5D:86:AF:59:08		
>	DESKTOP-USHOIPV	192.168.1.128		Liteon Technology Co...	74:DE:2B:D4:44:D9		
>	MACBOOKAIR-B3D3	192.168.1.146		Apple, Inc.	3C:A6:F6:46:B3:D3		
>	kali	192.168.1.165		Intel Corporate	64:5D:86:AF:59:08		
>	DESKTOP-F116MLC	192.168.1.172		Intel Corporate	64:5D:86:AF:59:08		
>	192.168.1.201	192.168.1.201		Private	00:17:61:12:A2:31		
>	PRISTINENAS	192.168.1.247	PRISTINEINFO		30:03:6C:0F:9D:7F		
>	PRISTINENAS	192.168.1.255	PRISTINEINFO		30:03:6C:0F:9D:7F		

7 alive, 5 dead, 244 unknown

Using Nmap Scanner

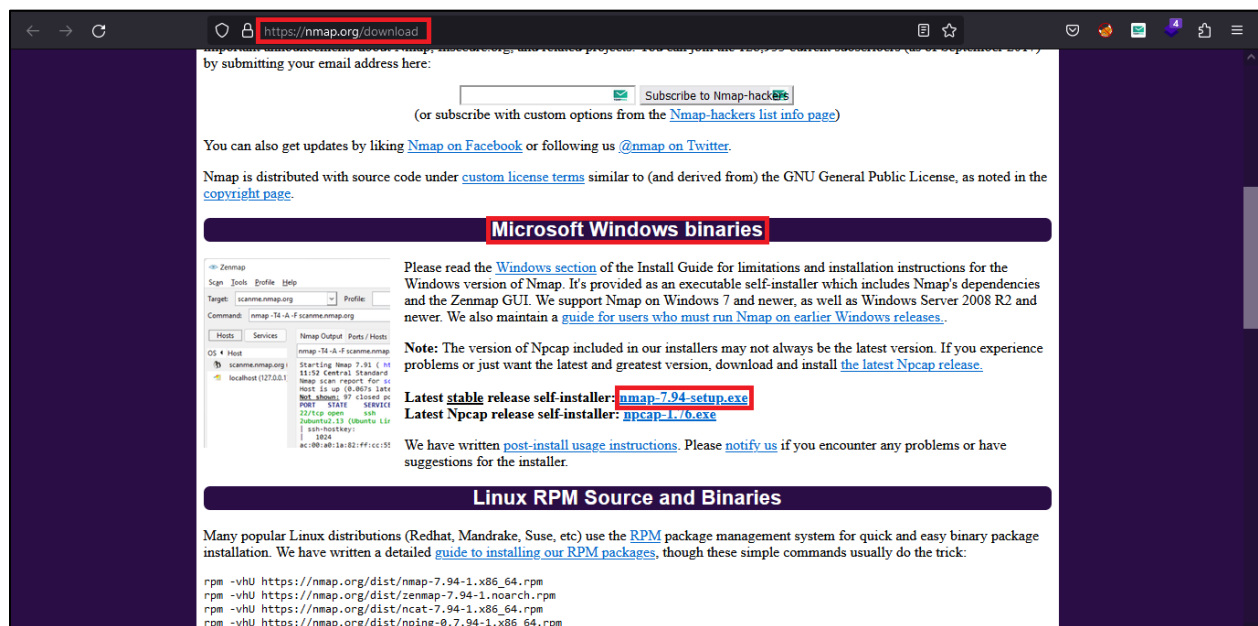
Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides several features for probing computer networks, including host discovery and service and operating system detection.

Installation of Nmap & Zenmap

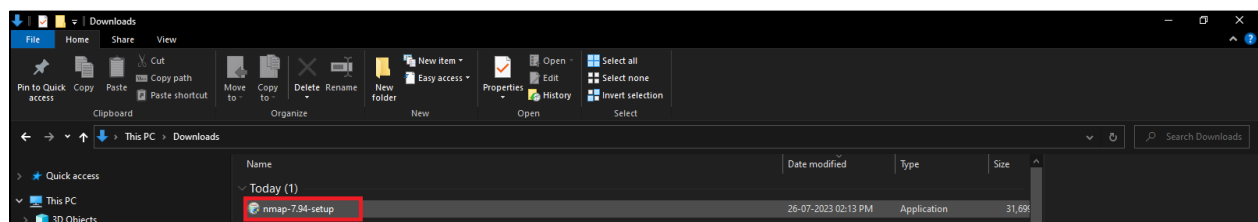
If we want to install the Nmap in windows, we can use the following steps:

Step 1: First, we need to go to the Nmap Website through the <https://nmap.org/download> in the system's internet browser. It is the link where we will download the Nmap setup file.

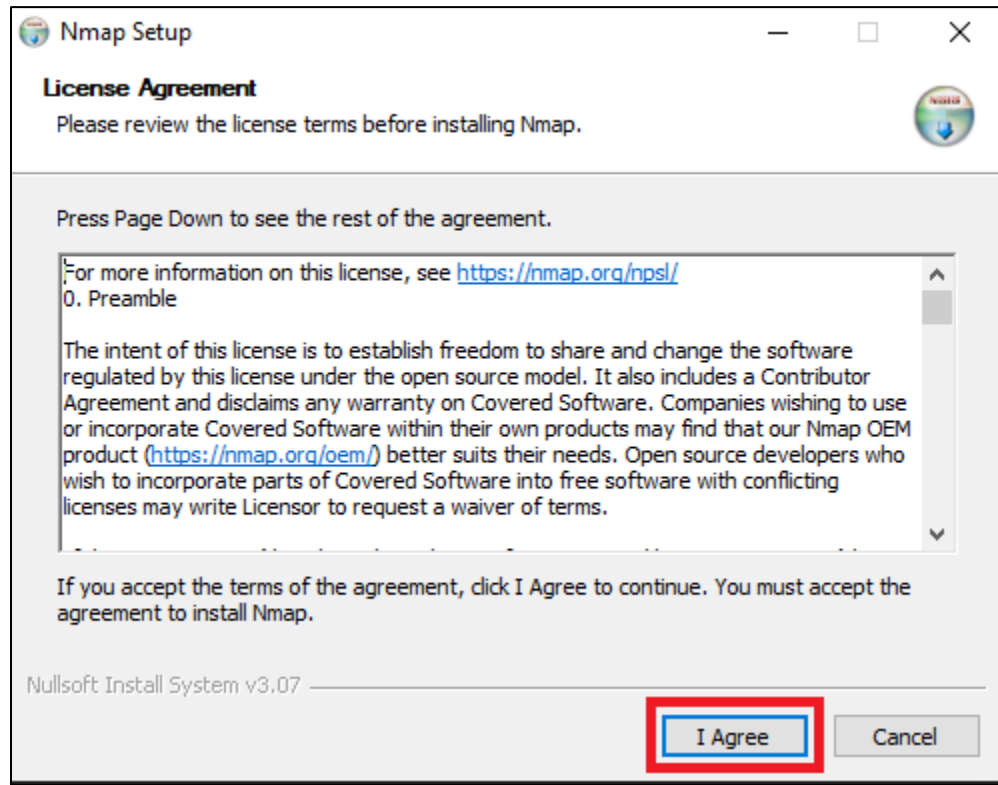
Step 2: Click on the Nmap Setup button to download setup file.



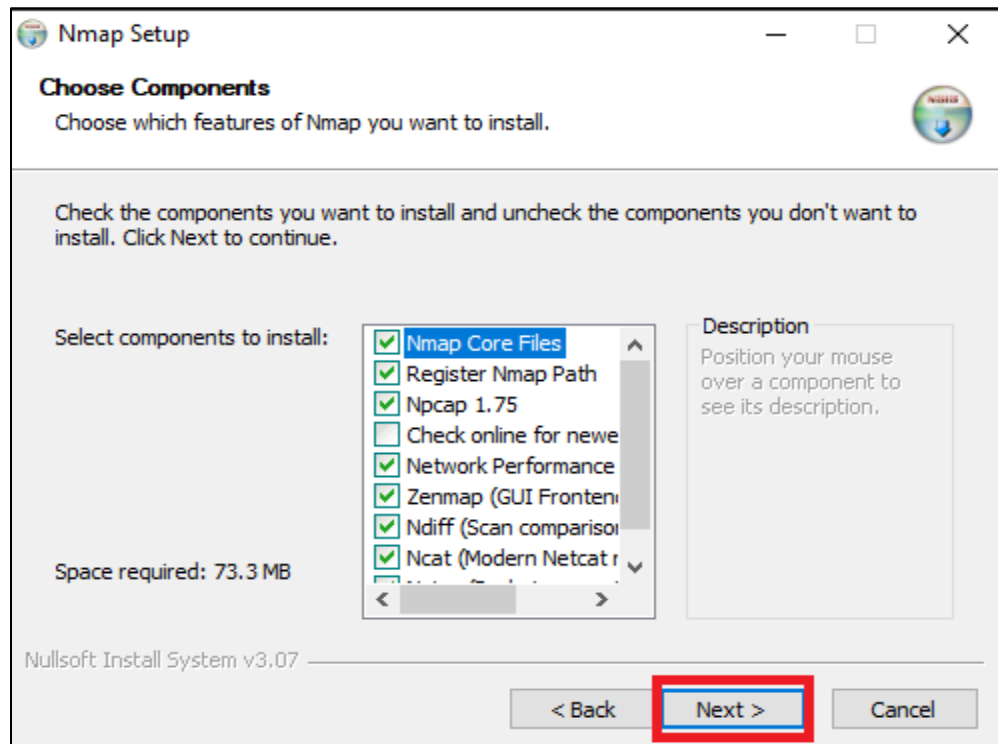
Step 3: Now, launch the Nmap EXE file from where we have downloaded this file in the system. After that, the Nmap installation window will open.



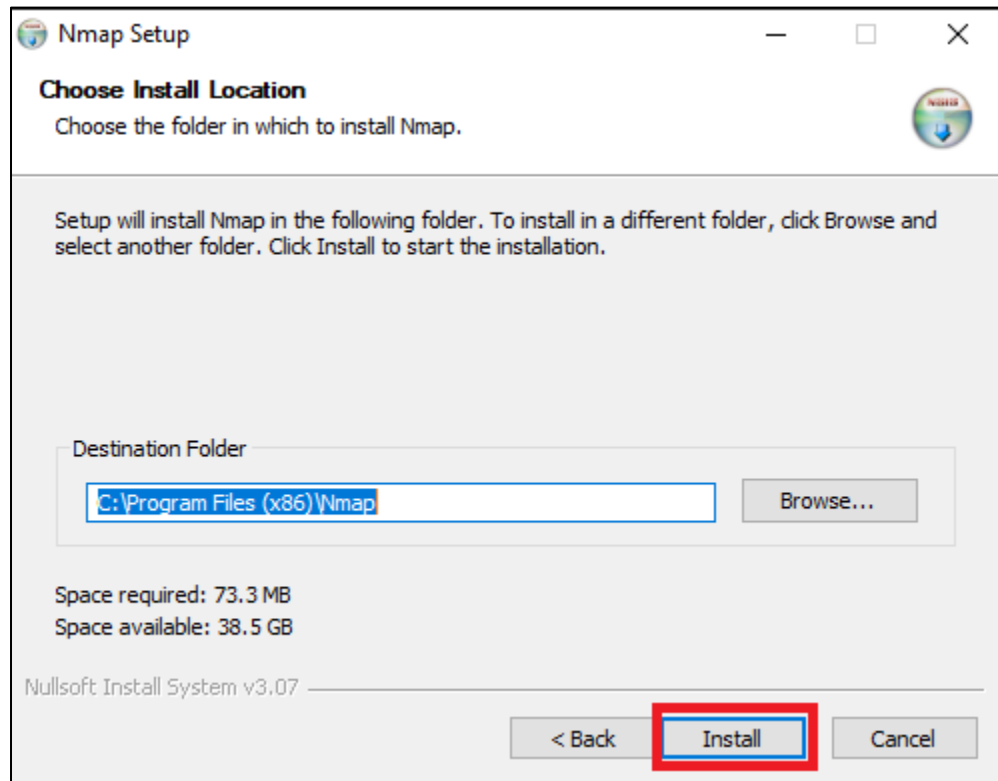
Step 4: Accept the User License Agreement and click on the Install button.



