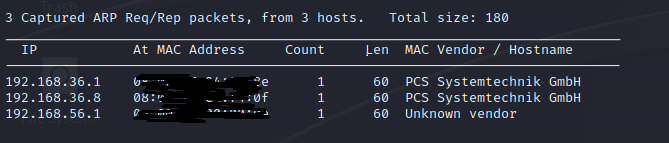
Név: Mr-Robot: 1

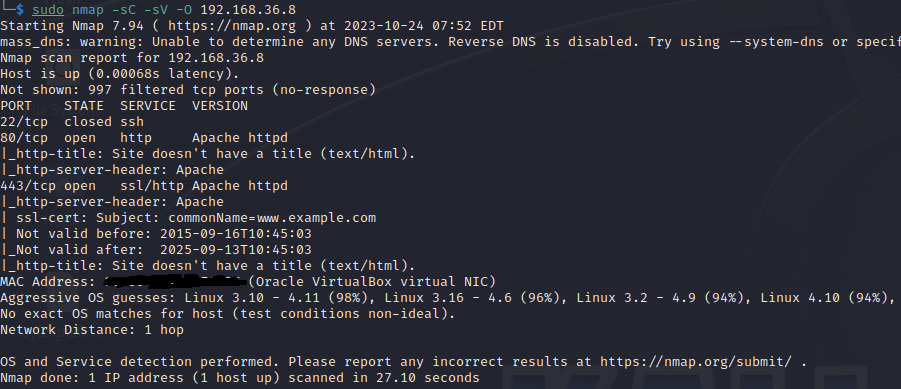
Megjelenés Dátuma: 2016.06.28

Szerző: Leon Johnson

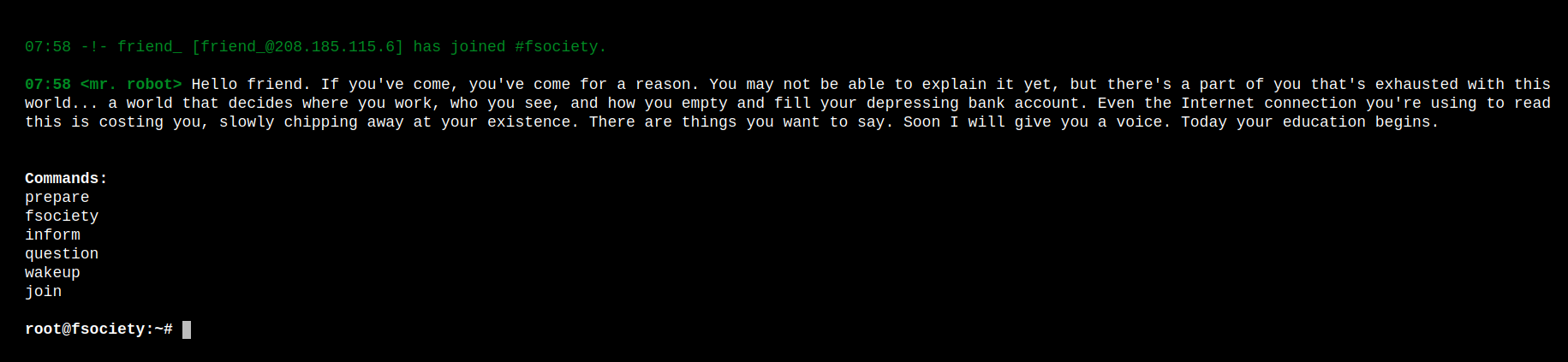
Leírás: A gép a Mr Robot sorozat által inspirált VM. szintjét nagyjából egy kezdő nehézségre tenném, használt programok közé tartozik az NMAP,Gobuster/Dirbuster,WPScan. A következőkben ezt a folyamatot fogom dokumentálni. A cél, hogy megszerezzünk 3 darab flag-et.  
  
