



Implementation of Intrusion Detection System (IDS) to Prevent and Detect Multiple Attacks

Mohd Nazri Ismail¹; Norhatta Mohd²;
Faculty of Defence Science and Technology

National Defence University of Malaysia (UPNM), Sungai

Besi, Kuala Lumpur, Malaysia¹;

MIIT, University of Kuala Lumpur²

ABSTRACT – In this research article discuss the how to prevent the Intrusion detection system (IDS) multiple attacks. Now a days IDS attacks are increases day to day. Intrusion detection system detection and prevent multiple attacks is the challenging task to current generation research.

Keywords— Intrusion detection system (IDS), Ping of Death Attack, DDOS attack, TCP, Snort Alert and Metasploit

I. INTRODUCTION

Nowadays, there are so many attacks on the network system. And most of the big company hired the great network analyst and network security officer to defend the network.

Every network system used the Intrusion Detection System and Intrusion Prevention System to detect and defend from the attacker. There are many types of IDS such as Snort, Sguil, OSSIM, OSSEC and many more. In this proposed project, we will try to show on how the snort will detect the attack.

Snort is an open source network intrusion prevention and detection system developed by Source fire. It combines the benefits of signature, protocol, and anomaly-based inspection methods and uses as a control system to monitor all network traffic and prevent network from any attack. Snort is compatible with open source operating systems and provides a good security services to network if configured with Linux open source operating systems.

II. LITERATURE SURVEY

2.1 Attacking Tools

A. SNMPENUM

We are using SNPENUM in backtrack3. SNMP Enumeration is a process of using SNMP to enumerate user accounts and

devices on a target system. SNMP has two passwords to access and configure the SNMP agent from the management station. The first is called a read community string. This password lets you view the configuration of the device or system. The second is called the read/write community string; it's for changing or editing the configuration on the device. By default read community string is public and read/write community string is private. If these passwords are not changed they can be used by an attacker to enumerate SNMP as SNMP Manager.

B. Metasploit

Metasploit was used as a software attack in Backtrack 3.

- Metasploit Framework is an open source penetration tool used for developing and executing exploit code against a remote target machine it, Metasploit frame work has the world's largest database of public, tested exploits. In simple words, Metasploit can be used to test the Vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems.
- SYN flooding is an attack vector for conducting a denial-of-service (DoS) attack on a computer server.
- Many users use metasploit for penetration, vulnerability scanning, meterpreter scripting and more
- Metasploit command using Synflood
 - Msfconsole
 - Use auxiliary/dos/tcp/synflood
 - Show options (to view option)
 - Set rhost (target IP address)

- (target ip address)
- Ifconfig
- Set INTERFACE (interface use to attack)
- Show options (to view option)
- Exploit
- In the final report, we will provide the screenshot of every step.

C. Nmap

In this project, we run Nmap through Windows 7 platform.

- Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network.
- Nmap – port scanner
 - Describing detail open ports on target host.
- How to Use Nmap:
 - nmap [IP Address of host] -p
 - This command will show all available ports on the host
 - It also will show the state of the port either open or close
 - Since we are using Zenmap (Nmap Gui) for Windows, we just need to put the host ip address and select the intense scan to scan thoroughly.

D. Ping of Death

On the Internet, ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments. In 1996, attackers began to take advantage of that feature when they found that a packet broken down into fragments could add up to more than the allowed 65,536 bytes. Many operating systems didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted. The example of command to use is like below:

Ping SITE-IP -l 65500 -n 10000000 -w 0.00001

2.2 IDS Software

Snort



Fig. 1 Snort was used as a software IDS through Windows 7 platform

Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching, and content matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified

• Snort Rules

- Rules are a different methodology for performing detection, which bring the advantage of 0-day detection to the table. Unlike signatures, rules are based on detecting the actual vulnerability, not an exploit or a unique piece of data. Developing a rule requires an acute understanding of how the vulnerability actually works.

• Snort Alert

- Generate an alert using the selected alert method, and then log the packet

III. METHODOLOGY

In this section, I will explain on how to test the snort and the flow of the attacking and detecting process.

