

JW4158-INFO8590-22S-Portfolio-2

John White

6714158

INFO8590

Table of Contents

Lab 3 - Network Security Monitoring	3
Description.....	3
Preparation	3
Observations	4
Screenshots.....	4
Reflection.....	7
References	8
Lab 4 – Network IDS and IPS Tools	9
Description.....	9
Preparation	9
Observations	9
Screenshots.....	10
Reflection.....	16
References	16

Lab 3 - Network Security Monitoring

Description

The purpose of this lab is to teach us how to perform a security scan of a network using GVM on Kali Greenbone. We will be comparing the results of scanning the network scan to the results of scanning a Windows laptop with it's firewall disabled.

Preparation

Because the Kali Linux template is broken on VSphere, I will perform this scan on my home network which includes my home router, my laptop, and a Kali VM running on the laptop. The IP configuration of my laptop and my Kali VM is shown in the screenshot section below.

After creating the Kali VM, these are the commands I ran in the terminal to install GVM and perform my scans:

```
sudo su
```

```
apt update
```

```
apt upgrade
```

```
systemctl enable ssh.service
```

```
apt install openvas
```

```
apt install gvm
```

```
gvm-setup (make sure you note down the password given at the end)
```

```
gvm-stop
```

```
gvm-feed-update
```

```
gvm-start
```

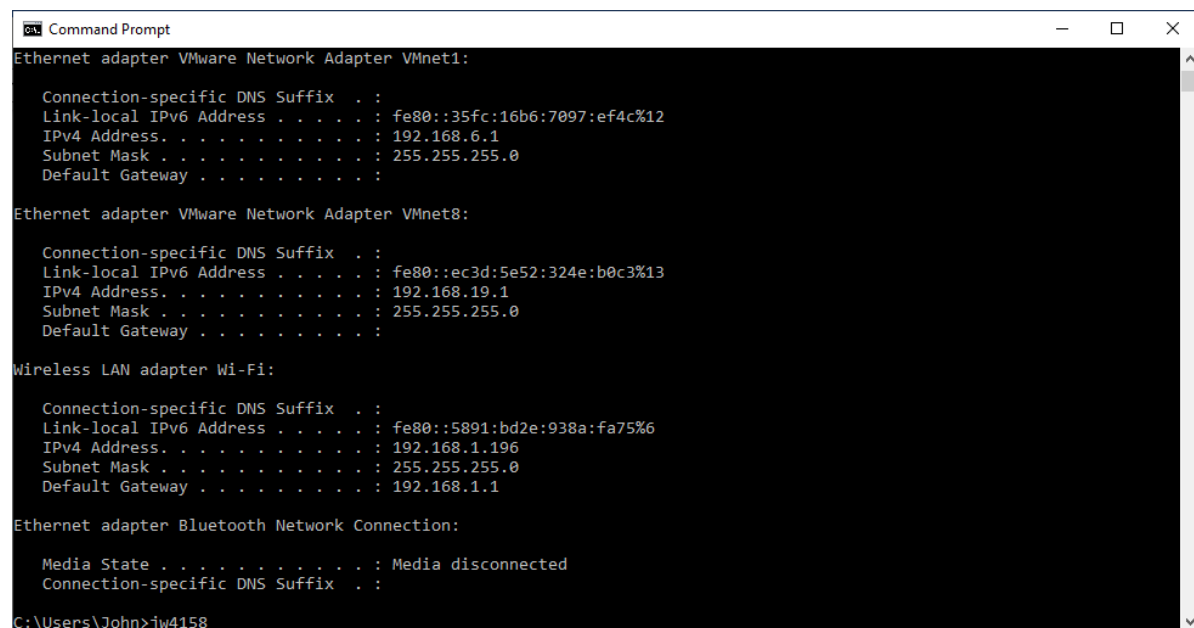
After this, the web page for GVM should automatically open. If it doesn't, navigate to 127.0.0.1:9392 and log in with the username: 'admin' and the password that was generated at the end of gvm-setup. Once we are logged in, we should confirm that our scan configurations have loaded. Go to Configuration > Scan Configs and wait for the list to populate. If this doesn't happen after a few minutes, refer to the Reflections section below for the solution that worked for me.

Observations

The first thing we will do is set up our targets. Go to Configuration > Targets and add a new target by clicking the 'New Target' icon in the top-left. Then, give it a name and put the desired IP or IPs in the 'Hosts' field. My targets are screenshotted below.

Next, we need to create our scan tasks. Go to Scans > Tasks and create a new task. Give it a name, specify the target, and check off the schedule box that says 'Once'. Once this is saved, run the task and wait for it to be completed. After the scan of the home network was done, I turned off the firewall on my Windows Laptop and scanned it's IP address afterwards. The results of both scans are below.

Screenshots



```
Command Prompt

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::35fc:16b6:7097:ef4c%12
    IPv4 Address. . . . . : 192.168.6.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::ec3d:5e52:324e:b0c3%13
    IPv4 Address. . . . . : 192.168.19.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

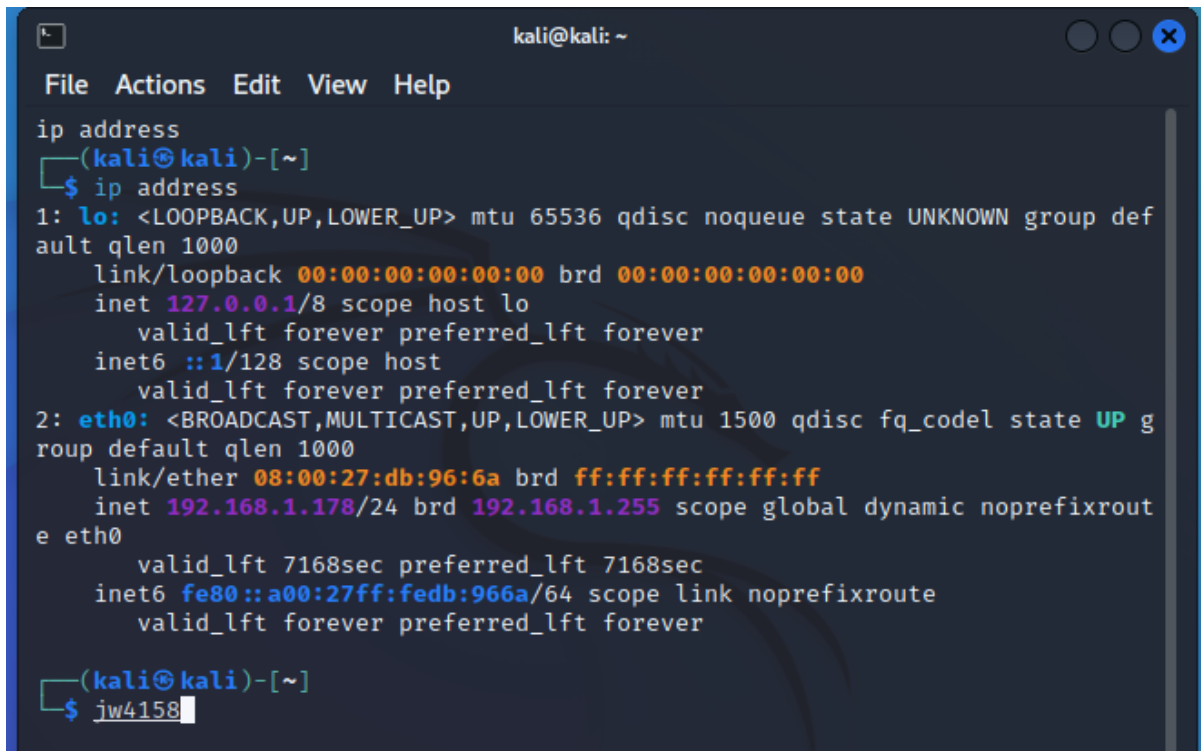
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5891:bd2e:938a:fa75%6
    IPv4 Address. . . . . : 192.168.1.196
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\John>jw4158
```

