**Name:** Bakhtiyorov Firdavs **ID:** 12214762

**Question 1]**

**a).    If you must perform a man-in-the-middle attack using ARP Spoofing in the topology. Where would you place yourself in the topology and which devices will you be connecting to?**

I will connect myself to the Switch. I will target PC1 and the Router to perform ARP Spoofing.

**b).**  **The PC1 is sending the ARP request, explain where will that request go and what is your role as a "man-in-the-middle" attacker?**

When PC1 sends an ARP request, I will reply with my MAC address pretending to be the Router.

**c).**  **Explain the COMPLETE activity in the topology if you as a "man-in-the-middle" attacker is initiating the ARP request. Draw the flowchart of the COMPLETE activity in the topology. Explain how will you get hold of the data?**

**PC1 sends ARP request ➔ "Who has Router's IP?"**

**Attacker quickly replies ➔ "I have it!" (provides attacker's MAC)**

**PC1 updates its ARP table with attacker's MAC address for Router**

**PC1 sends packets to Attacker instead of Router**

**Attacker forwards the packets to the real Router**

**Attacker can intercept, read, or modify the data**

**Question 2]**

**Part - 1]**

**What is significant about the contents of the destination address field?**

All hosts on the LAN will receive this broadcast frame. The host with the IP address of 192.168.1.1 (default gateway) will send a unicast reply to the source (PC host). This reply contains the MAC address of the NIC of the Default Gateway.

**Why does the PC send out a broadcast ARP prior to sending the first ping request?**

Before the PC can send a ping request to a host, it needs to determine the destination MAC address before it can build the frame header for that ping request. The ARP broadcast is used to request the MAC address of the host with the IP address contained in the ARP.

**What is the MAC address of the source in the first frame?**

f4:8c:50:62:62:6d

**What is the Vendor ID (OUI) of the Source’s NIC?**

IntelCor (Intel Corporation)

