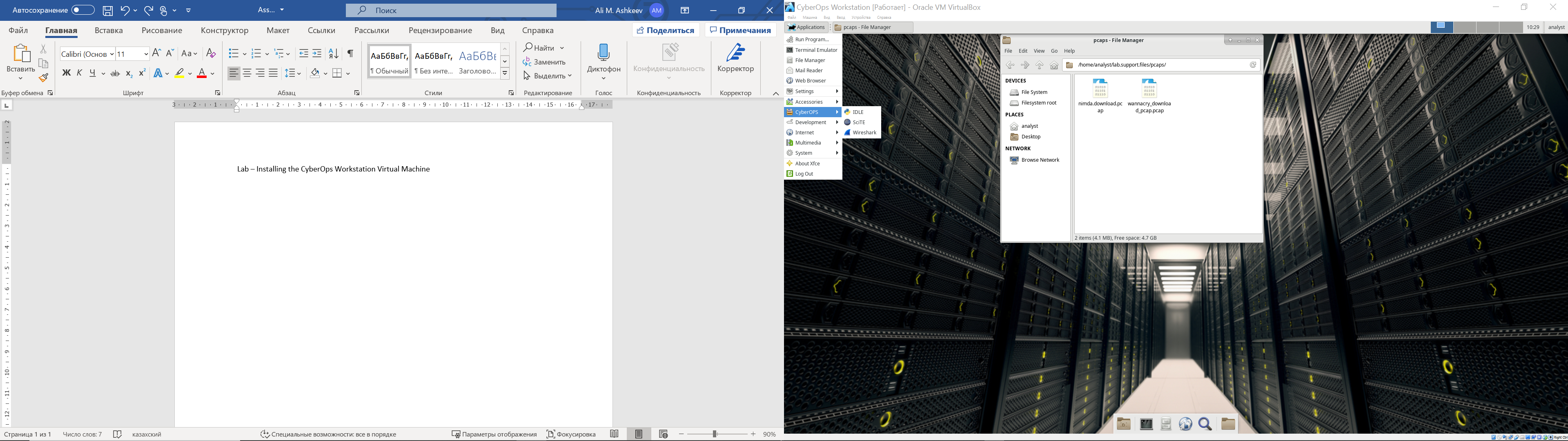
Ashkeyev Ali 18BD11079

**Lab – Installing the CyberOps Workstation Virtual Machine**



1. **List the applications in the CyberOPs menu.**

IDLE, SCiTE, Wireshark

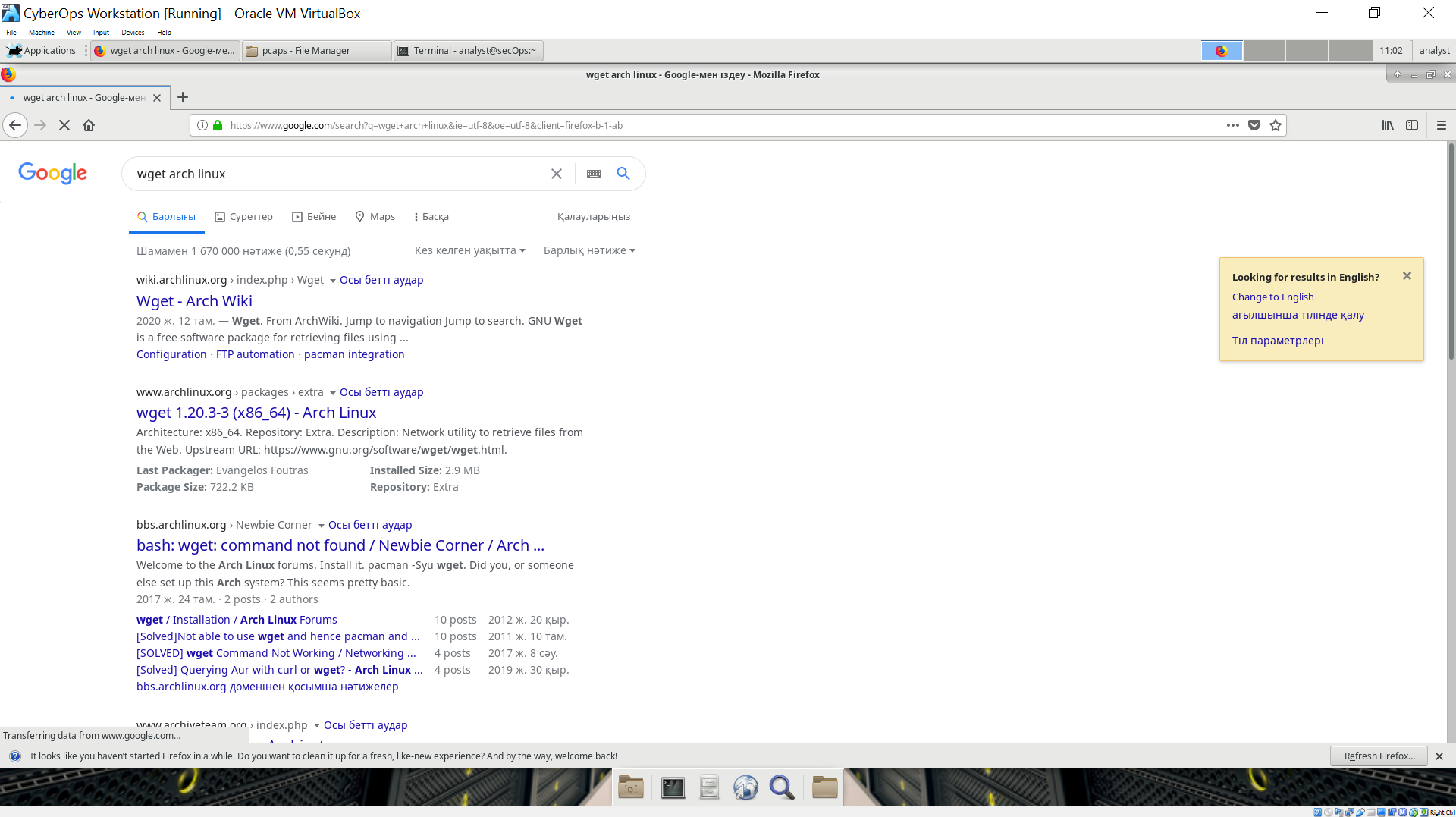
1. **Open the Terminal Emulator application. Type ip address at the prompt to determine the IP address of your virtual machine. What are the IP addresses assigned to your virtual machine?**

Изображение выглядит как компьютер

Автоматически созданное описание

192.168.1.8

**c. Locate and launch the web browser application. Can you navigate to your favorite search engine?**



Yes

**Reflection**

**What are the advantages and disadvantages of using a virtual machine?**

Advantages:

