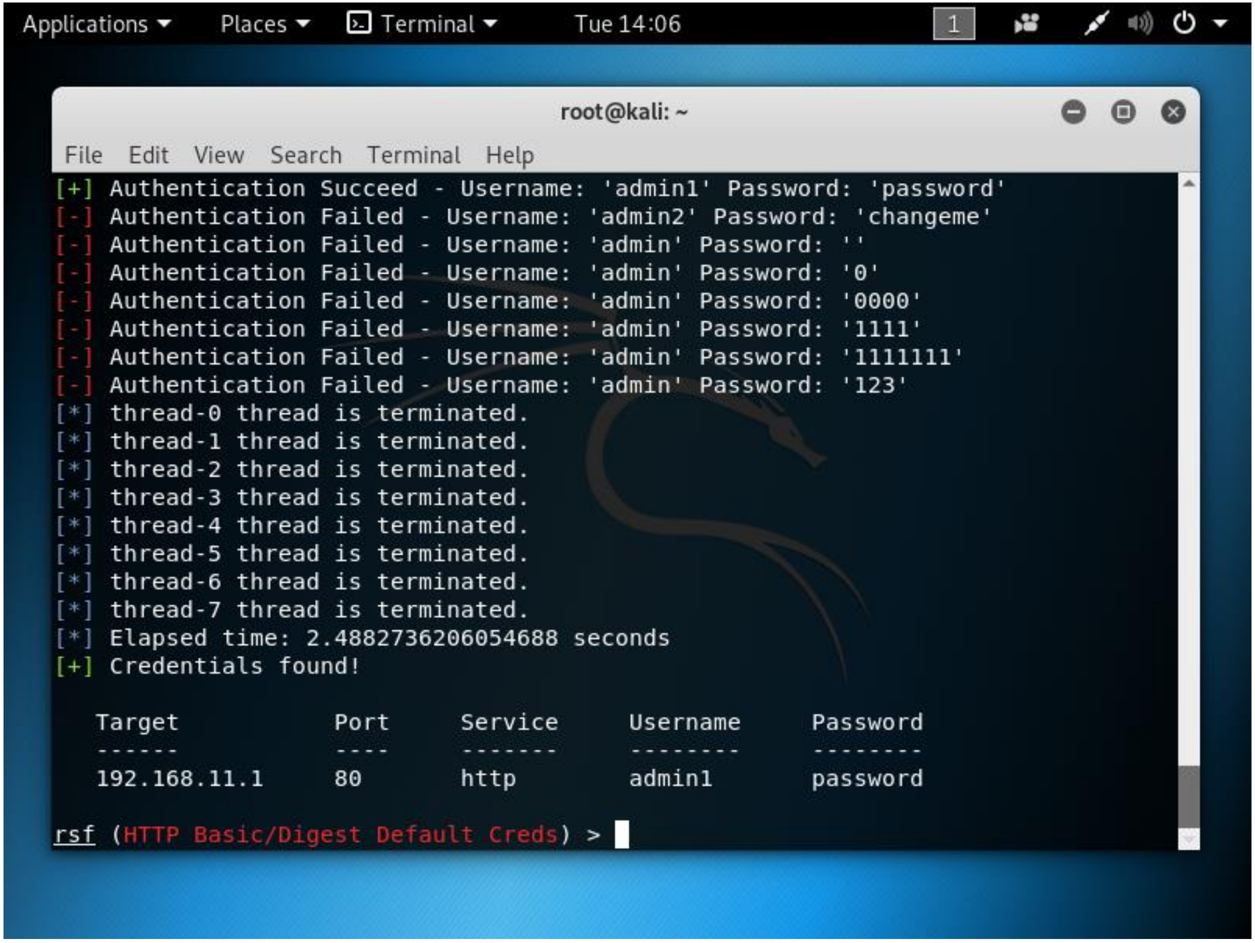
1. Provide a screenshot of your running results in Step 7. What is the username and password you find for Buffalo router? Also, describe on detail how the exploit found the username and password.