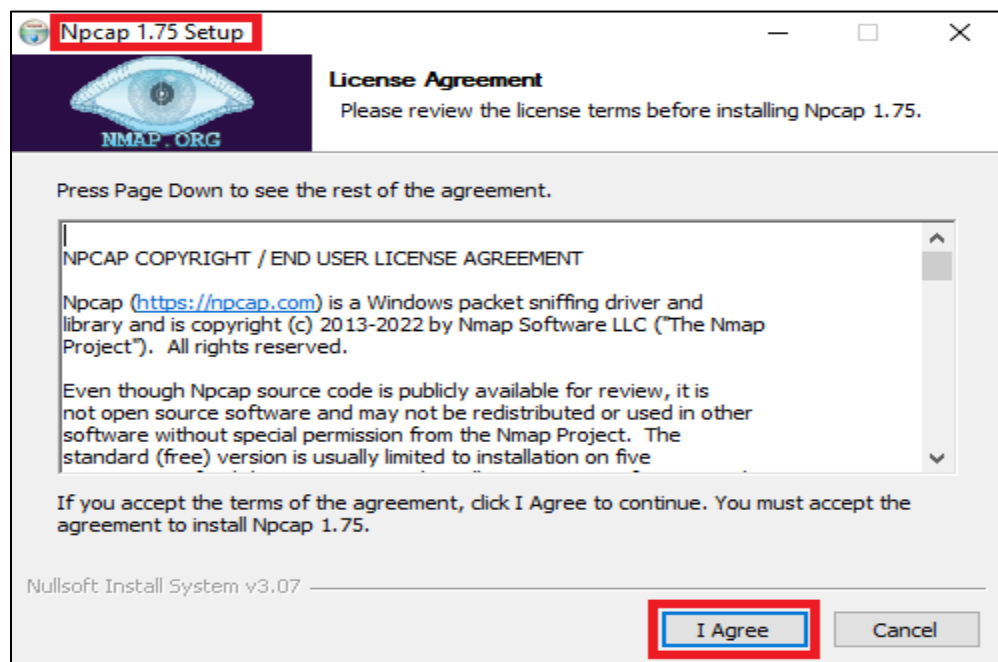
Step 5: Click on the Next button.



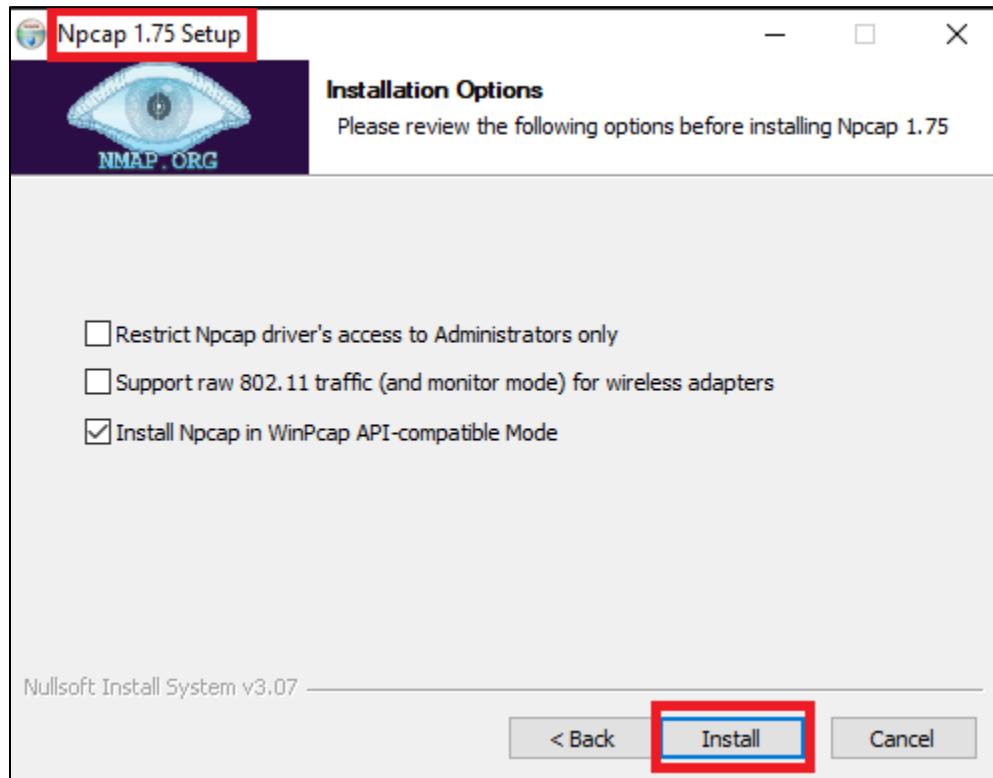
Step 6: Click on the Install button.



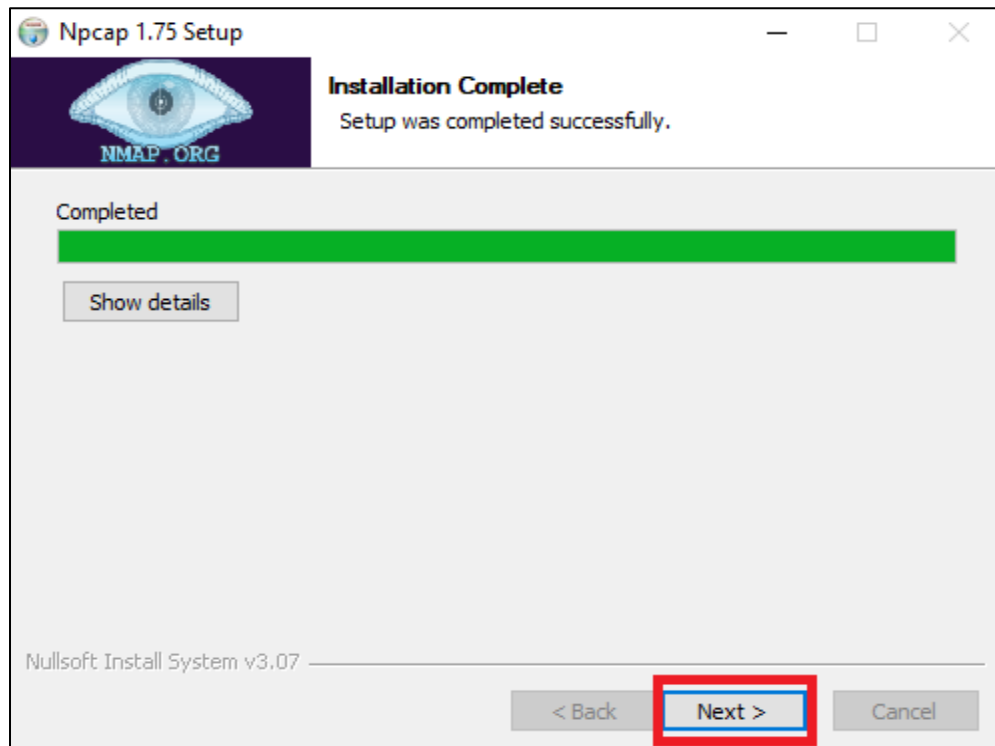
Step 7: Npcap is pre-requirement of Nmap it will be automatically installed, click on the I agree button.



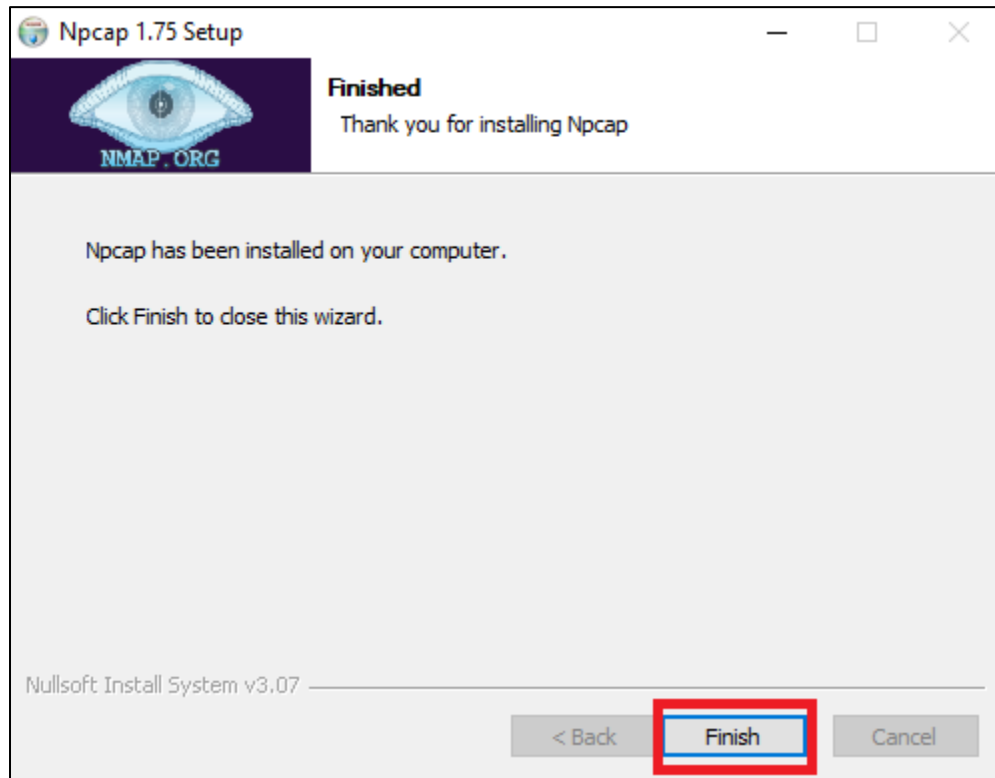
Step 8: Click on the Install button.



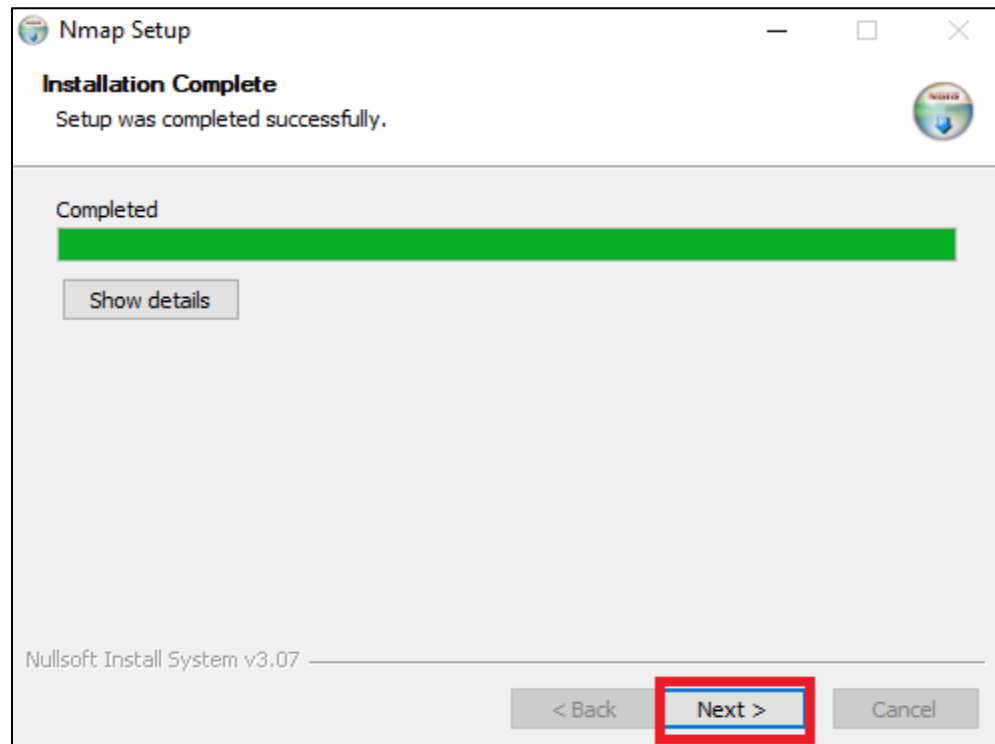
Step 9: Click on the Next button.



