**********************DAY-05___STM***************************

How Attacks Happens:

1.DOS (Denial of Service): DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Protection of DoS: packet filtering limit, packet filtering of ping and deny.

Intrusions:

Intrusion Detection:

Intrusion Detection System (IDS):

Intrusion Prevention System (IPS): Stop the attack itself, delete, modify, delete user session etc.

Most **IDPS** offer common evasion techniques.

Types of IDS/IDPS/ Classes of detection methodology:

1.Signature Based- Effective for detecting known threats.

2.Anomaly Based- Behavior-based

3.Host Based-

4.Network Based-

Stateful Protocol Analysis: Key development in IDPS tech was the use of protocol analyzers.

IDPS- false positive (incorrectly identification of malicious) and false negative (fails to identify malicious activity)

Source Ip, Source port, Packets, Timestamp etc., can help to analyze the intrusions.

Log stacks, Elastic Search, Kibana

Where to install Network Based IDPS:

Inline: Internet ---> firewall (IDS install-Protect against internet threats) ---> LAN

Offline: For internal threats from C1 to C2 (IDS install – protect against internal threats e.g., employee, malwares) port mirroring or Promiscuous switch help to do that. (Because switch has only destination port)

Internet ---> Firewall ---> switch --(IDS)--> computers

WAF (Web Application Firewall) for web application servers.

-------------------------------LAB------------------------------------

NAT ---->IDS ----> LAN n/w (Host only) ---> Host Client

Rules Selection:

System-->General Setup – For DNS configure

System-->Package Manager--->Package Installer-->SNORT

Services-->Snort--->Interfaces

Two interfaces LAN and WAN

We monitor the WAN.

Global Settings--> Enable Snort VRT-->snort code (snort.org generated code)

Enable GPLv2

-->Enable ET open

--> Enable OpenAppID

--> Enable AppID Open Text Rules

--> Enable FEODO Tracker Botnet C2 IP Rules

-->Update Interval --> Update Start Time

--> Hide Deprecated Rules Categories

--> Remove Blocked Hosts Interval (the amount of time you would like hosts to be blocked.)

-->SAVE

Go to Updates (Rules selected are listed) --->Update Rules

>Alerts

-->Blocked

-->**Pass Lists -->Add-->SAVE**

-->**Suppress (false positive) -->Add-->a blank list**

-->IP list

-->Log Mgmt

-->**Snort Interfaces --> Add**

--> INTERFACE-->SNAP LENGTH

-->Block offenders (work as IPS if checked)

-->SAVE

-->Click snort interface to check-->Play snort status

--

(nmap.org/downloads) -- download .exe

-->Open nmap

-->Put WAN ip and Scan

-->pfsense Dashboard-->Snort alerts

-->Services-->Snort-->Interface Setting overview—Edit

Go to Snort Interfaces and Stop service.

-->WAN categories

--> Snort Subscriber IPS Policy Selection-->check-->Balanced-->SAVE
Go to Snort Interfaces and Start service

==

dhclient –v = to get ip is host only mode.

===

Port Forwarding:

Static NAT: One public iP mapped to one private iP-->1:1 NAT

NAT Overload/PAT (Port address Transmission): Many private Ip's mapped to one Public iP. (By default, configured in Firewall)

==

yum install httpd

cd /var/www/html

create index.html

start httpd

curl http://localhost

In Pfsense:

Firewall-->Virtual IPs -->Add

IP Alias--->Interface-->WAN -->Address-->192.168.230.50 -->SAVE

Firewall-

NAT-->1:1-->Add

--> External subnet IP-->Address-> 192.168.230.50

--> Internal IP -->Address/mask--->Ip of client -->SAVE-->Apply Changes

(In Browser not going to start the website, because only mapping has been done)

Go

Firewall-->

Rules-->WAN--> Actions 1st one-->click on setting-->Uncheck the block private n/w -->SAVE --> Apply Changes.

Allow traffic for internal client:

