**Student Name:** **Coleton Sanheim Weight: \_\_\_\_2.0\_\_\_\_%**

**Student ID: 000862545**  **Marks: \_\_\_\_\_\_\_\_\_\_**

Lab 7: IDS/IPS – pfSense and Snort

# Learning Outcomes

* Perform basic IDS/IPS configuration, use setup document.
* Configure and analyze IDS and IPS policies.

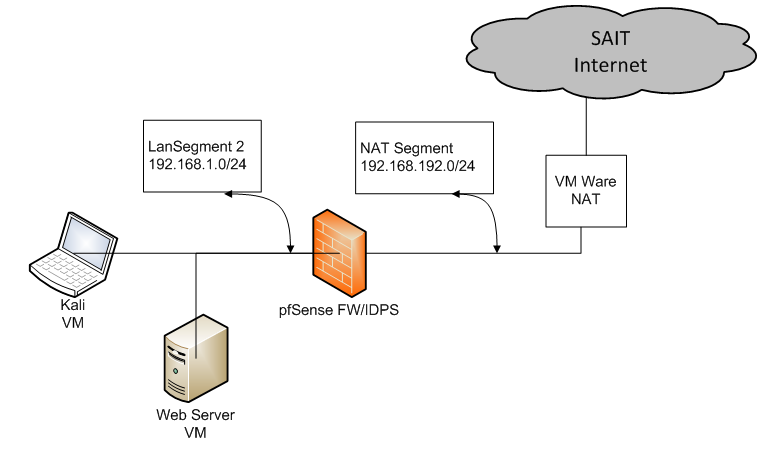
# Purpose

In this lab, you will use an open source IDS called Snort to watch for suspicious intrusion events.

# Tools

* pfSense VM (192.168.1.1) w/ Snort package
* Kali (192.168.1.98)
* VM web server (Ubuntu – 192.168.1.2)

# Topology



© 2017, Southern Alberta Institute of Technology

# Setup

Before you begin the lab activities, perform the steps below to set up your computer.

1. Set up a Ubuntu workstation in a VM using ISO with the following parameters:

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT
* Latest version of Wireshark with Winpcap

Reconfigure the network adapter:

* Change network adapter to LAN Segment 1 in the VM console
* Configure the IP address to: 192.168.1.2/24
* Configure the gateway to: 192.168.1.1

1. Install an Ubuntu web server by entering the following commands:
   * sudo apt install apache2
   * sudo apt install net-tools
2. Set up Kali in the VM using ISO with the following parameters:

* 3 CPU
* 4 GB of RAM
* 40 GB HDD
* Network Adapter: NAT
* Configure the IP address to: 192.168.1.98
* Configure the gateway to: 192.168.1.1

1. Set up an pfSense Firewall VM using ISO with the following parameters: (as per Lab 6 guide)

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT (WAN)

Reconfigure the network adapter:

* Change network adapter to LAN Segment 2 in the VM console
* Configure the IP address to: 192.168.1.1/24 (LAN)
* Configure the gateway to: NAT
* Change setting in /etc/network/interfaces
* Reboot server for the new IP address to take effect

1. Set up pfSense VM with Snort as per Lab 7 Setup document.

Update Snort rules

* Update snort rule with "sudo rule-update"

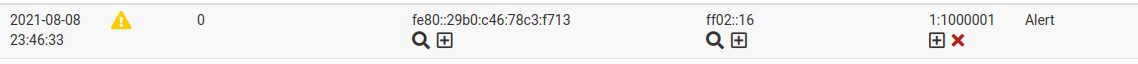
# Activities

## Open Event console

1. On your Ubuntu desktop or Kali, open pfSense Web Console and enter your username and password. Goto Services -> Snort -> Alerts