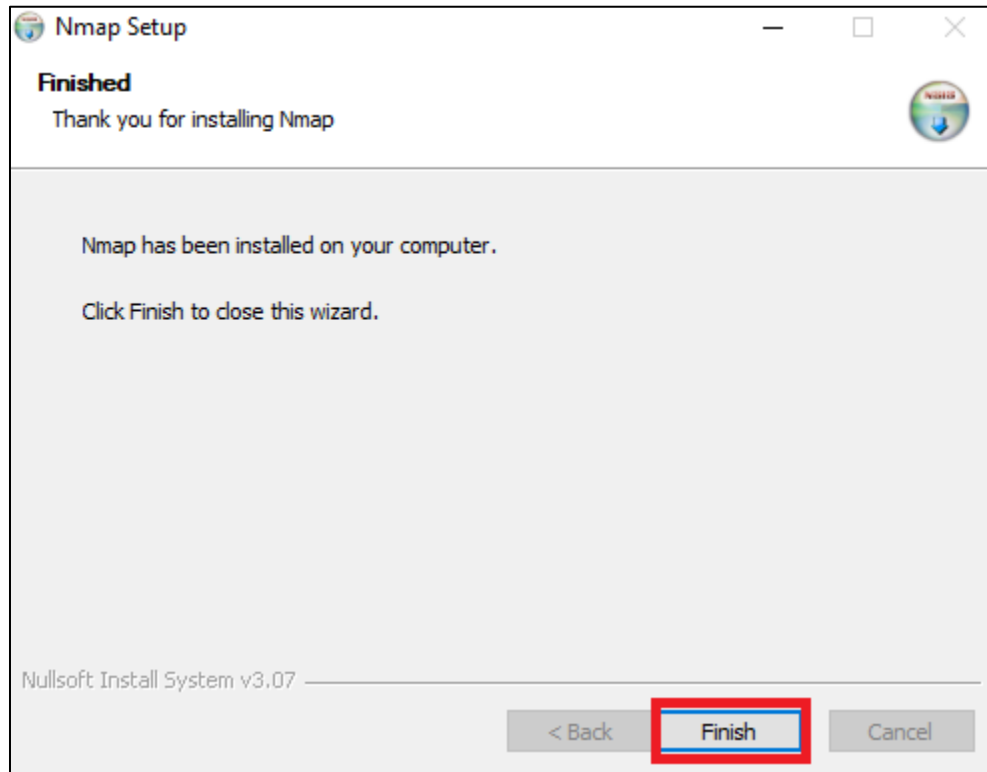
Step 10: Click on the Finish button.



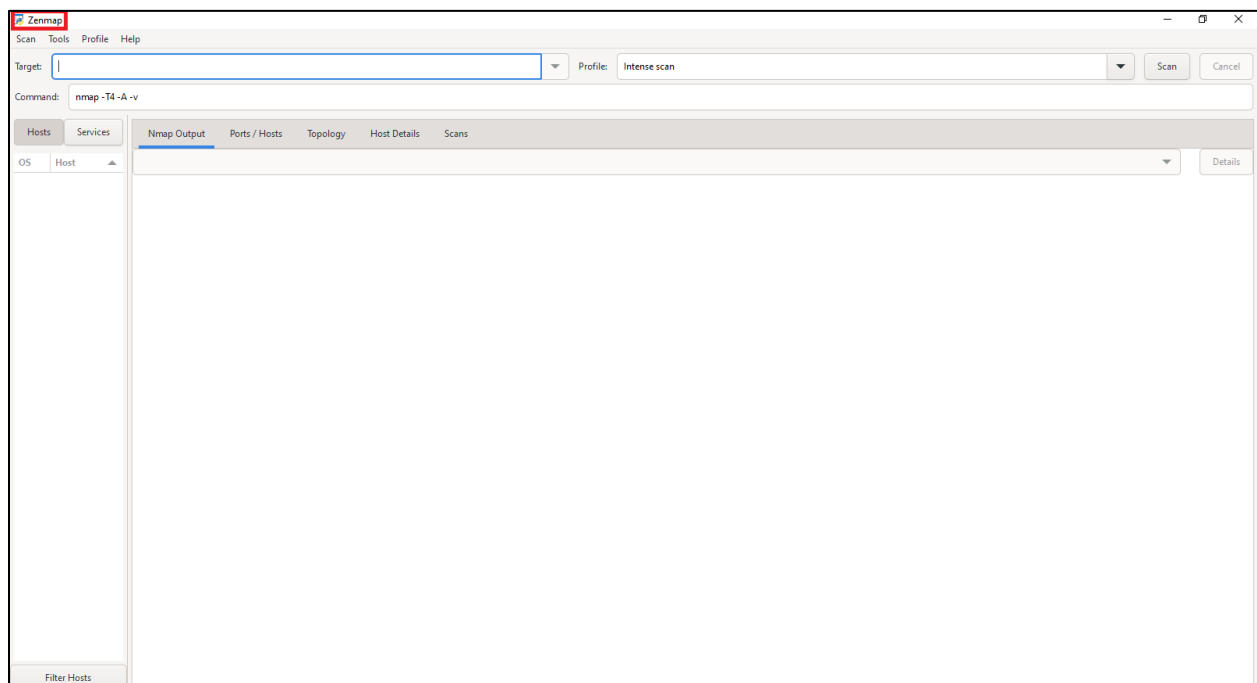
Step 11: Click on the Next button.



Step 12: Click on the Finish button, Nmap setup has been completed now we can launch Nmap in **GUI mode**, which is known as **Zenmap** and, we can launch **Nmap in CLI** which is called Nmap.



Step 13: Zenmap Interface where we can scan targets in **GUI mode**.



Step 14: Nmap where we can scan target in **CLI mode**.

```
C:\Users\Admin: nmap
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
```

Using Nessus Scanner

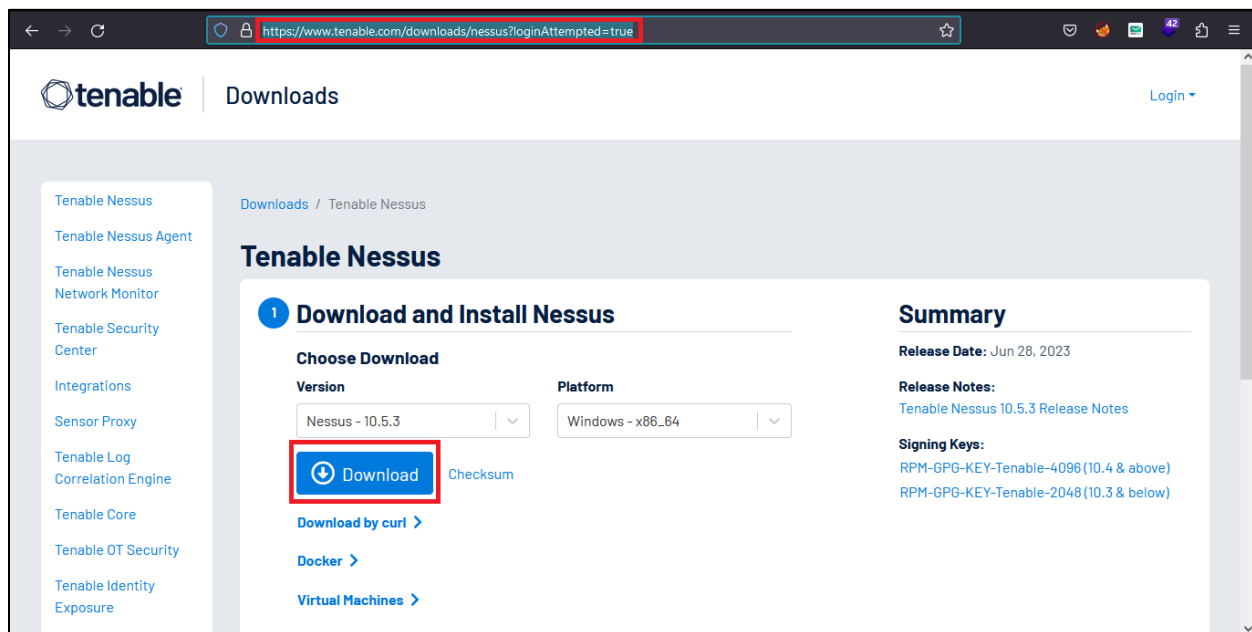
Nessus is a scanner developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

Installation of Nessus Scanner

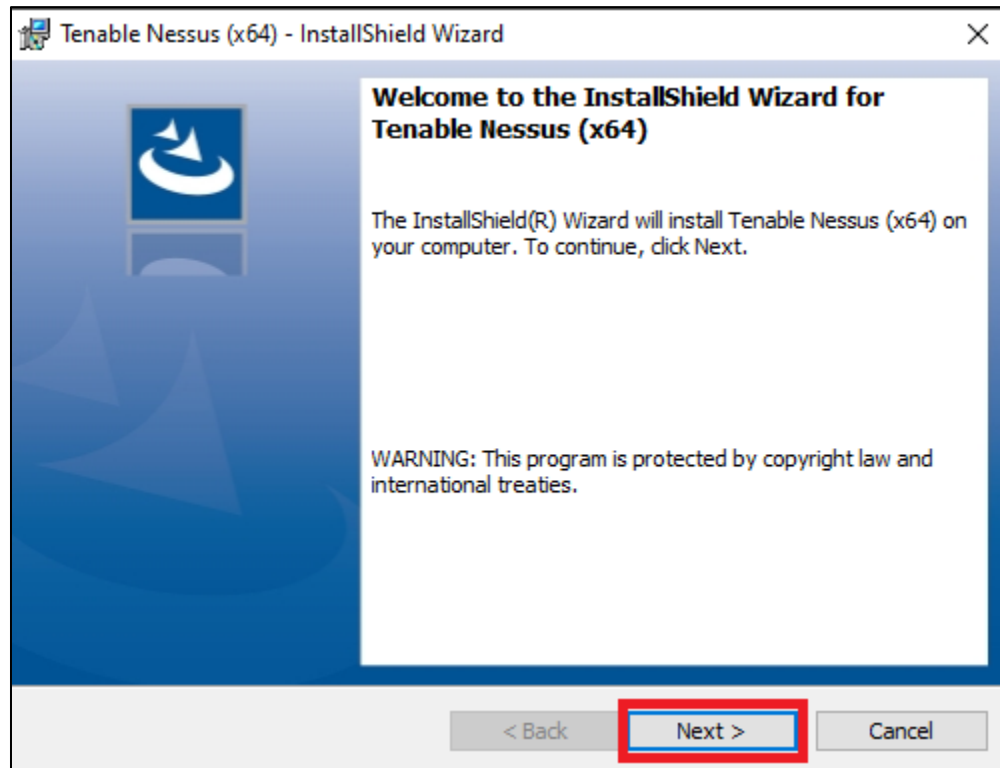
If we want to install the Nessus Scanner in windows, we can use the following steps:

Step 1: First, we need to go to the Nessus Scanner Website through the <https://www.tenable.com/downloads/nessus?loginAttempted=true> in the system's internet browser. It is the link where we will download the Nessus Scanner setup file.

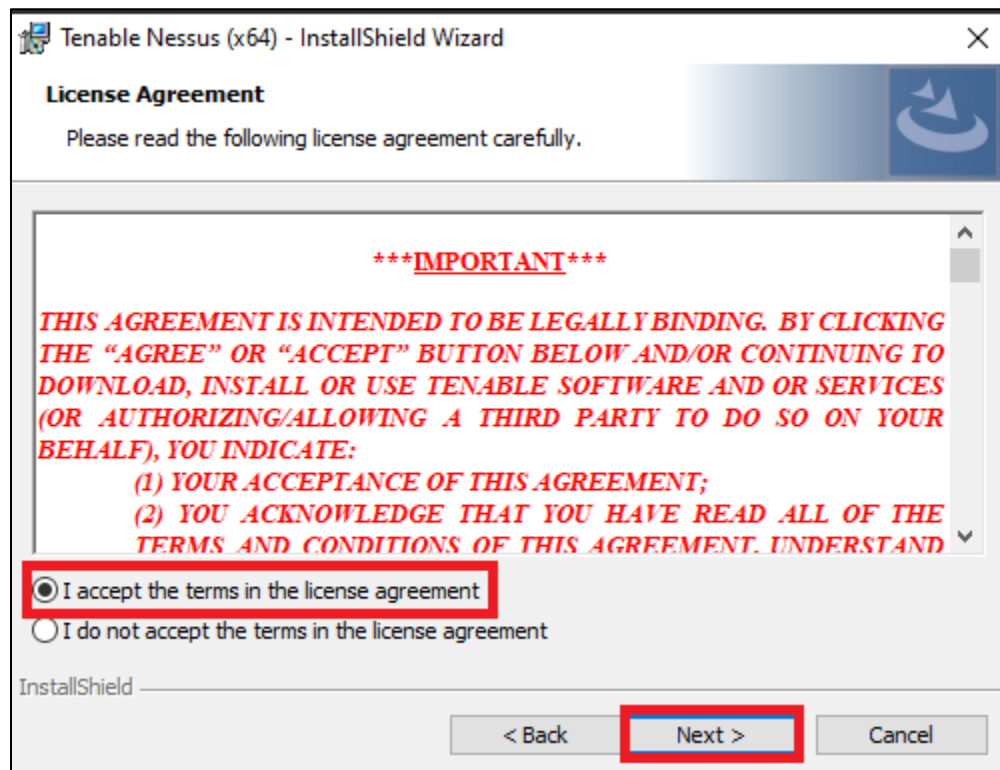
Step 2: Click on the Download button, which appears on a blue button on the page.



