Chapter 3

Digital Evidence Controls

Common Obstacles for Collecting Evidence by User

Computer users have an easy way to make investigations slower and more difficult. The following are just a few techniques used by criminals to evade discovery:

1. Changing the default location of the history files
2. Moving or renaming the history file or folder
3. Hiding and/or protecting history files with file system attributes and permissions
4. Deleting history files
5. Formatting the entire hard drive in an attempt to destroy evidence
6. Encrypting the entire volume
7. Not keeping history by disabling all logging (if supported by an application)

To Overcome previous uncovering attack by criminal to evade in collecting computer evidence the following point must be taken into consideration.

1. Understanding Password Cracking:

Passwords are very easy to be cracked by the hacker , and hacker can use that password to imitate the genuine user. The passwords can be cracked in the following ways:

a) Use of brute force.
b) Recover and exploit the password stored on the system
c) Make use of password decryption software.
d) Social engineering.

A)Brute Force

This methods is time consuming for cracker in search of a password to system but sometimes it may be effective whenever strong password policies are not applied. A brute force attacker attempts one possible passwords until he does not hits right passwords. This kinds of password cracking can be done using a program that scans all the words in a dictionary file's large lists and characters arrangements. If crackers know the passwords words arrangements , then according to this he may manipulate program execution so that he easily wash out evidence from computer systems. This password recovery program can be use in ethical hacking also whenever authorized persons not avialable.

B) Exploitation of Stored Passwords

If user stored the list of passwords information in somewhere in computer about various login in banks account, websites, email accounts etc. but this stored file not properly encrypted the cracker can easily crack this file and misuse it in wash out the evidence. So stored password must be properly encoded and hashed.

C) Interception of Passwords

Sometimes it is hard to crack the password file into computer system, so cracker can intercept the file in the form of network compatible during communication over the networks with help of network protocol. Hence use of non-secure authentication protocol like password authentication protocol during transmission

Send the plain text typed password then it can be evaded when possible.To avoid misuse of interception of password or illegal packets sniffer on communication path , we can use a time domain reflectometer (TDR) device over a cable to note down the illegal devices are attached to the cable by plotting graph of the reflections by detecting pulse rate of cable .

d) Password Decryption Software

Whenever password is protected in compacted files likes .zip,.rar and .arj files and send after encryption over any communicating medium then it may be decrypt the files to hack password if encryption algorithm is implemented inaccurately. The skilled cracker may use one-byte patching methods to alter

One byte in the package and database. When robust cryptography is used and compound code words are chosen , it is much more difficult to use basic and direct decryption.

e) Social Engineering

To crack password in this case , persons does not have technical expertise into any kind of software or programming algorithm. This types of attack use weakness of human user like carelessness or desire to be supportive to obtain access to genuine network of any organization. This kinds of talent are use by stalker to impress anybody by his attractive and influential personality and authoritative, commanding natures.

Using such kind of social engineering , intruders win the user and administrative trust or find out their weakness and knows authenticates user information and illegally handle all networks and misuse the information.

Preventive and Response measures to protect Password

1. Follow guidelines for generating strong passwords.
2. Configure settings so that user accounts are deactivated or locked out after a sensible numbers of incorrect password attempt.
3. Use EFS on Windows 2000/XP/.NET computers to encode files
4. Store critical data on network servers instead of storing it on local machines.
5. Do not rely on the password protection built into most applications.
6. Permit password shadowing on Unix/Linux Systems

7. Deactivate LAN Managers Authentication on Windows networks

8. Confirms that passwords are never sent across the networks in plain text format.

9. Use anti sniffer software and sniffer detection technique to protect against hackers who try to capture password traveling across the network.

Protecting the Network against Social Engineers

To protect against social engineering attacks , the administrative must imposed strong policy on forbidding exposing password and any other network information to anyone over any communicating medias.

The social invader is master in making users distrust their own doubts about his legitimacy with anyone so that organization top administrators implements strong rule to make relationship with anyone apart from official work in or outside organization.

Forensic Duplication :- *A Forensic duplicate contains the same digital data as the original piece of evidence.*

It is a document file containing every bit of information obtained from the source in a raw bit stream format. This files does not contain any extra data other than error message while reading the content from the original. After duplication process , forensic duplicate can be compressed.

Bit stream copy:- A bit by bit copy or duplicate of a piece of digital evidence from the original storage medium that permits examination of fragmentary or hidden data that cannot be reached by a computer's operating system is also known as "acquiring an image" or "making an image."

Rules of Forensic Duplication (Thumb Rule)

1. Make two copies of the original media(digital evidence)

a) One copy becomes the working copy on which investigation will be done.

b) One copy is a library / control copy for future reference.

c) Verify the integrity of the copies.

