Network Evaluation

ACME Inc.

Lukas Smith

CMP314: Computer Networking 2

BSc Ethical Hacking Year 3

2021/22

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

.

Abstract

The following report shall document the results of a security investigation into ACME Incorperated's network. Due to circumstances of the previous network managers departure, a review into the network documentation found a lack of current documentation. As it is essential to have up to date documentation to ensure network security, ACME Incorporated has requested a complete network evaluation.

This Network Evaluation performed on ACME Inc's network includes how the network was mapped, its current security weaknesses, an overall evaluation of the network, and how it should be improved. The report also includes a detailed network map, a subnet table with subnet calculations, and a table detailing the hosts currently in use and their open ports.

It was found during the investigation that the network is very insecure, as such several recommendations have been made. As well as this, some suggestions have been made regarding the network topology. The topology alongside the current subnetting in use was discussed and how it could be changed to fit the company requirements better.

Several main security concerns were pointed out during the Evaluation, mainly that the devices and their software were outdated. There were also significant concerns around default credentials and password complexity, leading to the suggestion of implementing a password policy across the network. Finally, several services are running on the network that are insecure or unnecessary.

.

Contents

.

.

.

1 INTRODUCTION

The following report shall document the results of a security investigation into ACME Incorporated's network. Due to circumstances of the previous network managers departure, a review of the network documentation found a lack of current documentation. As it is essential to have up to date documentation to ensure network security, ACME Incorporated has requested a complete network evaluation.

Therefore, this report aims to evaluate the current state of the network and its existing security. Following ACME Incorperateds request, this document shall include; a detailed diagram of the network, a subnet table detailing all subnets in use, an assessment of discovered security weaknesses, including available mitigations, and a critical evaluation of the whole network design.

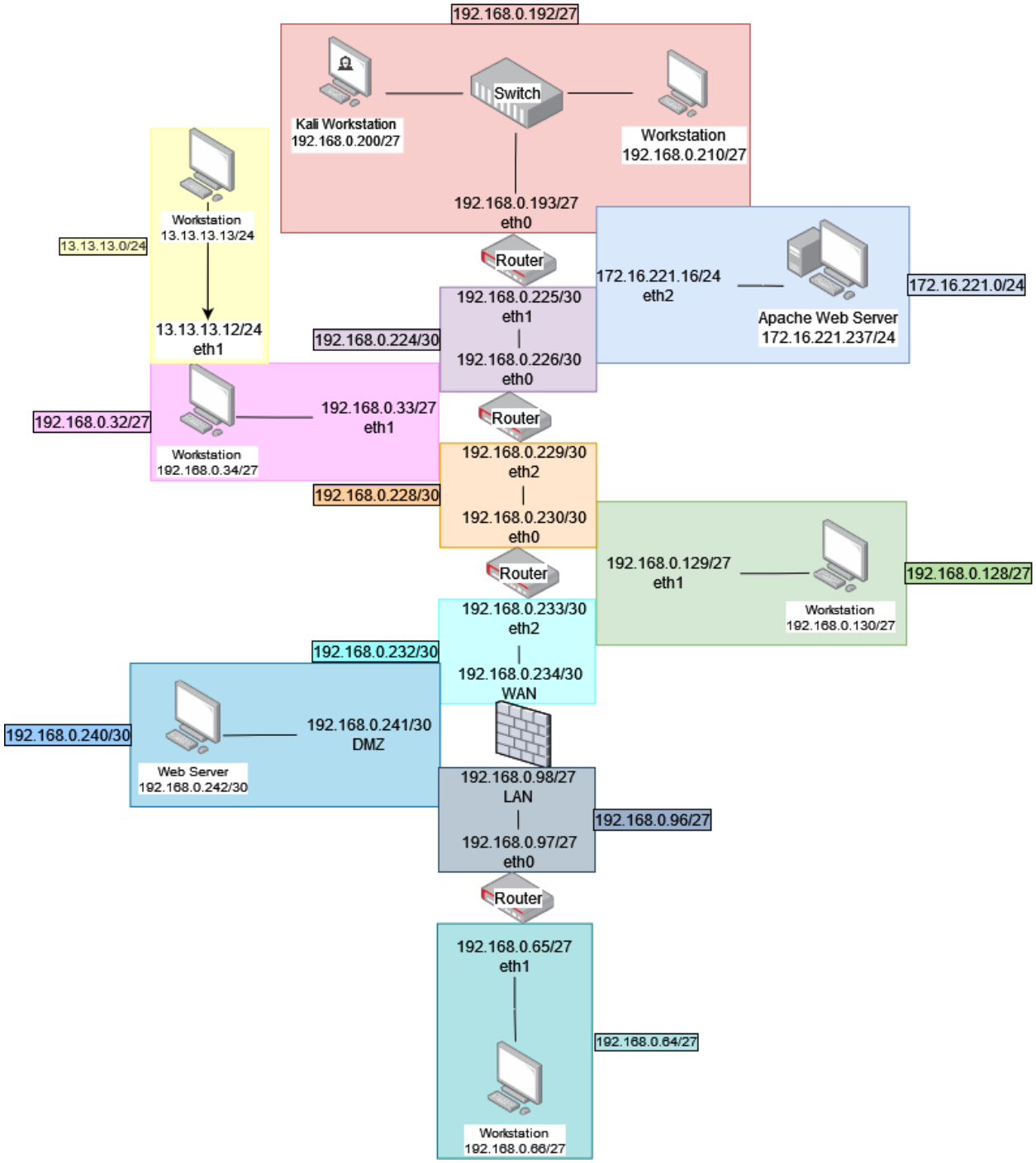
The tester has not been informed of ACME Incorperateds requirements regarding host needs and concerns about network instability. Meaning that multiple suggestions shall be noted in terms of the network's topology and the current subnetting in use; this should hopefully leave the company with multiple ideas that can be discussed. The one best suited to the company's requirements can then be chosen.

The tester has been provided with a Kali Linux machine (with the credentials root:toor) within the network to complete this investigation. However, no tools outwith ACME Incorporations installation of the machine will be used, per the companies request due to concerns regarding unproven tools.

As the Kali machine was isolated from the testers main machine, files could not be transferred to or from the device; instead, the tester has decided to use screenshots to detail the security investigation results.

2 NETWORK BREAKDOWN

2.1 NETWORK MAP



2.2 SUBNET TABLE

Subnet Address	Host Address Range	Broadcast Address	Used IP Addresses	Subnet Mask
13.13.13.0	13.13.13.1 – 13.13.13.254	13.13.13.255	13.13.13.12 13.13.13.13	255.255.255.0
172.16.221.0	172.16.221.1 – 172.16.221.254	172.16.221.255	172.16.221.16 172.16.221.237	255.255.255.0
192.168.0.32	192.168.0.33 – 192.168.0.62	192.168.0.63	192.168.0.33 192.168.0.34	255.255.255.224
192.168.0.64	192.168.0.65 – 192.168.0.94	192.168.0.95	192.168.0.65 192.168.0.66	255.255.255.224
192.168.0.96	192.168.0.97 – 192.168.0.126	192.168.0.127	192.168.0.97 192.168.0.98	255.255.255.224
192.168.0.128	192.168.0.129 – 192.168.0.158	192.168.0.159	192.168.0.129 192.168.0.130	255.255.255.224
192.168.0.192	192.168.0.193 - 192.168.0.222	192.168.0.223	192.168.0.193 192.168.0.200 192.168.0.210	255.255.255.224
192.168.0.224	192.168.0.225 – 192.168.0.226	192.168.0.227	192.168.0.225 192.168.0.226	255.255.255.252
192.168.0.228	192.168.0.229 – 192.168.0.230	192.168.0.231	192.168.0.229 192.168.0.230	255.255.255.252
192.168.0.232	192.168.0.233 – 192.168.0.234	192.168.0.235	192.168.0.233 192.168.0.234	255.255.255.252
192.168.0.240	192.168.0.241 – 192.168.0.242	192.168.0.243	192.168.0.241 192.168.0.242	255.255.255.252

See

Appendix F – Subnet Calculations for subnet calculations

2.3 USED IPS FURTHER DETAIL

This section contains a list of devices and their open ports for clarification.

