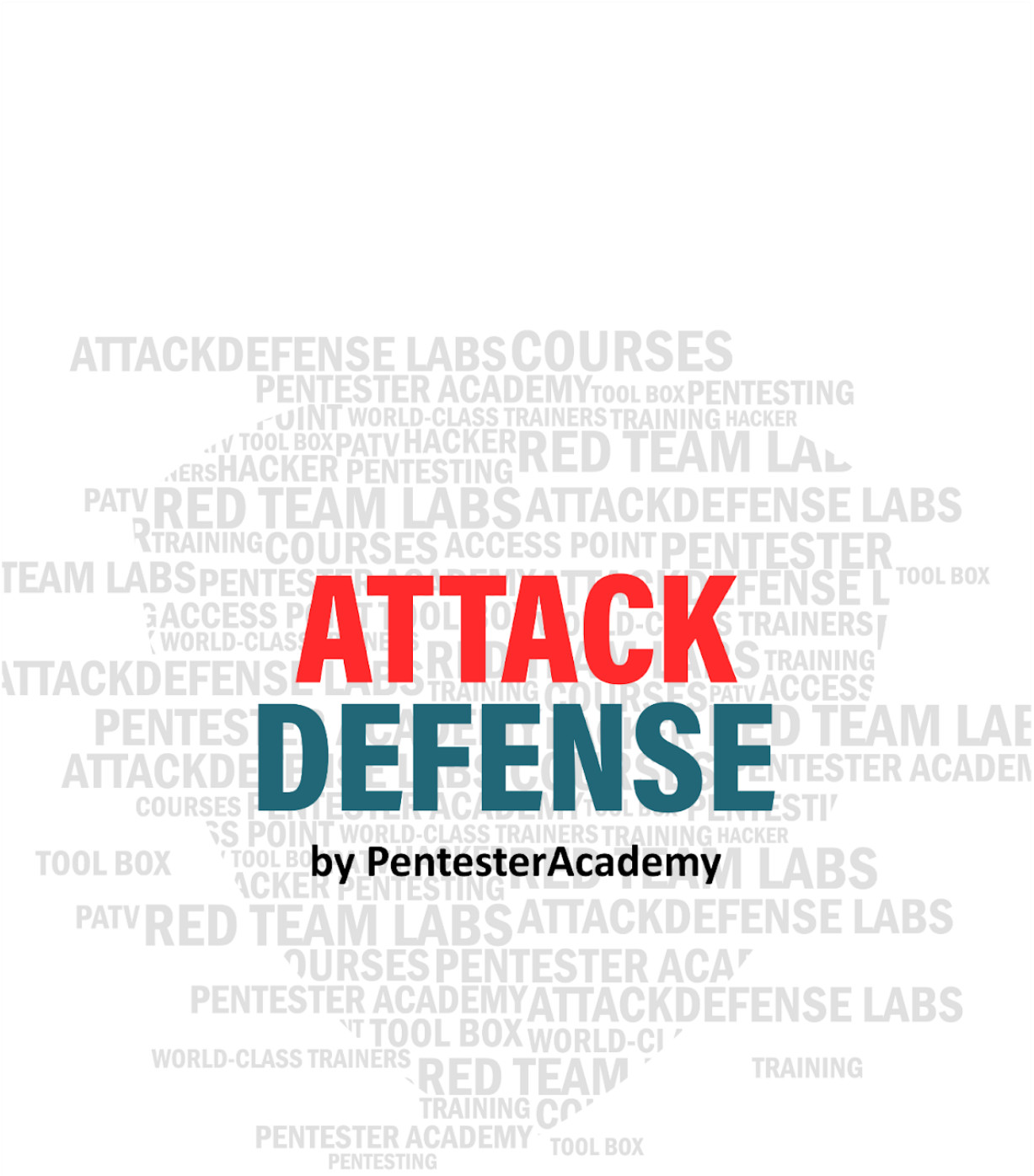
ATTACK
DEFENSE
by PentesterAcademy

Name	Bulk File Extraction
URL	https://www.attackdefense.com/challengedetails?cid=1793
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/). There is a file on this image which contains the email and phone number of “evil” user. The email of the user is “evil@attacker.co.uk” and the phone number is the flag for this lab.