Figure 1.1 - Laptop IP configuration



```

kali@kali: ~
File Actions Edit View Help

ip address
(kali@kali)-[~]
$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  aut qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
  roup default qlen 1000
    link/ether 08:00:27:db:96:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.178/24 brd 192.168.1.255 scope global dynamic noprefixrou
  t eth0
        valid_lft 7168sec preferred_lft 7168sec
    inet6 fe80::a00:27ff:fedb:966a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ iw4158

```

Figure 1.2- Kali IP Configuration

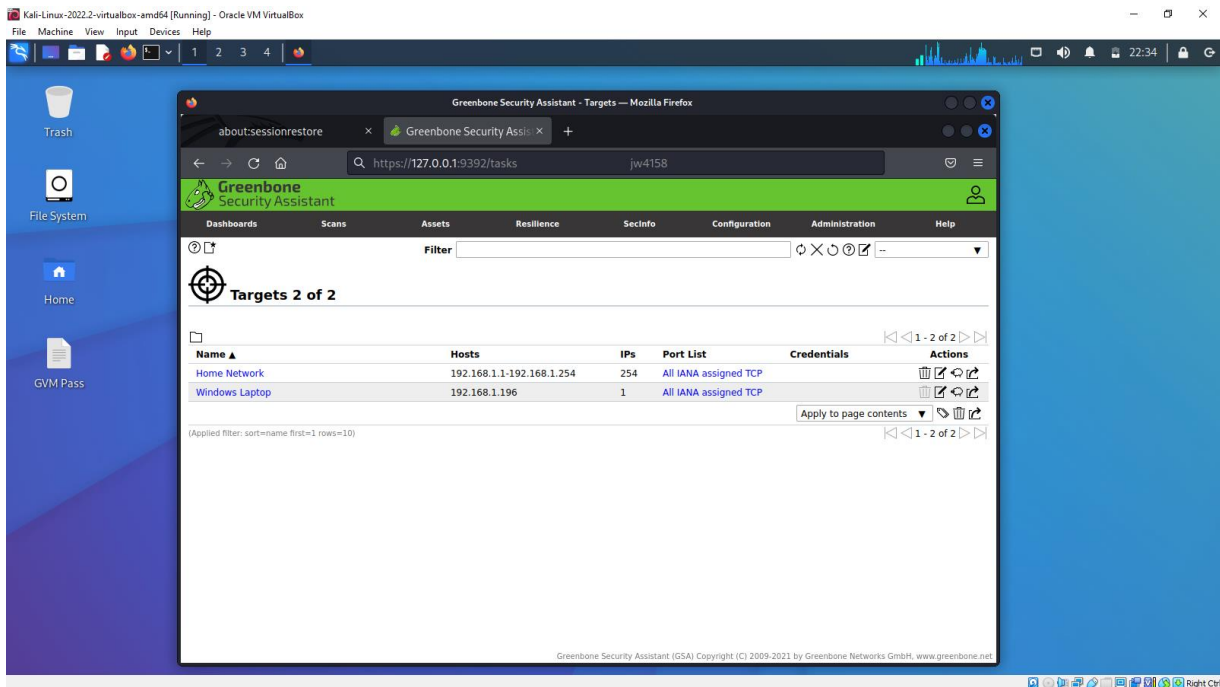


Figure 1.3 - GVM Targets

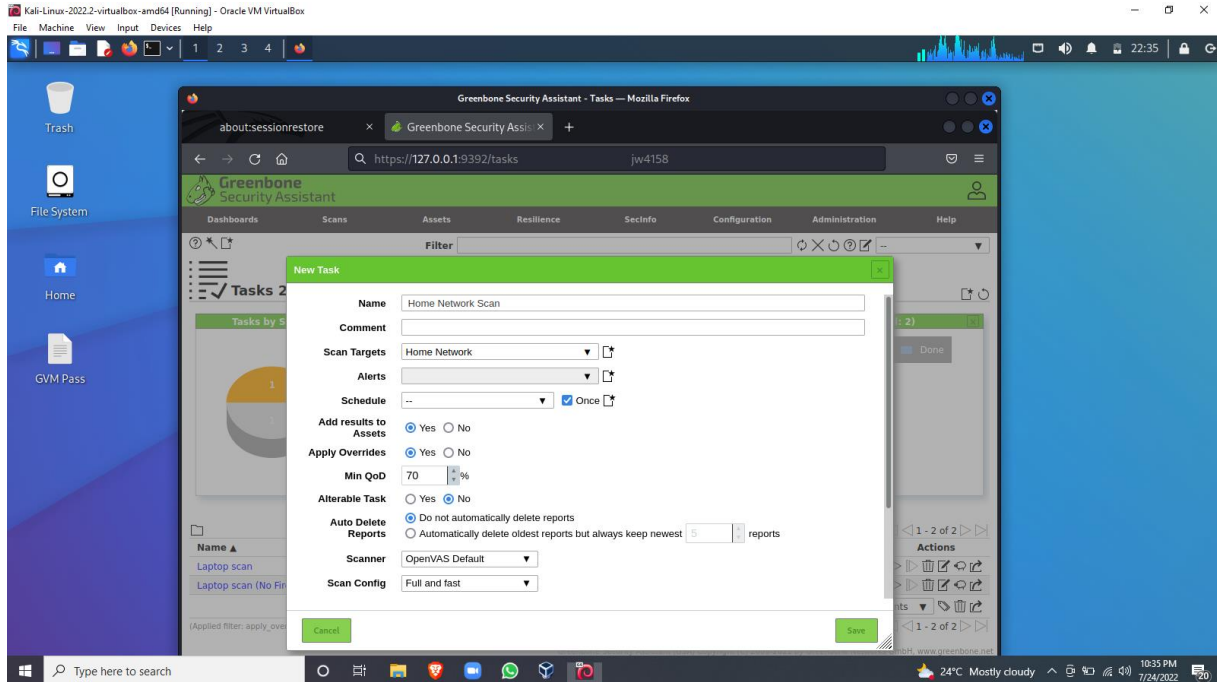


Figure 1.4 - Task settings for Home Network Scan

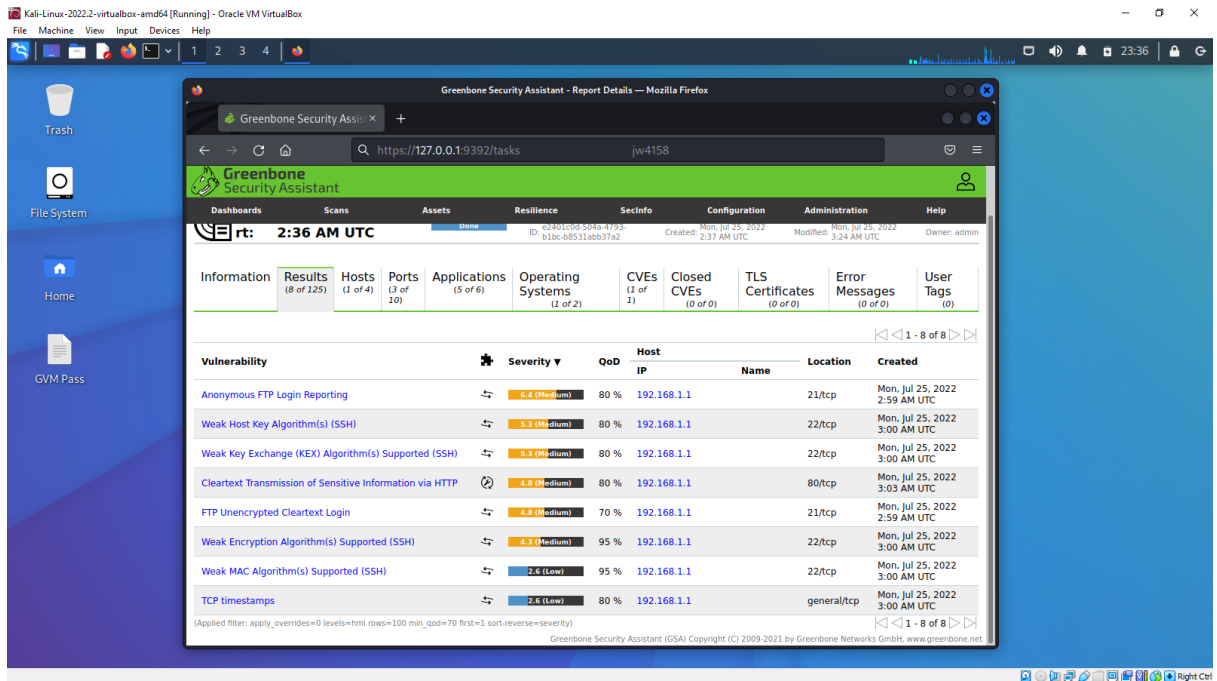


Figure 1.5 - Home network scan results

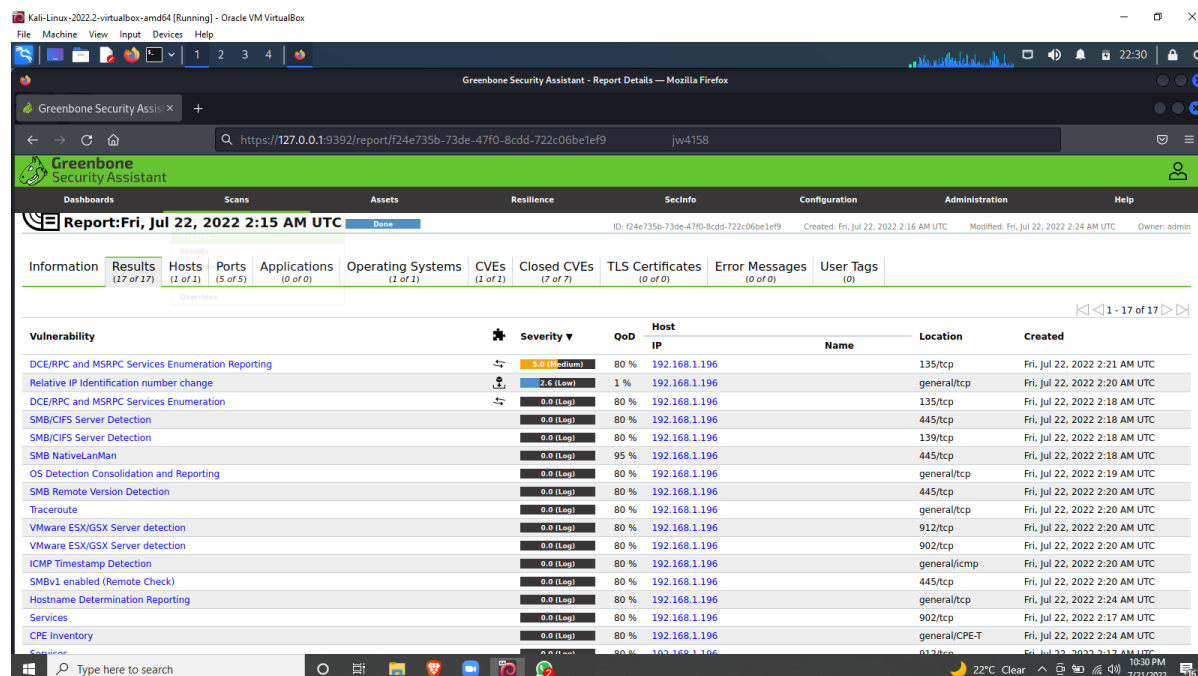


Figure 1.6 - Results from scanning the Windows laptop without the firewall

Reflection

When I configured Kali on VirtualBox, the issue I ran into was that my Scan Configs would not populate no matter how long I waited and creating any new one or trying to create a new task would result in a missing file error. To fix this, I ran the following commands in the terminal:

```
sudo su
gvm-stop
greenbone-feed-sync --type GVM_DATA
greenbone-feed-sync --type SCAP
greenbone-feed-sync --type CERT
gvm-feed-update -h
gvm-start
```

After this, they appeared immediately. I also tried to configure a Kali VM on vSphere but I was not able to run 'apt update' despite being able to ping kali.org from the terminal successfully. As such, I only performed a GVM scan on my home network rather than on pfSense. Based on the results of the scans, I would say that most of my network vulnerabilities are on my router. This makes sense as it is the device that is connecting to the outside network. The laptop seems to have only a few minor vulnerabilities unless the firewall is turned off.

Within organizations, GVM and similar tools are usually used for penetration testing. By testing the exploitability of these vulnerabilities, an organization can get a better sense of which areas of security they need to focus on or find specific flaws that need to be fixed right away.

References

1. eConestoga, 2022 (Lab 3 – Network Security Monitoring, retrieved from <https://conestoga.desire2learn.com/d2l/le/content/591148/viewContent/12779237/View> on July 24, 2022)

Lab 4 – Network IDS and IPS Tools

Description

The purpose of this workshop is to get us to learn how to configure an intrusion prevention system. We will be using Suricata and Snort for this.