2.3.1 Machines

Device Name	Used IPs	Ports	Services
Workstation	13.13.13.13	TCP 22	ssh
		UDP 631 (filtered)	ipp
		UDP 5353	zeroconf
Apache Web Server	172.16.221.237	TCP 80	http
		TCP 443	https
		UDP 5353	zeroconf
Workstation	eth0 - 192.168.0.34 eth1 - 13.13.13.12	TCP 22	ssh
		TCP 111	rpcbind
		UDP 111	rpcbind
		TCP 2049	nfs
		UDP 2049	nfs
		UDP 5353	zeroconf
Workstation	192.168.0.66	TCP 22	ssh
		TCP 111	rpcbind
		UDP 111	rpcbind
		TCP 2049	nfs
		UDP 2049	nfs
		UDP 5353	zeroconf
Workstation	192.168.0.130	TCP 22	ssh
		TCP 111	rpcbind
		UDP 111	rpcbind
		UDP 631 (filtered)	Ipp
		TCP 2049	nfs
		UDP 2049	nfs
		UDP 5353	zeroconf
Kali Workstation	192.168.0.200	TCP 22	ssh
		TCP 111	rpcbind
		UDP 111	rpcbind
		TCP 3389	ms-wbt-server
Workstation	192.168.0.210	TCP 22	ssh
		TCP 111	rpcbind
		UDP 111	rpcbind
		UDP 631 (filtered)	ipp
		TCP 2049	nfs
		UDP 2049	nfs
		UDP 5353	zeroconf

Web Server	192.168.0.242	TCP 22	ssh
		TCP 80	http
		TCP 111	rpcbind
		UDP 111	rpcbind
		UDP 631 (filtered)	ipp
		UDP 5353	zerconf

2.3.2 Routers and Firewall

Device Name	Used IPs	Ports	Services
Router 1	eth0 - 192.168.0.193 eth1 - 192.168.0.225 eth2 - 172.16.221.16	TCP 22	ssh
		TCP 23	telnet
		TCP 80	http
		UDP 123	ntp
		UDP 161	snmp
		TCP 443	https
Router 2	eth0 - 192.168.0.226 eth1 - 192.168.0.33 eth2 - 192.168.0.229	TCP 23	telnet
		TCP 80	http
		UDP 123	ntp
		UDP 161	snmp
		TCP 443	https
Router 3	eth0 - 192.168.0.230 eth1 - 192.168.0.129 eth2 - 192.168.0.233	TCP 23	telnet
		TCP 80	http
		UDP 123	ntp
		UDP 161	snmp
		TCP 443	https
Router 4	eth0 - 192.168.0.97 eth1 - 192.168.0.65	TCP 23	telnet
		TCP 80	http
		UDP 123	ntp
		UDP 161	snmp
		TCP 443	https
Firewall	WAN - 192.168.0.234 DMZ - 192.168.0.241 LAN - 192.168.0.98	TCP 53	domain
		UDP 53	domain
		TCP 80	http
		UDP 123	ntp
		TCP 2601	zebra
		TCP 2604	ospfd
		TCP 2605	bgpd

3 NETWORK MAPPING

The network mapping was broken into several sections as part of this network investigation. These sections are Host Discovery, Device Analysis, Further Scans and Firewall Investigation. In addition, vulnerability exploitation has also been included where appropriate to further the mapping process.

3.1 HOST DISCOVERY

3.1.1 Subnet Scanning

The tester started the network mapping by using the command 'ifconfig' to determine the subnet the Kali machine belonged to and to find the IP address it was assigned. As shown in ***Appendix A - IFCONFIG***, it was found that the machine had the subnet mask *255.255.255.224* and had the IP address *192.168.0.200*. This information was then used to do a subnet scan using the 'nmap' tool. Finally, the following command was run:

```
nmap 192.168.0.200/27
```

The result of this scan can be found in ***Appendix B – NMAP***. In addition, this scan revealed two additional hosts within the same subnet as the Kali machine. These are *192.168.0.193* and *192.168.0.210*. Of note in these results was a webserver hosted on *192.168.0.193*.

After discovering the list of subnets in ***Subnet Scanning Analysis,*** the tester did a further nmap scan on the address range of *192.168.0.0-255*. This scan confirmed the subnet ranges found and revealed several other devices found within these subnet ranges.

After the majority of the mapping phase had been completed, the tester then did a UDP scan of the entire network for comprehensiveness, which can be found at ***UDP Scans***.

3.1.2 Further Subnet Scanning

After discovering the device at *172.16.221.16* in ***Subnet Scanning Analysis***, a further subnet scan was done to find devices on this subnet. This scan revealed a webserver being hosted on *172.16.221.237*.

3.2 DEVICE ANALYSIS

3.2.1 Subnet Scanning Analysis

From the nmap scan results in Subnet Scanning, it was noted that port 80 was open on *192.168.0.193*, suggesting a webserver being hosted. By navigating to this site, it was found that the device was a 'VyOS Router'. As the SSH port and Telnet port were open, the tester decided to attempt to connect to the router using the device's default credentials (user: vyos, password: vyos) via Telnet. (VyOS, 2021)

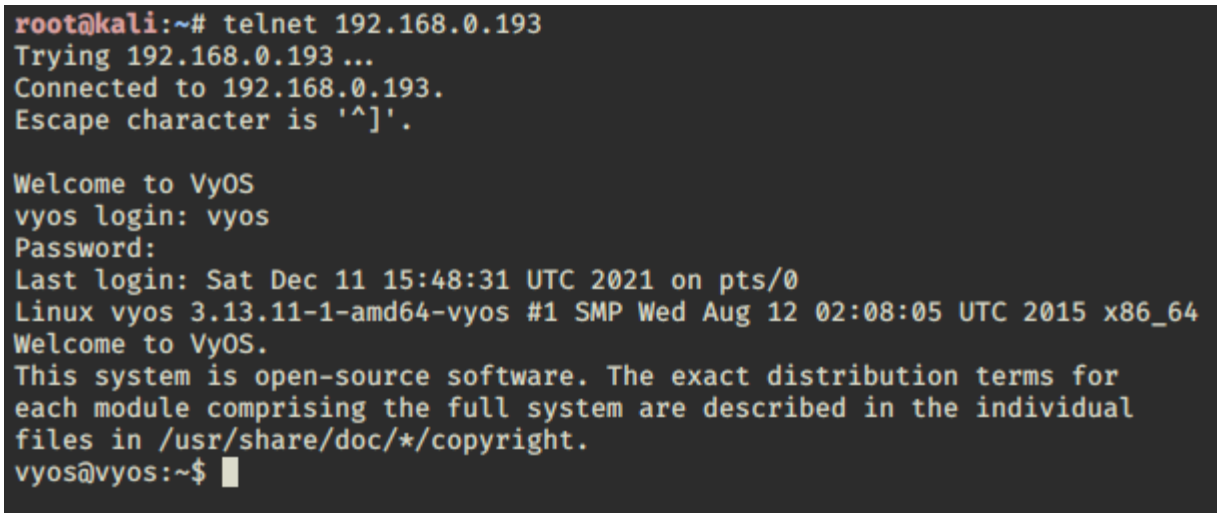


Figure 1 - Connecting to the VyOS Router

This router could also be accessed via SSH with the same credentials 'vyos:vyos'.

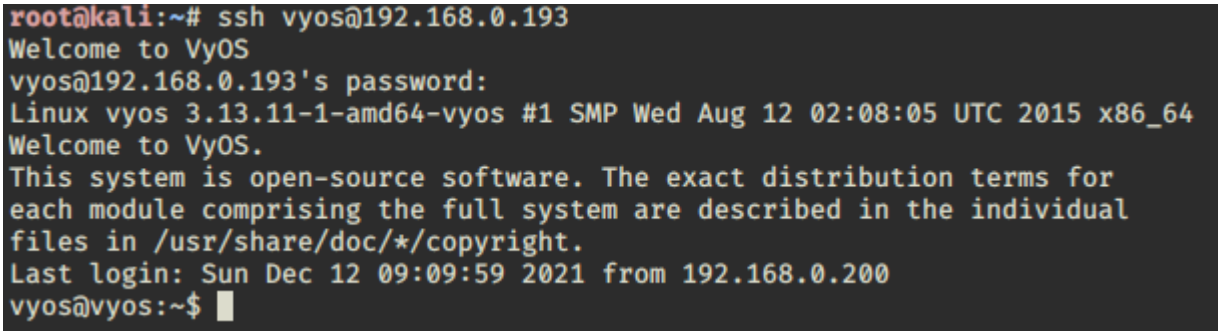


Figure 2 - SSHing into Router 1

From the router, the commands 'show interface' and 'netstat -rn' can be run to gather more information about the subnets and how that router connects to them and to find the routing table the router is using (seen in ***Appendix C – Router Show Interface and Netstat***). The output from these commands revealed a large majority of the subnets on the network. Next, the tester used these results to do another nmap scan of the *192.168.0.0-255* range, revealing the other routers on this IP range. Their router 'show interface' and 'netstat' commands are also shown in ***Appendix C***. This revealed several other devices which were added to the network map.

Revealed within the router route tables were subnets outwith the *192.168.0.0-255* range, which was also noted and used for further scans.

