# **CyberOps Midterm Answers**

## 1. Observe the Topology - ARP Spoofing Analysis

### (a) Where would you place yourself in the topology to perform ARP Spoofing?

I would place myself as a new device connected to the same switch as PC1, PC2, PC3, and PC4. I need to be in the same broadcast domain to listen and send ARP messages.

### (b) What happens when PC1 sends an ARP request?

PC1 sends an ARP broadcast asking "Who has this IP?" All PCs on the LAN receive it. As an attacker, I intercept the request and send a fake reply to PC1 and PC3, pretending to be each other.

### (c) Complete Activity with Flowchart

Step 1: PC1 sends ARP request.  
Step 2: Attacker intercepts and sends fake ARP replies.  
Step 3: PC1 and PC3 update their ARP tables with attacker's MAC.  
Step 4: Attacker intercepts and forwards traffic between PC1 and PC3.

## 2. Practical Activity #1 - Wireshark Ethernet Frame Analysis

### Part 1: Examining the Header Fields

#### Q1:

It is a broadcast address (ff:ff:ff:ff:ff:ff), meaning the frame is sent to all devices.

#### Q2:

The PC needs to find out the MAC address of the device with a certain IP before it can send packets.

#### Q3:

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

#### Q4:

f4:8c:50

#### Q5:

The first 6 hex digits.

#### Q6:

62:62:6d

### Part 2: Wireshark Capture on VM (I used TryHackMe.com’s online VM)

#### Q1:

Source: 02:ee:e6:6d:6e:59

#### Q2:

Destination: 02:c8:85:b5:5a:aa

#### Q3:

Ethernet II

#### Q4:

10.10.19.110

#### Q5:

8.8.8.8

#### Q6:

Destination MAC: 02:c8:85:b5:5a:aa (back to the PC)

#### Second Ping Test:

Source MAC: 02:ee:e6:6d:6e:59  
Destination MAC: 02:c8:85:b5:5a:aa  
Source IP: 10.10.84.32  
Destination IP: 172.16.0.40

#### Why destination IP changed but MAC stayed the same:

Because all traffic to other networks first goes through the same gateway, so the MAC address stays the same even if IP changes.

#### What does the preamble contain:

Synchronizing bits used by the NIC to detect the start of the frame (not shown in Wireshark).

## 3. Practical Activity #2 - Exploring Nmap

### Part 1: Exploring Nmap

#### What is Nmap?:

A tool to discover hosts and services on a network.

#### What is Nmap used for?:

Network scanning, auditing, and vulnerability finding.

#### What does the -A switch do?:

Enables OS detection, service version detection, and traceroute.

#### What does the -T4 switch do?:

Sets aggressive timing to make the scan faster.

### Part 2: Scanning

Localhost scan results: Open ports: 22 (SSH), 53 (DNS), 80 (HTTP), 81 (HTTP), 111 (RPC), 389 (LDAP), 631 (IPP), 3389 (RDP), 5432 (PostgreSQL), 5901 (VNC), 6001 (X11), 7777 (HTTP), 7778 (unknown).

Network scan results: Active hosts found depending on network (example not provided).

Remote server scan (scanme.nmap.org) results: IP Address: 45.33.32.156, Open ports: None found (all ports filtered), Filtered ports: All 1000 ports scanned, OS: Could not be determined clearly (possibly Linux).

### Reflection

How can Nmap help network security?  
- It finds open ports and running services so that weaknesses can be fixed.

How can threat actors use Nmap?  
- They use it to find targets and vulnerabilities they can attack.