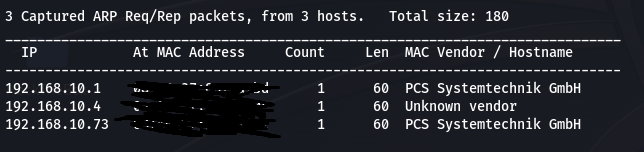
Név: Matrix: 1

Megjelenés dátuma: 2018.08.19

Szerző: Ajay Verma

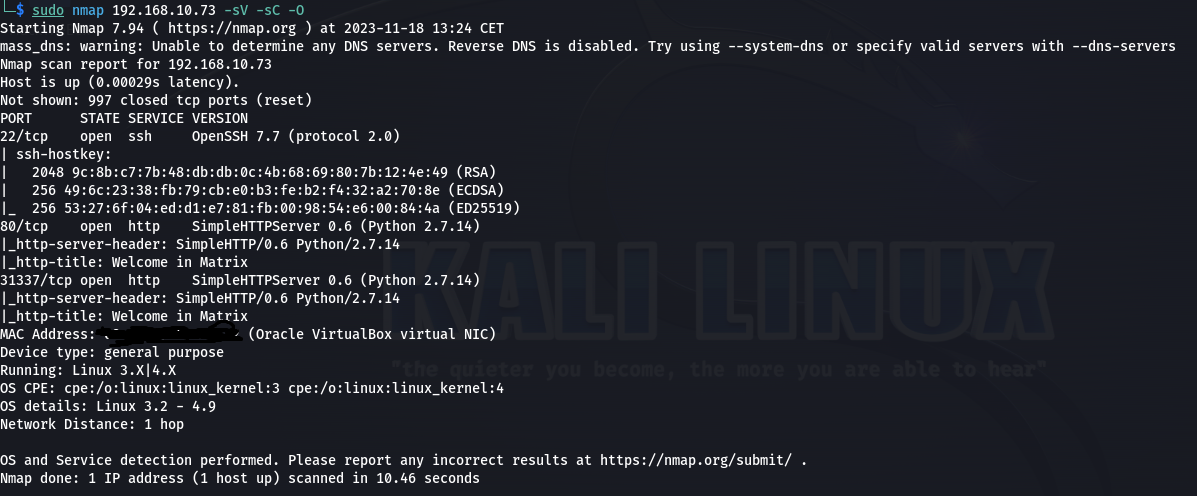
Leírás: Egy egyszerű CTF gép, amiben a root jogig kell eljutnunk. Sok easter egg és félrevezetés is megtalálható a gépben, ami nem ad nekünk plusz információt. A gépet egy kezdő/haladó szintre sorolnám.

