Wireshark Exercise

1. Overview

The learning objective of this lab is for you to gain first-hand experience on some of the networking protocols we discussed in class and analyzing packets. Here you can see different types of attacks in the traffic captured from the network. The questions will guide you through the attacks, You need to look at the header information and sometimes the data part of the packet to figure out the answers.

Lab environment: You can download and install Wireshark on your personal computer. `https://www.wireshark.org/`. Wireshark is also installed on the pre-built Ubuntu VM that has been provided for this class. Open Wireshark, then click on File > Open and open the files provided with this assignment.

Submission: Open the files assigned for each task using Wireshark and analyze the packets. Answer the following questions. Only submit typed reports electronically. No handwritten reports accepted.

Guide:

- You can Filter DHCP packets by typing 'bootp' in the filter field.
- Similarly filter any other protocl such as, tcp, http, dns, etc.
- You can search for any MAC address, for example if you are looking for MAC address 08:00:27:8F:4C:61 you can use 'eth.addr == 08:00:27:8F:4C:61' as your filter.
- Similarly search for an IP address using ip.addr
- 255.255.255.255 is the broadcast IP address for the local network.

2. Tasks

Part A: [36 points + 10 extra] p1.pcap

Open the p1.pcap file in Wireshark and answer the following questions by analyzing the packets.

1. [2 point] What is the IP address of the DHCP server assigning IP addresses?
2. [6 points] What are the assigned IP addresses for devices with these MACs?
   (a) 08:00:27:8F:4C:61
   (b) 08:00:27:76:1F:7C
   (c) 08:00:27:0C:66:53
3. [2 point] Did all of the above devices receive their IP address from the DHCP protocol? If not, which devices were not assigned their IP address by this protocol (identify by IP address)?
4. [8 points] A series of SYN packets are sent to a destination between frames 120 and 2121, and again between frames 2241 and 4250.
   (a) What is the purpose of these SYN packets?
   (b) What new information about the destination was obtained by the SYN packets between frames 120 and 2121?
   (c) What new information about the destination was obtained by the SYN packets between frames 2241 and 4250?

(d) What type of packet was returned to the source from the destination to indicate these new information? Explain.

5. [4 points] Between frames 4365 and 4368 a device utilizes the ARP protocol (Request/Reply)
   (a) What is the purpose of the ARP protocol?
   (b) Which device is collecting this information (IP and MAC)?
6. [8 points] Between frames 4371 and 4382 a device floods the LAN with ARP replies
   (a) Is this valid without an ARP request? Why?
   (b) What is suspicious about these ARP replies?
   (c) Which client (IP and MAC) are these ARP replies affecting and what is the purpose behind these ARP replies?
   (d) Who is the attacker in this scenario? (Identify with IP and MAC)?
7. [6 points] One of the clients downloaded a document from the server using HTTP
   (a) Was the attacker able to successfully intercept the entire document? Explain what is happening in this case.
   (b) What is the document media type?
   (c) Does the victim have any indication this file was intercepted?
8. [10 extra points] Try retrieving the actual file being downloaded by the client, and explain the steps you took in details. Answer the following questions in regard to the document downloaded. The answers to this question will not be graded if you do not describe your approach for retrieving the file in details. We have not learned how to do this in class, this is an extra credit activity for you to try to figure out on your own.
   (a) What is the month and year the document was published (shown in first page)?
   (b) What is the title of the page on page 25?

Part B: [20 points] p2.pcap

Answer the following questions using p2.pcap. This is a packet capture (from the attacker's machine) of a targeted, man in the middle attack using sslstrip to steal a username and password. This means that the attacker and the victim are both on the same network. The first three numbers of the IP address identifies the network, so in this case, both Victim and attacker's IP addresses start with the same numbers. The victim is trying to send packets to an address outside of this network through the gateway. The gateway's IP address also starts with the same numbers as the victim and attacker (since they are all in the same network).

1. [8 points] The arp spoof activity begins at packet #3:
   (a) Who is the attacker (What is his MAC address?)
   (b) Who is the attacker trying to impersonate (What IP address)?
   (c) Who is the victim IP? Hint: See the target IP address in the spoofed arp packets.
   (d) What is the attacker's ACTUAL IP? This can be found given the MAC address. Do not confuse it for the IP that the attacker is trying to impersonate!
2. [4 points] The victim begins browsing the web at packet 11. Packets 11 through 168 represent the traffic generated by google's instant search mechanism (i.e. results updated per keystroke). Packet 162 was his final query in this search, as he had finished typing the query string. What was his search string that he submitted to Google? Provide the search string, and explain which frame number you looked at. (Hint: it comes after q=)
3. [8 points] After Google.com, the victim next visits a website that enforces Strict Transport Security (TLS).

(a) There is a lot of advertising traffic in the packet capture. What is the second website the victim visits (domain name will suffice)? Hint: it's easiest to first search for SSL traffic handshake messages and then look around these frames for the http get request. Use the following filter: (ssl.handshake.type == 2)

(b) A HTTPS session is established in packets 1303 - 1322. Is this SSL handshake between the victim and the website; or between the attacker and the website?

(c) Packet 3284 is a plaintext HTTP POST request generated by the victim pressing the login button on the website form. What is the victim's username and password?