Firewall-->

Rules-->Add

Destination-->Single Host or alias ---Dest Address---client address

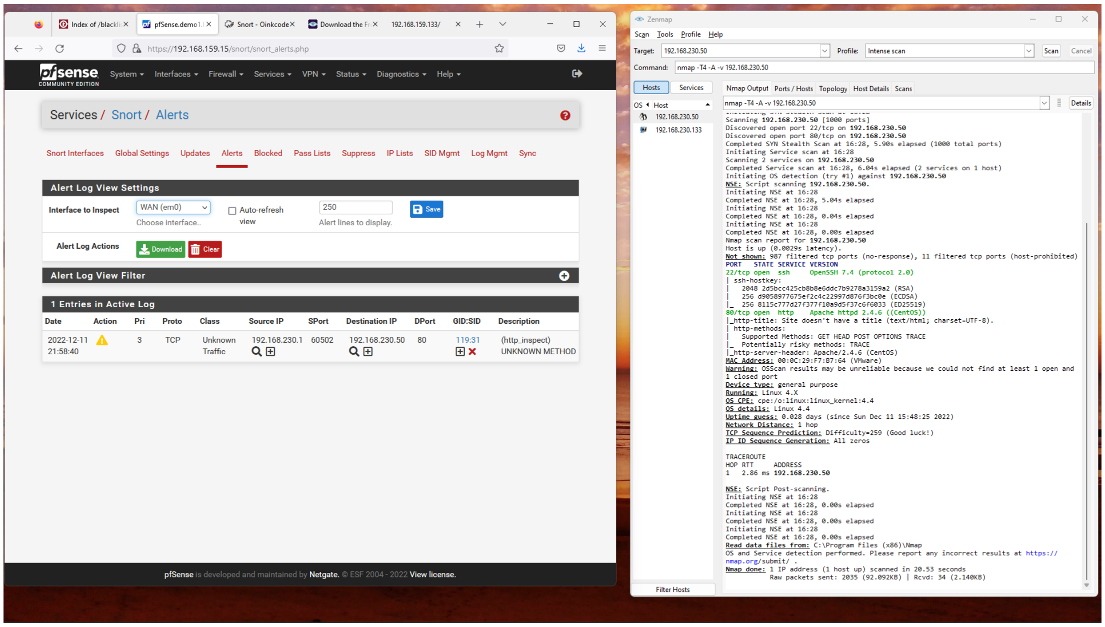
Destination Port Range-->first and third column (any)

Add tcp port-->

In Base Machine: firewall-cmd --add-port=80/tcp

Go to Browser -->Give Client IP.

You will get this--->



Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: WAN (em0) — Choose interface..

□ Auto-refresh view

250 — Alert lines to display.

Alert Log Actions

Alert Log View Filter

1 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-12-11 21:58:40	⚠	3	TCP	Unknown Traffic	192.168.230.1	60502	192.168.230.50	80	119:31	(http_inspect) UNKNOWN METHOD

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

Target: 192.168.230.50

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.230.50

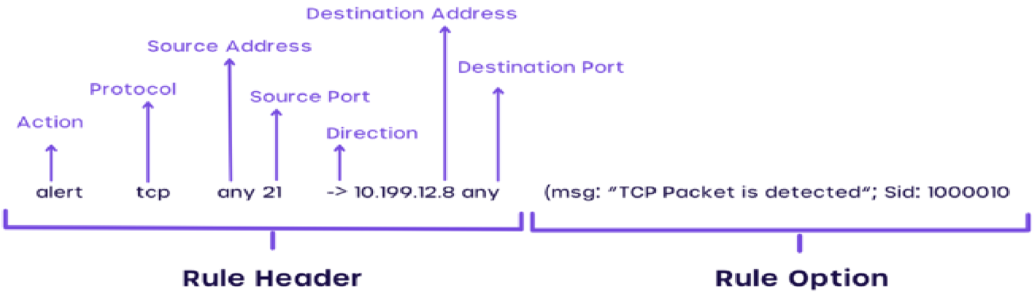
192.168.230.50
192.168.230.133

```
Scanning 192.168.230.50 [1000 ports]
Discovered open port 22/tcp on 192.168.230.50
Discovered open port 80/tcp on 192.168.230.50
Completed SYN Stealth Scan at 16:28, 5.90s elapsed (1000 total ports)
Initiating Service scan at 16:28
Scanning 2 services on 192.168.230.50
Completed Service scan at 16:28, 6.04s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.230.50
NSE: Script scanning 192.168.230.50.
Initiating NSE at 16:28
Completed NSE at 16:28, 5.04s elapsed
Initiating NSE at 16:28
Completed NSE at 16:28, 0.04s elapsed
Initiating NSE at 16:28
Completed NSE at 16:28, 0.00s elapsed
Nmap scan report for 192.168.230.50
Host is up (0.0029s latency).
Not shown: 987 filtered tcp ports (no-response), 11 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 2d5bcc425cb8b8e6ddc7b9278a3159a2 (RSA)
|   256 d9058977675ef2c4c22997d876f3bc0e (ECDSA)
|_  256 8115c777d27f377f10a9d5f37c6f6033 (ED25519)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS)
MAC Address: 00:0C:29:F7:B7:64 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Uptime guess: 0.028 days (since Sun Dec 11 15:48:25 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   2.86 ms 192.168.230.50

NSE: Script Post-scanning.
Initiating NSE at 16:28
Completed NSE at 16:28, 0.00s elapsed
Initiating NSE at 16:28
Completed NSE at 16:28, 0.00s elapsed
Initiating NSE at 16:28
Completed NSE at 16:28, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 20.53 seconds
           Raw packets sent: 2035 (92.092KB) | Rcvd: 34 (2.140KB)
```

