Experiment 04

**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**

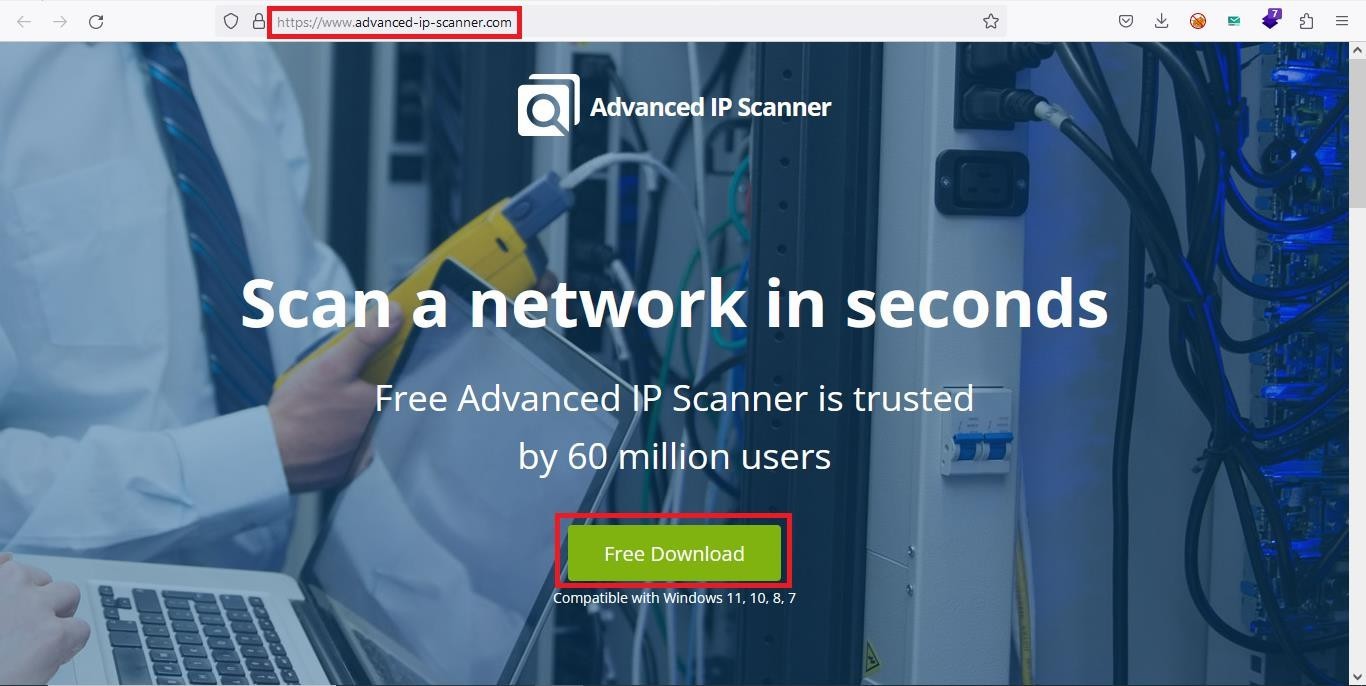
Reliable and free network scanner to analyze LAN. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off. It is easy to use and runs as a portable edition. It should be the first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

**Installation of Advance IP Scanner**

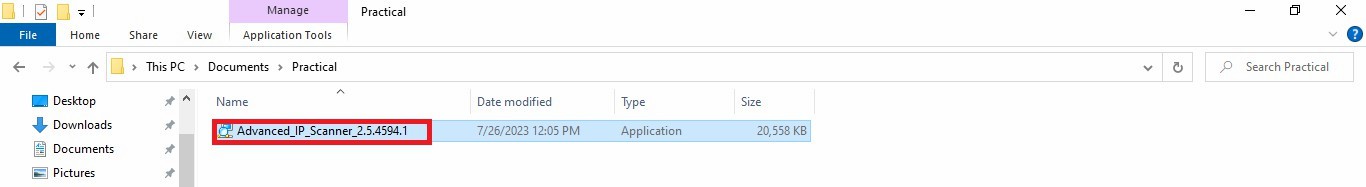
If we want to install the Advance IP Scanner in windows, we can use the following steps:

**Step 1:** First, we need to go to the Advance IP Scanner Website through the [https://www.advanced-ip-scanner.com](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.

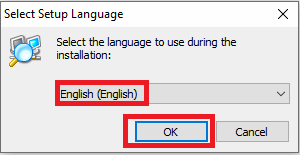
**Step 2:** Click on the Free Download button, which appears on a green button on the page.



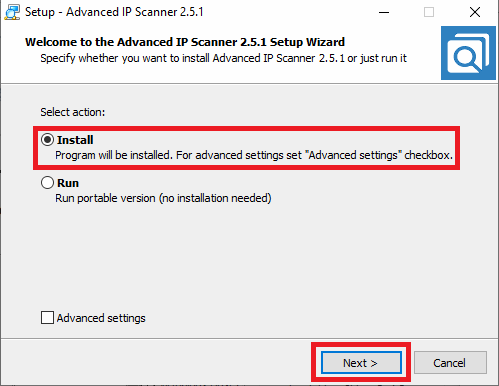
**Step 3:** Now, launch the Advance IP Scanner EXE file from where we have downloaded this file in the system. After that, the Advance IP Scanner installation window will open.



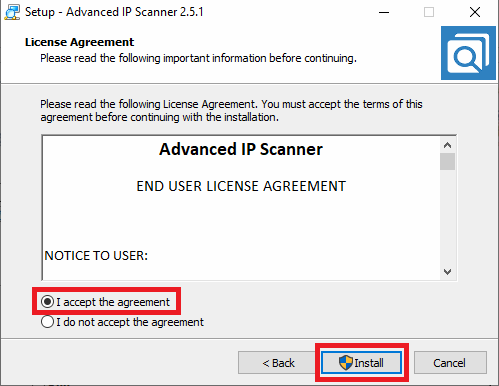
**Step 4:** Select the language and click on the OK button.



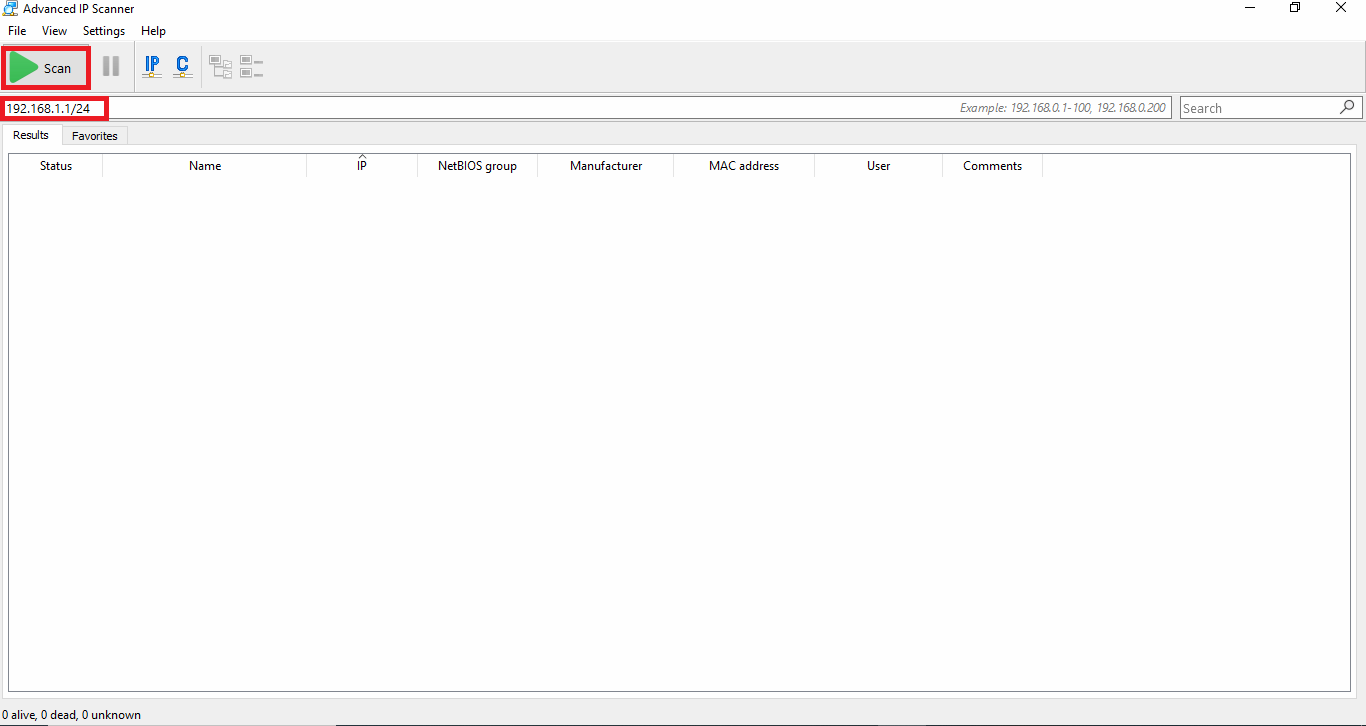
**Step 5:** Select the action Install and click on the Next button.



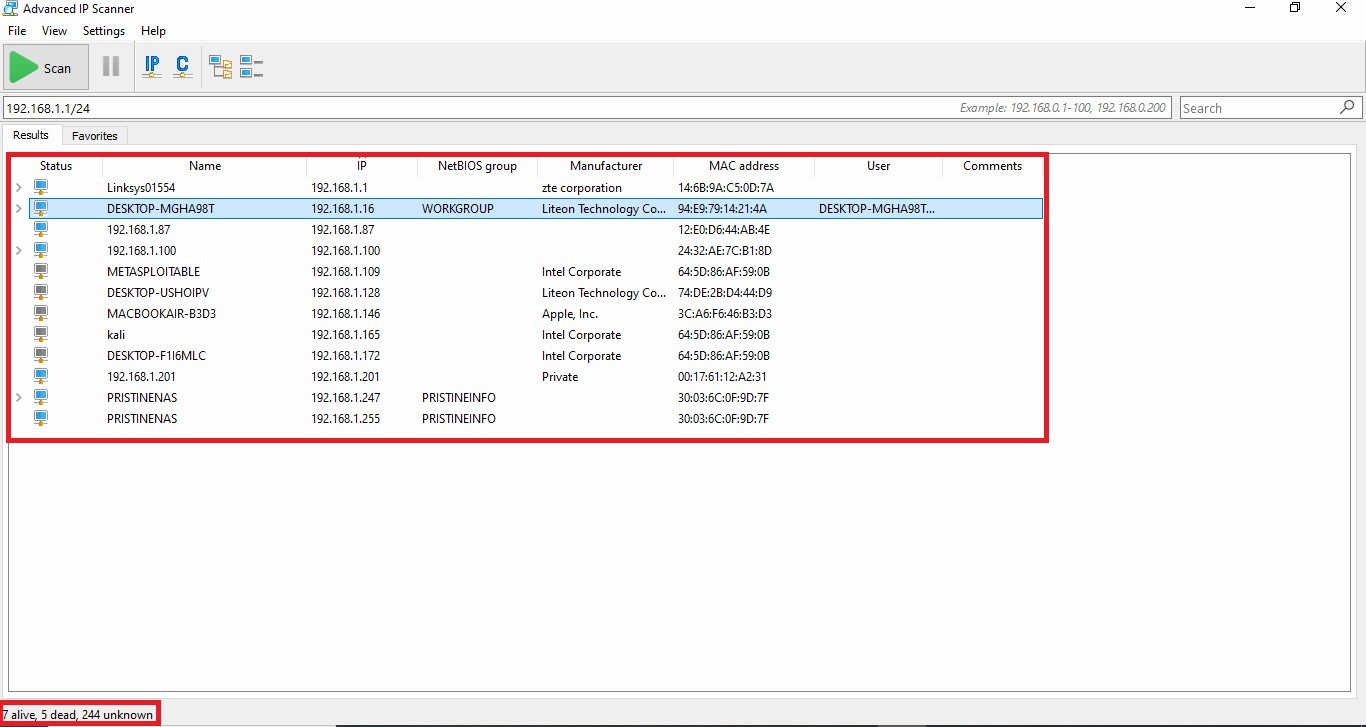
**Step 6:** Accept the User License Agreement and click on the Install button.



