Penetration Test Report: ToolsRUs

Executive Summary: The following report details the penetration test conducted against the target IP address 10.10.101.231. The test revealed several services running on the host, including SSH, HTTP, Apache Tomcat, and Apache Jserv. Notable findings indicated potential vulnerabilities associated with an outdated TomCat server and a protected web directory that could be susceptible to brute force attacks.

Testing Methodology:

1. **Initial Scanning:**
    - Conducted an aggressive Nmap scan on the target IP.
    - Identified open ports: SSH (22), HTTP (80), Tomcat (1234), and Apache Jserv (8009).
    - Services running included OpenSSH, Apache HTTPD, Apache Tomcat, and Apache Jserv.
2. **HTTP Enumeration:**
    - Executed a Gobuster scan to enumerate directories on the HTTP server.
    - Discovered two directories of interest: **/guidelines** and **/protected**.
    - Noted a potential username "bob" from the content found in **/guidelines**.
3. **Apache Tomcat Enumeration:**
    - Accessed Apache Tomcat server on port 1234, confirmed version 7.0.88.
    - Investigated **/protected** directory, which led to a basic authentication login prompt.
4. **Brute Force Attack:**
    - Utilized Hydra to perform a brute force attack on the **/protected** directory with username "bob".
    - Successfully obtained credentials: **bob:bubbles**.
5. **Vulnerability Scanning:**
    - Ran Nikto against the Tomcat manager interface with the obtained credentials.
    - Identified the manager interface at **/manager/html**.
6. **Exploitation with Metasploit:**
    - Launched Metasploit and searched for applicable Tomcat exploits.
    - Chose **tomcat_mgr_upload** exploit module.
    - Configured the module with credentials and target information.
    - Executed the exploit and obtained a shell on the target system.

- Confirmed root access.

Findings: The test uncovered an outdated TomCat server and exposed a basic authentication service that was vulnerable to brute force attacks. Using the credentials obtained, we were able to escalate privileges to root by exploiting the TomCat manager application.

Conclusion: The target IP was found to have critical vulnerabilities that allowed an attacker to escalate privileges and gain root access. Immediate remediation steps should include updating the TomCat server, strengthening password policies, and securing the TomCat manager interface.

Recommendations:

- Update the Apache Tomcat server to the latest version to address any known vulnerabilities.
- Implement account lockout policies to mitigate brute force attacks.
- Apply the principle of least privilege to service accounts.
- Regularly audit web application directories for unnecessary exposure to the web.