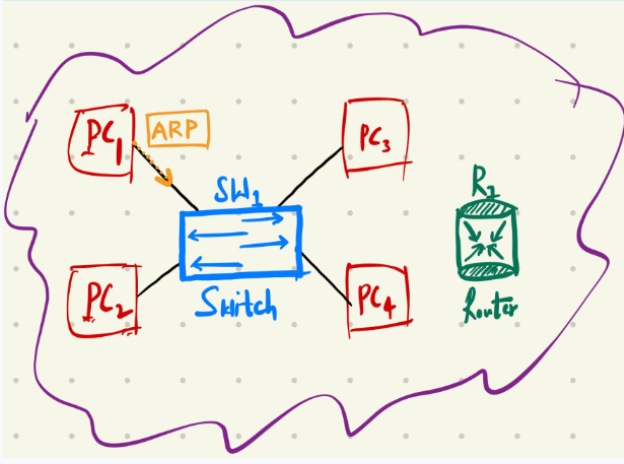
**ID:12214731 DIYORA BOBOKULOVA**

**MIDTERM   
[Q1].** Observe the topology below, where the PC1 is trying to send an ARP request.

**RUBRICS:**The rubrics criterion for the following question is practical knowledge and analytical skill **[15 marks]**



Explain the following aspects **thoroughly with relevant examples**:

    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 would place my attacker device (PC3) directly connected to the Switch SW1. It would allow me to observe and manipulate all traffic passing through the switch, particularly between PC1 and R1. Also, it would allow me to be invisible bridge between devices by replacing my MAC address with the R1’s MAC address.

**Target Devices:**

* **PC1**: The initiator of the ARP request.
* **Router R1**: The gateway.

**Visual representation**:

PC1 <--> PC3 (Attacker) <--> R1

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, it is broadcast across the network by Switch SW1. Thus, **every device** connected to SW1 (PC2, PC3, PC4, Router R1) receives the ARP request.

**As the Man-in-the-Middle attacker operating from PC3, my role is:**

* **Intercept** the ARP request.
* **Respond immediately with a spoofed ARP reply**, making PC1 believe that the Router’s IP is tied to my (PC3’s) MAC address.
* **Also send a spoofed ARP reply to Router R1**, making it think that PC1’s IP is linked to my MAC address.

**Outcome:**

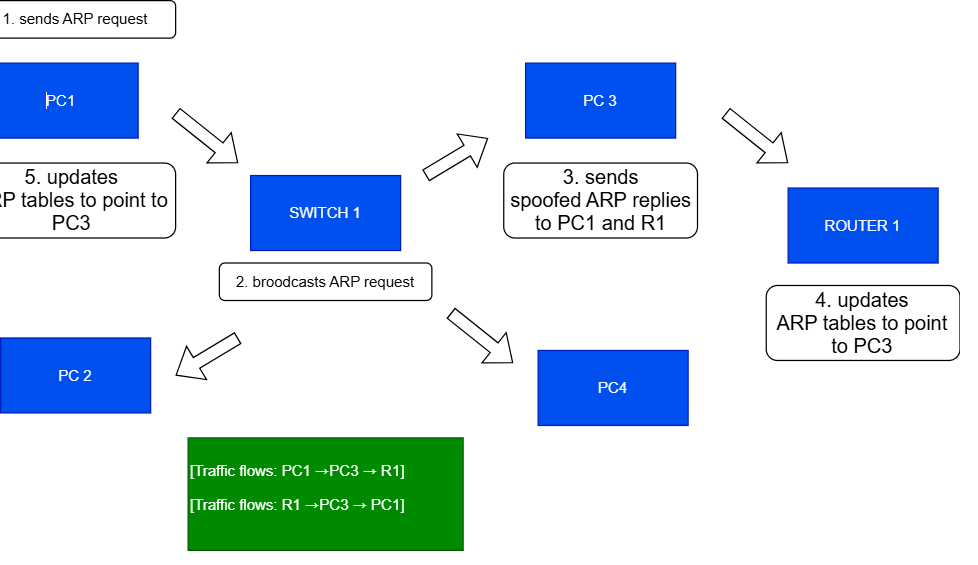
* PC1 thinks it’s talking to the Router, but it's actually sending data to PC3.
* Router R1 thinks it’s replying to PC1, but it's actually sending data to PC3.

Thus, all interactions between PC1 and R1 are captured by the attacker at PC3.

    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?