**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.



**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.

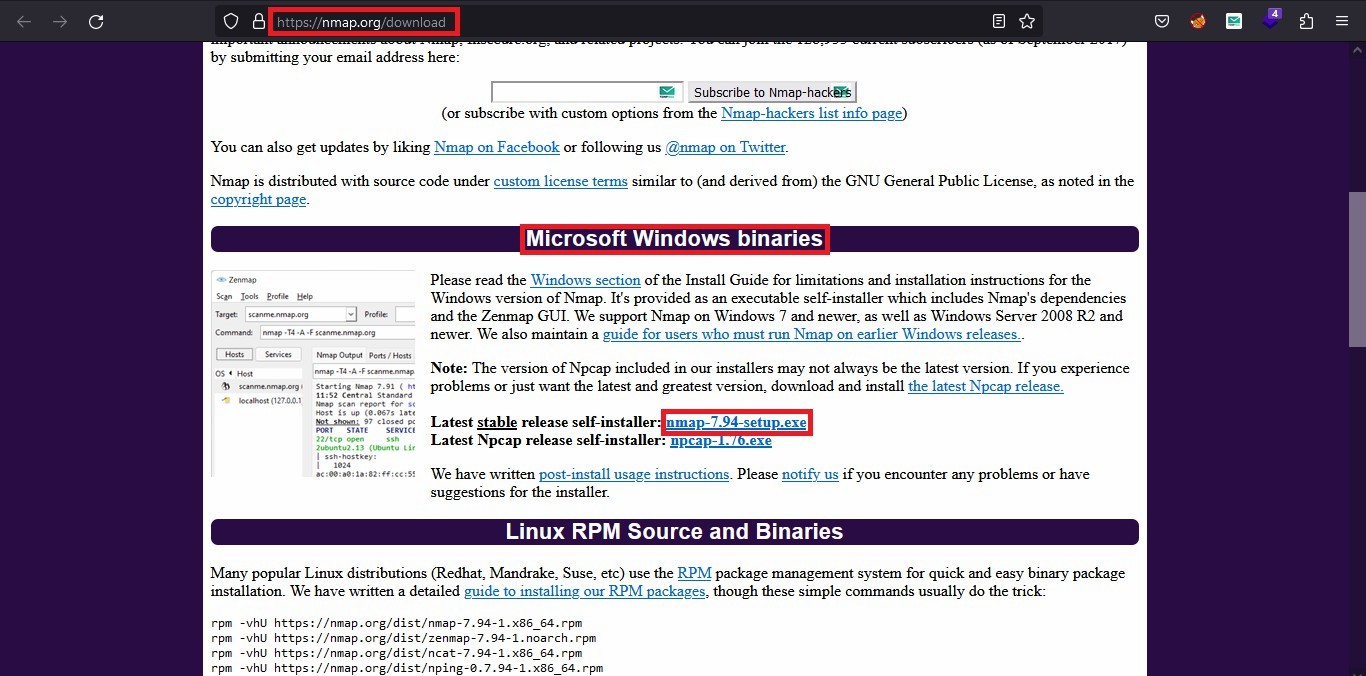
**Installation of Nmap & Zenmap**

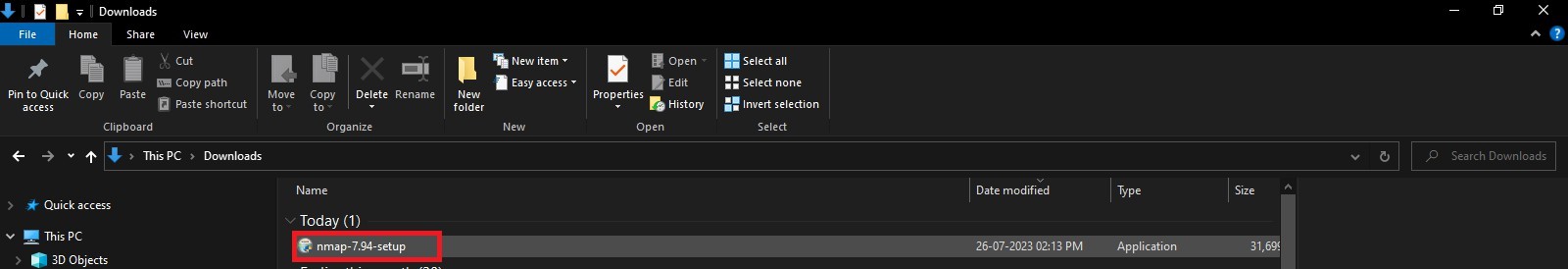
If we want to install the Nmap in windows, we can use the following steps:

**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.

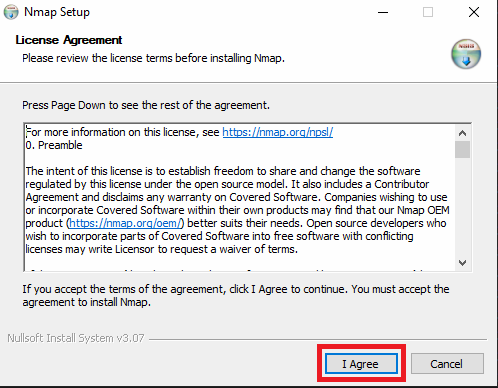
**Step 2:** Click on the Nmap Setup button to download setup file.

**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.

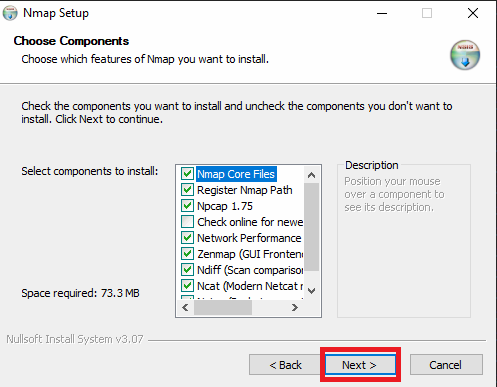




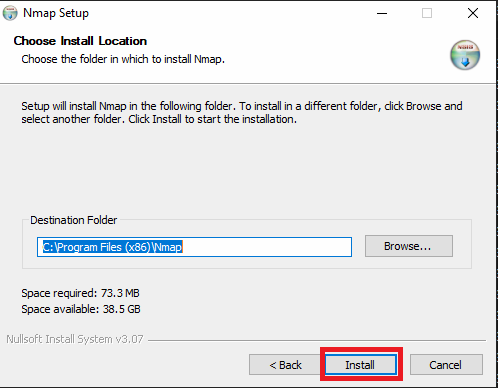
**Step 4:** Accept the User License Agreement and click on the Install button.



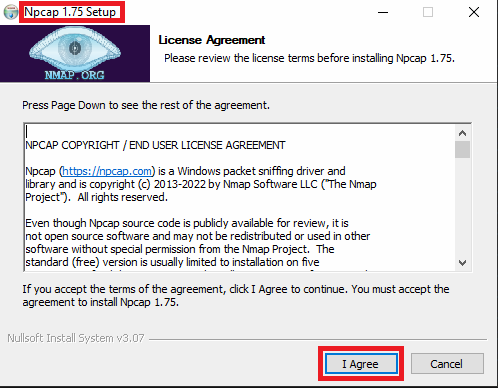
**Step 5:** Click on the Next button.



**Step 6:** Click on the Install button.

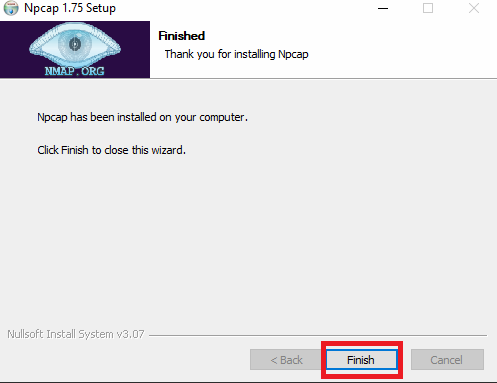
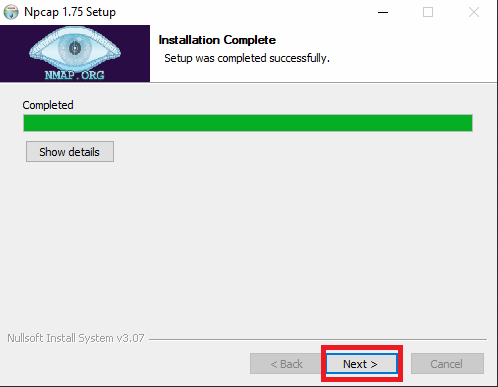


**Step 7:** Npcap is pre-requirement of Nmap it will be automatically installed, click on the I agree button.



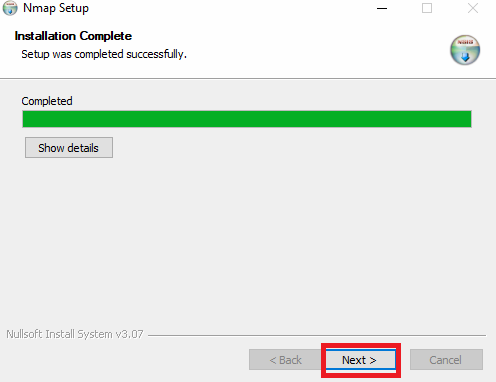
**Step 8:** Click on the Install button.

**Step 9:** Click on the Next button.



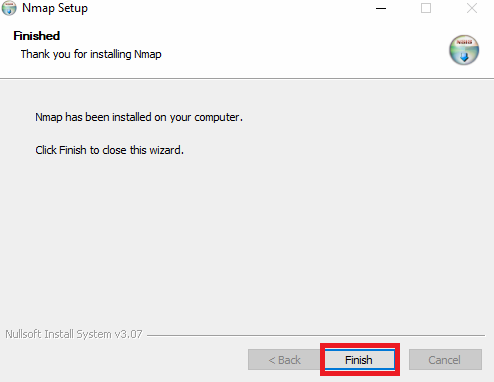
**Step 10:** Click on the Finish button.

