# lCIT 285 - Lab #12: Snort

## 1: Introduction

In this lab, we will learn about network intrusion detection with the open source tool, Snort while its running on your server (i.e. Metasploit VM). We will also use tshark, the text interface to Wireshark, to examine captured packets.

Both your Kali and Metasploitable VMs should be powered on to perform the necessary pings and scans. In this lab your Metasploit VM will act as a server running the IDS programyou’re your Kali VM will be the client. *In the questions below, if multiple alerts are generated of the same type, indicate the number of alerts of that type.*

1.1: In Metasploit, change to root then verify the tshark version on Metasploit is up to date.

**# sudo su -**

**# apt-get install snort tshark**

Configure the snort.conf file with **your Metasploit VM IP address**. This ensures traffic is captured by snort when sent to and from your Metasploit VM.

**# nano /etc/snort/snort.conf**

A screenshot of a cell phone

Description automatically generated

Find the line highlighted in the picture and change the IP listed to your Meta VM IP. Keep the /24 mask.

**References:**

* [Nmap.org – Reference Guide](https://nmap.org/book/man-briefoptions.html)
* [Nmap.org – Port Scanning Techniques](https://nmap.org/book/man-port-scanning-techniques.html)

## 2: Detecting Network Scans

In your **Linux** **server**, run the following command to watch for alerts. This command will continually monitor the specified file and print any new data that is added to that file.

**# snort -c /etc/snort/snort.conf -D**

**# tail -f /var/log/snort/alert**

2.1: From the client (Kali), ping the Linux server three times using ping's -c (count) option.

* Does anything show up in the snort alert log?
  + If there is an alert, list the snort alert name (found in the first line of the alert) and the classification, which is found in the second line, in the box below.
  + If nothing, just write “no alert.”

**# ping -c 3 METASPLOIT\_SERVER\_IP**

|  |  |  |
| --- | --- | --- |
| **Alerts Seen [Y/N]** | **Snort Alert Name** | **Classification** |
| **No alert** |  |  |

2.2: Scan the open ports on your Linux server. What alerts show up in the snort alert log (in the window where you left the tail -f command running)? List the snort alert name (found in the first line of the alert) and the classification, which is found in the second line, in the box below.

**# nmap -sT METASPLOIT\_SERVER\_IP**

|  |  |  |
| --- | --- | --- |
| **Alerts Seen [Y/N]** | **Snort Alert Name** | **Classification/Priority** |
| **Yes** | **Nmap.org** | **1** |

2.3: Use a stealthy FIN scan to identify open ports on your Linux server.

* How many alerts show up in the snort alert log?
* Is the FIN (-sF) scan more or less stealthy than the TCP connection (-sT) scan?
* Include one of the alerts in the box below, along with answers to the questions.
* If there are no alerts, write “no alerts”.

**# nmap -sF METASPOIT\_SERVER\_IP**

|  |  |  |
| --- | --- | --- |
| **Number of Alerts** | **Snort Alert Name** | **Classification/Priority** |
| **1** | **Nmap.org** | **1** |
| **More or Less Stealthy (?)** | | |
| **This is more stealthy** | | |
| **Alert Example** | | |
| 1 host up scanned in 5.10 sec | | |
| **What does the –sF scan do when packets are sent?** | | |
| **Sets just the TCP FIN bit.** | | |

2.4: Use a stealthy XMAS scan to identify open ports on your Linux server.

* How many alerts appear in the snort alert log?
* Is the XMAS (-sX) scan more or less stealthy than the TCP connection (-sT) scan?
* Include one of the alerts in the box below, along with answers to the questions.
* If there are no alerts, write “no alerts”.