Logical Diagram:

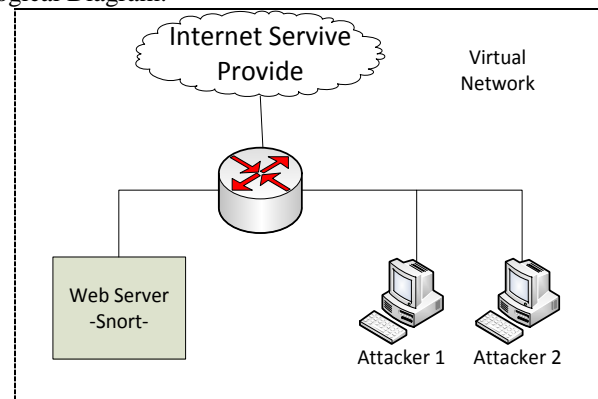


Fig. 2 Block Diagram of IDS attack

The Figure 3 below shows the flowchart of the first attack that we will use to test the snort. In this attack, we will

use metasploit in backtrack / kali linux to launch the DDOS attack on the victim.

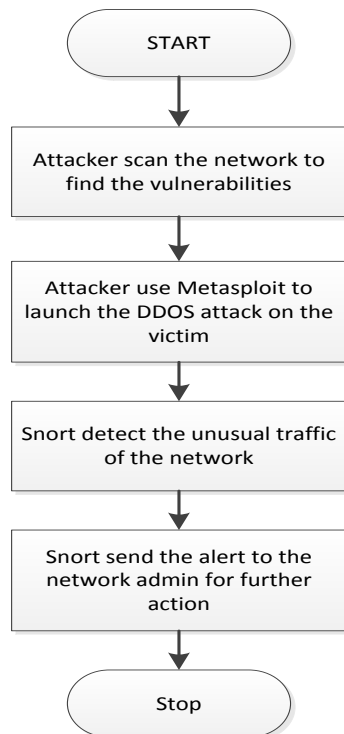


Fig. 3 shows the flowchart of the first attack

The Figure 4 below shows the flowchart of the second attack. We will use nmap on linux/backtrack to launch the port scan attack on the victim.

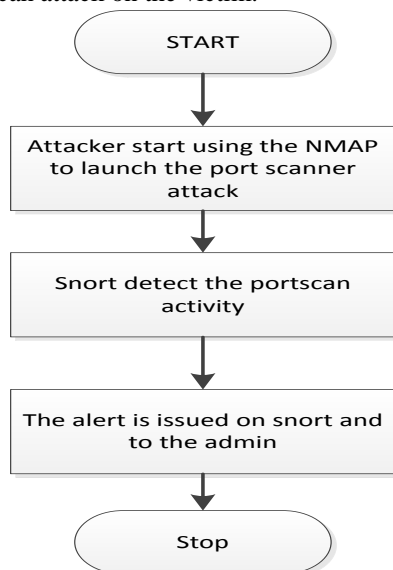


Fig.4 below shows the flowchart of the second attack

Figure 5 below shows the flowchart of the Ping of Death Attack and how snort detect and logged the attack.

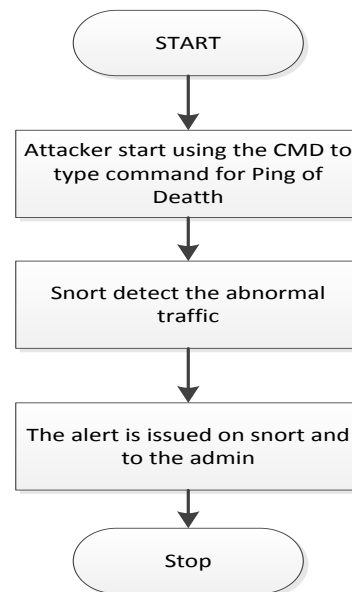


Fig. 5 Flow Chart of Ping of Death Attack

Figure 6 below shows the flow on how attacker starts the attack using SNMPENUM on Backtrack to gather the information about the host.

