CSCI180 Lab5 Report

Xiaoming Huang

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

1. **What is the IP address of the DHCP server assigning IP addresses?**
   192.168.56.1

2. What are the assigned IP addresses for devices with these MACs?
   (a) 08:00:27:8F:4C:61 —>192.168.56.9
   (b) 08:00:27:76:1F:7C —> 192.168.56.2
   (c) 08:00:27:0C:66:53 —> 192.168.56.3

3. **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)?**
   The second and the third received their IP addresses from DHCP protocol, as they have the DHCP request, while only the first does not.

4. **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?
   The attacker is sending these SYN packets with different destination port numbers, using brute-force to find out which one the destination Port is.

   (b) What new information about the destination was obtained by the SYN packets between frames 120 and 2121?
   Between frame 120 and 2121, the source IP is 192.168.56.9 and the destination IP is 192.168.56.2, so these frames are trying to get the port number of the receiver side, and the attack at the end successfully get the right destination port, which is 22, and build up the TCP connection with 192.168.56.2. And all the unsuccessful ones are the closed ports.

(c) What new information about the destination was obtained by the SYN packets between frames 2241 and 4250?

Similarly, between 2241 and 4250, attackers attempted to get the destination port number of 192.168.56.3, which is 22, and successfully built up a TCP connection at the end. And all the unsuccessful ones are the closed ports.

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

A SYN-ACK packet was sent to build the TCP connection. If the port is open and listening, the receiver will send this packet to go on the three-way handshake process. Then the attacker can build up the connection.

5. **Between frames 4365 and 4368 a device utilizes the ARP protocol (Request/Reply)**

(a) What is the purpose of the ARP protocol?

The purpose of ARP is to translate the IP address to a MAC address. When delivering the packet, the router broadcasts the IP address of the destination, the machine with this IP replies back. And the IP-MAC match will be stored locally in the ARP cache table.

(b) Which device is collecting this information (IP and MAC)?

08:00:27:8F:4C:61 —> 192.168.56.9

6. **Between frames 4371 and 4382 a device floods the LAN with ARP replies**

4371	215.574989	PCSSystemtec_8f:4c:61	PCSSystemtec_76:1f:7c	ARP	42	192.168.56.3 is at 08:00:27:8f:4c:61
4372	215.575050	PCSSystemtec_8f:4c:61	PCSSystemtec_0c:66:53	ARP	42	192.168.56.2 is at 08:00:27:8f:4c:61
4373	217.576232	PCSSystemtec_8f:4c:61	PCSSystemtec_76:1f:7c	ARP	42	192.168.56.3 is at 08:00:27:8f:4c:61
4374	217.576461	PCSSystemtec_8f:4c:61	PCSSystemtec_0c:66:53	ARP	42	192.168.56.2 is at 08:00:27:8f:4c:61
4375	219.576935	PCSSystemtec_8f:4c:61	PCSSystemtec_76:1f:7c	ARP	42	192.168.56.3 is at 08:00:27:8f:4c:61
4376	219.577178	PCSSystemtec_8f:4c:61	PCSSystemtec_0c:66:53	ARP	42	192.168.56.2 is at 08:00:27:8f:4c:61
4377	221.577692	PCSSystemtec_8f:4c:61	PCSSystemtec_76:1f:7c	ARP	42	192.168.56.3 is at 08:00:27:8f:4c:61
4378	221.577938	PCSSystemtec_8f:4c:61	PCSSystemtec_0c:66:53	ARP	42	192.168.56.2 is at 08:00:27:8f:4c:61
4379	223.578978	PCSSystemtec_8f:4c:61	PCSSystemtec_76:1f:7c	ARP	42	192.168.56.3 is at 08:00:27:8f:4c:61
4380	223.579205	PCSSystemtec_8f:4c:61	PCSSystemtec_0c:66:53	ARP	42	192.168.56.2 is at 08:00:27:8f:4c:61
4381	233.579535	PCSSystemtec_8f:4c:61	PCSSystemtec_76:1f:7c	ARP	42	192.168.56.3 is at 08:00:27:8f:4c:61
4382	233.579775	PCSSystemtec_8f:4c:61	PCSSystemtec_0c:66:53	ARP	42	192.168.56.2 is at 08:00:27:8f:4c:61

(a) Is this valid without an ARP request? Why?

No. We only know the IP, and if we want to flood the LAN, we would need to have the MAC IP of the device after ARP replies.