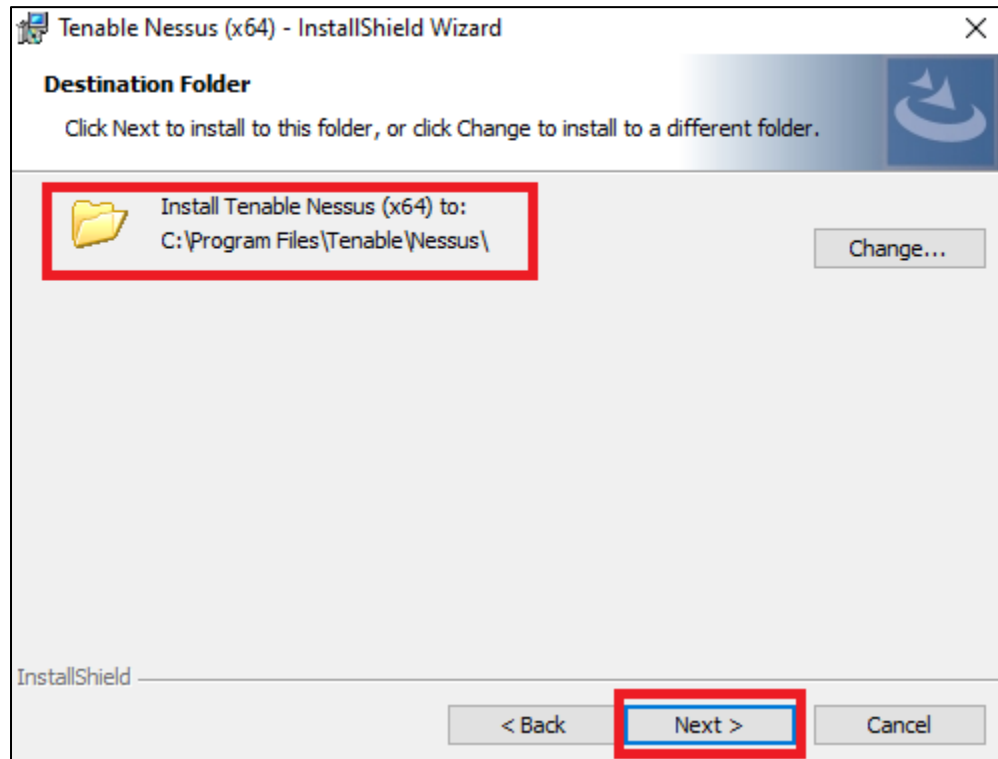
Step 3: Click on the Next button.



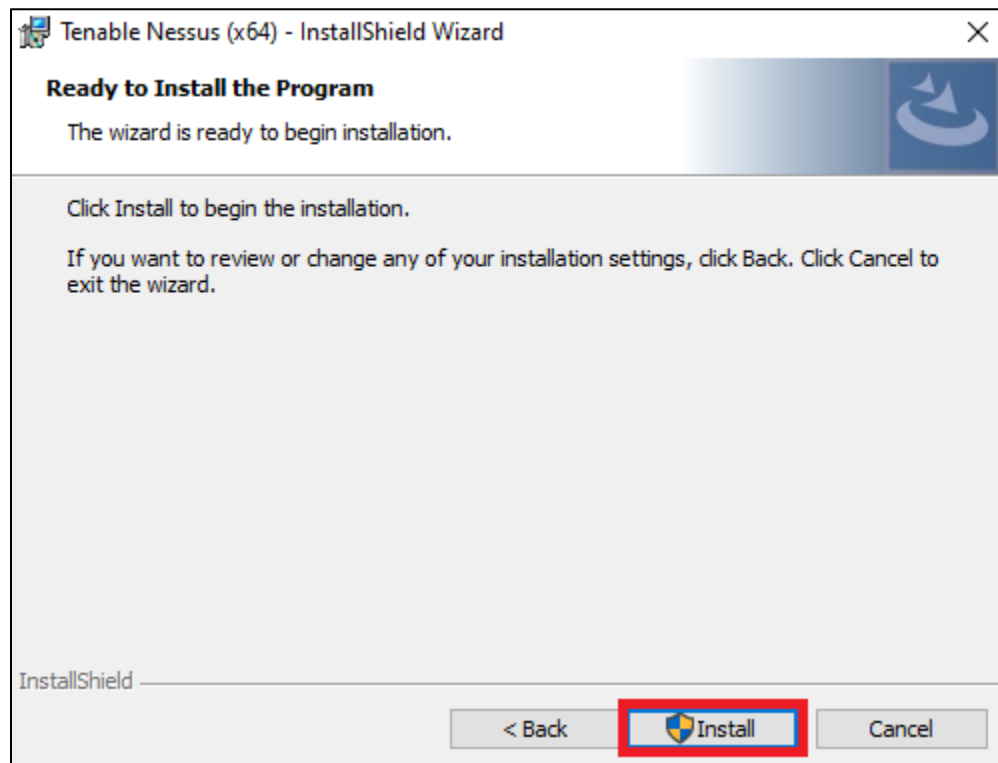
Step 4: Accept the User License Agreement and click on the Install button.



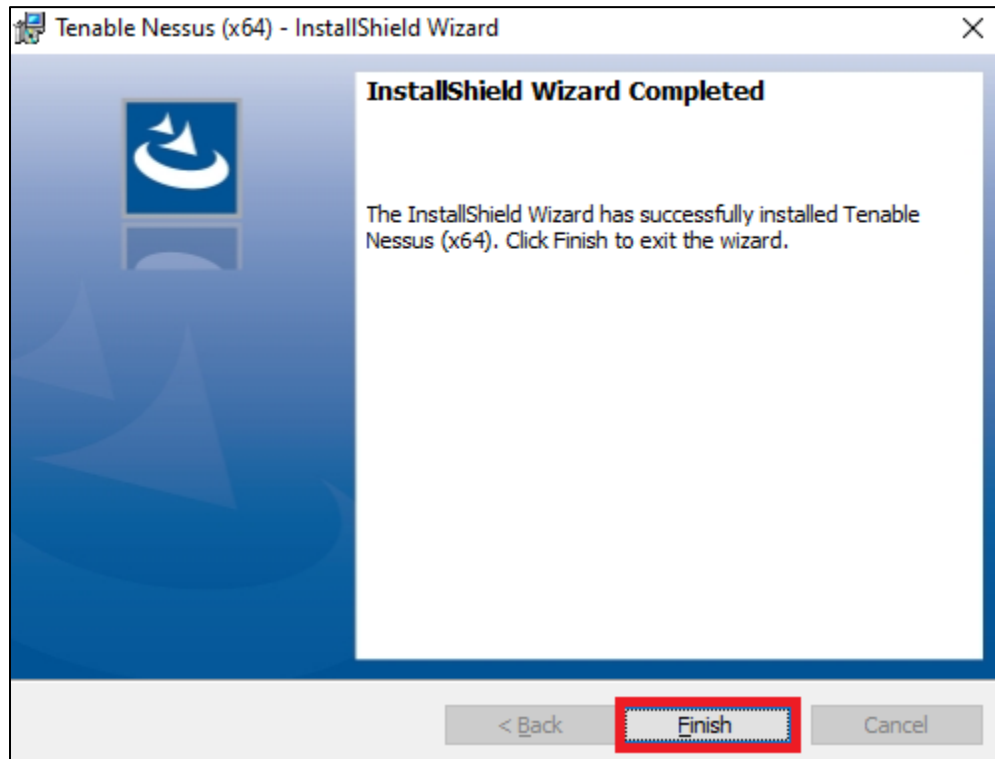
Step 5: Click on the Next button.



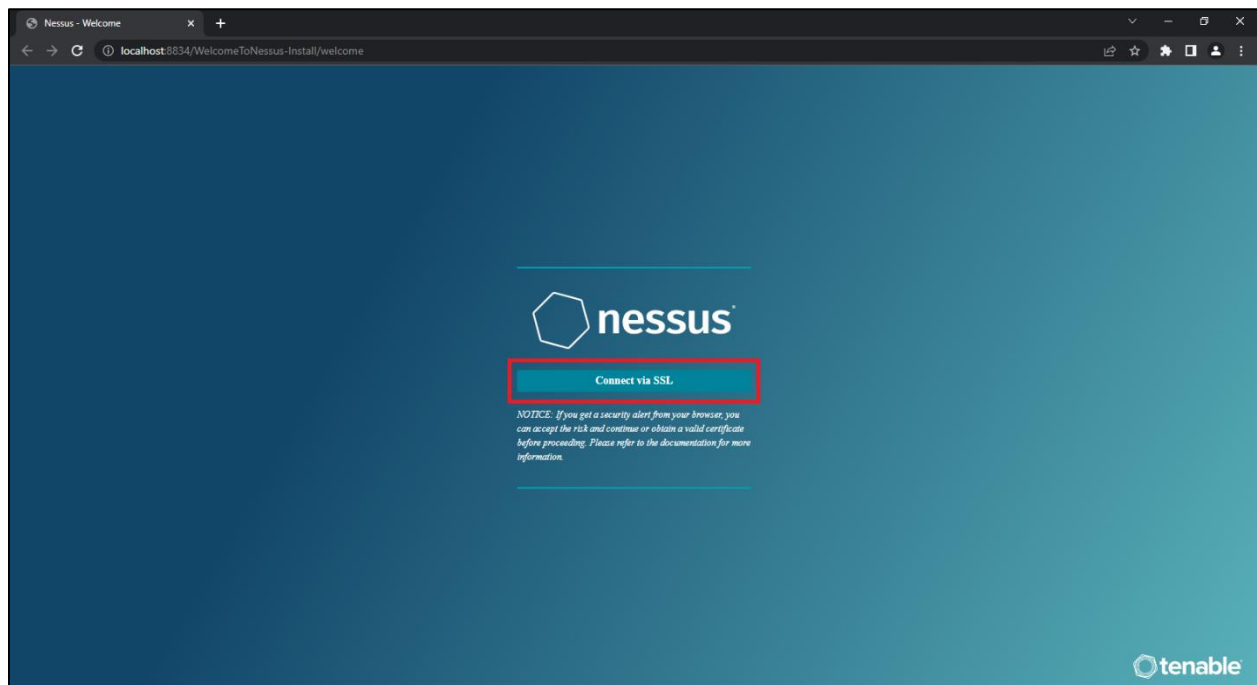
Step 6: Click on the Install button.