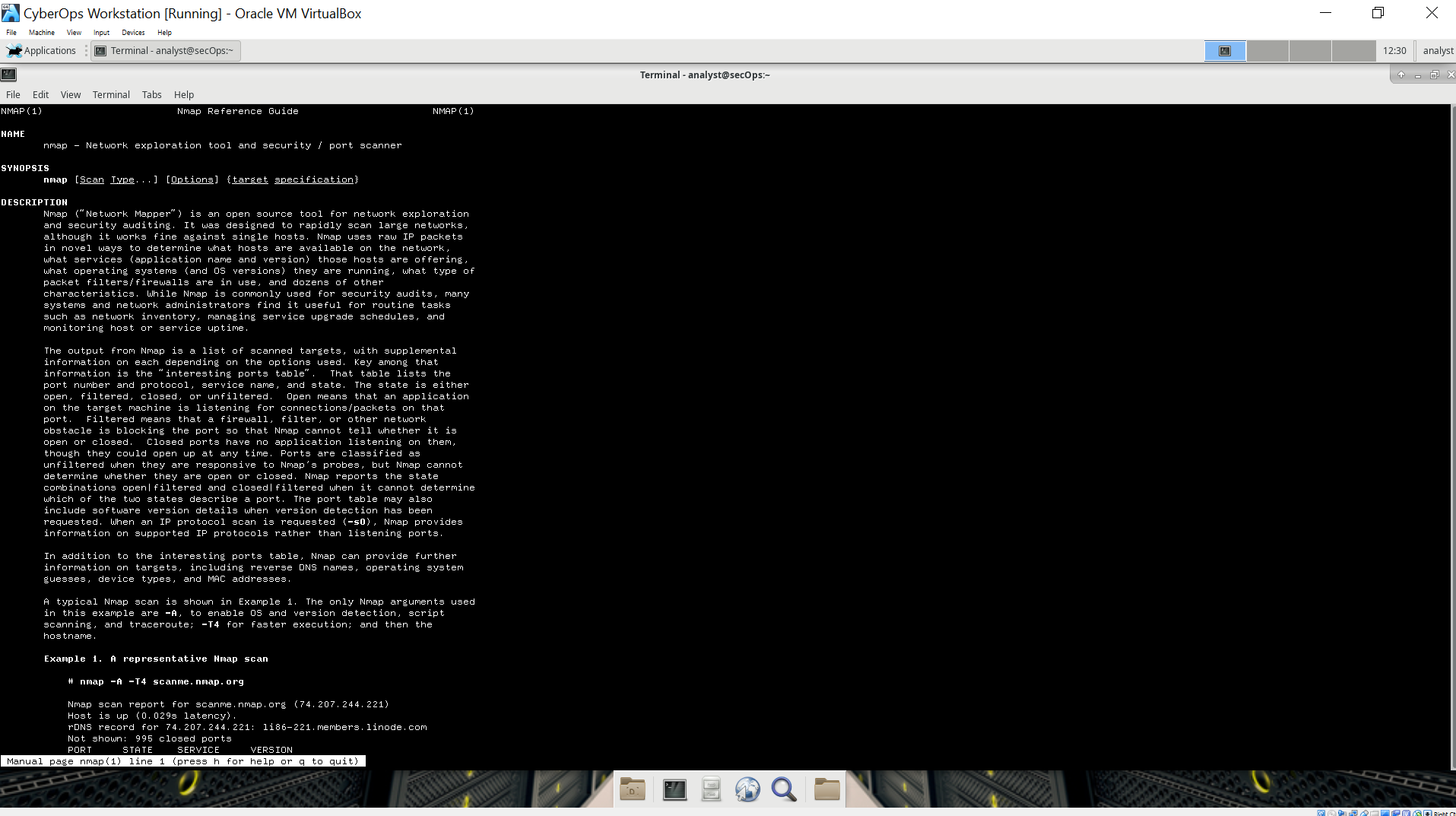
* Allows use multiple operation systems
* Virtual machine creates virtual disk, it means if vm crashes it does not affect on host machine
* Run virtual machines provides advantages in terms of security. For example, if you need to run an application with questionable security, you can run it in the guest operating system. So, if the app causes corruption, it will be temporary after the guest is closed. VMS also allow you to improve security forensics by tracking down flaws in guest operating systems and allowing the user to quarantine them for analysis.

Disadvantages:

* Virtual machines are less efficient than real machines because they access hardware indirectly.
* A virtual machine can be infected with the weaknesses of the host machine.

**Lab - Exploring Nmap**

**Part 1: Exploring Nmap**



a.

