IT357 Tools and Techniques in Defensive Security
Assignment 6 – Intrusion Detection and Prevention Systems
….We're just Snorting about…..

10 Questions – 50 Points

SAVE THIS AS A PDF, SUBMIT THE PDF DOCUMENT ON REGGIENET

Objective: To configure an Intrusion Detection & Prevention System running in conjunction with a Firewall.

Preparation:

For this assignment, you will use the Ubuntu-LAN VM, Win10-WAN and the pfSense web UI.

NOTE: Don't forget to set your Win10 power settings to "never" screen power and "never" sleep.

Pre-Setup steps for the scenario:

1. **Take a snapshot of your pfSense VM** before proceeding with this assignment. In the unlikely event that something is incorrectly configured, and you are unable to remove the problematic settings, it will be much easier to simply roll back to the previously good configuration and start over from there.
2. Before taking a snapshot in Proxmox, you will first want to shut down the VM. The best way to do this is choose option 6 from the pfSense console to "halt" the system.
3. With the VM shut down, in the control panel on the right side of the Proxmox web UI, select the **Snapshot** tab and click the **Take Snapshot** button. Once the snapshot is complete, don't forget to start the pfSense VM before continuing.

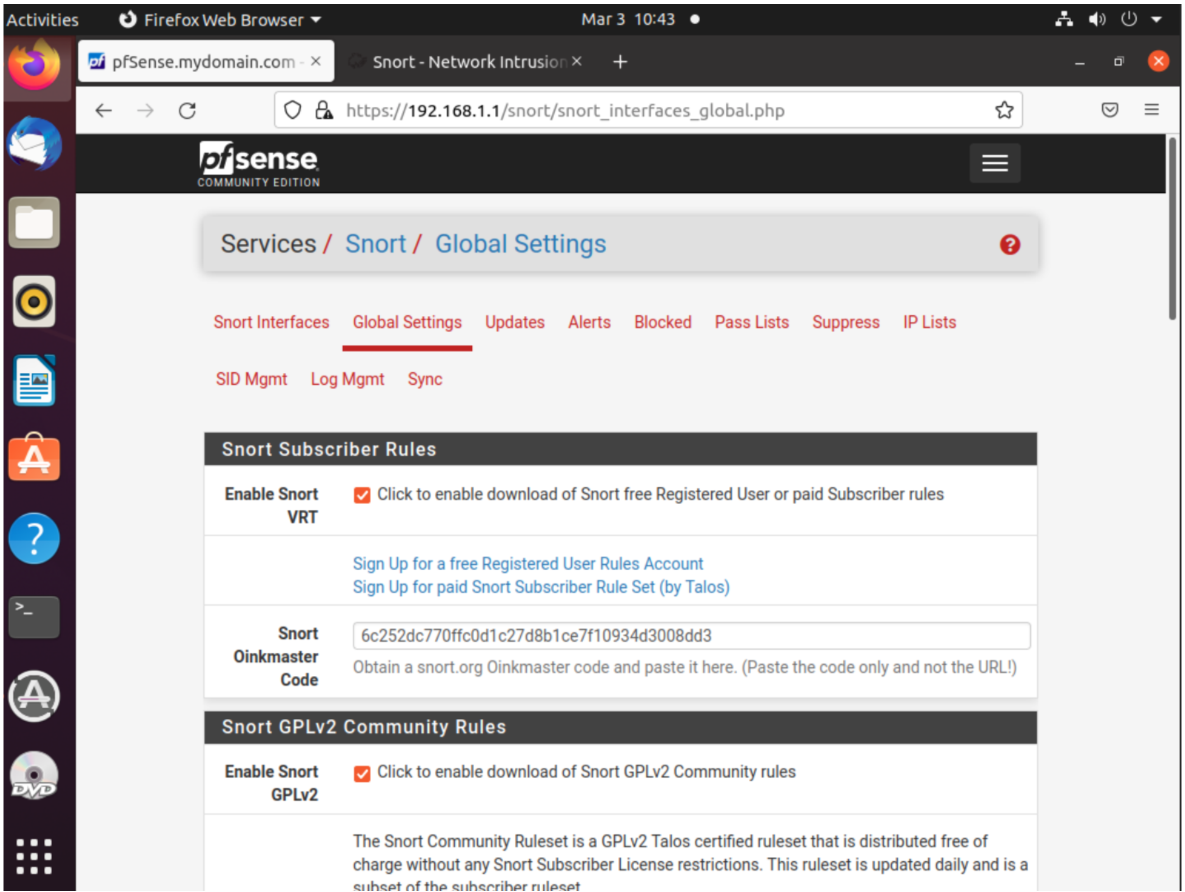
Part 1: Snort Setup in pfSense

Snort is an IDPS tool that can operate as a standalone service or can be easily integrated with several firewall systems. Enabling Snort within pfSense can be carried out by simply installing the Snort package.

1. Install the Snort package. From your Ubuntu-LAN VM, log into the pfSense web UI using its LAN interface IP address from a browser (e.g., https://192.168.1.1) and navigate to **System → Package Manager** and click on the **Available Packages** tab. Scroll down through the list of packages to find Snort. Click the green **Install** button and the **Confirm** button on the next page.
    a. Alternatively, you can use the search functionality on the Available Packages page to quickly find Snort in the list of packages.

2. Now that Snort is installed on pfSense, it is time to get it configured. Navigate to **Services → Snort** and click on the **Global Settings** tab. First, enable the download of various rule sets. Here, we are not necessarily enabling the rules, just allowing the download of different categories or groups or rules.
    a. Check the box to **Enable Snort VRT** under the *Snort Subscriber Rules*.
        i. You'll need your own Oinkmaster code to leverage the use of the free Snort rules. Click the link to **Sign Up for a free Registered User Rules Account**. A new tab should open the Snort Sign Up web page in your browser. Use your ISU email account to create a registered user account. If you already have a Snort account, you can simply click the **Sign In** link in the upper right-hand corner of the page.
        ii. Once the account has been created, click on your account name in the upper left-hand corner to open your account settings page. Click on the **Oinkcode** tab within the left-hand navigation pane. Copy your Oinkcode from this page and paste it into the **Snort Oinkmaster Code** field in the *Snort Subscriber Rules* section of the Snort Global Settings page of pfSense.
    b. Check the box for **Enable Snort GPLv2** in the *Snort GPLv2 Community Rules* section
    c. Check the box for **Enable ET Open** in the *Emerging Threats (ET)* Rules section
    d. Check the boxes for both the **Enable OpenAppID** and **Enable AppID Open Text Rules** in the *Sourcefire OpenAppID Detectors* section. These rules will allow us to identify traffic associated with specific applications.
    e. In the *Rules Update Settings* section, change the **Update Interval** to **1 Day** from the dropdown. This setting determines how often pfSense will check for and download new or updated rule sets.
    f. Q1) Leave the remaining settings on this page at their default. Click the blue **Save** button at the bottom of the page. (3 pts)

    [Insert



Services / Snort / Global Settings

Snort Subscriber Rules

Enable Snort VRT ☑ Click to enable download of Snort free Registered User or paid Subscriber rules

