Linux Privilege Escalation

Introduction to the Linux Shell

Leonardo Tamiano

Contents

1 Example: SSH Connection

Dockerfile

```
FROM ubuntu:latest

RUN apt-get update && apt-get install -y openssh-server sudo
RUN useradd -rm -d /home/sshuser -s /bin/bash -g root -G sudo sshuser
RUN echo "sshuser:password" | chpasswd
RUN mkdir /var/run/sshd

EXPOSE 22

CMD ["/usr/sbin/sshd", "-D"]
```

Manage docker

```
docker build -t ssh-lab .
docker run --name ssh-lab --rm -p 22:22 -d ssh-lab
docker exec -u root -t -i ssh-lab /bin/sh
```

Run `sftp` docker image

```
docker run -p 22:22 -d ssh-lab
```

Suppose we have to connect to an `sftp` server. We can execute the following command

```
ssh -o "UserKnownHostsFile=/dev/null" sshuser@127.0.0.1
```

In order to do this I have implicitly answered the following questions:

1. What program do I need to access the server?
2. What is the IP address of the server?
3. What is the username?
4. What is the password?

2 Terminal, TTY and Bash

Taken from:

- https://kevroletin.github.io/terminal/2021/12/11/how-terminal-works-in.html
- https://www.linusakesson.net/programming/tty/index.php

```
           (1)         (2)       (3)
user <---> xterm <---> tty <---> bash
```

- User input is converted into GUI events that are captured by xterm.
- Terminals such as `xterm` visualize output of commands and pass user input to command-line tools.
- The `tty` is an abstraction that handles the communication between a terminal and an interpreter.
- `Bash` is an implementation of a command-line interpreter that executes commands on the operating system.

3 Basic Information

When using a terminal, the first step is to understand how to extract basic information from the system.

The following command will help in a linux-based system.

- **username**

  ```
  whoami
  id
  ```

- **hostname**

  ```
  hostname
  ```

- **working directory**

  ```
  pwd
  ```

- **environment variables**

  ```
  env
  ```

- **which (and $PATH)**

  ```
  which which
  ```

4 Relative vs Absolute Paths

- **absolute path**

```
/home/leo/projects/FOUNDATIONS/yt-en/linux-privesc/01-introduction-shell/content/notes.org
```

- **relative path**

```
../../../certs-oscp/full/video/
```

5 File System Commands

Commands to move in the **File System**.

- **working directory**

```
pwd
```

- Change directory

```
cd
```

- List Files

```
ls
```

- Move Files

```
mv
```

- Copy Files

```
cp
```

- Remove Files

```
rm
```

6 Resource Management

- **disk devices**

  ```
  fdisk -l
  ```

- **disk usage**

  ```
  df -h
  du -h
  ```

- **processes**

  processes bounds by controlling terminal

  ```
  ps
  ```

  view sistem processes

  ```
  ps aux
  ```

  show hierarchy

  ```
  ps -axjf
  ```

- **network interfaces**

  ```
  ip address
  ip a
  ```

- **open ports**

  display all TCP listening ports, displaying PID/program names and resolve names with IP address

  ```
  netstat -ltp
  ```

6.1 Example: fdisk output

```
$ sudo fdisk -l backup.img

Disk backup.img: 31.9 GB, 31914983424 bytes, 62333952 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
```

```
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x00009590

              Device Boot      Start         End      Blocks   Id  System
backup.img1            8192     2496093     1243951    e  W95 FAT16 (LBA)
backup.img2         2496094    62333951    29918929    5  Extended
backup.img5         2498560     2564093       32767   83  Linux
backup.img6         2564096     2699263       67584    c  W95 FAT32 (LBA)
backup.img7         2703360    62333951    29815296   83  Linux
```

7 User Management

- Create new user with defaul settings

```
sudo useradd -m <USERNAME>
```

- Change user password

```
sudo passwd <USERNAME>
```

- Delete user

```
sudo userdel -r <USERNAME>
```

- List groups of a given user

```
groups <USERNAME>
```

- Create new group

```
groupadd <GROUPNAME>
```

- Add user to group

```
usermod -a -G <GROUPNAME> <USERNAME>
```

Two foundamental files related to user management are

- `/etc/passwd`, contains useful metadata for users.

```
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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
```

```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
sshuser:x:999:0::/home/sshuser:/bin/bash
```

- /etc/passwd, contains hashed passwords of users.

```
root:*:19842:0:99999:7:::
daemon:*:19842:0:99999:7:::
bin:*:19842:0:99999:7:::
sys:*:19842:0:99999:7:::
sync:*:19842:0:99999:7:::
games:*:19842:0:99999:7:::
man:*:19842:0:99999:7:::
lp:*:19842:0:99999:7:::
mail:*:19842:0:99999:7:::
news:*:19842:0:99999:7:::
uucp:*:19842:0:99999:7:::
proxy:*:19842:0:99999:7:::
www-data:*:19842:0:99999:7:::
backup:*:19842:0:99999:7:::
list:*:19842:0:99999:7:::
irc:*:19842:0:99999:7:::
_apt:*:19842:0:99999:7:::
nobody:*:19842:0:99999:7:::
ubuntu:!:19842:0:99999:7:::
systemd-network:!*:19869::::::
systemd-timesync:!*:19869::::::
messagebus:!:19869::::::
systemd-resolve:!*:19869::::::
sshd:!:19869::::::
sshuser:$y$j9T$OeC1gyHTe5zm5WKfFyzIN/$Ka2yBHIvDV6km05stxfMM.51OTzJdcu0NLIW5QxCQ43:19869::::::
```

8 Packages Management

In order to manage sytem packages we can use `apt` or `apt-get`.

- Install

  ```
  apt-get install fdisk
  ```

- Search

  ```
  apt search disk
  ```

- Remove

  ```
  apt-get purge fdisk
  ```

- Update

  Download package lists from upstream repositories and updates metadata.

  ```
  apt-get update
  ```

- Upgrade

  Fetch new versions of packages.

  ```
  apt-get upgrade
  ```

9 Refs

- https://kevroletin.github.io/terminal/2021/12/11/how-terminal-works-in.html
- https://www.linusakesson.net/programming/tty/