TNE20003 – Internet and Cybersecurity for Engineering Applications

**Portfolio Task – Lab 9 Credit Task**

Aims:

* To observe and investigate port scanning and intrusion detection.

Preparation:

* View [“Introduction to Cybersecurity”](https://swinburne.instructure.com/courses/54168/pages/topic-9-intro-to-cybersecurity?module_item_id=3765162) & “[Cybersecurity”](https://swinburne.instructure.com/courses/54168/pages/topic-10-cybersecurity?module_item_id=3775875)

Due Date:

* All tasks in this lab are to be completed and demonstrated to your Lab instructor preferably during or at the end of the current lab, but if you do not complete the tasks you may demonstrate it at the beginning of your next lab class.

# Task 1

Get an understanding of the lab.

The purpose of this lab is to learn about port scanning and intrusion detection systems (IDS). We will use a popular port scanner to scan another machine which has been set up with a popular IDS to detect such intrusions.

This work is to be carried out using the virtual machines used in lab 1.

You will use the **Snort** IDS and nmap port scanning software. You will scan one host from another. The scanned host is to have **Snort** running to detect intrusions. Both **Snort** and **nmap** are already installed on the Virtual Machines you downloaded for lab 1.

You may be asked for a password. All passwords are ***user***.

**Task 2 - Host configuration**

The two hosts should have been configured with IP addresses in the Pass task.

Take note of the two IP addresses. (Use ifconfig.)

Check connectivity between both hosts with a ping.

**Task 3 - Testing Snort**

Once connectivity is established validate that Snort is working on VM1.

Open a command prompt window and type: *sudo snort -i 3 -c /etc/snort/snort.conf -T*

You should see a series of messages, the last of which are:

*Snort successfully validated the configuration!*

*Snort exiting*

This may take quite some time.

TNE20003 – Internet and Cybersecurity  Page 2

Lab 9 – Credit Task

## **Task 4 -** Add a rule to detect pings

At the moment snort has default rules installed that allow it to detect different attacks. We will add an additional rule that will cause it to detect and report pings.

Edit the Snort config file using gedit (or your favourite Linux editor) to add a local rule.

*sudo gedit /etc/snort/rules/local.rules* Add the following line:

*alert icmp any any -> any any (msg:"ICMP"; sid:1000001;)*

This will detect messages from any network to any network that is an ICMP. The rule number is 1000001.

Now run snort in intrusion detection mode reporting all exceptions to the console *sudo snort -c /etc/snort/snort.conf -A console*

From VM2 ping this host. You should see a notification of the pings.

## **Task 5 -** Testing the IDS with some common attacks

Nmap

Port scanning is used to identify vulnerable ports on a host. From VM2 do a port scan of VM1.

