Security Operation Assessment Using Snort & Pfsense Firewall

BY AHMED PINGER

Introduction

Securing web applications is today's most common aspect of securing the enterprise. Web application hacking is on the rise with as many as 80% of cyber-attacks done at the web application level or via the web. Most corporations have secured their data at the network level, but have
overlooked the crucial step of checking whether their web applications are vulnerable to attack.

This project is devoted to presenting a solution to protect web pages that required passwords on HTML login pages or admin directories, from Brute Force Attacks. By performing a brute force password auditing against web servers using HTTP authentication, with Nmap, and detect and mitigate this attack using snort IDS/IPS on PFSense Firewall. And also presents a solution to protect a specific WordPress website that consists of vulnerable plugins, and can be exploited by Evil Hackers it will also be done by detecting and mitigating using snort IDS/IPS on PFSense Firewall.

For this project, we will use the methodology, which consists of the following steps.

1. Analysis & Design
2. Development
3. Testing
4. Documentation

By the end of this process, we will be able to mitigate the attacks performed on the Web Server, by applying rules on the Pfsense firewall and Snort IPS. And they are getting alerts of attacks on Snort.

Project Implementation Plan

Along with the whole project, we will be using the methodology discussed above, the **model.** The steps are given below

Analysis & Design:

1. Environment setup
2. Install Needed ISO's

Development:

1. Setup the environment (Reference in Topology)
2. Set up Snort as an IDS/IPS
3. Configure Snort to defend against Brute Force Attack and LFI attack

Testing:

1. Performing HTTP-Basic Authentication Brute Force Attack
2. Performing Local File Inclusion Attack
3. Check Alerts on Firewall/IPS

Documentation:

1. PPT
2. Gantt Chart
3. Proposal

Along with this whole methodology, we will be showcasing a **Topology** for the designed isolated network. The ppt for this entire project is also to be shared.

Keywords: Intrusion Prevention System (IPS), Snort, Firewall, Topology, mitigation.

Table Of Contents

Scope Of Work

Sr.No.	Tasks	Pass / Fail	Comments
1.	Setup Virtual Switches		
2.	Setup Web Server		
3.	Setup Attacker Machine		
4.	Setup Normal User Machine		
5.	Install Pfsense and do Some basic configuration		
6.	Install Snort		
7.	Apply rules on snort		
8.	Test		
9.	Documentation		

Project Flow

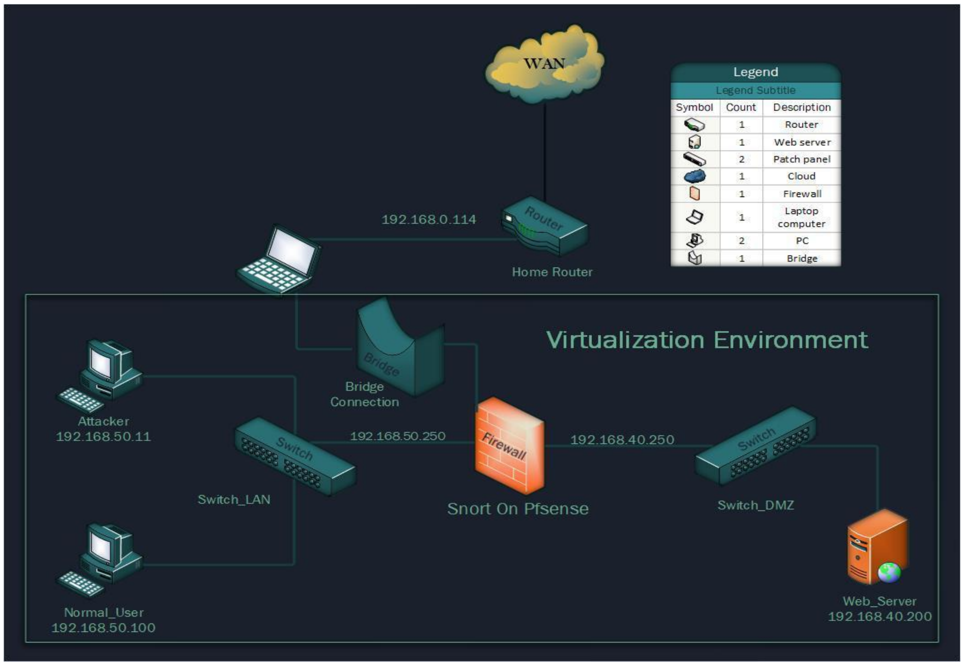
Analysis & Design:

1. Draft Environment
2. Install Needed ISO's

Draft Environment:

To set up the whole environment, first of all, we will design the topology then we will move further.

