

## Pickle Rick Write UP

Try Hack Me' den IP yi aldıktan sonra IP'ye nmap atıyoruz, nmap attıktan sonra 80 ve 22 portunun açık olduğunu görüyoruz , IP'mizi bu sefer arama motorunda aratıp siteye gidiyoruz bu sırada dirb kullanarak sitedeki izin veya dosyalara bakıyoruz .

```
└─# nmap -vv 10.10.94.73
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-15 11:54 EST
Initiating Ping Scan at 11:54
Scanning 10.10.94.73 [4 ports]
Completed Ping Scan at 11:54, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:54
Completed Parallel DNS resolution of 1 host. at 11:54, 0.02s elapsed
Initiating SYN Stealth Scan at 11:54
Scanning 10.10.94.73 [1000 ports]
Discovered open port 80/tcp on 10.10.94.73
Discovered open port 22/tcp on 10.10.94.73
Completed SYN Stealth Scan at 11:54, 1.98s elapsed (1000 total ports)
Nmap scan report for 10.10.94.73
Host is up, received echo-reply ttl 63 (0.13s latency).
Scanned at 2022-02-15 11:54:19 EST for 2s
Not shown: 998 closed ports
Reason: 998 resets
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
Raw packets sent: 1083 (47.628KB) | Rcvd: 1050 (41.996KB)
```

Burda bazı dosyaları görüyoruz. Bu izinleri denemeye başlıyoruz.

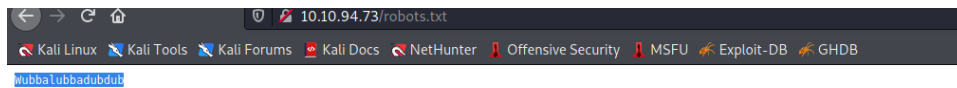
```
GENERATED WORDS: 4612

— Scanning URL: http://10.10.94.73/ —
⇒ DIRECTORY: http://10.10.94.73/assets/
+ http://10.10.94.73/index.html (CODE:200|SIZE:1062)
+ http://10.10.94.73/robots.txt (CODE:200|SIZE:17)
+ http://10.10.94.73/server-status (CODE:403|SIZE:299)

— Entering directory: http://10.10.94.73/assets/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Tue Feb 15 12:05:00 2022
DOWNLOADED: 4612 - FOUND: 3
```

IP' mizin robots.txt yazan dosyasına girdiğimizde bir yazı karşımıza geliyor.



Bu yazıyı kopyalıyoruz ve sitemizin index.html ' ine gidiyoruz burda kaynak kodumuzu açtığımızda karşımıza şöyle bir ekran geliyor

```

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <title>Rick is sup4r cool</title>
5 <meta charset="utf-8">
6 <meta name="viewport" content="width=device-width, initial-scale=1">
7 <link rel="stylesheet" href="assets/bootstrap.min.css">
8 <script src="assets/jquery.min.js"></script>
9 <script src="assets/bootstrap.min.js"></script>
10 <style>
11 .jumbotron {
12   background-image: url("assets/rickandmorty.jpeg");
13   background-size: cover;
14   height: 340px;
15 }
16 </style>
17 </head>
18 <body>
19
20 <div class="container">
21 <div class="jumbotron"></div>
22 <h1>Help Morty!</h1></div>
23 <p>Listen Morty... I need your help. I've turned myself into a pickle again and this time I can't change back!</p></div>
24 <p>I need you to <b>BURRED</b> Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
25 I have no idea what the <b>BURRED</b>, password was! Help Morty, Help!</p></div>
26 </div>
27
28 <!--
29 Note to self, remember username!
30
31 Username: <b>Pickles</b>
32
33 -->
34
35 </body>
36 </html>
37
38

```

Burda yazan username'i kopyalayip sitemizin login.php'sine gidiyoruz. Burda kopyaladığımız kullanıcı adını ve parolayı girdikten sonra karşımıza şöyle bir ekran çıkıyor.

Rick Portal
Commands
Poisons
Creatures
Poisons
Beth Clone Notes

Command Panel

Execute

Burda karşımıza bir command panel geliyor bu panele ls komutunu yazdığımızda karşımıza şu ekran geliyor

Command Panel

Execute

```

Sup3rS3cretPick13Ingred.txt
assets
c1ue.txt
denied.php
index.html
login.php
portal.php
robots.txt

```

Bu dosyaları tek tek deniyoruz ve Sup3rS3cretPick13Ingred.txt açtığımızda ilk key'i alıyoruz

```
mr. meeseek hair
```

İlk key'imizi aldıktan sonra diğer dosyalarımızı deniyoruz. Burda clue.txt yi denerken karşımıza boş bir şey çıkıyor bunun için üst dizinlere çıkıyoruz karşımıza bu çıkıyor

Command Panel

Commands

Execute

```
total 88
drwxr-xr-x 23 root root 4096 Feb 15 16:51 .
drwxr-xr-x 23 root root 4096 Feb 15 16:51 ..
drwxr-xr-x 2 root root 4096 Nov 14 2018 bin
drwxr-xr-x 3 root root 4096 Nov 14 2018 boot
drwxr-xr-x 14 root root 3269 Feb 15 16:51 dev
drwxr-xr-x 94 root root 4096 Feb 15 16:51 etc
drwxr-xr-x 4 root root 4096 Feb 19 2019 home
lrwxrwxrwx 1 root root 30 Nov 14 2018 initrd.img -> boot/initrd.img-4.4.0-1072-aws
drwxr-xr-x 21 root root 4096 Feb 19 2019 lib
drwxr-xr-x 2 root root 4096 Nov 14 2018 lib64
drwx----- 2 root root 16384 Nov 14 2018 lost+found
drwxr-xr-x 2 root root 4096 Nov 14 2018 media
drwxr-xr-x 2 root root 4096 Nov 14 2018 mnt
drwxr-xr-x 2 root root 4096 Nov 14 2018 opt
dr-xr-xr-x 136 root root 0 Feb 15 16:51 proc
drwx----- 4 root root 4096 Feb 19 2019 root
drwxr-xr-x 25 root root 880 Feb 15 16:52 run
drwxr-xr-x 2 root root 4096 Nov 14 2018/sbin
drwxr-xr-x 5 root root 4096 Feb 19 2019 snap
drwxr-xr-x 2 root root 4096 Nov 14 2018 srv
dr-xr-xr-x 13 root root 0 Feb 15 16:51 sys
drwxrwxrwt 8 root root 4096 Feb 15 17:39 tmp
drwxr-xr-x 10 root root 4096 Nov 14 2018 usr
drwxr-xr-x 14 root root 4096 Feb 19 2019 var
lrwxrwxrwx 1 root root 27 Nov 14 2018 vmlinuz -> boot/vmlinuz-4.4.0-1072-aws
/
```

Sonra gine dizinlere çıkarak 2 Key'i buluyoruz. Sonra yetki alarak clue.txt açarak son keyi buluyoruz.