Also revealed in the router tables were subnets *192.168.0.64/27, 192.168.0.96/27*, which were not found when initially scanning the IP address range, meaning that they were inaccessible from the Kali machine. However, these subnets were connected through the device *192.168.0.234,* where the *192.168.0.240/30* subnet was also connected. From the previous nmap scans, a device in the *192.168.0.240/30* subnet had already been discovered. Therefore, this device created a suitable route for the tester to explore these subnets further. (See ***Firewall Investigation***)

One of the devices found on the same subnet as the kali machine – *192.168.0.210* – was noted to have an NFS port and an SSH port open. NFS (Network File System) is a protocol used in Linux to share files across a network. The tester created a new directory and mounted the NFS share to the Kali machine.

```
root@kali:~# mkdir ~/NFS210
```

Figure 3 - Creating a directory to store the NFS

```
root@kali:~# mount 192.168.0.210:/ ~/NFS210
```

Figure 4 - Mounting the NFS

The files '/etc/passwd' and '/etc/shadow' were then copied from the NFS mount onto the testers desktop and passed through 'unshadow', a John the Ripper utility that combines the two files. Finally, these files are combined in a format that can be passed through 'John', which is used to brute force weak passwords using a password list.

```
root@kali:~/Desktop# unshadow passwd shadow > psswds.txt
```

Figure 5 - Using unshadow on the passwd and shadow files

Using this file and the wordlist 'rockyou', a comprehensive wordlist containing many popular leaked passwords, the command John was then run to find any weak passwords on all users. This command returned one set of credentials, 'xadmin:plums'.

```
root@kali:~/Desktop# john --wordlist=rockyou.txt psswds.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
plums            (xadmin)
1g 0:00:00:48 DONE (2021-12-11 19:28) 0.02067g/s 3471p/s 3471c/s 3471C/s rachael2..playpen
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Figure 6 - Results from John the Ripper

These credentials allowed for a successful login to *192.168.0.210* as 'xadmin' via SSH. Additionally, to see if any of the devices shared credentials, the tester then tried them out on several other devices. It was found that the credentials also worked on *192.168.0.34* through SSH.

As a part of testing shared credentials, the tester also tried this combination to log in to *192.168.0.130* from the kali machine. Unfortunately, this login was unsuccessful as a Public Key was required. However, the device could be logged into through *192.168.0.34* successfully.

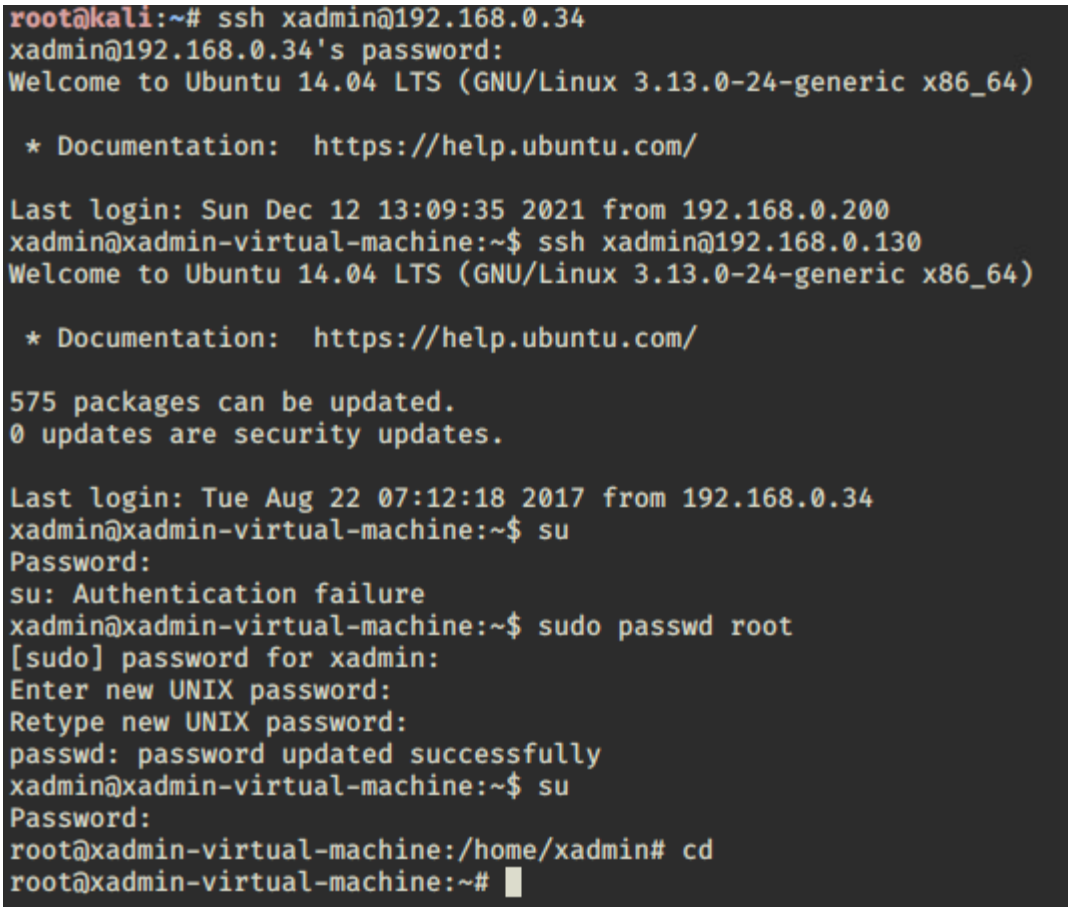


Figure 7 - Logging into 192.168.0.130 and getting root

Once logged into *192.168.0.130*, the account 'xadmin' has significant enough permissions to change the root password on the device. Changing the password allowed the tester to log in as root and add a set of SSH keys into the device; this allowed the tester to log in directly from the Kali device.

When the tester first logged in to *192.168.0.34* the command 'history' was run, and this revealed a previous SSH connection to the device *13.13.13.13*, using the same xadmin username. When running 'ifconfig' it was found that this device was connected through *13.13.13.12* on the eth1 port.

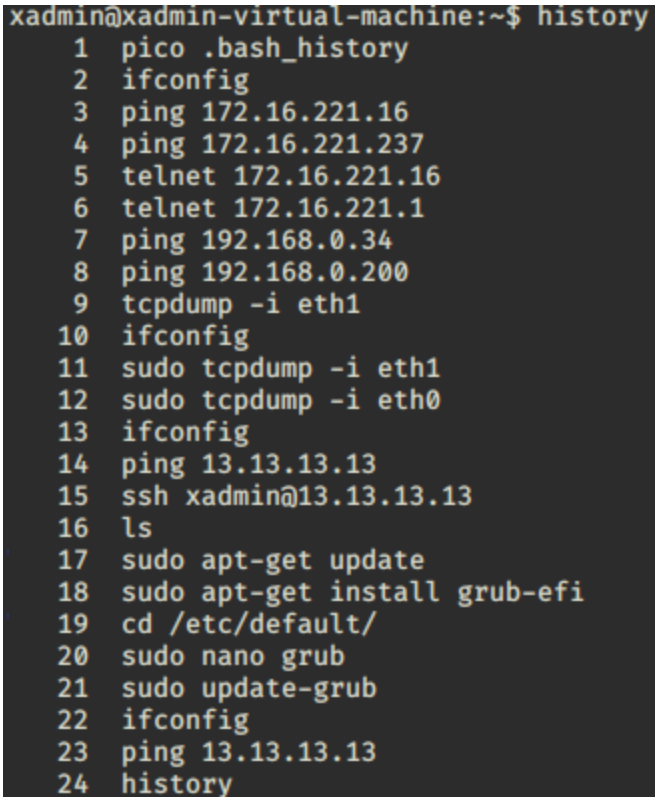


Figure 8 - History of 192.168.0.34

The 'xadmin:plums' credentials used on the other devices did not work when trying to ssh from *192.168.0.34* to *13.13.13.13*. The tester tried pinging *13.13.13.13* from the Kali machine and received the error 'Destination Net Unreachable', suggesting that the tester would have to access *13.13.13.13* through a tunnel through *192.168.0.34* as it was not directly accessible from the Kali Machine.

The root user is required when creating an SSH tunnel. As the tester was currently logged into 'xadmin', privilege escalation was required. In the same way, as on *192.168.0.130* the tester changed the password for the root account and then logged into it.

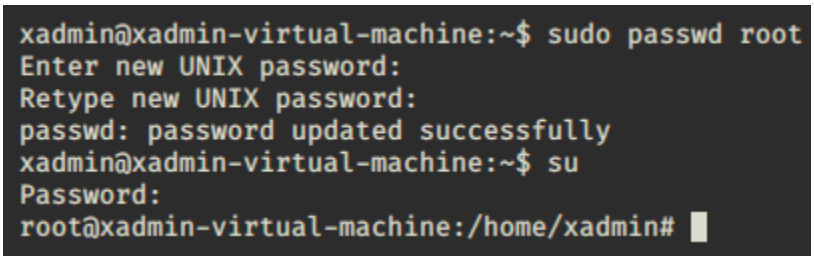


Figure 9 - Changing root password and logging into root

A tunnel was then set up using the root account with the IP addresses *3.3.3.1* and *3.3.3.2* and the device 'tun2'. The tester first edited the '/etc/ssh/sshd_config' file as root to allow tunnelling and then restarted the SSH service. A tunnel was then created between *3.3.3.1* and *3.3.3.2* to allow traffic to be sent through *192.168.0.34*. To allow traffic to be forwarded, the file 'fowarding' on the *192.168.0.34*

device was modified to 1. Finally, to finish setting up the connection, NAT was configured on *192.168.0.34,* and the connection was successfully established.

See ***13.13.13.13*** for screenshots.

After this tunnel was created, the tester could scan the *13.13.13.13* device (***13.13.13.13 Scan***). The scan result revealed the only open port, 22 (SSH). Hydra was run (using the Metasploit password list, as rockyou took too long) to brute-forece the credentials to login via SSH and gain access to the device. Hydra successfully found the credentials 'xadmin:!gatvol', which allowed for a login to the device.