**# nmap -sX METASPLOIT\_SERVER\_IP**

|  |  |  |
| --- | --- | --- |
| **Total Number of Alerts** | **Snort Alert Name** | **Classification/Priority** |
| **1** | **Nmap.org** | **1** |
| **More or Less Stealthy (?)** | | |
| **Less stealthy** | | |
| **Alert Example** | | |
| 1 host up scanned in 3.01 sec | | |
| **What does the –sX scan do?** | | |
| **Sets the FIN, PSH, and URG flags.** | | |

2.5: Attempt to make a scan stealthier by using IP fragmentation and the null scan.

* Does anything show up in the snort alert log?
* If there is an alert, list the snort alert name (found in the first line of the alert) and the classification, which is found in the second line, in the box below.
* If nothing, just write “no alert.”

**# nmap -f -sN METASLPOIT\_SERVER\_IP**

|  |  |  |
| --- | --- | --- |
| **Alerts Seen [Y/N]** | **Snort Alert Name** | **Classification/Priority** |
| **No** |  |  |
| **Number of Alerts ( 0 – 9)** | **More or Less Stealthy (?)** | |
|  |  | |
| **Alert Example** | | |
|  | | |
| **What does the –sN scan do?** | | |
| **-sN does a no port scan but a host scan** | | |

2.6: Perform a protocol scan on your Linux server to see what types of IP protocols it accepts. With this type of scan IP packet headers are used but are typically empty. The scan being performed can take some time to complete.

* Find an alert from the most recent nmap scan that **does not** have a message of “DESTINATION UNREACHABLE: PROTOCOL UNREACHABLE”. Use the web address included in the alert to research its meaning.
* Screen shot the alert found and provide a brief description of the alert below.

**# nmap -sO METASPLOIT\_SERVER\_IP**

Once the scan completes, issue the following in your Metasploit\_Server

**# ctrl+c**

**# cd /var/log/snort**

**# cat alert | less**

Text

Description automatically generated

## 3: Testing snort with pcap files

Packet sniffers like Wireshark and snort can save sniffed packets in a pcap (packet capture) file. These files can then be used for a variety of purposes, including testing that your network intrusion detection system correctly alerts on malicious traffic.

* **Transfer** **the** **slammer files from your Kali VM to your Metasploit VM**.
  + These files are in the Downloads folder of Kali.
* Use sftp to transfer them to your Metasploit VM.
  + When running snort against the files, provide the full path to the file.
  + If you are not receiving alerts, restart snort using the command from section 2.

Metasploit Commands to retrieve slammer files

**# sftp root@KALI\_IP**

**sftp> cd Downloads**

**sftp> get lab12-files.tar.bz2**

**sftp> exit**

Move to the change to the home directory if needed, then cecompress the lab12-files with the following command.

**# tar xjvf lab12-files.tar.bz2**

This creates a new directory called lab11-files. Change to this directory before proceeding with the rest of the lab.

**# cd lab11-files**

We will test snort with the following command:

**# snort -A console -q -c /etc/snort/snort.conf -S HOME\_NET=10.0.0.0/8 -r filename.pcap**

Where filename.pcap is replaced with the name of the file that contains the packets that we plan to use for testing snort.



3.1: Run snort using the command line above on both slammer1.pcap and slammer2.pcap. What output is generated for each pcap file? Write “no output” if no output is produced, indicating that snort did not alert on that pcap file.

|  |  |  |
| --- | --- | --- |
| **Slammer1.pcap** | | |
| Alerts Seen [Y/N] | Snort Alert Name | Classification/Priority |
| **No output** |  |  |

|  |  |  |
| --- | --- | --- |
| **Slammer2.pcap** | | |
| Alerts Seen [Y/N] | Snort Alert Name | Classification |
| **Yes** | **Slammer2.pcap** | **Alert** |

3.2: The bodies of both packets include the Slammer worm, but the headers differ. Examine the packet headers of both pcap files with tshark to find the answer.

* Why does snort alert on only one of the two slammer pcap files examined above? Be specific as possible in your answer to receive additional credit.

**# tshark -r slammer1.pcap**

**# tshark -r slammer2.pcap**

## Submission

Upload a completed copy of this document to Canvas by the due date.