EE6042: Network & Host-Security

Spring semester 2023
Assignment report

Assignment	2
Assignment title	Intrusion Detection Systems Assignment
Student name	Fionn Murray
Student ID number	18223451
Report submission date	25/04/2023

Introduction

This assignments tasks were completed using two virtual machines running in Oracle VirtualBox. Both machines, attacker and victim, were running Ubuntu 22.04.

The IP address of the machines for the examples in this report are:

- Attacker: 192.168.0.99
- Victim: 192.168.0.101

The attacks displayed in this assignment make use of NMAP, and HPING3 software, in the linux terminal on the attacking machine to perform them. The attacks are detected on the victim machine using snort, running the following command before performing any attacks:

- sudo snort -d -l /var/log/snort/ -g 192.168.0.101 -A console -c /etc/snort/snort.conf

this command displays the snort log file in the terminal as it is being written, allowing for much easier confirmation of the attack being detected by snort. The specific attacks are detected by snort by the rules setup in the snort config file discussed in this report. ‘A’ full indicates full alert mode, -A console can be used to output the alerts to the terminal window. ‘-u’ changes the default UID for snort on startup, and ‘g’ the GID. ‘c’ prints the found character data in the packet payloads to snort.conf. ‘-I’ specifies to snort to listen on the enp0s3 interface, this interface is chosen as it is run on the victim machine, detected with the ip addr command.

Attack 1, Large ICMP PING

The first attack chosen for this assignment is quite simple yet can be fairly effective when the victim is running a weaker machine such as this ubuntu virtual machine. The large ICMP ping attack, also known as the ping of death attack can be formed with a simple linux ping command using the victim machines IP. The following snort config rule was used to detect this attack:

```
560 ##################################################
561
562 alert icmp any any -> any any (msg:"ICMP Large Packet"; dsize:>50000; sid:100000001; rev:1;)
```

Figure 1, Snort Rule for Large ICMP Detection

For each of the rules throughout this report, 'alert' generates the alert in the snort log file when the given condition is met, 'ICMP' and 'TCP' are the given traffics type, the keyword 'any' allows for the detection of a scan from any attacking IP, with the second 'any' indicating any port. The following IP is that of the victim machine, again on any port. The chosen message 'msg' is the text produced by the alert in the log file. Finally the 'classtype' is used to categorise the attacks, the 'sid' to identify each unique snort rule, and 'rev' simply the revision number of the snort rule.

In this rule, snort flags a ICMP Large packet attack when a packet is pinged of a larger size than 50000bytes from another IP address.

This attack is performed by running this simple ping with the largest possible packet size on the attacking machine commands several times in succession in an attempt to overwhelm the victim machine with data:

- ping 192.168.0.101 -t -l 65500

Upon detection, the snort alert file looks like this:

```
 1 [**] [1:100000001:1] ICMP Large Packet [**]
 2 [Priority: 0]
 3 04/23-15:37:09.131035 192.168.0.99 -> 192.168.0.101
 4 ICMP TTL:64 TOS:0x0 ID:57003 IpLen:20 DgmLen:65528
 5 Type:8  Code:0  ID:62554   Seq:1  ECHO
 6
 7 [**] [1:100000001:1] ICMP Large Packet [**]
 8 [Priority: 0]
 9 04/23-15:37:09.131223 192.168.0.101 -> 192.168.0.99
10 ICMP TTL:64 TOS:0x0 ID:44018 IpLen:20 DgmLen:65528
11 Type:0  Code:0  ID:62554  Seq:1  ECHO REPLY
12
13 [**] [1:100000001:1] ICMP Large Packet [**]
14 [Priority: 0]
15 04/23-15:37:10.135920 192.168.0.99 -> 192.168.0.101
16 ICMP TTL:64 TOS:0x0 ID:57008 IpLen:20 DgmLen:65528
17 Type:8  Code:0  ID:62554   Seq:2  ECHO
18
19 [**] [1:100000001:1] ICMP Large Packet [**]
20 [Priority: 0]
21 04/23-15:37:10.136111 192.168.0.101 -> 192.168.0.99
22 ICMP TTL:64 TOS:0x0 ID:44215 IpLen:20 DgmLen:65528
23 Type:0  Code:0  ID:62554  Seq:2  ECHO REPLY
24
```

Figure 2, Large ICMP Packet snort alert segment

Attack 2, Ping, TCP, and XMAS Scans

The first attack performed on the victim machine is a simple TCP scan using Nmap. In this attack, nmap sends both TCP and UDP packets to a given port and analyses the response of the packets. In order to detect these attacks, the snort.conf file was configured to set up rules for detection. This can be done quite easily and the following rules were added to the config file:

```
570 # Rule for NMAP Ping Scan Detection
571
572 alert icmp any any -> 192.168.0.101 any (msg: "NMAP Ping Scan"; dsize:0;sid:10000003; rev: 1;)
573
574 # Rule for TCP Scan Detection
575
576 alert tcp any any -> 192.168.0.101 any (msg: "NMAP TCP Scan"; classtype:network-scan; sid:10000004; rev:2; )
577
578 # Rule for XMAS Scan Detection
579
580 alert tcp any any -> 192.168.0.101 any (msg:"Nmap XMAS Scan"; flags:FPU; classtype:network-scan; sid:1000005; rev:1; )
```

