EE6042/ET4028 – Host and Network Security

Unit 4

IDS Assignment

Ian Rowland

19190859

Table of contents

Table of Figures

Introduction

This IDS assignment was undertaken using the following machines:

Lubuntu 20.04, running on VMWare workstation player as both victim machine and IDS

Kali Linux, running on VMWare workstation player as the attacker machine.

The ip addresses of the two machines are listed below:

Victim Machine: 192.168.220.132 -- brd 192.168.220.255 scope global dynamic noprefix route ens33 -- Interface ens33 – altname enp2s1

Attacker machine: interface eth0 – ip address 192.168.220.133 --brd 192.168.220.255 scope global noprefix route eth0

Command used to start snort:

#sudo snort -A full -A console -q -u snort -g snort -k none -c /etc/snort/snort.conf -i ens33

Description of command components:

-A full: enables full alert mode, to log all alerts

-A console: displays all alerts on the console/terminal

-q: sets snort to quiet mode, so it will not display banners or status messages

-u: sets the user that snort will run as

-g: sets the group snort will run as

-k: specify alert output plug-in to use

-c: specify the location of the snort configuration file

-i: specify the netwok interface that snort should listen to. In this case, ens33

Attack 1: Bruteforce

Description:

A brute force attack is an attack where a hacker uses a number of, if not all available, possible combinations of letters, numbers, special characters, and upper and/or lower case letters to gain access to a host or service, and such attacks may be done using an automated system [1].

A text file containing the relevant passwords was created for the purposes of conducting such an attack, and is included as part of the submission for this assignment.

For the purposes of demonstrating the attack, the correct username and password for the victim machine are included in the respective txt files.

Attack Commands:

Msf > use auxiliary/scanner/ftp/ftp_login

Msf auxiliary(ftp_login) > set PASS_FILE PASS.txt

Msf auxiliary(ftp_login) > set USER_FILE user.txt

Msf auxiliary(ftp_login) > set RHOST 192.168.220.132

Msf auxiliary(ftp_login) > run

Metasploit is used to conduct the bruteforce attack, using the ftp_logon auxiliary. This can be used to define the password file, username file, and target machine, before executing the bruteforce with the “run” command.

Snort Rules:

alert tcp any any -> 192.168.220.132 any (msg:"Bruteforce attack detected: someone is trying to access the system"; pcre:"/USER|PASS|PASSW0RD|ian|fairy|pwd|admin/i"; flow:to_server, established; classtype:unsuccessful-user; threshold:type both, track by_src, count 4, seconds 20; sid:10000007; rev:1;)

Description of rule components:

Alert: - generate an alert when sufficient conditions are met.

Tcp: traffic type

Any Any – source ip address and source port, as attack can come from anywhere and any port.

192.168.220.132 any – destination ip address and destination port, as attack can occur on destination machine at any port.

Msg: Message content to be displayed in the alert.

Pcre: Snort will look for phrases and strings within the two “/” slashes and separate each phrase out by the “|”, to look for patterns in the traffic being detected. The “i” is meant to prevent case sensitivity.

Flow: triggers the alert based on the direction/flow of the traffic. In this case, the flow is set as “to_server”, to ensure alerts will be generated on traffic going to the ftp server on the victim machine.

Classtype: Categorises rule as detecting certain class of attack.

Threshold: Sends an alert whenever sufficient conditions for the traffic are met, based on Track, count and seconds below.

Track by_src: Tracks the traffic by the source.

Count: Defines the amount of times the traffic must be detected to generate an alert.

Seconds: The time period for which traffic is detected. If sufficient traffic is detected within this period, alert will be generated.

Sid: Identification number for snort rule.

Rev: revision number of rule.