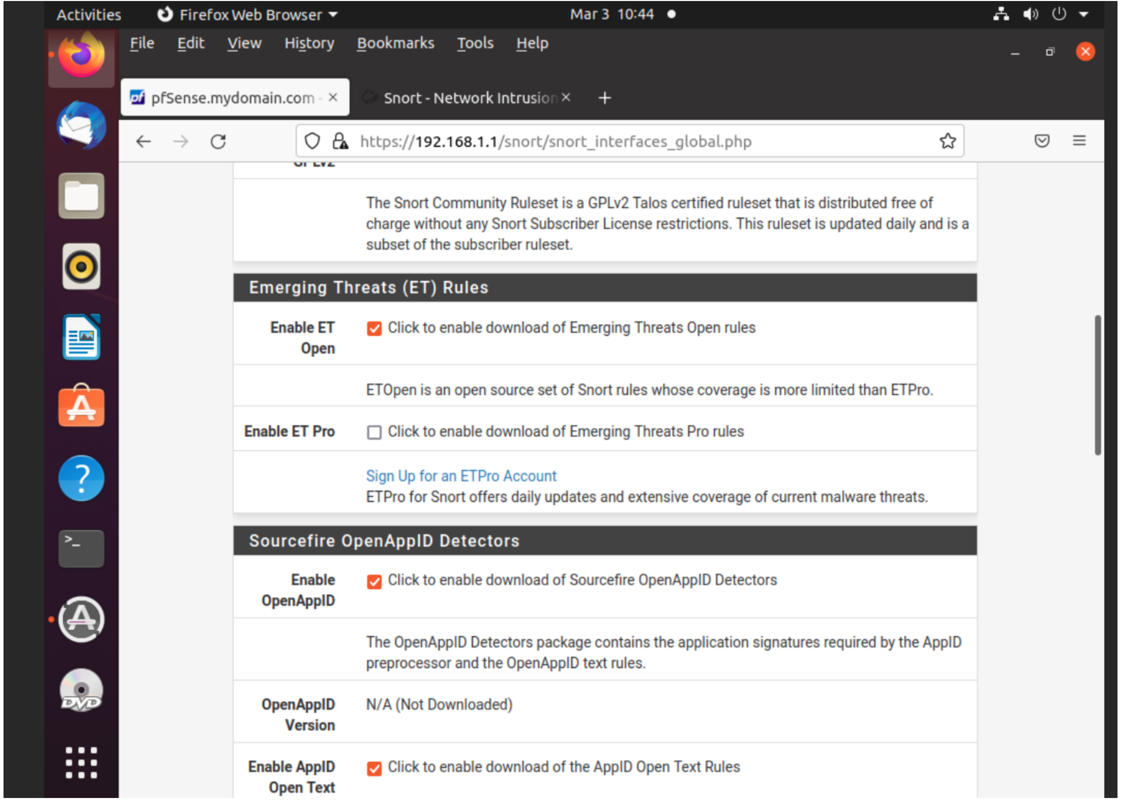
Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)

Snort Oinkmaster Code 6c252dc770ffc0d1c27d8b1ce7f10934d3008dd3
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☑ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset



The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☑ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

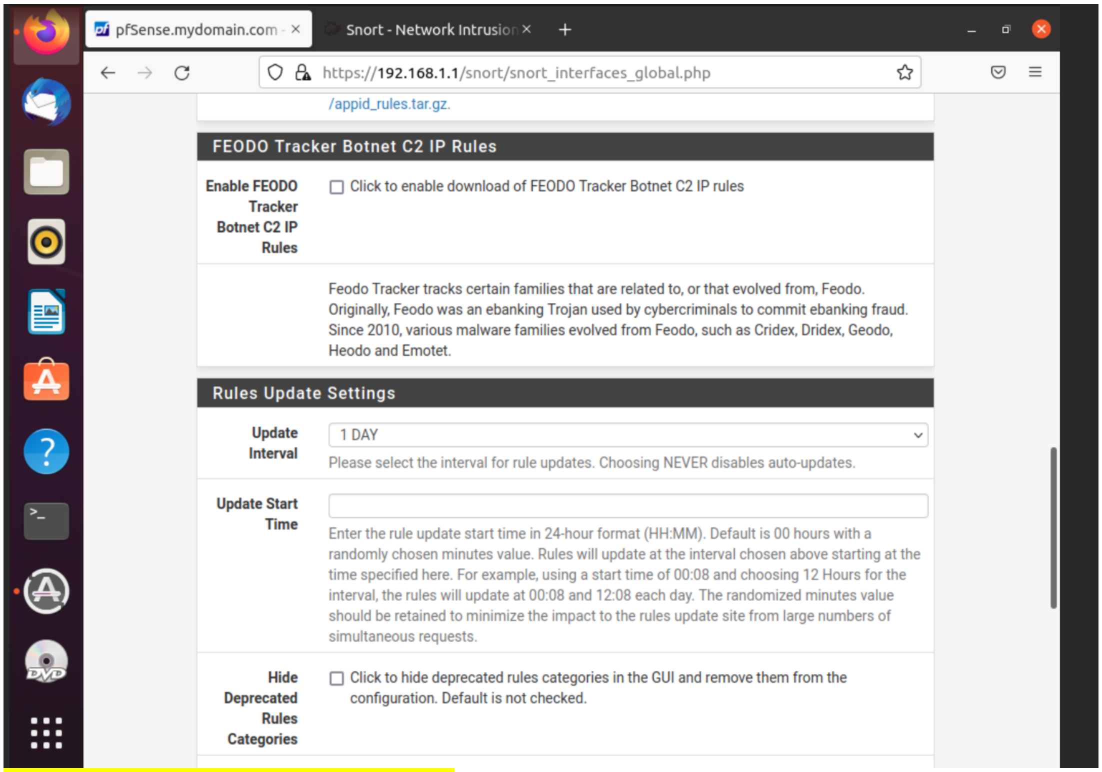
Enable OpenAppID ☑ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

OpenAppID Version N/A (Not Downloaded)

Enable AppID Open Text ☑ Click to enable download of the AppID Open Text Rules

g.
h.



pfSense.mydomain.com
Snort - Network Intrusion
https://192.168.1.1/snort/snort_interfaces_global.php