(b) What is suspicious about these ARP replies?

They are assigning 192.168.56.3 and 192.168.56.2 to the attacker's MAC address. And telling each other of this new relationship. What 192.168.56.9 did is that:
It tells "192.168.56.2" that, "192.168.56.3" is at MAC address "08:00:27:8F:4C:61"; and also tells "192.168.56.3" that "192.168.56.2" is at MAC address "08:00:27:8F:4C:61", whereas this MAC address is actually the attacker's.

This performs IP spoofing.

(c) Which client (IP and MAC) are these ARP replies affecting and what is the purpose behind these ARP replies?

Both of the following two are affected:

08:00:27:76:1F:7C —> 192.168.56.2

08:00:27:0C:66:53 —> 192.168.56.3

And the purpose of these is to do the ARP spoofing, and DoS attack on these two victims.

(d) Who is the attacker in this scenario? (Identify with IP and MAC)?

08:00:27:8F:4C:61 —> 192.168.56.9

7. **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.

Yes, http doesn't encrypt, so the attacker would be able to access the document.
At this point, the attacker would be able to pretend to be the sender and perform an MITM attack.

(b) What is the document media type?

PDF

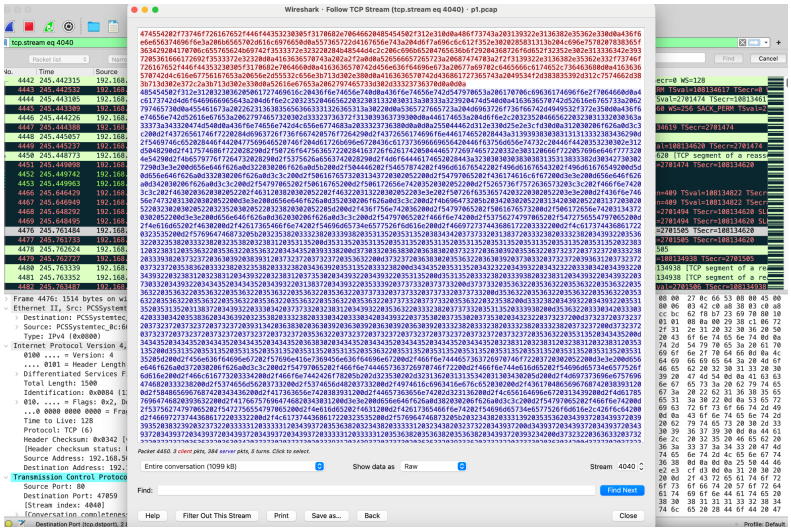
(c) Does the victim have any indication this file was intercepted?

No, since Man-in-the-middle attack makes the victim thought they actually receive from each other. And they won't be able to realize that they are tricked.

8. **Try retrieving the actual file being downloaded by the client, and explain the steps you took in detail. 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.**

Approach: I first search on HTTP, and there are several coming up, some are just HTTP requests and I work on those successful ones.

Then I went to the Follow/TCP Stream, and changed the data type to raw, and downloaded as pdf.



(a) What is the month and year the document was published (shown in first page)?

April 28, 1997

(b) What is the title of the page on page 25?

Atomic Energy Information

Part B: [20 points] p2.pcap

1. **The arp spoof activity begins at packet #3:**

   (a) Who is the attacker (What is his MAC address?)

   08:00:27:21:05:17

   (b) Who is the attacker trying to impersonate (What IP address)?

   192.168.1.1

   (c) Who is the victim IP? Hint: See the target IP address in the spoofed arp packets.

   192.168.1.247

   (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!

   Actual IP: 74.125.134.113

2. **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=)**

   Search string is "weather 32303".

   I looked at frame 162, and the packet data is "/search?hl=en&client=ubuntu&hs=Zgi&channel=fs&q=weather+32303&oq=weather+32303&gs_l=serp.3..0l2j0i30l2j0i5i30l3j0i8j0i8i30l2.44912.47718.0.48648.15.9.1.5.5.0.118.808.7j2.9.0.es%3B..0.0...1c.1.4.serp.hEw2INguST0".

3. **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)

   http://paypal.com

This is shown in the last HTTP frame before the first TLSv1 frame.

(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?

Still between the attacker and the victim. As the Destination MAC address is still 08:00:27:21:05:17

(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?

login_email =TARGETUSER

Login_password = ILOVETHEINTERNET