Elsőnek is scanneljük végig a hálózatot, hogy beazonosítsuk a hostot. Ezt a netdiscover paranccsal tudjuk megtenni.



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



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

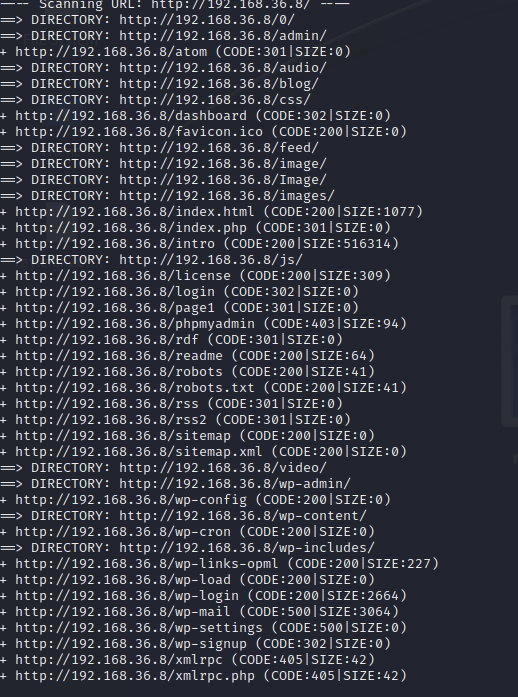


Ha megnyitjuk a böngészőnket és elmegyünk az adott ip-re akkor egy rövid töltés után egy üzenetet kapunk majd egy terminált amiben a megadott parancsokat tudjuk beírni.

* 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.

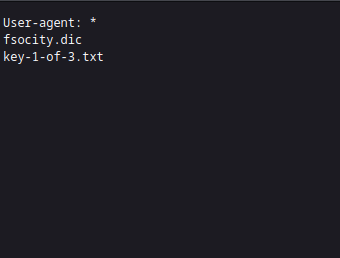
Ezekből a parancsokból, sok hasznos információt nem tudtunk meg, de nézzük meg, hogy milyen elérhető directoriek vannak még, amiket meg tudunk nézni. Ezt személy szerint a dirbuster(dirb) programmal fogom megnézni, de használható a gobuster is.

A parancs a következő: **dirb** [**http://ip-cím**](http://ip-cím)-r

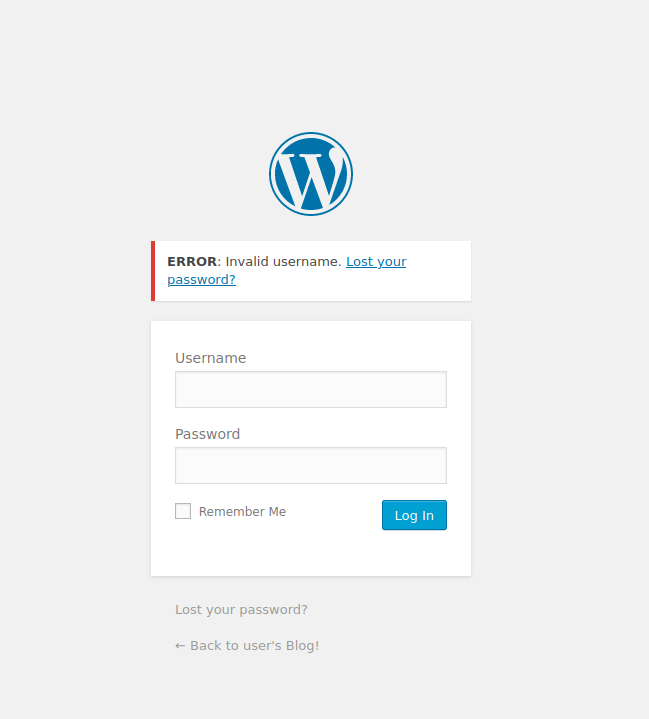


Sok érdekes dolgot találhatunk itt, minket itt a CODE:200 elemek érdekelnek elsősorban hiszen ezekre kaptunk OK választ a böngészőtől. Ezekből is a robots.txt ami nekünk hasznos lesz. Ha elnavigálunk ide, akkor találhatunk 1 filet és az első flaget is.

flag 1: 073403c8a58a1f80d943455fb30724b9



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.