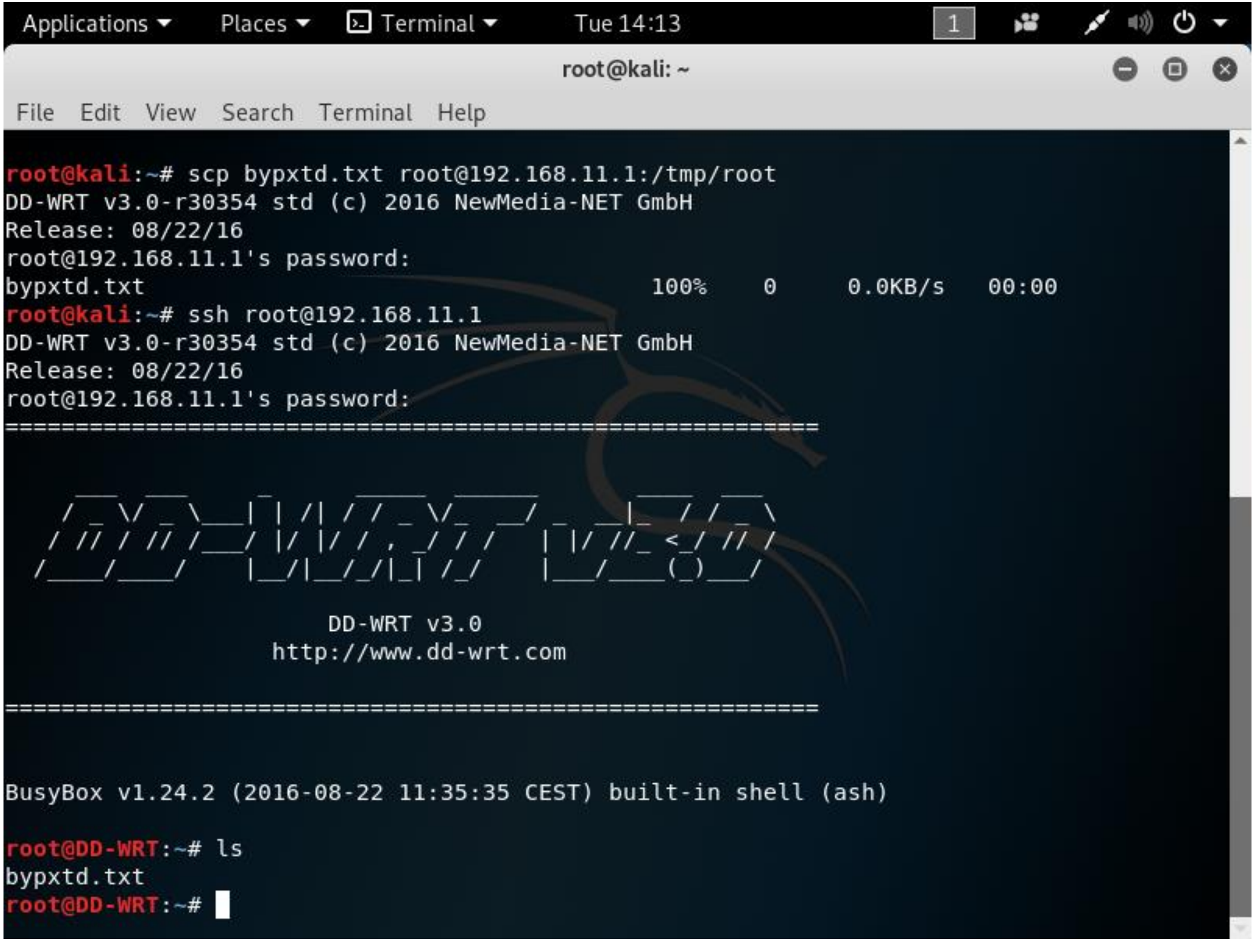


```
[+] Authentication Succeed - Username: 'admin1' Password: 'password'
[-] Authentication Failed - Username: 'admin2' Password: 'changeme'
[-] Authentication Failed - Username: 'admin' Password: ''
[-] Authentication Failed - Username: 'admin' Password: '0'
[-] Authentication Failed - Username: 'admin' Password: '0000'
[-] Authentication Failed - Username: 'admin' Password: '1111'
[-] Authentication Failed - Username: 'admin' Password: '1111111'
[-] Authentication Failed - Username: 'admin' Password: '123'
[*] thread-0 thread is terminated.
[*] thread-1 thread is terminated.
[*] thread-2 thread is terminated.
[*] thread-3 thread is terminated.
[*] thread-4 thread is terminated.
[*] thread-5 thread is terminated.
[*] thread-6 thread is terminated.
[*] thread-7 thread is terminated.
[*] Elapsed time: 2.4882736206054688 seconds
[+] Credentials found!

   Target          Port     Service     Username     Password
   ------          ----     -------     --------     --------
   192.168.11.1    80       http        admin1       password

rsf (HTTP Basic/Digest Default Creds) >
```