Preparation

To prepare for this lab, we will need to set up a pfSense router and a Windows desktop to configure it from. The upstream LAN address for the router will be 10.175.68.1. The rest of the IP addresses should be configured as shown in the screenshots below. In general settings on pfSense, set the DNS server to 8.8.8.8. We are now ready to install the IPS packages.

Observations

First, we will install and configure Suricata. Go to System > Package Manager > Available Packages and search for 'Suricata'. Install the only result. Once it is installed, we must configure it. Go to Services > Suricata and Add an interface. Next, under the Global Settings tab, configure Suricata as shown in Screenshots section below. Now that we have specified which rules we want, we now need to download the rules. Head to the Updates tab and click update. Now that we have the rules downloaded, we must enable them. Head back to the Interface Tab and edit the WAN interface we made earlier. Under the WAN Settings tab, configure as shown below. Next go to the WAN Categories tab, enable all the rules, and hit save. For the last step, go back to the Interfaces page and start the service on our WAN interface that we made. Suricata should now generate alerts when the rules are violated.

The process for installing and configuring Snort is very similar to the instructions above. Download and install Snort from the package manager, add a WAN interface, and configure the Snort Global Settings to specify the rules we want and to enable Snort to push messages and alerts to our firewall log. Then we just need to download the rules, enable them, and start the service on our WAN interface. I have included screenshots of the Global Settings page for Snort since it differs somewhat from Suricata.