```
root@kali:~# hydra -l xadmin -P /usr/share/wordlists/metasploit/password.lst 13.13.13.13 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-12 20:47:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 88397 login tries (l:1/p:88397), ~5525 tries per task
[DATA] attacking ssh://13.13.13.13:22/
[22][ssh] host: 13.13.13.13   login: xadmin   password: !gatvol
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-12 20:47:16
```

Figure 10 - Using hydra on 13.13.13.13

3.2.2 Further Subnet Scanning Analysis

The same VyOS HTTP site was running on *172.16.221.16*, so the tester attempted to log in to the router the same way the other routers were accessed. This method was successful, and displaying the routing table confirmed its place in the network map.

3.2.3 Firewall Investigation

The previous sections determined that the rest of the network would be accessible through the *192.168.0.240* subnet. Therefore, the only device on this subnet, *192.168.0.242,* was the best path for the tester. First, hydra was used to brute-force the credentials for the device. The password list 'rockyou' was once again used. Hydra was successful and found the login to be 'root:apple'

```
root@kali:~# hydra -l root -P /root/Desktop/rockyou.txt 192.168.0.242 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-12 00:01:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.0.242:22/
[STATUS] 178.00 tries/min, 178 tries in 00:01h, 14344223 to do in 1343:06h, 16 active
[STATUS] 138.00 tries/min, 414 tries in 00:03h, 14343987 to do in 1732:22h, 16 active
[22][ssh] host: 192.168.0.242   login: root   password: apple
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-12 00:07:09
```

Figure 11 - Hydra finds SSH login for root on 192.168.0.242

The tester logged into *192.168.0.242* through SSH and edited the '/etc/ssh/sshd_config' file to allow tunnelling and then restarted the SSH service.

The tester then created a tunnel on *1.1.1.1* and *1.1.1.2* to allow data to be sent through *192.168.0.242*. However, this did not forward the traffic successfully; to do this, the file 'forwarding', which allows forwarding traffic, had to be changed to 1. After doing this, the route to the host was added, followed by the route to the subnet. Finally, NAT was configured on device *192.168.0.242*, and the connection was successfully established.

Following this, the tester was able to run a nmap scan on the *192.168.0.64/27* subnet, meaning the tunnel was created and was forwarding traffic successfully.

See ***192.168.0.64/27*** for screenshots.

After setting up the tunnel, the tester did a further nmap scan of the address *192.168.0.234*. Unfortunately, this address was not in the original nmap scans, as it was discovered that all the ports were filtered before the tunnel was created. Therefore, scanning this device revealed a series of open ports (See ***192.168.0.234 Scan***). Noting that port 80 was open, the address was navigated through a browser which revealed a login form for pfSense, an Open Source Firewall distribution. The tester could log in to this page using the default credentials for this distribution (admin:pfsense (Netgate Docs, 2020)). Logging into the portal revealed all of the firewalls connections, and the network map was updated to show this.

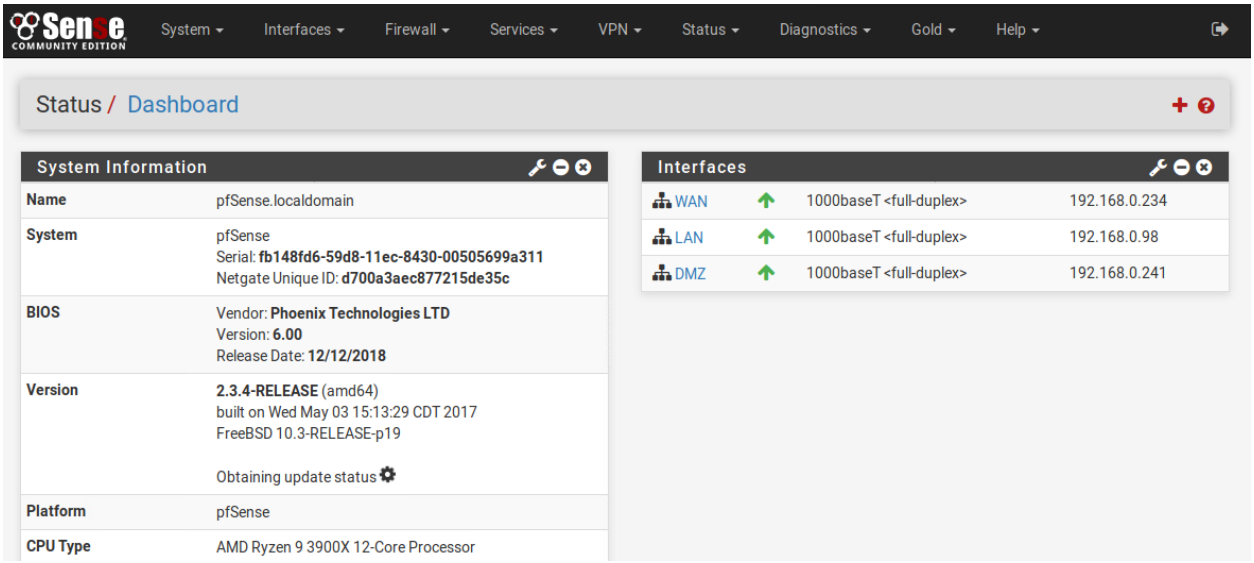


Figure 12 - PFSense Dashboard with Interfaces

From this point in the mapping phase, the tester would have significant enough access to disable the firewall entirely or configure it to allow the Kali machine to access the rest of the network. However, the tester wanted to also see if the rest of the network could be accessed without breaking into the firewall.

The tester found *192.168.0.66* when doing a subnet scan of *192.168.0.64/27* (See ***192.168.0.64/27 Subnet Scan)***; this device had both SSH and NFS ports open. When attempting to connect via SSH, it was found that the device required a Public Key to access it. To do this, the tester mounted the NFS drive, as it mounted at the 'root' directory.