Detection/Snort Output:

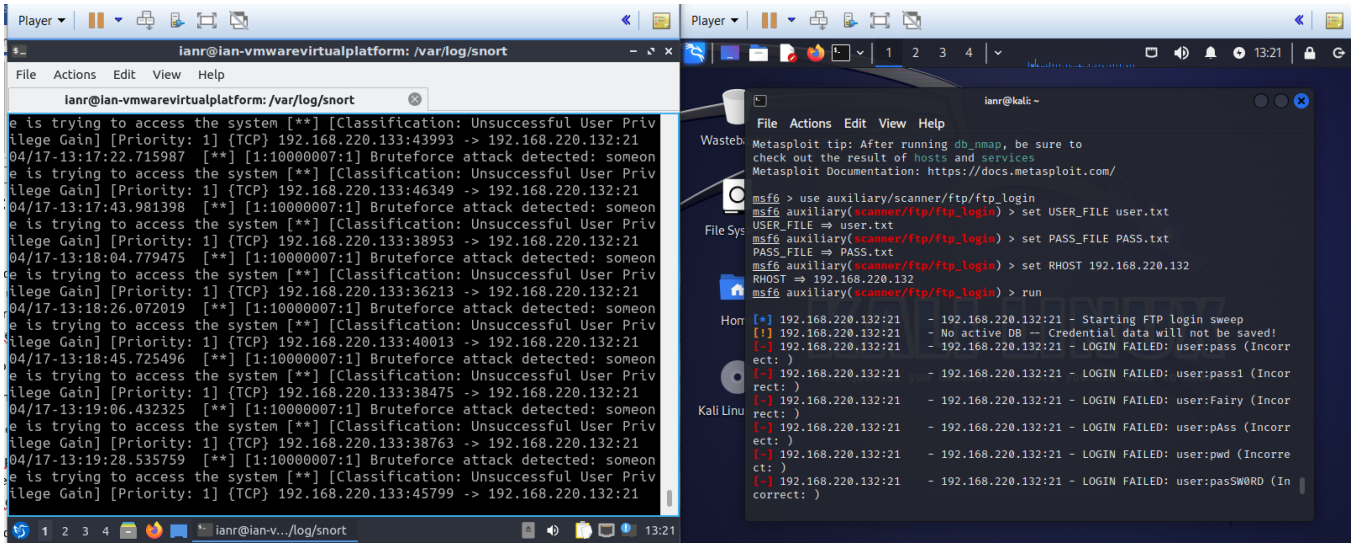

Figure 1. bruteforce

Rule and line location:

Rule location: snort.conf, line 571

Log file and alert location:

Alert file name: alert

Log file name: snort.log.1681733745

Alerts begin at line 13657 of alert file.

Traffic captured from line 2277 of log file when observed in wireshark.

Attack 2: DoS attack

Description: A denial of service attack is an attack where an attacker sets about making a machine or resource unavailable to the intended users by disrupting services of an internet connected host. DoS attacks are typically achieved by flooding a target machine with requests so as to overload the system [2].

Attack Commands:

sudo hping3 -V -1 -E dospacket.txt 192.168.220.132 -d 10 –flood

hping3 was used to conduct the DoS attack. The –flood component was used to flood the target machine with the packets generated by the command, to allow for the attack to be detected.

Snort Rules:

alert icmp any any -> 192.168.220.132 any (msg:"DoS attack detected! Someone is trying to bring down the system!!";content:"beepboop"; itype:8; classtype:denial-of-service; sid:10000009; rev:1; detection_filter:track by_src, count 500, seconds 5;)

Description of rule components:

Alert: Generates alert upon condition for rule being fulfilled.

Icmp: Traffic type

Any any: Source IP and Source port, as attack can come from anywhere.

192.168.220.132 any: destination IP and Destination port, as attack can occur on destination machine at any port.

Msg: Message content to be displayed in the alert.

Content: Searches for content in the attackers packet file. In this case, the content was “beepboop” which was contained in the dospacket.txt file.

Itype: Tests the value of the ICMP type field. In this case, it is set to echo requests, which are of itype 8.

Classtype: Categorises rule as detecting certain class of attack.

Detection_filter: Option used to filter out traffic based on certain factors, such as tracked, Count and seconds below.

Track by src: Tracks the traffic by the source.

Count: Defines the amount of times the traffic must be detected to generate an alert.

Seconds: The time period for which traffic is detected. If sufficient traffic is detected within this period, alert will be generated.

Sid: Identification number for snort rule.