Username: admin1
Password: password

The exploit utilized the dictionary attack method, which is a form of brute force technique by trying possibilities derived from a dictionary.

2. Following Step 9. After successfully SSH to the router. Simply upload a .txt file using scp command. Named this file [your_pawprint].txt. For example, if your pawprint is 'tiger', create a file named 'tiger.txt' in local and upload this file to your router use 'scp' command. Show screenshots similar to Figure 10, use ls command to display your .txt file on the screenshot and the command you used to upload your .txt file.



```
root@kali:~# scp bypxtd.txt root@192.168.11.1:/tmp/root
DD-WRT v3.0-r30354 std (c) 2016 NewMedia-NET GmbH
Release: 08/22/16
root@192.168.11.1's password:
bypxtd.txt                              100%    0     0.0KB/s   00:00
root@kali:~# ssh root@192.168.11.1
DD-WRT v3.0-r30354 std (c) 2016 NewMedia-NET GmbH
Release: 08/22/16
root@192.168.11.1's password:
==========================================================


     ___  ___     _     ______  ______        ____  ___
    / _ \/ _ \___| | /| / / _ \/_  __/  _  __|_  / / _ \
   / // / // /___/ |/ |/ / , _/ / /    | |/ //_ <_/ // /
  /____/____/    |__/|__/_/|_| /_/     |___/____(_)___/


                       DD-WRT v3.0
                   http://www.dd-wrt.com

==========================================================


BusyBox v1.24.2 (2016-08-22 11:35:35 CEST) built-in shell (ash)

root@DD-WRT:~# ls
bypxtd.txt
root@DD-WRT:~# 
```

3. The other firmware commonly used on the routers is OpenWRT. Search online documentation and give your opinion on DD-WRT vs OpenWRT, provide a detailed comparison table with three rows.

Between DD-WRT vs. OpenWRT, it seems DD-WRT is good initially for beginners as it is simple and easy to use without the technical necessities required of OpenWrt, and it also has a large community of users able to assist you. However, if you are more knowledgeable then I would suggest OpenWRT because it offers more flexibility and control and is generally more advanced in features in comparison to DD-WRT if you know what you are doing.