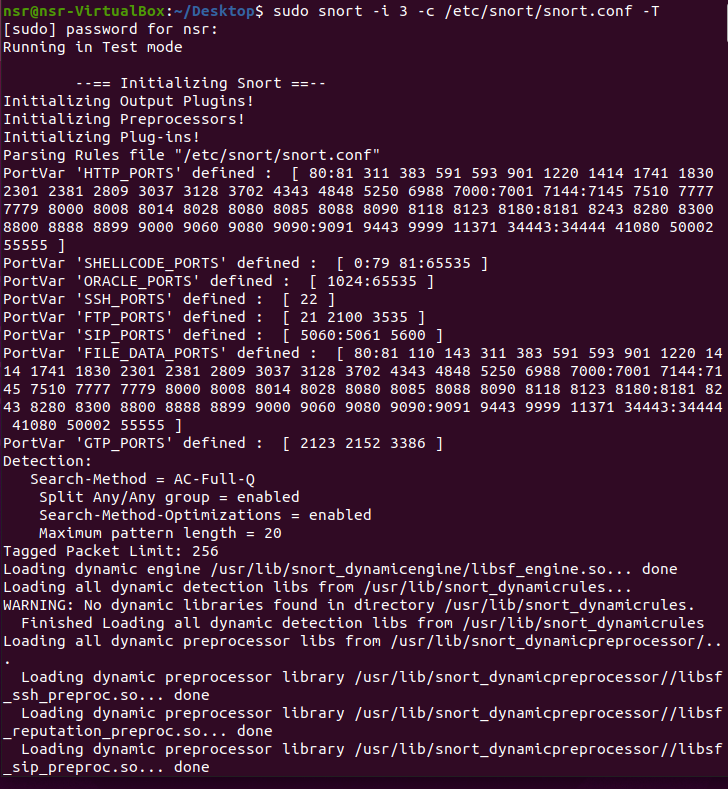
*nmap -system-dns -v -A ipaddress*

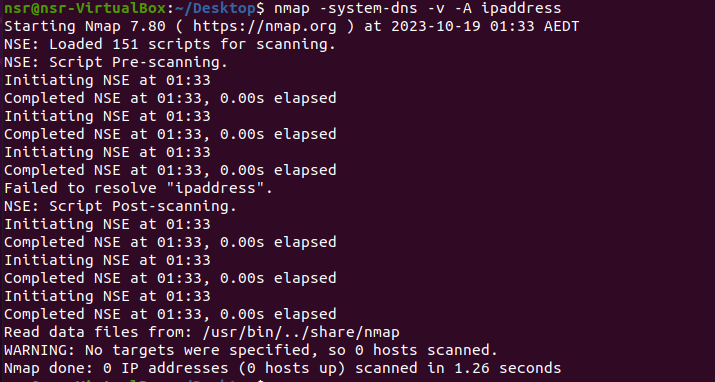
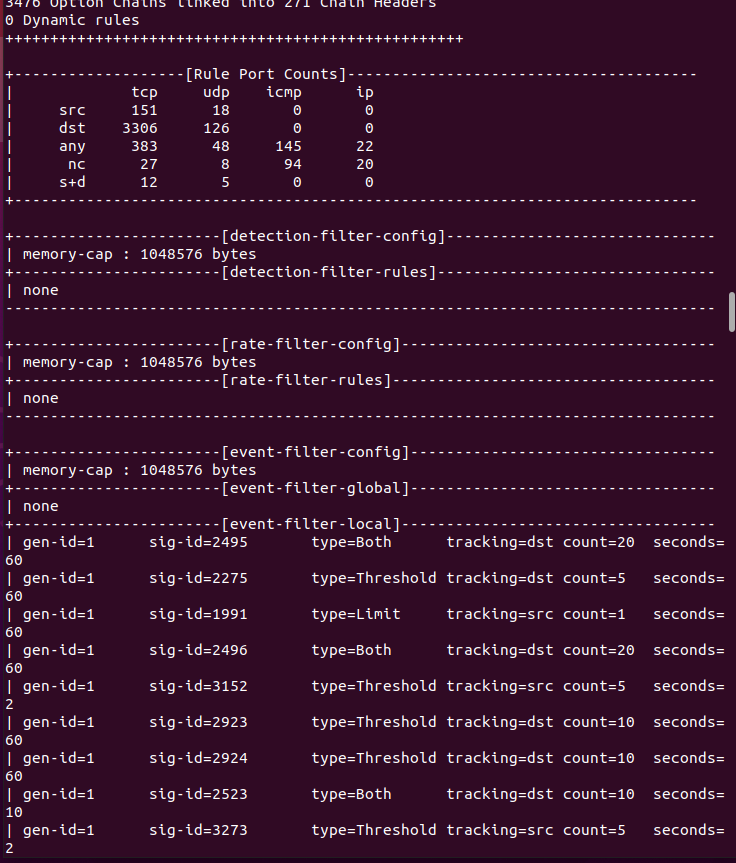
What information is shown as a result of the nmap output?