Screenshots

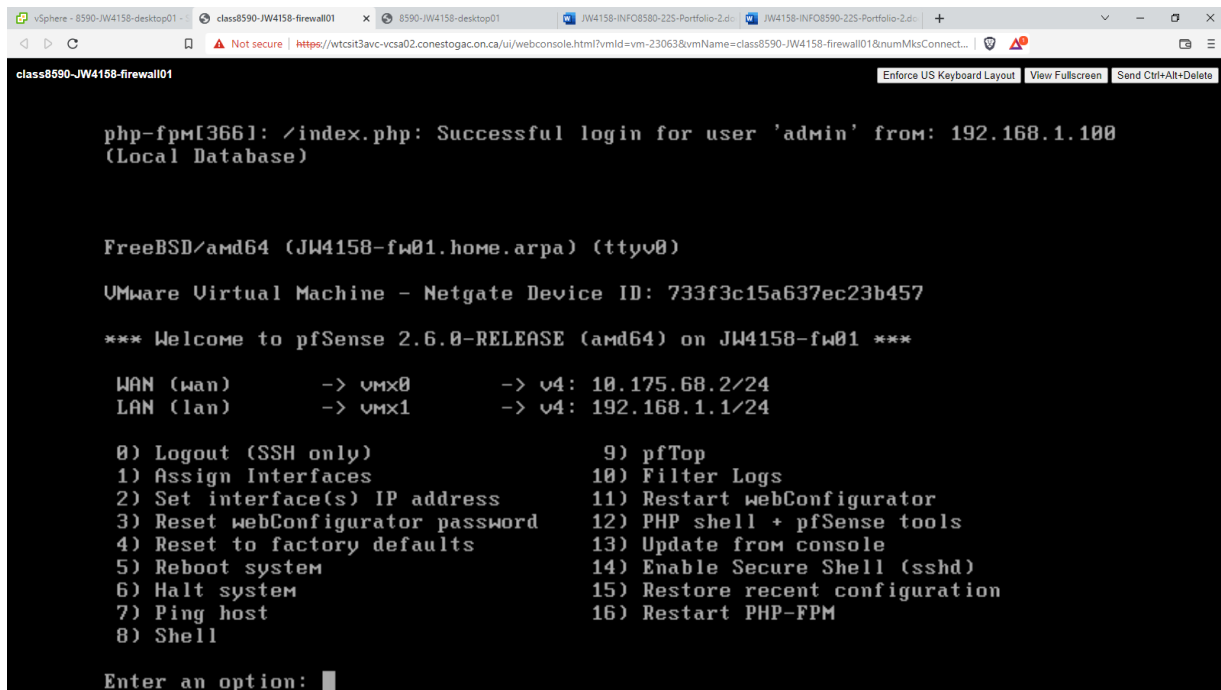


Figure 2.1 - pfSense router IP configuration

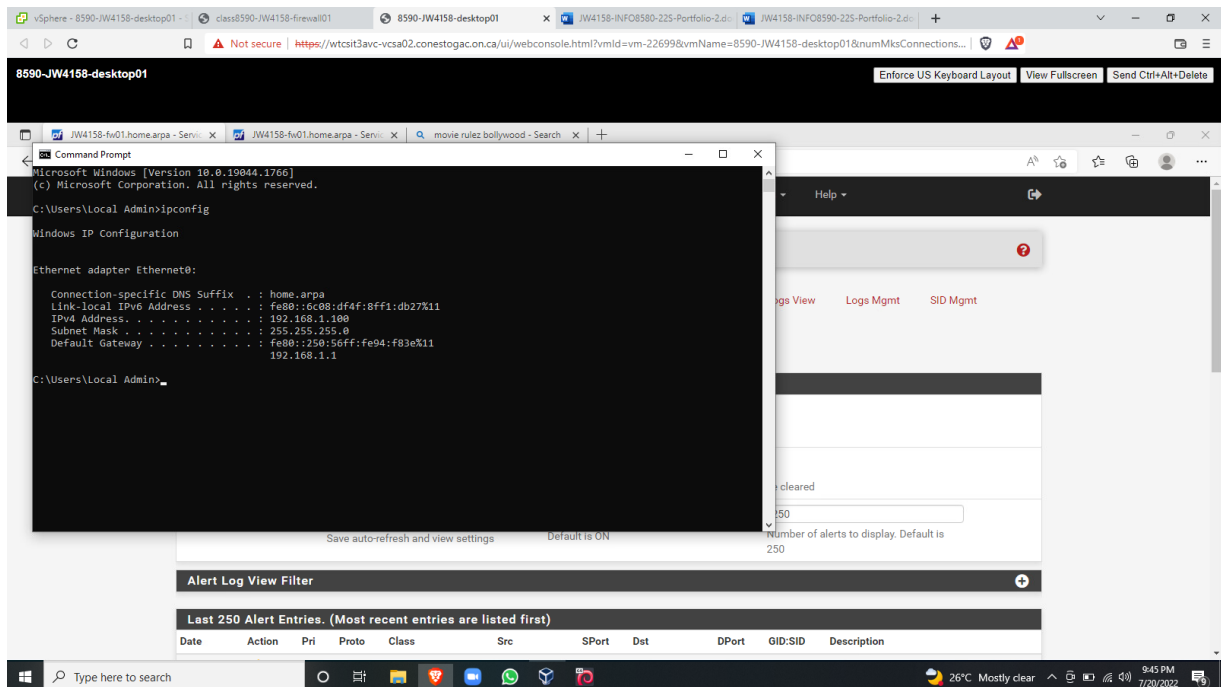


Figure 2.2 - Windows desktop IP configuration

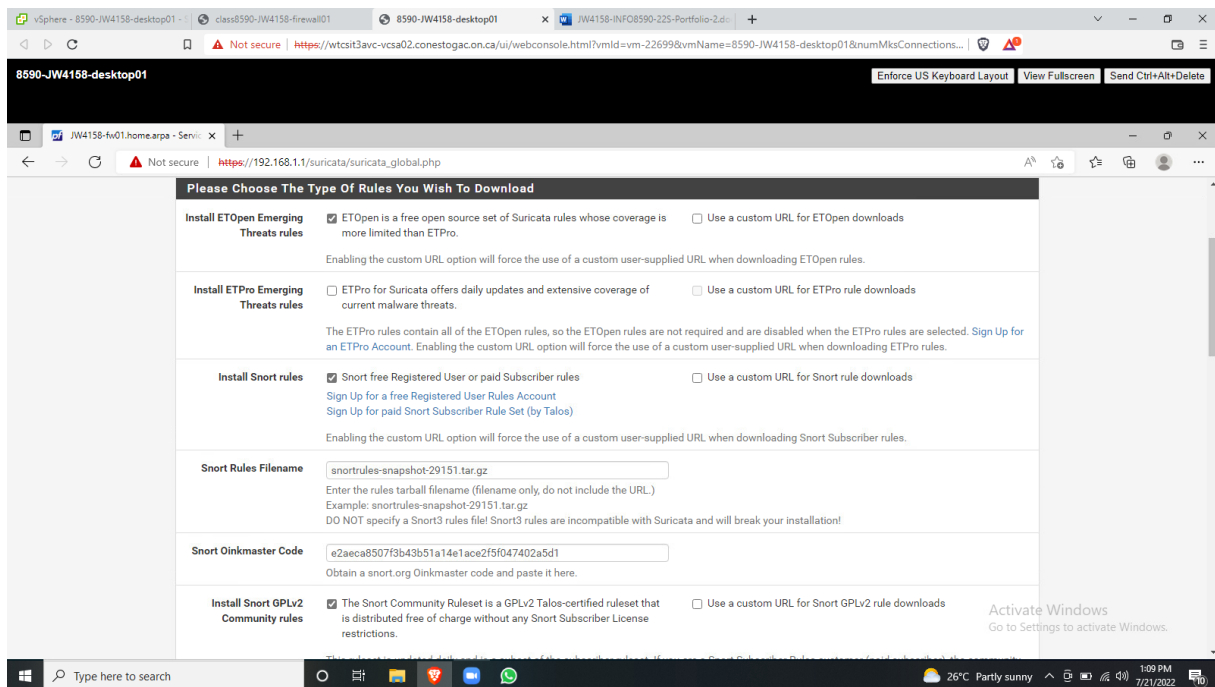


Figure 2.3 - Suricata Global Settings Part 1

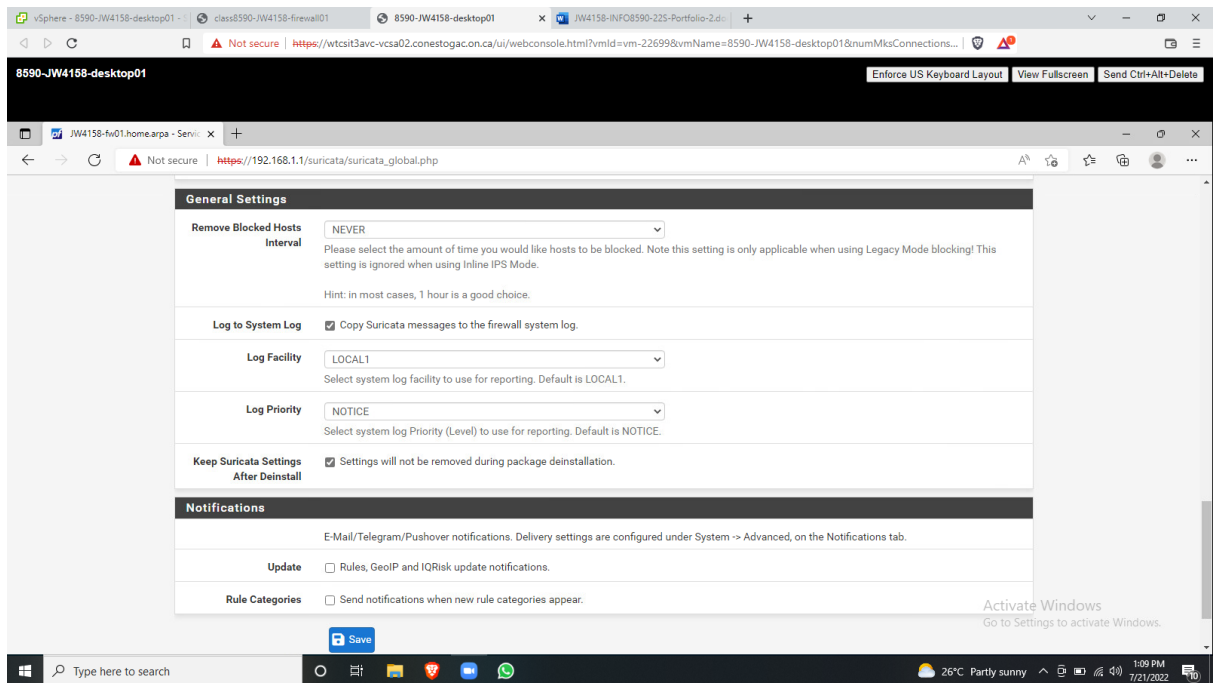


Figure 2.4 - Suricata Global Settings Part 2

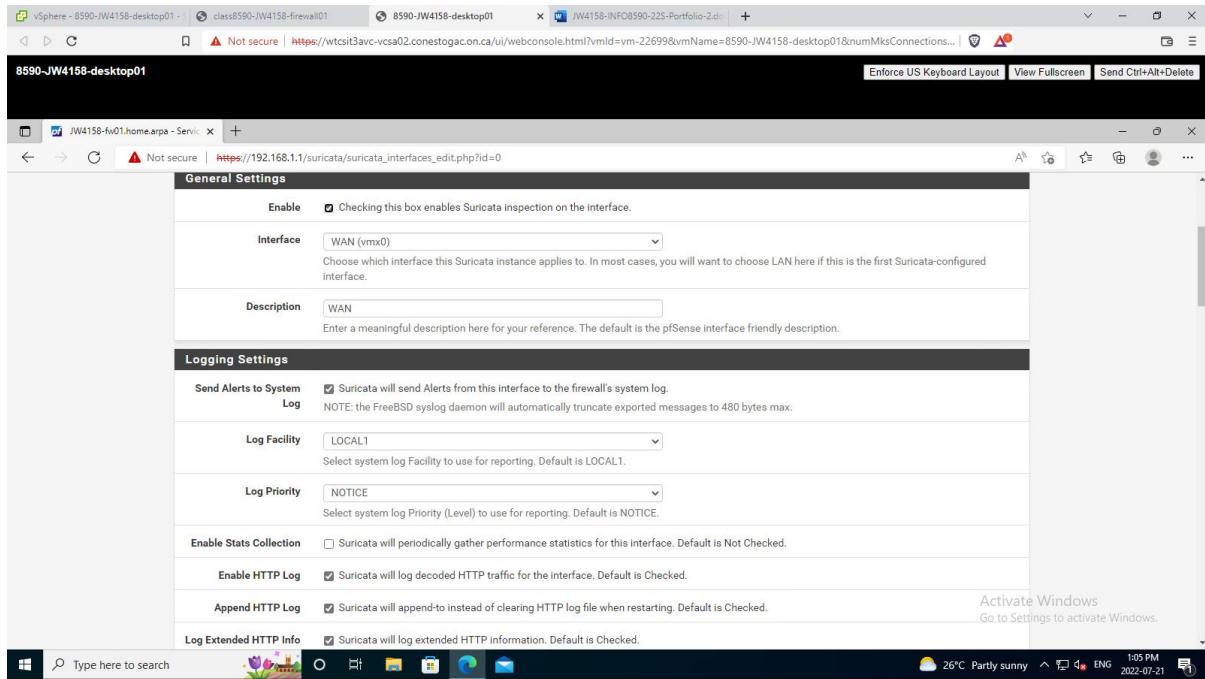


