Lab 5 - Networking

Frankie Fazlollahi

Tasks:

Part A: p1.pcap

1. The IP address of the network adapter assigning IP addresses is: 192.168.56.1.
2. The assigned IP addresses for the adapters with these MACs are:
    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. 192.168.56.9 did not receive its IP address from the DHCP protocol.
4. A series of SYN packets are sent to a destination between frames 120 and 2121, and again between frames 2241 and 4250.
    a. The purpose of these SYN packets is to determine if the target is open and listening as well as revealing the presence of security devices between the sender and the target.
    b. From the SYN packets sent between frames 120 and 2121 we saw that port 86 is of the target (192.168.56.2) is running and has some kind of security device, such as a firewall, because the only response the sender got from the target was from port 86 saying “Destination Unreachable (Host administratively prohibited).”

c. From the SYN packets sent between frames 2241 and 4250 we saw that port 80 of the target (192.168.56.3) is open and listening as shown by it sending several [SYN, ACK] packets back to the sender.

d. The destination (192.168.56.2) sent a Destination Unreachable (Host administratively prohibited) packet to the source from port 86 which shows that port 86 is running but has some kind of security device. The destination (192.168.56.3) sent a [SYN, ACK] packet to the source from port 80 which shows that port 80 is open and listening.

5. Between frames 4365 and 4368 an adapter utilizes the ARP protocol (Request/Reply)
    a. The purpose of the ARP protocol is to find the MAC address of the device with the IP address we ask for.
    b. The adapter with IP address: 192.168.56.9 and MAC address: 08:00:27:8F:4C:61 is collecting this information.
6. Between frames 4371 and 4382 an adapter floods the LAN with ARP replies
    a. This is valid because the ARP cache updates everytime it receives a reply, even if it did not send any ARP request.
    b. All of the ARP replies say that each of the IP addresses have the same one MAC address of 08:00:27:8F:4C:61.
    c. These ARP replies are affecting adapters with IP addresses and MAC addresses 192.168.56.2, 08:00:27:76:1F:7C and 192.168.56.3, 08:00:27:0C:66:53. These ARP replies are poisoning the ARP cache by updating these IP addresses to have the incorrect MAC address of 08:00:27:8F:4C:61.

7. One of the clients downloaded a document from the server using HTTP
    a. The attacker is in the middle of the victim and the server that the victim is trying to download from. So each time the victim sends a request it goes to the attacker, then the attacker sends it to the server. Also, when the server tries to send the document, it goes to the attacker, then the attacker sends it to the victim.
    b. The document media type is a pdf.
    c. The only possible indication that the victim had that this file was intercepted was that there was a retransmission.

Part B: p2.pcap

1. The arp spoof activity begins at packet #3.
    a. The attacker's MAC address is 08:00:27:21:05:17.
    b. The attacker's actual IP address is 74.125.134.113.
    c. The attacker is trying to impersonate 192.168.1.1.
    d. The victim's IP is 192.168.1.247.
2. The search string he submitted to Google was "weather 32303". I found this by going to packet 162 (the packet of the final query) and expanded the Hypertext Transfer Protocol. Under that, I found the Full Request URI, which was "http://www.google.com/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". In this I saw that he entered "weather+32303" which meant that his search string was "weather 32303" since the "+" indicates a space.

3. After Google.com, the victim next visits a website that enforces Strict Transport Security.
    a. The second website the victim visits is http://www.paypal.com/
    b. This SSL handshake is between the attacker and the website.
    c. The victim's username is "TARGETUSER" and their password is "ILOVETHEINTERNET".