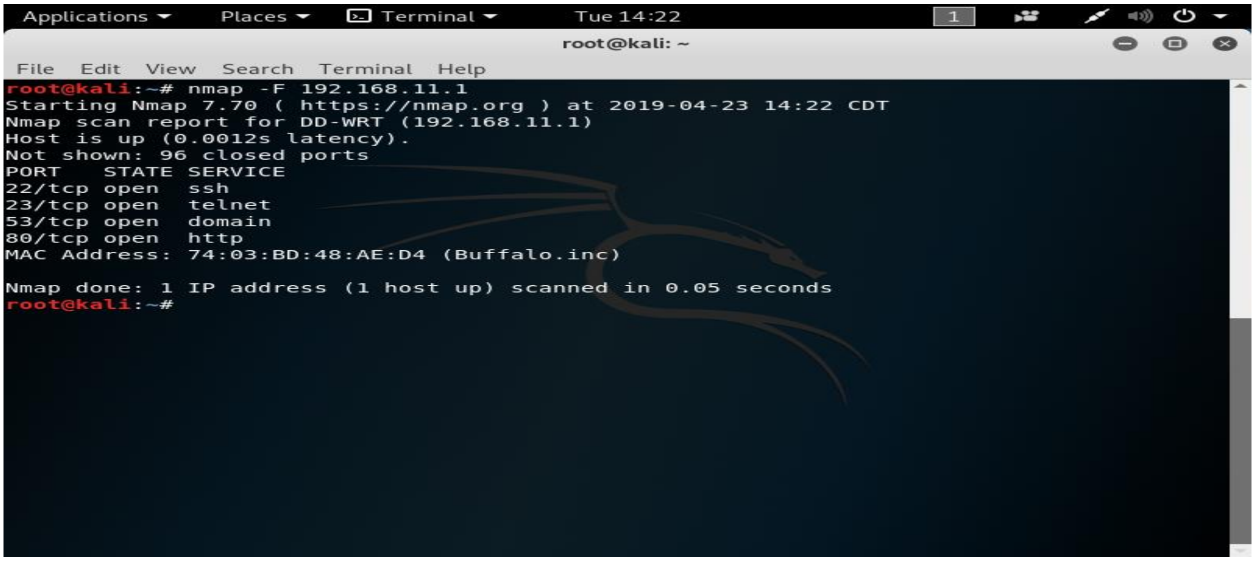
DD-WRT

Strengths	**Weaknesses**
Supports many routers	Less control for the sake of simplicity
Large community	Less in-depth support available
Easy to use without too much knowledge	Large pool of routers, therefore potentially more bugs

OpenWRT

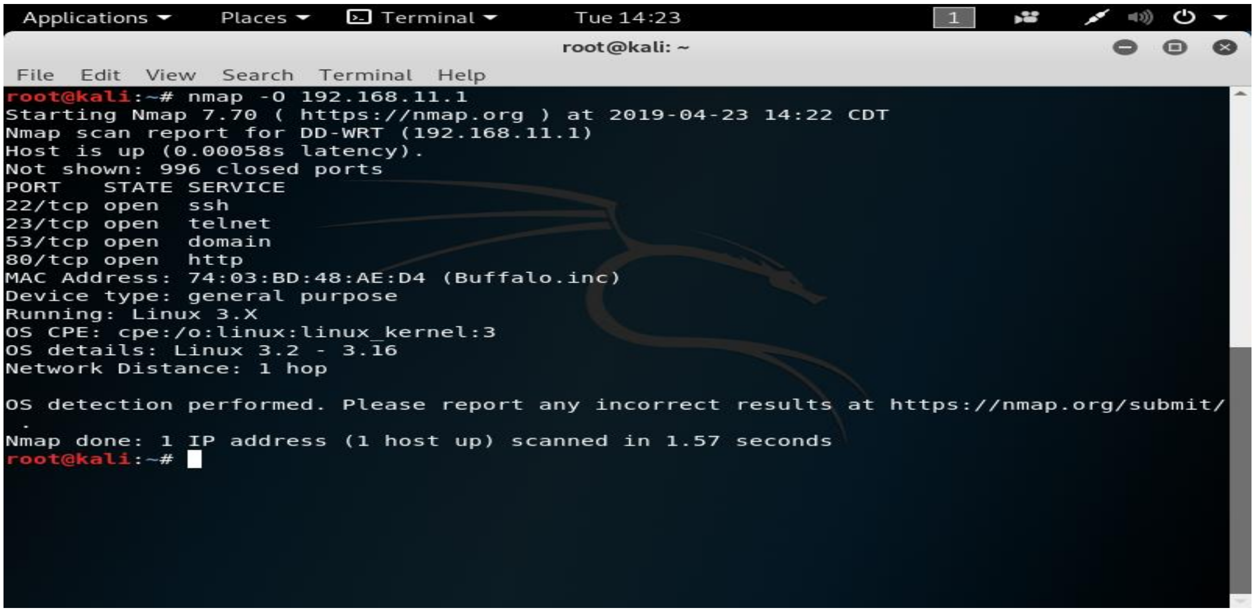
Strengths	**Weaknesses**
More fine control over DD-WRT	Supports fewer routers
Been around long, so relatively bug free	Requires more technical knowledge
Advanced VPN functionality	Difficult to configure

4. Once you ssh to the router, use 5 linux commands to gather system information. Add screenshots and explanation for each executed command.