Setting Up Topology Diagram:

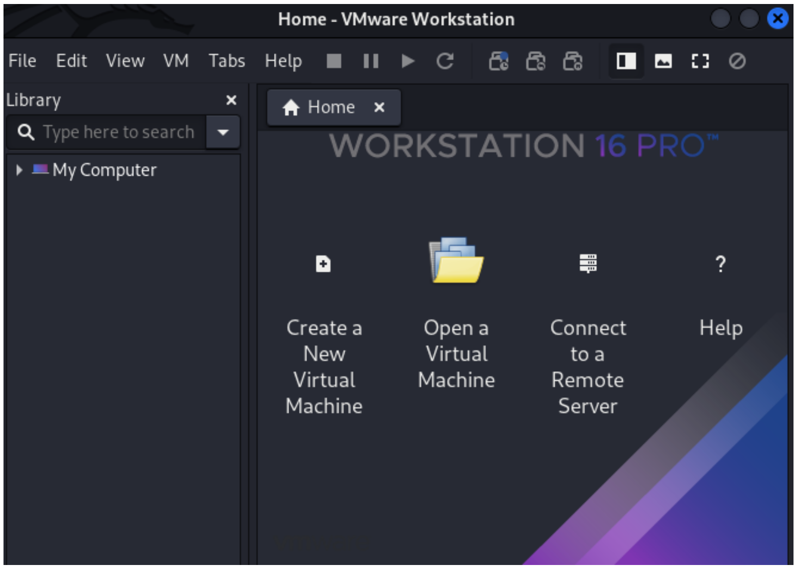


Symbol	Count	Description
	1	Router
	1	Web server
	2	Patch panel
	1	Cloud
	1	Firewall
	1	Laptop computer
	2	PC
	1	Bridge

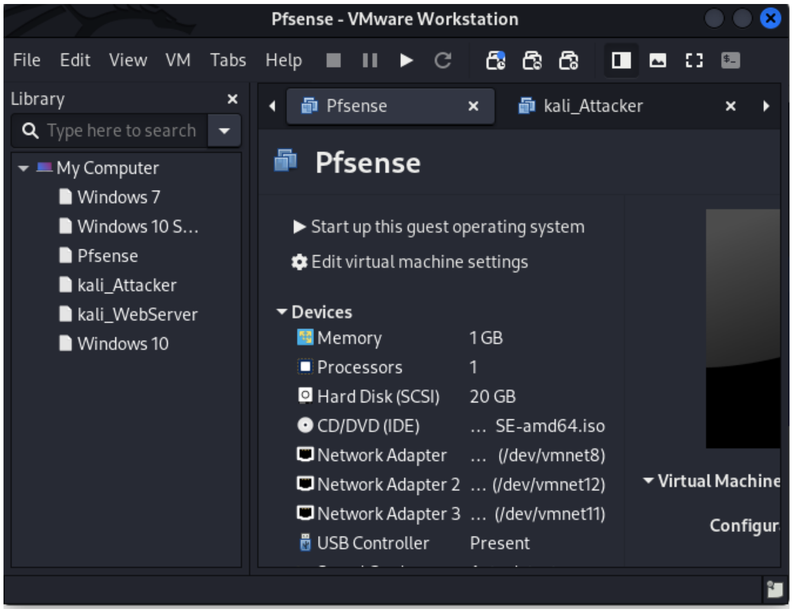
I have used MS Visio to design this topology, after this, we will be installing Vmware workstation Pro to implement this topology.

Setup VMware:

In this step firstly we will be installing VMware Workstation, then after installing it on a system, we will be downloading all of the ISO files and installing them into VMware.


