Operation Security Using SNORT , PFSense

2022

Portfolio Project

PROPOSED: Muhammad Affan

TABLE OF CONTENTS

INTRODUCTION

Web application security is a central component of any web-based business. The global nature of the Internet exposes web properties to attack from different locations and various levels of scale and complexity. Web application security deals specifically with the security surrounding websites, web applications and web services such as APIs.

The world today runs on apps, from online banking and remote work apps to personal entertainment delivery and e-commerce. It's no wonder that applications are a primary target for attackers, who exploit vulnerabilities such as design flaws as well as weaknesses in APIs, open-source code, third-party widgets, and access control.

Common attacks against web applications include:

- Brute force
- Credential stuffing
- SQL injection and form jacking injections
- Cross-site scripting
- Cookie poisoning
- Man-in-the-middle (MITM) and man-in-the-browser attacks
- Sensitive data disclosure
- Insecure deserialization
- Session hijacking

DESCRIPTION OF THE PROJECT

This project is about the protection of web applications that are protected using passwords and usernames . We used Brute Force attacks to test in our project .

By performing a brute force password auditing against web servers that are
using HTTP authentication with Nmap and detect this attack using snort IDS/IPS on PFSense Firewall.

NEED FOR THE STUDY

As technology changes, it becomes increasingly challenging for businesses of all types to keep their personal and customer's information on the web secure.

Web security is important to keeping hackers and cyber-thieves from accessing sensitive information. Without a proactive security strategy, businesses risk the spread and escalation of malware, attacks on other websites, networks, and other IT infrastructures. If a hacker is successful, attacks can spread from computer to computer, making it difficult to find the origin.

Hacked websites are mostly used to retarget your potential customers and your website visitors. Another reason why website security is important - is to keep your customers safe.

We've seen a 150% growth in vulnerabilities reported in 2021 compared to 2020 which is a significant increase. Meanwhile, 29% of the WordPress plugins with critical vulnerabilities received no patch.

A study was made that stated that **there is an attack every 39 seconds** on average on the web and the non-secure usernames and passwords that are being used give attackers more chance of success.

DEFINITIONS

BRUTE FORCE ATTACK

A brute force attack is uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. The attacker submits combinations of usernames and passwords until they finally guess correctly.

Once successful, the actor can enter the system masquerading as the legitimate user and remain inside until they are detected. They use this time to move laterally, install back doors, gain knowledge about the system to use in future attacks, and, of course, steal data.

Brute force attacks have been around as long as there have been passwords. They not only remain popular, but are on the rise due to the shift to remote work.

WEBSERVER:

A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job of a web server is to display website content through storing, processing and delivering webpages to users. Besides HTTP, web servers also support SMTP (Simple Mail Transfer Protocol) and FTP (File Transfer Protocol), used for email, file transfer and storage.

FIREWALL:

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

INTRUSION DETECTION SYSTEM:

An intrusion detection system (IDS) is an application that monitors network traffic and searches for known threats and suspicious or malicious activity. The IDS sends alerts to IT and security teams when it detects any security risks and threats.

Most IDS solutions simply monitor and report suspicious activity and traffic when they detect an anomaly. However, some can go a step further by taking action when it detects anomalous activity, such as blocking malicious or suspicious traffic.

IDS tools typically are software applications that run on organizations’ hardware or as a network security solution. There are also cloud-based IDS solutions that protect organizations’ data, resources, and systems in their cloud deployments and environments.

INTRUSION PREVENTION SYSTEM:

An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.

OBJECTIVES

The objective of this project is to secure the web servers so that no attacker can use any of the techniques to damage or penetrate into the webserver . Using HTTP Brute Force attack we will check whether the attacker is able to get the user credentials of the website . We will use PFSense and Snort to block the attacker from getting into the webpage .

MATERIALS

VIRTUAL MACHINES :

I have used 4 virtual machines in this which are

1. Kali Linux (Attacker Machine)
2. Ubuntu Linux (Apache 2 Webserver)
3. Windows 10 (Normal User)
4. PFSense

WEBSERVER:

In this project Apache2 webserver is used as a victim webpage. The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

The Apache HTTP Server ("httpd") was launched in 1995 and it has been the most popular web server on the Internet since April 1996. It has celebrated its 25th birthday as a project in February 2020.

The Apache HTTP Server is a project of The Apache Software Foundation.

FIREWALL:

PFSense is used as a firewall which is a good option as it provides free network firewall distribution, based on the FreeBSD operating system with a custom kernel and including third party free software packages for additional functionality. pfSense software, with the help of the package system, is able to provide the same functionality or more of common commercial firewalls, without any of the artificial limitations. It has successfully replaced every big name commercial firewall you can imagine in numerous installations around the world, including Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro, and more.

