Title

Advanced Exploitation Lab – Chained Exploit Demonstration

Objective

The objective of this lab was to perform an advanced exploitation task by
chaining vulnerabilities and demonstrating remote code execution using Metasploit and a customized Python exploit from Exploit-DB.

Lab Environment

Attacker Machine : Kali Linux (VMware)
Target Machine : Metasploitable2
Target IP : 192.168.79.129
Tools Used : Metasploit, Python, Exploit-DB

Exploit Chain Description

1. A client-side vulnerability (stored XSS) was identified in the web application.

2. The vulnerability was conceptually chained to a server-side weakness.

3. Apache Tomcat Manager with default credentials was exploited using Metasploit to gain remote code execution.

4. A Python-based proof-of-concept exploit from Exploit-DB was customized
to demonstrate exploit adaptation.

🔹 Exploit Log Table

Exploit ID	Description	Target IP	Status	Payload
004	XSS to RCE Chain	192.168.79.129	Success	Meterpreter

🔹 Python Exploit Customization (IMPORTANT)

A Python exploit targeting the vsFTPd 2.3.4 backdoor was downloaded from
Exploit-DB and modified by changing the target IP address and adjusting the
command payload. This demonstrated the ability to customize public exploits
for a specific lab environment.

🔹 Findings

- Stored XSS vulnerability
- Weak/default credentials on Tomcat Manager
- Presence of outdated services (vsFTPd 2.3.4)
- Improper access control

🔹 Remediation

- Sanitize and validate user input
- Disable default credentials
- Restrict access to administrative interfaces
- Regularly update and patch services