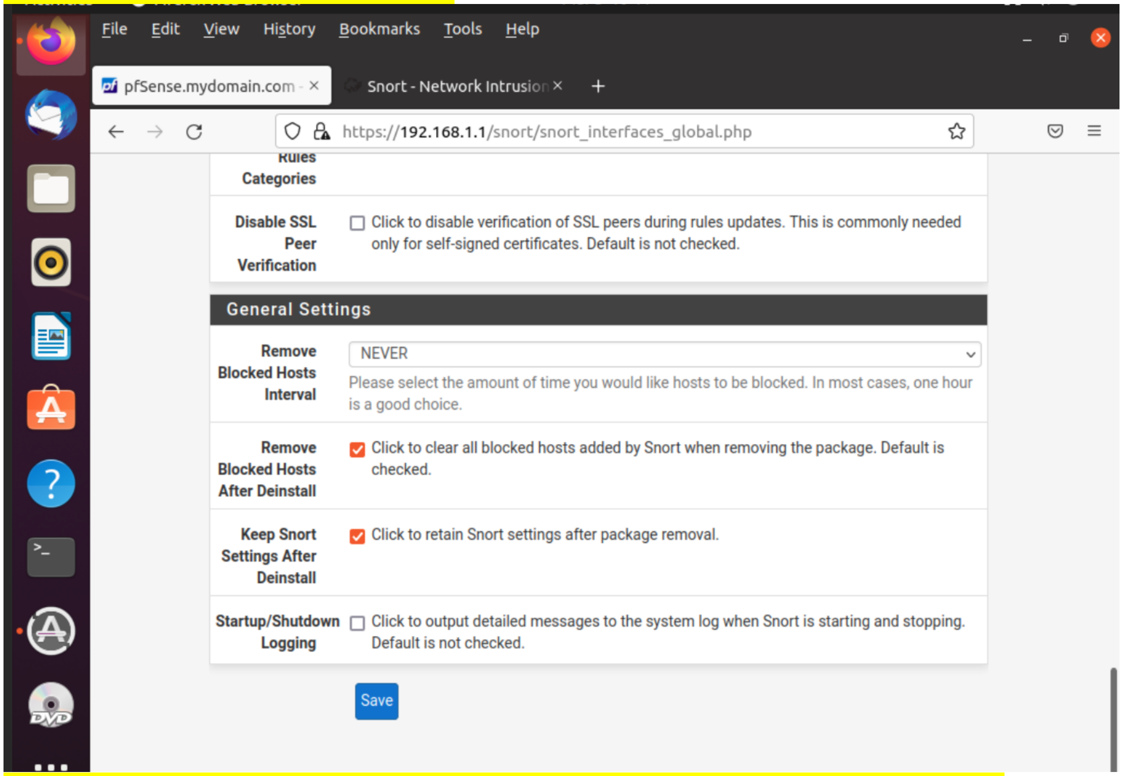
/appid_rules.tar.gz.

FEODO Tracker Botnet C2 IP Rules

Enable FEODO Tracker Botnet C2 IP Rules	□ Click to enable download of FEODO Tracker Botnet C2 IP rules
	Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.

Rules Update Settings

Update Interval	1 DAY Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Update Start Time	Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.
Hide Deprecated Rules Categories	□ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.



File
Edit
View
History
Bookmarks
Tools
Help
pfSense.mydomain.com
Snort - Network Intrusion
https://192.168.1.1/snort/snort_interfaces_global.php

Rules Categories	
Disable SSL Peer Verification	□ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

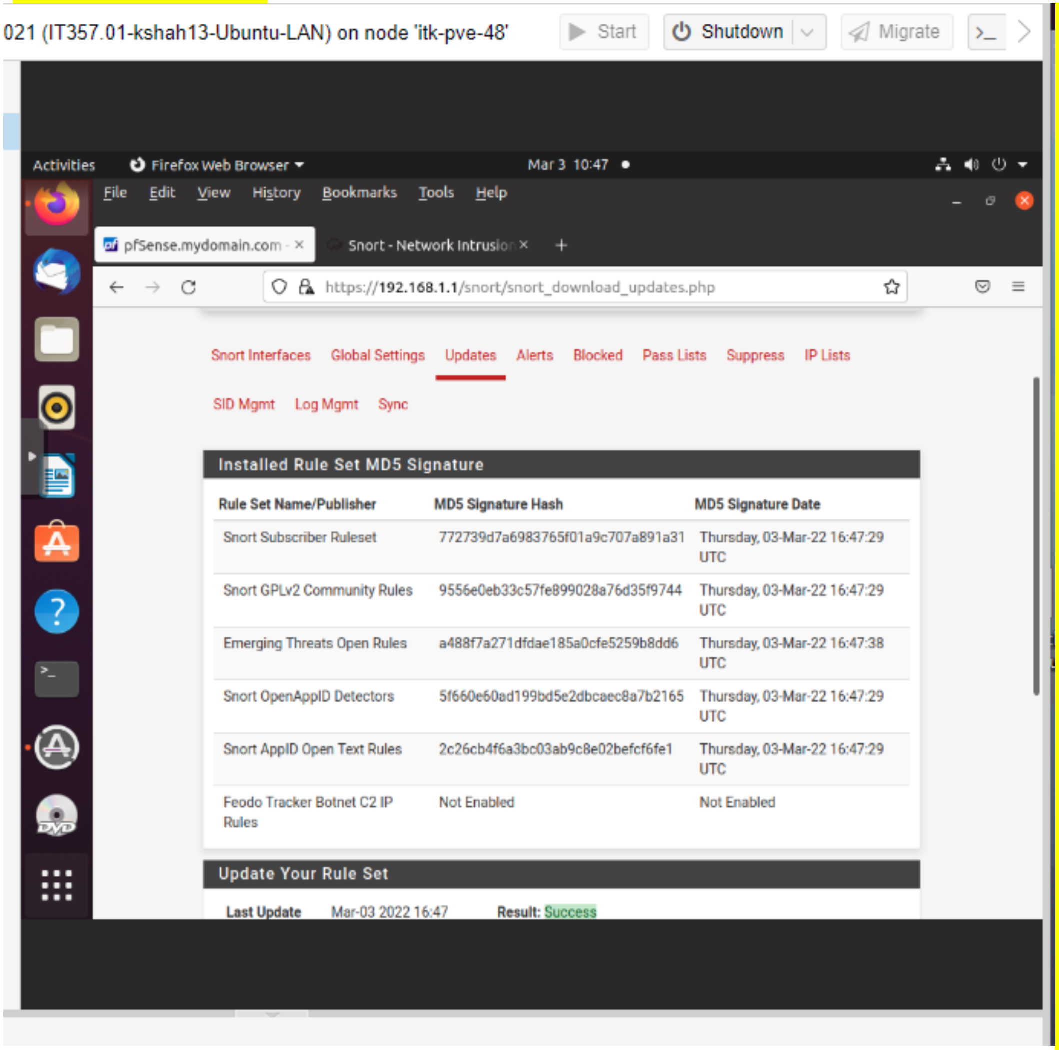
General Settings

Remove Blocked Hosts Interval	NEVER Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.
Remove Blocked Hosts After Deinstall	☑ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	☑ Click to retain Snort settings after package removal.
Startup/Shutdown Logging	□ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

one or more screen shots here showing the contents of your Global Settings page. Prove to me you've done the above steps.]

3. Back at the top of the Snort page, click on the **Updates** tab. You'll notice that none of your rule sets have been downloaded yet. In the *Update Your Rule Set* section click on the blue **Update Rules** button. A task window will open showing that the download is in progress.
   Q2) Once the download is complete, you will see that the Installed Rule Set table will be populated with the rule set hashes and dates. (3 pts)

   [Insert a screen shot here of the updated Installed Rule Set table.]



Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	772739d7a6983765f01a9c707a891a31	Thursday, 03-Mar-22 16:47:29 UTC
Snort GPLv2 Community Rules	9556e0eb33c57fe899028a76d35f9744	Thursday, 03-Mar-22 16:47:29 UTC
Emerging Threats Open Rules	a488f7a271dfdae185a0cfe5259b8dd6	Thursday, 03-Mar-22 16:47:38 UTC
Snort OpenAppID Detectors	5f660e60ad199bd5e2dbcaec8a7b2165	Thursday, 03-Mar-22 16:47:29 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Thursday, 03-Mar-22 16:47:29 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update Mar-03 2022 16:47 **Result:** Success

4. Snort is installed, we have our rule sets downloaded, now let's apply Snort inspection to an interface and choose the rules that we want to apply.
   a. Still on the Snort service configuration pages, click on the **Snort Interfaces** tab to the far left. Click on the green **Add** button on the right of the page. This will open a new page for the WAN interface. pfSense will correctly assume that the WAN interface will be your first choice of interfaces to inspect traffic.

   b. Verify that the **Enable** box is checked and that **WAN** is selected for **Interface** in the *General Settings* section. Leave all other settings at their default for now and click the blue **Save** button at the bottom of the page.
   c. Click the **Save** button. Notice that additional sub-tabs will now be available for the WAN interface under the Snort Interfaces parent tab.