**Step-by-Step Activity:**

1. **PC3 (attacker) is connected to SW1 and R1**
2. **PC1 sends ARP request** ("Who has the Router's IP?").
3. **SW1 broadcasts the ARP request** to all connected devices.
4. **Attacker PC3 gets to know the MAC address of R1**
5. **Attacker PC3 sends a spoofed ARP reply**:
   * To PC1: "Router's IP is at my MAC add*ress."*
   * To R1: "PC1's IP is at my MAC address."
6. **PC1 and Router R1 update their ARP tables** based on the fake replies.
7. **All traffic from PC1 destined for R1 is now redirected through PC3.**
8. **PC3 captures/sniffs/modifies** the traffic.
9. **Packets are forwarded to maintain network integrity and avoid suspicion.**



**[Q2].** Download the [Practical\_Activity#1](https://drive.google.com/file/d/1pLEyHMeI2i3_r7_Th4tXF9wsb3llZ4Tv/view?usp=share_link) and complete the lab on your VM. Paste the screenshots and responses in the **Word file (YOURSTUDENTID\_CyberOps\_Midterm.docx)**

**RUBRICS:**The rubrics criterion for the following question is conceptual knowledge and practical skill **[10 marks]**

**Part 1: Examine the Header Fields in an Ethernet II Frame**

**Part 2: Use Wireshark to Capture and Analyze Ethernet Frames**

**PART 1.**

**Questions and Answers**

**What is significant about the contents of the destination address field?**The destination address is a broadcast address (ff:ff:ff:ff:ff:ff).  
That’s the Ethernet version of *screaming into the void*: It means the frame is intended for all devices on the local network.

**Why does the PC send out a broadcast ARP prior to sending the first ping request?**Because it doesn’t know the MAC address of the gateway yet!  
Before it can send an IP packet (ping), it needs to know where physically (MAC address) to send it.

**What is the MAC address of the source in the first frame?**The MAC address of the source is: f4:8c:50:62:62:6d  
(That’s the unique "license plate" on your PC’s NIC.)

**What is the Vendor ID (OUI) of the Source’s NIC?**The Vendor ID, aka OUI (Organizationally Unique Identifier), is the first 3 octets:  
f4:8c:50  
This part tells you the manufacturer. In this case, it’s Intel Corporation (because it's labeled IntelCor\_62:62:6d).

**What portion of the MAC address is the OUI?**The first 24 bits (or first 6 hexadecimal digits).  
Like in f4:8c:50:62:62:6d, the f4:8c:50 part is the OUI.

**What is the Source’s NIC serial number?**The NIC's serial number is the last 24 bits (or last 6 hexadecimal digits):  
62:62:6d

**Part 2: Use Wireshark to Capture and Analyze Ethernet Frames**

**What is the IP address of the default gateway for the host H3?** 10.0.0.1

A computer screen shot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.**

**A computer screen shot of a computer screen

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Source MAC address:** d2:a9:6f:00:a6:02 (02:a9:6f:00:a6:02)

**Destination MAC address:** 3e:fc:b7:13:94:28 (3e:fc:b7:13:94:28)

**Frame Type:** 0x0800 (IPv4)

**Source IP**: 10.0.0.13

**Destination IP:** 10.0.0.1

**Examine the new data in the packet list pane of Wireshark.**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Source MAC address:** d2:a9:6f:00:a6:02 (02:a9:6f:00:a6:02)

**Destination MAC address:** 3e:fc:b7:13:94:28 (3e:fc:b7:13:94:28)

**Frame Type:** 0x0800 (IPv4)

**Source IP**: 10.0.0.13

**Destination IP:** 172.16.0.40

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

When Host H3 sends a packet to a remote IP address (such as 172.16.0.40), it does not send the packet directly to that destination. Instead, H3 forwards the packet to its default gateway (router) because the destination IP is outside of H3's local network.

The destination MAC address stays the same (the MAC address of the router) because Ethernet frames are only concerned with delivering packets to the next immediate device on the path — in this case, the router. The router then forwards the packet toward its final destination, adjusting the Ethernet frame as necessary.

Thus, the IP address in the packet reflects the final destination (172.16.0.40), but the MAC address reflects the next hop (the router).

**What does the preamble in an Ethernet frame contain?**

The preamble in an Ethernet frame contains a sequence of bits used for synchronization between sending and receiving devices. Specifically, it consists of 7 bytes of alternating 1s and 0s ("10101010") followed by 1 byte indicating the start of the frame ("10101011").

The preamble allows devices to lock onto the data stream and prepare to properly receive the frame. Wireshark does not display the preamble because it is processed and removed by the network interface card (NIC) before the packet reaches the software level.

**[Q3].** Download the [Practical\_Activity#2](https://drive.google.com/file/d/1mh20tkkXpY2N1wI0iu9cBIrrA14_Qx5d/view?usp=share_link) and complete the lab on your VM. Paste the screenshots and responses in the **Word file (YOURSTUDENTID\_CyberOps\_Midterm.docx)**

**RUBRICS:**The rubrics criterion for the following question is conceptual knowledge and practical skill **[10 marks]**

**Part 1: Exploring Nmap**

**Part 2: Scanning for Open Ports**

**PART 1:**

**Q1. What is Nmap?**Nmap (Network Mapper) is an open-source tool for network exploration and security auditing.

**Q2. What is Nmap used for?**It is used for network discovery, managing service upgrade schedules, monitoring host or service uptime, and security auditing.