Home - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Home
WORKSTATION 16 PRO™
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
Help

Now finally we have installed **VMware 16 Pro.** Now after this it's time to download &install all of the ISO



Devices

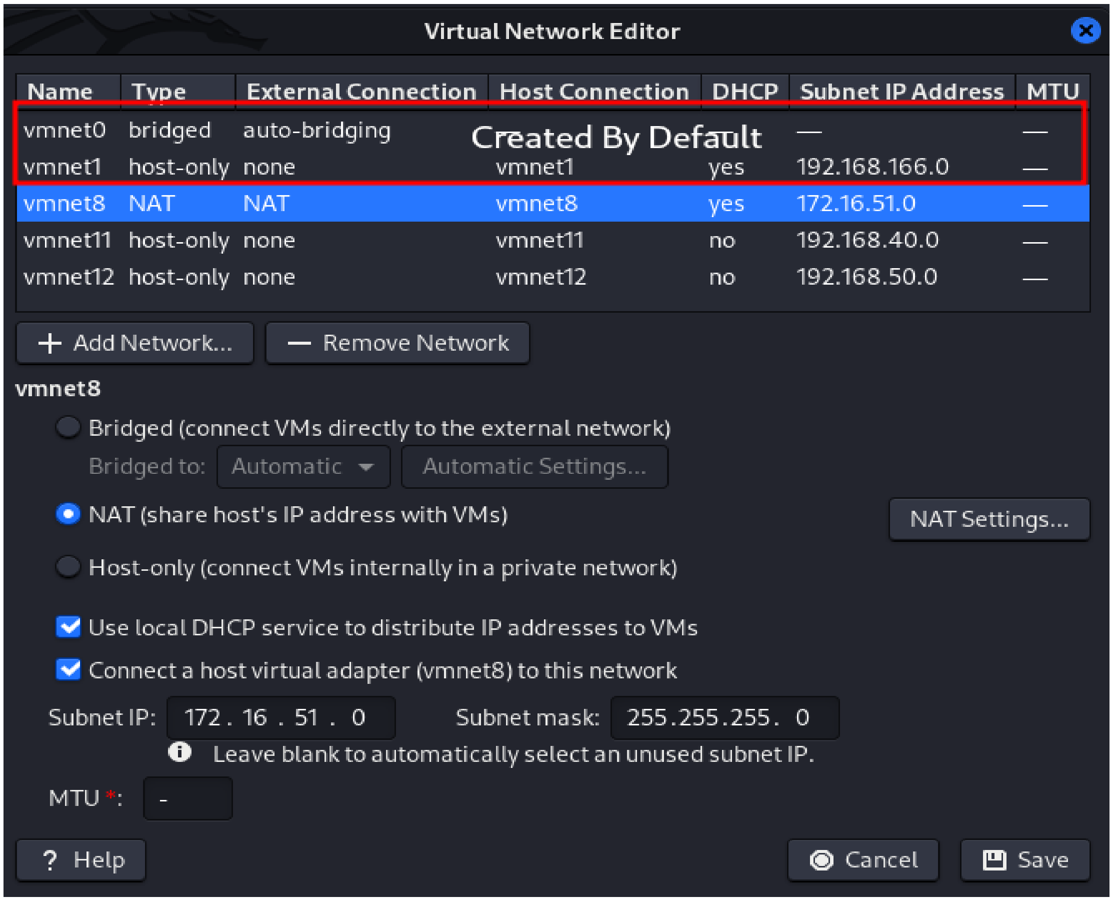
Memory	1 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	… SE-amd64.iso
Network Adapter	… (/dev/vmnet8)
Network Adapter 2	… (/dev/vmnet12)
Network Adapter 3	… (/dev/vmnet11)
USB Controller	Present

Now we have perfectly installed and done the basic configuration of all of the machines, so we can start using them.

Setting Up Virtual Switches:

Open the virtual network editor from the upper left corner in Vmware Pro and start setting up the following:

1. Create Vmnet 8 and set it up to Bridge Network and Enable DHCP
2. Create Vmnet 11 and set it up to Host-only mode and assign the IP address of ***192.168.40.0***.
3. Create Vmnet 12 set it up to Host-only mode and assign the IP address of ***192.168.50.0***.



