ET4028 – Host & Network Security

Intrusion Detection System Assignment

By:

Ryan O'Connor - 17209382

Lecturer:

Reiner Dojen

Submitted to the University of Limerick in partial fulfilment of the requirements for:

Bachelor of Science in Mobile Communications & Security

Department of Electronics & Computer Engineering

University of Limerick

16th April 2021

General Information

This project was undertaken using VMware and two virtual machines. The first machine was a Kali Linux machines and it was the attacker machine. The second was the victim machine and it was an Ubuntu machine. The IP addresses for each machine were as follows:

- Attacker: *192.168.20.128*
- Victim: *192.168.20.129*

Attack One – Null Port Scan using NMAP

Description:

A **null port scan attack** is when a packet is sent to a port with no flags set, this port is a TCP port. It is important to note that no flags are set, this is what makes it a null port scan attack when compared to traditional TCP port scan attacks. The expected result of this type of attack is no response. The target does not know how to manage the request and the packet is discarded with no response sent. The target will only send a packet in response if the port is closed. The command to carry out the attack was as follows:

'nmap -sN 192.168.20.129'

Attack Location:

Log file location: snort.log.1618531587 Line No.: 3 (for port 80).

Alert file location: Alert_PortScan Line No.: 13-17 (for port 80).

Rule Location:

Snort.conf file location: Line No.: 586

Description of components:

alert tcp any any -> 192.168.20.129 1:100 (msg:"Warning!! Possible NMAP Port Scan!!"; flags:0; classtype:network-scan; sid:100000001; rev:1;)

- **Alert**:
  - Rule action allowing generation of alert when condition is met.
- **Tcp:**
  - Type of traffic, in this case TCP (Transmission control protocol).
- **Any:**
  - Source IP address, Snort will look at all options.
- **Any:**
  - Source port, snort will look at all ports.
- **192.168.20.129**
  - Destination IP address, snort will only look at this one.
- **1:100**
  - Destination IP address, snort will look at range of 1:100. (Used shorten output)
- **Msg: "***Warning!! Possible NMAP Port Scan!!***"**
  - Snort will include the message inserted with the alert.
- **Flags: 0**
  - Flag keyword, snort will look for no flags being set. (Null scan)
- **Classtype:**
  - Used to categorise the rule as the type of attack, network scan in this case.
- **Sid:** *100000001*

- Used to uniquely identify the snort rule, set as *100000001* in this case.
- **Rev:** *1*
  - Revision of the snort rule, also allow rule to be uniquely identified.

Attack Two – Denial of Service using HPING3 (Verbose)

Description:

A **denial-of-service attack** is when an attacker wants to shut down a machine or network, therefore making it inaccessible to the intended users. It is achieved by flooding the target with traffic. Usually an attacker would carry out this attack on a number of machines all attacking the victim machine, this is known as a distributed denial of service attack (DDOS). In this case, the -E was used to fill the packet's data with the contents of the file *data.txt (string: 'Ryan')*. The -V indicates that the verbose output is enabled. The command to carry out the attack was as follows:

'hping3 -V -1 -d 5 -E data.txt 192.168.20.129'

Attack Location:

Log file location: snort.log.1618531707 Line No.: 1 (for the first packet).

Alert file location: Alert_dos Line No.: 1-5 (for the first packet).

Rule Location:

Snort.conf file location: Line No.: 589

Description of components:

alert icmp any any -> 192.168.20.129 88 (msg:"Warning!! Possible DDOS Probe!!"; content:"Ryan"; itype:8; classtype:denial-of-service; sid:100000002; rev:1;)

- **Alert**:
  - Rule action allowing generation of alert when condition is met.
- **Icmp:**
  - Type of traffic, in this case ICMP (Internet Control Message Protocol).
- **Any:**
  - Source IP address, Snort will look at all options.
- **Any:**
  - Source port, snort will look at all ports.
- **192.168.20.129**
  - Destination IP address, snort will only look at this one.
- **88**
  - Destination IP address, snort will look at port 88 in this case.
- **Msg: "***Warning!! Possible DDOS Probe!!"*
  - Snort will include the message inserted with the alert.
- **Content:** *"Ryan"*
  - Searching for specific content in packet. In this case "Ryan" was inserted into the *data.txt* file that was included in the attack command. As explained above.
- **itype:** 8
  - itype keyword used to detect attacks that use type field in ICMP packet header. In this case, the type 8 is used which is an Echo Request.
- **Classtype:**
  - Used to categorise the rule as the type of attack, denial of service request here.
- **Sid:** *100000002*

- Used to uniquely identify the snort rule, set as *100000002* in this case.
- **Rev:** *1*
  - Revision of the snort rule, also allow rule to be uniquely identified.

Attack Three – Brute Force FTP Attack using NCRACK

Description:

A **brute force attack**, also known as a dictionary attack, is an attack where an attacker works through a dictionary of possible passwords and/or usernames and tries them all. In this case, a brute force attack is carried out on an FTP (File Transfer Protocol). Using custom made dictionaries and the ncrack software, the attack was carried out. The command to carry out the attack was as follows:

'ncrack -U user.txt -P pass.txt ftp://192.168.20.129'

Attack Location:

Log file location: snort.log.1618531830 Line No.: 1 (User Victim).

Alert file location: Alert_BruteForce Line No.: 1-6.

Rule Location:

Snort.conf file location: Line No.: 592

Description of components:

alert tcp any any -> 192.168.20.129 21 (msg:"Warning!! Possible Brute Force, A host is trying to access FTP!!"; pcre:"/USER|PASS/i"; flow:to_server; threshold: type threshold, track by_src, count 3, seconds 60; classtype:unsuccessful-user; sid:100000003; rev:1;)

- **Alert**:
  - Rule action allowing generation of alert when condition is met.
- **Tcp:**
  - Type of traffic, in this case TCP (Transmission control protocol).
- **Any:**
  - Source IP address, Snort will look at all options.
- **Any:**
  - Source port, snort will look at all ports.
- **192.168.20.129**
  - Destination IP address, snort will only look at this one.
- **21**
  - Destination IP address, snort will look at port 21 in this case.
- **Msg:** *"Warning!! Possible Brute Force, A host is trying to access FTP!!"*
  - Snort will include the message inserted with the alert.
- **PCRE**:"/USER|PASS/i"
  - Snort will look for everything between the two forward slashes. In this case, looking for USER or PASS. The 'i' allows ignoring of case sensitivity.
- **Flow**: to_server
  - Keyword used in conjunction with session tracking, in this case it will trigger on client requests from A to B or client to server using to_server.
- **Threshold:**
  - Type threshold
    - Alerts every time the event takes place during time interval
  - Track by_src

        - The count is maintained for each unique source ip address.
    - Count 3
        - The amount of rule matching in the time period specified in seconds below. Three in this case.
    - Seconds 60
        - Time period which count is accrued. Sixty seconds in this case.
- **Classtype:**
    - Used to categorise the rule as the type of attack, unsuccessful user login here.
- **Sid:** *100000003*
    - Used to uniquely identify the snort rule, set as *100000003* in this case.
- **Rev:** *1*
    - Revision of the snort rule, also allow rule to be uniquely identified.