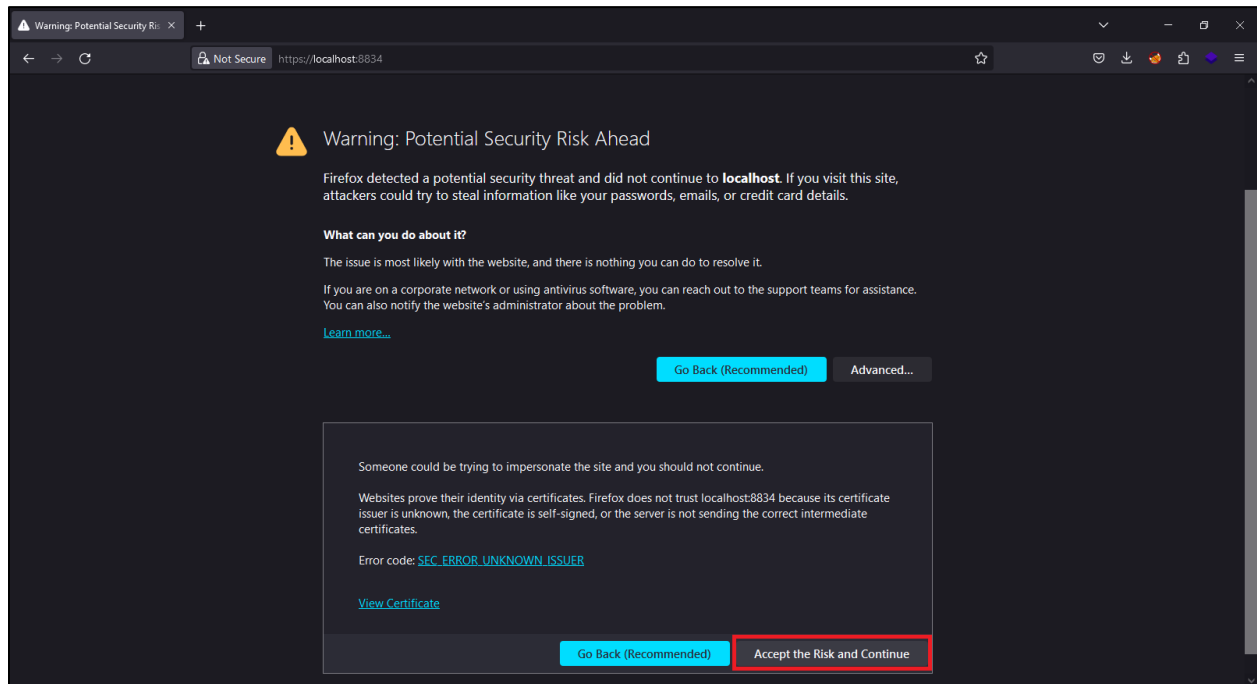
Step 7: Click on the Finish button.



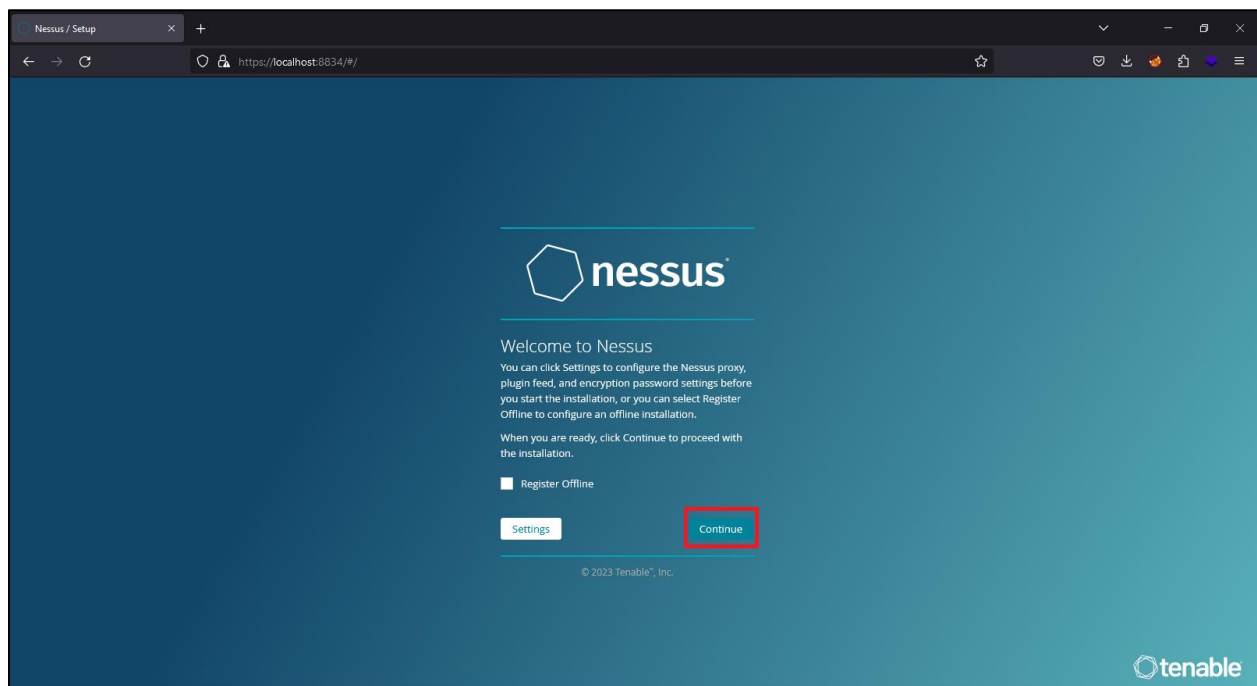
Step 8: Click on the Connect via SSL button.



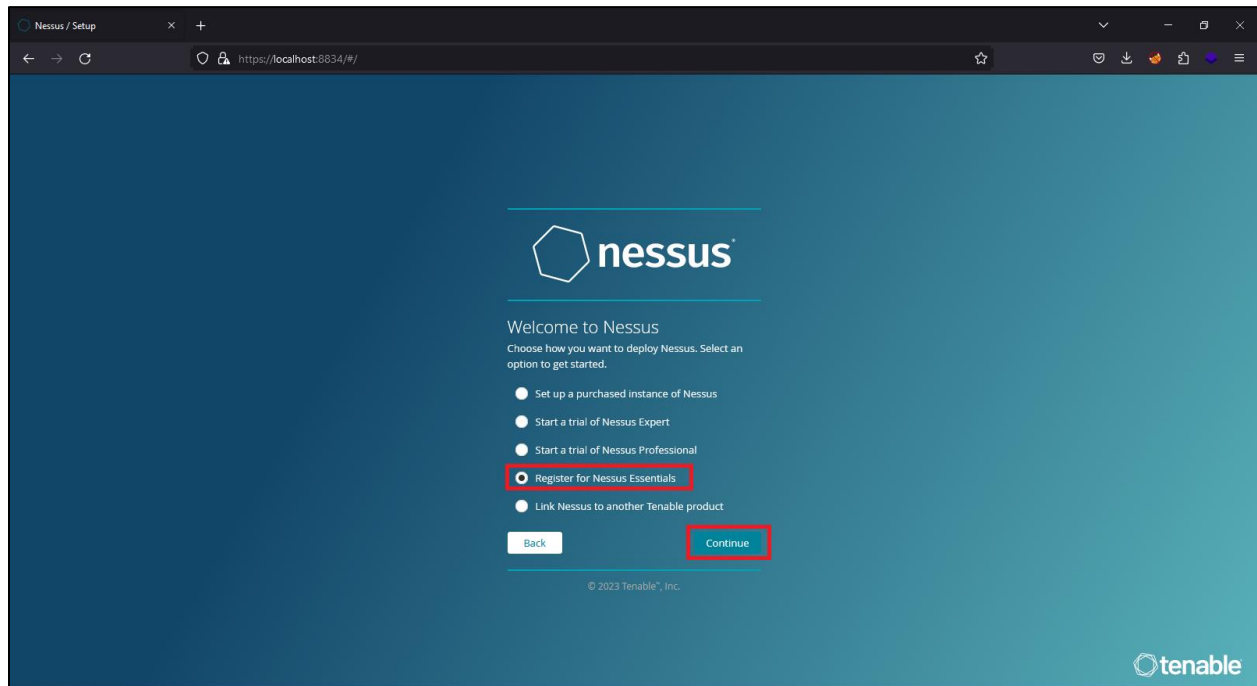
Step 9: Click on the Accept the Risk and Continue button.



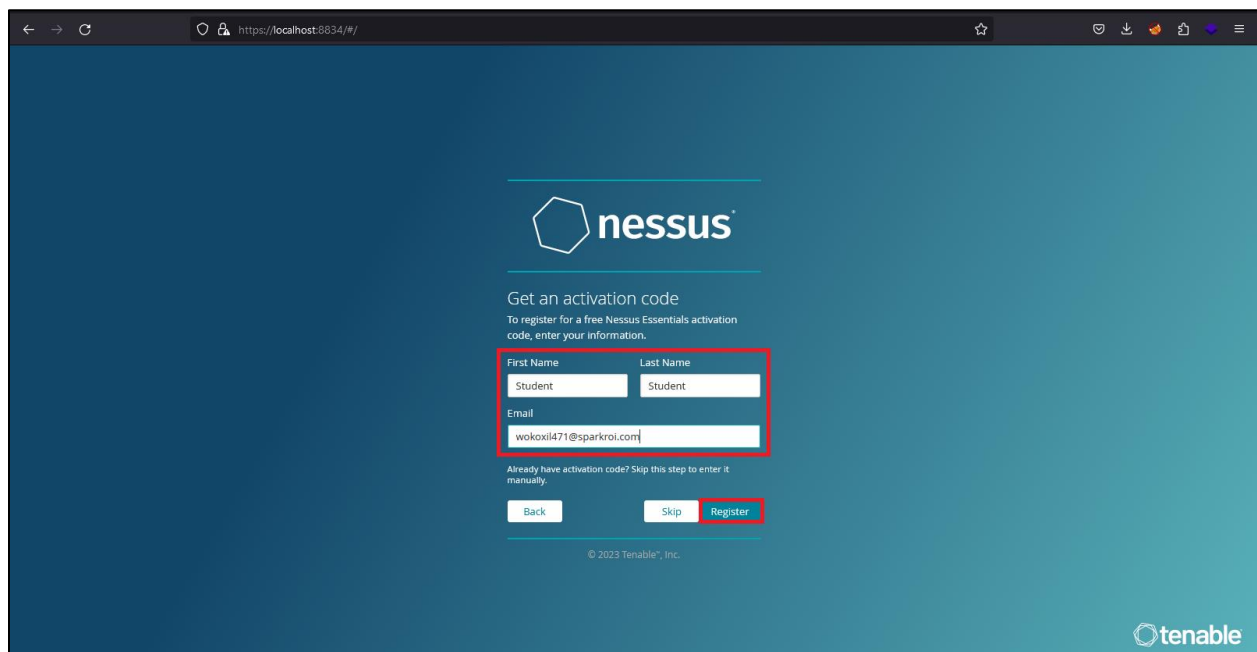
Step 10: Click on the Continue button.



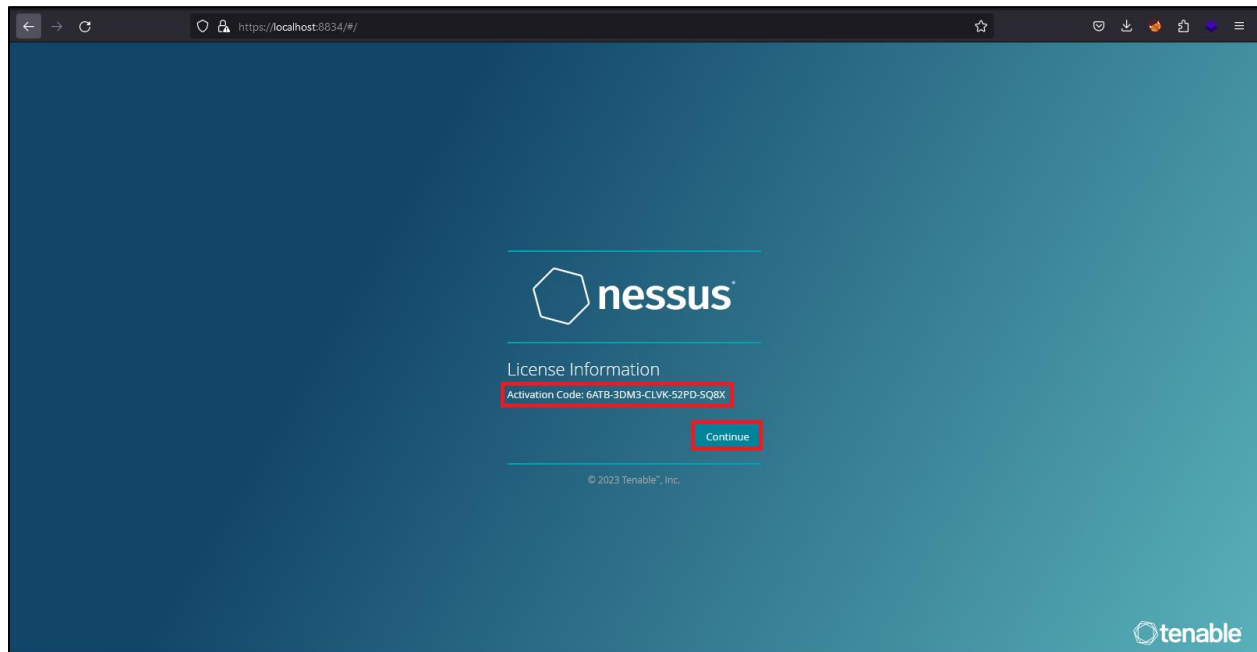
Step 11: Select the Register for Nessus Essentials and click on the Continue button.