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

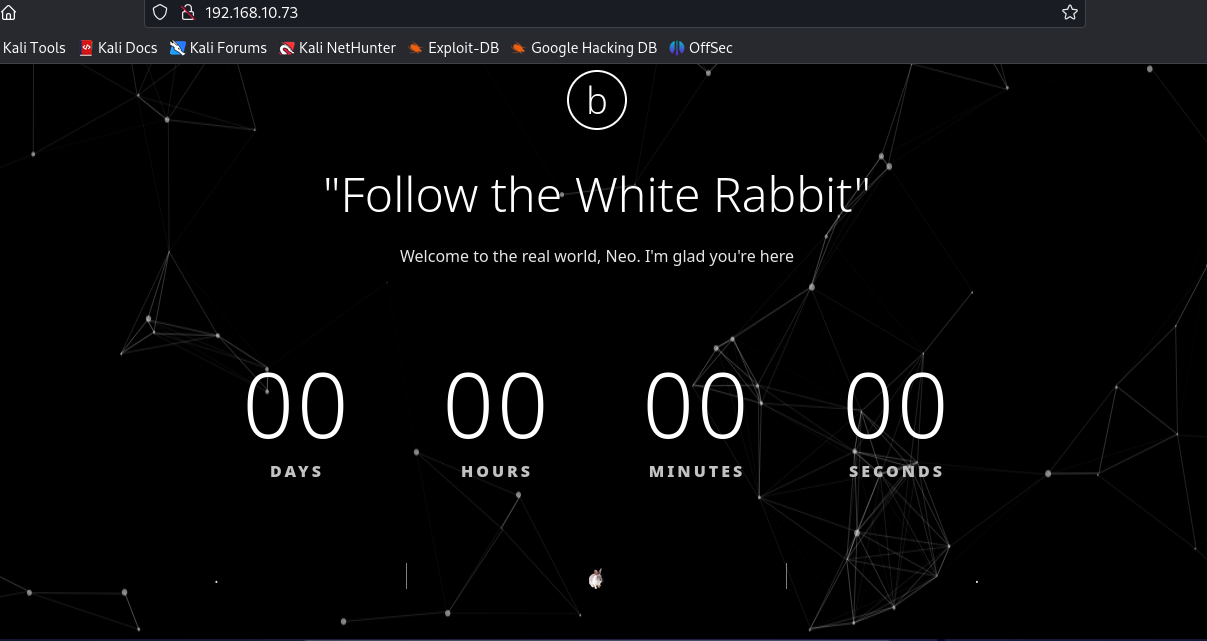
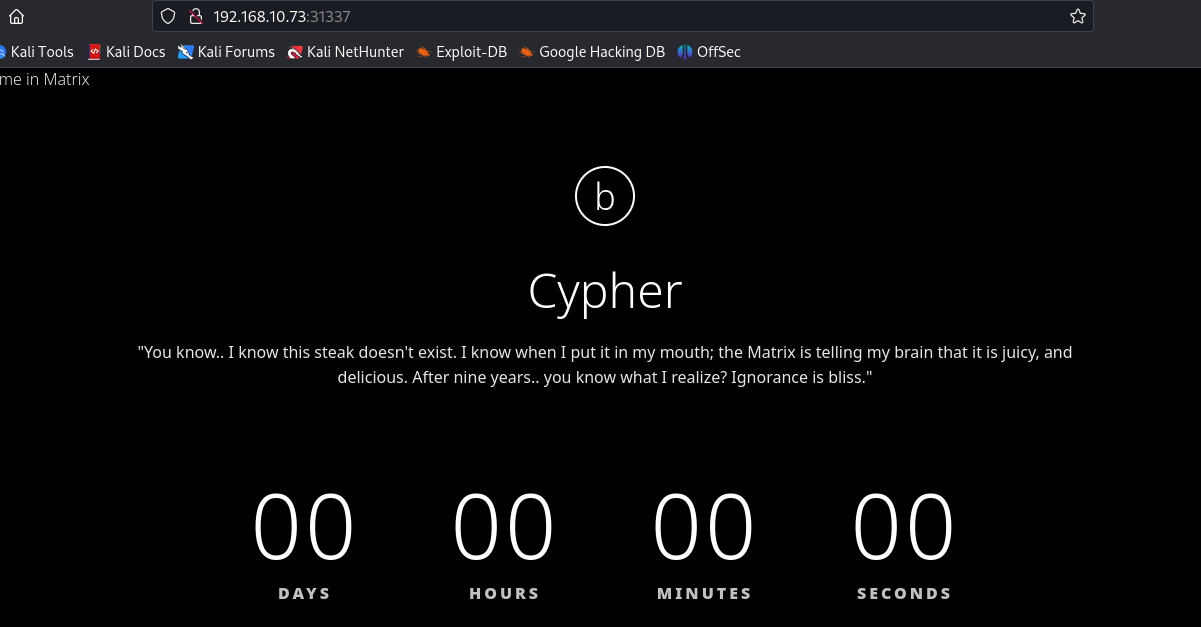


Következőnek megnézem a nyitott portokat és néhány vizsgálatot is elvégzek az nmap-el

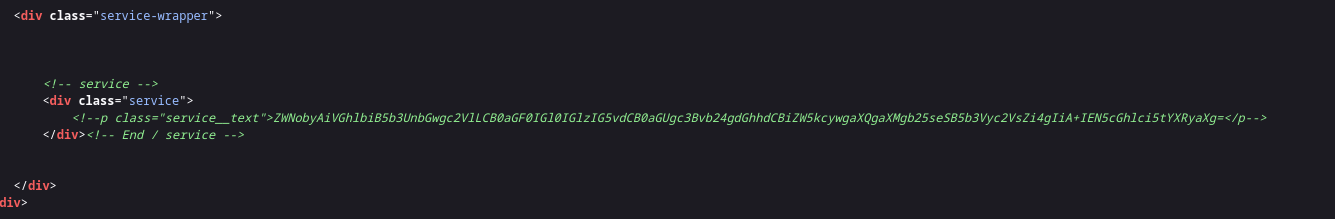
sudo nmap 192.168.10.73 -sV -sC –O



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

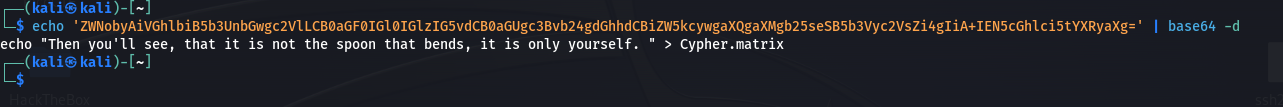


Ha megnézzük a 80-as porton található weboldal forráskódját akkor nem találunk semmi érdekeset. Viszont ha a 31337-es porton találhatóét vizsgáljuk meg akkor találhatunk valami érdekeset.



