Bennett Hall

Professor Anthony Duhaime Candeias

CISC 6680

April 1st, 2021

Lab 4: Intrusion Detection System Lab

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

**PCAP 1 - Slammer Worm**

1) What is the IP address of the victim system?

   **192.0.2.2**

2) What is the port number being attacked?

   **1434**

3) What packet number triggered the first threat signature detection?

   **1**

4) What is the total number of threat detection alerts generated in Cloudshark?

   **20**

**PCAP 2 - MS08-067**

5) What is the IP address of the victim system?

   **10.5.11.67**

6) What is the IP address of the attacker?

   **10.5.11.103**

7) What port number is being exploited?

**445**

8) What packet number triggered the first high threat signature detection?

**144**

9) What is the total number of signatures triggered?

**3**

10) What packet number triggered the IPC$ share access alert?

**58**

**PCAP 3 - MS10-002-Aurora**

11) What is the IP address of the victim system?

**10.5.11.68**

12) What is the IP address of the attacker?

**10.5.11.103**

13) What packet number triggered the first high threat signature detection?

**604**

14) What is the total number of signatures triggered?

**2**

15) Which IP is hosting a web service?

**10.5.11.103**

16) What is the name of the gif transported via port 80?

**mKoJASSGpvKkfGng.gif**

**Short Answers**

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

**In this packet capture we are seeing a cyber attack called the slammer worm. The slammer worm is an SQL injection attack that causes a denial of service against its target. A DoS attack has the potential to render a target inoperative. The victim of the attack has an IP address of 192.0.2.2 and they are being attacked via port 1434. There were a total of 20 threat alerts generated in this attack, beginning with port number 1. 18 of the packets had a medium severity rating and 2 of them had a low severity rating. There were a total of 10 packets and the only two protocols listed by Cloudshark were ICMP and DCERPC. Using the slammer worm it's possible to slow internet traffic or stop it altogether.**

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

**In this packet capture we are seeing a remote code execution attack that comes from a specially crafted RPC request. Accooring the official Microsoft release about this attack, MS08-067, a successful attacker could bypass authentication protocols, run arbitrary code, and gain privilege escalation. This attack can be used to create a worm that propagates itself and spreads to other devices on a network. The victim's IP address is 10.5.11.67 and the attacker's IP address is 10.5.11.103. Port 445 is the one being exploited. There were a total of 3 threat signatures present in this packet capture, beginning with packet 144. In packet 144 the attacker attempted to gain admin privileges. The threat signature in packet 144 has a high severity rating. The other two threat signatures both had a medium severity rating. Packet 58, one of the two medium severity threat signature packets, triggered the IPC$ share access alert. This packet capture had a total of 184 packets and included a mix of protocols. The protocols included ARP, SMB, TCP, NBNS, DCERPC, among others.**

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

**This packet capture shows us a remote code execution that exploits a vulnerability in Internet Explorer called Aurora. If a user was redirected to a specially crafted page, generated by a malicious actor, the remote code would execute. According to the official Microsoft release, MS10-002, users with admin privileges are more likely to be impacted. This means that the attackers are seeking admin level privileges through the attack. The IP address of the victim is 10.5.11.68 and the IP address of the attacker is 10.5.11.103. A total of 2 threat signatures were detected. They were from packets 604 and packet 627. Both threat alerts were network trojans with a high severity. It appears that the attacker is hosting a web service and is sending out trojan horses to users who seek access to the service. It also appears that the trojan is being delivered via a gif that the victim requested from the attacker. This packet**

**capture had a total of 887 packets. There were a mix of protocols used including TCP, NBNS, HTTP, among others.**

## Work Cited

1. Microsoft Corporation. “Microsoft Security Bulletin MS08-067.” Microsoft Security Bulletin MS08-067 - Critical. Accessed April 1st, 2021.

2. Microsoft Corporation. “Microsoft Security Bulletin MS10-002.” Microsoft Security Bulletin MS10-002 - Critical. Accessed April 1st, 2021.