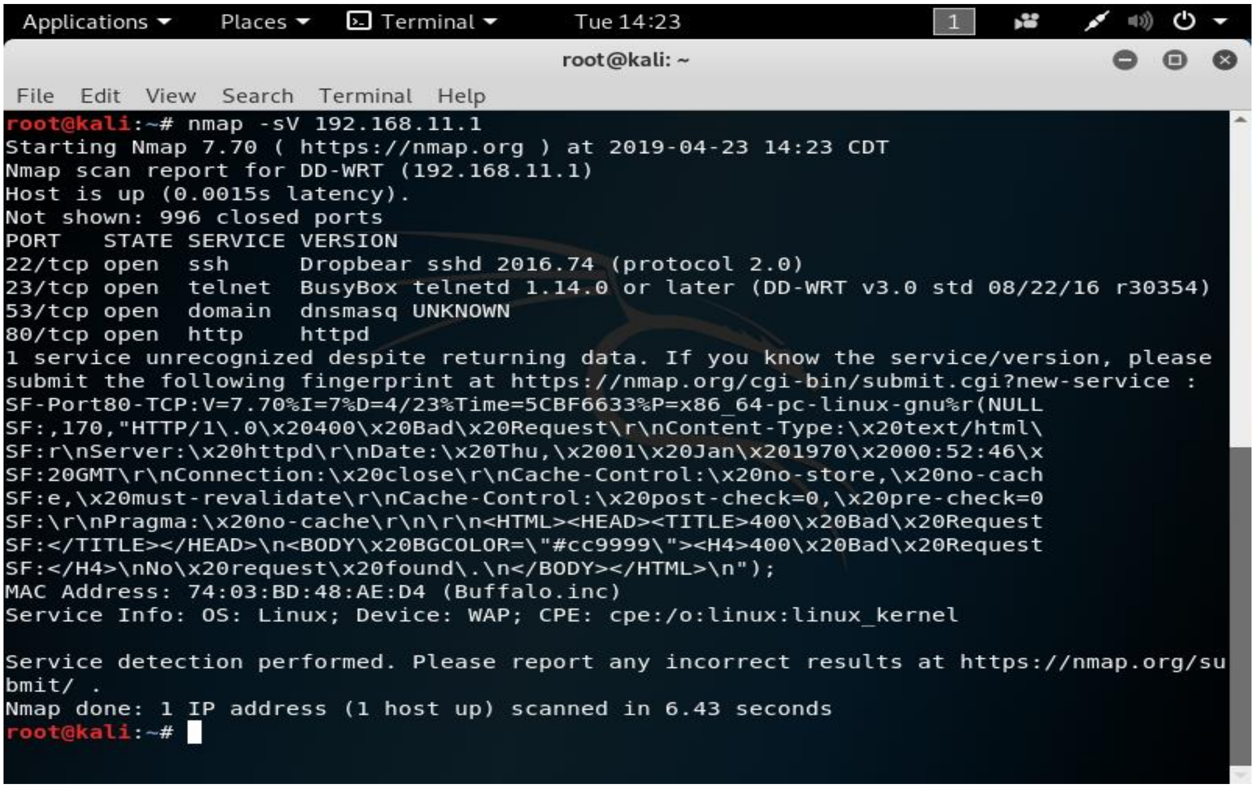
```
root@kali:~# nmap -F 192.168.11.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 14:22 CDT
Nmap scan report for DD-WRT (192.168.11.1)
Host is up (0.0012s latency).
Not shown: 96 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http
MAC Address: 74:03:BD:48:AE:D4 (Buffalo.inc)

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
root@kali:~#
```