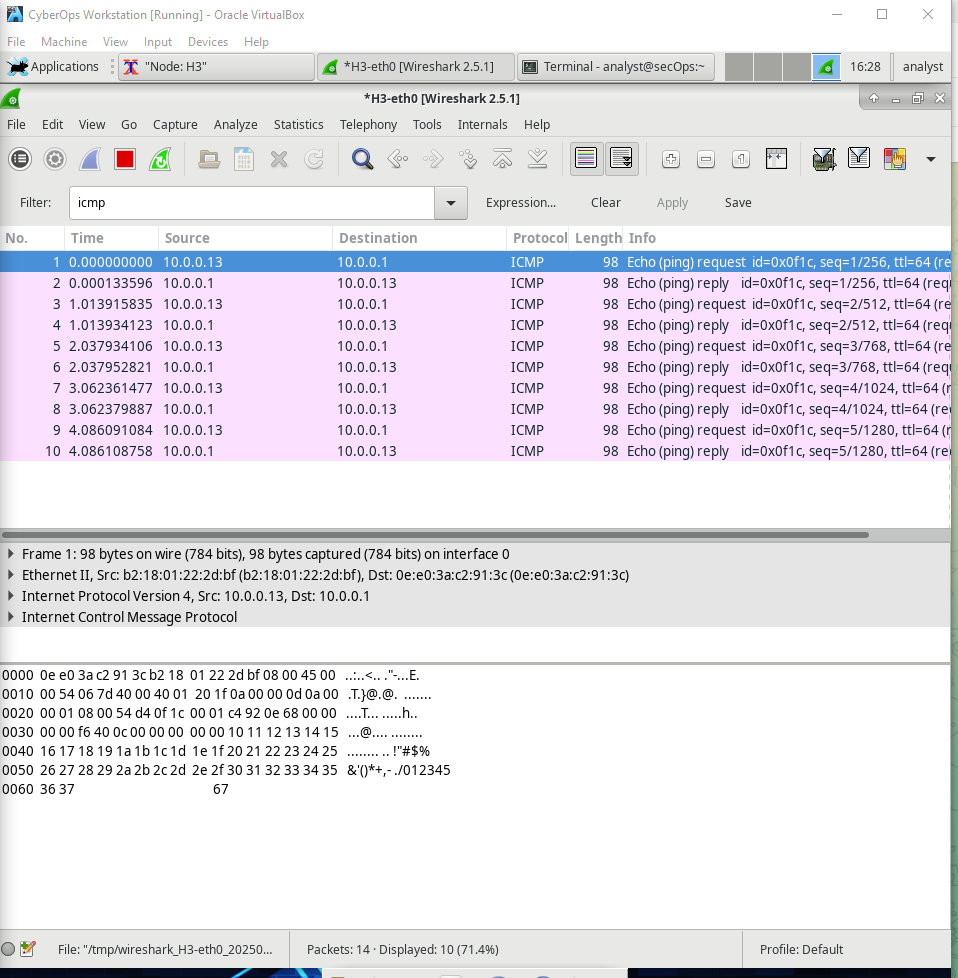
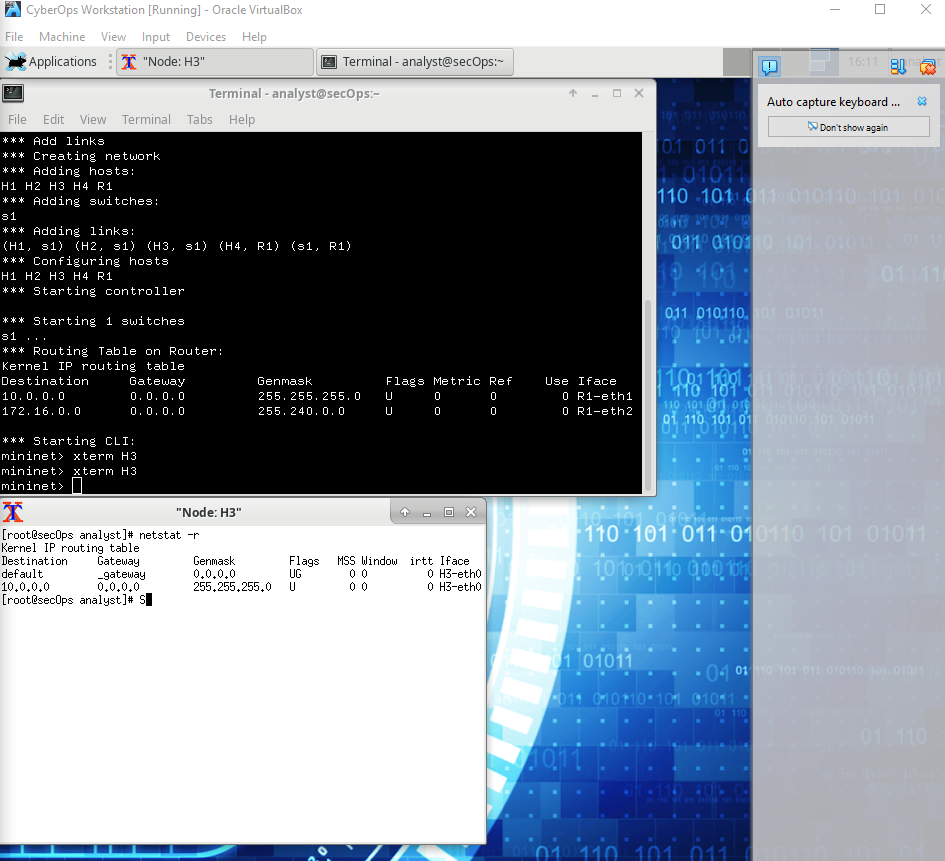
**What portion of the MAC address is the OUI?**

The first 3 octets of the MAC address indicate the OUI.

