Securing legacy systems Report ­­

Ayodele Esho

Student ID: 201499108

Contents

[Abstract 1](#_Toc103267334)

[Introduction 1](#_Toc103267335)

[Basic Tasks 1](#_Toc103267336)

[Questions 5](#_Toc103267337)

[Analyze Network Traffic 7](#_Toc103267338)

[Questions 8](#_Toc103267339)

# Abstract

Deter lab (Defense Technology Experimental Research Laboratory) is a computing facility used for cybersecurity researchers to engage in research. In this report I will be performing all the Basic tasks with a short description explaining how to complete task and what I have learned from the task.

# Introduction

This report is the detailed explanation of the laboratory session tasks created by Securing Legacy Systems – JHUISI. The task first begins with Snort. Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998.

# Basic Tasks

Start Snort Without Rules

1. Open an SSH client on your computer such as putty and connect to

users.deterlab.net

Graphical user interface, application

Description automatically generated

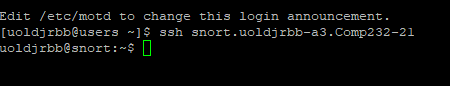
The SSH Client that I’m using is called Putty. I have entered the Hist name, which will allow me to connect to the server.

1. Login using your Deter username and password

Graphical user interface, text

Description automatically generatedOnce logged into the server with my details I am presented with this screen. The screen shows that. I am currently logged in and connected to my server.

1. SSH into snort. [experiment name]. [project name]



I have now SSH into my snort experiment. My location has now changed.



4. Start snort without any rules by entering the command "sudo snort --daq nfq -Q

-v".

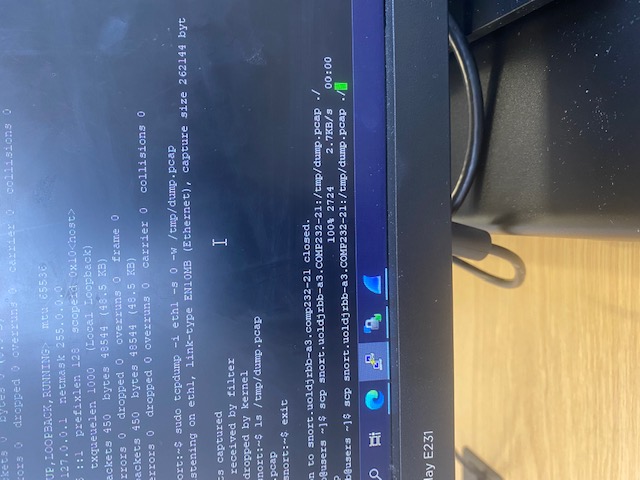
Once the command has been entered, I’m presented with this screen.

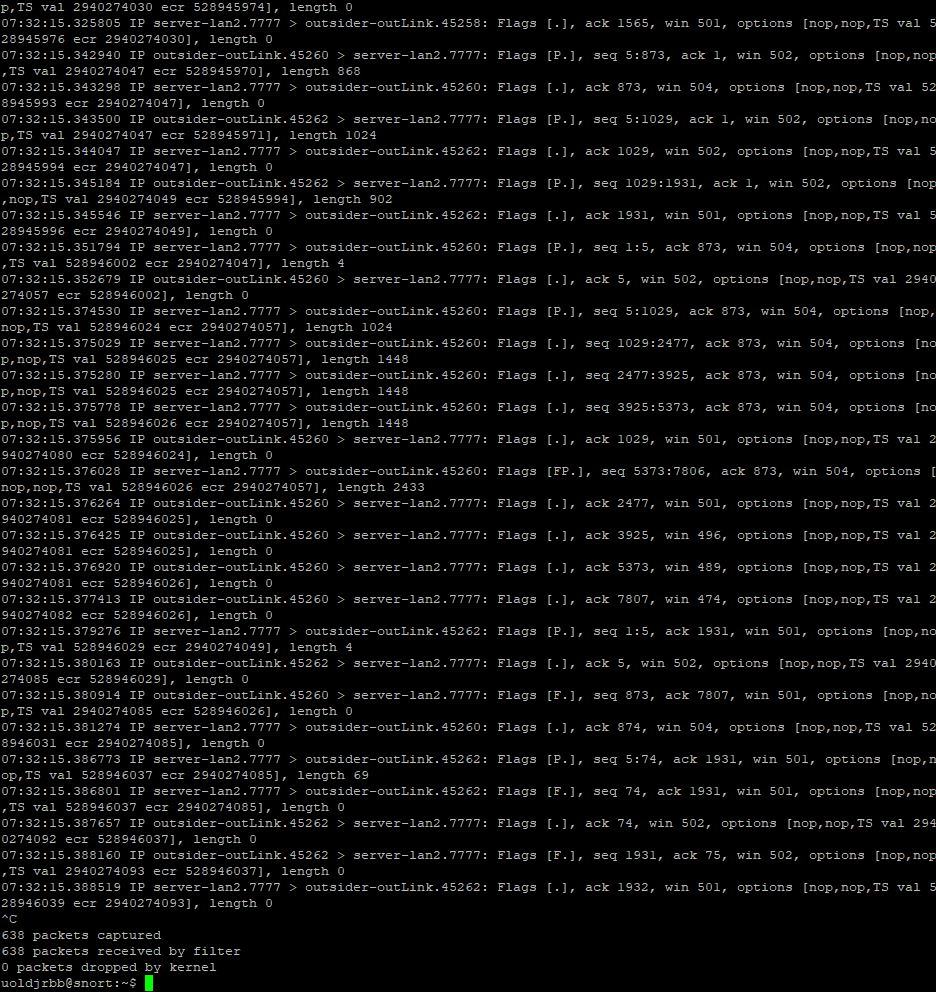
5. You should see a large number of packets being reported by Snort.