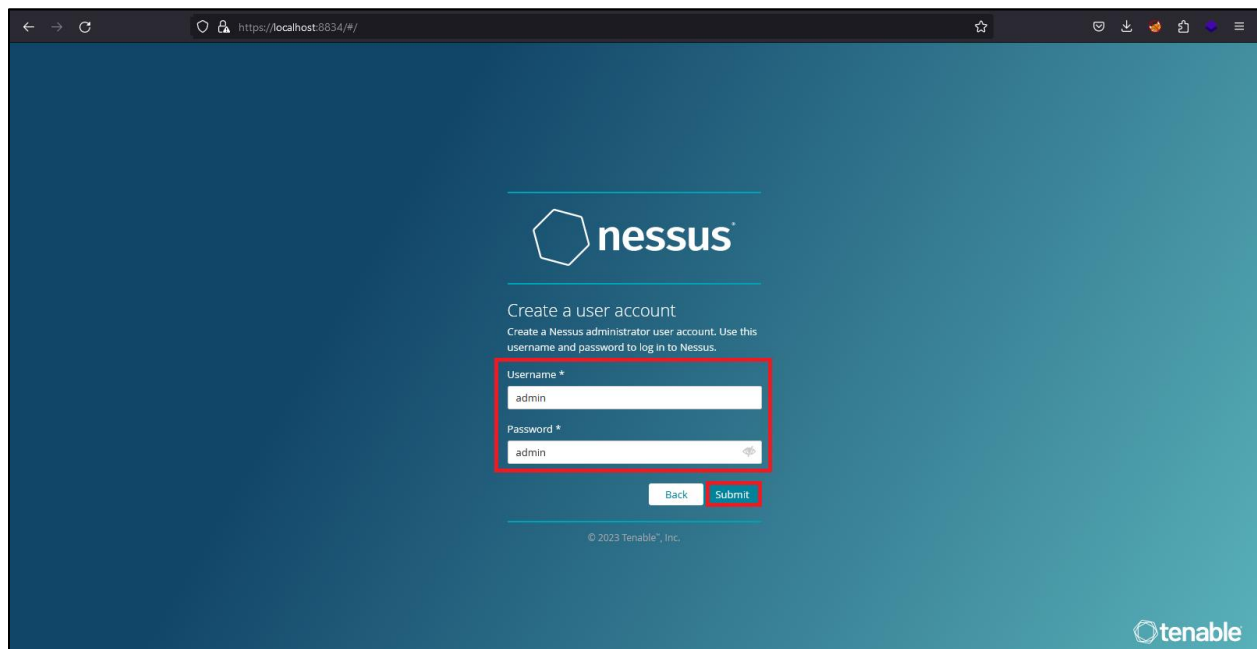
Step 12: Enter the user details and click on the Register button.



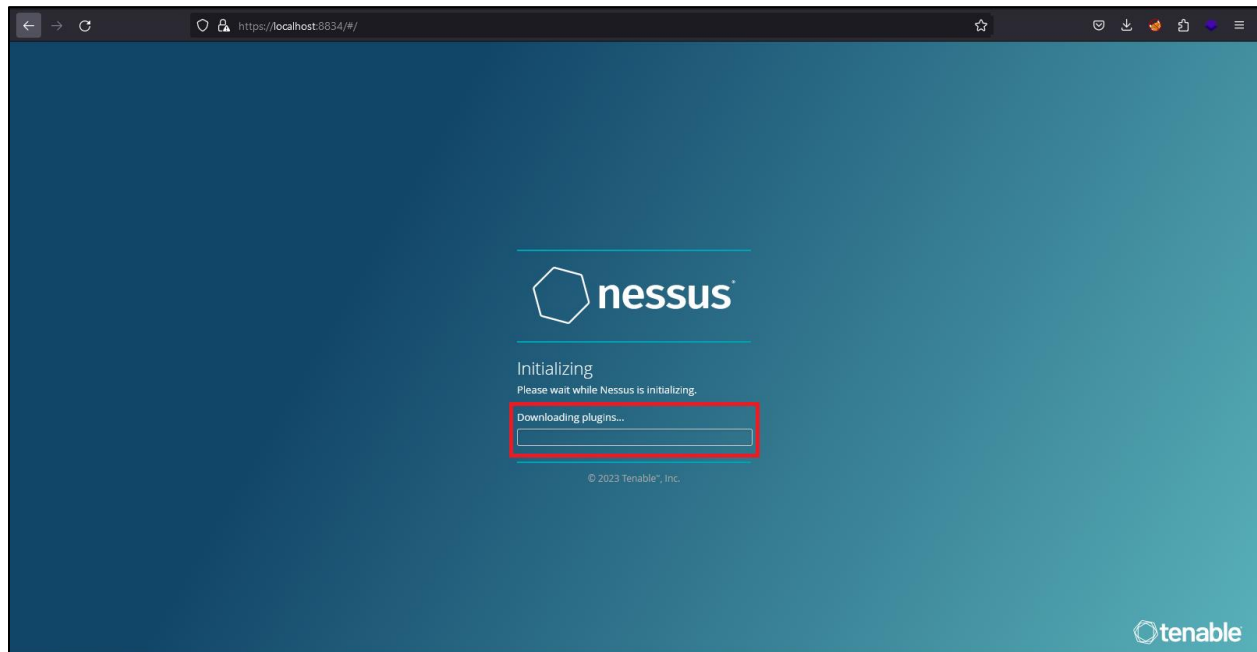
Step 13: Click on the Continue button.



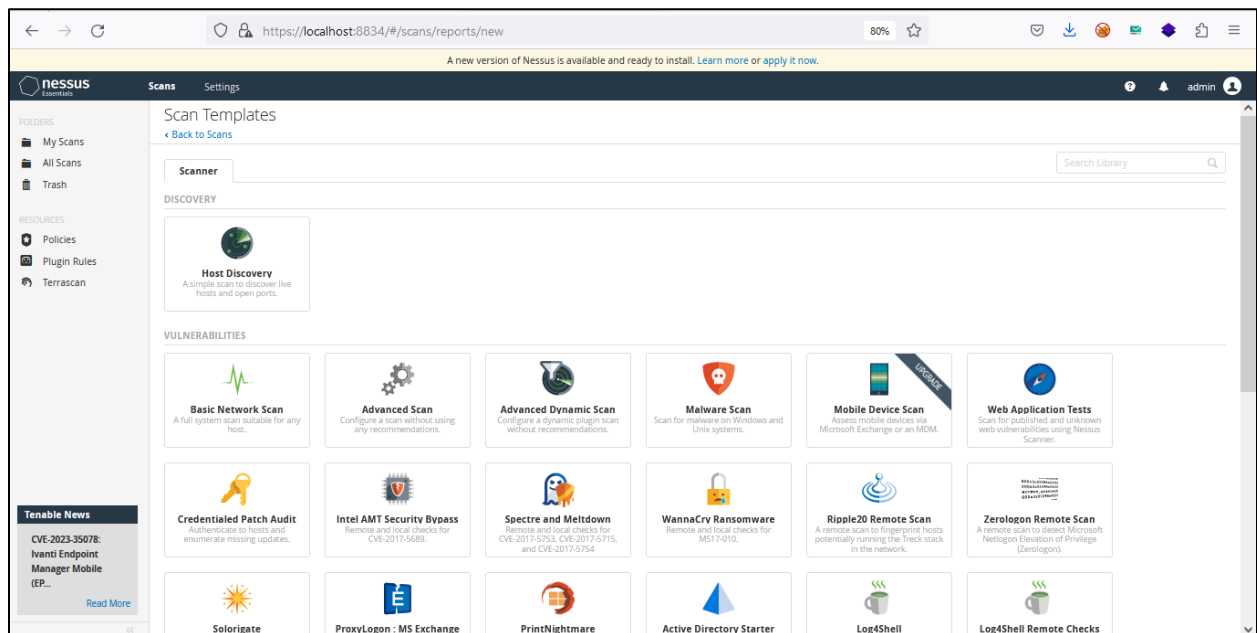
Step 14: Now create a user with any username and password and click on the Continue button.



Step 15: Plugins will be downloaded.



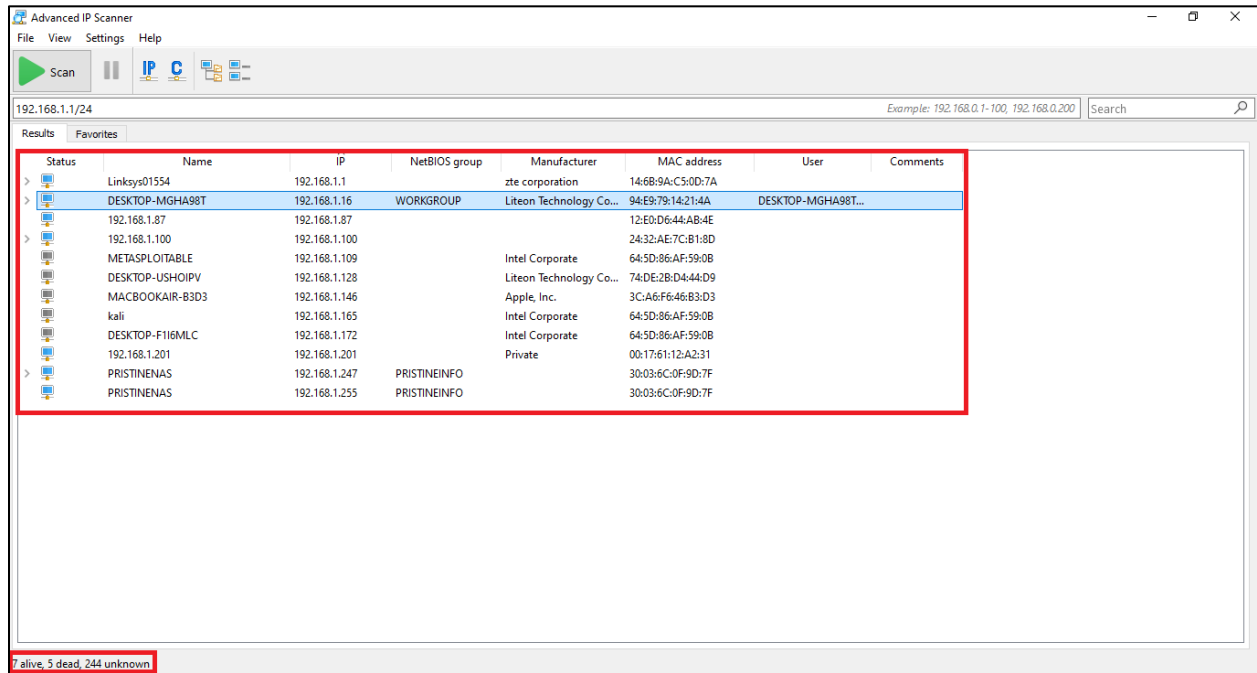
Step 16: Nessus scanner is successfully installed and running.



Learning Objective 1: Ping Sweeping with the help of Ping Sweeper tool for Active Host Enumeration in Network and map the Network.

Using Advance IP Scanner for:

Active Host Enumeration



The screenshot shows the Advanced IP Scanner interface. The target IP range is 192.168.1.1/24. The results table lists 12 active hosts with their names, IP addresses, NetBIOS groups, manufacturers, MAC addresses, and users. A red box highlights the results table, and a status bar at the bottom indicates 7 alive, 5 dead, and 244 unknown hosts.