5. Navigate to the **WAN Categories** sub-tab.
   a. Under the *Snort Subscriber IPS Policy Selection* section, check the box for **Use IPS Policy**. This will add the **IPS Policy Selection** setting. For this setting, choose **Security** from the drop down. This setting simplifies the selection of snort rules to enable based on the policy you have chosen.
   b. In the *Select the rulesets (Categories) Snort will load at Startup* section, click on the light blue **Select All** button to the left. This should automatically select the Snort GPLv2 rules, all of the ET Open Rules (Emerging Threats) in the left column, and all of the OPENAPPI rules (OpenAppID) rules in the far right column. Click the blue **Save** button.

6. The downloaded rulesets have been applied to the interface, however, not all rules within a ruleset are enabled by default.
   a. Click on the **WAN Rules** sub-tab.
   b. Click on the **Category Selection** drop down near the top of the window will allow you to view or modify the rules within the different rulesets or categories.
   c. From the **Category Selection** drop down, select **emerging-scan.rules**. Scroll down to the *Selected Category's Rules* section and you will see the full list of rules that make up the Emerging Threats Scans ruleset. Notice that there are many that are not enabled, designated by the red **X** along the left-hand margin.
   d. Up in the *Rule Signature ID Enable/Disable Overrides* section, click on the green **Enable All** button to enable all of the rules in this ruleset.
   e. Click the blue **Apply** button.

7. Not all threats can be easily identified strictly by signatures. Some detections will benefit from pre-processing by the IDS. Select the **WAN Preprocs** sub-tab.
   a. Scroll down to find and expand the *Application ID Detection* section. Check the **Enable** box to allow the IDS to use OpenAppID.
   b. Expand the *Portscan Detection* section. Check the **Enable** box to enable port scanning detection on the WAN interface.
   c. Leave the remaining default settings in place. Scroll to the bottom of the page.
   d. Click the blue **Save** button.

8. Navigate back to the **Snort Interfaces** parent tab. Under the Snort Status column you should see a red "**x**" and a blue triangle in the WAN table row.
   a. Click on the blue triangle button to enable the Snort service on the WAN interface. It'll take just a minute while the red "**x**" turns into a spinning gear and eventually it will turn into a green check mark indicating that the service is now

running on the interface.

Part 2: Port Scan

We will use Nmap from the Win10-WAN VM to scan the WAN interface of pfSense to test that Snort is working. Snort should generate alerts on port scans. But, to ensure we get a fair amount of IDS alerts, we are going to throw a pretty extensive scan with scripts at it.

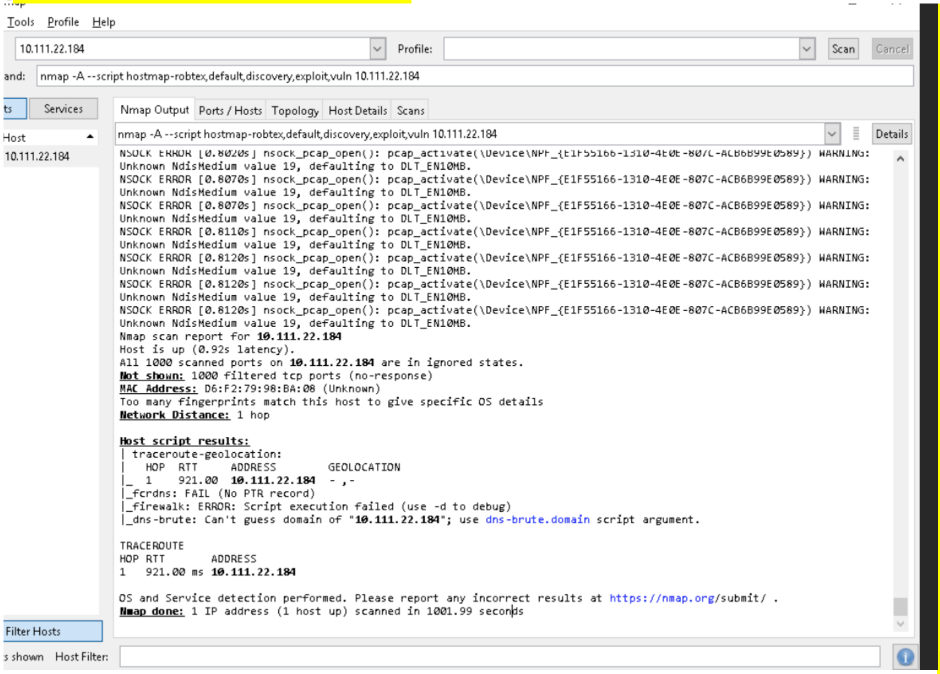
1. Switch to your Win10-WAN VM. Remember, this machine is on the outside, the "Internet" side of the pfSense firewall.
2. Turn off Windows Firewall.
3. Scan your target with Zenmap, the Windows GUI version of Nmap
    a. In the **Command** field of the Zenmap UI, enter the following:

```
nmap -A --script hostmap-
robtex,default,discovery,exploit,vuln [pfSense-WAN-IP]
```

    Note that this command is case sensitive, there are no spaces after the commas, and that [*pfSense-WAN-IP]* will be the actual IP address of your pfSense's WAN interface. The IP address is usually in the 10.x.y.z range.

    b. Click "Scan".
    c. Q3) Nmap will show "Nmap done: 1 address scanned" or a similar message with an output of the results from the scan. (3 pts)

[Insert a screenshot here of the Nmap window after it is completed.]



10.111.22.184

Profile:

and: nmap -A --script hostmap-robtex,default,discovery,exploit,vuln 10.111.22.184