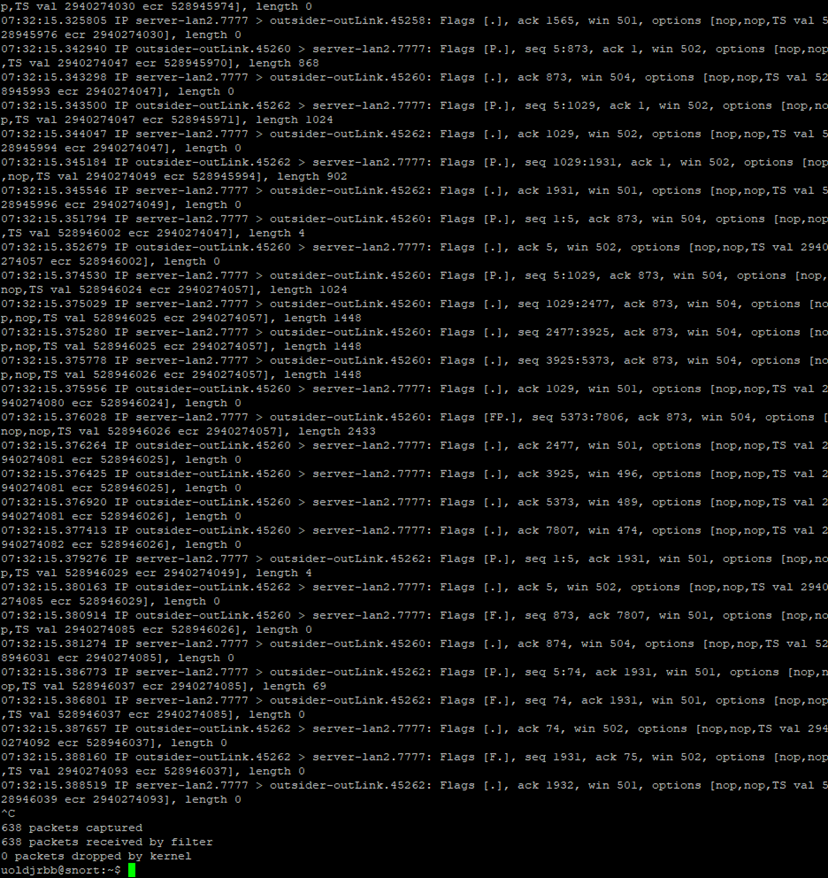
Here is a picture of the packets being reported by snort

6. Open another terminal and SSH again into users.deterlab.net and then snort.

In this terminal run tcpdump to capture the data







As shown 638 packets have been captured after running tcpdump

# Questions

1. What happens to the traffic to client1 when Snort is not running?
2. Is this a good thing?
3. Based on Snort's output what can you say about the application? What port does it connect to?
4. Please attach a graph of the traffic over time to your answers