Figure 2.5 - Suricata WAN Settings Part 1

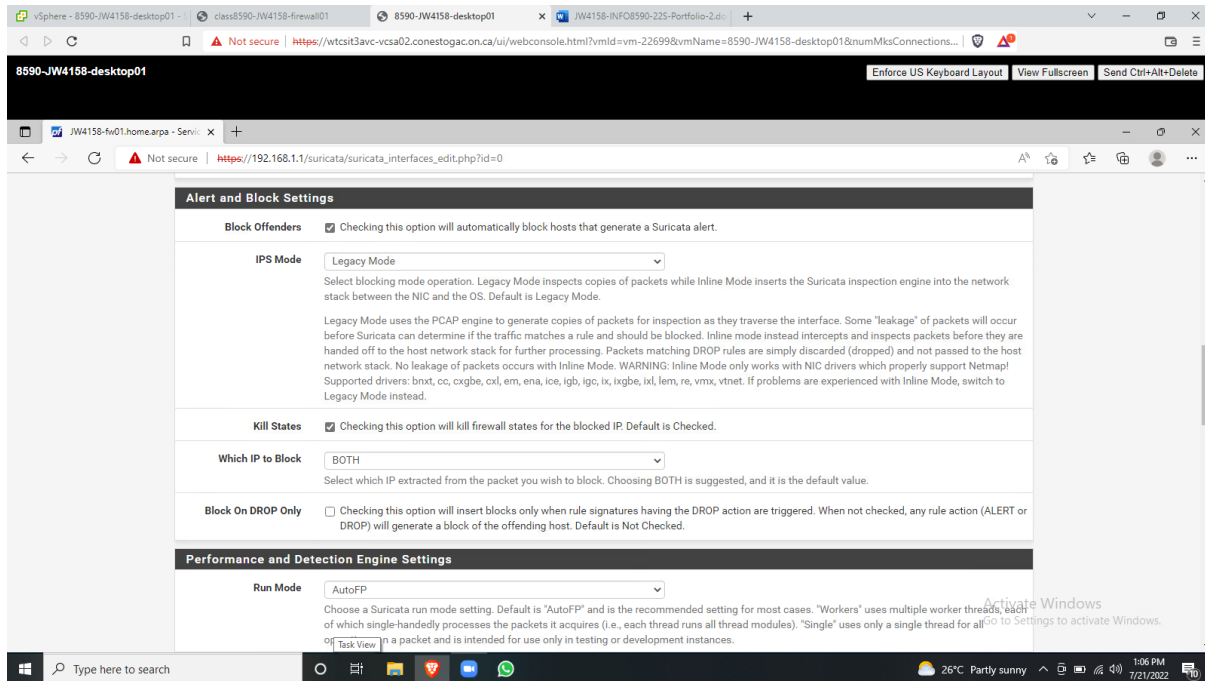


Figure 2.6 - Suricata WAN Settings Part 2

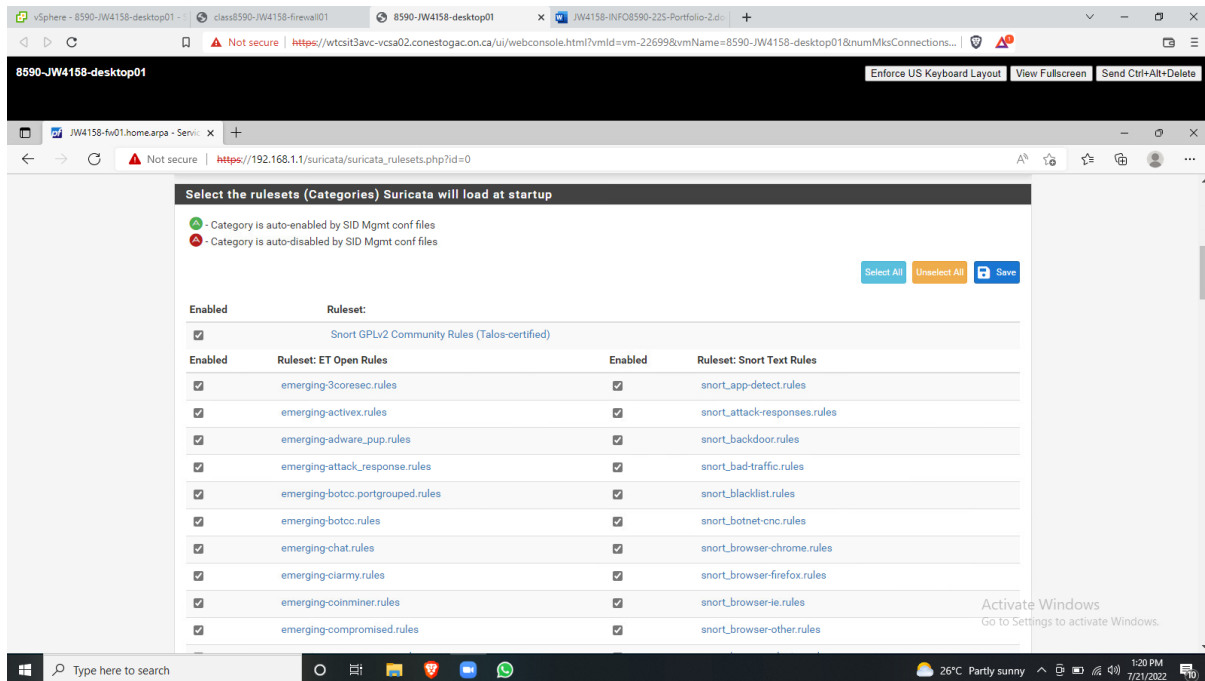


Figure 2.7 - Suricata - Enabling the rules in WAN Categories

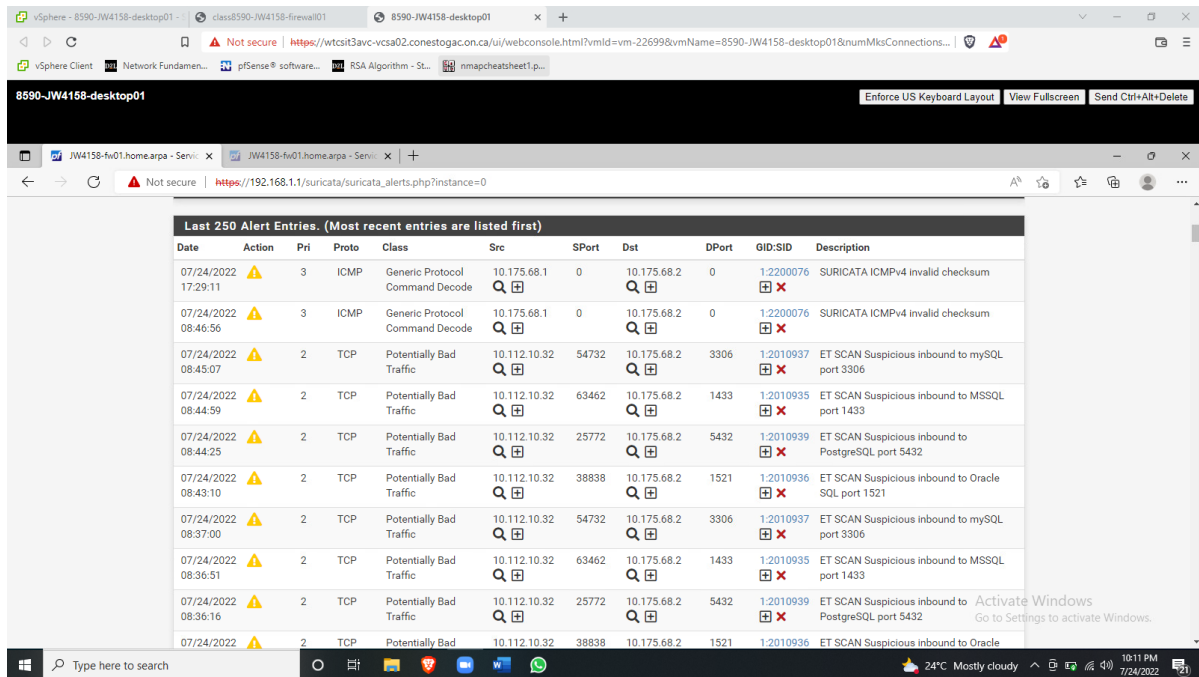


Figure 2.8 - Suricata Alerts

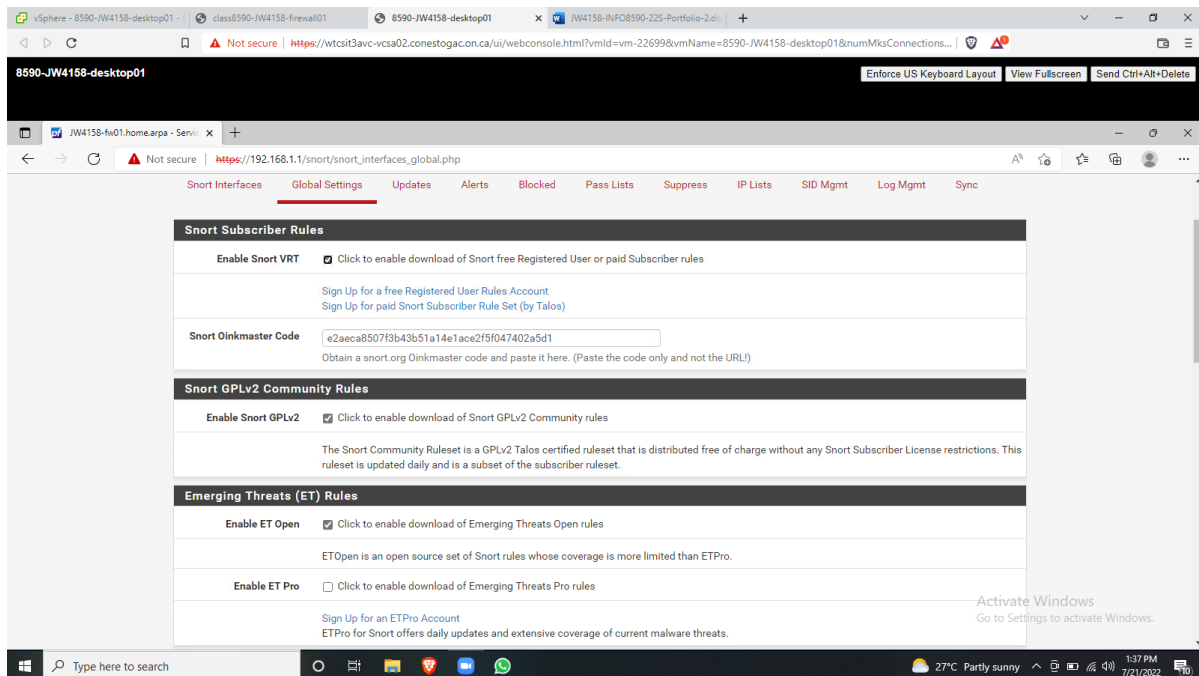


Figure 2.9 - Snort Global Settings Part 1