```
root@kali:~# mkdir ~/NFS66
root@kali:~# mount 192.168.0.66:/ ~/NFS66
```

Figure 13 - Mounting 192.168.0.66

The tester then generated an SSH key to move to the NFS drive. This file was used to overwrite the 'authorized-keys' file, and then the NFS drive was unmounted from the testers system.

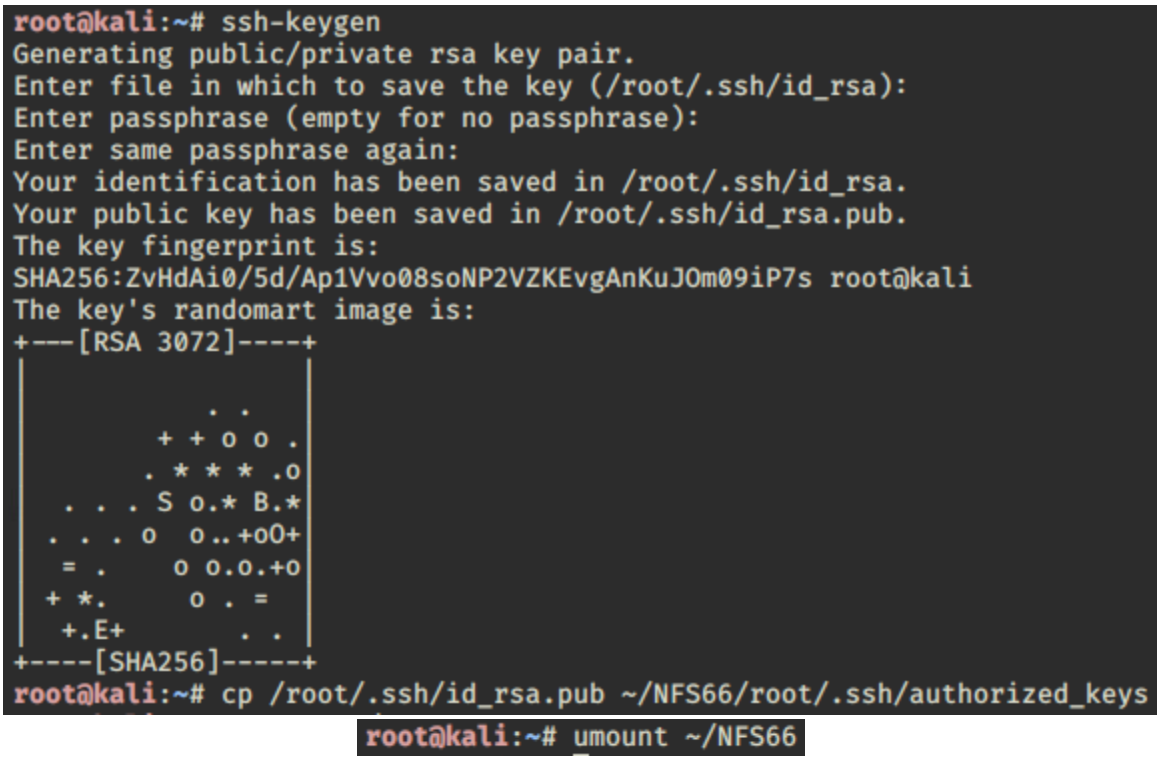


Figure 14 - Generating SSH Key and copying it to 192.168.0.66 and unmounting the NFS

The Public Key then allowed the tester to log in to *192.168.0.66* without requiring a password.

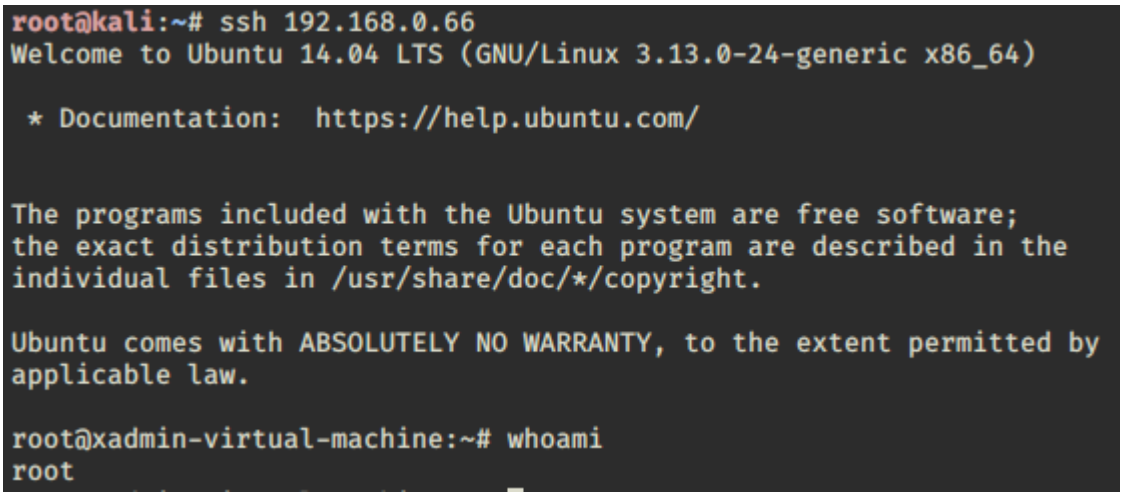


Figure 15 - Logged into 192.168.0.66 as root

From this device, another SSH tunnel was set up to the subnet *192.168.0.96/27*, which was connected to the firewall. The tunnel setup was the same as earlier in the report but instead used *2.2.2.1* and *2.2.2.2*, and *tun1*. The tester attempted to ping the firewall's LAN port to confirm the correct setup of the tunnel; as this was successful, the tunnel had been set up correctly.

The correct setup of the tunnel allowed for an nmap scan of *192.168.0.96/27*, doing so revealed the firewall and the final router, which was accessed using the same 'vyos:vyos' credentials as all the other routers and the tables were shown to confirm the final network map. (See ***192.168.0.97***)

4 SECURITY WEAKNESSES

Following the network mapping, this part of the report shall summarise the main concerns for the network. Instead of addressing the entire network, the tester has decided to break it down by device type, making it easier to use when fixing the network.

4.1 WORKSTATIONS

4.1.1 NFS

Devices *192.168.0.34* and *192.168.0.130* have an NFS setup where the user can only mount the drive at the 'xadmin' directory, which is reasonable as the user does not have access to sensitive data files, but they do have write permissions. However, devices *192.168.0.66* and *192.168.0.210* are set up insecurely, as mounting these devices mounts them at the 'root' directory, allowing for the extraction of sensitive files such as 'shadow' and 'passwd', and allowed editing of the 'authorized_keys' file, allowing anyone to gain access to the device. Therefore, it is suggested that all NFS devices should be set up only in the specific directories that require access and set to 'read only' unless there is a specific reason to do otherwise.

4.1.2 Weak Passwords

Three sets of credentials were brute-forced on the workstations due to their lack of complexity (root:apple, xadmin:plums, xadmin:!gatvol). One of these credentials was also shared by another device. In order to reduce the chance of passwords being cracked, greater password complexity should be used; this can be done by increasing password length, using more symbols and numbers or switching to passphrases. Additionally, passwords should be unique so that the impact is significantly reduced in the case of a breach. An excellent way to cover all of this is to implement a password policy, and several examples are readily available online. (Dunham, 2020)

4.1.3 SSH

A more secure alternative to securing the weak passwords used for the SSH logins is to switch all devices to using private key authentication, with each device having its own unique key. It is also suggested that the 'root' user should not be able to log in via SSH unless a specific circumstance requires this, in which case 'AllowUsers' ensures that the root user can only be logged in from a specific device.

If passwords are more convenient, another option would be to counteract brute-forcing by implementing a hash limit. Applying this limits the number of times a login can be attempted per a set amount of time, considerably increasing the time it would take to brute-force a login. (RimuHosting, 2021)

4.2 WEB SERVERS

4.2.1 Outdated Versions

A nikto scan was done on both servers to reveal more information. The webserver hosted on *192.168.0.242* is running Apache version 2.4.10, and at the time of this report, that specific version has 11 CVE vulnerabilities (CVE Details, 2021). Additionally, the webserver being hosted on *172.16.221.237*,

is also outdated, with the current version being 2.2.22, which as of the time of this report, has 13 known CVE vulnerabilities (CVE Details, 2021). Therefore, the Apache version is recommended to be updated to the latest version on both servers. Updating the server version will ensure that the vulnerabilities are patched.

4.2.2 Shellshock

Inspecting the Nikto scan on *192.168.0.242* revealed that the webserver was vulnerable to 'ShellShock', a bash shell vulnerability, which allows the attacker to create a shell on the vulnerable machine to gain remote access to it. The bash version needs to be updated or an alternative interpreter must be used to protect against this vulnerability.

4.2.3 WordPress

Dirb was run on both webservers to investigate any additional information. Dirb revealed that WordPress was run on *172.16.221.237* (See ***Appendix E – Webserver Investigation***). WPScan was then used to brute force the password the for 'admin' user, which was successful.