2. The working copy is used for the analysis.

3.The library copy is stored for disclosure purpose or in the event that the working copy becomes corrupted.

4.If performing a drive to drive imaging use clean media to copy.

5. Verify the integrity of all images using hash values.

In short we can say that 5 GB of drive results in 5 GB of forensic data. No extra data is stored within a file , except in the case where errors occurred in a read operation from the original.

The working from a duplicate images provides following features,

a) Preserves the original digital evidence.
b) Prevents inadvertent alteration of original digital evidence during examination.
c) Allow recreation of the duplicate image if necessary.
d) Digital evidence can be duplicated with no degradation from copy to copy.

Restored image : Restoration of a forensic duplicate or qualified forensic duplicate to another storage media results in restored image. The partition tables are updated with the new values , as the forensic duplicate is restored to the destination hard drive.

Restored image may involve some modification in the original image. To create a qualified forensic duplicate , tools like SafeBack,EnCase,or dd can be used.

Mirror Image : A Hardware that does a bit – to – bit copy from one HDD to another is used to generate a mirror image. Generating mirror image presents extra step in forensic investigation process.

We can easily make working copies if your organization has the capability to keep the original drive detained from computer system being examined. The analyst will be obligatory to generate a working copy of the mirror image for study if the original is returned.

Hardware copiers like Logicube's forensic SF-5000 and intellectual computer answers image MASSter Solo-2 professional plus.

Forensic Duplication Tool Requirements:

It satisfy the following criteria

1. The tool shall make a bitstream duplicate or an image of an original disk or partition.
2. The tool shall not alter the original disk
3. The tool will be able to verify the integrity of a disk image file.
4. The tool shall log I/O errors.
5. The tool's documentation shall be correct.
6. The tool should create a mirror image or forensic duplicate of the original storage media.
7. The tool must be able to handle read errors.
8. The tool should not make any changes to the source medium.

9. The tool must have the capability to be held up to scientific review . Results must be verifiable by the third party.

10. If there are no errors accessing the source, then the tool shall create a bitstream duplicate or image of the source.

11. If there are I/O errors accessing the source , then the tool shall create a qualified bitstream dplicate or image of the source.

12. The tool shall log I/O errors in an accessible and readable form, including the type of errors and location of errors.

13.The tool shall be able to access disk drives through one or more well-defined interfaces.

14. The tools working procedures should be correctly documented so that it should be matched with expected result.
15. It also keep information of copied data over larger destination area.
16. Whenever destination is smaller that source documents in terms of memory then it will be notified to source regarding copy or transfer action.

Forensic duplication tools are

a.SafeBack(www.forensic-intl.com)
b. Ghost(www.symantec.com)
c.DD(Standard UNIX/Linux utility)
d.Encase(www.encase.com)
e.Mareware f.FTK(www.accessdata.com)
g.ProDiscover Basic

Memory Image Acquisition Technique

Volatile memory, or Random Access Memory (RAM), contains a wealth of information regarding the current state of a device. Memory forensics techniques examine RAM to extract information such as passwords, encryption keys, network activity, open files and the set of processes and threads currently running within an operating system. This information can help investigators reconstruct the events surrounding criminal use of technology or computer security incidents. Since then, investigators and researchers alike have begun to recognize the important role that memory forensics can play in a robust investigation.

Techniques used to extract volatile memory images from target systems are defined as either hardware-based or software-based solutions. Software-based solutions rely on the operating system in order to perform memory capture. Hardware-based solutions in contrast, directly access the volatile memory of the target system. To date, hardware-based solutions for memory acquisition have been considered the most reliable as it is difficult to obtain a complete and accurate memory snapshot from software.

There are two types of Memory Acquisition Technique

a) Availability

b) Atomicity

A) The availability criteria stipulates that the technique must work on arbitrary computers and/or devices — essentially meaning that the method be operating system agnostic and not require specialised techniques. The availability factor stating that a technique that is characterized by a high availability does not make any assumptions about particular pre-incident preparatory measures and can be applied without knowledge of the execution environment and without requiring that any pre-configurations exist prior to its execution.

B)The atomicity of a technique reflects the demand to produce an accurate and complete image of a host's volatile storage, which encompasses the fidelity and reliability requirements

Limitations:

The acquisition OS approach involves far more complexity than existing software based approaches as it involves snatching control of the host entirely away from the existing host OS. This requires an entire new OS in order to operate the host hardware.The most prominent problem with the prototype lies in its highly constrained nature

Newer IO devices which use DMA require additional changes to the acquisition OS kernel in order to work with the quarantined memory scheme in use. We have avoided IO devices such as network and disk for reasons of simplicity (due to the plethora of network drivers) and integrity of host storage.