Figure 3, NMAP detection snort rules

The first scan run for this attack is the Ping scan run using the following command:

- nmap -sP 192.168.0.101 -disable-arp-ping

then the TCP Scan:

- nmap -sT 192.168.0.101

and finally the XMAS Scan

- sudo nmap -sX 192.168.0.101

The outputted snort log file looks like this:

```
 1 [**] [1:10000005:2] NMAP TCP Scan [**]
 2 [Classification: Detection of a Network Scan] [Priority: 3]
 3 04/23-15:44:07.336283 192.168.0.99:38729 -> 192.168.0.101:1720
 4 TCP TTL:57 TOS:0x0 ID:39782 IpLen:20 DgmLen:40
 5 **U*P**F Seq: 0xB0AED7F4  Ack: 0x0  Win: 0x400  TcpLen: 20  UrgPtr: 0x0
 6
 7 [**] [1:1000006:1] Nmap XMAS Scan [**]
 8 [Classification: Detection of a Network Scan] [Priority: 3]
 9 04/23-15:44:07.336283 192.168.0.99:38729 -> 192.168.0.101:1720
10 TCP TTL:57 TOS:0x0 ID:39782 IpLen:20 DgmLen:40
11 **U*P**F Seq: 0xB0AED7F4  Ack: 0x0  Win: 0x400  TcpLen: 20  UrgPtr: 0x0
12
13 [**] [1:10000005:2] NMAP TCP Scan [**]
14 [Classification: Detection of a Network Scan] [Priority: 3]
15 04/23-15:44:07.336283 192.168.0.99:38729 -> 192.168.0.101:53
16 TCP TTL:54 TOS:0x0 ID:53575 IpLen:20 DgmLen:40
17 **U*P**F Seq: 0xB0AED7F4  Ack: 0x0  Win: 0x400  TcpLen: 20  UrgPtr: 0x0
18
19 [**] [1:1000006:1] Nmap XMAS Scan [**]
20 [Classification: Detection of a Network Scan] [Priority: 3]
21 04/23-15:44:07.336283 192.168.0.99:38729 -> 192.168.0.101:53
22 TCP TTL:54 TOS:0x0 ID:53575 IpLen:20 DgmLen:40
23 **U*P**F Seq: 0xB0AED7F4  Ack: 0x0  Win: 0x400  TcpLen: 20  UrgPtr: 0x0
24
```

Figure 4, NMAP snort alert log file

Attack 3, Denial Of Service

The final attack of this assignment, is similar to the first but slightly more effective. Rather than attacking the machine several time with large packets, a Denial Of Service attack (DOS) attempts to overwhelm a system with endless useless packets which are identical to the real packet requests. This attack is most commonly seen being used to target large web servers to deny customers of the sites access and driving down business of the site. The goal of this attack is to cause significant downtime to the victim machine. Hping3 is used to demonstrate the attack here, a free packer generator or TCP/IP.

The following snort rule was used in the configuration to detect the DOS attack:

```
564
565 alert tcp any any -> 192.169.0.101 80 (msg:"Possible TCP flood attack detected"; flags:S; threshold:type both, track by_src, count 100, seconds 5; sid:100000002; rev:1;)
```

Figure 5, Snort DOS detection rule

This rule flags on the detection of more than 100 TCP SYN packets in a 5 second period coming from the same IP address. This flags as a potential flood attack. 'Threshold' sets the threshold number for packets and the timing window to avoid false positive that could be triggered by normal traffic.

The attack is performed using the following command in hping3:

- hping3 -S –flood -V -p 80 192.168.0.101

'S' sets the SYN flag in the TCP packet header to initiate a TCP connection. Then, 'flood' tells hping3 to ignore the response of the packet and to send packets as quickly as possible. 'V' then sets the output to verbose for packet information. Finally the port and IP address for the attack are then set.

Upon detection, the snort alert file produces this alert:

```
1 [**] [1:10000005:2] Possible TCP flood attack detected [**]
2 [Classification: Detection of Denial of Service Attack] [Priority: 2]
3 04/23-15:07:48.905985 172.253.116.95:443 -> 192.168.0.101:34994
4 TCP TTL:122 TOS:0x0 ID:0 IpLen:20 DgmLen:60 DF
5 ***A**S* Seq: 0xD34FD2B7  Ack: 0xA3F63065  Win: 0xFFFF  TcpLen: 40
6 TCP Options (5) => MSS: 1412 SackOK TS: 2477296903 2481646639 NOP WS: 8
```

Figure 6, Snort DOS attack detection alert