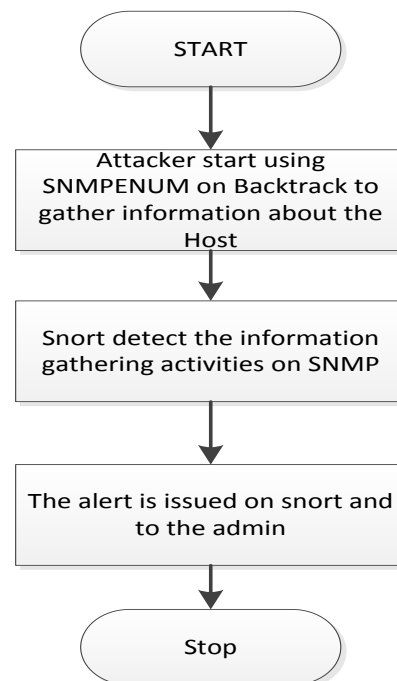


Fig 6 flow on how attacker starts the attack using SNMPENUM

IV. RESULT AND ANALYSIS

A. Portscan Attack

This is how we used the Zenmap (Nmap Gui for Windows) to launch the portscan attack on the Host IP Address (IDS)

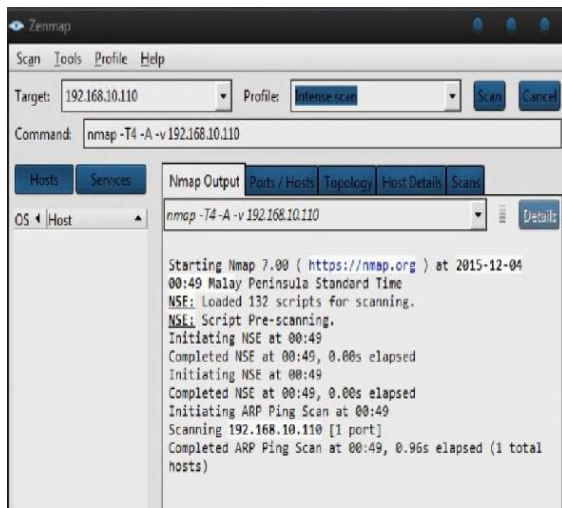


Fig.7 Operating Window of Zenmap

B. Portscan Alert / Log

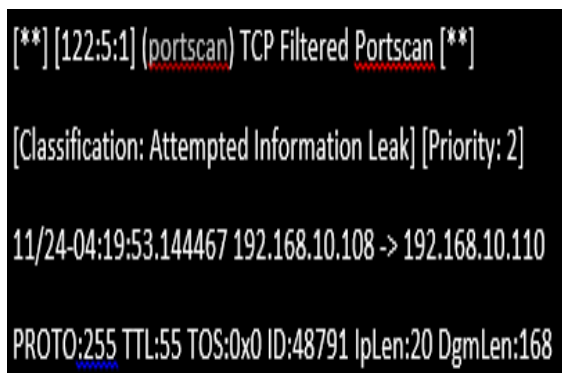


Fig 8 shows the alert logged by Snort for Portscan attack.

The figure 8 above shows the alert logged by the Snort for Portscan attack.

[192.168.10.108 -> 192.168.10.110]

This shows that the attacker from 192.168.10.108 is trying to scan port on the Snort [192.168.10.110] [TTL:55] is a mechanism that limits the lifespan or lifetime of data in a computer or network

iplen - the IP header length.

dgmlen - total packet length as seen by the IP layer, inclusive of IP header, any higher layer headers, and the payload.

C. DDOS Attack

The figure 9 below shows how we test the snort using msfconsole which is Metasploit on Backtrack.