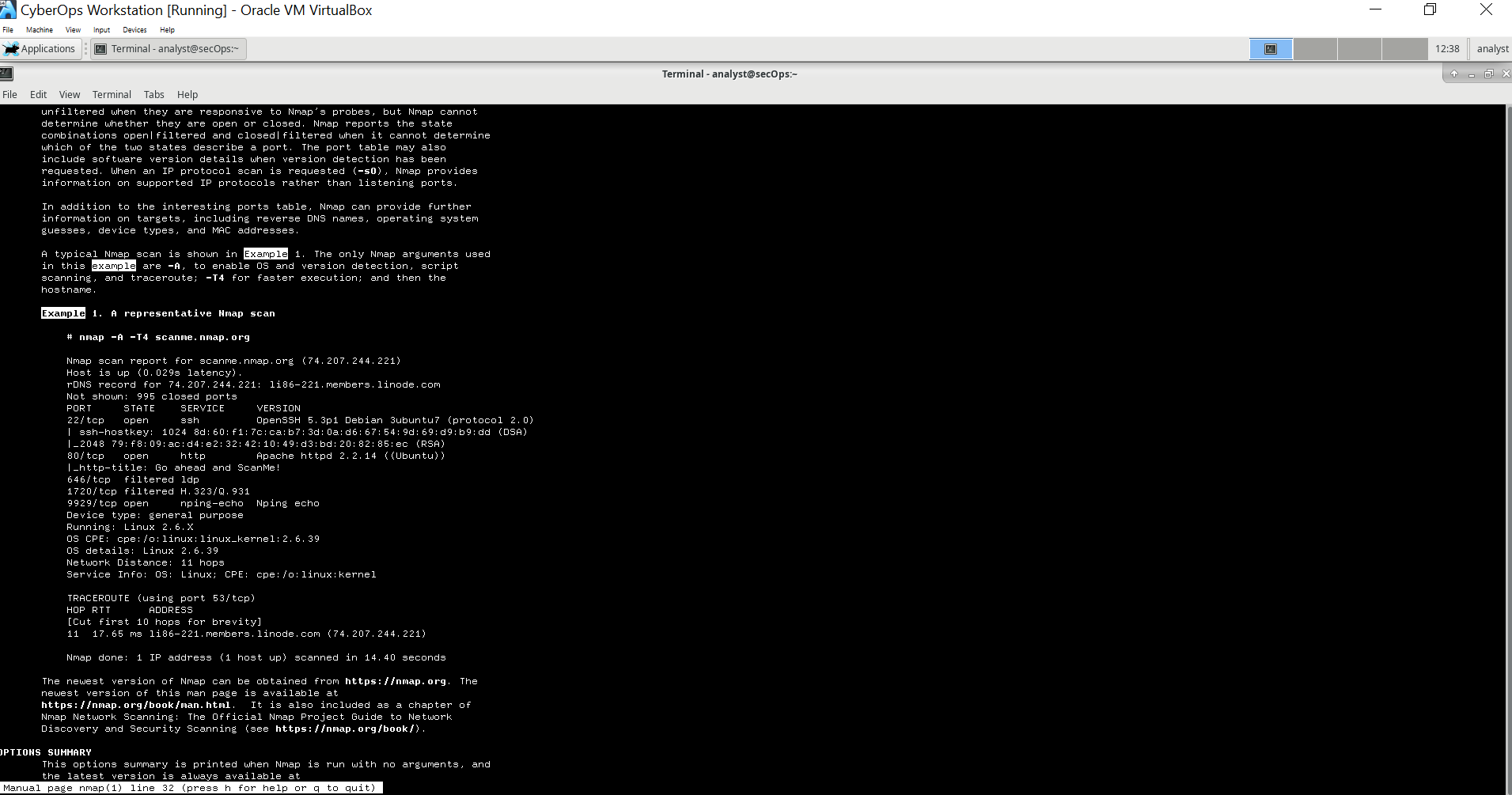
**What is Nmap?**

Open source tool for network exploration and security auditing. It can scan large networks as well as single host.

**What is nmap used for?**

With raw IP packets it determines what hosts are available in the network, what services those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Network administrators uses it for, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

d. While in the man page, you can use the up and down arrow keys to scroll through the pages. You can also press the space bar to forward one page at a time. To search for a specific term or phrase use enter a forward slash (/) or question mark (?) followed by the term or phrase. The forward slash searches forward through the document, and the question mark searches backward through the document. The key n moves to the next match.



