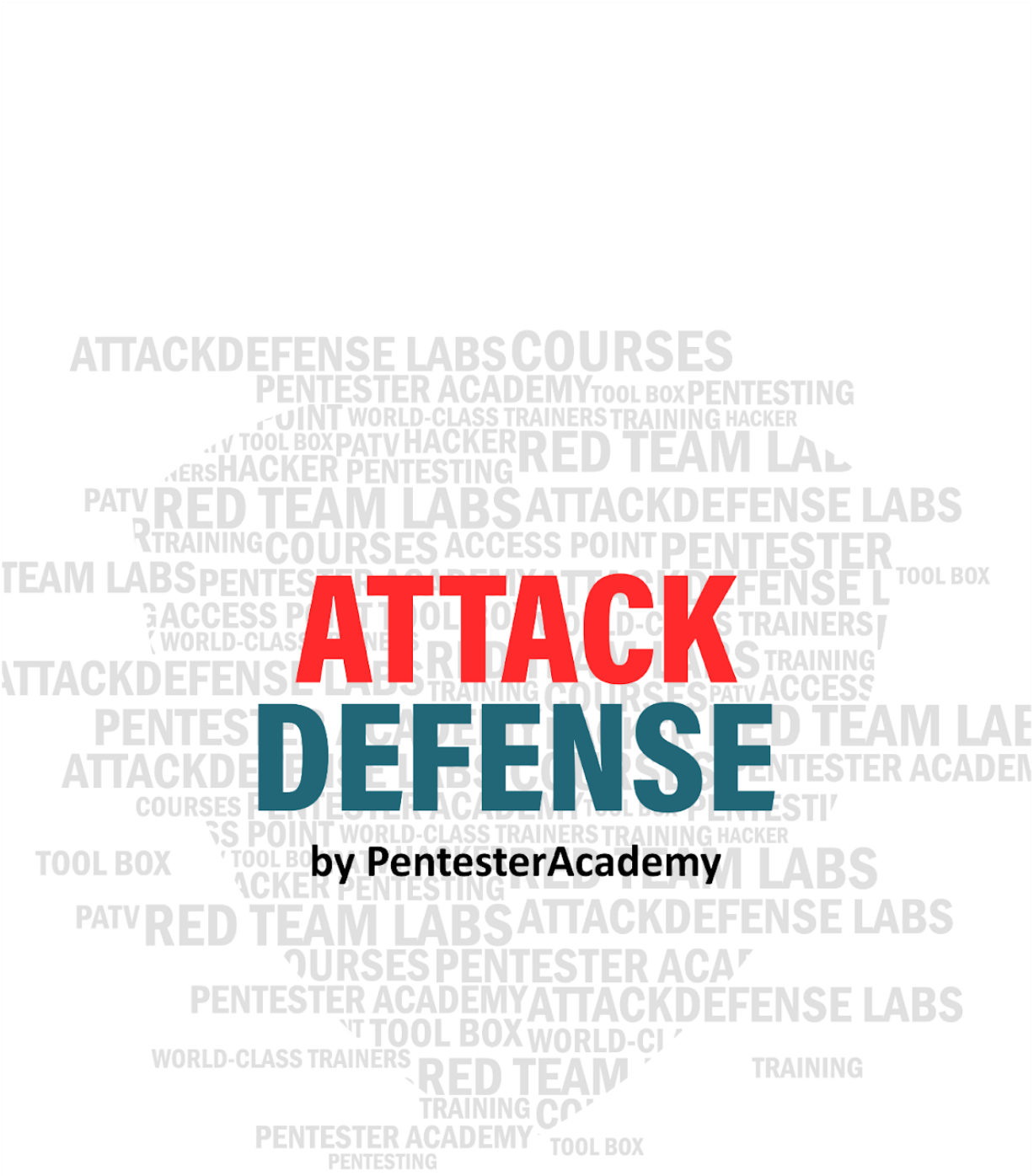
ATTACK
DEFENSE
by PentesterAcademy

Name	Mounting Disk Image (Python)
URL	https://www.attackdefense.com/challengedetails?cid=1800
Type	Forensics: Disk Forensics

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.

Image mounting involves mounting the evidence disk image on the local system so the data on the disk can be analysed and inspected.

In this lab, an evidence hard disk image is present on an external disk mounted on '/dev/sdc'. The mount-disk.py python script is present in /bin directory of the lab machine. Also, a flag file is kept in the /root directory of the disk image filesystem.

Objective: Mount the evidence disk image using mount-disk.py script and retrieve the flag!

Solution:

Step 1: Verify that the external hard drive is mounted.

Command: df -h

```
root@localhost:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       2.0G  1.6G  211M  89% /
devtmpfs        1.5G     0  1.5G   0% /dev
tmpfs           1.5G     0  1.5G   0% /dev/shm
tmpfs           1.5G  448K  1.5G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.5G     0  1.5G   0% /sys/fs/cgroup
/dev/sdb        976M  2.6M  907M   1% /root
/dev/sdc        240M  105M  120M  47% /mnt/evidence
tmpfs           300M     0  300M   0% /run/user/0
root@localhost:~#
```

The external disk is mounted at /mnt/evidence directory.

Step 2: Change to the external disk, list the contents and copy the evidence disk image to the /root directory for analysis.

Commands:
cd /mnt/evidence
ls
cp evidence.img /root

```
root@localhost:~# cd /mnt/evidence/
root@localhost:/mnt/evidence# ls
evidence.img  lost+found
root@localhost:/mnt/evidence# cp evidence.img /root
root@localhost:/mnt/evidence#
```

Step 3: Change to the /root directory and check the file type of copied evidence disk image.

Commands:
cd /root
ls
file evidence.img

```
root@localhost:/mnt/evidence# cd /root
root@localhost:~# ls
evidence.img
root@localhost:~# file evidence.img
evidence.img: DOS/MBR boot sector; partition 1 : ID=0x1, start-CHS (0x1,0,1), end-CHS (0x65,63,32), startsect
or 2048, 206848 sectors, extended partition table (last)
root@localhost:~#
```

Step 4: Use the 'mount-disk.py' python script to mount the disk image.

Note: The mount python script is already copied to the /bin directory.

Command: mount-disk.py evidence.img

```
root@localhost:~# mount-disk.py evidence.img
Looks like a MBR or VBR
Must be a MBR
Type 1:Start 2048:Total sectors 206848
<empty>
<empty>
<empty>
root@localhost:~#
```

The script has detected a partition at 2048 sector and the script has mounted the image in the media directory.

Step 5: Change to the media directory.

Commands:
cd /media
ls -lha

```
root@localhost:~# cd /media
root@localhost:/media# ls -lha
total 24K
drwxr-xr-x  3 root root 4.0K Feb 13 05:53 .
drwxr-xr-x 22 root root 4.0K Nov 12 01:14 ..
drwxr-xr-x 21 root root  16K Jan  1  1970 part0
root@localhost:/media#
```

The image is mounted inside the part0 directory.

Step 6: Retrieve the flag stored in the /root directory.

Commands:
cd part0/root/
ls
cat flag.txt

```
root@localhost:/media# cd part0/root/
root@localhost:/media/part0/root# ls
flag.txt
root@localhost:/media/part0/root# cat flag.txt
56d9076a6a54a622b84570d94d9473a0
root@localhost:/media/part0/root#
```

Flag: 56d9076a6a54a622b84570d94d9473a0