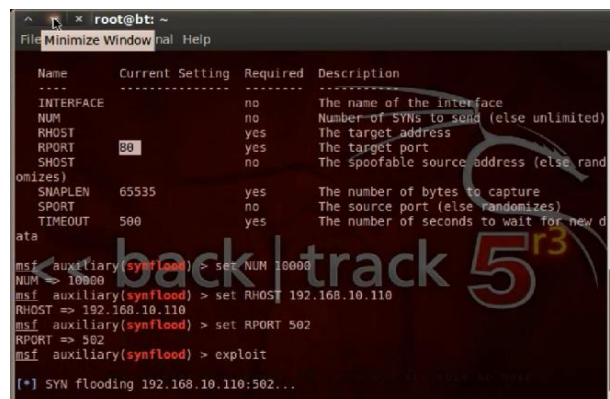


Fig. 9 Test the snort using msfconsole

D. DDOS Alert / Log

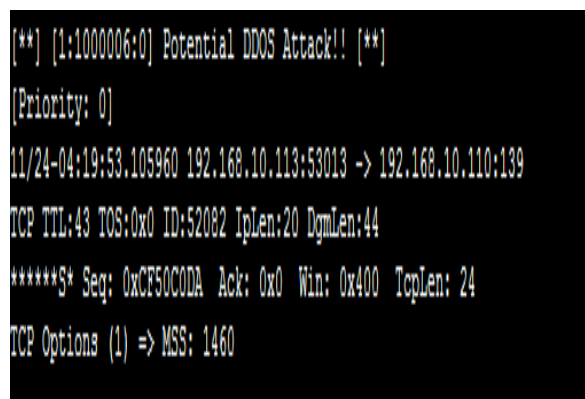


Fig. 10 alert logged by the Snort for DDOS attack.

The figure above shows the alert logged by the Snort for DDOS attack.

[192.168.10.113 -> 192.168.10.110]

shows that the attacker from 192.168.10.113 is trying to DDOS TCP port on the Snort [192.168.10.110]

[TTL:43] is a mechanism that limits the lifespan or lifetime of data in a computer or network

iplen - the IP header length.

dgmlen - total packet length as seen by the IP layer, inclusive of IP header, any higher layer headers, and the payload.

E. Ping of Death Attack

The figure below shows how we test the snort using Ping of Death command on CMD.



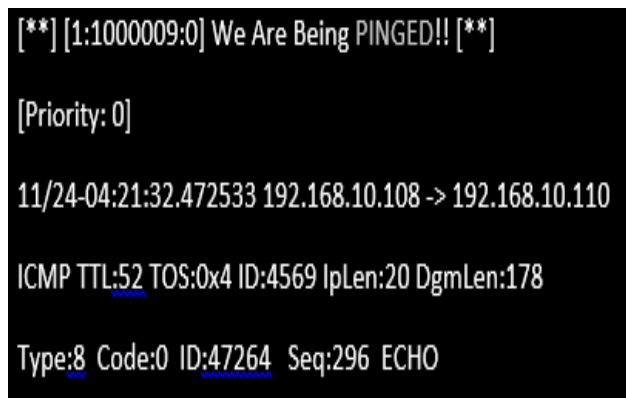
```
C:\Windows\System32>ping 192.168.10.110 -l 65500 -n 10000000 -w 0.00001

Pinging 192.168.10.110 with 65500 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 192.168.10.110:
    Packets: Sent = 6, Received = 0, Lost = 6 (100% loss),
    Control-C
^C
C:\Windows\System32>
```

Fig. 11. test the snort using Ping of Death command on CMD.

Ping of Death Alert / Log



```
[**] [1:1000009:0] We Are Being PINGED!! [**]

[Priority: 0]

11/24-04:21:32.472533 192.168.10.108 -> 192.168.10.110

ICMP TTL:52 TOS:0x4 ID:4569 IpLen:20 DgmLen:178

Type:8 Code:0 ID:47264 Seq:296 ECHO
```

Fig. 12 Ping of Death Alert / Log

[192.168.10.108 -> 192.168.10.110]

This shows that the attacker from 192.168.10.108 is trying to ping the Snort [192.168.10.110]

ICMP is used to relay a query message which basically be done by pinging the targeted ip address.