Rev: revision number of rule

Detection/Snort Output:

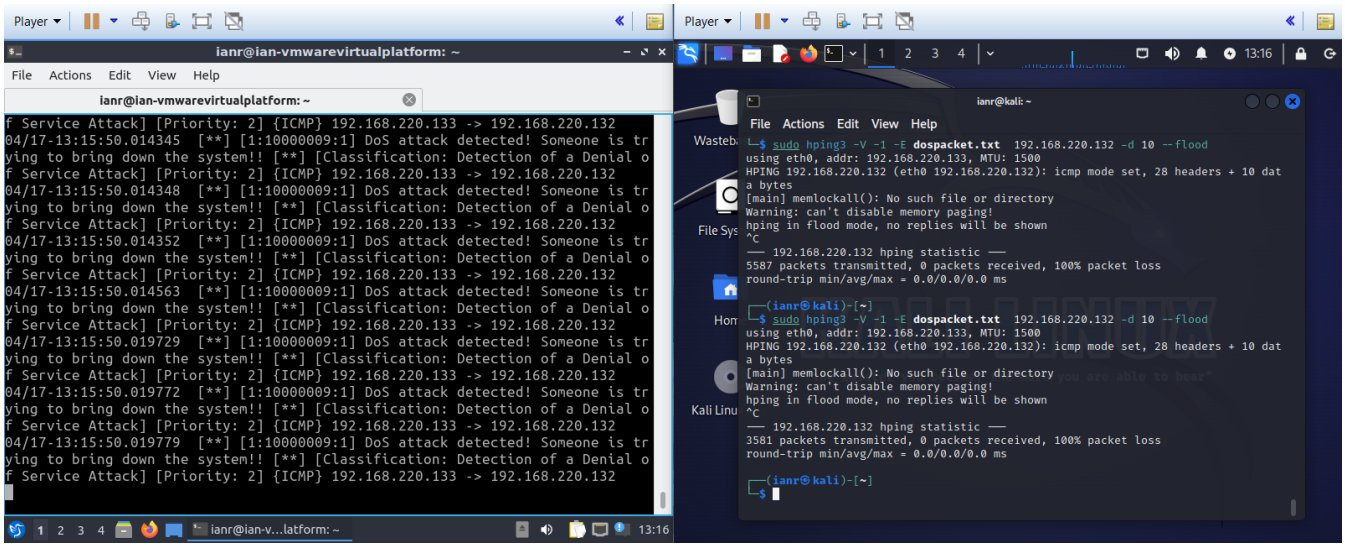

Figure 2. DoS attack

Rule and line location:

Rule location: snort.conf, line 577

Log file and alert location:

Alerts start at line 1 of alert file, and continue to line 7650 (Xmas scan alerts start at 7651)

Alerts captured in line 1 of log file, when opened in wireshark.

Alert file name: alert

Log file name: snort.log.1681733745

Attack 3: Port Scan – Xmas Scan

An Xmas scan is a type of port scan that are used within packets associated with them. This type of scan is designed to manipulate the PSH, URG and FIN flags of a TCP header[3]. Xmas scans can be executed using Nmap by using the -sX option in an Nmap command [4].

Description:

Attack Commands:

sudo nmap -sX 192.168.220.132

nmap was used to conduct this scan/attack. Using the -SX option triggers nmap to start an Xmas scan of the target machine, based on the ip address provided.

Snort Rules:

alert tcp any any -> 192.168.220.132 any (msg:"Xmas scan has been initiated against the system. Someone is scanning the ports on the system.";classtype:network-scan; dsize:0; flags:FPU; sid:10000008;rev:1;)

Description of rule components:

Alert: Generates alert upon condition for rule being fulfilled

TCP: Traffic type

Any any: Source IP and Source port, as attack can come from anywhere

192.168.220.132 any: destination IP and Destination port, as attack can occur on destination machine at any port

Msg: Message content to be displayed in the alert

Classtype: Categorises rule as detecting certain class of attack

Dsize: Determines size requirement for packets to trigger the alert.

Flags: Specifies the flags that the traffic/packets must have in order to trigger the alert. FPU dictates that the FIN, PSH and URG flags must be present in order to generate the alert, thereby meeting the requirements for an Xmas scan.

Sid: Identification number for snort rule.