10.111.22.184

nmap -A --script hostmap-robtex,default,discovery,exploit,vuln 10.111.22.184

```
NSOCK ERROR [0.8020s] nsock_pcap_open(): pcap_activate(\Device\NPF_{E1F55166-1310-4E0E-807C-ACB6B99E0589}) WARNING:
Unknown NdisMedium value 19, defaulting to DLT_EN10MB.
NSOCK ERROR [0.8070s] nsock_pcap_open(): pcap_activate(\Device\NPF_{E1F55166-1310-4E0E-807C-ACB6B99E0589}) WARNING:
Unknown NdisMedium value 19, defaulting to DLT_EN10MB.
NSOCK ERROR [0.8070s] nsock_pcap_open(): pcap_activate(\Device\NPF_{E1F55166-1310-4E0E-807C-ACB6B99E0589}) WARNING:
Unknown NdisMedium value 19, defaulting to DLT_EN10MB.
NSOCK ERROR [0.8110s] nsock_pcap_open(): pcap_activate(\Device\NPF_{E1F55166-1310-4E0E-807C-ACB6B99E0589}) WARNING:
Unknown NdisMedium value 19, defaulting to DLT_EN10MB.
NSOCK ERROR [0.8120s] nsock_pcap_open(): pcap_activate(\Device\NPF_{E1F55166-1310-4E0E-807C-ACB6B99E0589}) WARNING:
Unknown NdisMedium value 19, defaulting to DLT_EN10MB.
NSOCK ERROR [0.8120s] nsock_pcap_open(): pcap_activate(\Device\NPF_{E1F55166-1310-4E0E-807C-ACB6B99E0589}) WARNING:
Unknown NdisMedium value 19, defaulting to DLT_EN10MB.
NSOCK ERROR [0.8120s] nsock_pcap_open(): pcap_activate(\Device\NPF_{E1F55166-1310-4E0E-807C-ACB6B99E0589}) WARNING:
Unknown NdisMedium value 19, defaulting to DLT_EN10MB.
Nmap scan report for 10.111.22.184
Host is up (0.92s latency).
All 1000 scanned ports on 10.111.22.184 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: D6:F2:79:98:BA:08 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Host script results:
| traceroute-geolocation:
|   HOP  RTT     ADDRESS        GEOLOCATION
|_  1    921.00  10.111.22.184  - ,-
|_fcrdns: FAIL (No PTR record)
|_firewalk: ERROR: Script execution failed (use -d to debug)
|_dns-brute: Can't guess domain of "10.111.22.184"; use dns-brute.domain script argument.

TRACEROUTE
HOP RTT       ADDRESS
1   921.00 ms 10.111.22.184

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1001.99 seconds
```

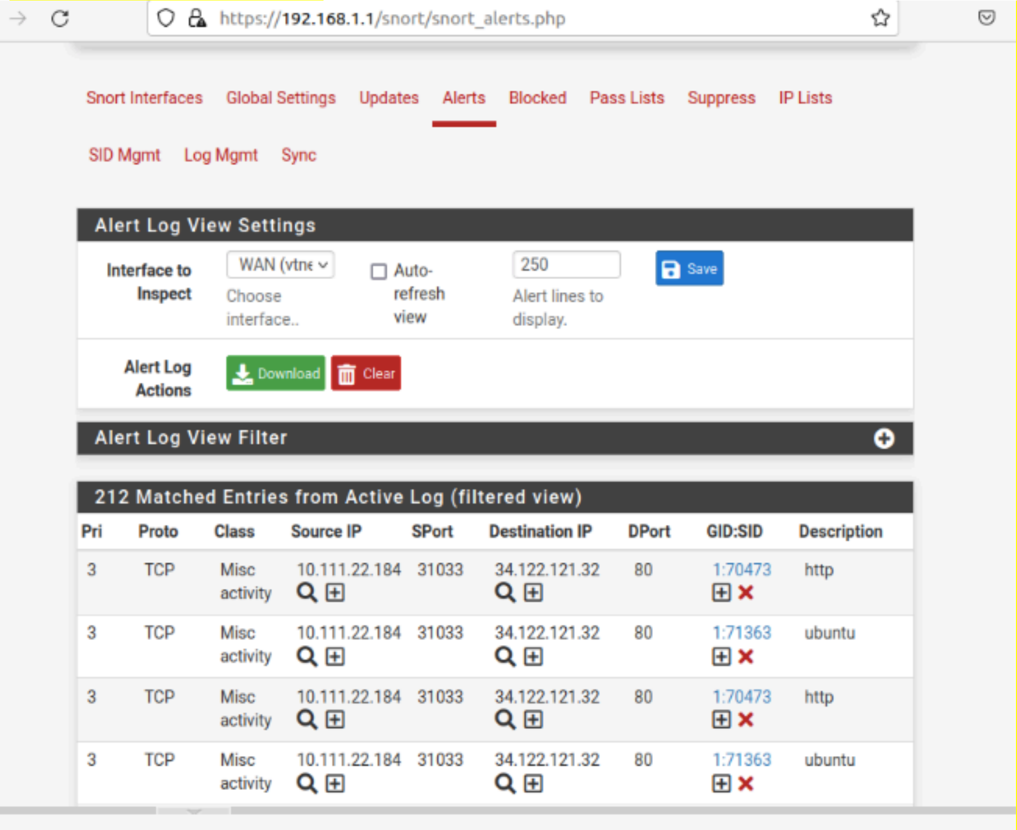
Part 3: Review and Tuning of Snort Alerts

Switch back to the **Ubuntu-LAN VM**.

1. Navigate to **Services** → **Snort** and click on the **Alerts** tab.

   Q4) You should see quite a few alerts, some should say NMAP and a type of scan. (3 pts)

   [Insert a screenshot here of Snort alerts in the web interface.]



https://192.168.1.1/snort/snort_alerts.php

Alert Log View Settings

Interface to Inspect: WAN (vtne — Choose interface..

☐ Auto-refresh view

250 — Alert lines to display.

Alert Log Actions

Alert Log View Filter

212 Matched Entries from Active Log (filtered view)

Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
3	TCP	Misc activity	10.111.22.184 🔍 ⊞	31033	34.122.121.32 🔍 ⊞	80	1:70473 ⊞ ✕	http
3	TCP	Misc activity	10.111.22.184 🔍 ⊞	31033	34.122.121.32 🔍 ⊞	80	1:71363 ⊞ ✕	ubuntu
3	TCP	Misc activity	10.111.22.184 🔍 ⊞	31033	34.122.121.32 🔍 ⊞	80	1:70473 ⊞ ✕	http
3	TCP	Misc activity	10.111.22.184 🔍 ⊞	31033	34.122.121.32 🔍 ⊞	80	1:71363 ⊞ ✕	ubuntu

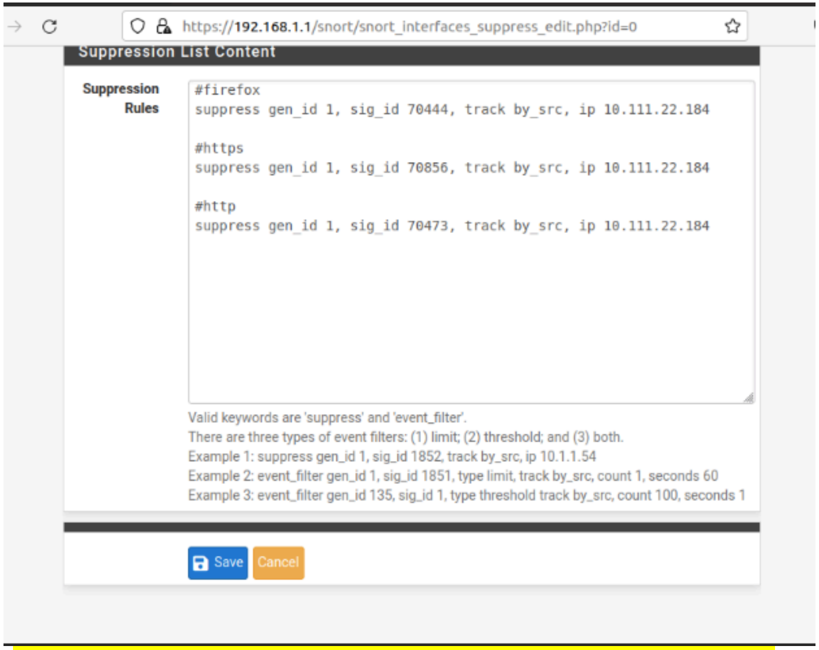
2. Let's assume that your Win10-WAN VM is a known safe member of your organization tasked with running external Nmap scans of your network. So, we'll want to suppress alerts associated with Nmap scans coming from this device.
   a. Identify at least one of the alerts in your list that has a Description starting with "ET SCAN Nmap".
   b. Find the "**+**" icon for this alert near the Win10-WAN IP address under the **Source IP** column. Click this "**+**" icon to add this alert to the list of suppressed alerts. Before you suppress the alert, make sure the IP address is correct for

Win10-WAN VM…..otherwise, you just suppressed the IP of an attacker.

