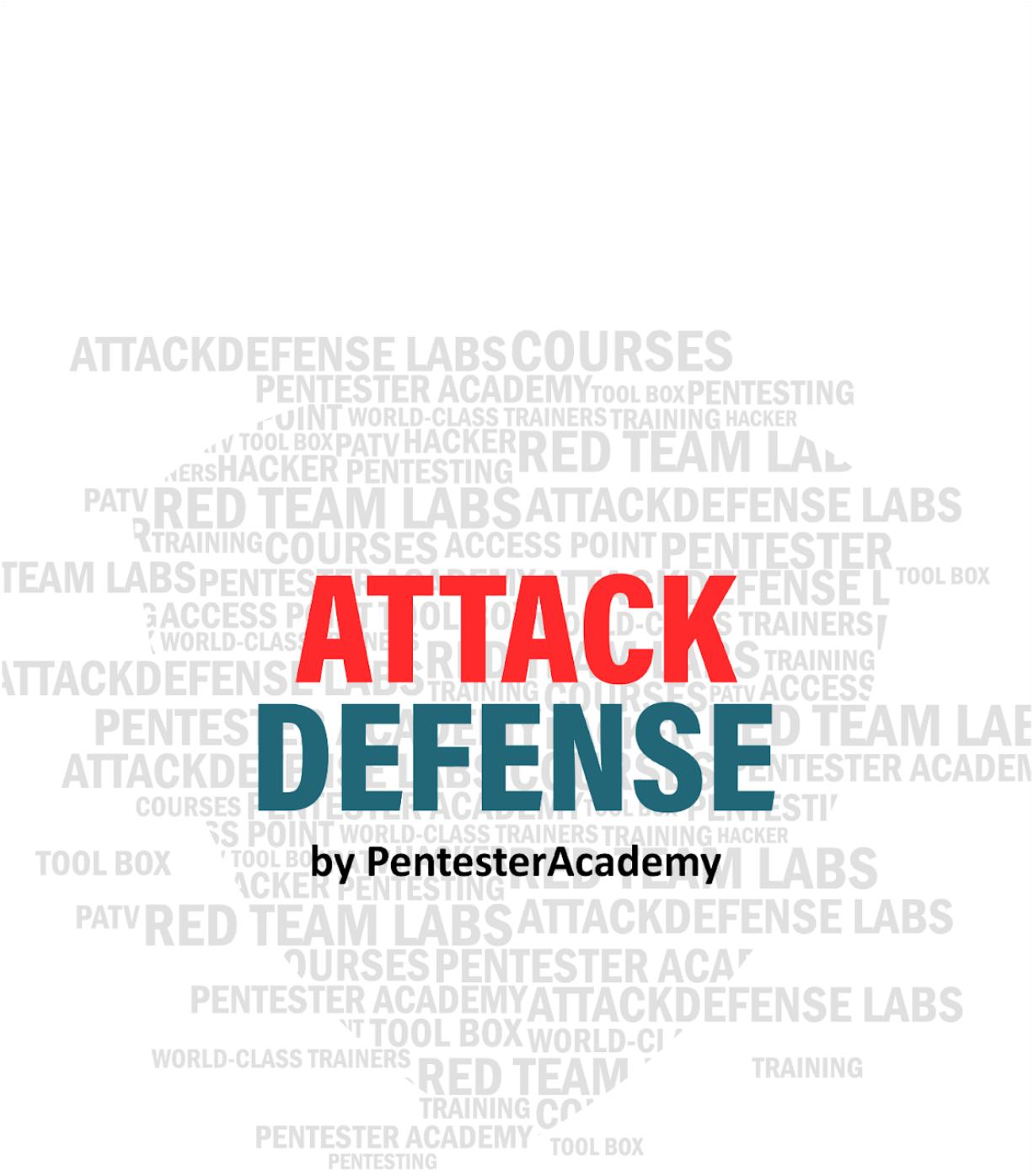
ATTACK
DEFENSE
by PentesterAcademy

Name	Mounting Disk Image (Raw mount)
URL	https://www.attackdefense.com/challengedetails?cid=1799
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 dd tools are installed on the lab machine. Also, a flag file is kept in the /root directory of the disk image filesystem.

Objective: Mount the evidence disk image 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: Create a directory to mount the evidence disk image. Mount it using the 'mount' utility. Then check its content.

Commands:
mkdir output
mount evidence.img output

```
root@localhost:~# mkdir output
root@localhost:~# mount evidence.img output
mount: /root/output: wrong fs type, bad option, bad superblock on /dev/loop0, missing codepage or helper prog
ram, or other error.
root@localhost:~#
```

The mount failed due as the offset of the filesystem is different than that of the disk image.

Step 5: Use the 'fdisk' utility to find the correct offset for this disk image.

Command: fdisk -l evidence.img

```
root@localhost:~# fdisk -l evidence.img
Disk evidence.img: 102 MiB, 106954752 bytes, 208896 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0014c70f

Device         Boot Start    End Sectors  Size Id Type
evidence.img1        2048 208895  206848  101M  1 FAT12
root@localhost:~#
```

The filesystem starts at 2048 sector.

Step 6: Mount the image while passing read-only and offset as arguments.

Note: The mount utility will take the offset value in bytes. As each sector is 512 bytes long so the total will be 2048 x 512 bytes.

Command: mount evidence.img output -o ro,offset=$((2048*512))

```
root@localhost:~# mount evidence.img output -o ro,offset=$((2048*512))
root@localhost:~# ls output/
bin   dev  home  lib64       media  opt   root  sbin  sys  usr
boot  etc  lib   lost+found  mnt    proc  run   srv   tmp
root@localhost:~#
```

The image was mounted successfully.

Step 7: Retrieve the flag stored in the /root directory.

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

```
root@localhost:~# cd output/root/
root@localhost:~/output/root# ls
flag.txt
root@localhost:~/output/root# cat flag.txt
56d9076a6a54a622b84570d94d9473a0
root@localhost:~/output/root#
```

Flag: 56d9076a6a54a622b84570d94d9473a0