**What does the switch -T4 do?**

Nmap -A -T4 scanme.nmap.org

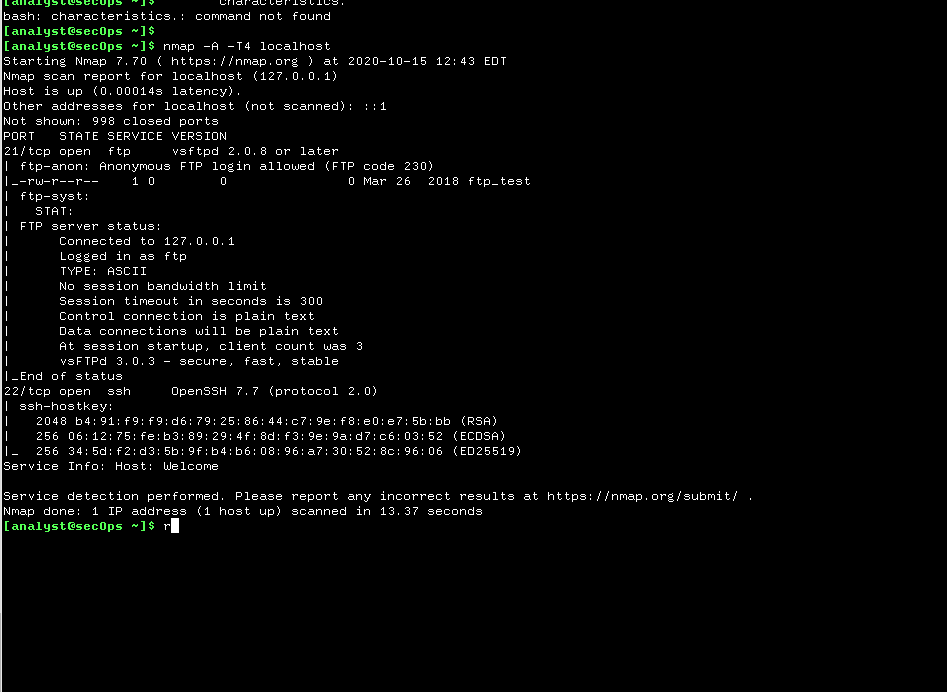
**What does the switch -A do?**

Enable OS and version detection, script running and traceroute

**What does the switch -T4 do?**

For faster execution

**Part 2: Scanning for Open Ports**



1. **Review the results and answer the following questions.**

**Which ports and services are opened?**

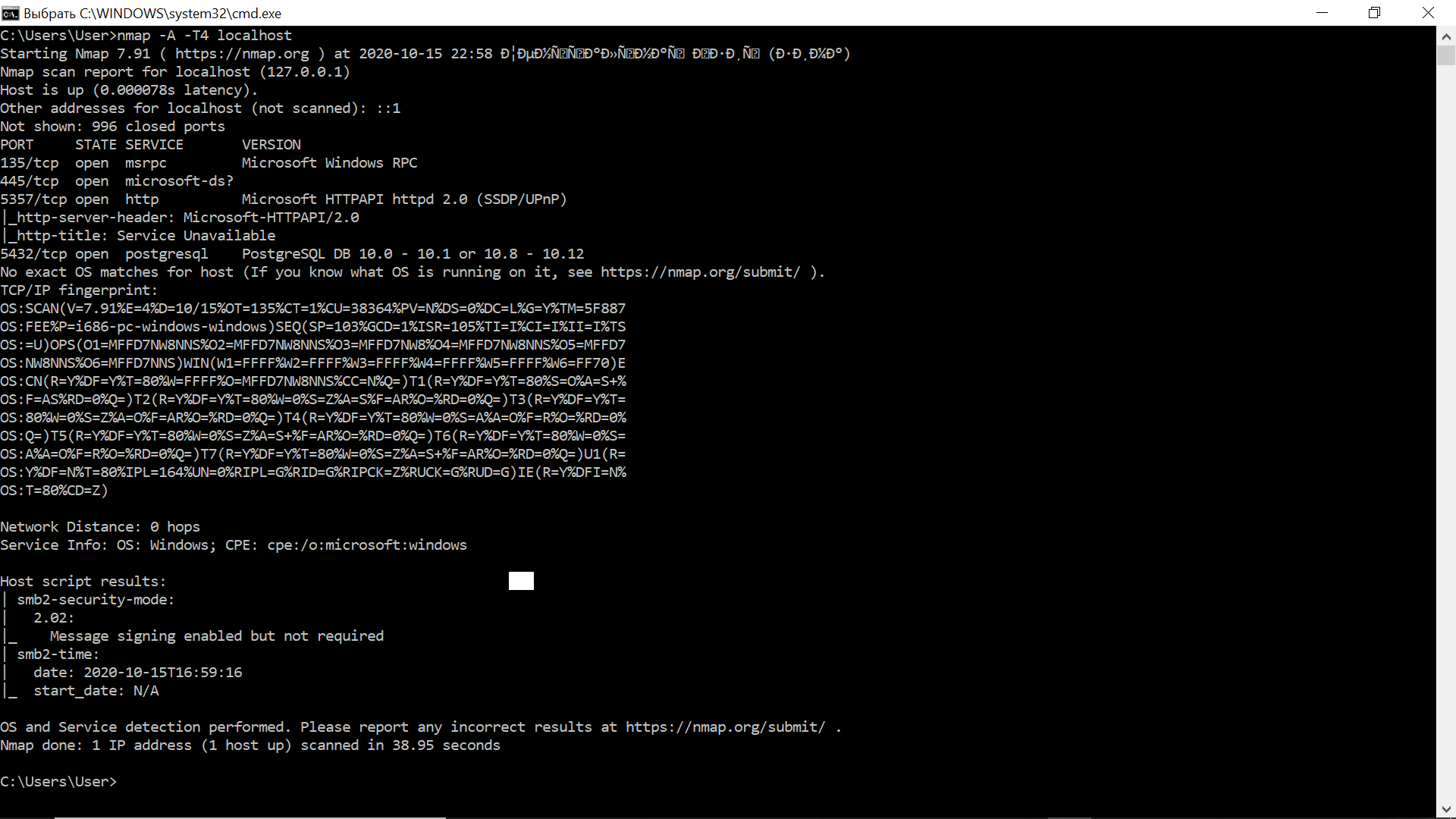
In cyberops it is opened: 21/tcp: ftp, 22/tcp:ssh