NOTE: Suppressing alerts still allows Snort to process the rule but disables alerting. Suppression is more beneficial when making exceptions for specific alerts associated with specific IP addresses.

3. Navigate to the **Suppress** tab for the Snort service. There should be an automatically generated list with a name similar to "wansuppress_xxxxxx" located in the *Configured Suppression Lists* section. Click on the pencil edit icon for this list entry. Then after your screenshot, click "cancel".

   Q5) On the **Edit Suppression List** page and under the *Suppression List Content*, you should now see a rule created for the alert(s) you just suppressed. (3 pts)



https://192.168.1.1/snort/snort_interfaces_suppress_edit.php?id=0
Suppression List Content
Suppression Rules

```
#firefox
suppress gen_id 1, sig_id 70444, track by_src, ip 10.111.22.184

#https
suppress gen_id 1, sig_id 70856, track by_src, ip 10.111.22.184

#http
suppress gen_id 1, sig_id 70473, track by_src, ip 10.111.22.184
```

Valid keywords are 'suppress' and 'event_filter'.
There are three types of event filters: (1) limit; (2) threshold; and (3) both.
Example 1: suppress gen_id 1, sig_id 1852, track by_src, ip 10.1.1.54
Example 2: event_filter gen_id 1, sig_id 1851, type limit, track by_src, count 1, seconds 60
Example 3: event_filter gen_id 135, sig_id 1, type threshold track by_src, count 100, seconds 1

   [Insert a screen shot here of the created Suppression Rules.]

4. Let's generate some traffic from the Ubuntu-LAN VM for the OpenAppID component of Snort.

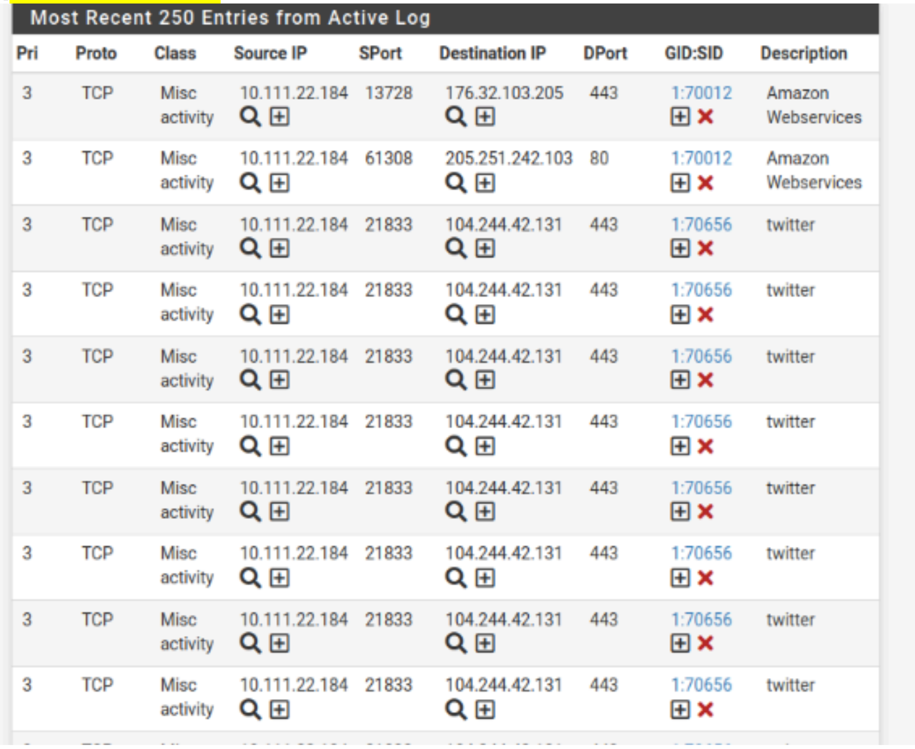
   NOTE: Before continuing, verify that the Snort service is still running by navigating to the **Snort Interfaces** tab and check the Snort Status for the WAN interface. If it is stopped as indicated by the red "**x**", click the blue triangle to restart the service.

   Open another browser tab and navigate to a few of the web sites in the list below. You may want to click around on a few links or buttons on each of the sites before continuing to the next site.

www.amazon.com
www.facebook.com
www.spotify.com
www.pandora.com

5. Q6) Navigate back to the Snort Service **Alerts** tab. You should now see a bunch of new alerts with a GID:SID value similar to 1:7xxxx and just a single word in the Description column. These might include: http, https, mozilla, amazon, facebook, etc. (3 pts)

   [Insert a screen shot here of the newly generated alerts.]



Most Recent 250 Entries from Active Log

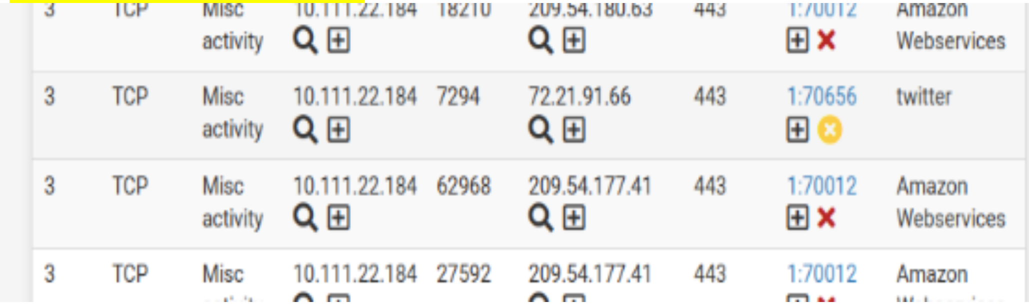
Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
3	TCP	Misc activity	10.111.22.184	13728	176.32.103.205	443	1:70012	Amazon Webservices
3	TCP	Misc activity	10.111.22.184	61308	205.251.242.103	80	1:70012	Amazon Webservices
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter
3	TCP	Misc activity	10.111.22.184	21833	104.244.42.131	443	1:70656	twitter

   NOTE: if you can't see all of this in one screen……make your SPICE VM window a bit bigger. You should see all of this info on one screen and one row. Then take your screenshot.

6. The OpenAppID rules can be useful for many things. Among those might be for tracking usage of certain applications or services that may be unwanted or go against your organizations security policy. However, they can also generate a lot of unnecessary noise in your alerts. Using suppression for OpenAppID rules stops the alerts but, the IDS is still processing packets to identify the associated application putting an unnecessary load on your system resources. For these it might be best to disable the rule altogether.