**Q3. What is the nmap command used in Example 1?**The command is nmap -v -A scanme.nmap.org.

**Q4. What does the switch -A do?**It enables OS detection, version detection, script scanning, and traceroute.

**Q5. What does the switch -T4 do?**Sets the timing template for faster execution, ideal for networks with low latency.

**Part 2: Scanning for Open Ports**

**Step 1: Scan your localhost.**

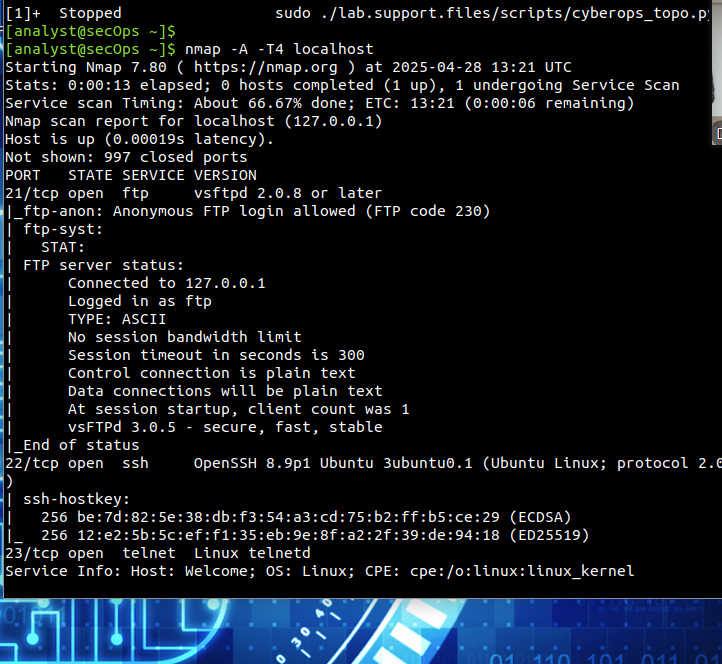
**Which ports and services are opened?**

Port 21/tcp: ftp service is running vsftpd 2.0.8 or later. Anonymous FTP login is allowed.

Port 22/tcp: ssh service is running OpenSSH 8.9p1 Ubuntu 3ubuntu1.1 (Ubuntu Linux; protocol 2.0). The host key fingerprint (ECDSA) is also provided.

Port 23/tcp: telnet service is running Linux telnetd.

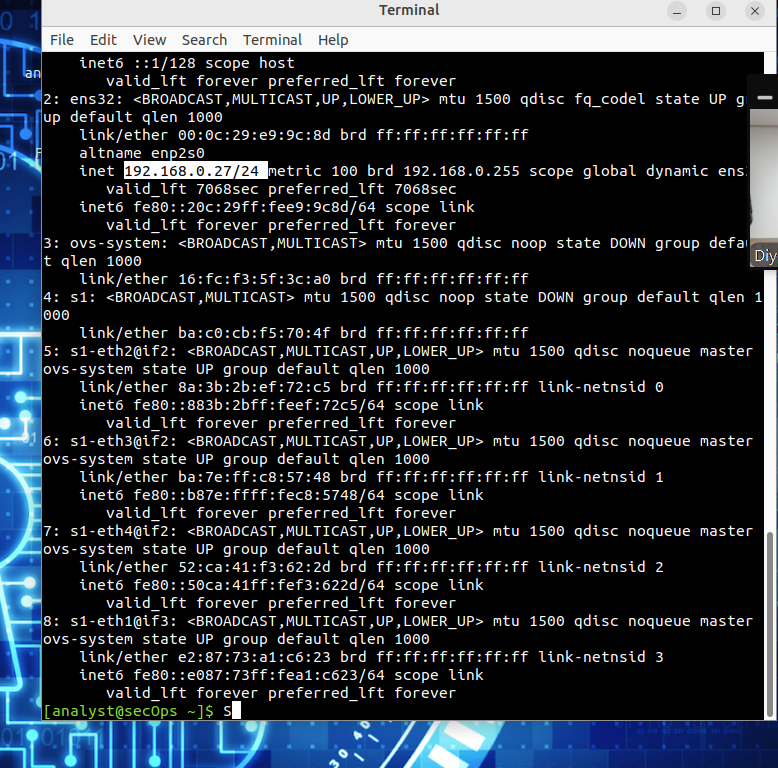
The service info indicates "Welcome; OS: Linux; CPE: cpe:/o:linux:linux\_kernel".

****

**STEP 2. Scan your network**

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

*192.168.0.27/24*

****

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

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

Site is provided by the Nmap developers for safe public Nmap scanning practice.

A computer screen shot of a black screen

AI-generated content may be incorrect.

**Which ports and services are opened?**

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)

1309/tcp open tcpwrapped

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

6881/tcp open bittorrent-tracker?

21/tcp open ftp vsftpd 2.0.8 or later

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)

23/tcp open telnet Linux telnetd

Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

**Which ports and services are filtered?**

There was no filtered services.

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

192.168.0.11

**What is the operating system?**

Linux (with CPE: cpe:/o:linux:linux\_kernel)

**Reflection Question**

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 helps with network security by allowing administrators to identify open ports, detect vulnerabilities, ensure only necessary services are running, and audit network configurations.
  + Threat actors can use Nmap maliciously to discover vulnerable systems, gather information about the network, identify weak points, and plan attacks such as exploiting unpatched services.