**Step 11:** Click on the Next button.

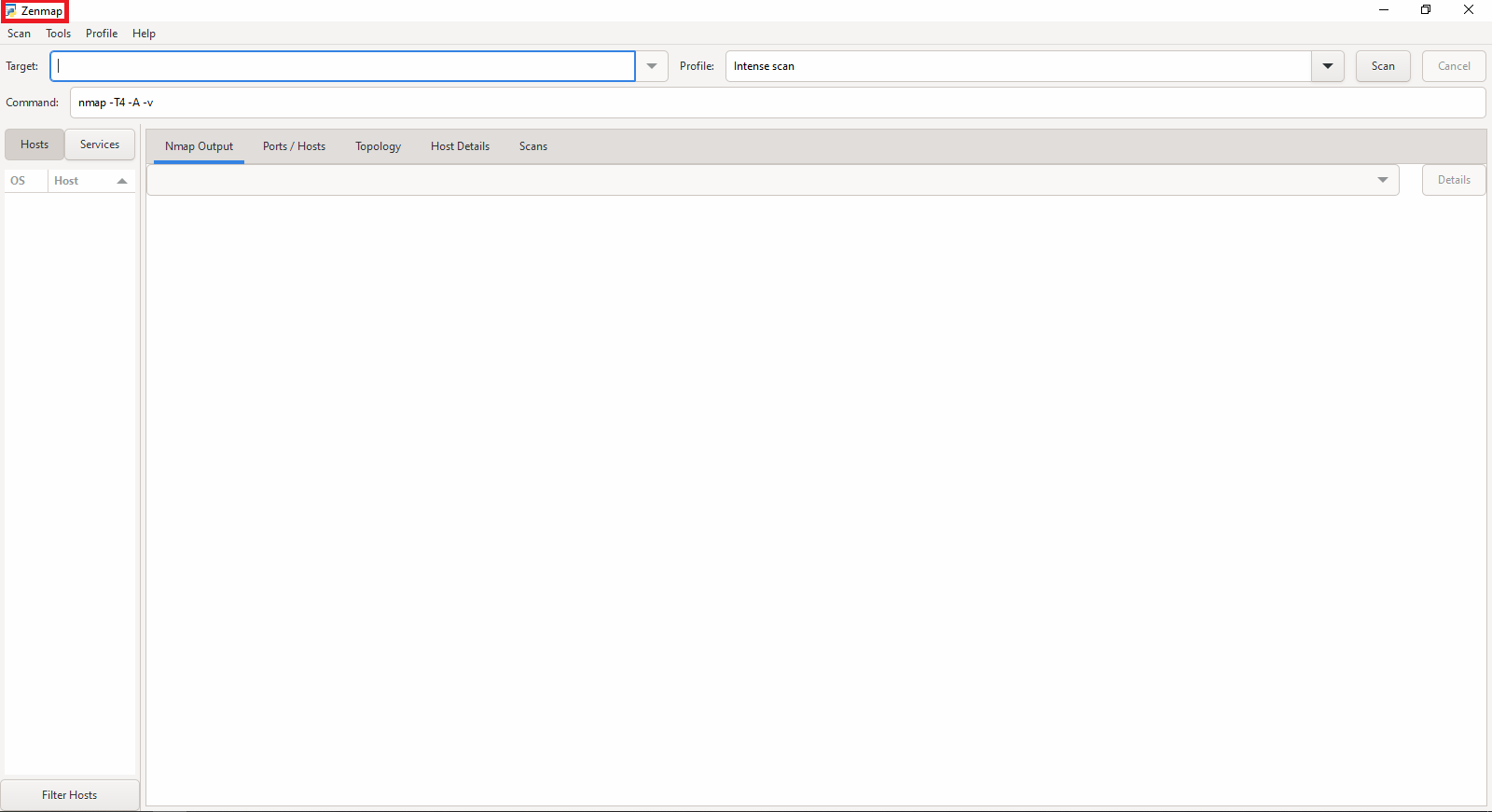


**Step 12:** Click on the Finish button, Nmap setup has been completed now we can launch Nmap

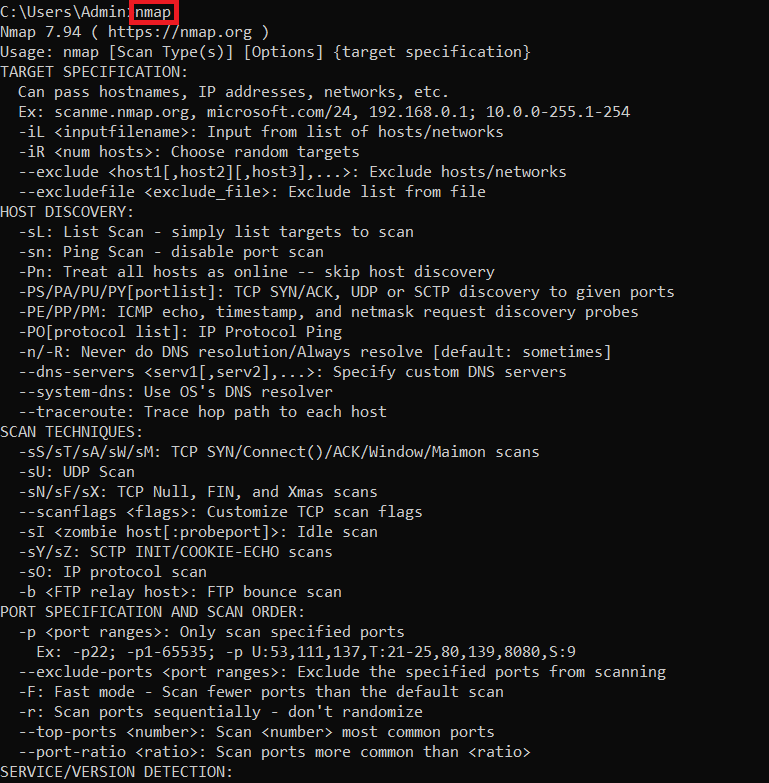
in **GUI mode, which is known as Zenmap** and, we can launch **Nmap in CLI** which is called Nmap.



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



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



**Using Nessus Scanner**

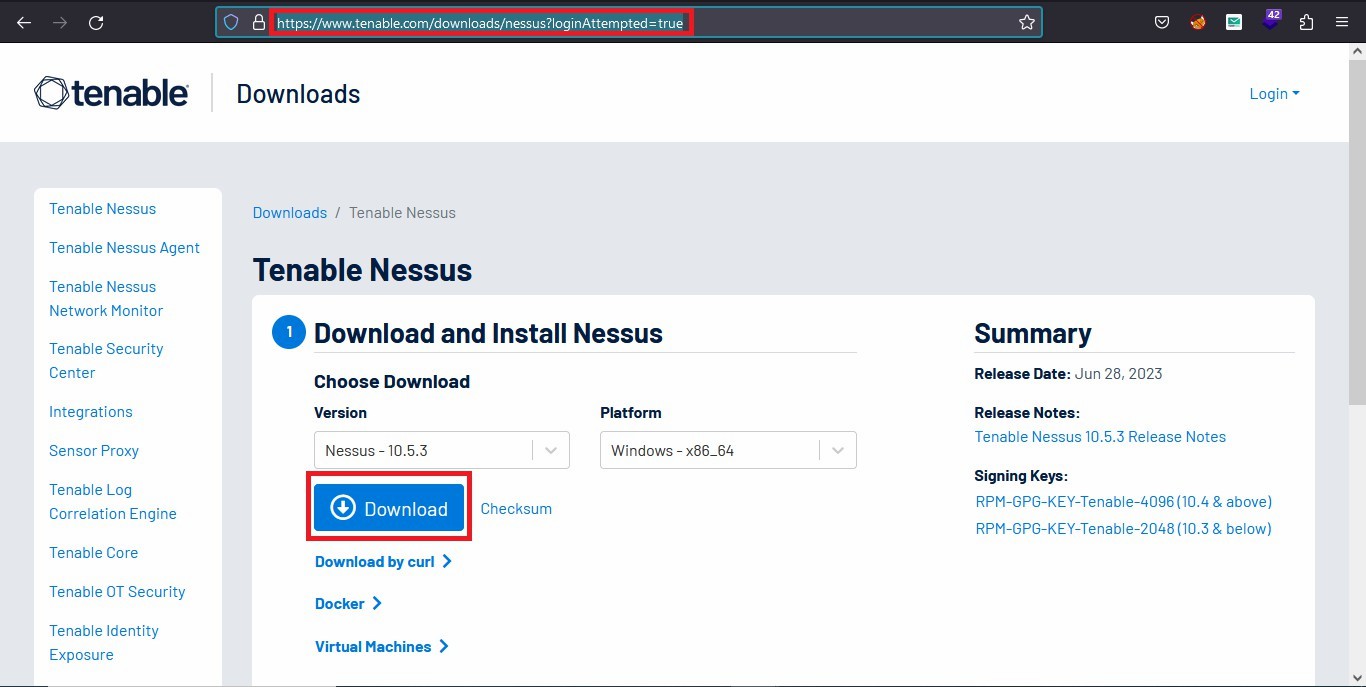
Nessus is a scanner developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

**Installation of Nessus Scanner**

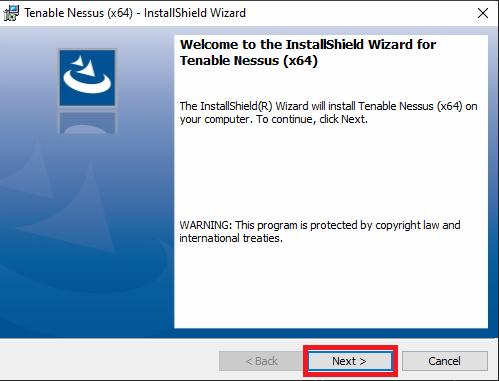
If we want to install the Nessus Scanner in windows, we can use the following steps:

**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.

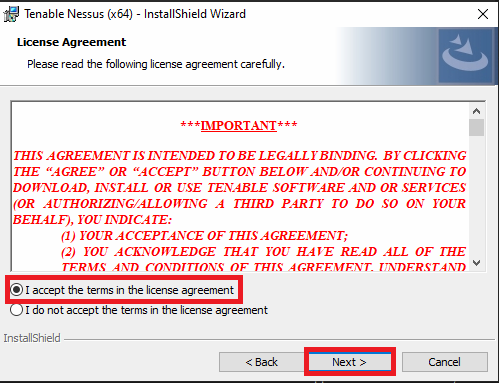
**Step 2:** Click on the Download button, which appears on a blue button on the page.



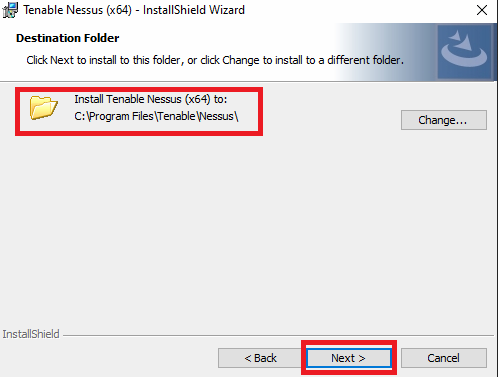
**Step 3:** Click on the Next button.



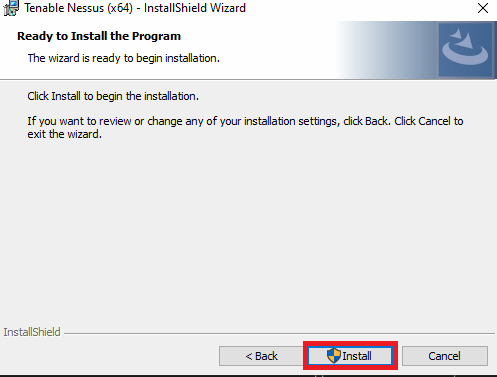
**Step 4:** Accept the User License Agreement and click on the Install button.



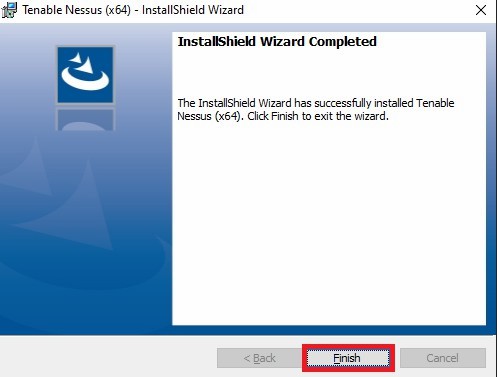
**Step 5:** Click on the Next button.



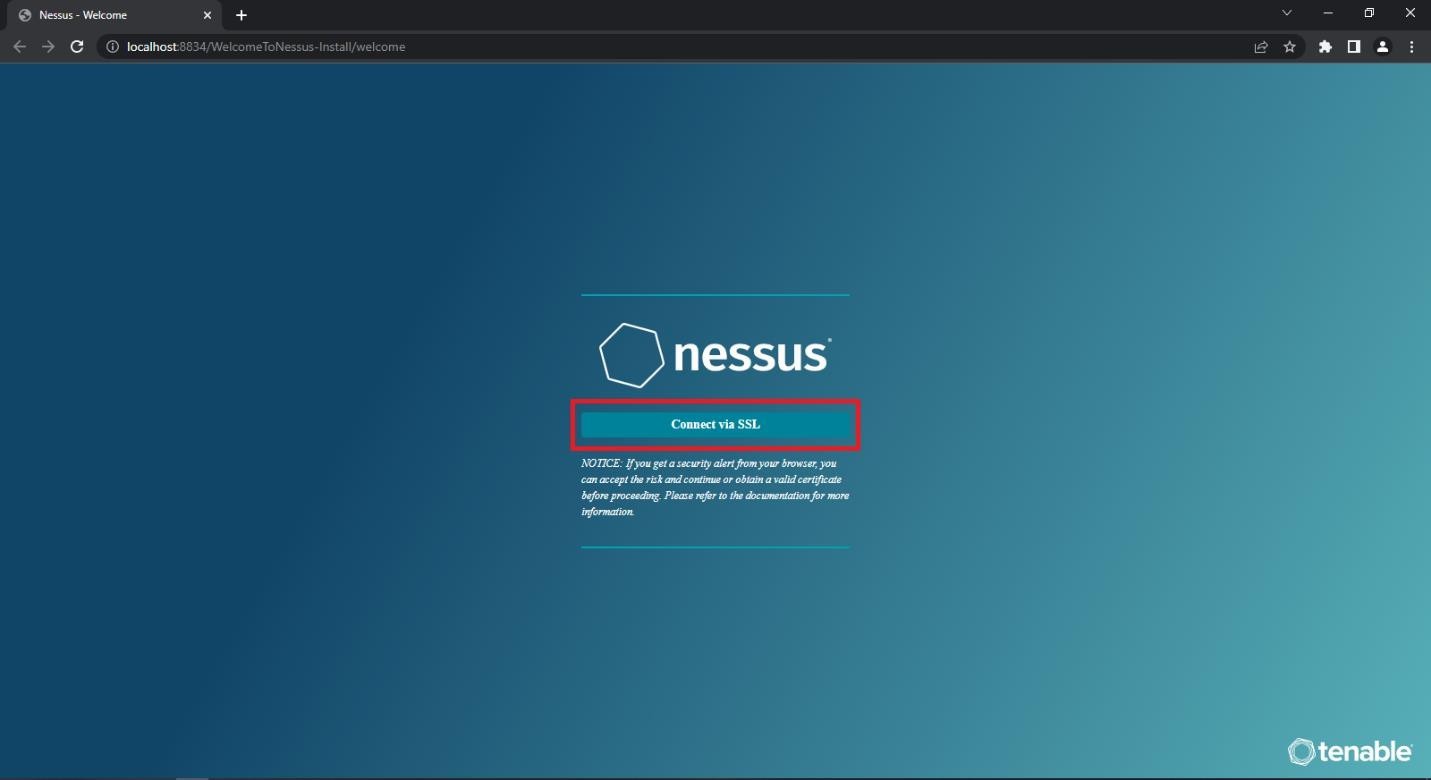
**Step 6:** Click on the Install button.