```
root@kali:~# wpscan --url 172.16.221.237/wordpress/ --passwords Desktop/rockyou.txt --usernames admin --max-threads 16
```

Figure 16 - WPScan to brute-force the admin credentials

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

Figure 17 - Successfully brute-forced

Gaining access to the admin panel allows the user to do almost anything they want to the site, including vandalising it, changing the credentials to lock out legitimate users and uploading dangerous packages.

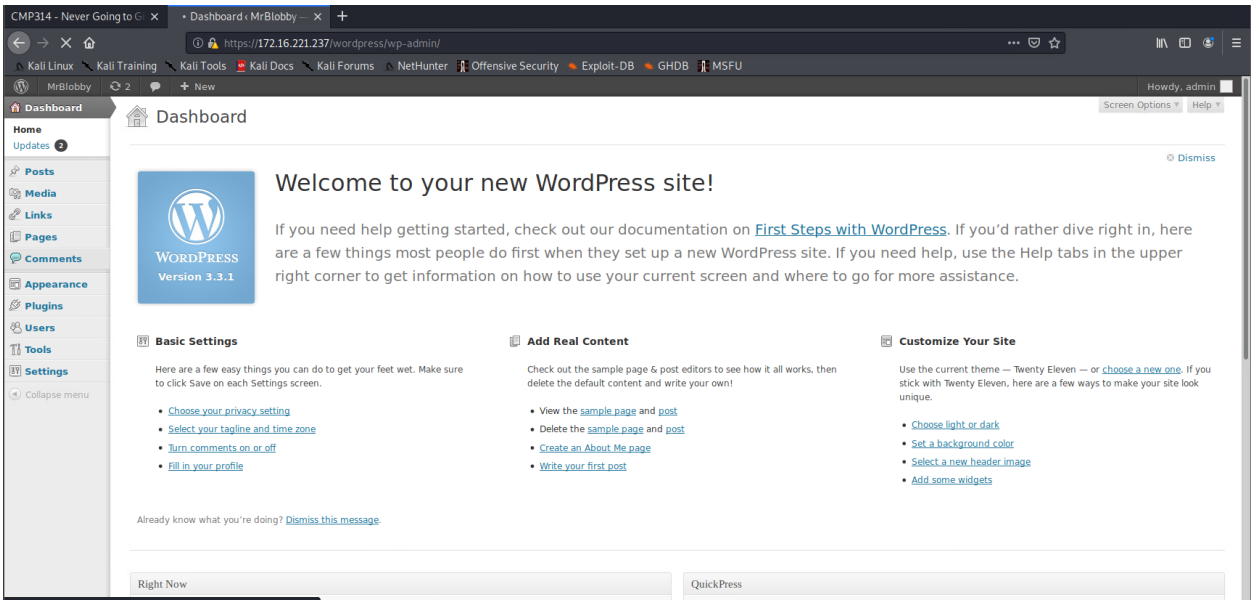


Figure 18 - Accessing the WordPress admin panel

Also, during the WPScan, the version of WordPress was revealed, 3.3.1. Unfortunately, this version is highly outdated, meaning it has a substantial number of potential vulnerabilities. (WPScan,

2019)Therefore, it is suggested that WordPress is also updated to the latest available version and that users password complexity is increased to reduce the chance of successful brute force attacks.

4.2.4 HTTP

Both web servers can be accessed through HTTP. It is highly suggested that this is changed to HTTPS (although *172.16.221.237* has HTTPS, it is not the default) and enforced instead of HTTP to ensure all communication between the servers and the users is encrypted to avoid stolen sensitive information.

4.3 ROUTERS

4.3.1 Default Credentials

All the VyOS routers on the network use the default credentials 'vyos:vyos' available from the VyOS documentation. It is highly suggested that the credentials on all routers be changed. As well as moving away from default credentials, the routers should also be given unique credentials for each router. With unique credentials, in the event of one routers credentials being obtained, not all routers would become compromised.

4.3.2 Telnet

Telnet is incredibly insecure, as the data is transmitted in plaintext, meaning tools such as 'wireshark' can monitor the traffic and capture any sensitive information being transmitted. Instead, it is suggested that a more secure communication protocol is used, such as SSH. Router one is already making use of this. However, the telnet port should be closed in conjunction. It should be noted that credentials should still be changed regardless of the communication protocol used, as they can still be brute-forced.

4.3.3 HTML

It is suggested that the webservers hosted on the routers should be disabled unless there is a specific reason otherwise. These default webservers allow anyone with access to the network to find out what router OS is being used, which assisted the tester in finding the router's credentials, as the default credentials were in use. If it is decided to keep the webservers enabled, they should be changed from the default VyOS page to make it harder for an attacker to identify the routers OS.

4.4 FIREWALL

4.4.1 Default Credentials

The firewall uses default credentials 'admin:pfsense', which can be found on the pfSense documentation. As this is very easy for an attacker to find, it is suggested that these credentials be changed to something more complex. As well as changing the credentials, the new credentials must not be similar to any other device on the network.

As well as the credentials, the hostname is the default 'pfSense'. It is suggested that the hostname is changed. Changing the hostname would make it significantly harder for an attacker cannot identify the software from the name.

4.4.2 Outdated Version

The current version of pfSense installed is outdated and has several known vulnerabilities. Therefore it is recommended to be updated to the latest version to ensure that these vulnerabilities are patched (Tenable, 2018).

4.4.3 Timeout

The login page does not timeout the user after a specific time, leaving the login session vulnerable to attackers. If the session is compromised, an attacker would have unlimited access to the login page as they would never be timed out. It is suggested that the login session is timed out after 10/15 minutes of inactivity, meaning an attacker would not be able to hijack the session if the user forgets to log out.

5 NETWORK DESIGN CRITICAL EVALUATION

The following section outlines an overall evaluation and recommendation for the current network topology, security, and subnetting. As the requirements of ACME Inc are unknown to the tester, general suggestions have been made with an explanation as to why they could be used rather than others, leaving ACME Inc to decide which suggestion would suit them best.

5.1 TOPOLOGY

The current networks topology is adequate; however, a further topology investigation may be necessary depending on the company needs, of which the tester has not been informed. The setup is inexpensive and easily scalable at present as no devices need to be taken down when introducing new devices. However, if one of the routers connections were to go down, several devices could become isolated from the network as there is no redundancy. For example, if the connection between Router 2 and Router 3 were to break, almost half the networks devices would be isolated from each other, which could have severe ramifications for productivity and profits.

A possible recommendation would be to change the current topology to one which includes redundancy and also to incorporate Spanning Tree Protocol. For example, a Mesh Hybrid topology could be used; it should be noted, this topology is more expensive; however, it provides reliability and stability. Furthermore, this topology ensures that even if one router connection were lost, there would still be an alternative path for the traffic to follow. Implementing these changes would ensure that only a minor section of the network would become isolated in the event of an outage, reducing the total effect on the network.

Many different resources are available (***DNSstuff, 2019***) that describe the pros and cons of each topology, and the tester would suggest a further investigation into these to best suit the company needs.

5.2 SECURITY

As displayed in the previous sections, several concerning security flaws exist within the ACME Inc network. The main concern is outdated software and outdated security practices. Outdated software is the biggest issue, as it means that the devices are vulnerable to a significant number of exploits. Therefore, the first port of call should ensure that every device is updated to the latest version. Once this has been done, work through each device to ensure the credentials are unique and complex and close unnecessary ports, such as the HTTP servers and the telnet protocols.

A firewall is an excellent solution to improve security in the network; however, in this case, it has been misconfigured. Combining reconfiguring the devices on the network and reconfiguring the firewall only to allow trusted traffic should ensure that the firewall works properly and keeps the network secure.

As well as the current firewall, other firewalls could be installed to create more obstacles for an attacker. For example, installing a firewall on the workstations so that only trusted devices can connect

to them would significantly slow down an attacker. Instead, the attacker would have to make their way through several layers of protection to reach their goal, which can, in some cases, deter an attacker entirely.

5.3 SUBNETTING

The current subnetting on the network is suitable for the network as it uses the exact number of hosts for the router subnets. Although the device subnets currently only have a couple of addresses in use, if this remains the same, a subnet mask that uses fewer hosts may be more appropriate for the device subnets. However, these subnets leave room for scalability if the company decides to introduce more devices to the network. Therefore, minor changes may need to be made here, depending on the company requirements.

6 CONCLUSIONS

It is clear that there are significant flaws in the current network setup; however, as described in the report, they can all be quickly resolved. In the networks current state, an attacker would be able to gain access to all of the devices without much effort due to the outdated software, misconfiguration and lack of password complexity and uniqueness.

Without a quick resolution, the network is vulnerable to malicious attackers, who would be able to access sensitive information, damage the network and possibly reconfigure it to lock ACME Inc out.

A significant number of the testers recommendations are to ensure that devices are updated to the latest versions, as outdated software is more prone to vulnerability. Therefore, this should be the main priority to ensure that the network is secure. Also suggested is the closure of unused ports or insecure protocols and implementing a password policy.

The current network topology may not meet the company requirements. Possible recommendations to change this have been cited to ensure that the network has alternative paths if there are broken connections. It is up to ACME Inc if they wish to pursue this further, depending on their requirements for the network.

As soon as a new Network Manager is on-site, the security issues and concerns mentioned in this report must be corrected quickly to ensure the network and company assets are protected.

REFERENCES

CVE Details, 2021. *CVE Details.* [Online]
Available at: https://www.cvedetails.com/vulnerability-list.php?vendor_id=45&product_id=66&version_id=529730&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=
[Accessed 21 December 2021].

CVE Details, 2021. *CVE Details.* [Online]
Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-490988/Apache-Http-Server-2.2.22.html
[Accessed 21 December 2021].

Dunham, R., 2020. *NIST Password Guidelines – What You Need to Know.* [Online]
Available at: https://linfordco.com/blog/nist-password-policy-guidelines/
[Accessed 21 December 2021].

Netgate Docs, 2020. *User Management and Authentication.* [Online]
Available at: https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html
[Accessed 20 December 2021].

RimuHosting, 2021. *Preventing Brute Force SSH Attacks.* [Online]
Available at: https://rimuhosting.com/knowledgebase/linux/misc/preventing-brute-force-ssh-attacks
[Accessed 20 December 2021].

Tenable, 2018. *pfSense < 2.3.5 Multiple Vulnerabilities.* [Online]
Available at: https://www.tenable.com/plugins/nessus/109037
[Accessed 21 December 2021].

VyOS, 2021. *VyOS Documentation.* [Online]
Available at: https://docs.vyos.io/en/latest/installation/install.html#permanent-installation
[Accessed 11 December 2021].

WPScan, 2019. *WordPress 3.3.1 Vulnerabilities.* [Online]
Available at: https://wpscan.com/wordpress/331
[Accessed 21 December 2021].

APPENDICES

APPENDIX A - IFCONFIG

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.200  netmask 255.255.255.224  broadcast 192.168.0.223
        inet6 fe80::20c:29ff:feb4:e1ce  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b4:e1:ce  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 585 (585.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 2628 (2.5 KiB)
        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 6  bytes 318 (318.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

APPENDIX B – NMAP SCANS

192.168.0.200 Subnet scan

```
root@kali:~# nmap 192.168.0.200/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-10 13:30 EST
Nmap scan report for 192.168.0.193
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
MAC Address: 00:50:56:99:6C:E2 (VMware)

Nmap scan report for 192.168.0.210
Host is up (0.000086s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
MAC Address: 00:0C:29:AA:6E:93 (VMware)

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

Nmap done: 32 IP addresses (3 hosts up) scanned in 26.94 seconds
```

192.168.0.0-255 Scan

```
root@kali:~# nmap 192.168.0.0-255
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-11 13:16 EST
Nmap scan report for 192.168.0.33
Host is up (0.0034s 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 (0.0039s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap scan report for 192.168.0.129
Host is up (0.0038s 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 (0.0038s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap scan report for 192.168.0.225
Host is up (0.0022s 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 (0.0035s 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 192.168.0.229
Host is up (0.0034s 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 (0.0038s 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 192.168.0.233
Host is up (0.0038s 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 192.168.0.242
Host is up (0.0040s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap scan report for 192.168.0.193
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
MAC Address: 00:50:56:99:6C:E2 (VMware)
```

```
Nmap scan report for 192.168.0.210
Host is up (0.00016s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
MAC Address: 00:0C:29:AA:6E:93 (VMware)

Nmap scan report for 192.168.0.200
Host is up (0.0000040s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (13 hosts up) scanned in 47.01 seconds
```

172.16.221.237 Subnet Scan

```
root@kali:~# nmap 172.16.221.16/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-11 21:33 EST
Nmap scan report for 172.16.221.16
Host is up (0.00044s 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 (0.00075s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 256 IP addresses (2 hosts up) scanned in 47.19 seconds
```

192.168.0.234 Scan

```
root@kali:~# nmap 192.168.0.234
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-12 05:55 EST
Nmap scan report for 192.168.0.234
Host is up (0.011s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
2601/tcp open  zebra
2604/tcp open  ospfd
2605/tcp open  bgpd

Nmap done: 1 IP address (1 host up) scanned in 17.23 seconds
```

192.168.0.64/27 Subnet Scan

```
root@kali:~# nmap 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-11 23:22 EST
Nmap scan report for 192.168.0.66
Host is up (0.0047s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap done: 32 IP addresses (1 host up) scanned in 15.02 seconds
```

192.168.0.96/27 Subnet Scan