1. What does the "-Q" option do in Snort?

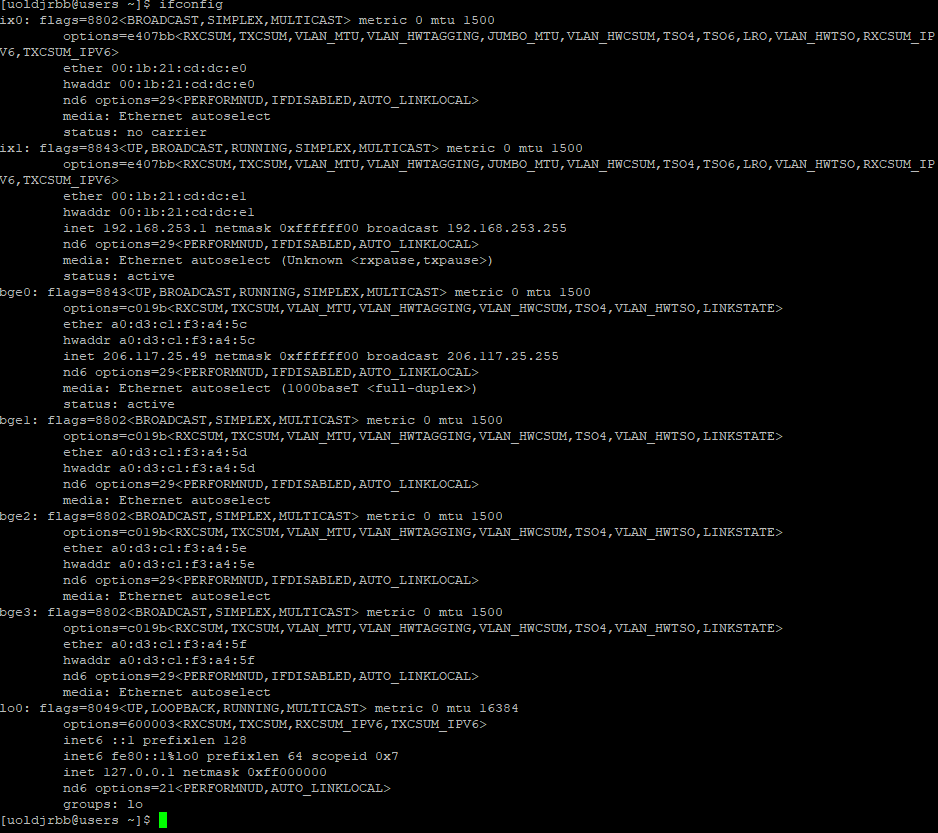
The “-q” option is snort stands for quite mode

1. What does the "--daq nfq" option do in Snort?

The command “—daq nfg is used to confirm that nfq is ready to drop traffic.

# Analyze Network Traffic

1. Connect to router. [experiment name].[project name]
2. Use ifconfig to determine which network interfaces connect to which network.



Once ifconfig is ran this is the output.

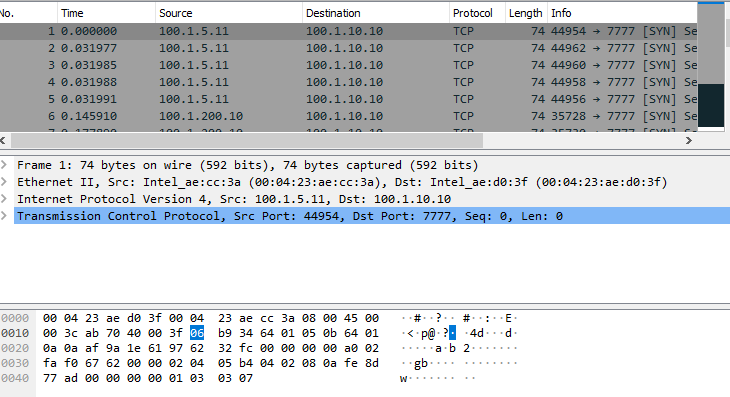
3. Run tcpdump to capture the data going to the server. This should be on the

interface with an IP Address in the 10.0.1.0 / 24 range. You can run tcpdump using

the command "sudo tcpdump -i [interface] -s 0 -w /tmp/dump.pcap"



1. Let this run for around a minute before terminating it by pressing control + c.
2. Copy this data to your computer via SCP and open it using Wireshark. You can use a tool like WinSCP to accomplish this.



# Questions

5. The request that the client sends the server is broken into four parts. What are

these parts and what order do they appear in? How are these parts separated in?

the request?

* URL
* Method
* Headers
* Body