nmap -F scans the 100 most common ports



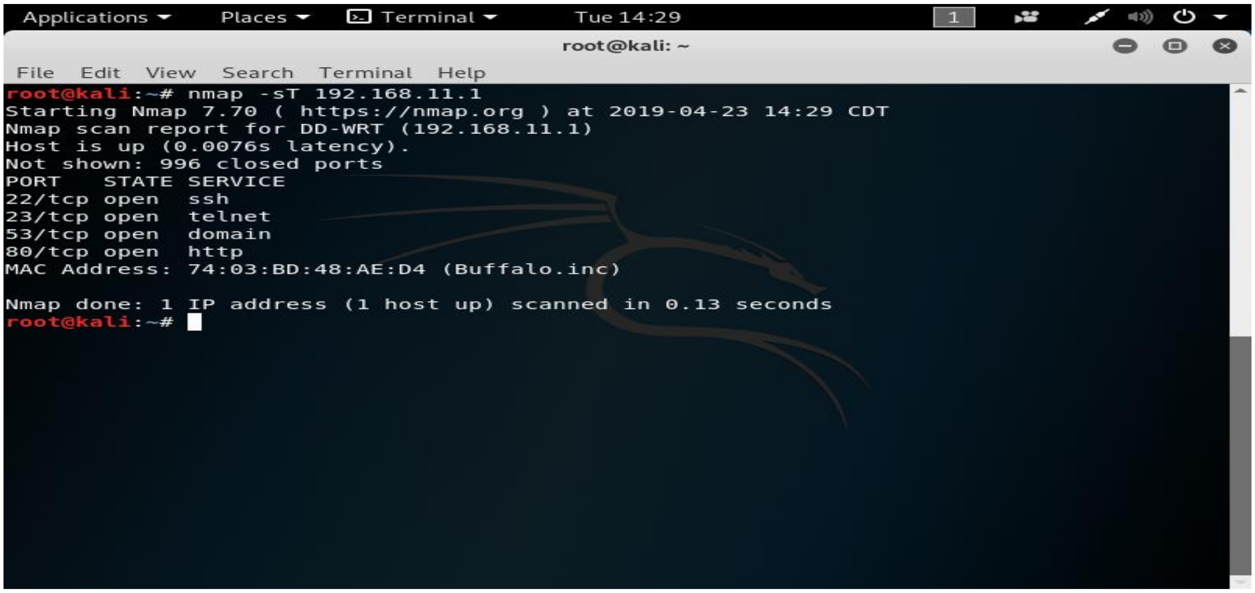
```
root@kali:~# nmap -O 192.168.11.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 14:22 CDT
Nmap scan report for DD-WRT (192.168.11.1)
Host is up (0.00058s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http
MAC Address: 74:03:BD:48:AE:D4 (Buffalo.inc)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
root@kali:~#
```