```
root@kali:~# nmap 192.168.0.96/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-13 06:01 EST
Nmap scan report for 192.168.0.97
Host is up (0.0076s 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 192.168.0.98
Host is up (0.011s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
2601/tcp open  zebra
2604/tcp open  ospfd
2605/tcp open  bgpd

Nmap done: 32 IP addresses (2 hosts up) scanned in 19.70 seconds
```

UDP Scans

```
Nmap scan report for 192.168.0.230
Host is up (0.00056s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp
```

```
Nmap scan report for 172.16.221.237
Host is up (0.00069s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
5353/udp open  zeroconf
```

```
Nmap scan report for 13.13.13.13
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT     STATE         SERVICE
631/udp  open|filtered ipp
5353/udp open          zeroconf
```

```
Nmap scan report for 192.168.0.33
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.34
Host is up (0.00071s latency).
Not shown: 911 closed ports, 86 open|filtered ports
PORT     STATE SERVICE
111/udp  open  rpcbind
2049/udp open  nfs
5353/udp open  zeroconf

Nmap scan report for 192.168.0.66
Host is up (0.0025s latency).
Not shown: 918 closed ports, 79 open|filtered ports
PORT     STATE SERVICE
111/udp  open  rpcbind
2049/udp open  nfs
5353/udp open  zeroconf

Nmap scan report for 192.168.0.97
Host is up (0.0028s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.98
Host is up (0.0036s latency).
Not shown: 998 open|filtered ports
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
```

```
Nmap scan report for 192.168.0.129
Host is up (0.00079s latency).
Not shown: 969 closed ports, 29 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.130
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
2049/udp open          nfs
5353/udp open          zeroconf

Nmap scan report for 192.168.0.225
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp
```

```
Nmap scan report for 192.168.0.226
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT      STATE         SERVICE
123/udp   open          ntp
161/udp   open          snmp
1030/udp  open|filtered iad1
1088/udp  open|filtered cplscrambler-al
19039/udp open|filtered unknown
19792/udp open|filtered unknown
21000/udp open|filtered irtrans
21060/udp open|filtered unknown
21104/udp open|filtered unknown
21282/udp open|filtered unknown
21320/udp open|filtered unknown
21476/udp open|filtered unknown
21948/udp open|filtered unknown
23354/udp open|filtered unknown
23608/udp open|filtered unknown
23965/udp open|filtered unknown
33355/udp open|filtered unknown
36669/udp open|filtered unknown
44923/udp open|filtered unknown
49201/udp open|filtered unknown
49360/udp open|filtered unknown
52503/udp open|filtered unknown
59207/udp open|filtered unknown

Nmap scan report for 192.168.0.229
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.230
Host is up (0.00091s latency).
Not shown: 933 closed ports, 65 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp

Nmap scan report for 192.168.0.233
Host is up (0.00085s latency).
Not shown: 768 closed ports, 230 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp
```

```
Nmap scan report for 192.168.0.242
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
5353/udp open          zeroconf

Nmap scan report for 192.168.0.193
Host is up (0.00036s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp
MAC Address: 00:50:56:99:6C:E2 (VMware)

Nmap scan report for 192.168.0.210
Host is up (0.00039s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
111/udp  open          rpcbind
631/udp  open|filtered ipp
2049/udp open          nfs
5353/udp open          zeroconf
MAC Address: 00:0C:29:AA:6E:93 (VMware)

Nmap scan report for 192.168.0.200
Host is up (0.0000040s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
111/udp open  rpcbind

Nmap scan report for 192.168.0.234
Host is up (0.0021s latency).
Not shown: 998 open|filtered ports
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
```

13.13.13.13 Scan

```
Nmap scan report for 13.13.13.13
Host is up (0.0037s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
```

APPENDIX C – ROUTER SHOW INTERFACE AND NETSTAT

192.168.0.193

```
vyos@vyos:~$ show interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.193/27                  u/u
eth1             192.168.0.225/30                  u/u
eth2             172.16.221.16/24                  u/u
lo               127.0.0.1/8                       u/u
                 1.1.1.1/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
1.1.1.1         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    0.0.0.0         255.255.255.0   U         0 0          0 eth2
192.168.0.32    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.64    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.96    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.128   192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.192   0.0.0.0         255.255.255.224 U         0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.252 U         0 0          0 eth1
192.168.0.228   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
192.168.0.232   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
192.168.0.240   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
```

192.168.0.33

```
root@kali:~# telnet 192.168.0.33
Trying 192.168.0.33 ...
Connected to 192.168.0.33.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Oct 23 22:22:25 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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             192.168.0.226/30               u/u
eth1             192.168.0.33/27                u/u
eth2             192.168.0.229/30               u/u
lo               127.0.0.1/8                    u/u
                 2.2.2.2/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
2.2.2.2         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    192.168.0.225   255.255.255.0   UG        0 0          0 eth0
192.168.0.32    0.0.0.0         255.255.255.224 U         0 0          0 eth1
192.168.0.64    192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.96    192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.128   192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.192   192.168.0.225   255.255.255.224 UG        0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.252 U         0 0          0 eth0
192.168.0.228   0.0.0.0         255.255.255.252 U         0 0          0 eth2
192.168.0.232   192.168.0.230   255.255.255.252 UG        0 0          0 eth2
192.168.0.240   192.168.0.230   255.255.255.252 UG        0 0          0 eth2
```

192.168.0.129

```
root@kali:~# telnet 192.168.0.129
Trying 192.168.0.129 ...
Connected to 192.168.0.129.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Oct 23 22:22:46 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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             192.168.0.230/30               u/u
eth1             192.168.0.129/27               u/u
eth2             192.168.0.233/30               u/u
lo               127.0.0.1/8                    u/u
                 3.3.3.3/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
3.3.3.3         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    192.168.0.229   255.255.255.0   UG        0 0          0 eth0
192.168.0.32    192.168.0.229   255.255.255.224 UG        0 0          0 eth0
192.168.0.64    192.168.0.234   255.255.255.224 UG        0 0          0 eth2
192.168.0.96    192.168.0.234   255.255.255.224 UG        0 0          0 eth2
192.168.0.128   0.0.0.0         255.255.255.224 U         0 0          0 eth1
192.168.0.192   192.168.0.229   255.255.255.224 UG        0 0          0 eth0
192.168.0.224   192.168.0.229   255.255.255.252 UG        0 0          0 eth0
192.168.0.228   0.0.0.0         255.255.255.252 U         0 0          0 eth0
192.168.0.232   0.0.0.0         255.255.255.252 U         0 0          0 eth2
192.168.0.240   192.168.0.234   255.255.255.252 UG        0 0          0 eth2
```

192.168.0.225

```
root@kali:~# telnet 192.168.0.225
Trying 192.168.0.225 ...
Connected to 192.168.0.225.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Dec 11 21:41:16 UTC 2021 on pts/1
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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             192.168.0.193/27               u/u
eth1             192.168.0.225/30               u/u
eth2             172.16.221.16/24               u/u
lo               127.0.0.1/8                    u/u
                 1.1.1.1/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
1.1.1.1         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    0.0.0.0         255.255.255.0   U         0 0          0 eth2
192.168.0.32    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.64    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.96    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.128   192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.192   0.0.0.0         255.255.255.224 U         0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.252 U         0 0          0 eth1
192.168.0.228   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
192.168.0.232   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
192.168.0.240   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
```

192.168.0.226

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

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Dec 11 21:34:41 UTC 2021 on pts/0
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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.226/30                  u/u
eth1             192.168.0.33/27                   u/u
eth2             192.168.0.229/30                  u/u
lo               127.0.0.1/8                       u/u
                 2.2.2.2/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
2.2.2.2         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    192.168.0.225   255.255.255.0   UG        0 0          0 eth0
192.168.0.32    0.0.0.0         255.255.255.224 U         0 0          0 eth1
192.168.0.64    192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.96    192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.128   192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.192   192.168.0.225   255.255.255.224 UG        0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.252 U         0 0          0 eth0
192.168.0.228   0.0.0.0         255.255.255.252 U         0 0          0 eth2
192.168.0.232   192.168.0.230   255.255.255.252 UG        0 0          0 eth2
192.168.0.240   192.168.0.230   255.255.255.252 UG        0 0          0 eth2
```

192.168.0.229

```
root@kali:~# telnet 192.168.0.229
Trying 192.168.0.229 ...
Connected to 192.168.0.229.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Dec 11 21:48:34 UTC 2021 on pts/2
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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             192.168.0.226/30               u/u
eth1             192.168.0.33/27                u/u
eth2             192.168.0.229/30               u/u
lo               127.0.0.1/8                    u/u
                 2.2.2.2/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
2.2.2.2         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    192.168.0.225   255.255.255.0   UG        0 0          0 eth0
192.168.0.32    0.0.0.0         255.255.255.224 U         0 0          0 eth1
192.168.0.64    192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.96    192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.128   192.168.0.230   255.255.255.224 UG        0 0          0 eth2
192.168.0.192   192.168.0.225   255.255.255.224 UG        0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.252 U         0 0          0 eth0
192.168.0.228   0.0.0.0         255.255.255.252 U         0 0          0 eth2
192.168.0.232   192.168.0.230   255.255.255.252 UG        0 0          0 eth2
192.168.0.240   192.168.0.230   255.255.255.252 UG        0 0          0 eth2
```