**What is the Source’s NIC serial number?**

62:62:6d

**Part - 2]**



**What is the MAC address of the PC’s NIC?**

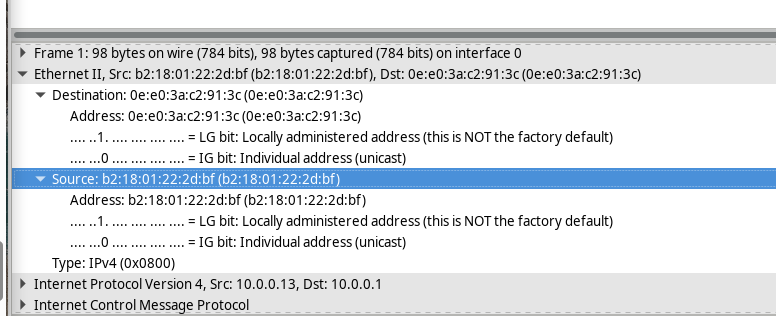
b2:18:01:22:2d:bf

**What is the default gateway’s MAC address?**

0e:e0:3a:c2:91:3c

**What type of frame is displayed?**

IPv4(0x0800)

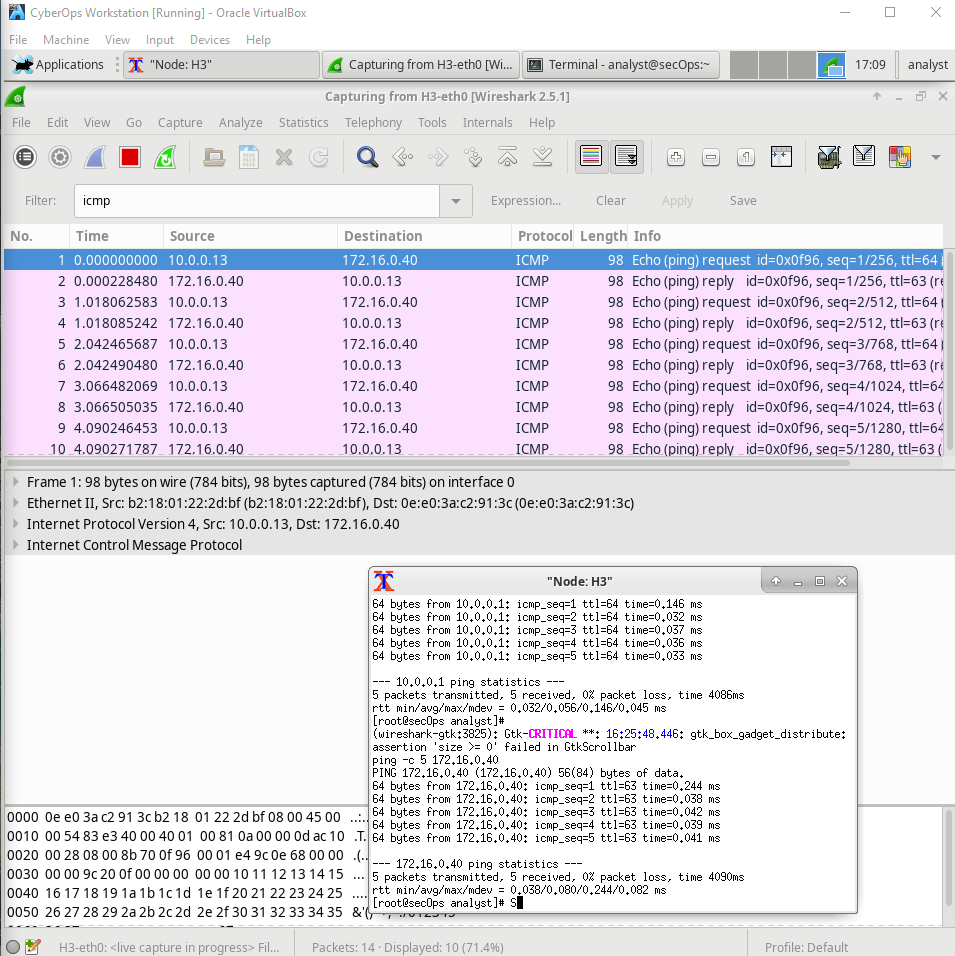


**What is the source IP address?**

10.0.0.13

**What is the destination IP address?**

10.0.0.1



**Source:**

10.0.0.3

**Destination:**

172.16.0.40

**Why has the destination IP address changed, while the destination MAC address remained the same?**

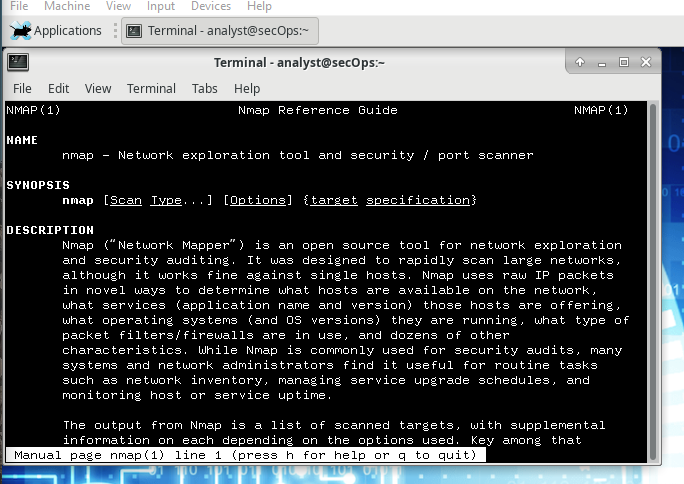
**Layer 2 frames never leave the LAN. When a ping is issued to a remote host, the source will use the Default Gateway’s MAC address for the frame destination. The Default Gateway receives the packet, strips the Layer 2 frame information from the packet and then creates a new