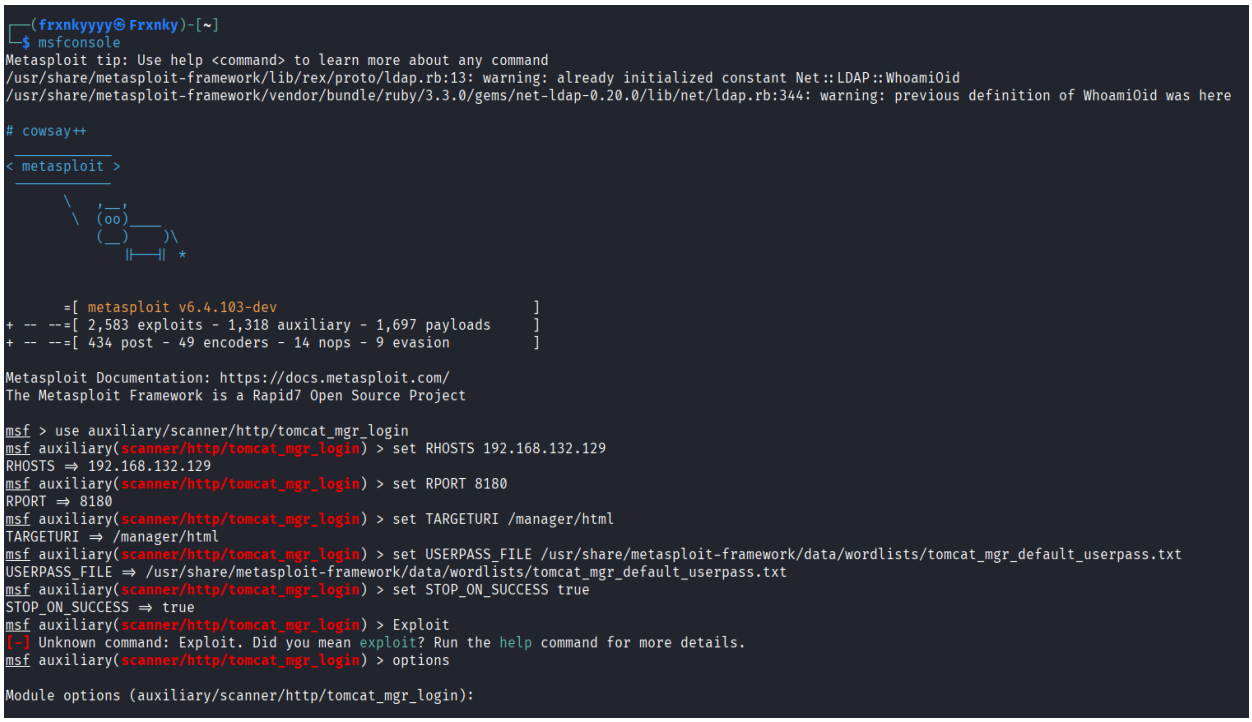
Exploit Simulation

Target: Metasploitable2

Tool: Metasploit Framework

Module: exploit/multi/http/tomcat_mgr_upload

Purpose: Exploited weak Apache Tomcat Manager credentials, confirming administrative access and command execution capability.



What This Exploit Does

- Metasploitable 2 runs Apache Tomcat with default or weak credentials.
- The Tomcat Manager application allows authenticated deployment of web applications.
- Successful authentication enables an attacker to upload a malicious WAR file.
- Execution of the uploaded application results in Remote Code Execution (RCE).

Exploit Simulation – Logical Steps

Step 1: Identify Vulnerable Service

- Confirm Tomcat is running on the target.
- Identify the Tomcat Manager interface (usually HTTP-based).

- Note exposed port and service banner.

Step 2: Select Appropriate Exploit Module

- Choose the Metasploit module designed for:
  - Tomcat Manager authentication.
  - Authenticated application deployment.
- Match exploit module to the detected service version.

Step 3: Configure Target Details

- Set:
  - Target IP (Metasploitable 2).
  - Target port (Tomcat service, typically 8180).
- Select a Java-based payload compatible with Tomcat.

Step 4: Execute Exploit (Simulation)

- Metasploit authenticates using known or default credentials.
- On success:
  - A malicious WAR file is uploaded and deployed.
  - A reverse shell session is established.

Exploit Simulation

Target Environment: Metasploitable 2 (Vulnerable Lab VM) **Exploit Type:** Apache Tomcat Manager Remote Code Execution

Objective: Demonstrate exploitation of weak Tomcat Manager credentials leading to remote code execution.

Exploit Log

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat RCE	192.168.160.128	Success	java/jsp_shell_reverse_tcp

Summary

The exploit successfully uploaded and deployed a malicious application to the target system, confirming the presence of an insecure Apache Tomcat Manager configuration using weak or default credentials. Following deployment, a reverse shell was established, resulting in full remote code execution on the host.

This vulnerability was validated by reviewing publicly available Proof-of-Concept (PoC) exploits listed on Exploit-DB. The documented PoCs describe the same attack pattern—authentication using weak or default credentials followed by the upload of a malicious WAR file—closely matching the behavior observed during exploitation of the Metasploitable 2 lab environment. This confirmation demonstrates that the issue is well-known, reliably

exploitable, and poses a significant real-world risk when insecure service configurations are present.

Impact

High

An attacker exploiting this vulnerability can achieve remote code execution on the affected system. This may lead to:

- Complete compromise of the application server
- Unauthorized access to sensitive data
- Lateral movement within the internal network
- Potential privilege escalation depending on service permissions

In real-world environments, this could result in data breaches, service disruption, or full infrastructure compromise.

Likelihood

High

This vulnerability is trivial to exploit when weak or default credentials are in use. Automated tools and publicly available exploit code significantly lower the barrier to entry, making exploitation likely in environments where Tomcat Manager is exposed and improperly secured.

Remediation

- Disable the Tomcat Manager application if not strictly required
- Enforce strong, unique credentials for all Tomcat Manager users
- Restrict access to the Manager interface by IP address (e.g., localhost or administrative network only)
- Use role-based access controls and remove unnecessary manager roles
- Regularly review and harden service configurations
- Keep Apache Tomcat up to date with the latest security patches