Name	Type	External Connection	Host Connection	DHCP	Subnet IP Address	MTU
vmnet0	bridged	auto-bridging			—	—
vmnet1	host-only	none	vmnet1	yes	192.168.166.0	—
vmnet8	NAT	NAT	vmnet8	yes	172.16.51.0	—
vmnet11	host-only	none	vmnet11	no	192.168.40.0	—
vmnet12	host-only	none	vmnet12	no	192.168.50.0	—

Created By Default

vmnet8

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

● NAT (share host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

☑ Use local DHCP service to distribute IP addresses to VMs

☑ Connect a host virtual adapter (vmnet8) to this network

Subnet IP: 172 . 16 . 51 . 0 Subnet mask: 255.255.255. 0

Leave blank to automatically select an unused subnet IP.

MTU *: -

Now we have completed our first part which is **Analysis & Design**

Development:

1. Setup and Configure Web Server
2. Setup an Attacker Machine
3. Install and configure Pfsense Firewall
4. Set up Snort as an IDS/IPS
5. Configure Snort to defend against Brute Force Attack and LFI attack

Setup and Configure Web Server:

As we have already installed kali Linux as our web server and done the basic configuration e.g updating & upgrading, our next task would be to install LAMP and WordPress, then apply HTTP-Basic authentication on the ***admin*** and ***Wp-admin*** directories. So let's start the configuration.

***Note*:** In this process, we will be using **MariaDB** instead of **MySQL.**

Installing LAMP:

In the first part e.g. **Analysis & Design,** we had installed Linux, so now it's time to install Apache. Use the following commands to install Apache on Kali.

1. **sudo apt install apache2 apache2-utils**
2. **sudo service apache2 start**
3. **sudo service apache2 enable**

These commands will install it as well as start it and set it up to automatically start upon boot up.
Now our next step should be installing MariaDB.

Installing MariaDB:

To install MariaDB on Kali use the following command:

1. **sudo apt install mariadb**

This will install MariaDB on Kali then you have to do some basic configuration that is what you desire e.g. add users according to your choice then make a database for WordPress.
After installing **MariaDB** the next step would be to install **PHP** & **PHPMyAdmin**.

Installing PHP & PHPMyAdmin:

Installing **PHP** is almost the same procedure as for **Apache** and **MariaDB** so for installing **PHP** use the following command:

- **sudo apt install php**

This will install and do all the necessary configurations to run **PHP.**

After this we will be installing the **PHPMyAdmin** file from their website and extracting it into the following folder:

- **/var/www/html/admin**

This will do some basic configuration for the Admin panel, now you have to do some basic configuration as you desire.

Now we are done with installing **LAMP,** it's time to install WordPress

Installing WordPress:

Installing WordPress is not a very difficult task, first of all, you have to install a WordPress file from their website and simply extract it in the following folder:

- **/var/www/html/wordpress**

So, after extracting it, connect it with the database and open the following URL:

- **localhost/wordpress**

This will open the WordPress installation page for You, so you can easily put the required details and install it easily, and can view your website with the same URL.

Finally, we have successfully been able to use our fully functional website, but we want to make it vulnerable for demonstration purposes, so we will install the following plugin from ExploitDB

- **WordPress Plugin Site Editor 1.1.1**

This plugin will make our website vulnerable to the **Local File Inclusion** Attack

Now we have successfully configured our web server, the next step would be to apply **HTTP-Basic Authentication** on **/admin** & **/wordpress/wp-admin.** To make them password protected.

Making Admin Directories Password Protected:

To make these directories password protected, we have to use the following commands.

