

Exploitation Report

1. Objective

The purpose of this task was to verify the vulnerabilities identified during earlier scanning activities by performing exploitation in a controlled laboratory environment. The objective was not to cause damage, but to confirm whether the weaknesses could actually be exploited and to understand the possible impact of such attacks in a real-world scenario.

2. Scope of Assessment

- Target Systems: Metasploitable / DVWA Virtual Machine
- Target IP Address: 192.168.75.131
- Assessment Type: Controlled exploitation (lab environment)
- Environment: Academic / Educational

All activities were carried out strictly for learning purposes and within a closed lab setup.

3. Tools Used

The following tools were used during the exploitation process:

- Nmap – Used to re-verify open ports and running services
- Metasploit Framework – Used for service enumeration and exploitation
- Burp Suite – Used to intercept and analyze HTTP requests
- sqlmap – Used to test and exploit SQL Injection vulnerabilities

4. Methodology

The exploitation process was performed in a structured manner:

1. Nmap scans were used to confirm exposed services on the target system.
2. Metasploit was used to enumerate and attempt exploitation of the Apache Tomcat Manager service.
3. Burp Suite was used to observe and validate application behavior by intercepting HTTP traffic.
4. SQL Injection vulnerabilities were tested on DVWA using sqlmap.

5. All successful exploitation steps and their outcomes were documented using screenshots and logs.

5. Exploitation Performed

5.1 Apache Tomcat Manager Exploitation

The Apache Tomcat Manager service running on port 8180 was tested using Metasploit's Tomcat login module. During testing, default credentials were found to be valid, which allowed successful authentication to the Tomcat Manager interface.

Impact:

If exploited by an attacker, unauthorized access to the Tomcat Manager could allow deployment of malicious applications, modification of server settings, or further compromise of the system.

5.2 SQL Injection Exploitation (DVWA)

The SQL Injection module in DVWA was tested using sqlmap. The tool successfully detected SQL Injection vulnerabilities caused by improper input validation. Database interaction was confirmed through automated queries.

Impact:

A successful SQL Injection attack could allow attackers to extract sensitive database information or manipulate backend data.

6. Validation Using Burp Suite

Burp Suite was used to intercept and analyze HTTP requests sent to both the Tomcat Manager and DVWA applications. The captured requests and responses confirmed the behavior of the applications and validated the exploitation workflow.

7. Risk and Impact Analysis

The exploitation results showed that both service-level and application-level vulnerabilities were present and exploitable. If such weaknesses exist in a production environment, they could lead to unauthorized access, data leakage, or complete system compromise.

8. Remediation Recommendations

To reduce the identified risks, the following measures are recommended:

- Disable default credentials and restrict access to the Tomcat Manager interface
- Implement strong authentication and role-based access control
- Use proper input validation and parameterized queries to prevent SQL Injection
- Regularly update and patch all server components
- Perform periodic vulnerability assessments and penetration testing

9. Conclusion

This exploitation lab demonstrated how vulnerabilities identified during scanning can be practically exploited in a controlled environment. The exercise highlights the importance of secure configuration, regular patching, and continuous security testing. Addressing these issues can significantly reduce the risk of successful attacks in real-world systems.