Status	Name	IP	NetBIOS group	Manufacturer	MAC address	User	Comments
>	Linksys01554	192.168.1.1		zte corporation	14:68:9A:C5:0D:7A		
>	DESKTOP-MGHA98T	192.168.1.16	WORKGROUP	Liteon Technology Co...	94:E9:79:14:21:4A	DESKTOP-MGHA98T...	
>	192.168.1.87	192.168.1.87			12:E0:D6:44:AB:4E		
>	192.168.1.100	192.168.1.100			24:32:AE:7C:B1:8D		
>	METASPLOITABLE	192.168.1.109		Intel Corporate	64:5D:86:AF:59:08		
>	DESKTOP-USHOIPV	192.168.1.128		Liteon Technology Co...	74:DE:2B:D4:44:D9		
>	MACBOOKAIR-B3D3	192.168.1.146		Apple, Inc.	3C:A6:F6:46:B3:D3		
>	kali	192.168.1.165		Intel Corporate	64:5D:86:AF:59:08		
>	DESKTOP-F116MLC	192.168.1.172		Intel Corporate	64:5D:86:AF:59:08		
>	192.168.1.201	192.168.1.201		Private	00:17:61:12:A2:31		
>	PRISTINENAS	192.168.1.247	PRISTINEINFO		30:03:6C:0F:9D:7F		
>	PRISTINENAS	192.168.1.255	PRISTINEINFO		30:03:6C:0F:9D:7F		

7 alive, 5 dead, 244 unknown

Learning Objective 2: Port Scanning with the help of Nmap and Zenmap tool for **Open Ports and Services** running on target host.

Using Nmap and Zenmap for:

#Port Scanning

#OS Detection

#Service Enumeration

Commands to scan target with Nmap:

Scan a single target: `nmap pristine.lab.meta1`



```
lab@pristine: ~  
$ nmap pristine.lab.meta1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 04:49 EDT  
Nmap scan report for pristine.lab.meta1 (192.168.1.53)  
Host is up (0.0059s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```


Scan a range of IP addresses:

Command: **nmap 192.168.1.1-100**

```
lab@pristine: ~  
--(lab@pristine)-[~]  
-$ nmap 192.168.1.1-100  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 05:00 EDT  
Nmap scan report for 192.168.1.1 (192.168.1.1)  
Host is up (0.027s latency).  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
23/tcp    filtered telnet  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap scan report for 192.168.1.15 (192.168.1.15)  
Host is up (0.013s latency).  
All 1000 scanned ports on 192.168.1.15 (192.168.1.15) are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap scan report for 192.168.1.19 (192.168.1.19)  
Host is up (0.0069s latency).  
All 1000 scanned ports on 192.168.1.19 (192.168.1.19) are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap scan report for 192.168.1.27 (192.168.1.27)  
Host is up (0.015s latency).  
Not shown: 994 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsecure  
912/tcp   open  apex-mesh  
2323/tcp  open  3d-nfsd
```

Scan an entire subnet using CIDR notation:

Command: **nmap 192.168.1.0/24**

```
lab@pristine: ~  
--(lab@pristine)-[~]  
-$ nmap 192.168.1.0/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 05:06 EDT  
Nmap scan report for 192.168.1.1 (192.168.1.1)  
Host is up (0.0029s latency).  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
23/tcp    filtered telnet  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap scan report for 192.168.1.15 (192.168.1.15)  
Host is up (0.0066s latency).  
All 1000 scanned ports on 192.168.1.15 (192.168.1.15) are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap scan report for 192.168.1.19 (192.168.1.19)  
Host is up (0.0052s latency).  
All 1000 scanned ports on 192.168.1.19 (192.168.1.19) are in ignored states.  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap scan report for 192.168.1.27 (192.168.1.27)  
Host is up (0.010s latency).  
Not shown: 994 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsecure  
912/tcp   open  apex-mesh  
2323/tcp  open  3d-nfsd
```

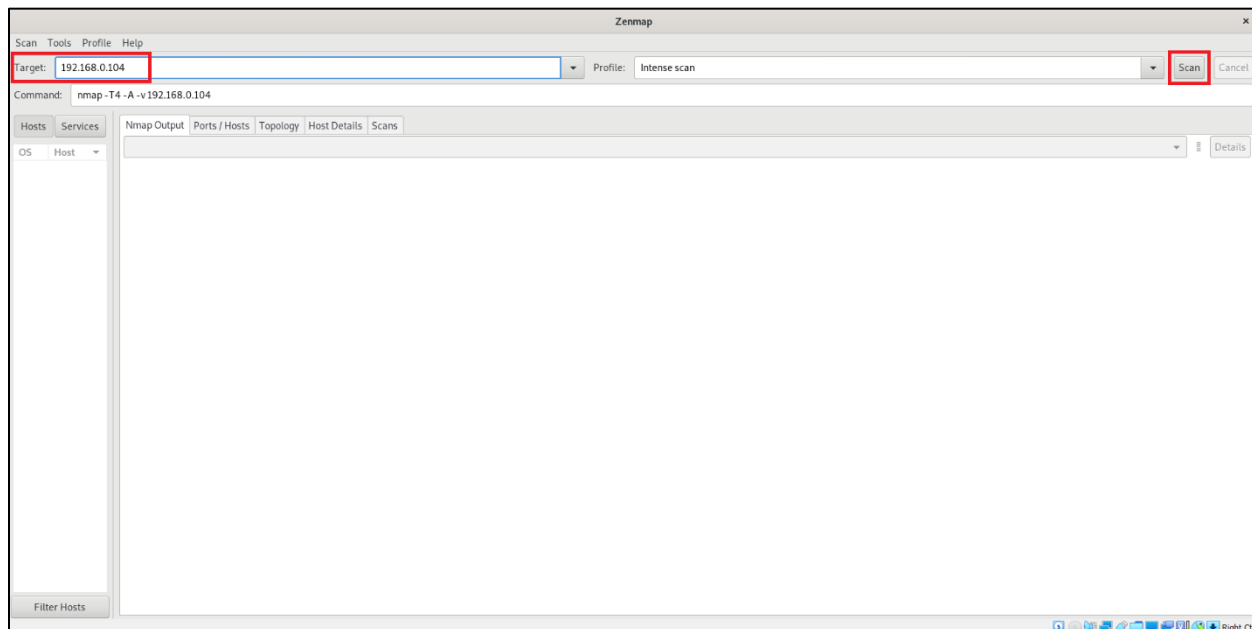
Detect the operating system of a target:

Command: sudo nmap -O pristine.lab.unknown -p 80

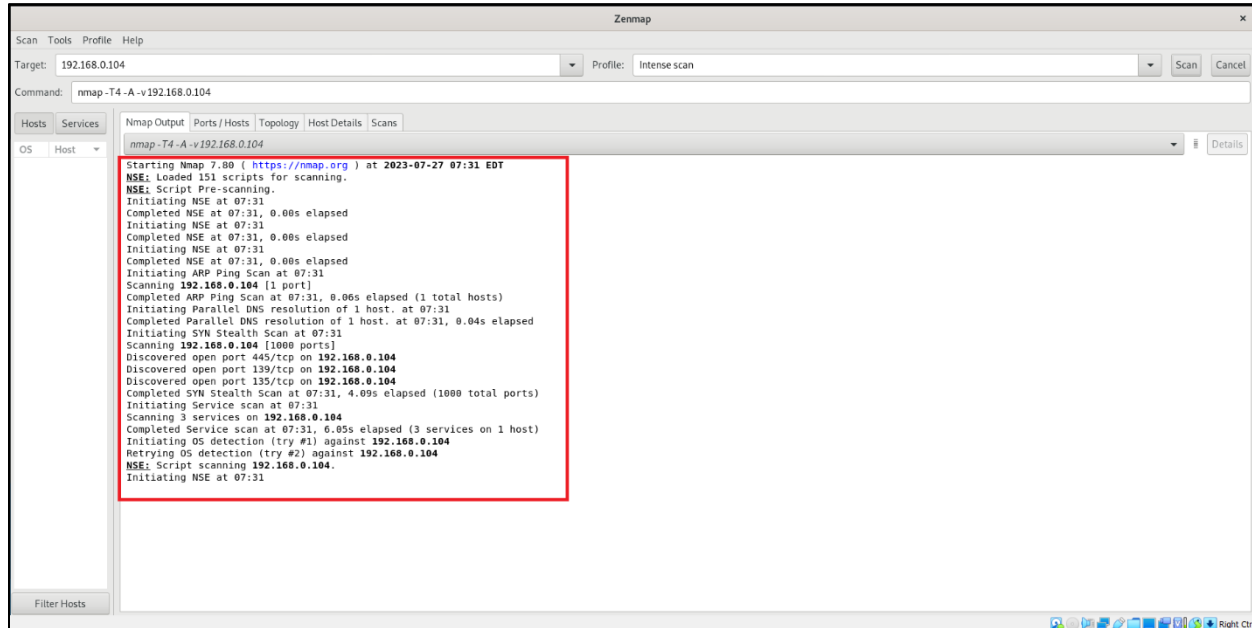
```
lab@pristine: ~  
$ sudo nmap -O pristine.lab.unknown -p 80  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-23 05:36 EDT  
Nmap scan report for pristine.lab.unknown (192.168.1.53)  
Host is up (0.015s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address:   
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds  
  