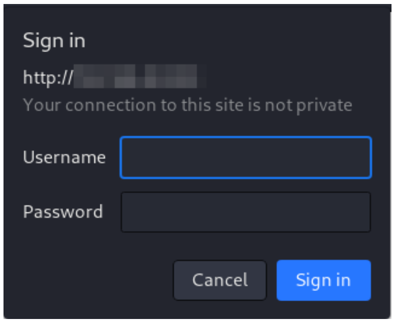
1. **sudo apt install nginx**
2. **sudo htpasswd -c /etc/nginx/.htpasswd *USER NAME***
3. **sudo nano /etc/apache2/sites-available/000-default.conf**

This will open the text editor for you, so scroll down to the bottom, and paste the following.

```
<Directory "/var/www/html/admin">
        AuthType Basic
        AuthName "admin area"
        AuthUserFile /etc/nginx/.htpasswd
        Require valid-user
</Directory>
```

```
<Directory "/var/www/html/wordpress/wp-admin">
        AuthType Basic
        AuthName "admin area"
        AuthUserFile /etc/nginx/.htpasswd
        Require valid-user
</Directory>
```

Then restart your Apache server, this will make those directories password protected like this:



Sign in

http://[redacted]

Your connection to this site is not private

Setup an Attacker Machine:

By default, Kali Linux comes with all the necessary hacking tools, so we don't have to install them separately, so we have already done the attacker machine installation in the previous step and already updated and upgraded it. So actually we don't have to do any kind of configuration at this point, so we can easily move further to the next step, which is installing a normal user machine.

Setup a Normal User Machine:

We have already done the installation of a normal user machine in the previous step and already updated it. So actually we don't have to do any kind of configuration at this point, so we can easily move further to the next step, which is installing a Pfsese firewall.

Setup a Pfsense Firewall:

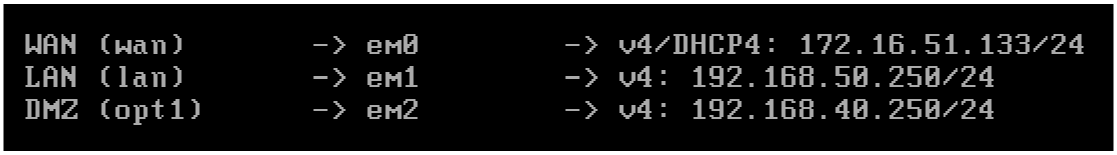
Setting up Pfsense in VMware is a bit tricky, so we have previously done the basic things, like installing and all these things. So the first step for us, at this point is to set up three interfaces for WAN, LAN, and DMZ. So, for this, we have to assign all three interfaces to Pfsense, which are:

1. **Vmnet 8**
2. **Vmnet 11**
3. **Vmnet 12**

And assign these respectively to

1. **WAN (Vmnet 8) em0**
2. **LAN (Vmnet 12) em1**
3. **DMZ(Vmnet 11) em2**

And assign IP addresses according to Topology.



```
WAN (wan)        -> em0        -> v4/DHCP4: 172.16.51.133/24
LAN (lan)        -> em1        -> v4: 192.168.50.250/24
DMZ (opt1)       -> em2        -> v4: 192.168.40.250/24
```

Now we have done all the necessary configuration of the Pfsense firewall, so it’s time to install and configure Snort on Pfsense.

Installing and Configuring Snort on Pfsense:

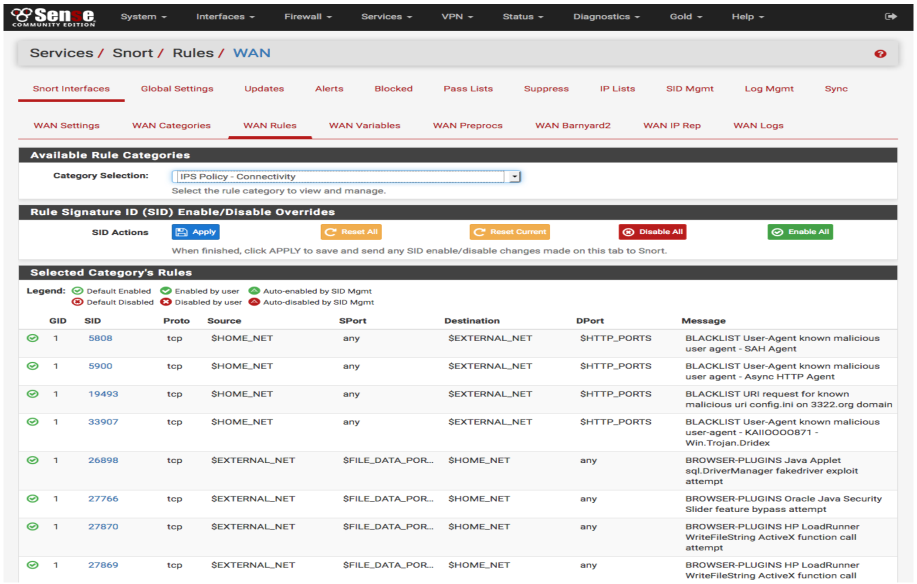
To install Snort, simply open the web portal of pfsense and head over to packages and search for snort and simply click install. This will install snort on pfsense. So now it’s time to do some basic configuration, so go to snort and add all three interfaces, then update them. After updating them, go to custom rules and add the following rules.