   Q7) To do this, identify an OpenAppID alert you would like to disable in the list (these would be the ones that typically have a single word for the Description and have a GID:SID similar to 1:7xxxx) and click on the red "x" under the GID:SID column. (3 pts)

[Insert a screen shot here of the disabled alert that now should have a yellow "**x**".]

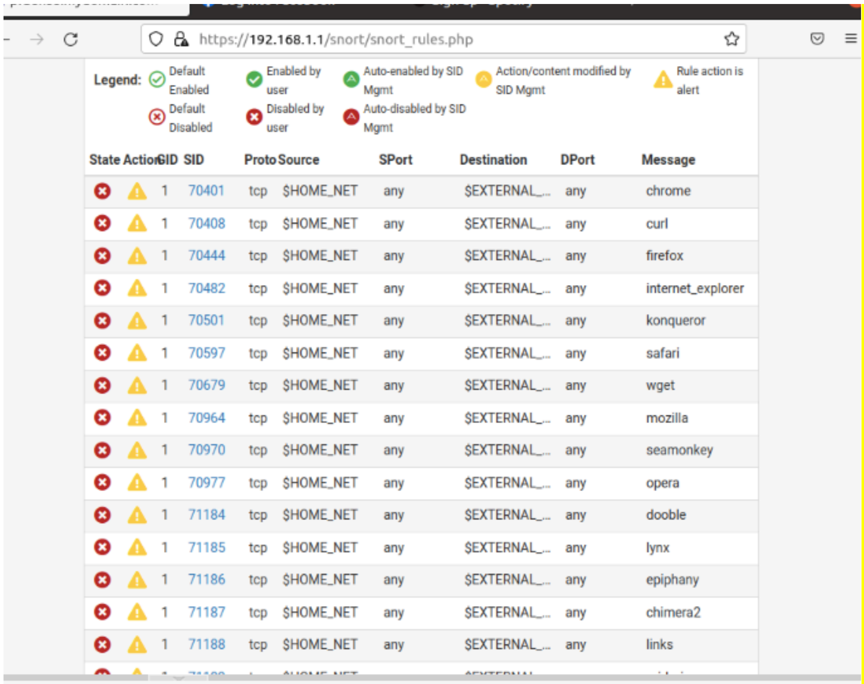


3	TCP	Misc activity	10.111.22.184 🔍 ⊞	18210	209.54.180.63 🔍 ⊞	443	1:70012 ⊞ ✕	Amazon Webservices
3	TCP	Misc activity	10.111.22.184 🔍 ⊞	7294	72.21.91.66 🔍 ⊞	443	1:70656 ⊞ ✕	twitter
3	TCP	Misc activity	10.111.22.184 🔍 ⊞	62968	209.54.177.41 🔍 ⊞	443	1:70012 ⊞ ✕	Amazon Webservices
3	TCP	Misc	10.111.22.184	27592	209.54.177.41	443	1:70012	Amazon

7. Another way to disable rule sets would be to disable an entire rule set or category from the rules assigned to an interface.
   a. Navigate back to the **Snort Interfaces** tab and edit the WAN interface by clicking on the pencil. From the WAN interface settings click on the **WAN Rules** sub-tab.
   b. For the **Category Selection** near the top of the page, click the drop down menu and select **openappid-webbrowser.rules**.
   c. Let's assume that your organization does not care to track which web browsers are being used. Scrolling down to the *Selected Category's Rules* will show a long list of rules identifying different web browsers. Click on the red **Disable All** button under the *Rule Signature ID (SID) Enable/Disable Overrides* section.
   d. Click the blue **Apply** button.

Q8) You should now see that all the browser identification rules have been disabled, indicated by the "X" in the State column.

[Insert a screen shot he



https://192.168.1.1/snort/snort_rules.php

Legend: ○ Default Enabled ✓ Enabled by user ● Auto-enabled by SID Mgmt ● Action/content modified by SID Mgmt ⚠ Rule action is alert
⊗ Default Disabled ☒ Disabled by user ● Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
☒	⚠	1	70401	tcp	$HOME_NET	any	$EXTERNAL_...	any	chrome
☒	⚠	1	70408	tcp	$HOME_NET	any	$EXTERNAL_...	any	curl
☒	⚠	1	70444	tcp	$HOME_NET	any	$EXTERNAL_...	any	firefox
☒	⚠	1	70482	tcp	$HOME_NET	any	$EXTERNAL_...	any	internet_explorer
☒	⚠	1	70501	tcp	$HOME_NET	any	$EXTERNAL_...	any	konqueror
☒	⚠	1	70597	tcp	$HOME_NET	any	$EXTERNAL_...	any	safari
☒	⚠	1	70679	tcp	$HOME_NET	any	$EXTERNAL_...	any	wget
☒	⚠	1	70964	tcp	$HOME_NET	any	$EXTERNAL_...	any	mozilla
☒	⚠	1	70970	tcp	$HOME_NET	any	$EXTERNAL_...	any	seamonkey
☒	⚠	1	70977	tcp	$HOME_NET	any	$EXTERNAL_...	any	opera
☒	⚠	1	71184	tcp	$HOME_NET	any	$EXTERNAL_...	any	dooble
☒	⚠	1	71185	tcp	$HOME_NET	any	$EXTERNAL_...	any	lynx
☒	⚠	1	71186	tcp	$HOME_NET	any	$EXTERNAL_...	any	epiphany
☒	⚠	1	71187	tcp	$HOME_NET	any	$EXTERNAL_...	any	chimera2
☒	⚠	1	71188	tcp	$HOME_NET	any	$EXTERNAL_...	any	links

re showing the list of disabled web browser rules.]

Part 4. Snort and pfSense for Intrusion Prevention

We have been using Snort on pfSense to generate alerts for application awareness and to detect potentially malicious traffic. However, we have the capability to block IP addresses associated with Snort alerts. Effectively converting our Snort installation into an Intrusion Prevention System.

1. Begin by going to **Services → Snort** and click on the **Global Settings** tab. Scroll down to the bottom section, *General Settings*. The first setting here, **Remove Blocked Hosts Interval**, sets the time for how long an IP that triggers an alert will be blocked. For the assignment, change **Remove Blocked Hosts Interval** to **15 min**. Click the blue **Save** button at the bottom of the page.

2. Next, navigate to the **Snort Interfaces** tab and click the pencil icon for the WAN interface to edit the interface settings. In the *Block Settings* section, check the box for **Block Offenders**. This should open up a few more settings. Leave the IPS Mode set to the default Legacy Mode but, change the **Which IP to Block** setting to **SRC** (a.k.a source IP). Click the blue **Save** button.

3. Then back to **Snort Interfaces** tab and click on the blue triangle to start the WAN interface again.

4. Let's verify Snort's blocking capabilities by sending a specially crafted packet that has

both the SYN and the FIN flags set. We allowed the signature to detect this type of packet earlier when we enabled all the emerging-scan rules.

a. To run the test, switch back to the **Win10-WAN VM** and use the nping application from the command line.