frame header with the next hop’s MAC address. This process continues from router to router until the packet reaches its destination IP address.**

**Wireshark does not display the preamble field of a frame header. What does the preamble contain?**

**The preamble field contains seven octets of alternating 1010 sequences, and one octet that signals the beginning of the frame, 10101011.**

**Question 3]**

**Part - 1]**

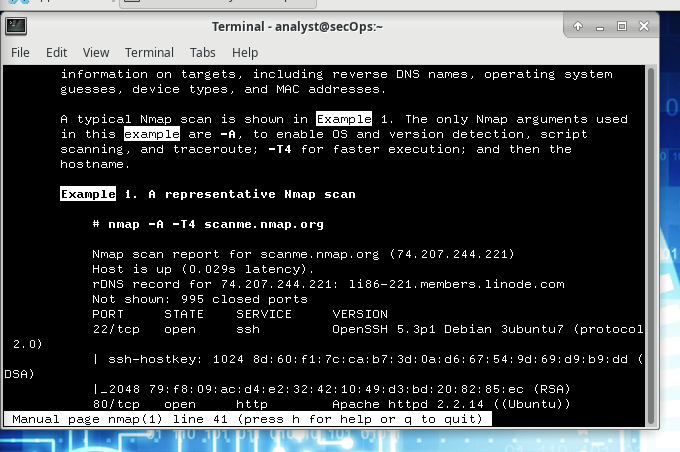


**What is Nmap?**

Nmap is a network exploration tool and security / port scanner.

**What is nmap used for?**

Nmap is used to scan a network and determine the available hosts and services offered in the network. Some of the nmap features include host discovery, port scanning and operating system detection. Nmap can be commonly used for security audits, to identify open ports, network inventory, and find vulnerabilities in the network.