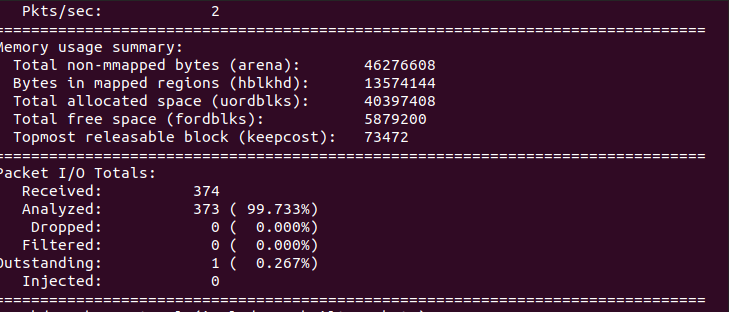
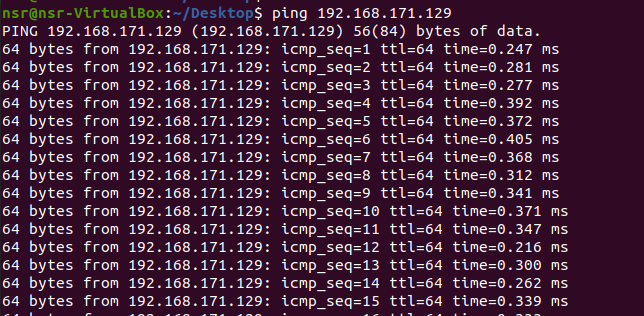
What messages did Snort generate as a result of the port scan? Use wireshark to identify some of them.

Tunnelling Attack

Use the hts and htc commands from the previous lab to see if tunnelling of telnet through http using can be detected by Snort.



A screenshot of a computer

Description automatically generated

## **Task 6 -** Assessment of this lab

Show the instructor that you have got Snort running and have carried out the attacks listed. The instructor will also ask you the following questions. The last two questions are particularly important.

1. What is port scanning?

Port scanning is the process of systematically scanning a computer's ports to find ones that are open or closed.

1. What is Intrusion Detection?

Intrusion Detection is the process of monitoring a network or system for suspicious or unauthorized activities or policy violations. It involves collecting and analyzing information from various areas within a computer or a network to identify potential security threats.

1. Why is port scanning a threat to an organisation?

Port scanning can be a threat to an organization because it can be the first step in identifying weaknesses in a network's security. Cyber-attackers use port scanning to discover open ports and services that may be vulnerable to exploitation. Knowing open ports can aid in launching targeted attacks, making it crucial for organizations to detect and respond to such activities.

1. Did Snort detect the tunnelling of telnet through port 80?

Snort is capable of detecting various types of network-based attacks and suspicious activities, including tunneling. However, successful detection depends on the specific rules and configurations in place. If Snort was properly configured and the tunneled traffic matched a defined rule, then it would have detected the tunneled telnet connection through port 80.

1. How should an organisation deal with port scanning in its security policy?

+ Implementing intrusion detection systems like Snort to detect and log scanning activities.

+ Defining procedures for responding to port scanning incidents, which may include blocking the scanning IP address.

+ Regularly scanning its own network to identify and address potential vulnerabilities.

+ Educating employees about the risks of port scanning and how to report suspicious activities.

+ Maintaining up-to-date security measures, including firewalls and access controls.

1. What might be some of the limitations of an Intrusion Detection System such as Snort?

+ False Positives: IDS systems may generate alerts for normal traffic, leading to unnecessary investigations.

+ False Negatives: IDS systems might not detect advanced or zero-day attacks that don't match existing patterns.

+ Resource Intensive: Snort requires processing power and memory, and monitoring high-speed networks can be resource-intensive.

+ Complex Configuration: Proper configuration and rule management can be complex.

+ Dependence on Signature Updates: IDS systems depend on timely updates to recognize new threats.

+ These answers provide an overview of the topics and considerations involved in Task 6. Specifics may vary depending on the organization's needs and security policies.

TNE20003 – Internet and Cybersecurity  Page 3

Lab 9 – Credit Task