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

ftp: vsftpd, ssh: OprnSSH

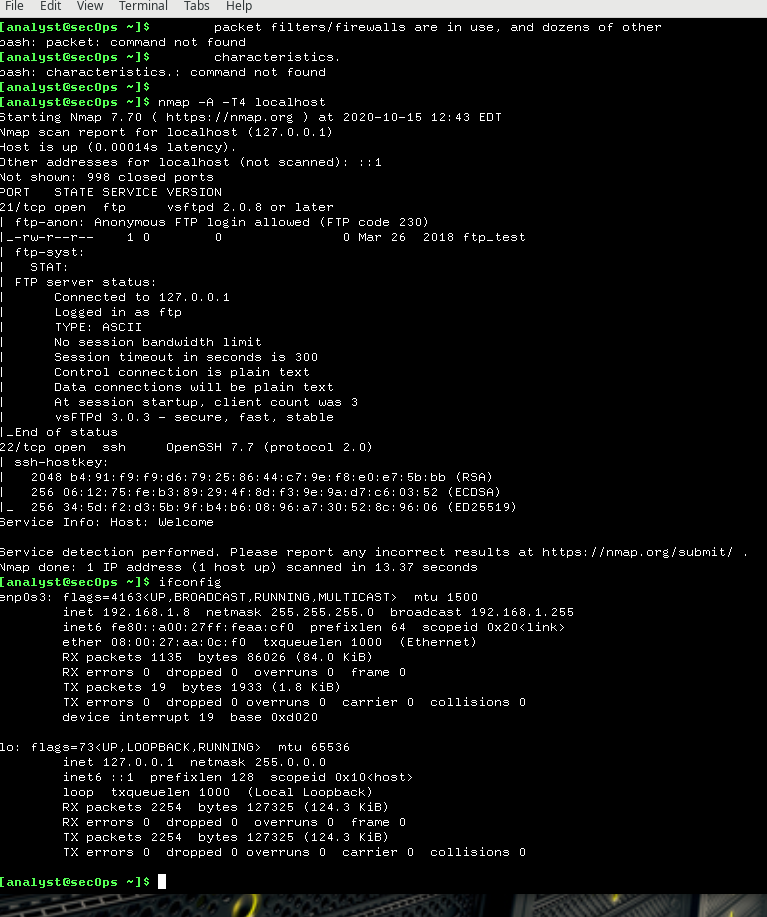
**What is the operating system?**

In this cybercops it is not identified. But for example in host machine it identified that it is windows10

