Tutorial 4
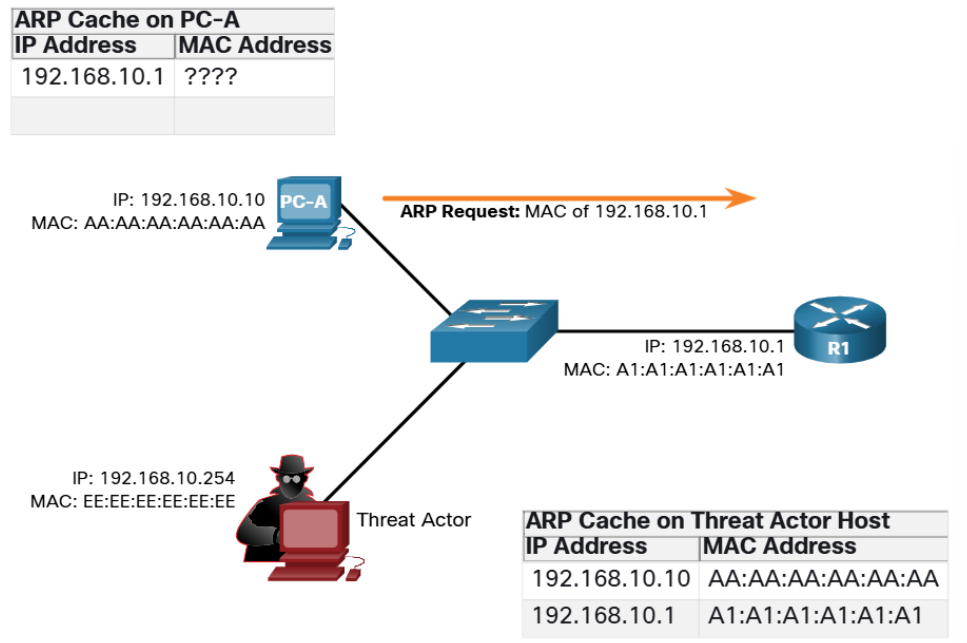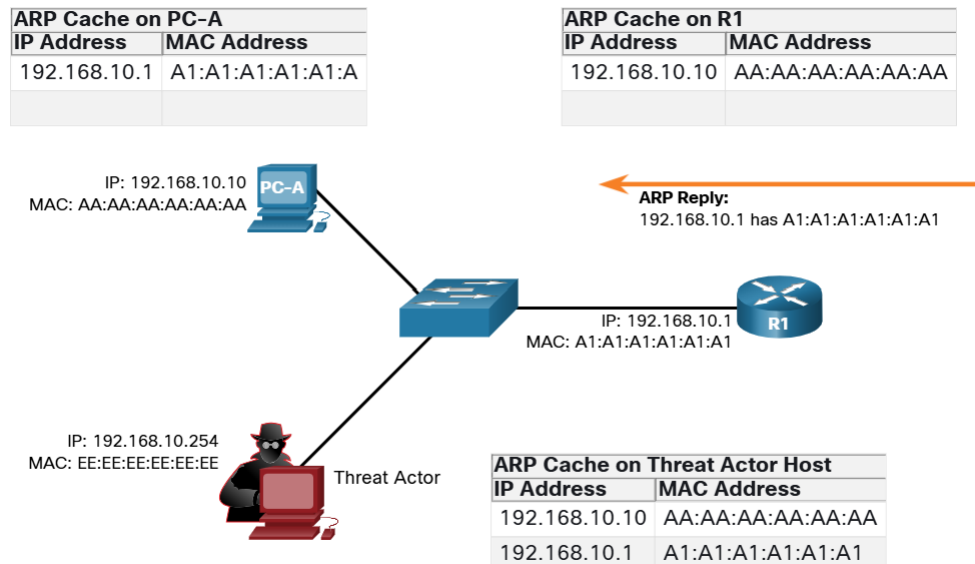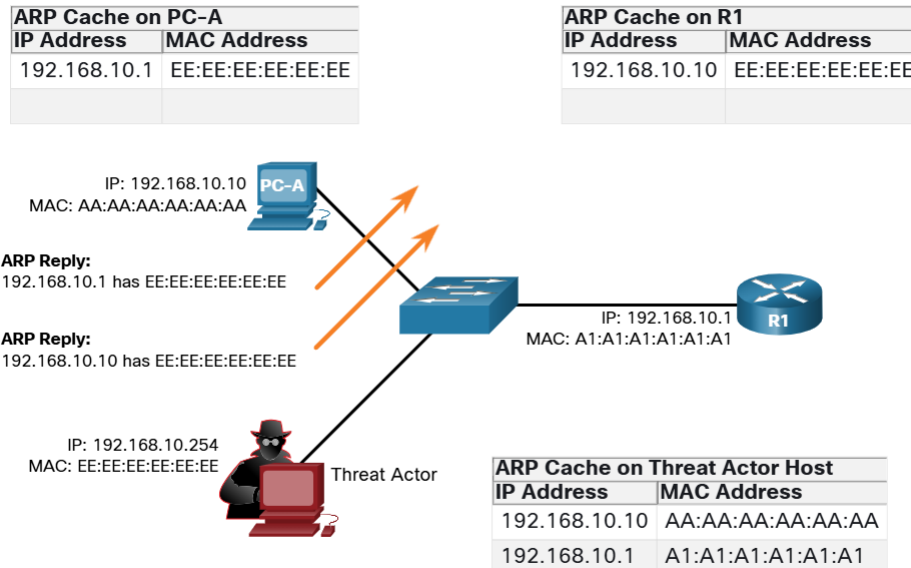
1. Reference to 3.8.2 ARP Cache Poisoning on cisco.netacad.net.

