Derrick Lee
Lab 4
CSCI 180
November 18, 2019

1 Part A: p1.pcap

1.1

The IP address of the network assigning IP addresses via DHCP is 192.168.56.1

1.2

```
08:00:27:8F:4C:61 192.168.56.9
08:00:27:76:1F:7C 192.168.56.2
08:00:27:0C:66:53 192.168.56.3
```

1.3

No, 192.168.56.9 (108:00:27:8F:4C:61) did not receive their IP address from DHCP. 192.168.56.2 and 192.168.56.3 had IP's assigned via DHCP as they sent DHCP requests from 0.0.0.0 to the broadcast address

1.4

a) These SYN packets were sent to seemingly random ports. This could be to check the target for ports that are open and listening for new connections.

b) Between frames 120 and 2121, port 22 (used for SSH) responded with a SYN, ACK. This gave information that the server is listening on port 22.

c) New information given between frames 2241 and 4250 is that port 80 (used for HTTP) is also open.

d) The packet that was returned was a SYN-ACK, which tells the client that the server is listening on the port and is accepting connections, attempting to process a TCP three way handshake. Other ports do not respond with a SYN-ACK as they are not accepting connections and closed to external machines.

1.5

a) ARP is used to translate IP addresses to MAC addresses.

b) 08:00:27:8F:4C:61 (192.168.56.9) is asking for the MAC address of 192.168.56.2 and 192.168.56.3. 08:00:27:76:1F:7C (192.168.56.2) and 08:00:27:0C:66:53 (192.168.56.3) respond with their corresponding MAC addresses.

1.6

a) ARP replies are valid without a request as a machine may need to notify others when their IP changes.

b) These ARP replies are suspicious as they are not just assigning different IP addresses to their MAC address, but also that the IP addresses being assigned are already being used by other machines.

c) 192.168.56.3 (08:00:27:0C:66:53) and 192.168.56.2 (08:00:27:76:1F:7C) are affected as their IP addresses are being redirected to point to the ARP broadcaster's MAC address 08:00:27:8F:4C:61. These replies are being sent to these two affected machines so that IP to MAC translations between the two point to the attacker instead of one another.

1.7

a) The attacker was successful in executing a MITM attack.

The corresponding machine MAC addresses (last octet) are listed for each IP address (last two octets):

```
56.2 => 7C (real/client)
     => 61 (attacker)
56.3 => 53 (real/server)
     => 61 (attacker)
56.9 => 61 (real/attacker)
```

Attacker machine is shown in bold.

1) 56.2 (7C) tries to download a file from 56.3 (53).
2) 56.2 (7C) -HTTP GET-> 56.3 (**61**) -TCP-> 56.3 (53) (forwarded GET request)
3) 56.3 (53) -TCP-> 56.2 (**61**) -TCP-> 56.2 (7C) (forwarded GET response)

The attacker intercepts connections between the victim 56.2 (7C) and the server 56.3 (53), acting as a proxy in between the two to both pass along request data and view (or potentially modify) the content.

b) Document media type is listed in the HTTP response Content-Type header as application /pdf.

c) Since the document was forwarded to the victim, they would have been able to receive the requested pdf file as expected and thus possibly not notice that it was intercepted.

1.8

One method to retrieve the file being downloaded is to export the 2 pdf files via File > Export Objects > HTTP. These files can't be opened individually since it's a single pdf split into two parts, so they are combined with the following command with cat:

```
cat DoD5200_1ph\(1\).pdf DoD5200_1ph\(2\).pdf > DoD5200_1ph.pdf
```

An alternative method is to reconstruct the file from the packet responses directly with the required data in packets 4576 and 7860. Then select the packet responses and exporting the bytes (reassembled TCP) directly via Wireshark or copy it as a hex stream and convert it to a binary file with the following command:

```
xxd -r -p input_file output_file
```

After this, we have two binary files that can be combined with the cat command same as above.

a) This document was published April 1997.

b) The authority that issued this document is the DoD Directive 5200.1, "Information Security Program," December 13, 1996

c) Page 25's title is "Atomic Energy Information"

2 Part B: p2.pcap

2.1

a) Attacker's MAC address is 08:00:27:21:05:17.

b) Attacker's real IP address is 192.168.1.38.

c) Attacker is trying to impersonate 192.168.1.1 which is usually the router.

d) The victim's IP is 192.168.1.247 as the ARP packets are being sent to this machine.

2.2

The user searched "weather 32303" in Google. In packet 162, the search query (q=weather+32303 , where space is encoded as a +) is shown in the HTTP request where the search query is provided in a url parameter in the GET request.

The full GET request URI is the following:

```
/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.les%3B..0.0...1c
    .1.4.serp.hEw2INguST0
```

2.3

a) The victim next visits www.paypal.com

b) The TLS response is sent to the attacker's machine (08:00:27:21:05:17) so the handshake is between the website and the attacker.

c) The victim's username is TARGETUSER and their password is ILOVETHEINTERNET. This was found in the HTTP POST application/x-www-form-urlencoded form data.