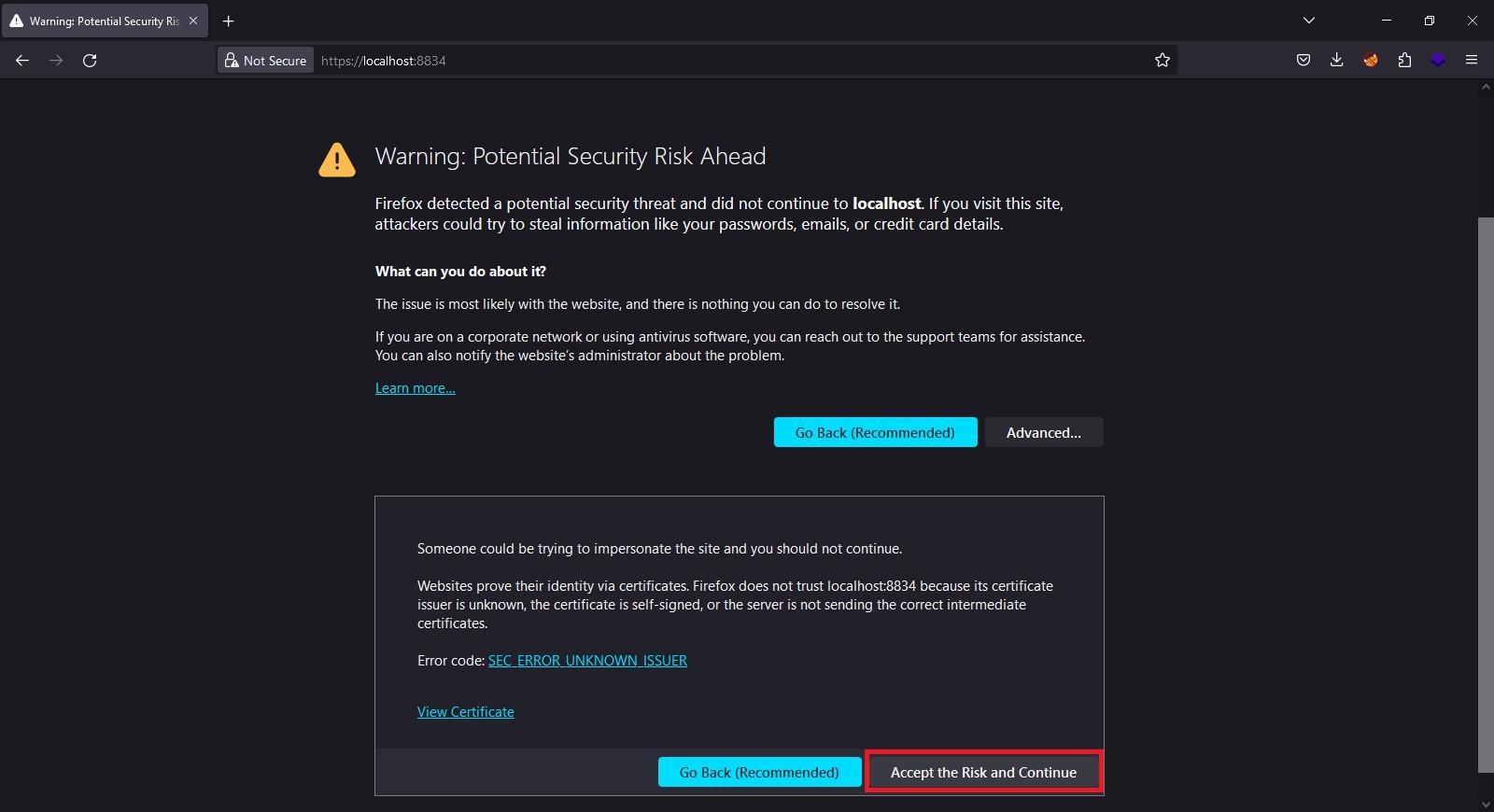
**Step 7:** Click on the Finish button.



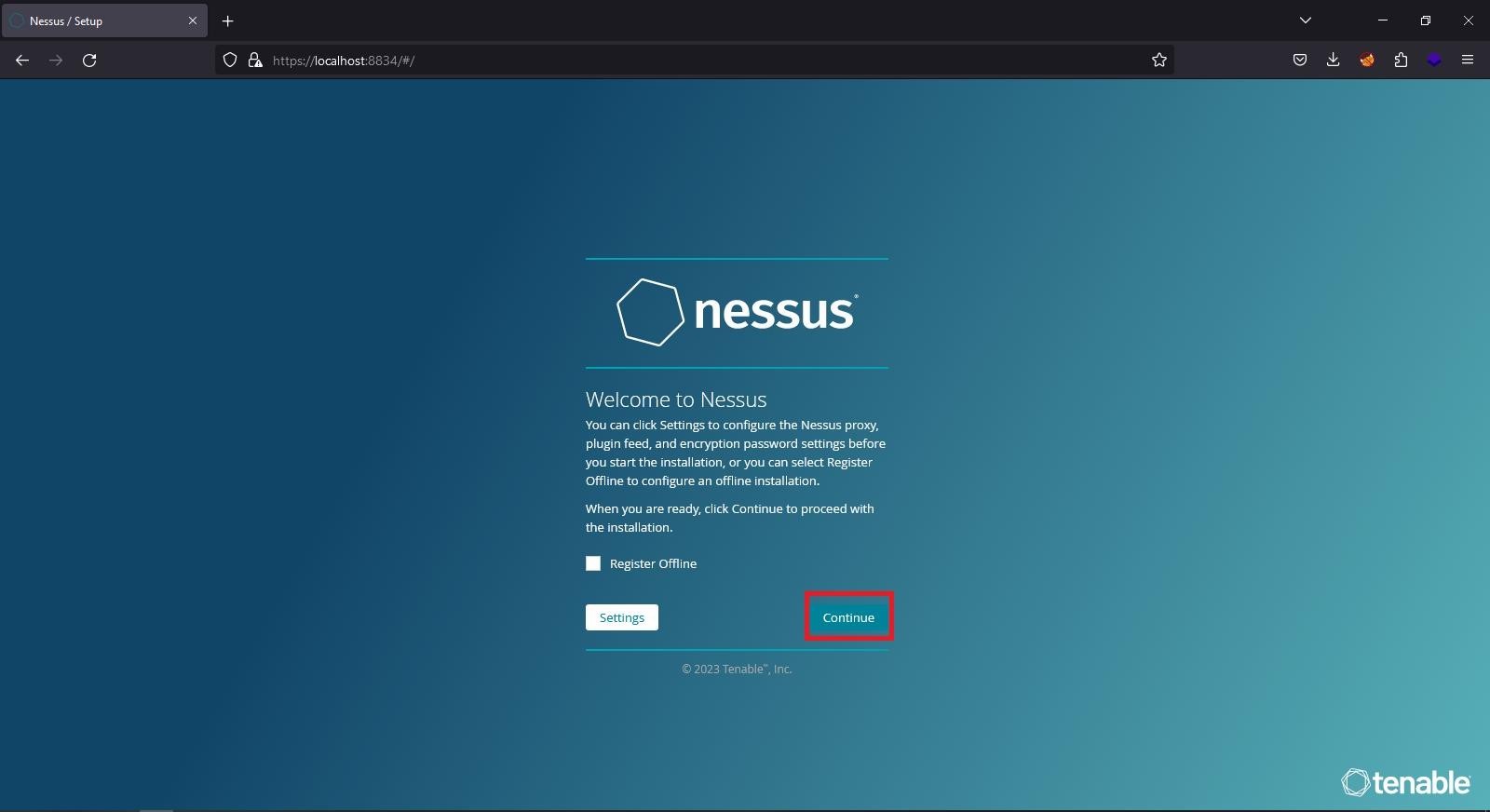
**Step 8:** Click on the Connect via SSL button.



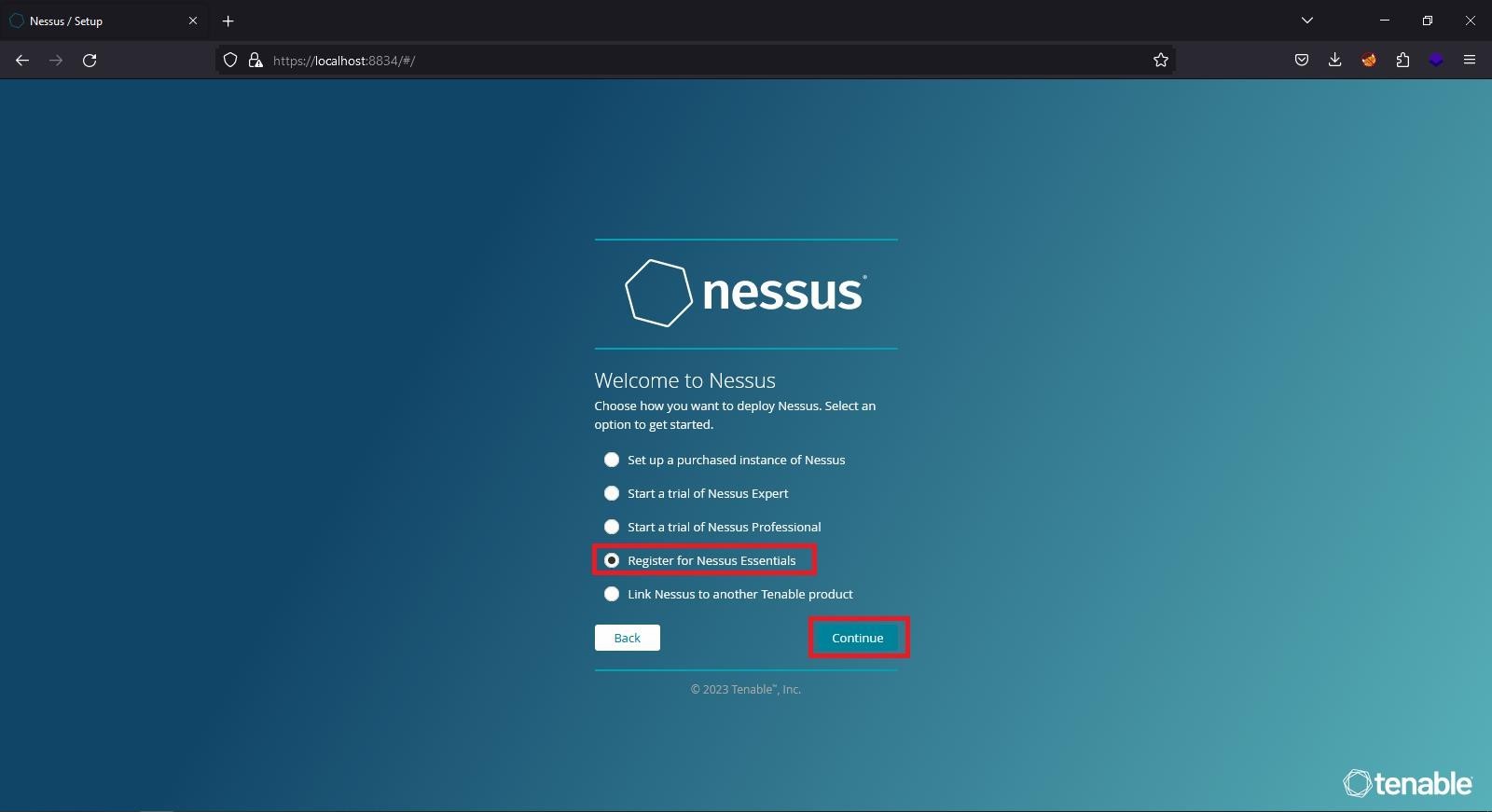
**Step 9:** Click on the Accept the Risk and Continue button.