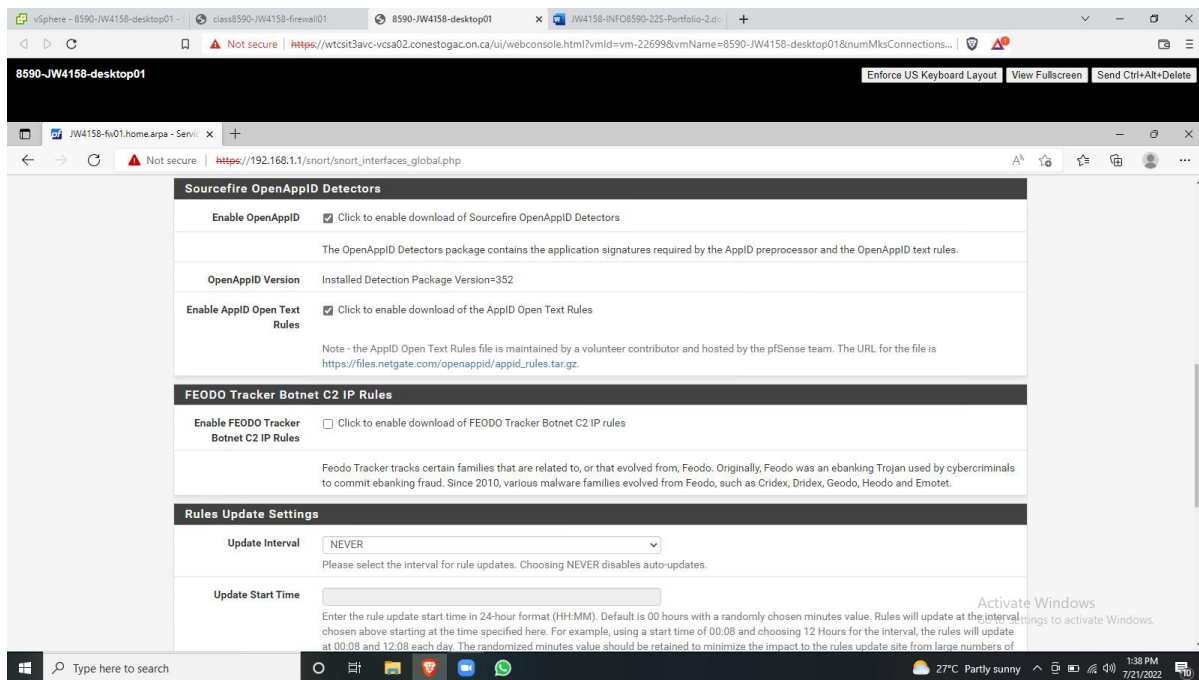


Figure 2.10 - Snort Global Settings Part 2

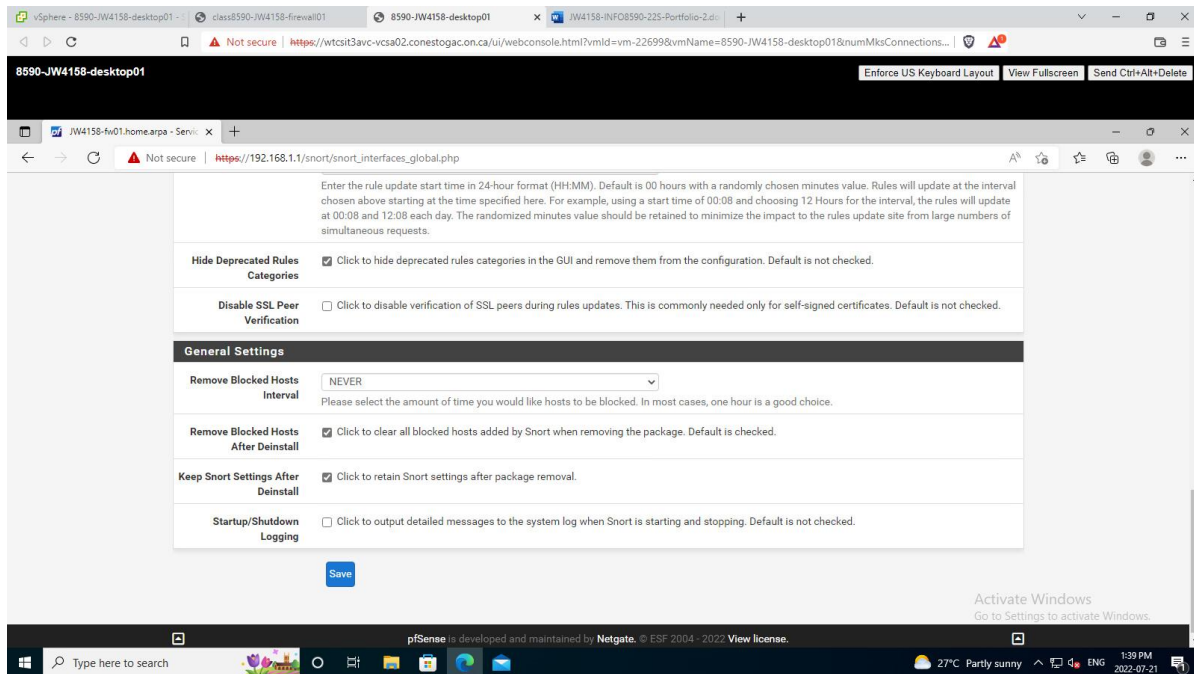


Figure 2.11 - Snort Global Settings Part 3

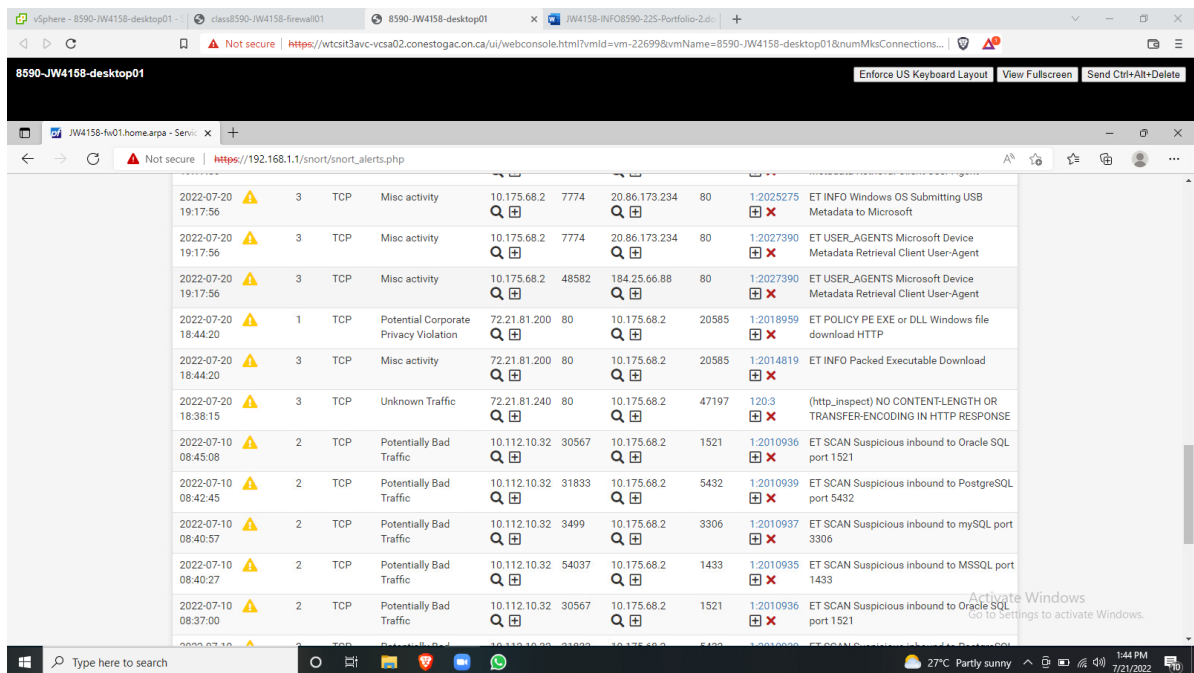


Figure 2.12 - Snort Alerts

Reflection

This lab was straightforward, one thing that stood out to me was that it could take several hours or possibly over a day for suspicious traffic alerts to appear in the log. This made troubleshooting much more difficult but luckily, I did not run into any problems. As mentioned in the previous lab, I was not able to configure a Kali machine on vSphere and so I did not do a scan on pfSense.

References

1. eConestoga, 2022 (Lab 4 – Network IDS and IPS Tools, retrieved from <https://conestoga.desire2learn.com/d2l/le/content/591148/viewContent/12779238/View> on July 24, 2022)