192.168.0.230

```
root@kali:~# telnet 192.168.0.230
Trying 192.168.0.230 ...
Connected to 192.168.0.230.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Dec 11 21:39:49 UTC 2021 on pts/0
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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             192.168.0.230/30               u/u
eth1             192.168.0.129/27               u/u
eth2             192.168.0.233/30               u/u
lo               127.0.0.1/8                    u/u
                 3.3.3.3/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
3.3.3.3         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    192.168.0.229   255.255.255.0   UG        0 0          0 eth0
192.168.0.32    192.168.0.229   255.255.255.224 UG        0 0          0 eth0
192.168.0.64    192.168.0.234   255.255.255.224 UG        0 0          0 eth2
192.168.0.96    192.168.0.234   255.255.255.224 UG        0 0          0 eth2
192.168.0.128   0.0.0.0         255.255.255.224 U         0 0          0 eth1
192.168.0.192   192.168.0.229   255.255.255.224 UG        0 0          0 eth0
192.168.0.224   192.168.0.229   255.255.255.252 UG        0 0          0 eth0
192.168.0.228   0.0.0.0         255.255.255.252 U         0 0          0 eth0
192.168.0.232   0.0.0.0         255.255.255.252 U         0 0          0 eth2
192.168.0.240   192.168.0.234   255.255.255.252 UG        0 0          0 eth2
```

192.168.0.233

```
root@kali:~# telnet 192.168.0.233
Trying 192.168.0.233 ...
Connected to 192.168.0.233.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Dec 11 21:50:25 UTC 2021 on pts/1
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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.230/30                  u/u
eth1             192.168.0.129/27                  u/u
eth2             192.168.0.233/30                  u/u
lo               127.0.0.1/8                       u/u
                 3.3.3.3/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
3.3.3.3         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    192.168.0.229   255.255.255.0   UG        0 0          0 eth0
192.168.0.32    192.168.0.229   255.255.255.224 UG        0 0          0 eth0
192.168.0.64    192.168.0.234   255.255.255.224 UG        0 0          0 eth2
192.168.0.96    192.168.0.234   255.255.255.224 UG        0 0          0 eth2
192.168.0.128   0.0.0.0         255.255.255.224 U         0 0          0 eth1
192.168.0.192   192.168.0.229   255.255.255.224 UG        0 0          0 eth0
192.168.0.224   192.168.0.229   255.255.255.252 UG        0 0          0 eth0
192.168.0.228   0.0.0.0         255.255.255.252 U         0 0          0 eth0
192.168.0.232   0.0.0.0         255.255.255.252 U         0 0          0 eth2
192.168.0.240   192.168.0.234   255.255.255.252 UG        0 0          0 eth2
```

192.168.0.97

```
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: Sat Oct 23 22:18:52 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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.97/27                   u/u
eth1             192.168.0.65/27                   u/u
lo               127.0.0.1/8                       u/u
                 4.4.4.4/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
4.4.4.4         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    192.168.0.98    255.255.255.0   UG        0 0          0 eth0
192.168.0.32    192.168.0.98    255.255.255.224 UG        0 0          0 eth0
192.168.0.64    0.0.0.0         255.255.255.224 U         0 0          0 eth1
192.168.0.96    0.0.0.0         255.255.255.224 U         0 0          0 eth0
192.168.0.128   192.168.0.98    255.255.255.224 UG        0 0          0 eth0
192.168.0.192   192.168.0.98    255.255.255.224 UG        0 0          0 eth0
192.168.0.224   192.168.0.98    255.255.255.252 UG        0 0          0 eth0
192.168.0.228   192.168.0.98    255.255.255.252 UG        0 0          0 eth0
192.168.0.232   192.168.0.98    255.255.255.252 UG        0 0          0 eth0
192.168.0.240   192.168.0.98    255.255.255.252 UG        0 0          0 eth0
```

172.16.221.16

```
root@kali:~# telnet 172.16.221.16
Trying 172.16.221.16 ...
Connected to 172.16.221.16.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Sat Dec 11 21:45:00 UTC 2021 on pts/2
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 interface
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.193/27                  u/u
eth1             192.168.0.225/30                  u/u
eth2             172.16.221.16/24                  u/u
lo               127.0.0.1/8                       u/u
                 1.1.1.1/32
                 ::1/128
vyos@vyos:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
1.1.1.1         0.0.0.0         255.255.255.255 UH        0 0          0 lo
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
172.16.221.0    0.0.0.0         255.255.255.0   U         0 0          0 eth2
192.168.0.32    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.64    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.96    192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.128   192.168.0.226   255.255.255.224 UG        0 0          0 eth1
192.168.0.192   0.0.0.0         255.255.255.224 U         0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.252 U         0 0          0 eth1
192.168.0.228   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
192.168.0.232   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
192.168.0.240   192.168.0.226   255.255.255.252 UG        0 0          0 eth1
```

APPENDIX D – SETTING UP THE SSH TUNNEL

192.168.0.64/27

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

```
root@xadmin-virtual-machine:/etc/ssh# service ssh restart
ssh stop/waiting
ssh start/running, process 3694
root@xadmin-virtual-machine:/etc/ssh#
```

```
root@kali:~# ssh -w0:0 root@192.168.0.242
root@192.168.0.242's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

Last login: Sun Dec 12 08:48:16 2021 from 192.168.0.200
root@xadmin-virtual-machine:~# ip addr add 1.1.1.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
```

```
root@kali:~# ip addr add 1.1.1.1/30 dev tun0
root@kali:~# ip link set tun0 up
```

```
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
```

```
root@kali:~# route add -host 192.168.0.234 tun0
root@kali:~# route add -net 192.168.0.64/27 tun0
```

```
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 1.1.1.0/30 -o eth0 -j MASQUERADE
```

13.13.13.13

```
root@xadmin-virtual-machine:~# nano /etc/ssh/sshd_config
root@xadmin-virtual-machine:~# service ssh restart
ssh stop/waiting
ssh start/running, process 2856
root@xadmin-virtual-machine:~# exit
exit
xadmin@xadmin-virtual-machine:~$ exit
```

```
root@kali:~# ssh -w2:2 root@192.168.0.34
```

```
root@xadmin-virtual-machine:~# ip addr add 3.3.3.2/30 dev tun2
root@xadmin-virtual-machine:~# ip link set tun2 up
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
```

```
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 3.3.3.0/30 -o eth1 -j MASQUERADE
```

```
root@kali:~# ip addr add 3.3.3.1/30 dev tun2
root@kali:~# ip link set tun2 up
root@kali:~# route add -net 13.13.13.0/24 tun2
root@kali:~# ping 13.13.13.13
PING 13.13.13.13 (13.13.13.13) 56(84) bytes of data.
64 bytes from 13.13.13.13: icmp_seq=1 ttl=63 time=2.06 ms
64 bytes from 13.13.13.13: icmp_seq=2 ttl=63 time=1.35 ms
```

APPENDIX E – WEBSERVER INVESTIGATION

Nikto 172.16.221.237

```
root@kali:~# nikto -h 172.16.221.237
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.221.237
+ Target Hostname:    172.16.221.237
+ Target Port:        80
+ Start Time:         2021-12-13 22:37:23 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 45778, size: 177, mtime: Tue Apr 29 00:43:57 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were fou
nd: index.html
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-12-13 22:37:43 (GMT-5) (20 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nikto 192.168.0.242

```
root@kali:~# nikto -h 192.168.0.242
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.242
+ Target Hostname:    192.168.0.242
+ Target Port:        80
+ Start Time:         2021-12-13 22:37:11 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Unix)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header '93e4r0-cve-2014-6278' found, with contents: true
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ 8725 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2021-12-13 22:37:33 (GMT-5) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Dirb 172.16.221.237

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

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

START_TIME: Mon Dec 13 22:56:40 2021
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: Mon Dec 13 22:57:24 2021
DOWNLOADED: 50732 - FOUND: 92
```

Dirb 192.168.0.242

```
root@kali:~# dirb http://192.168.0.242/

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

START_TIME: Mon Dec 13 22:56:50 2021
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:543)

---- 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 13 22:57:00 2021
DOWNLOADED: 9224 - FOUND: 4
```

APPENDIX F – SUBNET CALCULATIONS

Subnet Calculation Explanation

$$\text{Number of Hosts} = 2^{\text{Host Bits}}$$

Usable Addresses = Number of Hosts – 2

Subnet Address = *.*.*.x (x is the first address in the subnet)

Broadcast Address = *.*.*.y (y is the Number of hosts + First address number)

Using the above calculations, the Kali Machine, for example, is on the Subnet *192.168.0.192/27,* which has a usable host range of *192.168.0.193-192.168.0.222* and a broadcast address of *192.168.0.223*.

Calculating Subnets

Network bits in red. Host bits in blue.

/24 = 255.255.255.0

255 255 255 0

11111111.11111111.11111111.00000000

Number of Hosts = 256

Usable addresses = 254

/27 = 255.255.255.224

255 255 255 224

11111111.11111111.11111111.11100000

Number of Hosts = 32

Usable addresses = 30

/30 = 255.255.255.252

255 255 255 252

11111111.11111111.11111111.11111100

Number of Hosts = 4

Usable addresses = 2