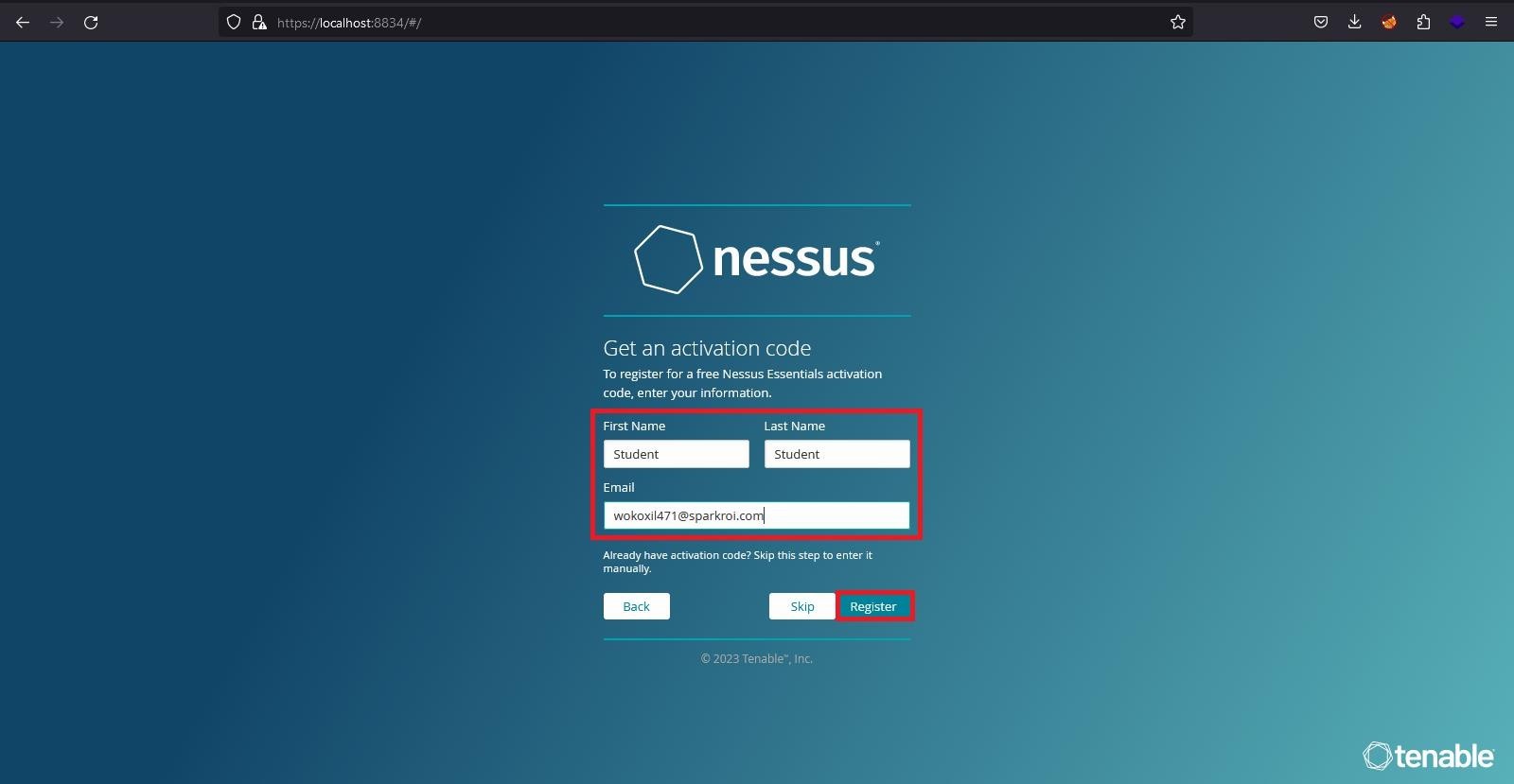
**Step 10:** Click on the Continue button.



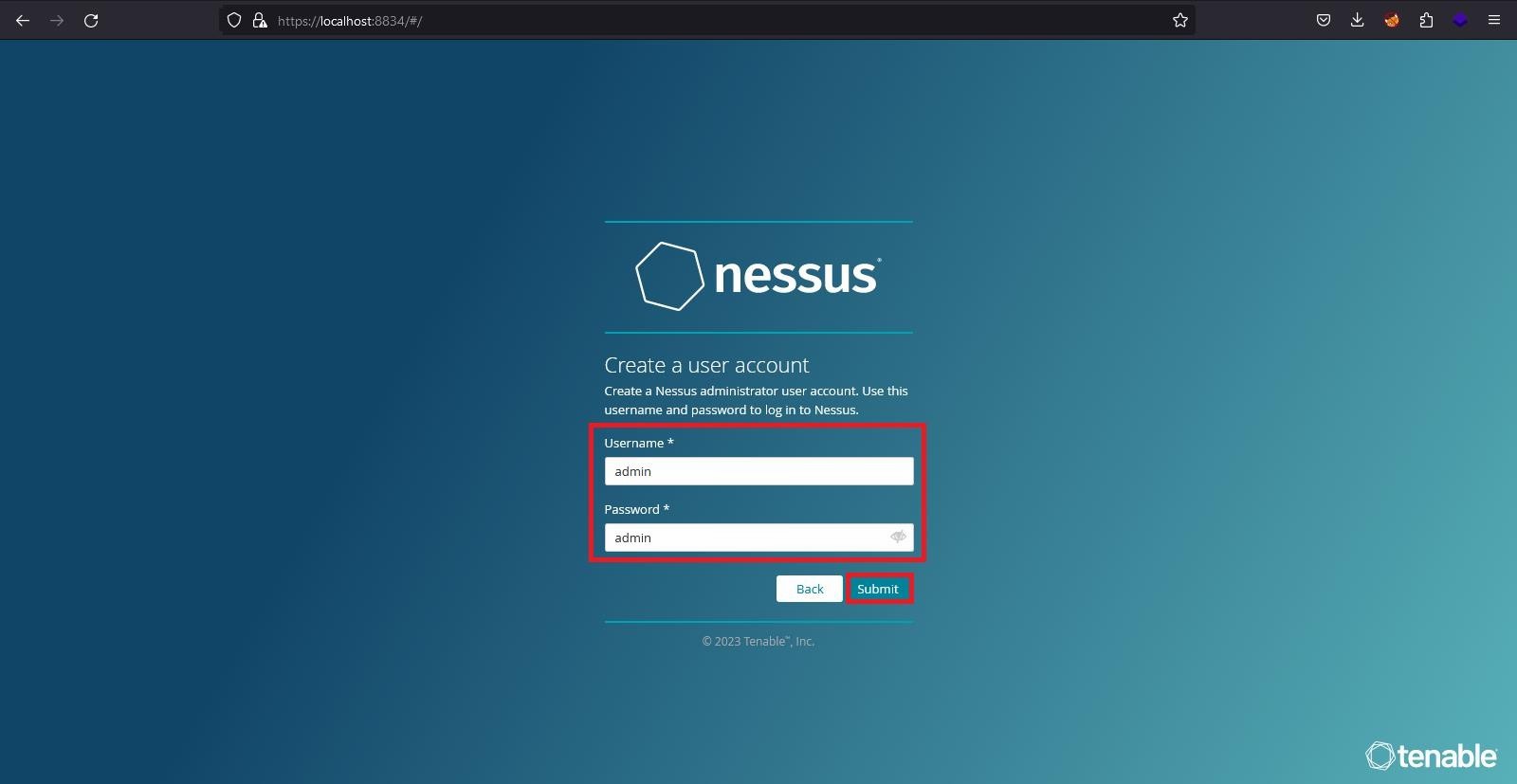
**Step 11:** Select the Register for Nessus Essentials and click on the Continue button.

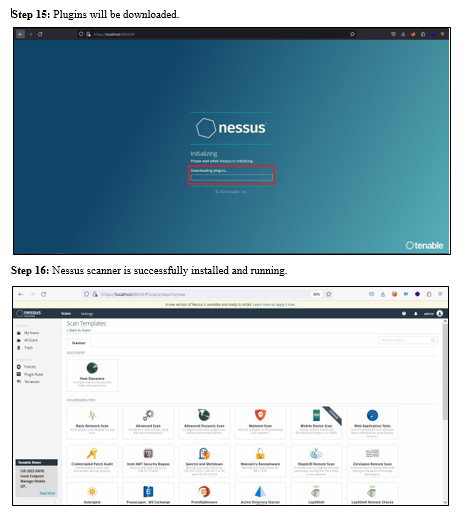


**Step 12:** Enter the user details and click on the Register button.



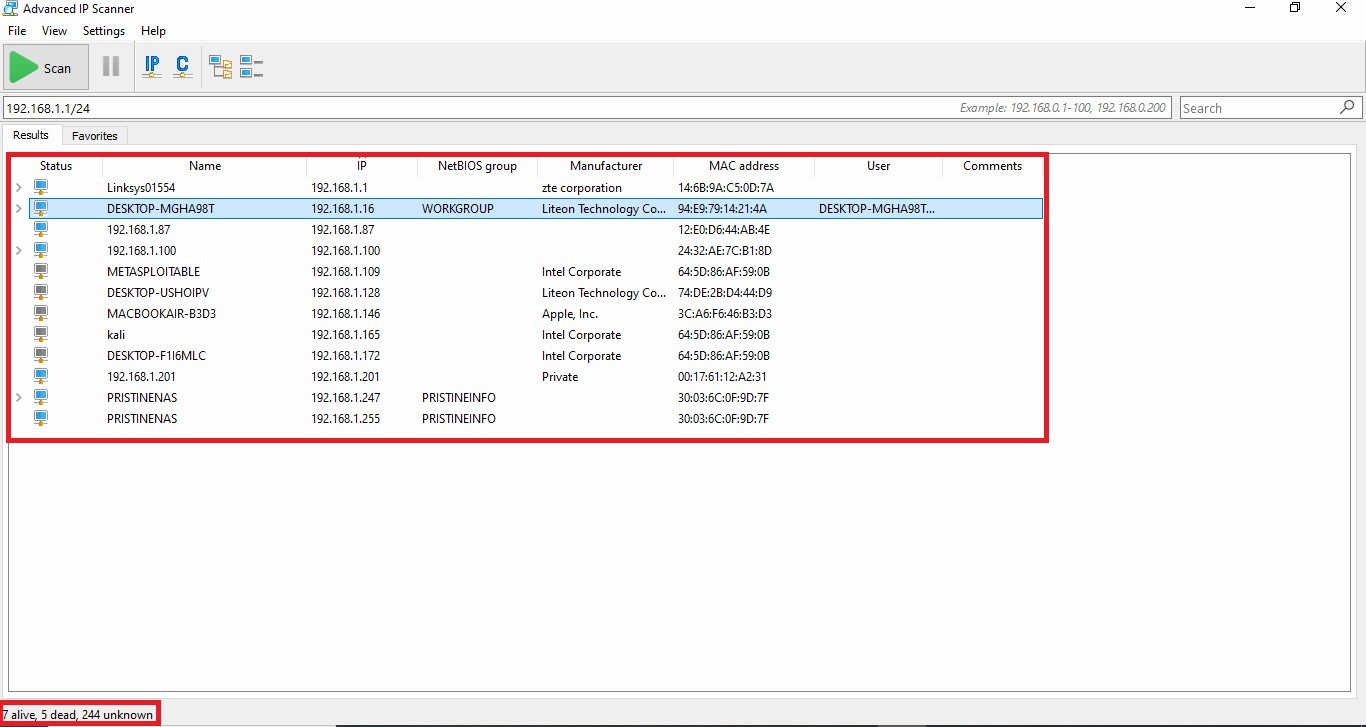
**Step 14:** Now create a user with any username and password and click on the Continue button.