[TTL:52] is a mechanism that limits the lifespan or lifetime of data in a computer or network

iplen - the IP header length.

dgmLen - total packet length as seen by the IP layer, inclusive of IP header, any higher layer headers, and the payload.



```
[**] [1:1000006:0] Potential DDOS Attack!! [**]

[Priority: 0]

11/24-04:21:36.249739 192.168.10.108:4243 -> 192.168.10.110:10243

TCP TTL:128 TOS:0x0 ID:31241 IpLen:20 DgmLen:52 DF

***A*** Seq: 0x89EDEF82 Ack: 0x1852D8DF Win: 0x410C TcpLen: 32

TCP Options (3) => NOP NOP TS: 1582762 3058479
```

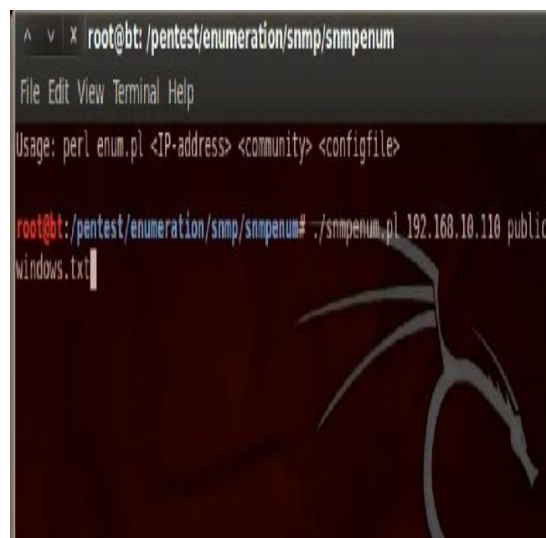
Fig. 13 DDOS Attack' alert

The 'Potential DDOS Attack' alert also triggered when we test the snort by Ping of Death Attack because we sent to many packets to the host so that the snort alerted that it will be a potentially a DDOS attack

E. SNMP Attack

Simple Network Management Protocol (SNMP) is an application-layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol / Internet Protocol (TCP/IP) protocol suite.

To test Snort detection on SNMP Attack, we used 'SNMPENUM' on Backtrack. Since we configured snort on Windows 7, the command we used is: snmpenum.pl 192.168.10.110 public windows.txt



```
root@bt: /pentest/enumeration/snmp/snmpenum

File Edit View Terminal Help

Usage: perl enum.pl <IP-address> <community> <configfile>

root@bt: /pentest/enumeration/snmp/snmpenum# ./snmpenum.pl 192.168.10.110 public windows.txt
```

Fig. 14 - test Snort detection on SNMP Attack

4.7 SNMP Alert / Log

```
[**] [1.1421:11] SNMP AgentX/tcp request [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
11/24-04:19:54.300818 192.168.10.108:53013->192.168.10.110:705  
TCP TTL:51 TOS:0x0 ID:509 Iplen:20 Dgmlen:44  
*****S* Seq: 0xCF50C0DA Ack: 0x0 Win: 0x400 TcpLen: 24  
TCP Options (1) => MSS: 1460
```

Fig. 15 Test Snort detection on SNMP Attack

[192.168.10.113 -> 192.168.10.110]

This shows that the attacker from 192.168.10.113 is trying to get some information about the host on 192.168.10.110

[Classification: Attempted Information Leak]: this alerted that this attack is trying to attempt or get the information about the host.

[TTL:51/64] is a mechanism that limits the lifespan or lifetime of data in a computer or network

iplen - the IP header length.

dgmlen - total packet length as seen by the IP layer, inclusive of IP header, any higher layer headers, and the payload.

REFERENCES

- [1] E. <https://snort.org/>
- [2] <http://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-snmp-for-reconnaissance-0150181/>
- [3] <https://github.com/eldondev/Snort>
- [4] https://en.wikipedia.org/wiki/Ping_of_death
- [5] <https://scadasecurity636.wordpress.com/2014/06/23/ddos-attack-using-metasploit/>