**What is the nmap command used?**

Nmap -A -T4 scanme.nmap.org

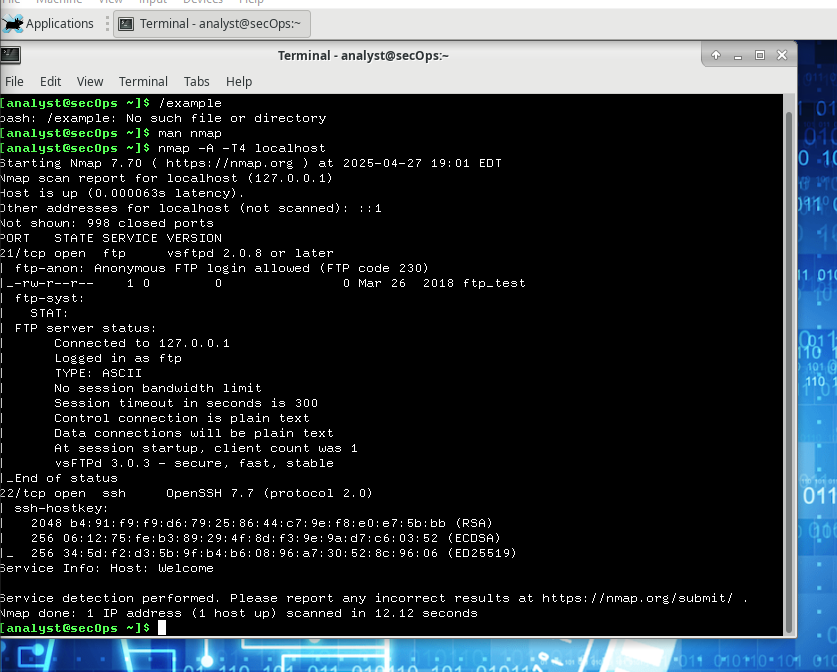
**What does the switch -A do?**

-A: Enable OS detection, version detection, script scanning, and traceroute

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

-T4 for faster execution by prohibiting the dynamic scan delay from exceeding 10 ms for TCP ports. -T4 is recommended for a decent broadband or ethernet connection.

**Part - 2]**

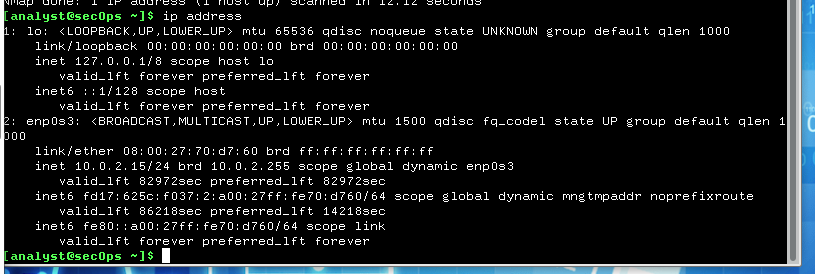


**Which ports and services are opened?**

**21/tcp: ftp, 22/tcp: ssh**

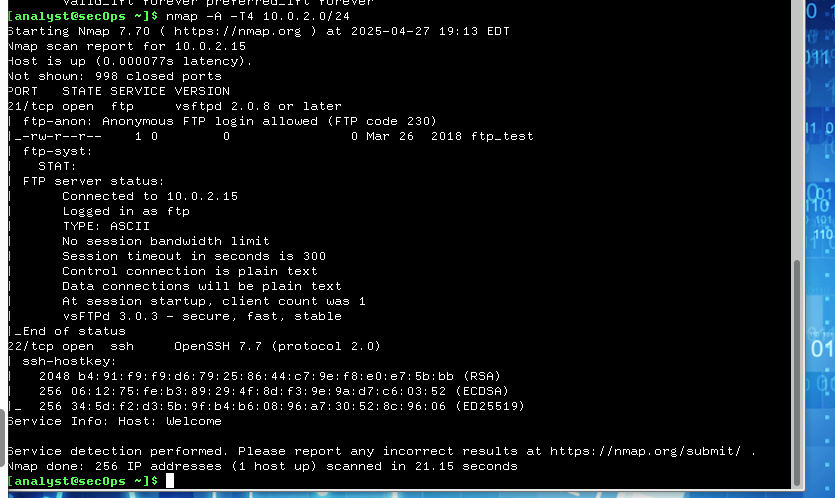
**For each of the open ports, record the software that is providing the services.**