IDS mode

Rules format for snort:

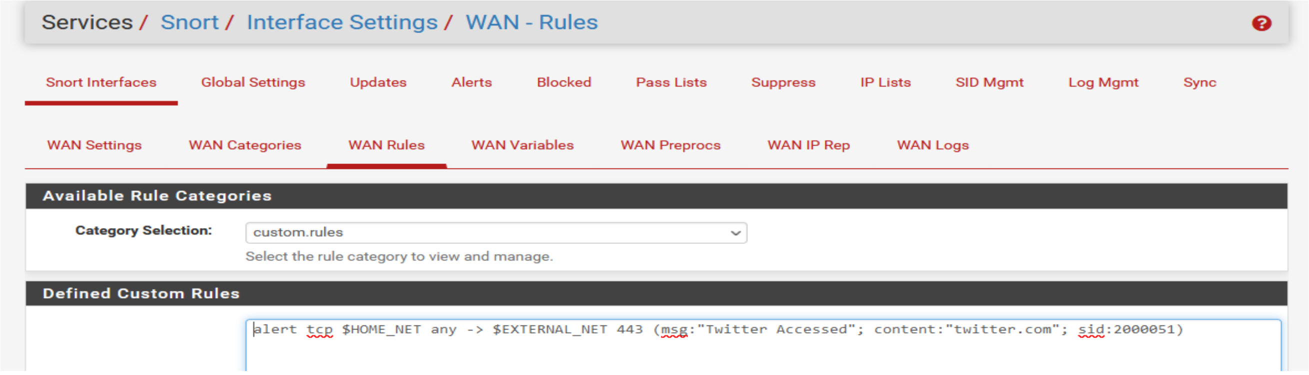
https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm#content



Action –Alert, **Protocol-, Source Ip**-any, **Source Port**- any, **Direction, Destination Ip, Destination Port, msg:** 'alert message' **(compulsory), Sid:** min 7digits (Compulsory)**, Rev:**1, **Content:** in.url, **offset**

Services—Snort-->Edit Interface

WAN Rules->Category selection: custom.rules **-->** Defined custom rules



Available Rule Categories

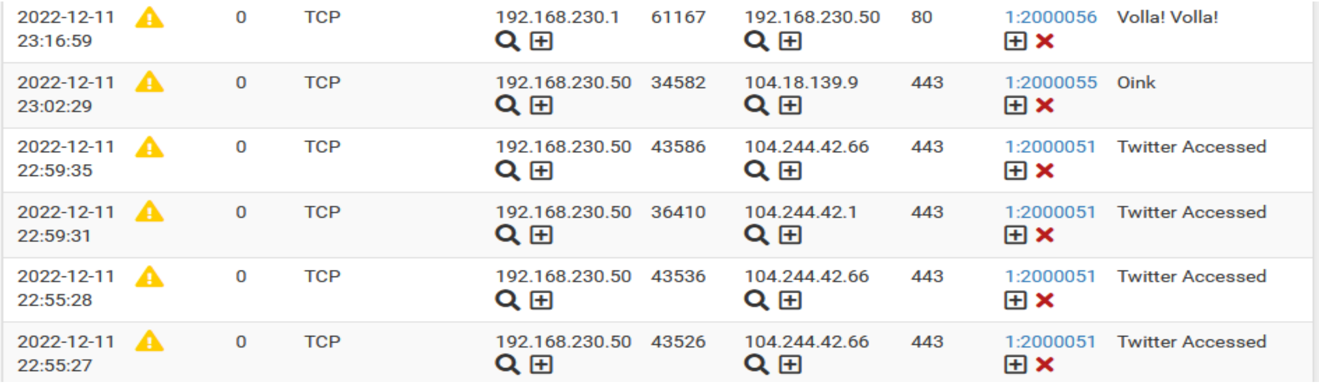
Category Selection: custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"Twitter Accessed"; content:"twitter.com"; sid:2000051)
```

Click into pfsense and see the alert. It will show the "twitter accessed" alert.



2022-12-11 23:16:59	⚠	0	TCP	192.168.230.1	61167	192.168.230.50	80	1:2000056	Volla! Volla!
2022-12-11 23:02:29	⚠	0	TCP	192.168.230.50	34582	104.18.139.9	443	1:2000055	Oink
2022-12-11 22:59:35	⚠	0	TCP	192.168.230.50	43586	104.244.42.66	443	1:2000051	Twitter Accessed
2022-12-11 22:59:31	⚠	0	TCP	192.168.230.50	36410	104.244.42.1	443	1:2000051	Twitter Accessed
2022-12-11 22:55:28	⚠	0	TCP	192.168.230.50	43536	104.244.42.66	443	1:2000051	Twitter Accessed
2022-12-11 22:55:27	⚠	0	TCP	192.168.230.50	43526	104.244.42.66	443	1:2000051	Twitter Accessed