Bennett Hall

Professor Anthony Duhaime Candeias

CISC 6680

March 14th, 2021

Lab 3: Advanced Packet Analysis

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

PCAP 1 - Angler Attack

1) What domain name is the Javascript loaded from?

   killtime365.com

2) What is the web page you are redirected to?

   programmierbrucken.cerritosliposurgery.com

3) What is the name of the malicious Javascript?

   min.js

PCAP 2 - ARP Storm

4) What is the MAC address of the attacker?

   00:07:0d:af:f4:54

5) What protocol is used in this packet capture?

   ARP

6) What is the attack name that is occurring in the PCAP?

   ARP storm attack

PCAP 3 - IRCD Attack

7) Which IP is the attacker?

172.16.192.130

8) Which IP is the victim?

172.16.192.132

9) Which service was exploited?

Internet Relay Chat Daemon

10) Which port was exploited?

6667

11) What port was accessed via Telnet in packet number 2647?

4444

12) Which packet number did an IRC error occur?

2134

PCAP 4 - Shell Shock

13) Which packet number did the HTTP communication start?

14

14) What field in the HTTP header was used in the attack?

User Agent

15) What file was requested in packet number 41 through this attack?

bin/cat /etc/passwd

16) Which web page was attacked in the HTTP based attack?

cgi-bin/netstat.cgi

17) What CVE is referenced in the threat signature?

CVE-2014-6271

Short Answers

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

In this packet capture we are seeing a cyber attack called the Angler Attack. The Angler Attack involves redirecting the user (target) to a malicious website, killtime365.com, that contains malicious javascript called min.js. We can see the source and destination IP addresses. There are a total of two packets in this packet capture. The only protocol used was HTTP. The exchange redirects to a webpage called programmierbrucken.cerritosliposurgery.com. All of this evidence should be sufficient to help detect the Angler Attack.

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

In this packet capture we can see an attacker executing a cyberattack called ARP Storm. The attacker is exploiting the ARP protocol, as seen under the protocol column in the pocket capture. In an ARP Storm Attack the attacker is attempting to flood its target with packets in an effort to disrupt service and carry out a DoS attack. The same ARP is seen multiple times in the attempt to flood the target. If we look at the details of any packet we can actually see the MAC address of the attacker. This packet capture has a total of 622 packets and the ARP protocol was the only one used. We can see an IPv6 address that indicates there's a loopback. All of this evidence should help to show us how to detect an ARP Storm attack and prevent the DoS attempt from being successful.

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

This packet capture shows an attacker, with IP address 172.16.192.130 is attacking the victim with an IP address of 172.16.192.132. The attacker and the victim are in the same network. We can see this because the IP addresses are class B addresses and the first 16 bits for both the attacker IP address and the victim IP address match. The attacker is seeking to exploit Internet Relay Chat (IRC) to take advantage of their victim. Port 6667 was exploited and port 2134 shows an IRC error. During the exchange of data in this packet capture Telnet was accessed via

port 4444. There are 2,828 packets in this packet capture and a mix of protocols including TCP, FTP, Rlogin, EXEC, SMTP, among others. 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. This information should be enough to help detect the IRC chat, identify who the attacker is, and hopefully allows us to respond and thwart the attack from being successful.

21) In 1-2 Paragraphs explain what occurred in PCAP 4.

This packet capture is showing us an attack, called Shell Shock, where attackers are able to execute arbitrary code via a crafted environment. The attacker is using bash and interacting with an HTTP server. We can see the TCP headers and exchange of communication via the TCP handshake. We can see that a file was requested in packet 41. The file is bin/cat /etc/passwd. We can also see what web page was attacked if we look at the information after 'GET." The web page is cgi-bin/netstat.cgi. The CVE is referenced in the threat assessment tool. The CVE is CVE-2014-6271. This CVE seeks privilege escalation. There are a total of 51 packets and a mixture of different protocols used. This evidence should help to detect the Shell Shock attack.