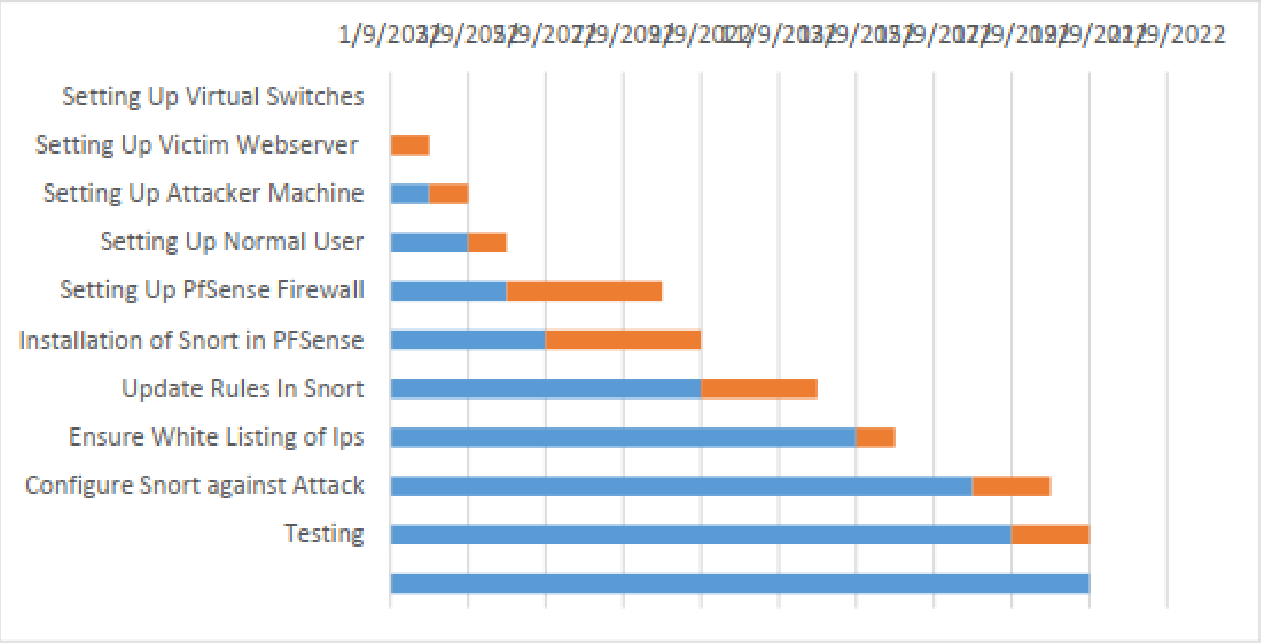
SNORT:

Snort is a good option for a IDS/IPS . SNORT is a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging. SNORT uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activity.

Using SNORT, network admins can spot denial-of-service (DoS) attacks and distributed DoS (DDoS) attacks, Common Gateway Interface (CGI) attacks, buffer overflows, and stealth port scans. SNORT creates a series of rules that define malicious network activity, identify malicious packets, and send alerts to users .