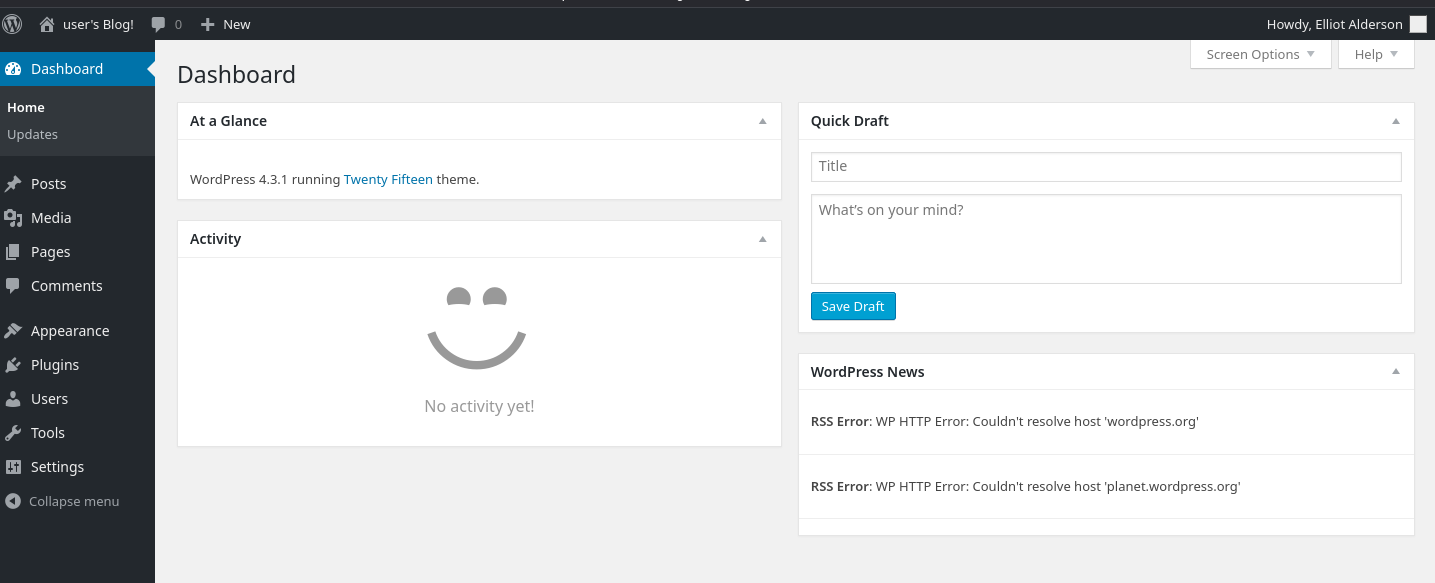


Most egy bruteforce támadást hajtottam végre az elliot nevű felhasználó ellen az fsocity.dic pedig jelszóként használtam fel ebben a műveletben. Az eredmény pedig a következő lett:

**elliot – ER28-0652**

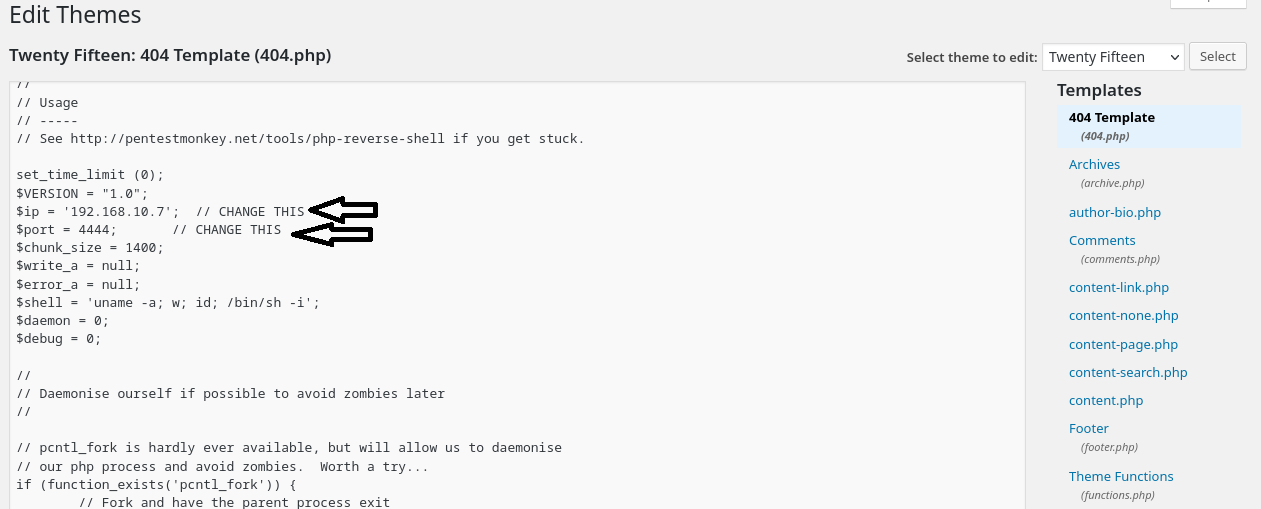
siker!

Beléptünk a WordPress admin panelbe.

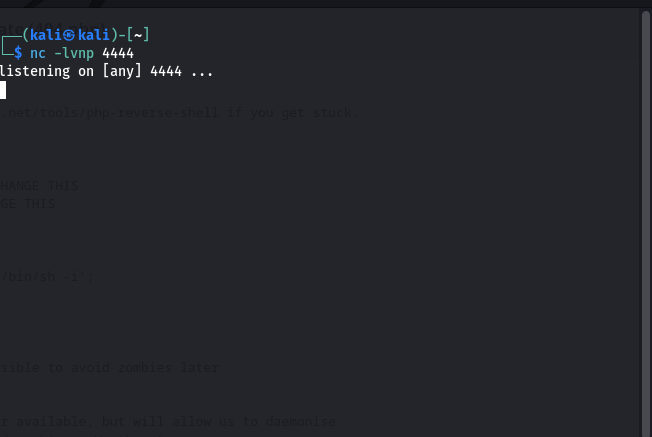


Innen tudunk egy reverse shellt feltölteni és így bejutni a gépbe, majd onnan eljutni a root jogig. Én ezt a pentestmonkey weboldalról letöltött shellt fogom használni, amiben átírom az ip-t és a portot.

<https://pentestmonkey.net/>

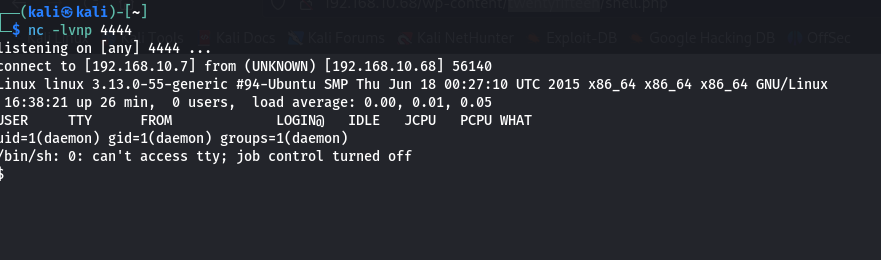


Ez után elindítunk egy listenert ami várni fogja, hogy felcsatlakozzunk rá.