lab@pristine: ~  
$
```

Using Zenmap for Port Scanning:

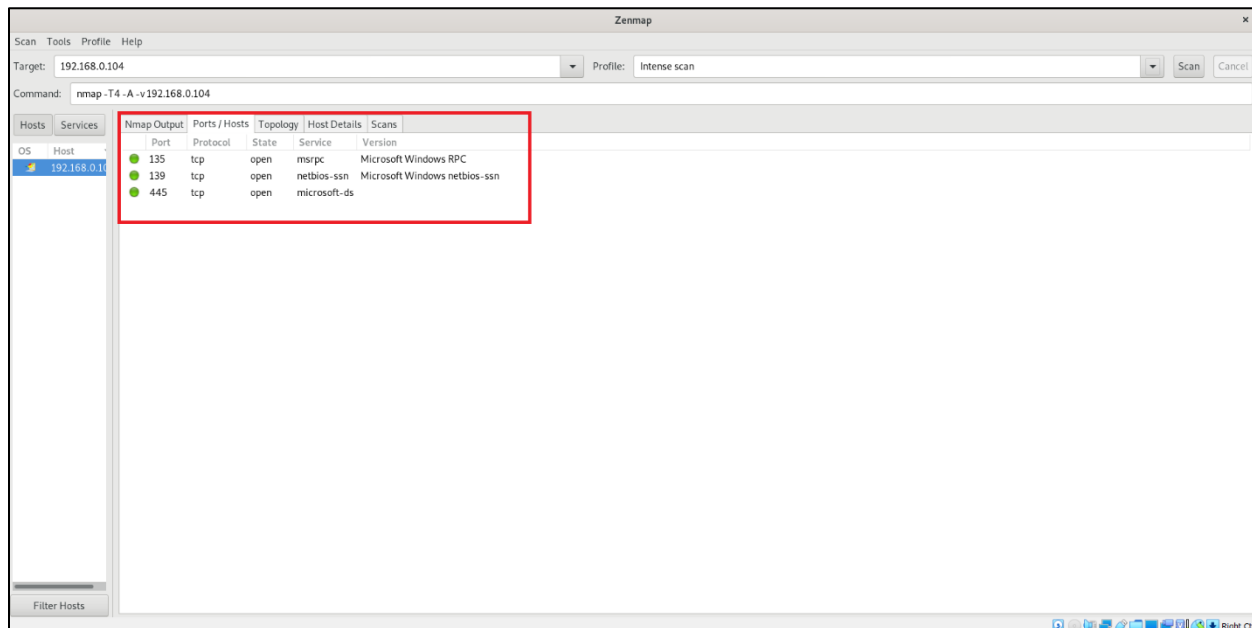
Step 1: Enter target IP address in target field to perform Port Scanning.



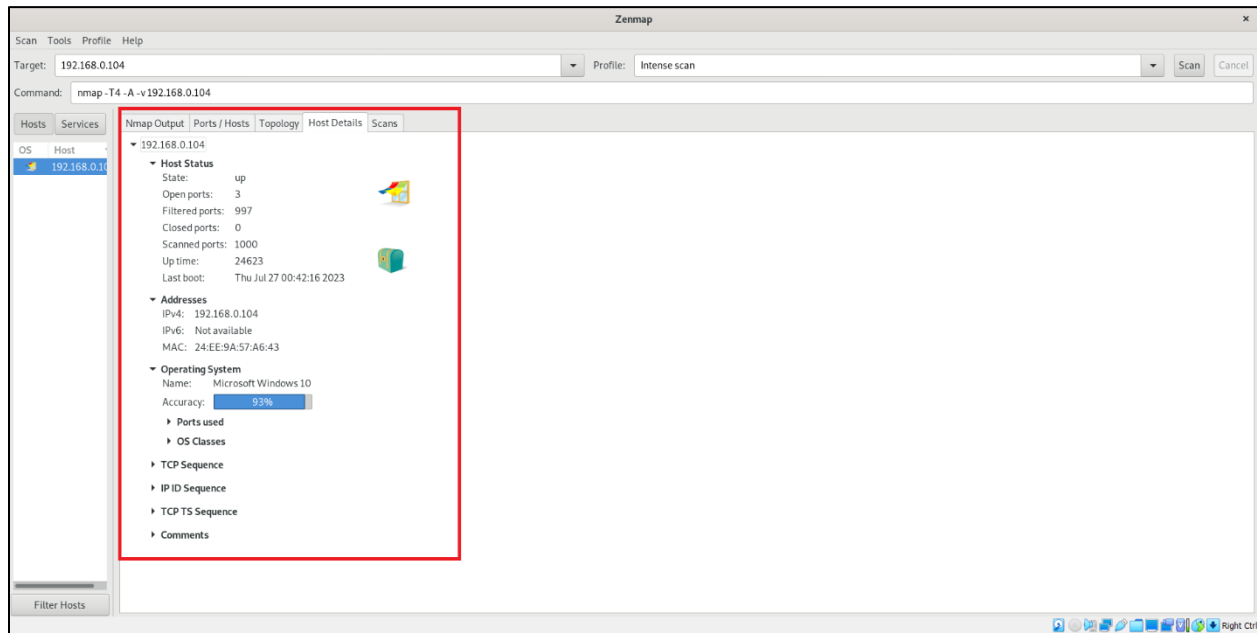
Step 2: Port scanning has been started.



Step 3: List of open ports and services which are running on victim machine.



Step 4: Victim host details where OS has been detected.

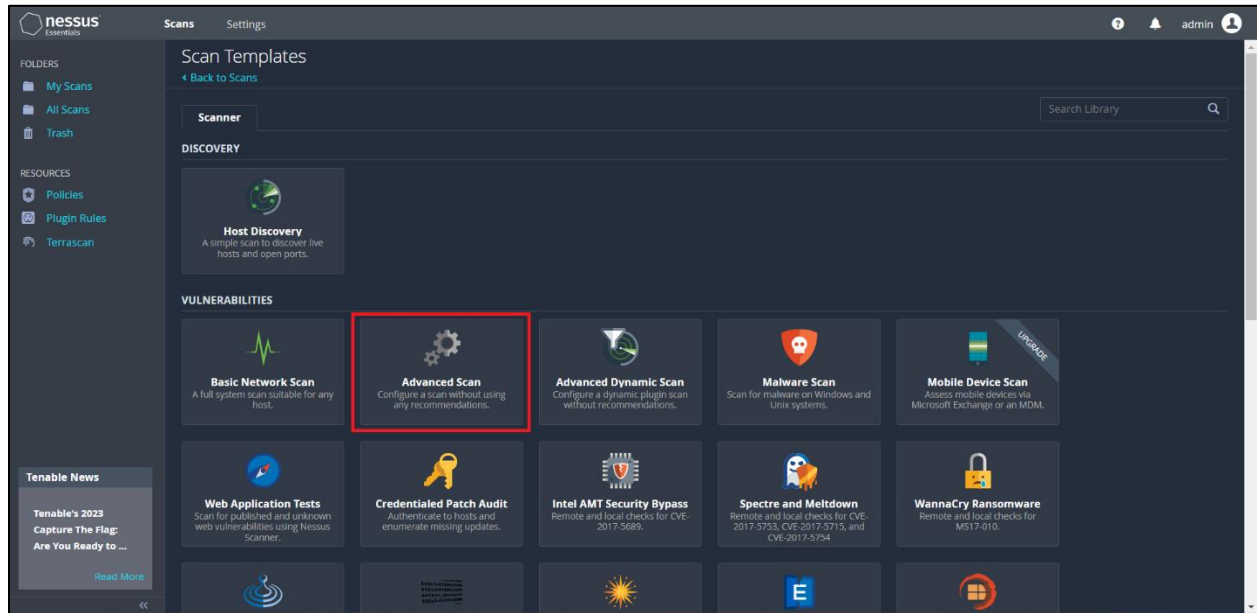


Learning Objective 3: Vulnerability Assessment with the help of Nessus scanner to find loopholes from target host.

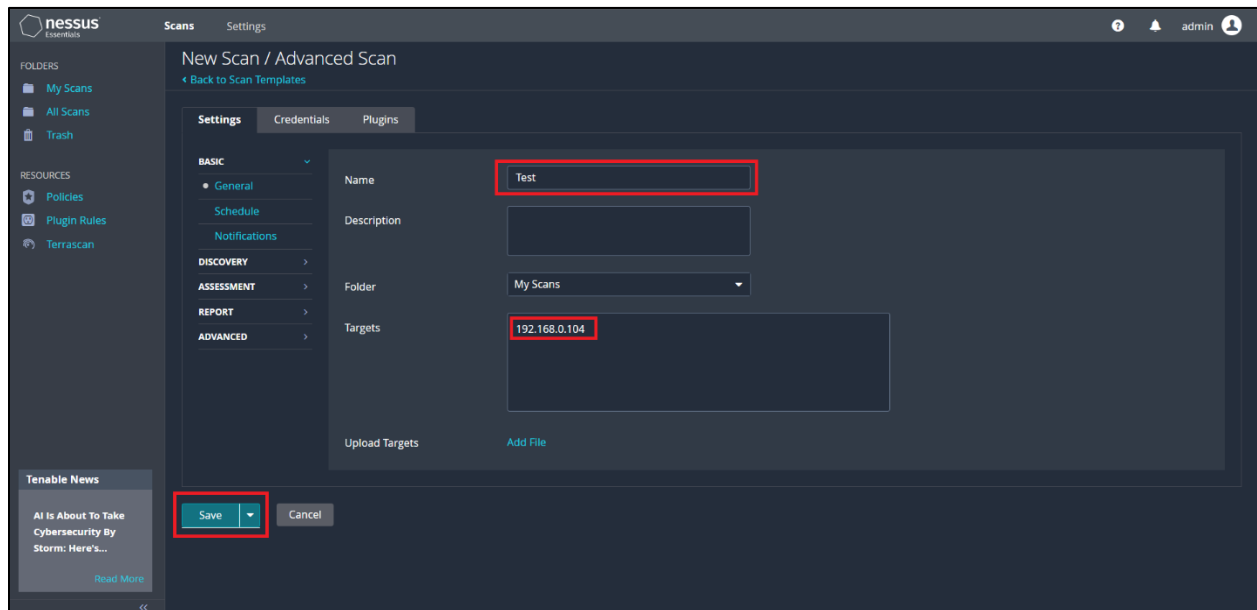
Using Nessus Scanner:

#Vulnerability Assessment

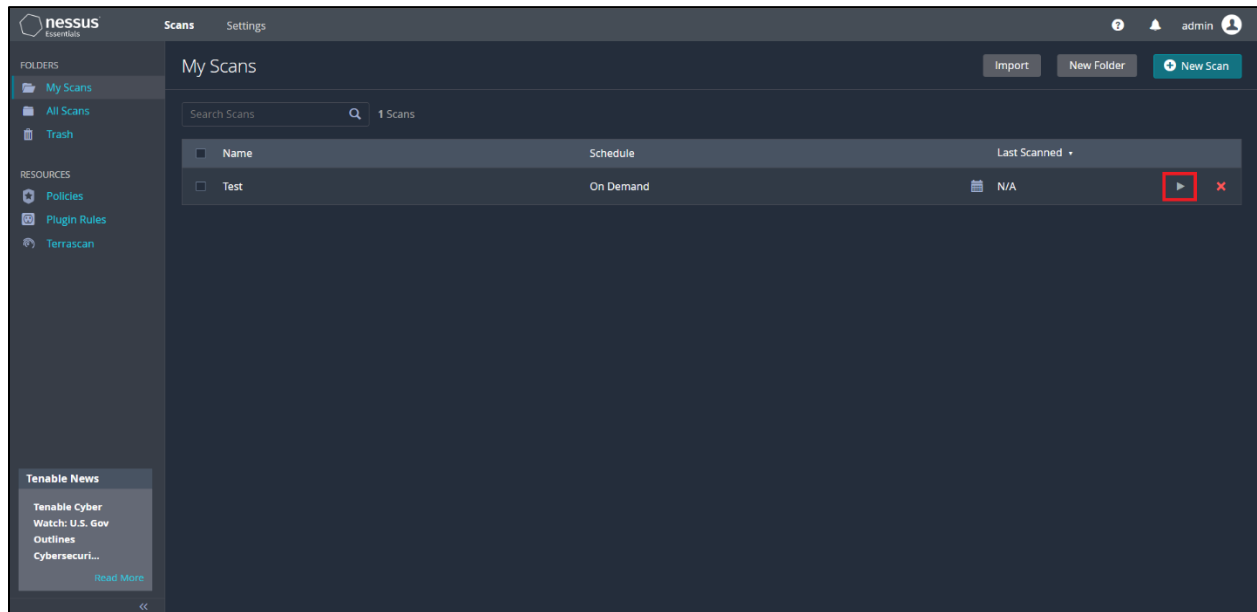
Step 1: Select Advance Scan option to scan the target.



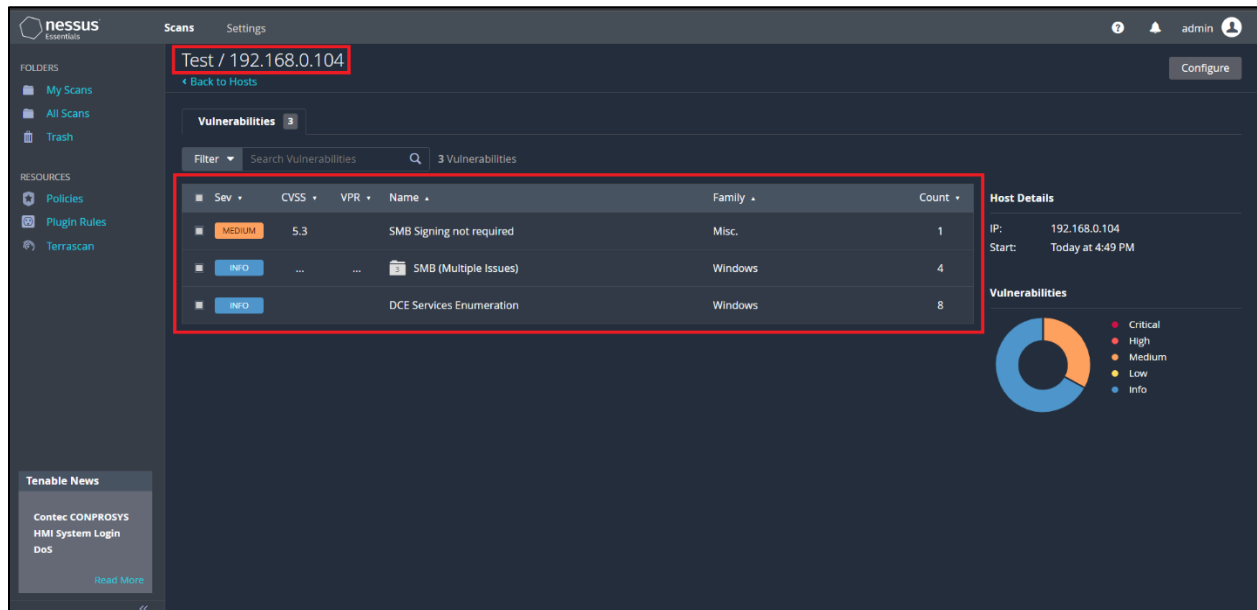
Step 2: Provide Name for your scan and target IP and save the scan.



Step 3: Launch the scan.



Step 4: Scanning will be done and vulnerabilities will be listed.



Learning Outcomes: The student should have the ability to perform:

LO1: Ping Sweeping with the help of ping sweeper tool for active host enumeration.

LO2: Port scanning and Service enumeration with the help of Nmap and Zenmap tool.

LO3: Able to perform Vulnerability Assessment with the help of Nessus Scanner.

Course Outcomes: Upon completion of the course students will be able to understand the concept of Network Scanning and able to perform and map the network.

Conclusion: Through this experiment we learned the concept of Ping Sweeping, Port Scanning and Vulnerability Assessment.

For Faculty Use:

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				