**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**



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

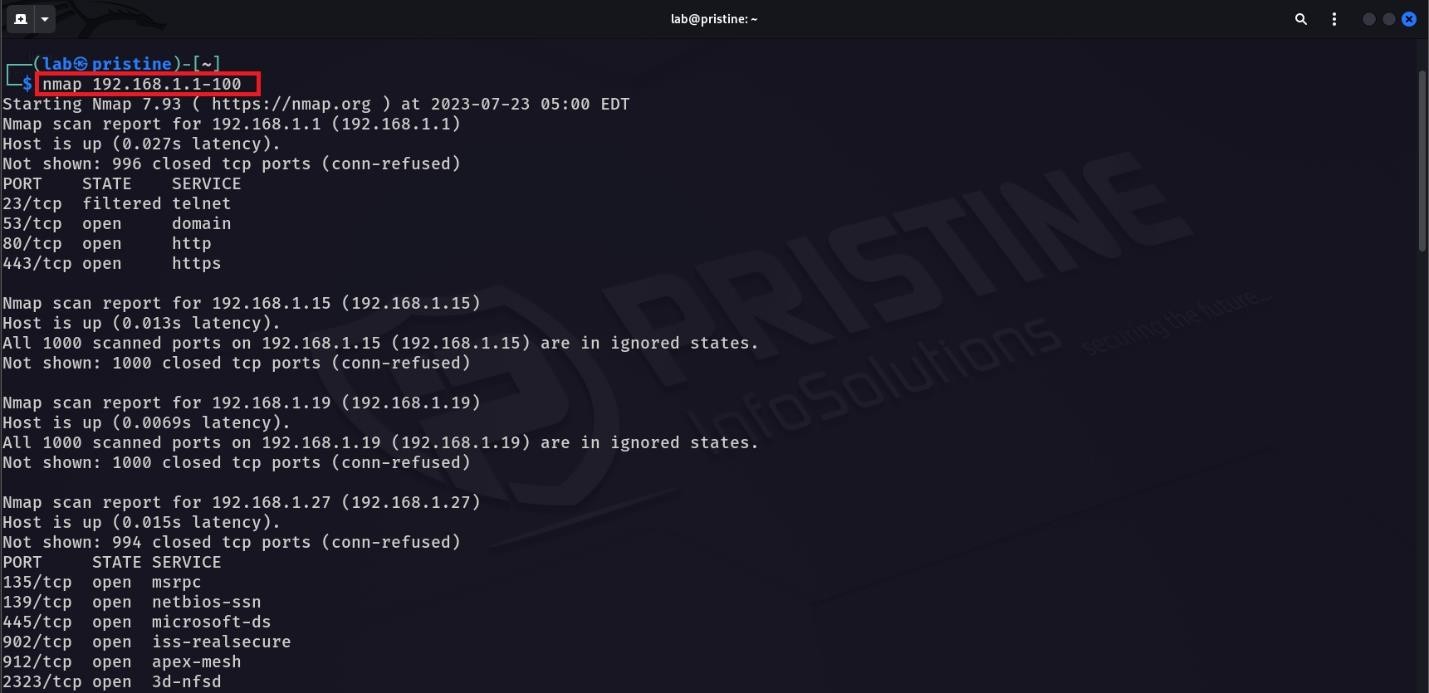
**Using Nmap and Zenmap for:**

**#Port Scanning #OS Detection**

**#Service Enumeration**

**Commands to scan target with Nmap:**

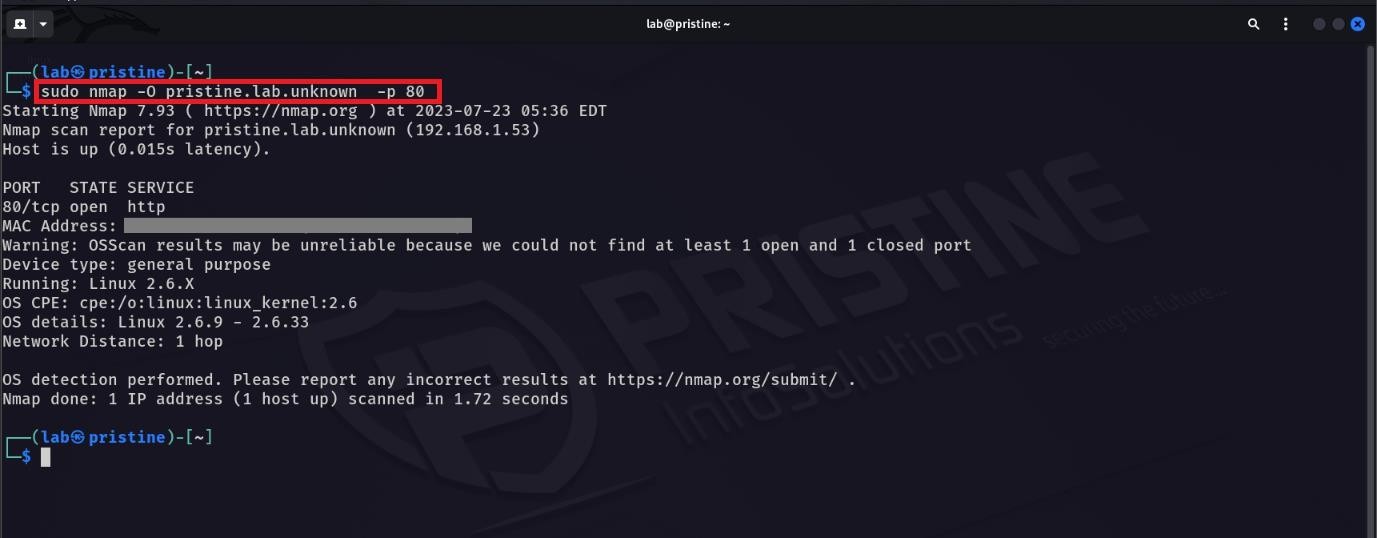
**Scan a range of IP addresses: Command: nmap 192.168.1.1-100**



**Scan an entire subnet using CIDR notation: Command: nmap 192.168.1.0/2**

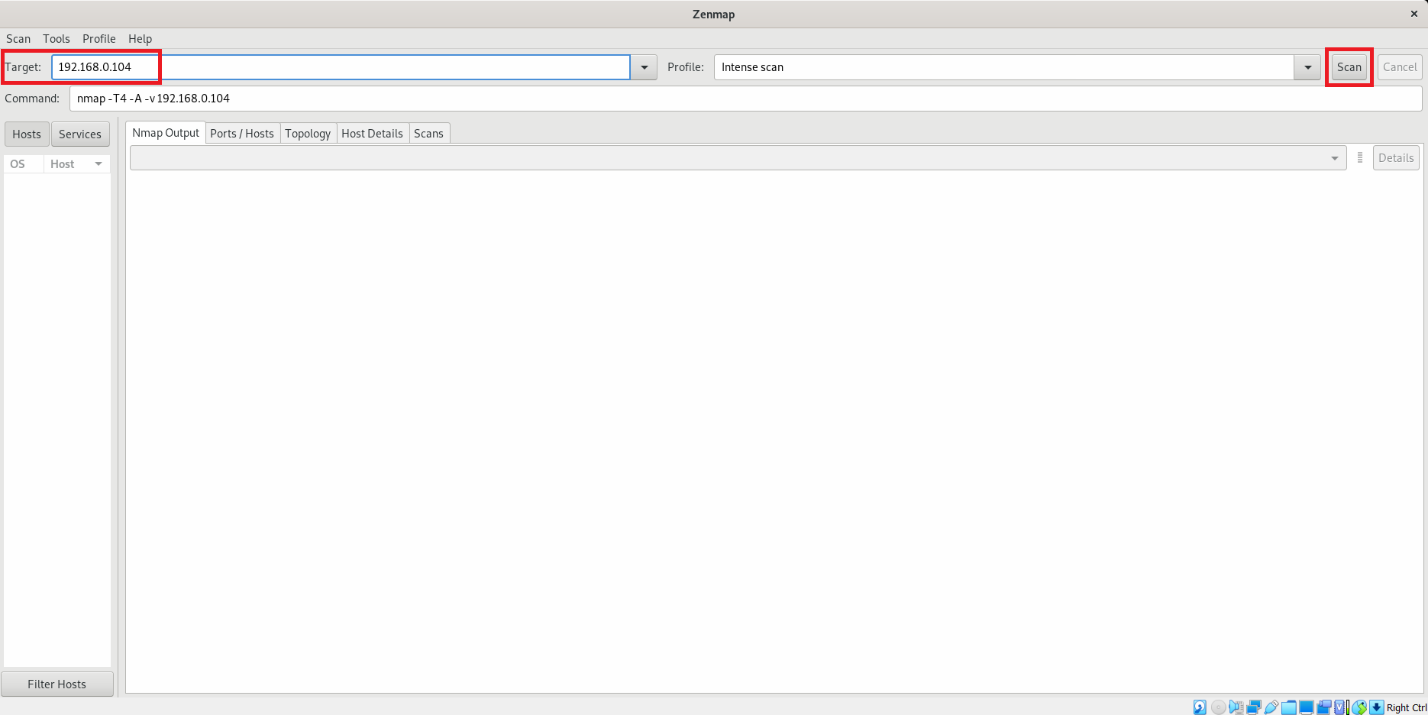
**Detect the operating system of a target:**