1. **# alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SERVER-WEBAPP Site Editor WordPress plugin local file access attempt"; flow:to_server,established; content:"/ajax_shortcode_pattern.php?"; fast_pattern:only; http_uri; content:"ajax_path="; nocase; http_uri; metadata:policy max-detect-ips drop, service http; reference:cve,2018-7422; classtype:web-application-attack; sid:47424; rev:1;)**

2. **# alert tcp any any -> 192.168.40.200 80 (msg:"HTTP AUTH brute force attack"; content:"535 Authentication failed."; nocase; classtype:attempted-user; threshold:type threshold, track by_src, count 2, seconds 60; sid:1000500; rev:6;)**

These rules will alert whenever the attacks occur e.g **LFI / Brute Force Attack,** so now we are ready to mitigate the attacks, for this, initially, you have to apply these rules on all three interfaces and enable all of them.

Now, by the end of this step, we can get alerts, if something suspicious happens in our network. So on onwards, we can move towards the next step which is testing if the applied setting worked or not.



Services / Snort / Rules / WAN

Available Rule Categories

Category Selection: IPS Policy - Connectivity

Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Selected Category's Rules

Legend: Default Enabled, Enabled by user, Auto-enabled by SID Mgmt, Default Disabled, Disabled by user, Auto-disabled by SID Mgmt

	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	1	5808	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - SAH Agent
✓	1	5900	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - Async HTTP Agent
✓	1	19493	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST URI request for known malicious uri config.ini on 3322.org domain
✓	1	33907	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user-agent - KAII0000871 - Win.Trojan.Dridex
✓	1	26898	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS Java Applet sql.DriverManager fakedriver exploit attempt
✓	1	27766	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS Oracle Java Security Slider feature bypass attempt
✓	1	27870	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function call attempt
✓	1	27869	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function call

Testing:

We will do the testing in two of the following phases.

1. **Testing whether that snort can detect a Brute Force attack or not.**
2. **Testing whether that snort can detect an LFI attack or not.**

Testing Brute Force Attack:

To launch a brute force attack against the Web Server, head over to the attacker machine and use the following command.

```
nmap -p80 --script http-brute --script-args 'http-brute.hostname=192.168.40.200,http-brute.method=POST,http-brute.path=/admin/,userdb=/usr/share/nmap/nselib/data/usernames.lst,passdb=/usr/share/nmap/nselib/data/passwords.lst' -v 192.168.40.200 -n
```

This command will brute force the password of HTTP-Basic Authentication, but it will fail because of snort IPS, Now go to Pfsense portal and go to alerts, in the tab of alerts you will be seeing the alerts.

Testing LFI Attack:

Launching an LFI attack is simpler than a Brute Force attack, Head over to an attacker machine open a normal browser, and paste the following in the browser.

- **http://192.168.40.200/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd**

This URL will request a **passwd** file from the web server, but we will be getting an alert on snort, so now we have successfully tested our snort rules.

Acronyms

IPS = Intrusion Prevention System
HTTP = HyperText Transfer Protocol
LFI = Local File Inclusion
XSS = Cross-Site Scripting
IDS = Intrusion Detection System
DHCP = Dynamic Host Configuration Protocol
IP = Internet Protocol
LAMP = Linux, Apache, MySQL, PHP
URL = Universal Resource Locator