Bennett Hall

Professor Anthony Duhaime Candeias

CISC 6680

February 24th, 2021

Lab 2: Network and Web Recon Analysis

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

PCAP

1) What packet number was the HTTP method of OPTIONS used?

   2067

2) What is the total number of frames sent in this PCAP?

   2224

3) Besides MySQL what other Database protocol was scanned for?

   pgSQL

4) What service or protocol was scanned for in packet 1169?

   Potential VNC Scan 5900-5920

PCAP 2

5) What file was accessed in packet number 4705?

   robots.txt

6) What host(domain name) was accessed in packet number 4705?

   scanme.nmap.org

7) What was the user agent string used in packet number 4705?

Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)

8) What packet number was mysql scanned (3306)?

15

PCAP 3

9) What is the user agent string used in this PCAP?

Mozilla/4.75 (Nikto/2.1.4) (Evasions:None) (Test:map_codes)

10) What is the hostname of the site being scanned?

www.sec542.org

11) Why does this packet capture have so many 404 errors?

This packet capture has errors because the user input, specifically the input for the file extension, was not not correct. The client was unable to access the desired file because they plugged in a file extension that did not match the extension of the desired file. Multiple attempts were made to access the file, hence the return of so many error messages.

12) Which filter did you use to just show the 404 errors?

http contains 404

13) Which base directory had the most requests?

ZJ2qzIGY

Short Answers

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

This packet capture shows a client running an Nmap service and version detection scan of their own system. We can see that the source IP address and destination IP addresses is 127.0.0.1. This is the loopback IP address. Several different TCP and UDP protocols, as well as other services, were used including http, DNS, TLS, and a VNC scan. We see that the client was attempting to access a couple of databases including MySQL and pgSQL. If we refer to the info section we can see the successful connection established by the scan as noted by the SYN > SYN/ ACK > ACK. We can also see where a connection was not established with the packets that responded to the communication requests with an RST. There were a total of 2,224 packets in this packet capture.

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

In this packet capture we see a client running an Nmap port scan of their local host network. You will see that the source and destination IP addresses match and the addresses are in fact private IP addresses. Nmap is used to scan for open ports and also gain insight into a network. The first few packets were exchanged with IPv4 addresses. We can also see that much of the communication was also done using IPv6 addresses, which are noticeably longer than the IPv4 address. The IPv6 addresses were triggered by the ICMP protocol. We can also see that the client scanned mySQL and attempted to access a text file (robots). Various different protocols were used, including DNS, Http, ICMPv6 among others. The communication resulted in a lot of RST responses to the SYN requests. There were a total of 5,164 packets in this packet capture.

16) In 1-2 Paragraphs explain what occurred in PCAP 3.

This packet capture is showing us a Nikto scan. A Nikto scan looks for vulnerabilities in a system by scanning servers and files among other things. In this packet capture the client is using multicasting to send a packet to multiple destination computers as seen by the destination in the first packet with a 224 IPv4 address prefix. The client is also communicating within their local network as we can see by the loopback IP address 127.0.0.1. There are a lot of error messages in this packet capture because the client was trying to access a file, but put in the wrong file extension. The communication resulted in a lot of RST responses to the SYN requests. This packet capture has a total of 23,545 packets and uses a mix of different protocols including MDNS, Http, and TCP.