Rev: revision number of rule

Detection/Snort Output:

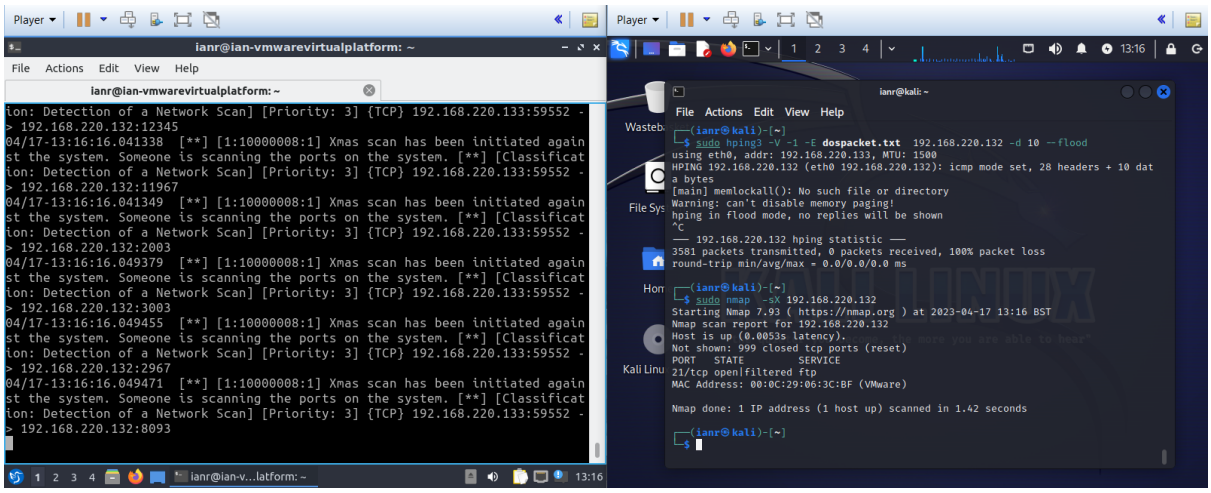

Figure 3. Xmas Scan

Rule and line location:

Rule location: snort.conf, line 574

Log file and alert location:

Alerts start at line 7651 of alert file, and continue to line 13656 (bruteforce alerts start at line 13657)

Captured log starts from line 1276 of log file, when opened in wireshark.

Alert file name: alert

Log file name: snort.log.1681733745

Additional Info:

The alert details for each attack are all contained in one file, with starting lines and line ranges for each attack having been clarified in the relevant sections.

Alert file name: alert

Log file name: snort.log.1681733745

The users and PASS txt files are the files used for the bruteforce attack.

The dospacket file, containing the dummy string “beepboop” is used for the dos attack.

The required options for the snort rules are used as follows:

Pcre: used for the bruteforce attack, attack 1.

Flow: used for the bruteforce attack, attack 1.

Itype: used for the Dos attack, attack 2.

Content: used for the DoS attack, attack 2.

Bruteforce logs(attack 1): Alerts start from line 13657 of alert file(as viewed in VSCode), and line 2277 of log file(as viewed in wireshark) – snort rule at line 571 in snort.conf

DoS logs (attack 2): Alerts start from line 1 of alert file(as viewed in VSCode), and line 1 of log file(as viewed in wireshark) – snort rule at line 577 in snort.conf

Xmas Scan Logs (attack 3): Alerts start from line 7651 of alert file(as viewed in VSCode), and line 1276 of log file(as viewed in wireshark) –snort rule in line 574 of snort.conf

References:

[1] tutorialspoint.com, n.d, “Metasploit - Brute-Force Attacks”, available: https://www.tutorialspoint.com/metasploit/metasploit_brute_force_attacks.htm , accessed: 12th April 2023

[2] Gogoi, M., Mishra, S., 2018, “DETECTING DDoS ATTACK USING Snort”, available: https://www.researchgate.net/publication/338660054_DETECTING_DDoS_ATTACK_USING_Snort , accessed: 12th April 2023

[3]plixer.com, 2015, “Understanding Xmas Scans”, available: https://www.plixer.com/blog/understanding-xmas-scans/ , accessed: 13th April 2023

[4]nmap.org, n.d, “TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX)” , available: https://nmap.org/book/scan-methods-null-fin-xmas-scan.html , accessed: 13th April 2023