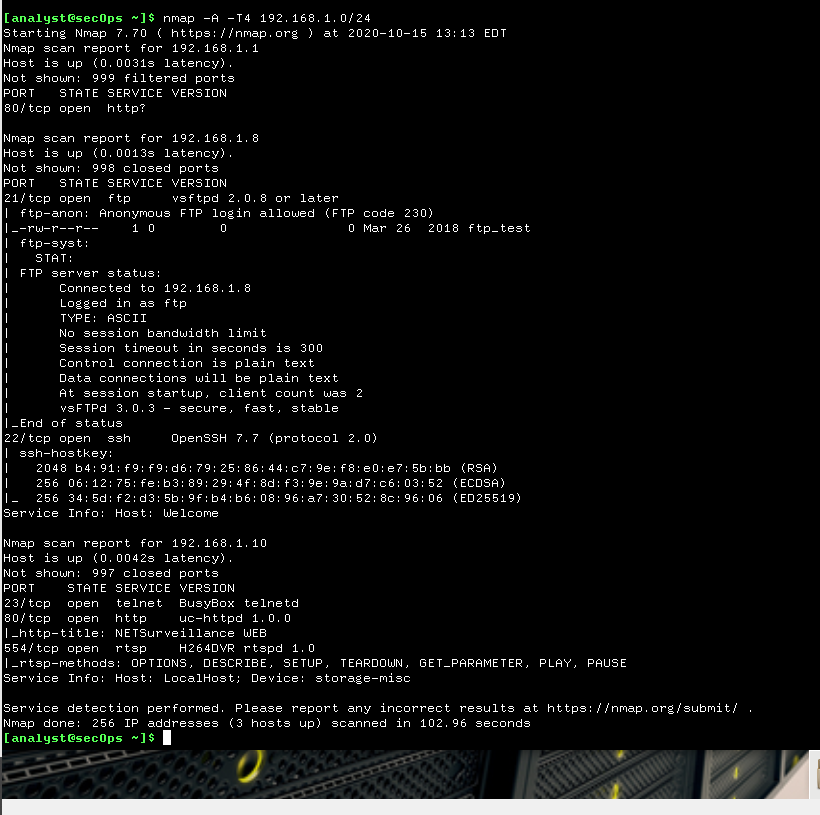
****

**Step 2: Scan your network.**

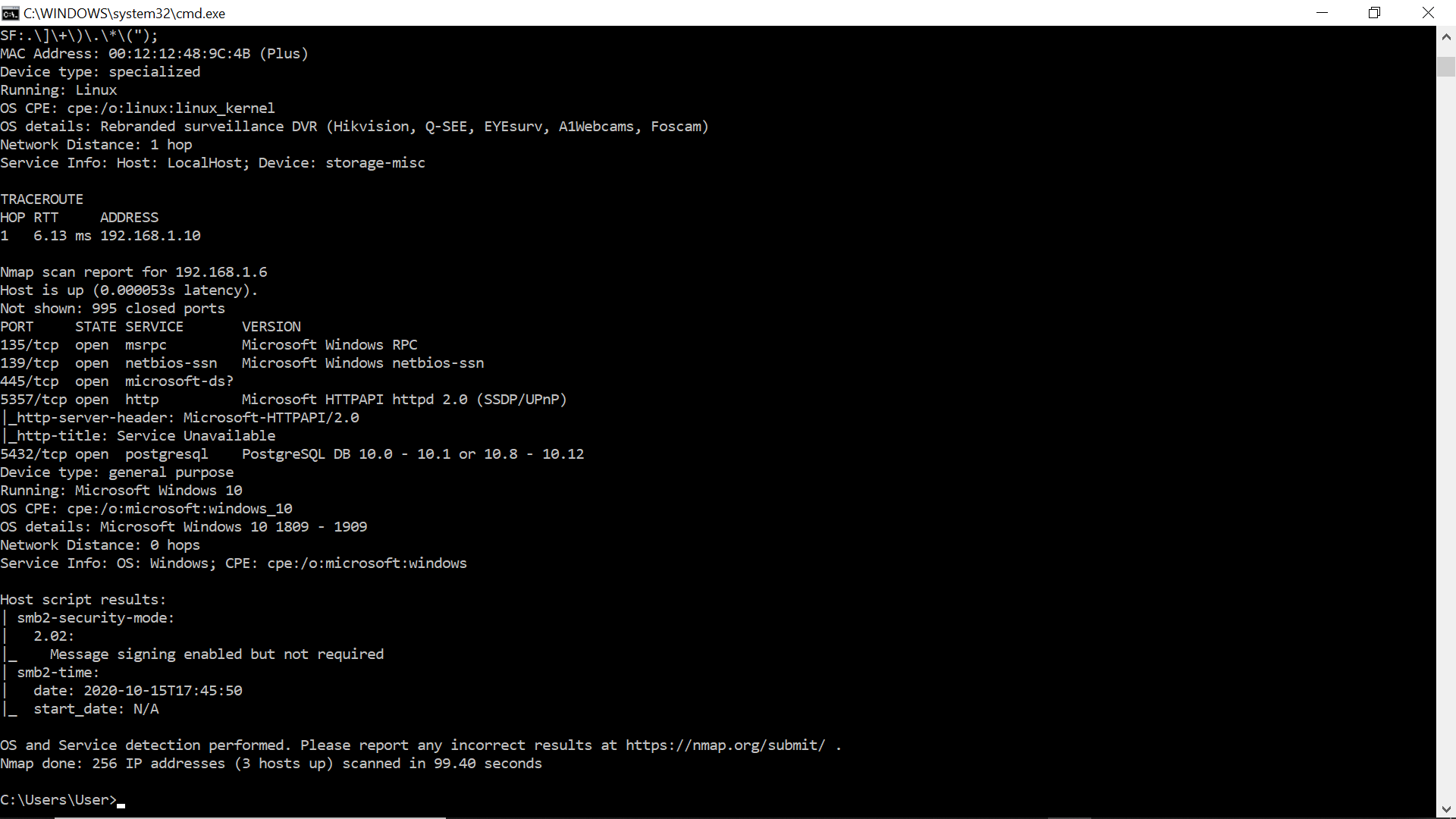
1. **Record the IP address and subnet mask for your VM. Which network does your VM belong to?**



