htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

GNU/Linux - Securing access

Laboratory protocol

Figure 1: Grouplogo

Subject: ITSI|ZIVK
Class: 3AHITN
Name: Stefan Fürst, Marcel Raichle
Gruppenname/Nummer: Dumm und Dümmer/7
Supervisor: ZIVK
Exercise dates:
Submission date:

Contents

1 Task definition

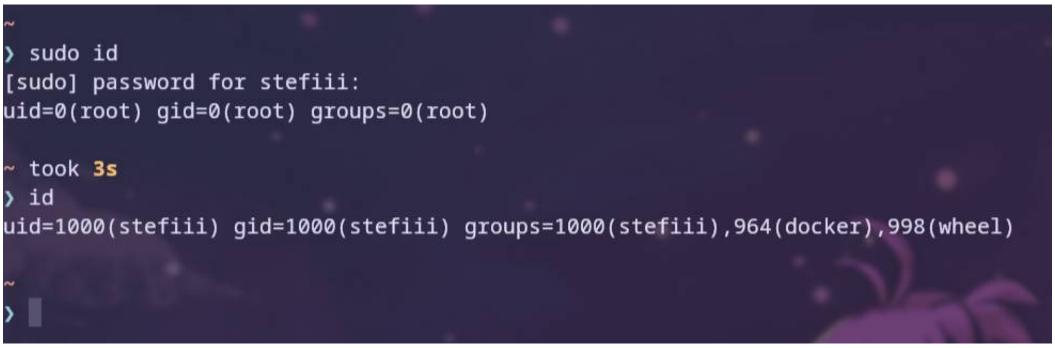
2 Summary

3 Exercise Execution

3.1 Privileged rights

3.1.1 Explanation of the sudo command

The `sudo` command or **S**uper**U**ser **DO** temporarily elevates privileges and runs the set command as root, which can be seen by running the `sudo id` command.[1]



```
~
❯ sudo id
[sudo] password for stefiii:
uid=0(root) gid=0(root) groups=0(root)

~ took 3s
❯ id
uid=1000(stefiii) gid=1000(stefiii) groups=1000(stefiii),964(docker),998(wheel)

~
❯
```

Figure 2: sudo id

As seen in the figure, when the `id` command is used with `sudo`, the id displayed is 0, which is the user id of the root user, and without sudo it displays the normal user id of the user who executed the command.

3.1.2 Granting and restricting users' sudo access

To grant someone permission to run any command with `sudo`, the `usermod -aG sudo username` command is used, which appends the given to the sudo group, giving them permission to run any command with sudo.
In order to restrict the commands that can be elevated by a user or to configure other settings related to this, it is necessary to edit the configuration file, which is located at `/etc/sudoers`.
There are several ways to edit it. The `visudo` command uses the editor set in the `$EDITOR` environment variable and opens the sudoers file with it, and when you exit the editor and save it, it also checks for errors before applying the changes. The sudoers file can also be directly edited using `echo` in the dockerfile.

```
#only allowing ram-alois to edit the ssh configuration file
RUN echo "ram-alois ALL=(root) /bin/nano /etc/ssh/sshd_config" >> /etc/sudoers
#only allowing ram-berta to add users
RUN echo "ram-berta ALL=(root) /sbin/useradd" >> /etc/sudoers
#only allowing to ram-ram to view and read add files
RUN echo "ram-ram ALL=(root) /bin/ls" >> /etc/sudoers
RUN echo "ram-ram ALL=(root) /bin/cat" >> /etc/sudoers
```

I chose nano over vim for editing the ssh config file, as running vim as sudo effectively gives the user full sudo access, as it is possible to open a terminal in it and escape the normal editor mode in numerous ways, so its just easier to give the user nano.
insert screenshots of the thing

3.1.3 Setting up a password policy

```
RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_confi
RUN sed -i '/retry=3/ s/$/ucredit=-1 dcredit=-1 ocredit=-1/' /etc/pam.d/common-password
RUN sed -i '/ocredit=-1/ a password\trequisite\t\t\tpam_pwhistory.so remember=5 use_authto
RUN sed -i '/yescrypt/ s/$/ minlen=10/' /etc/pam.d/common-password
```

4 References

References

[1] Sara Zivanov. Linux Sudo Command {How to Use It +Examples}. *Knowledge Base by phoenixNAP*, June 2024.

5 List of figures

List of Figures