nmap -O detects operating system



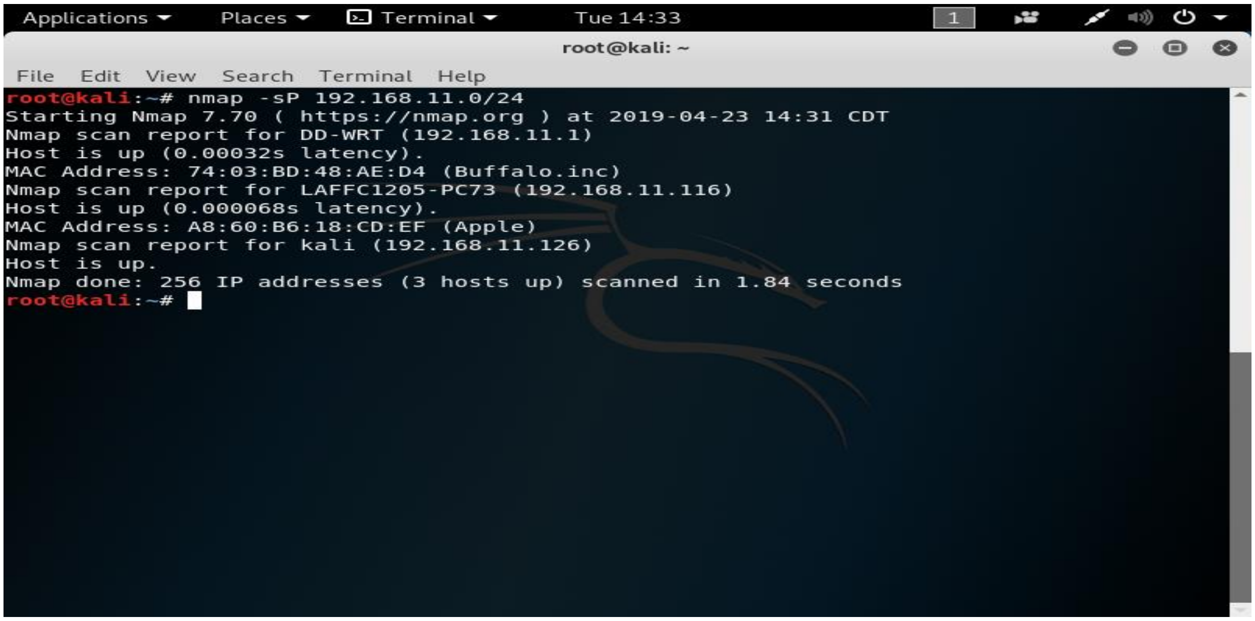
```
root@kali:~# nmap -sV 192.168.11.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 14:23 CDT
Nmap scan report for DD-WRT (192.168.11.1)
Host is up (0.0015s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd 2016.74 (protocol 2.0)
23/tcp open  telnet  BusyBox telnetd 1.14.0 or later (DD-WRT v3.0 std 08/22/16 r30354)
53/tcp open  domain  dnsmasq UNKNOWN
80/tcp open  http    httpd
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.70%I=7%D=4/23%Time=5CBF6633%P=x86_64-pc-linux-gnu%r(NULL
SF:,170,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html\
SF:r\nServer:\x20httpd\r\nDate:\x20Thu,\x2001\x20Jan\x201970\x2000:52:46\x
SF:20GMT\r\nConnection:\x20close\r\nCache-Control:\x20no-store,\x20no-cach
SF:e,\x20must-revalidate\r\nCache-Control:\x20post-check=0,\x20pre-check=0
SF:\r\nPragma:\x20no-cache\r\n\r\n<HTML><HEAD><TITLE>400\x20Bad\x20Request
SF:</TITLE></HEAD>\n<BODY\x20BGCOLOR=\"#cc9999\"><H4>400\x20Bad\x20Request
SF:</H4>\nNo\x20request\x20found\.\n</BODY></HTML>\n");
MAC Address: 74:03:BD:48:AE:D4 (Buffalo.inc)
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds
root@kali:~# 
```

nmap -sV detects service versions



```
root@kali:~# nmap -sT 192.168.11.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 14:29 CDT
Nmap scan report for DD-WRT (192.168.11.1)
Host is up (0.0076s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
53/tcp open  domain
80/tcp open  http
MAC Address: 74:03:BD:48:AE:D4 (Buffalo.inc)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
root@kali:~# 
```

nmap -sT finds the most commonly used TCP ports



```
root@kali:~# nmap -sP 192.168.11.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-23 14:31 CDT
Nmap scan report for DD-WRT (192.168.11.1)
Host is up (0.00032s latency).
MAC Address: 74:03:BD:48:AE:D4 (Buffalo.inc)
Nmap scan report for LAFFC1205-PC73 (192.168.11.116)
Host is up (0.000068s latency).
MAC Address: A8:60:B6:18:CD:EF (Apple)
Nmap scan report for kali (192.168.11.126)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.84 seconds
root@kali:~# 
```

nmap -sP finds the running servers and devices