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

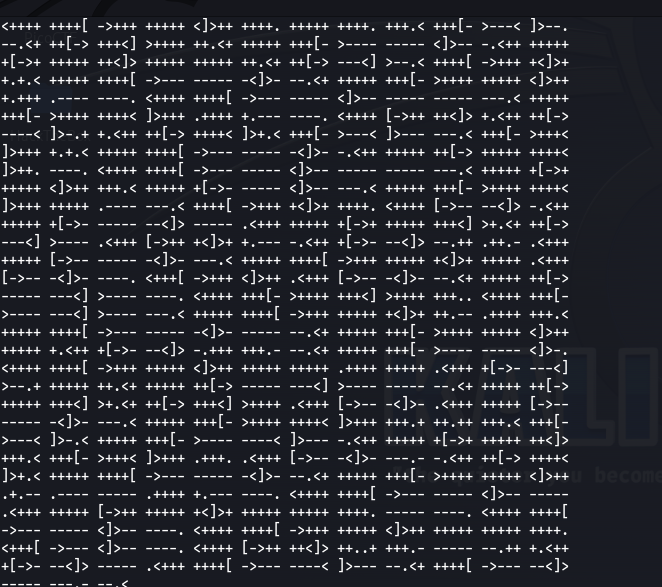
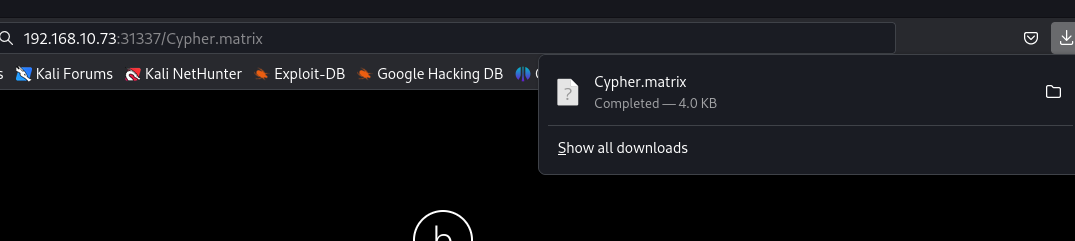
echo 'ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=' | base64 –d



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 filet. A file tartalma egy brainfuck programkód. Az interneten találhatunk is erre egy decodert.



A weboldal a következő: <https://www.dcode.fr/brainfuck-language>

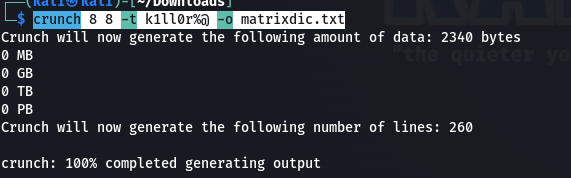
A következő eredményt dobta ki:

You can enter into matrix as guest, with password k1ll0rXX

Note: Actually, I forget last two characters so I have replaced with XX try your luck and find correct string of password.

Generáljunk egy wordlistet a crunch programmal, amiben az utolsó két X helyét kiegészítjük.

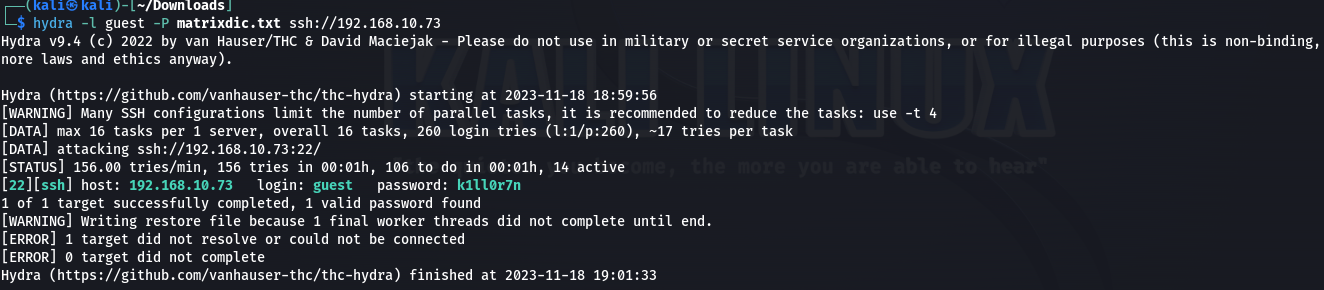
crunch 8 8 -t k1ll0r%@ -o matrixdic.txt



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

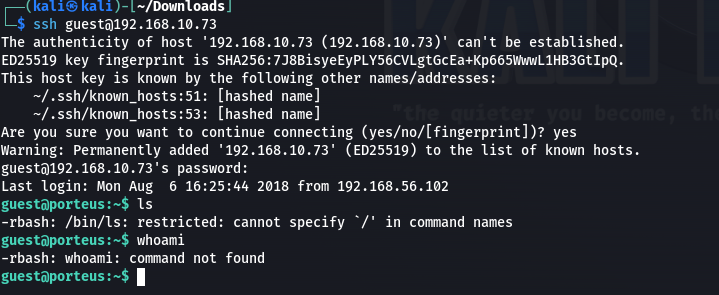
Ezután pedig hydrával bruteforceoljuk az ssh portot.

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



a jelsző: k1ll0r7n

Ha bejelentkezünk az ssh-n keresztül a következő fogad.



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

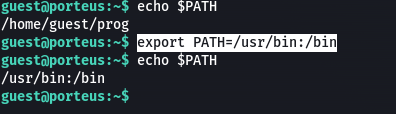
pl: echo /\*  
echo /home/guest/\*

Találunk is egy /home/guest/prog/vi filet. Ha simán beírjuk a terminálba, hogy vi majd a következőt beírjuk kaphatunk egy használható shellt.

:!/bin/bash



export PATH=/usr/bin:/bin



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 filet

