**Lab - Exploring Nmap**

**Topology**

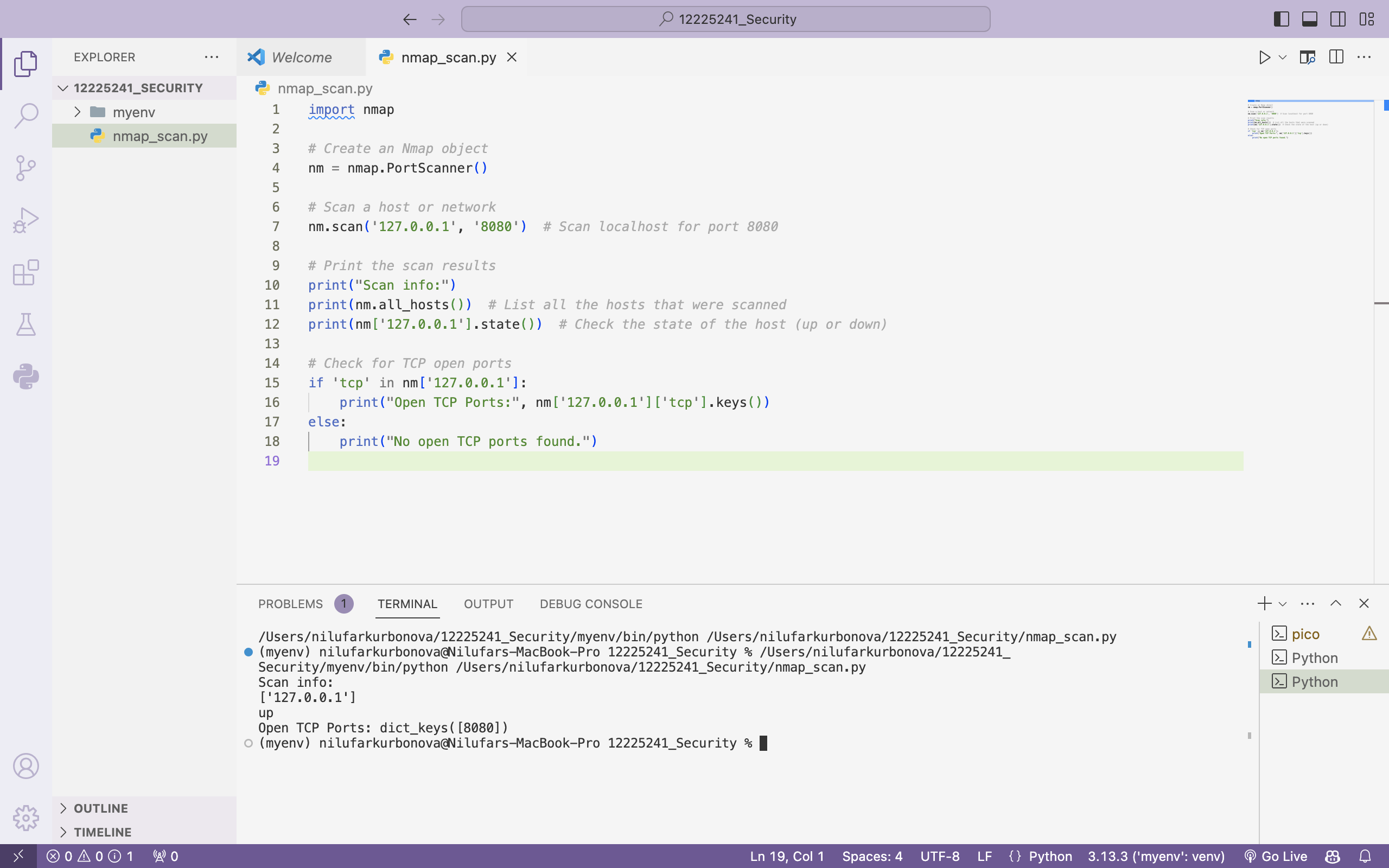
**Part 1**

### **Summary:**

In this lab, we explored the Nmap utility by utilizing manual pages (man nmap) to understand its functionality and common options.

* **Step 1:** We accessed the Nmap manual pages using the man command in the terminal.
* **Step 2:** We used navigation commands (up/down arrows, space bar) to read through the man page.
* **Step 3:** We searched for specific terms within the man page using the / (forward search) and n (next match) commands to find examples of usage and detailed explanations.

We also ran a series of Nmap scans on localhost and external servers to detect open ports and services.