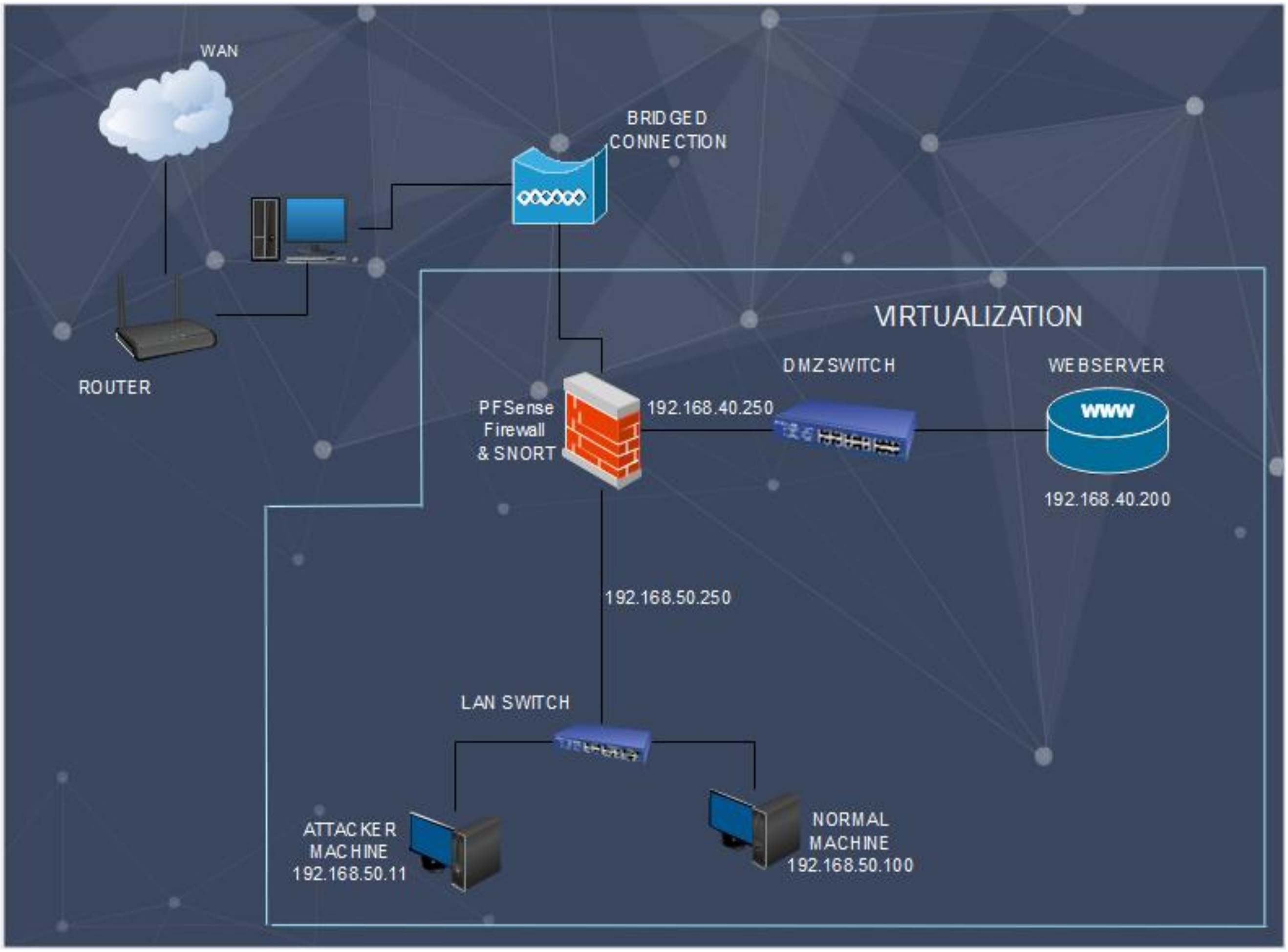
GANTT CHART

TASK NAME	PROGRESS	START DATE	END DATE	DURATION
Setting Up Virtual Switches	Completed	01-Sep-22	02-Sep-22	1
Setting Up Victim Webserver	Completed	02-Sep-22	03-Sep-22	1
Setting Up Attacker Machine	Completed	03-Sep-22	04-Sep-22	1
Setting Up Normal User	Completed	04-Sep-22	05-Sep-22	1
Setting Up PfSense Firewall	Completed	05-Sep-22	09-Sep-22	4
Installation of Snort in PFSense	Completed	09-Sep-22	13-Sep-22	4
Update Rules In Snort	Completed	13-Sep-22	16-Sep-22	3
Ensure White Listing of Ips	Completed	16-Sep-22	17-Sep-22	1
Configure Snort against Attack	Completed	17-Sep-22	19-Sep-22	2
Testing	Completed	19-Sep-22	21-Sep-22	2



PROJECT-FLOW

Setting up a Topology Diagram:



Development

Setting up the virtual environment :

First we will create 2 virtual network adapters :

LAN VMnet11 -→ 192.168.40.0

LAN2 VMnet12 -→ 192.168.50.0

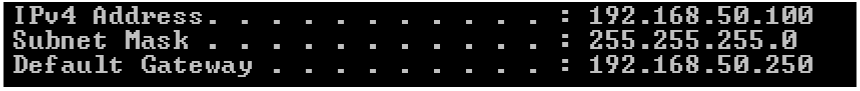
1. ### Setup a Normal user machine :

   Windows 7 is used as a normal user machine . Configuration is as follows

   Static IP : 192.168.50.100

   Subnet Mask : 255.255.255.0

   Default Gateway : 192.168.50.250



```
IPv4 Address. . . . . . . . . . . : 192.168.50.100
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.50.250
```

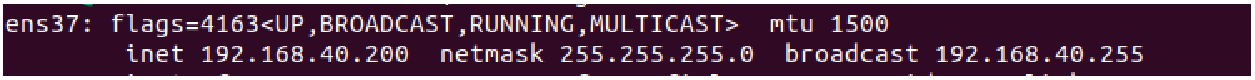
2. ### Setup a Victim Webserver machine :

   We will setup a Ubuntu Linux machine in VMWare Workstation and install Apache 2 Webserver in Ubuntu machine .
   To install apache webserver we will follow the following commands :
   Sudo apt install -y apache2 apache2-util

This will install the apache2 webserver in the machine and to check the status of the webserver we will enter the command
Sudo systemctl status apache2

To enable user authentication in the webpage we will enter the following command :
Sudo htpasswd -c /etc/apache2/.htpasswd (username)
Then we will enter the password for the username we entered before .