192.168.1.8 netmask 255.255.255.0



Nmap in Cyberops virtualbox



Nmap in windows host machine

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

3 hosts up

**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.**

192.168.1.1

192.168.1.8

ftp: vsftpd, ssh: Openssh

192.168.1.10:

23/tcp: telnet: BusyBox

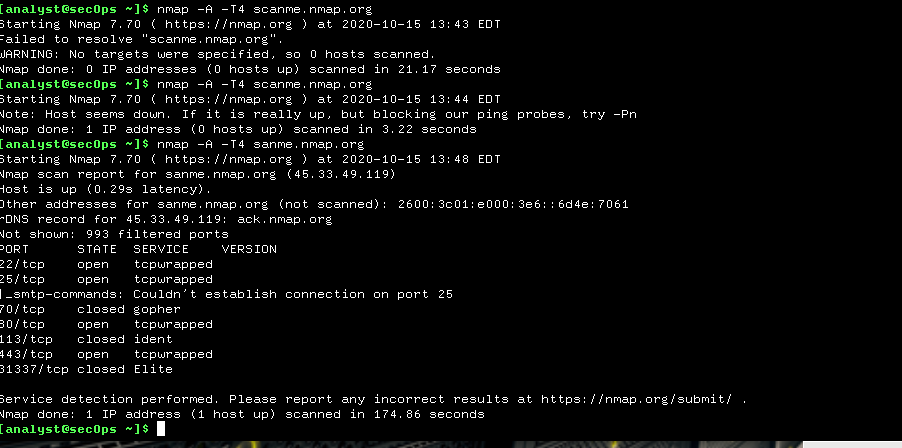
80/tcp: http: uc-httpd

554/tcp: rtsp H264DVR rtspd

**Step 3: Scan a remote server.**

1. **Open a web browser and navigate to scanme.nmap.org. Please read the message posted. What is the purpose of this site?**

Site about nmap, it has information about Nmap commands and test installation.



1. **At the terminal prompt, enter nmap -A -T4 scanme.nmap.org.**



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

22/tcp: ssh, 80/tcp: http, 9929/tcp: nping-echo, 31337/tcp: tcpwrapped

**Which ports and services are filtered?**

1026/tcp: LSA-or-nterm, 1027/tcp: IIS, 1028/tcp: unknown, 2019/tcp: ms-lsa, 1030/tcp: iad1, 1031/tcp: iad2, 1032/tcp: iad3, 1033/tcp: netinfo, 1034/tcp: zincite-a, 1035/tcp: multidropped

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

45.33.32.156

**What is the operating system?**

Linux

**Reflection**

**Nmap is a powerful tool for network exploration and management. How can Nmap help with network security? How can Nmap be used by a threat actor as a nefarious tool?**

It can be used to explore internal network for open ports and be sure that all the systems are probably patched against security concerns, but at the same time hackers can use it to identify open ports in your system.