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



**Using Zenmap for Port Scanning:**

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

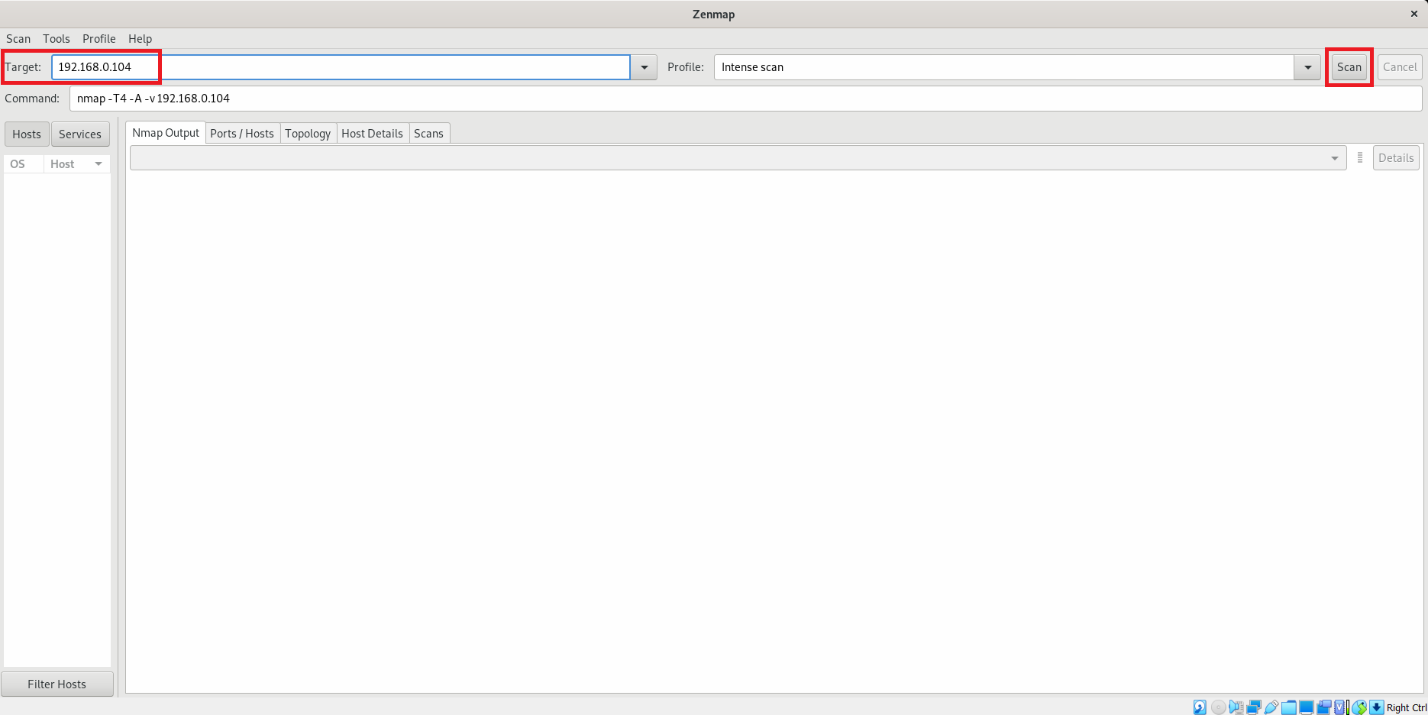


**Step 2:** Port scanning has been started.

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

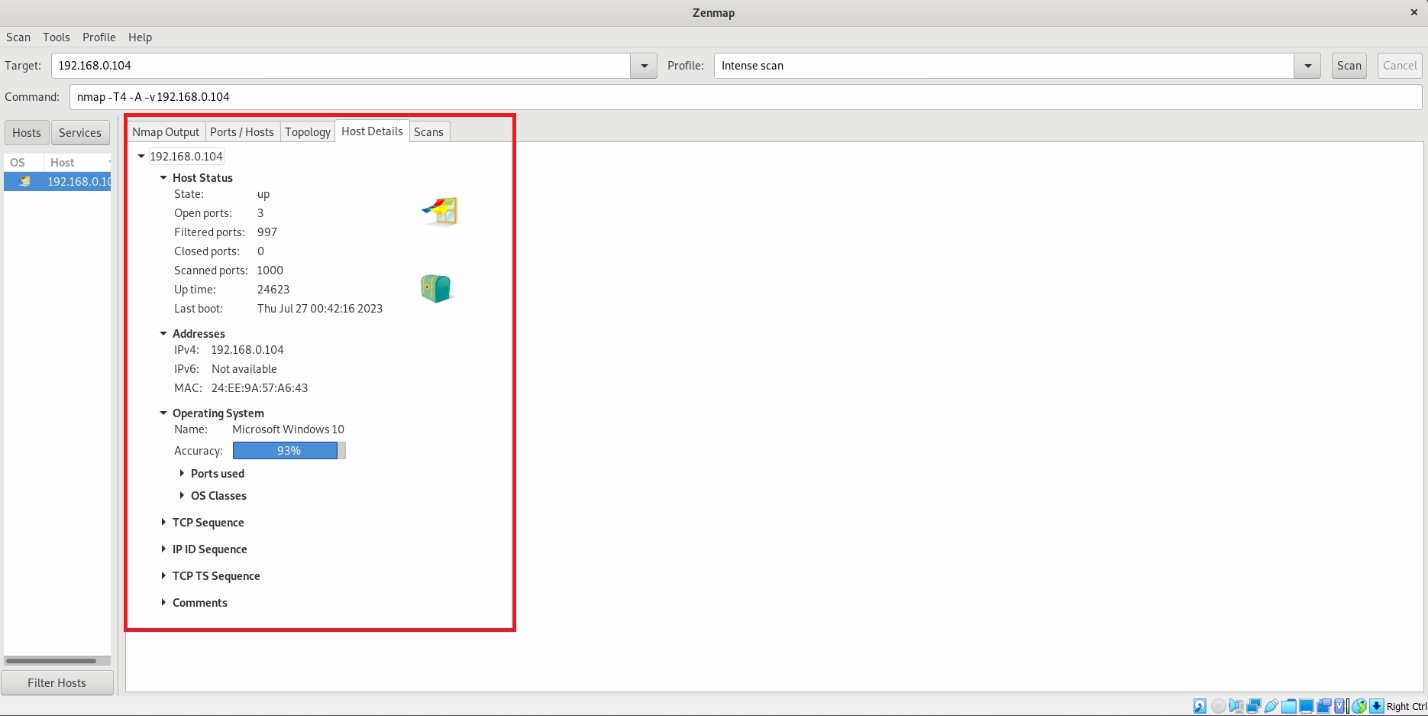
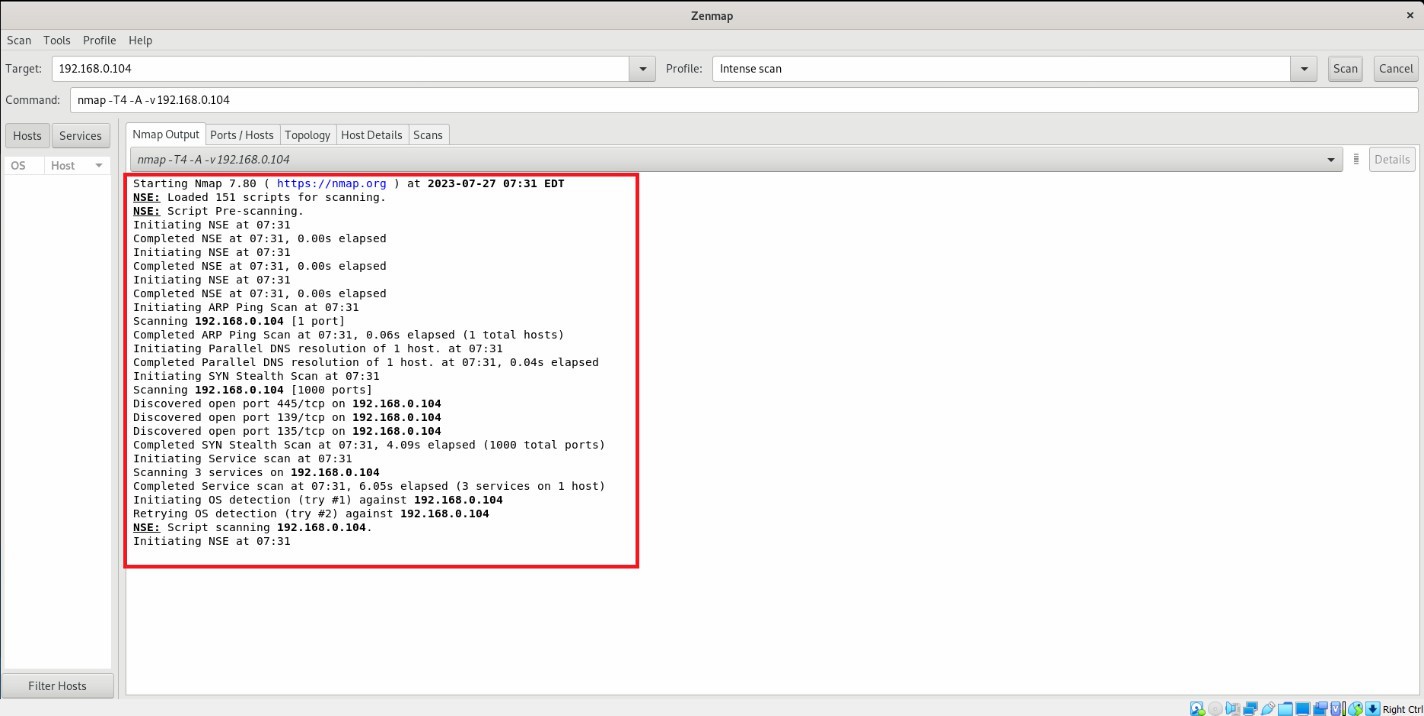
**Using Zenmap for Port Scanning:**