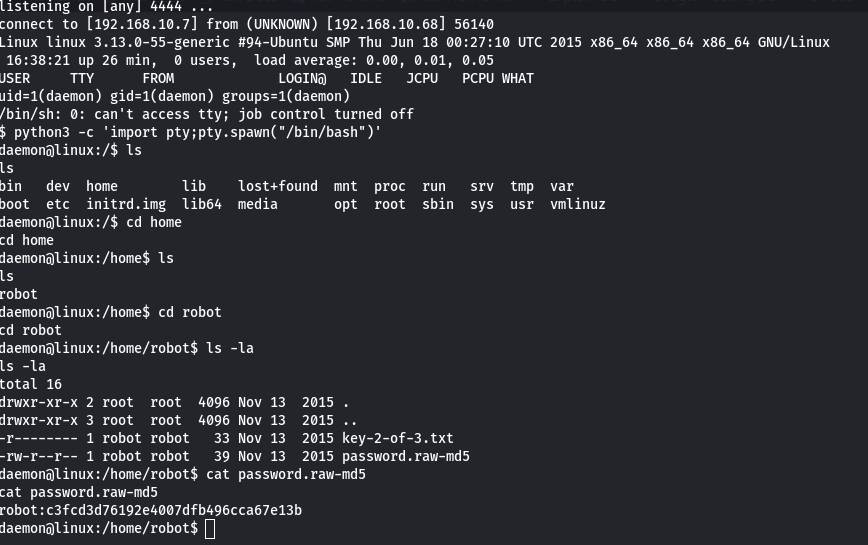


Ha ez is megvan, akkor elnavigálunk a következő címre:

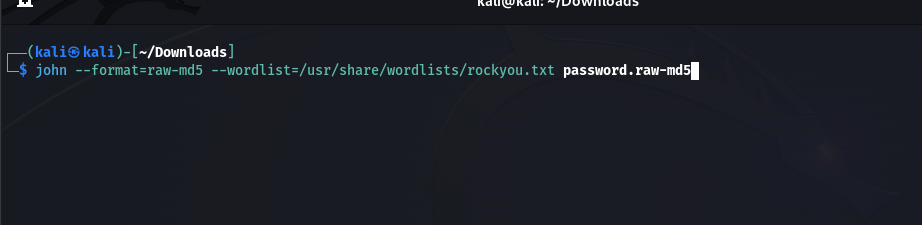
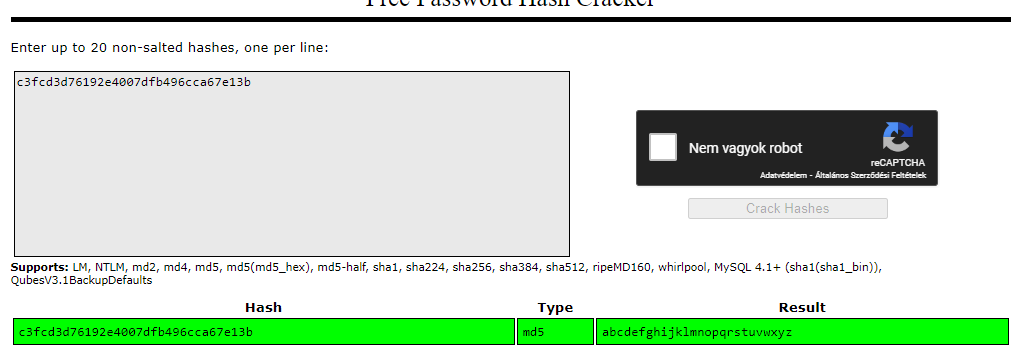
<http://ip-cím/wp-content/twentyfifteen/shellnev.php> és ha mindent jól csináltunk a következőt kell, hogy kapjuk.



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.