Objective: Extract the files from the disk image using the bulk extractor tool and retrieve the flag!

Solution:

Step 1: Use the bulk extractor to extract the files from the given disk image.

Command: bulk_extractor evidence.img -o output

```
root@attackdefense:~# bulk_extractor evidence.img -o output
bulk_extractor version: 1.6.0
Hostname: attackdefense.com
Input file: evidence.img
Output directory: output
Disk Size: 1072693248
Threads: 16
Attempt to open evidence.img
11:51:06 Offset 67MB (6.26%) Done in  0:00:12 at 11:51:18
11:51:08 Offset 150MB (14.08%) Done in  0:00:19 at 11:51:27
11:51:11 Offset 234MB (21.90%) Done in  0:00:20 at 11:51:31
11:51:13 Offset 318MB (29.72%) Done in  0:00:18 at 11:51:31
```

```
11:51:16 Offset 402MB (37.54%) Done in  0:00:18 at 11:51:34
11:51:19 Offset 486MB (45.36%) Done in  0:00:17 at 11:51:36
11:51:22 Offset 570MB (53.18%) Done in  0:00:15 at 11:51:37
11:51:25 Offset 654MB (61.00%) Done in  0:00:13 at 11:51:38
11:51:28 Offset 738MB (68.82%) Done in  0:00:10 at 11:51:38
11:51:32 Offset 822MB (76.64%) Done in  0:00:08 at 11:51:40
11:51:36 Offset 905MB (84.46%) Done in  0:00:05 at 11:51:41
11:51:39 Offset 989MB (92.28%) Done in  0:00:02 at 11:51:41
All data are read; waiting for threads to finish...
```

Note: The process will take some time.

```
All Threads Finished!
Producer time spent waiting: 0 sec.
Average consumer time spent waiting: 22.8731 sec.
*****************************************
** bulk_extractor is probably I/O bound. **
**        Run with a faster drive        **
**      to get better performance.       **
*****************************************
MD5 of Disk Image: afd06ad98f9f8a08c113a2edb9c1360f
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 57.8216 sec.
Total MB processed: 1072
Overall performance: 18.5518 MBytes/sec (1.15948 MBytes/sec/thread)
Total email features found: 92
root@attackdefense:~#
```

Step 2: Navigate to the output folder.

Command: cd output

```
root@attackdefense:~/output# ls
aes_keys.txt              email_domain_histogram.txt  httplogs.txt        rar.txt
alerts.txt                email_histogram.txt         ip_histogram.txt    report.xml
ccn_histogram.txt         email.txt                   ip.txt              rfc822.txt
ccn_track2_histogram.txt  ether_histogram.txt         jpeg_carved.txt     sin.txt
ccn_track2.txt            ether.txt                   json.txt            sqlite_carved.txt
ccn.txt                   exif.txt                    kml.txt             telephone_histogram.txt
domain_histogram.txt      find_histogram.txt          ntfsusn_carved.txt  telephone.txt
domain.txt                find.txt                    pii_teamviewer.txt  unrar_carved.txt
elf.txt                   gps.txt                     pii.txt             unzip_carved.txt
root@attackdefense:~/output#
```

Step 3: Utilise the grep utility to find the information.

Command: grep -rnw "evil@attacker.co.uk" . --color

```
root@attackdefense:~/output#
root@attackdefense:~/output# grep -rnw "evil@attacker.co.uk" . --color
./email_histogram.txt:33:n=1    evil@attacker.co.uk
./email.txt:52:134750238        evil@attacker.co.uk     Et Av.\x0D\x0AMr evil,evil@attacker.co.uk,+912999949811,"
./domain.txt:52:134750243       attacker.co.uk  .\x0D\x0AMr evil,evil@attacker.co.uk,+912999949811,"
root@attackdefense:~/output#
```

This reveals the flag to us.

Flag: +912999949811

References:

1. Bulk Extractor (https://github.com/simsong/bulk_extractor)