Network Configuration
Static IP : 192.168.40.200
Subnet Mask : 255.255.255.0
Gateway : 192.168.40.255

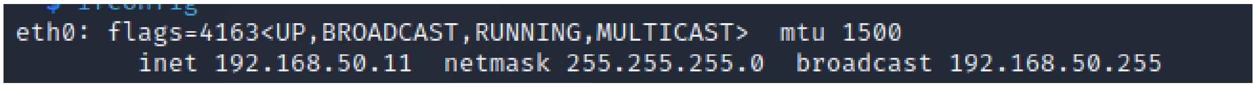


```
ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.200  netmask 255.255.255.0  broadcast 192.168.40.255
```

3. Setup an Attacker machine :

Kali Linux is used as an attacker machine . The configurations are as follows

Network Configuration
Static IP : 192.168.50.11
Subnet Mask : 255.255.255.0
Gateway : 192.168.50.255



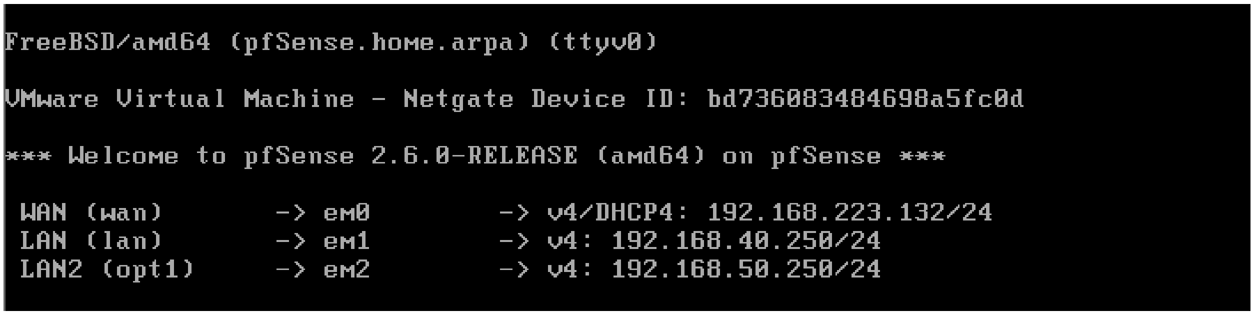
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.11  netmask 255.255.255.0  broadcast 192.168.50.255
```

4. Setup PFSense and Snort:

Setup a PFSense Machine on VMWare Workstation . We will add network adapters which will be :

LAN VMnet11

LAN2 VMnet12



```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: bd736083484698a5fc0d

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.223.132/24
 LAN (lan)       -> em1        -> v4: 192.168.40.250/24
 LAN2 (opt1)     -> em2        -> v4: 192.168.50.250/24
```

Then we will setup SNORT package in PFSense using package installer .

We will create an account on snort for the oinkmaster code and enter that code in SNORT and then download the VRT rules in Snort package . After downloading the Rules we will update the rules once again . We will install all the rules including snort community , VRT , emerging threat rules . Then we will create an Alias and Pass list .

To configure Snort for port scan detection we have to add a LAN2 interface to Snort Interfaces . And check all Snort GPLv2 Community Rules.

We also have to add custom rules to defend against HTTP Brute Force Attack . To do this we have to add this line

```
alert tcp any any -> 192.168.40.200 80 (msg:"HTTP AUTH brute force attack"; classtype:attempted-user; detection_filter:track by_src, count 4,  seconds 1; sid:1000500; rev:6;)
```

TESTING

To perform testing of our firewall and rules we will perform an http Brute Force attack on our Webserver .

We will use Nmap tool and the http-Brute force script . The brute force script uses the database files usernames.lst and passwords.lst which are located at /nselib/data/ to try each password for every user to ultimately find a valid credential for a valid account .

To perform the Brute Force Attack we will use Nmap and the http-brute script .

We will use the command : nmap -script http-brute -p 80 192.168.40.200 -d –script-args http-brute.path=/auth-basic/

We will check alerts , blocked hosts . the attacker host will be blocked for 30 mins as we have configured , the normal users will still be able to have the access to the webserver during blocked period .

REFERENCES

https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/

https://www.techtarget.com/whatis/definition/Web-server

https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/

https://turbofuture.com/internet/How-to-Set-Up-an-Intrusion-Detection-System-Using-Snort-on-pfSense-20

https://www.snort.org/

https://pfsense.org/

https://hub.packtpub.com/brute-forcing-http-applications-and-web-applications-using-nmap-tutorial/