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

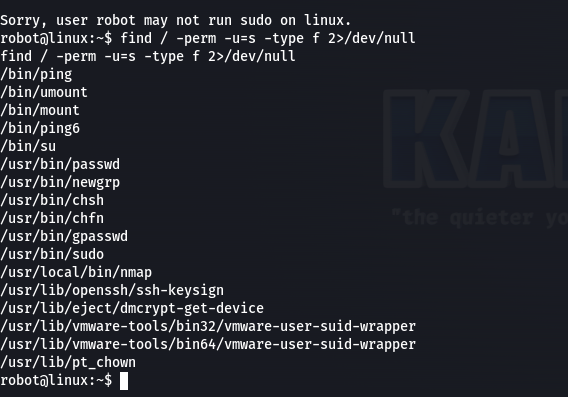
és a következő flag is megvan:

flag 2: 822c73956184f694993bede3eb39f959

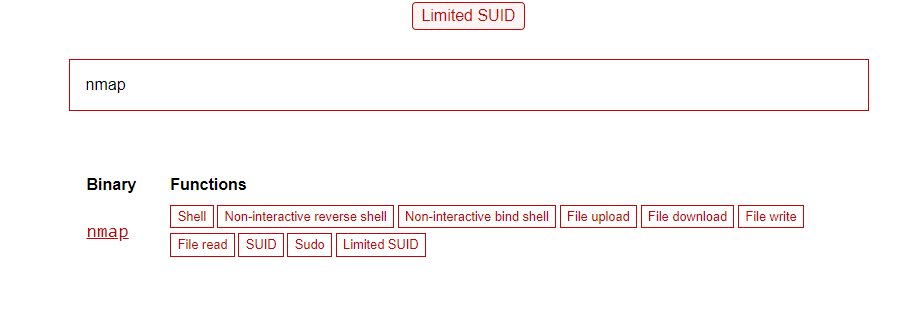
Már csak 1 flag van hátra és egy root jog, hogy kimaxoljuk ezt a feladatot. Most, hogy a robot userbe vagyunk, nézzünk szét is egy kicsit, hogy milyen jogosultságaink vannak. A sudo –l parancsra nem dob ki semmit és a mappánkban sincs már semmi használható. Egy kis ügyeskedés után találhatunk érdekes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

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

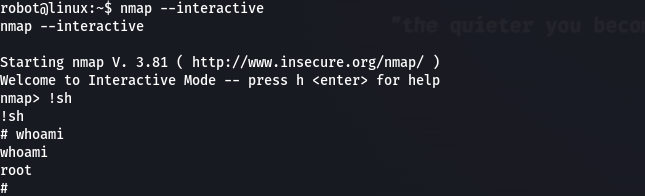
Ez a parancs kilistázza az összes SUID filet a gépen, amivel ha találunk nem jól beállított filet egyszerűen végezhetünk egy privilege escalationt.



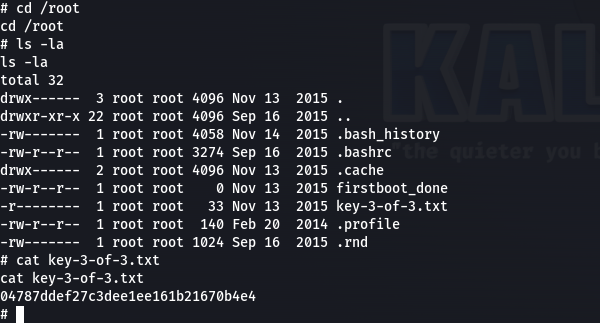
Ezekből sokat nem tudunk felhasználni általában, sőt van olyan is, hogy egyáltalán nem tudjuk őket felhasználni. Viszont jelenleg nem ez a helyzet. Van 1 ami kitűnik. /usr/local/bin/nmap. A <https://gtfobins.github.io/> oldalon több száz ilyen nem jól konfigurált példa van. Ilyen itt az nmap is.



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



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



flag 3: 04787ddef27c3dee1ee161b21670b4e4