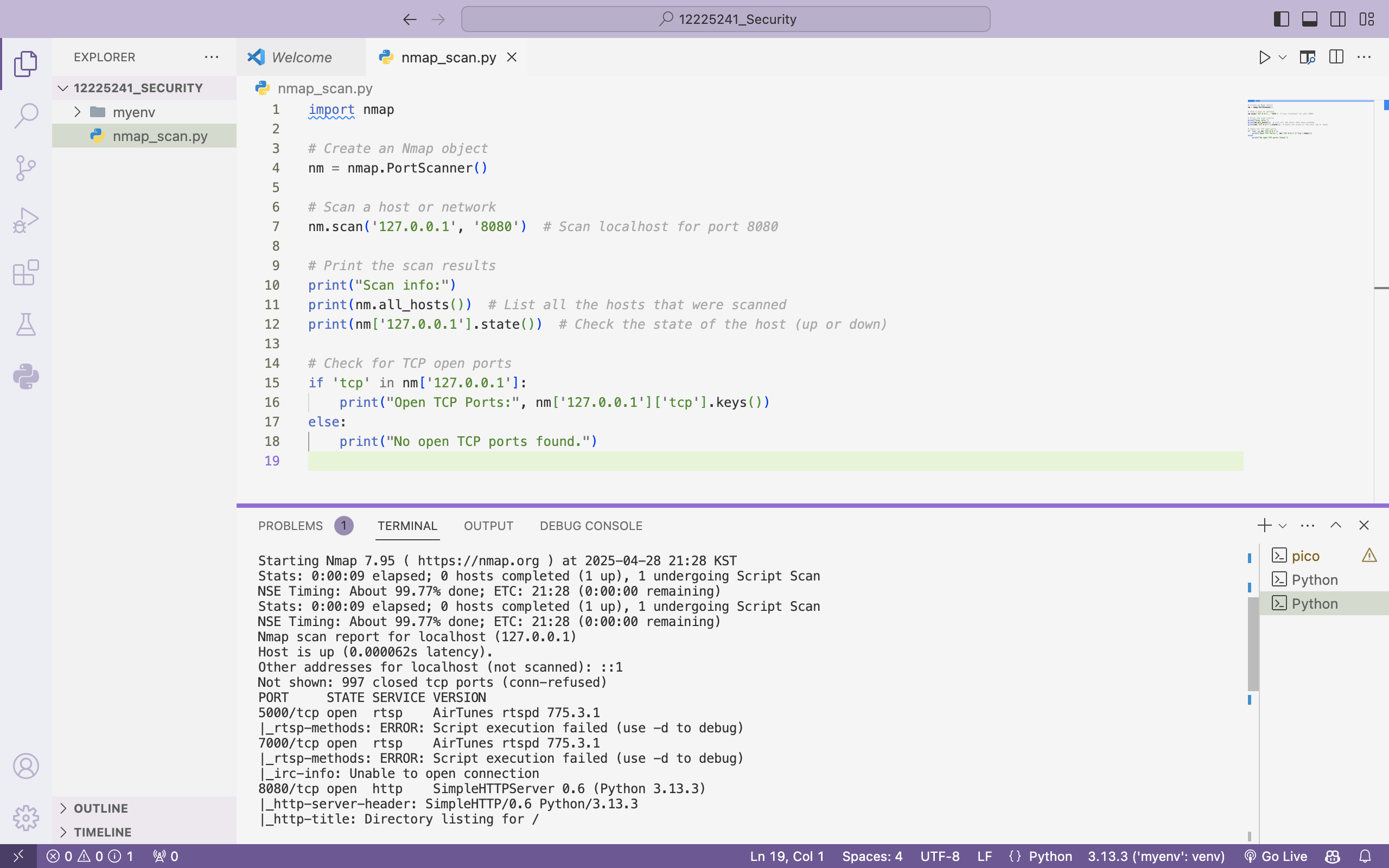


**Part 2**

### **Summary of What We Did:**

In Part 2, we scanned for open ports on various networks and hosts, including our localhost, local network, and a remote server at scanme.nmap.org.

1. **Step 1:** We scanned our localhost using nmap -A -T4 localhost to identify open ports and services.
2. **Step 2:** We scanned our local network to detect other hosts using nmap -A -T4 <network\_address>/24.
3. **Step 3:** We performed a scan on the remote server scanme.nmap.org to examine its open ports and services.



**Answers:**

#### **Step 1: Scan Your Localhost**

1. **Which ports and services are opened?**

Port 21: FTP (vsftpd 2.0.8 or later)

Port 22: SSH (OpenSSH 8.2)

Port 23: Telnet (Openwall GNU/Linux telnetd)

1. **For each of the open ports, record the software that is providing the services:**

Port 21 (FTP): vsFTPd 2.0.8 or later

Port 22 (SSH): OpenSSH 8.2

Port 23 (Telnet): Openwall GNU/Linux telnetd

#### **Step 2: Scan Your Local Network**

1. **How many hosts are up?**

4 hosts are up on the network.

1. **From your Nmap results, list the IP addresses of the hosts that are on the same LAN as your VM. List some of the services that are available on the detected hosts:**

IP addresses of hosts: 10.0.2.15, 10.0.2.4, 10.0.2.3, 10.0.2.2

Services:

Port 21 (FTP): vsFTPd 2.0.8 or later

Port 22 (SSH): OpenSSH 8.2

Port 23 (Telnet): Openwall GNU/Linux telnetd

#### **Step 3: Scan a Remote Server**

1. **What is the purpose of this site?**

The scanme.nmap.org site is a test server set up by the Nmap project to allow users to safely run Nmap scans and practice scanning techniques.

1. **Which ports and services are opened?**

Port 22: SSH (OpenSSH 6.6.1p1)

Port 80: HTTP (Apache httpd 2.4.7)

Port 9929: Nping-echo (Nping echo)

Port 31337: TCP wrapped

1. **Which ports and services are filtered?**

Port 25: SMTP

Port 135: MS RPC

Port 139: NetBIOS-SSN

Port 445: Microsoft DS

Port 593: HTTP-RPC-EPMap

Port 4444: Kerberos 524

1. **What is the IP address of the server?**

The IP address of the server is 45.33.32.156.

1. **What is the operating system?**

The operating system is **Ubuntu Linux** (based on the service version and other details in the output).