Reconnaissance & Scanning Results

TOOL	Finding
Nmap	Multiple open ports detected (FTP,SSH etc.)
Shodan	No public exposure (Private IP)
Subdomain Finder	www.example.com found
Wappalyzer	Cloudflare CDN, HTTP/2 detected
Metasploit	Basic tomcat scan executed (No successful exploitation)
SHA256	File integrity hash generated successfully

Recon Summary:
During reconnaissance, tools like Shodan, Subdomain Finder, and Wappalyzer were used. No major public exposure was found. One subdomain was identified and technology stack revealed Cloudflare CDN and HTTP/2 usage.

Exploitation Attempt Log

Exploit	Target IP	Status
Tomcat Scanner	192.168.71.130	Connection Refused

CVSS Risk Assessment Table

Vulnerability	CVSS	Priority
Open Port 445	6.5	Medium
Tomcat Service	8.0	High

This table represents basic vulnerability risk scoring based on CVSS standard.