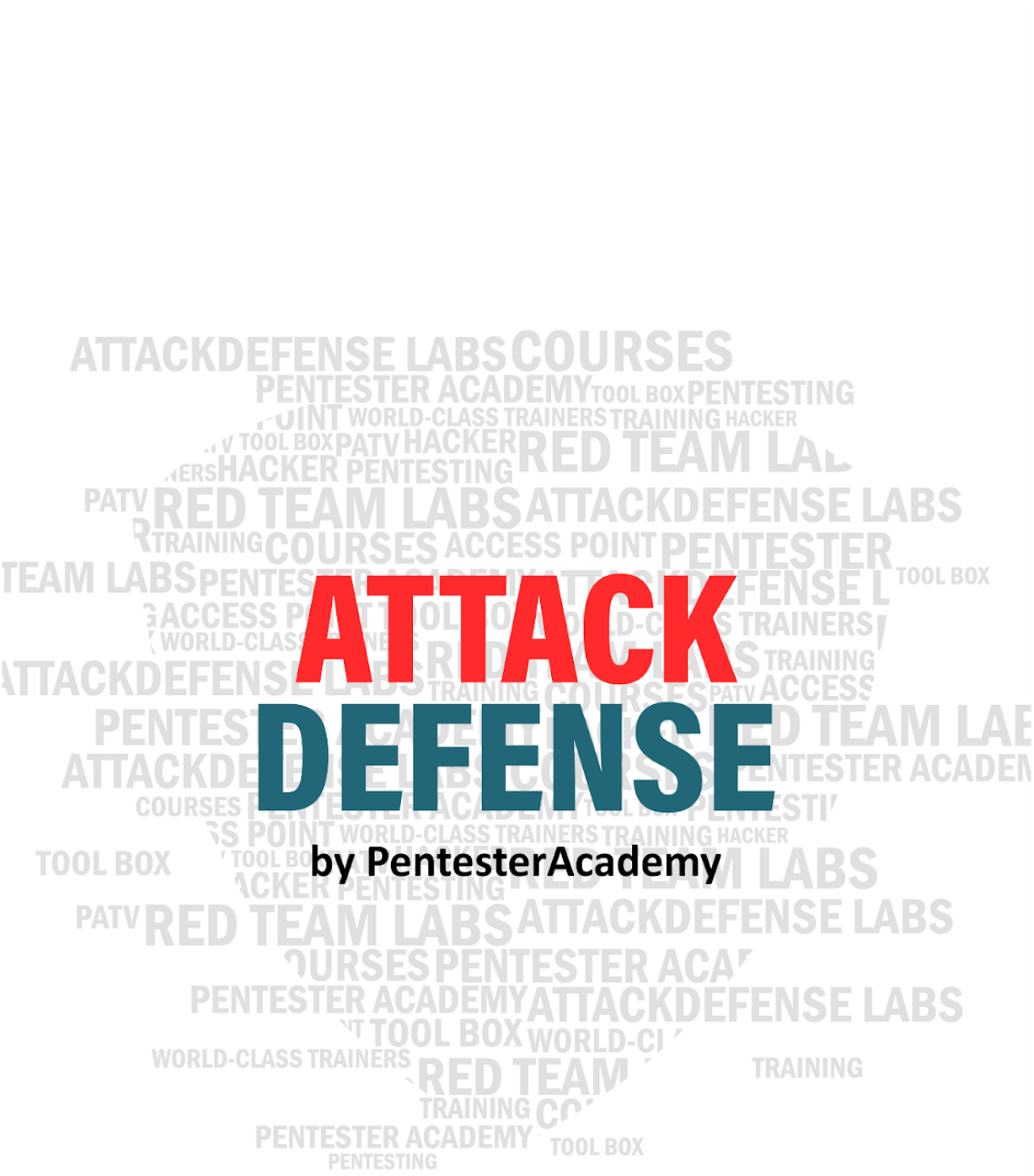
ATTACK
DEFENSE
by PentesterAcademy

| Name | File Carving (Scalpel) |
|---|---|
| URL | https://www.attackdefense.com/challengedetails?cid=1792 |
| 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.

In this lab, a disk image file “evidence.img” is provided in the home directory of the root user (/root/). One of the PDF files present on the disk contains the flag.

**Objective:** Extract files from the given image using Scalpel and retrieve the flag!

**Solution:**

**Step 1:** Use the scalpel tool to process the disk image and extract the stored files.

**Command:** scalpel evidence.img -o output

```
root@attackdefense:~# scalpel evidence.img -o output
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/evidence.img"

ERROR: The configuration file didn't specify any file types to carve.
(If you're using the default configuration file, you'll have to
uncomment some of the file types.)

See /etc/scalpel/scalpel.conf.
root@attackdefense:~#
```

The configuration file (i.e. /etc/scalpel/scalpel.conf) should contain the extensions of the files which the user wants to carve.

**Step 2:** Modify the configuration file and allow PDF extension for carving by uncommenting the pdf extensions.

```
#
#-----------------------------------------------------------------------
# ADOBE PDF
#-----------------------------------------------------------------------
#
        pdf     y       5000000 %PDF    %EOF\x0d    REVERSE
        pdf     y       5000000 %PDF    %EOF\x0a    REVERSE
#
#-----------------------------------------------------------------------
```

**Step 3:** Delete the already created empty “output” directory and run the scalpel tool again.

**Commands:**
rm -rf output
scalpel evidence.img -o output

```
root@attackdefense:~# rm -rf output/
root@attackdefense:~# scalpel evidence.img -o output
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/evidence.img"

Image file pass 1/2.
evidence.img: 100.0% |*****************************************************************************************| 1023.0 MB
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 1 files
Carving files from image.
Image file pass 2/2.
evidence.img: 100.0% |*****************************************************************************************| 1023.0 MB
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 1, elapsed = 3 seconds.
root@attackdefense:~#
```

The carved images are stored in the ‘output’ directory.

**Step 4:** Navigate to the output directory and inspect the carved files.

**Commands:**
cd output
ls -lha

```
root@attackdefense:~# cd output/
root@attackdefense:~/output# ls -lha
total 16K
drwxr-xr-- 3 root root 4.0K Feb 11 09:44 .
drwx------ 1 root root 4.0K Feb 11 09:44 ..
-rw-r--r-- 1 root root  394 Feb 11 09:44 audit.txt
drwxr-xr-x 2 root root 4.0K Feb 11 09:44 pdf-1-0
root@attackdefense:~/output#
```

**Step 5:** Change to pdf-1-0 directory and list the contents. Convert the PDF file to text format and retrieve the flag.

**Commands:**
cd pdf-1-0/
ls
pdftotext 00000000.pdf output
cat output

```
root@attackdefense:~/output# cd pdf-1-0/
root@attackdefense:~/output/pdf-1-0# ls
00000000.pdf
root@attackdefense:~/output/pdf-1-0# pdftotext 00000000.pdf output
root@attackdefense:~/output/pdf-1-0# cat output
ff8a95f5989fe663b4d8c4d82d32c2d0


root@attackdefense:~/output/pdf-1-0#
```

**Flag:** ff8a95f5989fe663b4d8c4d82d32c2d0

**References:**

1. Scalpel (https://github.com/sleuthkit/scalpel)