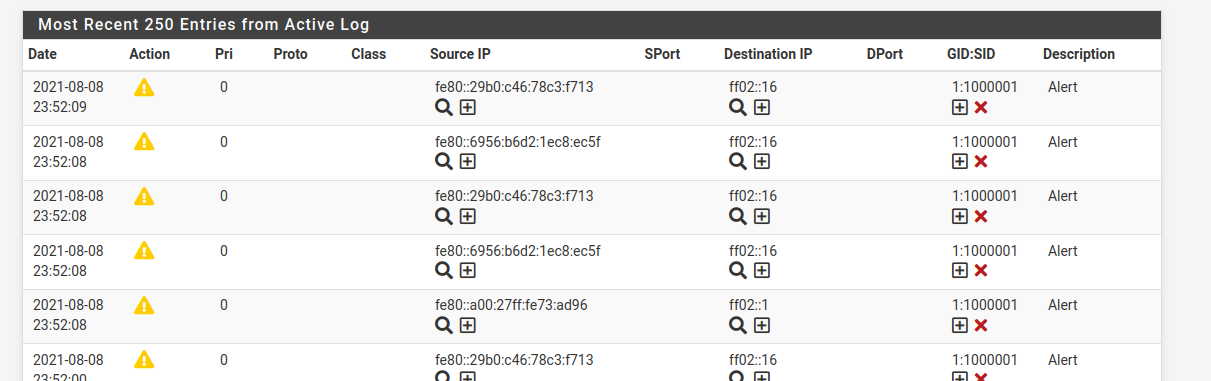
## Review the Security Event dashboard

Click any event and study the Snort rule, source and destination IP, and the activity that caused the event to trigger.



## Generate a security event in Snort

1. On the VM workstation, start Wireshark and listen for all traffic.
2. On the VM web server, confirm that the web server is running.
3. Open a terminal in Kali and send a ping to the web server.
4. Demonstrate that the ping triggered a signature in Snort.



Question: What is the name of the signature triggered?

Answer: \_\_\_**1:1000001**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**^ this is the custom SID we defined because it wasn’t catching anything otherwise**

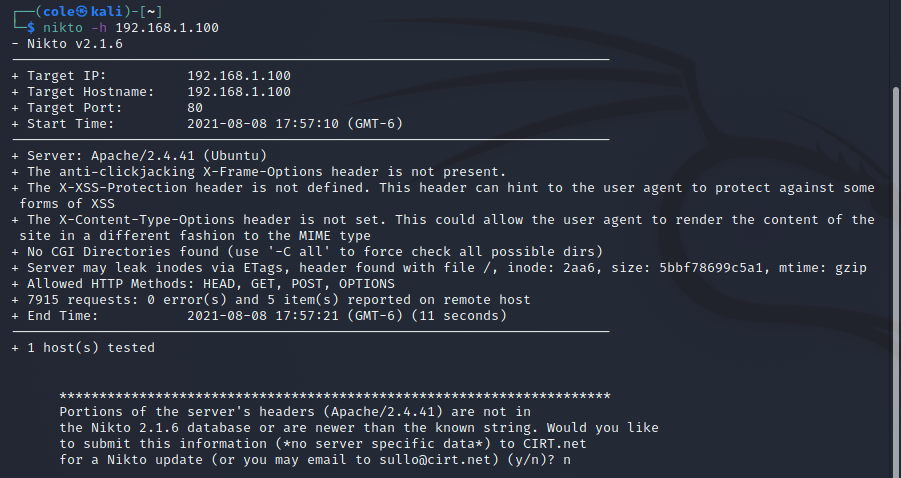
**Note that because of this, all snort security events are going to look similar**

## Scan the VM web server

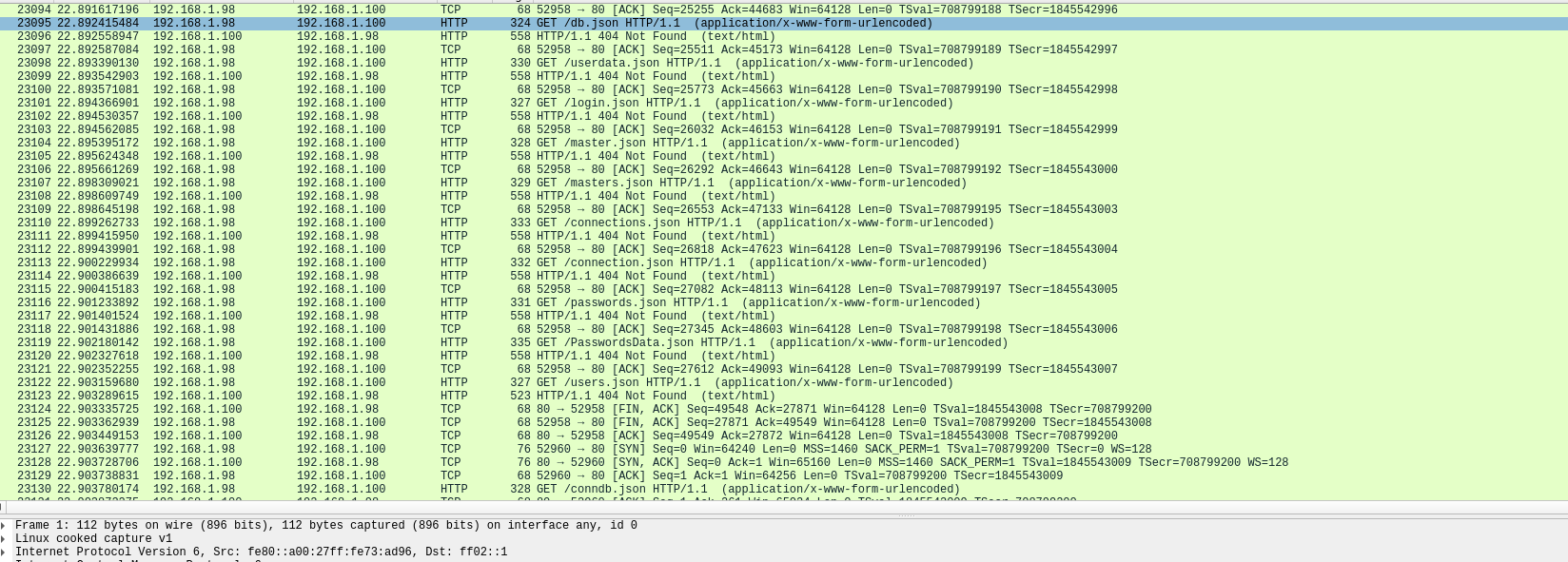
1. Open a terminal in Kali and issue the following command:

# nikto -h 192.168.0.2

1. Demonstrate the scan result for the web server scan.



1. Demonstrate the Wireshark packets for the web server scan.

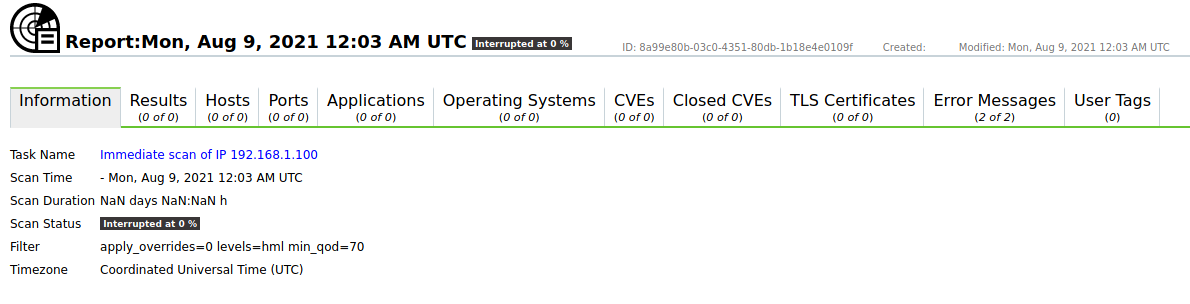


1. Demonstrate the security events triggered in Snort

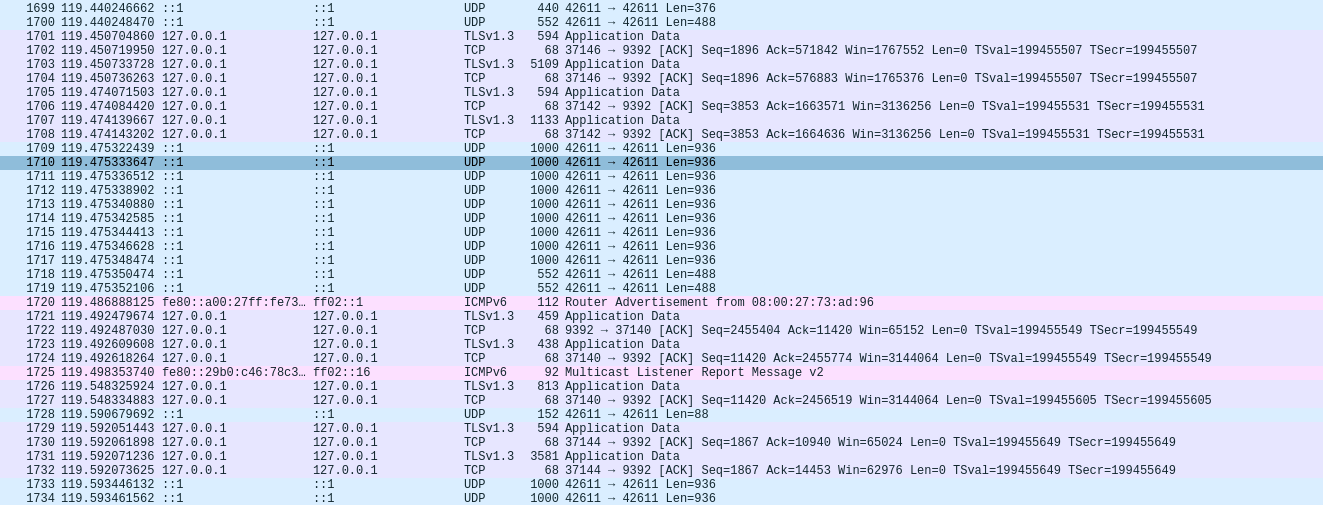


## Scan the VM web server

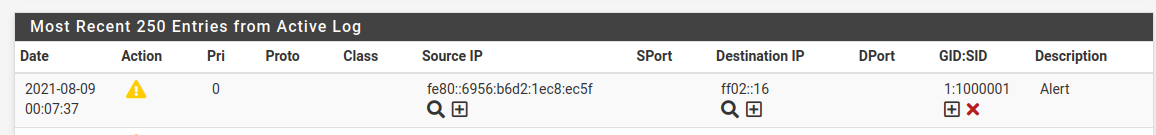
1. Using Kali, start Wireshark, open browser and bring up OpenVAS and perform scan on web server.