    a) Illustrate ARP request between PC-A and R1 based on the following diagram.

    ARP Cache on PC-A

IP Address	MAC Address
192.168.10.1	????

    IP: 192.168.10.10 **PC-A**
    MAC: AA:AA:AA:AA:AA:AA

    ARP Request: MAC of 192.168.10.1

    IP: 192.168.10.1
    MAC: A1:A1:A1:A1:A1:A1 **R1**

    IP: 192.168.10.254
    MAC: EE:EE:EE:EE:EE:EE   Threat Actor

    ARP Cache on Threat Actor Host

IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

    b) Illustrate ARP reply between PC-A and R1 based on the following diagram.

    ARP Cache on PC-A

IP Address	MAC Address
192.168.10.1	A1:A1:A1:A1:A1:A

    ARP Cache on R1

IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA

    IP: 192.168.10.10 **PC-A**
    MAC: AA:AA:AA:AA:AA:AA

    ARP Reply:
    192.168.10.1 has A1:A1:A1:A1:A1:A1

    IP: 192.168.10.1 **R1**
    MAC: A1:A1:A1:A1:A1:A1

    IP: 192.168.10.254
    MAC: EE:EE:EE:EE:EE:EE   Threat Actor

    ARP Cache on Threat Actor Host

IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

c) Explain in detailed on how ARP Cache Poisoning works based on the following diagram.

ARP Cache on PC-A	
IP Address	MAC Address
192.168.10.1	EE:EE:EE:EE:EE:EE

ARP Cache on R1	
IP Address	MAC Address
192.168.10.10	EE:EE:EE:EE:EE:EE

ARP Cache on Threat Actor Host	
IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

2. Differentiate Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA).

3. Illustrate the techniques used in IP attacks.

4. Explain **THREE (3)** different types of attack to an organization.

5. Differentiate Adware, Spyware and Ransomware.

6. Illustrate Reconnaissance Attacks, Access Attacks and DoS Attacks. In addition, give an example for each type of attack.

7. Most organizations employ a defense-in-depth approach to security. It requires a combination of networking devices and services working together. Illustrate this approach.

8. a) Compare and contrast **TWO (2)** social engineering attacks.   (4 marks)

    b) Which of these two social engineering attacks is more commonly encountered among businesses? Include your reasons to support your answer.   (4 marks)

9.   Network applications use TCP or UDP ports. Threat actors conduct port scans of targeted devices to discover the services they offer.
    a) Illustrate TCP SYN Flood attack.

    b) Explain UDP Flood attack.