Bennett Hall

Professor Anthony Duhaime Candeias

CISC 6680

February 1st, 2021

Lab 1: Packet Capture Analysis

****Please note that the answers to each question are in bold beneath the question****

PCAP 1: HTTP

1) What is the Web Architecture used in this server?

   Cloudflare-nginx

2) What is the title of the HTML page that was visited?

   www.wireshark.org:8080

3) Which HTTP method was used to retrieve the page?

   GET/ HTTP/1.1

4) Which number frame sent the HTTP GET Request?

   4

5) Which number frame returned a response for the HTTP Request?

   24

PCAP 2: Telnet

6) What is the login username?

   fake

7) What is the password?

user

8) What Warning was issued?

No Kerberos tickets issued.

9) What OS is the server?

OpenBSD 2.6-beta (OOF)

10) When was the last telnet login?

Thursday December 2, 21:32:59

11) Which number frame did the telnet traffic begin?

4

<u>PCAP 3: MISC</u>

12) What is the DNS server being used in this network conversation (IP Address)?

150.108.4.11

13) What IP Address did star.c10r.facebook.com resolve to?

31.13.74.1

14) Which DNS request had the most answers (Domain Name)?

msocsp.com

15) What is the total number of DNS queries?

4

<u>Short Answers</u>

16) In 1-2 Paragraphs explain what occurred in PCAP 1.

This packet capture is about the client communicating with the server via http. Http is a TCP protocol and it's found on layer 7 of the OSI model, the application layer. Http gives us the ability to view the content on a website. This PCAP is showing us how the http content is accessed via the exchange of data frames. This PCAP has a total of 28 frames. Frame number 4 contains the GET/ HTTP/ 1.1 which is the frame that sends the request. Frame number 24 returned the response. If we use the "follow stream" tool we will be able to see more information including the web architecture used in this service (Cloudflare-nginx) and what HTML page was visited (www.wireshark.org:8080) among other tidbits of information.

17) In 1-2 Paragraphs explain what occurred in PCAP 2.
This packet capture is about telnet which is the protocol that the client used to communicate with the server. Telnet is a TCP protocol that allows virtual access to a computer and also allows for communication or the exchange of data. Telnet operates at level 7 of the OSI model, the application layer. Telnet is not a protocol that should not be used because it uses plaintext, meaning it's not secure. There are a total of 272 frames in this PCAP. If you utilize the "follow stream" tool you will easily be able to view the login ID (fake) and the password (user). Frame number 4 is where the telnet traffic begins. Using the "follow stream" tool we can also access other information about the operating system, the last time that there was a telnet login, and a warning message. We can also see that yahoo.com was a part of the communication if we use the "follow stream tool."

18) In 1-2 Paragraphs explain what occurred in PCAP 3.
This packet PCAP has a total of 1,644 frames of data. There are a mix of protocols that were used to communicate between the client and the server. They include ARP, DNS, ICMP, DHCP, OCSP, HTTP, and TLS (among others). These various protocols do not all use TCP. In fact DNS and DHCP use UDP. ICMP has no ports and does not use TCP or UDP. DNS resolves domain names to IP addresses, allowing us the ability to put in the name of a website instead of having to use it's IP address to visit the intended destination. We can see the DNS frames highlighted in light blue. Using the "DNS Activity" tool we learn that there are four DNS queries and we can learn which DNS request had the most answers (msocsp.com). If we look at the DNS frames we can see the information that's exchanged as the DNS server resolves the domain name to the appropriate IP address. With the DNS filter we can see that Facebook was resolved to an IP address. Using a DNS filter we can see the IP address of the DNS server.