1. Demonstrate some of the Wireshark packets from the scan.



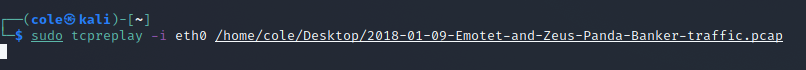
1. Demonstrate the security events triggered in Snort.



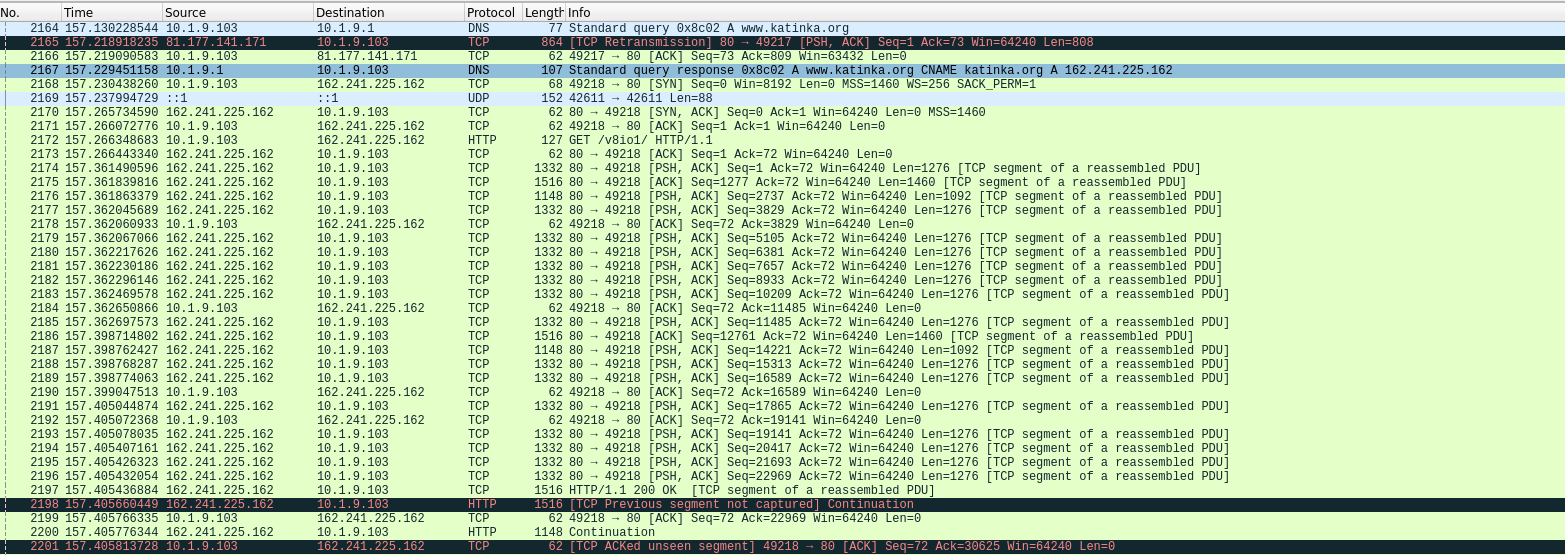
## TCPreplay of a Trojan

1. Using Kali, start Wireshark, open a terminal window and issue the following command:

$ sudo tcpreplay -i eth1 /home/zeus-sample-1.pcap



1. Demonstrate the Wireshark packets for the TCPreplay.



1. Demonstrate the security events triggered in Snort.