**ftp: vsftpd, ssh: OpenSSH**



**Which network does your VM belong to?**

**It has an IP address of 127.0.0.1/8 and it is part of the 10.0.2.15/24 network.**

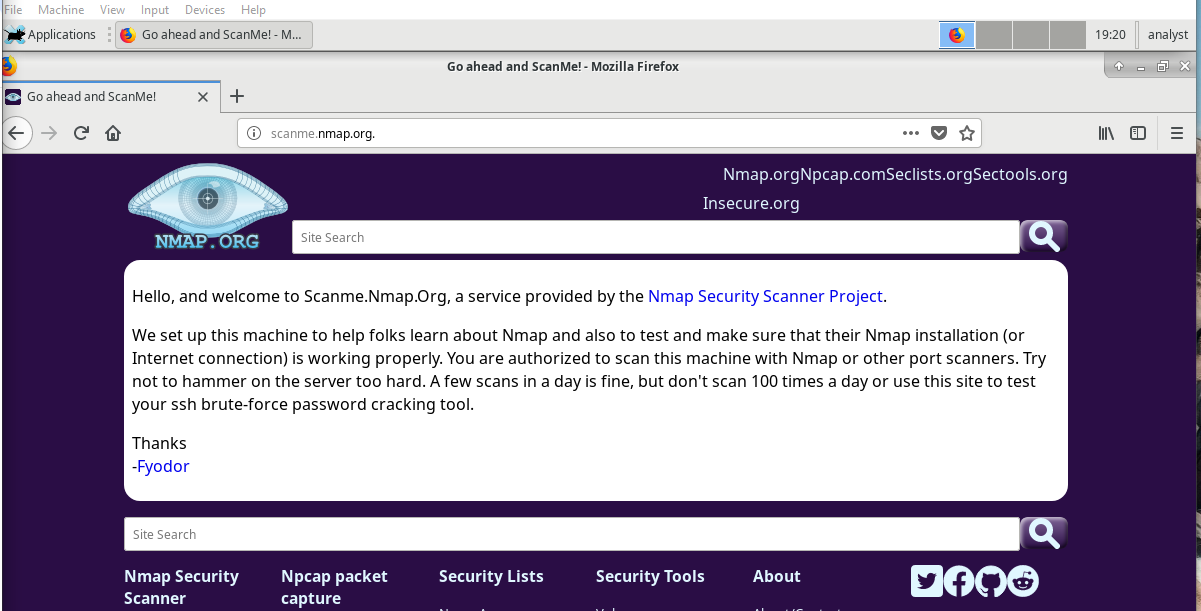


**How many hosts are up?  
1 host is up.**

**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.**

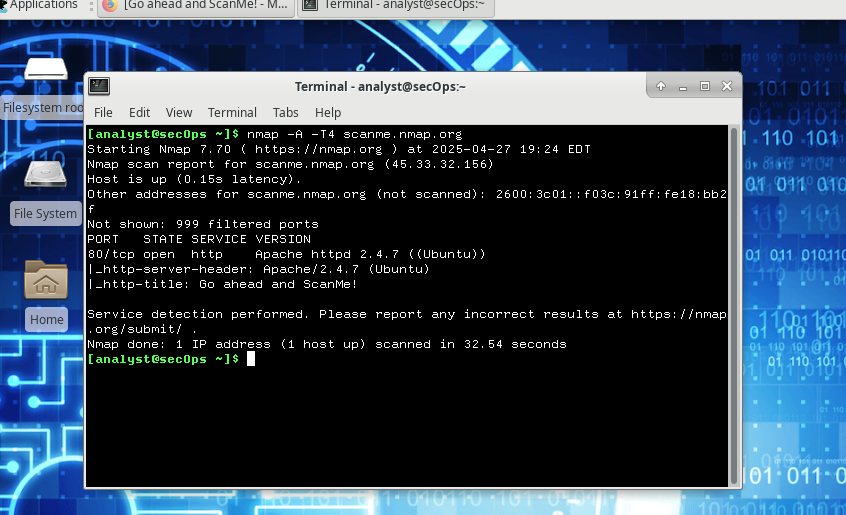
**IP address:** 10.0.2.15

**Services:** FTP (vsftpd 2.0.8 or later), SSH (OpenSSH 7.7)



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

This site allows users to learn about Nmap and test their Nmap installation.



**Which ports and services are opened?**

**Port 80/tcp** is open, running **HTTP.**

**Which ports and services are filtered?**

**999 ports** are **filtered**

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

The IP address of the server is **45.33.32.156.**

**What is the operating system?**

The server is running **Ubuntu**

**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?**

Nmap can be used to scan an internal network for specific open ports to identify the extent of a security breach. It can also be used to inventory a network to ensure that all the systems are probably patched against security concerns. On the other hand, nmap can be used for reconnaissance to determine open ports and other information about the network.