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

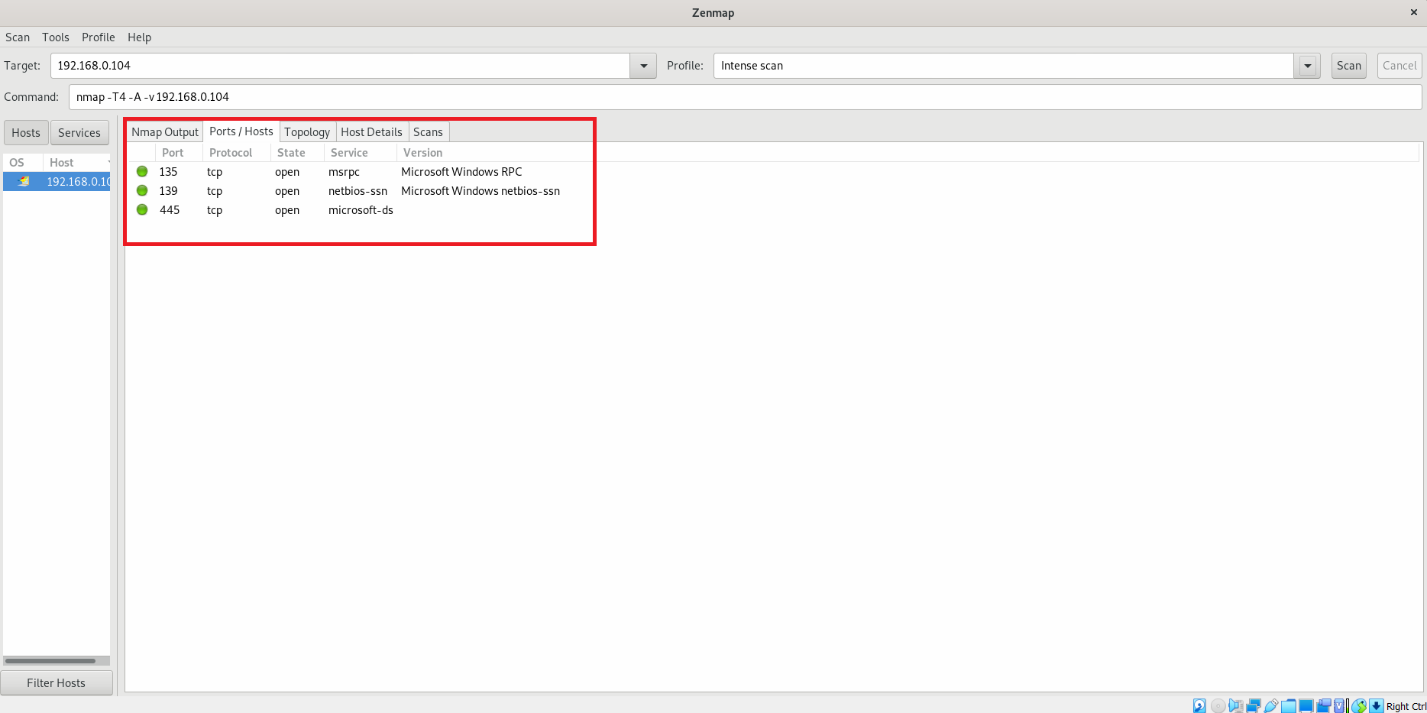


**Step 2:** Port scanning has been started.

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



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

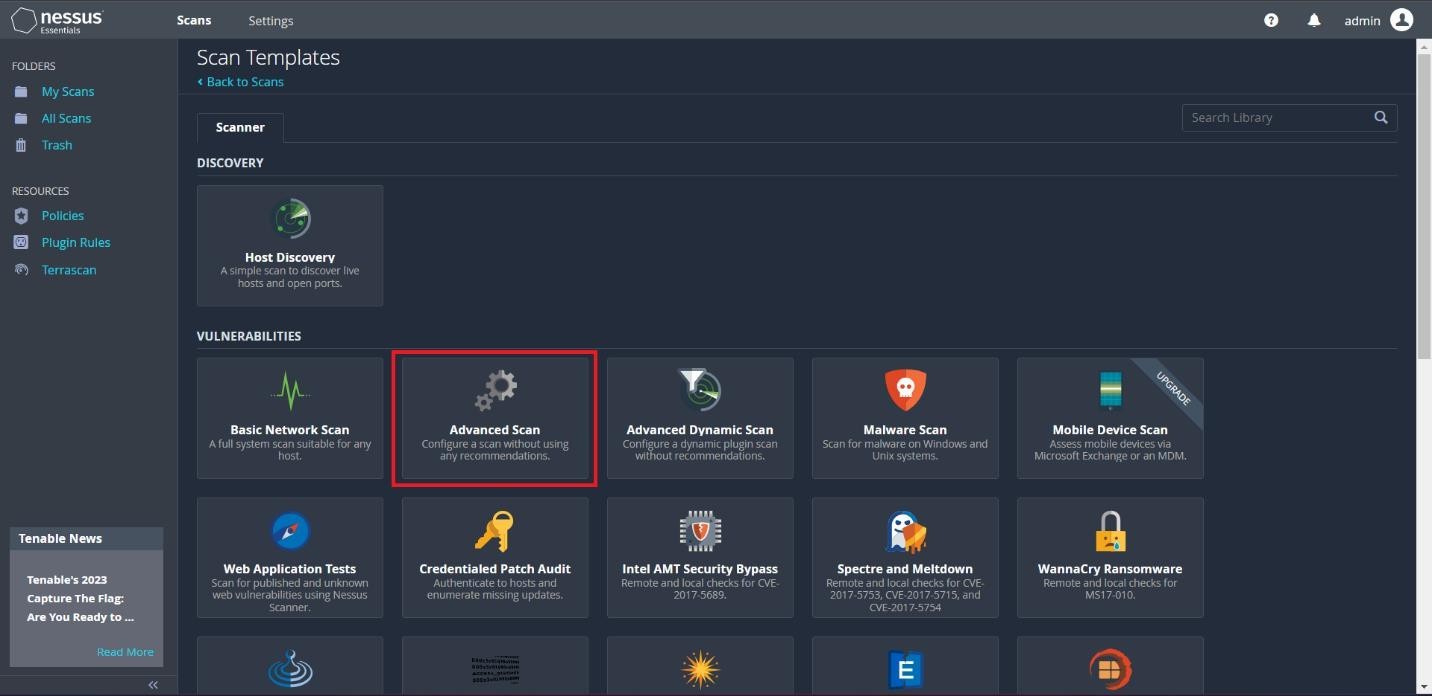


**Learning Objective 3: Vulnerability Assessment** with the help of **Nessus** scanner to find loopholes from target host**.**

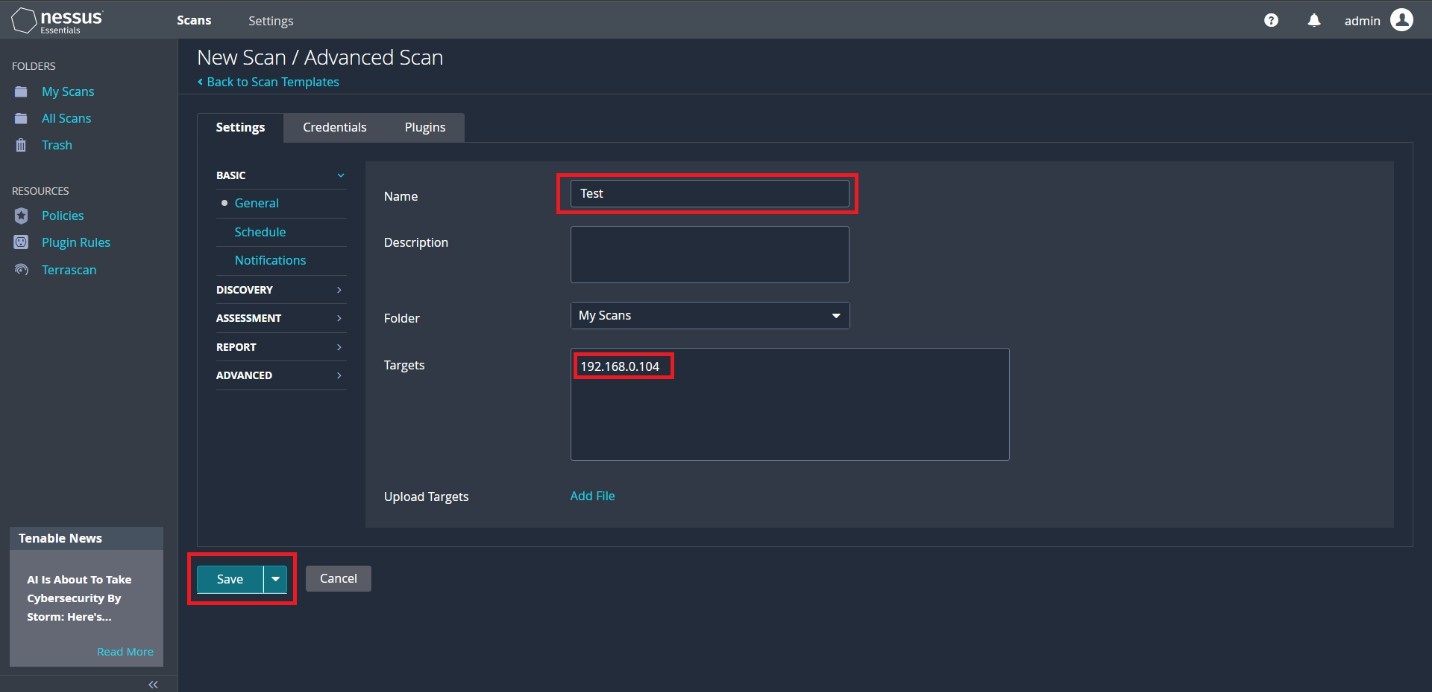
**Using Nessus Scanner:**

#Vulnerability Assessment

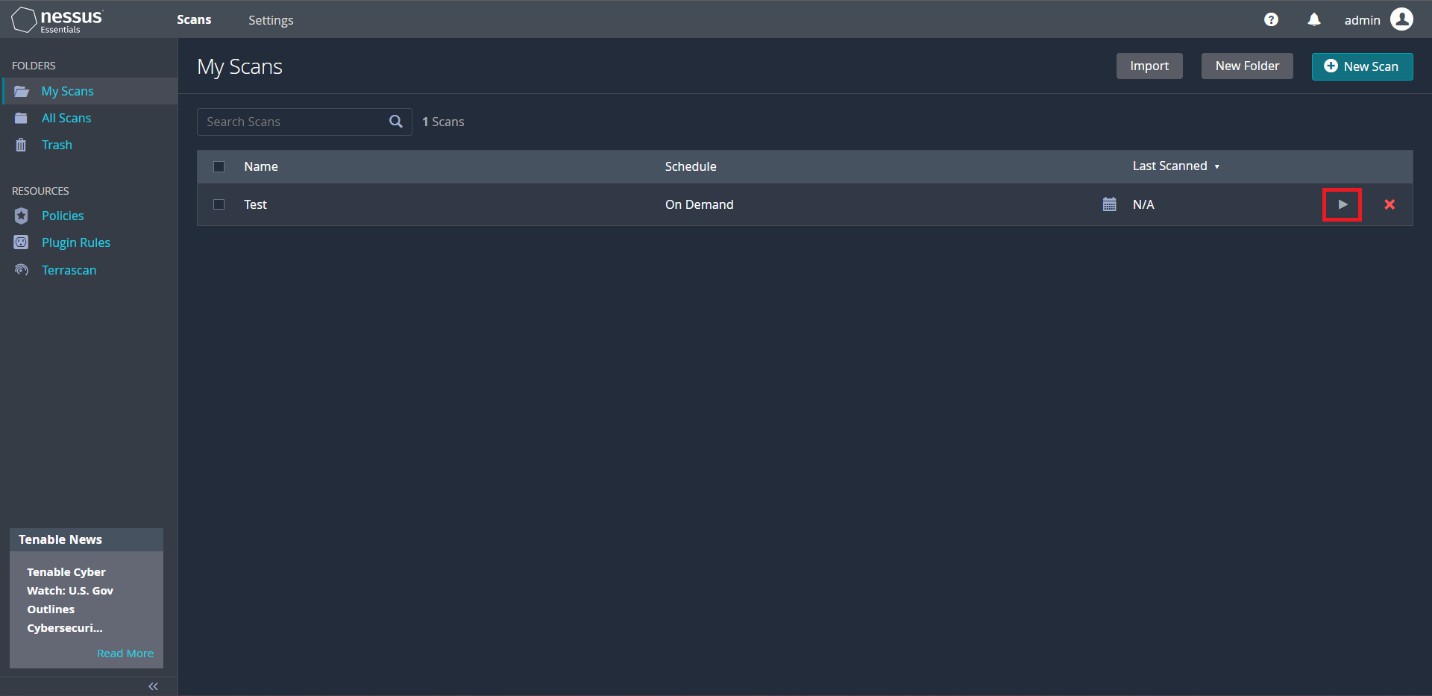
**Step 1:** Select Advance Scan option to scan the target.



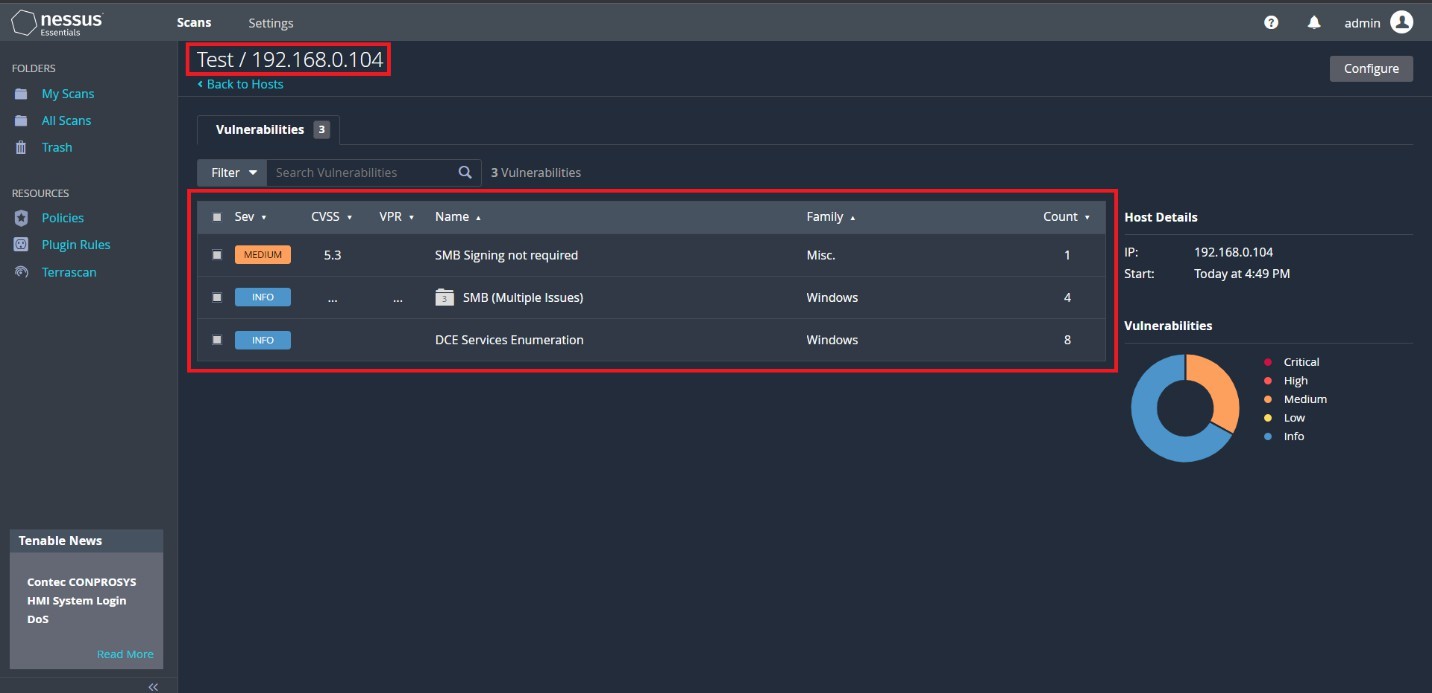
**Step 2:** Provide Name for your scan and target IP and save the scan.



**Step 3:** Launch the scan.



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

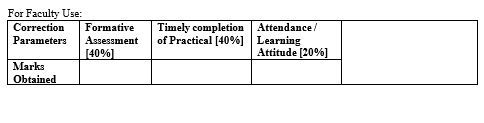


**Learning Outcomes:** The student should have the ability to perform:

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** |  |  |  |