Analyzing packet captures using Wireshark

**Objective 1**

Analyze the following packet capture and answer these questions

Capture file to this objective: e**xample.pcap**

1. In this capture there is an ARP request for IP address 192.168.1.221. What is the mac address and the IP address of the requestor? MAC: 20:c0:47:c2:69:24 IP: 192.168.1.1
2. What is the mac address and IP address of the first device to respond? MAC: f8:4d:89:60:87:57 IP: 192.168.1.242
3. How may devices respond to this ARP request? 3
4. What protocol was used to transfer data to host 192.168.1.121? What is the secure version of this protocol? IPV4, IPV6
5. What was the username and password used for login for this data transfer?

Username: pikachu

Password: INeverLikedPokemon

**Objective 2**

Analyze the following packet capture and answer these questions

Capture file: **network\_attack.pcap**

Attack 1: ARP Attacks

1. Review the packets in the capture file and explain what is taking place in each of the three packets.

A device is asking for the owner of the other IP address. 00:50 is the true MAC address for this IP address. A malicious device says they’re the new owner of that IP address.

1. What type of attack is this?

ARP poisoning

1. What is the MAC address of the good device?

00:50:56:f9:f5:54

1. What is the MAC address of the hacker's device?

00:0c:29:1d:b3:b1

1. What negative impact might this type of attack have?

This can be used to perform a man in the middle attack, where all date can be sent to the hacking device

Attack Two: DHCP Attacks

Analyze the following packet capture and answer these questions

Capture file: **network\_attack.pcap**.

1. Review the packets captured and explain in simple terms what is taking place. The attacker sent a bunch of forged DHCP messages with a spoofed MAC address, the DHCP server then tries to respond to these messages and as a result the pool of IP addresses used by the DHCP server are eliminated.
2. What type of attack is this?

DHCP starvation

1. Why is the destination IP `255.255.255.255` for all packets?

The DHCP packet is being broadcast on the entire network.

1. What negative impact might this type of attack have?

A DHCP starvation attack can result in a DoS attack or MITM attack.

Attack Three: TCP Attacks

Analyze the following packet capture and answer these questions

Capture file: **network\_attack.pcap**.

1. Review the packets captured and explain in simple terms what is taking place.

Someone is running a syn scan on this network checking for open ports.

1. What type of attack is this?

Syn scan

1. Is this type of activity always an attack? In other words, can a security professional benefit from what is taking place?

It’s not always an attack, you can also check for open ports using this scan.

1. What negative impact might this type of attack have?

A hacker could attack an open port and perform a syn flood.

Bonus Objective

Analyze the following packet capture and answer the questions

Files needed for this objective: **encrypted\_dump.pcap, premaster.txt**

**HINT:** You will need the premaster.txt file to help answer these questions

Find the encrypted session that uses the below master key

Master-Key: D5230B2F78928A2DA043853E9D63C9E75110BF367CCA4A4732332B6C33ED40AC1DFF2EF3E4CD121A904D537D49D688D4

1. What is the packet / frame number where you found the master-key?
2. What was the Cipher used for this encrypted session?
3. What was the common Cipher between these endpoints?
4. Can you explain why the session cipher and the common are the same?