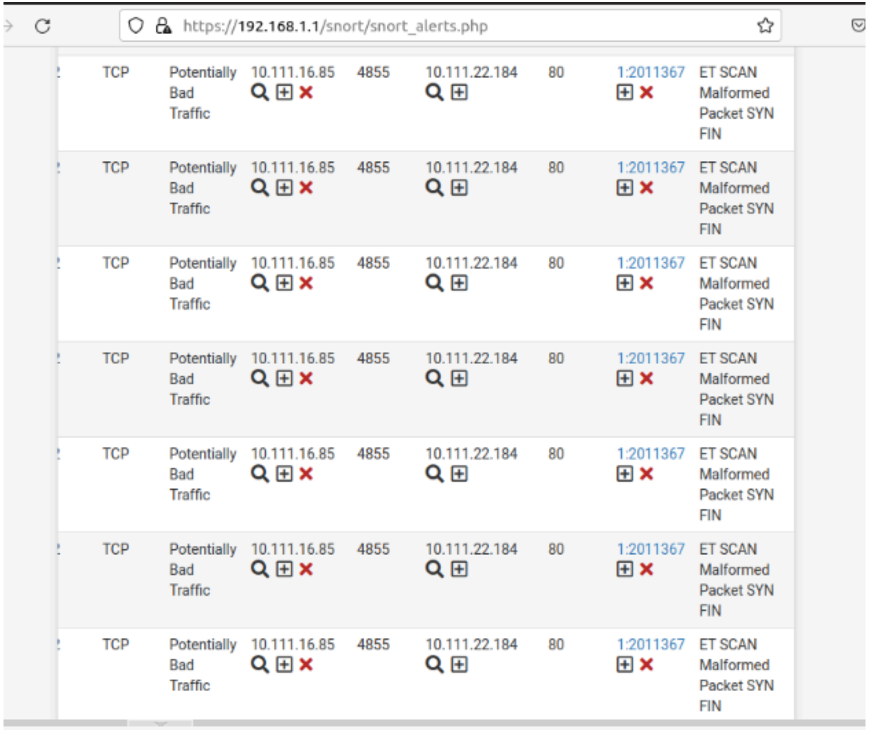
   From the command line run the following command:

   ```
   nping –tcp -c 10 -flags SF -p 80 [pfSense-WAN-IP]
   ```

   The command will send 10 TCP connection packets with both the SYN and FIN flags set to port 80 of the pfSense WAN interface.

5. Switch back to the Snort **Service** page on pfSense and click on the **Alerts** tab.

   Q9) You should now see about 10 alerts with a description containing “Malformed Packet SYN FIN”. (3 pts)



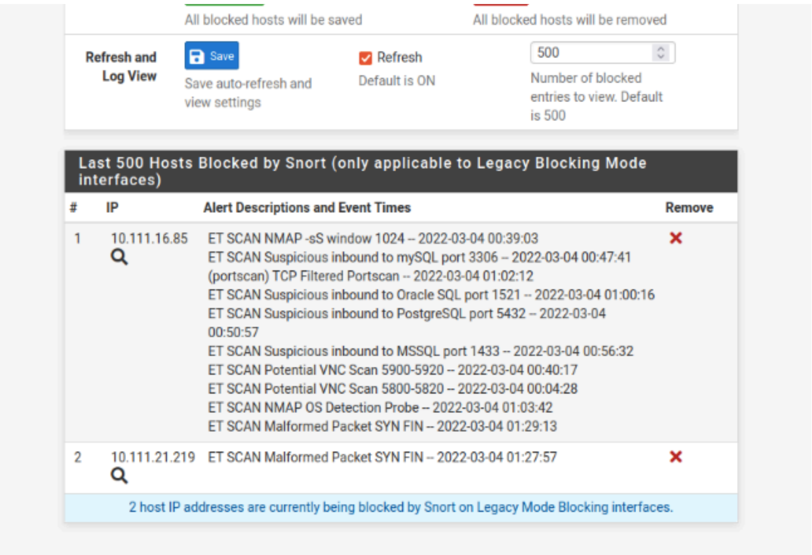
https://192.168.1.1/snort/snort_alerts.php

:	TCP	Potentially Bad Traffic	10.111.16.85 🔍 ⊞ ✕	4855	10.111.22.184 🔍 ⊞	80	1:2011367 ⊞ ✕	ET SCAN Malformed Packet SYN FIN
:	TCP	Potentially Bad Traffic	10.111.16.85 🔍 ⊞ ✕	4855	10.111.22.184 🔍 ⊞	80	1:2011367 ⊞ ✕	ET SCAN Malformed Packet SYN FIN
:	TCP	Potentially Bad Traffic	10.111.16.85 🔍 ⊞ ✕	4855	10.111.22.184 🔍 ⊞	80	1:2011367 ⊞ ✕	ET SCAN Malformed Packet SYN FIN
:	TCP	Potentially Bad Traffic	10.111.16.85 🔍 ⊞ ✕	4855	10.111.22.184 🔍 ⊞	80	1:2011367 ⊞ ✕	ET SCAN Malformed Packet SYN FIN
:	TCP	Potentially Bad Traffic	10.111.16.85 🔍 ⊞ ✕	4855	10.111.22.184 🔍 ⊞	80	1:2011367 ⊞ ✕	ET SCAN Malformed Packet SYN FIN
:	TCP	Potentially Bad Traffic	10.111.16.85 🔍 ⊞ ✕	4855	10.111.22.184 🔍 ⊞	80	1:2011367 ⊞ ✕	ET SCAN Malformed Packet SYN FIN
:	TCP	Potentially Bad Traffic	10.111.16.85 🔍 ⊞ ✕	4855	10.111.22.184 🔍 ⊞	80	1:2011367 ⊞ ✕	ET SCAN Malformed Packet SYN FIN

[Insert a screen shot here showing the newly generated alerts.]

6. Now click on the **Blocked** tab.

   Q10) You should see the IP of your Win10-WAN VM listed among the Hosts Blocked list. (3 pts)



All blocked hosts will be saved

All blocked hosts will be removed

Refresh and Log View	Save Save auto-refresh and view settings	☑ Refresh Default is ON	500 Number of blocked entries to view. Default is 500

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	10.111.16.85	ET SCAN NMAP -sS window 1024 -- 2022-03-04 00:39:03 ET SCAN Suspicious inbound to mySQL port 3306 -- 2022-03-04 00:47:41 (portscan) TCP Filtered Portscan -- 2022-03-04 01:02:12 ET SCAN Suspicious inbound to Oracle SQL port 1521 -- 2022-03-04 01:00:16 ET SCAN Suspicious inbound to PostgreSQL port 5432 -- 2022-03-04 00:50:57 ET SCAN Suspicious inbound to MSSQL port 1433 -- 2022-03-04 00:56:32 ET SCAN Potential VNC Scan 5900-5920 -- 2022-03-04 00:40:17 ET SCAN Potential VNC Scan 5800-5820 -- 2022-03-04 00:04:28 ET SCAN NMAP OS Detection Probe -- 2022-03-04 01:03:42 ET SCAN Malformed Packet SYN FIN -- 2022-03-04 01:29:13	✗
2	10.111.21.219	ET SCAN Malformed Packet SYN FIN -- 2022-03-04 01:27:57	✗

2 host IP addresses are currently being blocked by Snort on Legacy Mode Blocking interfaces.

[Insert a screen shot here showing the Hosts Blocked list.]

SAVE THIS AS A PDF, SUBMIT THE PDF DOCUMENT ON REGGIENET