4 Live Data Collection

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand live data collection on Microsoft Windows Systems.
- Understand live data collection on Unix-based Systems.
- Understand the importance of data collection.
- Interpret and apply various tools for data collection.
- Distinguish different methods for collection in the Windows and UNIX system.

Understand what data you hold, how you are using it, and make sure that you are practising good data hygiene.

—David Mount

4.1 Introduction

In Chapter 2, we discussed the basic definition, types, and rules of digital evidences. Now, the first question that comes to our minds is: "How are these digital evidences collected?" Therefore, in this chapter, we discuss the facts or evidences that will be used to create the case file to take actions against an offender.

As we know, digital evidence is "Information of value to a criminal case that is stored or transmitted in digital form." The term "computer forensic" involves identification, sunder out, preparation of documents, and storing information that is kept or sent over in electronic or magnetic form basically considered as digital evidence. For example, in fingerprints, digital evidence is visible as the files are stored on disk that can be easily accessible by standard file management tools (like Windows Explorer), or can be hidden using special method or a software. The main purpose of computer forensic is to find these hidden evidences in order to increase facts value.

Different standards have been created which are used to find out and preserve digital evidences There are a number of the procedures accepted by law. Those are:

1. If evidence is not collected and handled according to the proper standards, the judge may deem the evidence inadmissible when it is presented and the jury members will never get a chance to evaluate it or consider it in making their decision.
2. If the proof is admitted, the opposing lawyer can attack its quality by questioning the witnesses.

Such an attack will produce doubt in jury members' minds causing them to disregard the proof in creating their decision—and maybe even taint the quality of the whole case.

Scanned by CamScanner

4.2 The Facts in a Criminal Case

Legal process of searching, examining, preserving, and exhibiting facts or evidence is generally governed by the law of authority of the court. This process will introduce an evidence. As an investigator, a person should first become familiar with the applicable laws. These rules are collected in a document called "rules of evidence."

The rules of a federal court can be different from the rules of a state court. Before introducing evidence in court, it is important to find out the existence of that evidence. Although the detailed description has already been discussed in Chapter 3, we repeat the definition of evidence for the sake of convenience.

4.2.1 Definition of Evidence

Evidence can generally be defined as the means by which an alleged fact, the truth of which is subjected to scrutiny, is established or disproved. The legal significance of any given piece of evidence lies in its influence on the judge or jury at trial.

—Debra Little John Shinder

4.2.2 Evidence Admissibility

There are certain requirements for evidence to be admissible or acceptable by court:

1. Evidence should be competent.
2. Evidence should be relevant.
3. Evidence should be material.
4. Evidence should be obtained legally.

Standards of Forensic Examination

Surpassing the minimum requirements of admissibility is always safest. If extra precautions are taken by investigators, it will not only decrease the possibility of evidence being rejected by a judge, but it will also help in getting an impression by jury.

Some organizations provide standard forensic governing examination methods or procedures for their members.

Standards regarding some digital evidence handling are:

1. The originality of the evidence should be preserved.
2. There should be an exact copy of the original, if possible, in order to maintain integrity of the evidence.
3. The copies should be preserved on a disk with no other documents available on the disk. That is, disk should be cleaned before placing copies in it.

4.2.3 Collection of Digital Evidences

The first person to become aware of a cybercrime is always a network administrator. If the company has an IT incident response team, then this team will stop the crime progress immediately and freeze it before any law enforcement authorities take over.

There are several people involved in the process of collecting digital evidences—the first respondent (usually an officer or a security person, who reaches the crime scene first), the investigators, and the crime scene specialists and technicians; there is also someone 'in-charge' of the crime scene able to take proper decisions. This is usually the senior investigator. It is also important that the members of the organization should cooperate in the process of investigation.

Scanned by CamScanner

Every member of the investigators team should be aware of his/her role and should cooperate. Integrity in investigation team members is also an essential part in order to collect evidences successfully.

4.3 People Involved in Data Collection Techniques

Only a specialist in computer forensic should touch the system; care has to be taken to protect the computers from alteration and damage. The criminals, who plant Trojan horses or something similar, usually make their systems ready in such a way that all the evidences automatically get destroyed after rebooting or shutting down the systems by anyone except themselves.

There are several people involved in evidence collection techniques—first respondent (usually an officer or a security person), investigators (usually a senior investigator), and the crime scene technicians (usually a person who is an expert in computer forensic). These people have been assigned with specific roles.

4.3.1 *Role of First Respondent*

The first respondent is the one who appears in crime locations, usually an officer or a security person. As shutting down or rebooting the system may destroy some important information or even evidence, the first respondent should not power off or restart the system, nor should he access the system to seek the evidence.

He/she should follow the following process:

1. **Identifying the crime location:** The person (usually an officer), who arrives first at the crime scene, should be able to identify depth of the crime and restrict access to the crime location. This location can be as wide as a room, or can consist of several rooms, or even multiple buildings. Constructing a list of computer systems that might have been involved in the crime scene is one of the tasks a first respondent should be able to do.
2. **Protecting the crime scene:** All the devices, including nonfunctional computers, mobile phones, notebooks, PDAs, or other portable devices, are considered a part of the crime scene. First respondent should freeze the condition of all the devices and wait for the IT incident response team or investigator in-charge to decide if any equipment can be excluded.
3. **Preserving temporary and tampered evidences:** An evidence that could disappear or destroyed before the arrival of investigation team should be preserved and maintained by the first respondent. If there is surveillance (CCTV) available, then it is easier to have a record of the crime. But if there is no surveillance, then identifying crime scene is a challenge for investigators.

4.3.2 *Role of Investigators*

IT incident response team has authority of collecting evidences before any law enforcement team arrives. To handle all the activities at the location of crime is generally the responsibility of an investigator. He/she will be responsible for:

1. **A Chain of order:** An investigator should make sure that everyone at the crime scene is aware of the chain of order. Chain of order refers to the flow investigation process. All the systems and other equipment at the crime scene should not be touched, replaced, accessed, or unplugged without the permission of a senior investigator. The role of investigator is to control and manage the investigation.

   In case a senior investigator has to leave the location of crime, he/she should assign a person with similar designation to stay in contact with that person until all the facts and evidences has been collected and shifted to a secure storage area.

Scanned by CamScanner

2. **Conducting the crime scene search:** Officers should seek all the systems, written documents and notes, manuals, and log files related to the crime. It involves mobile phones, printers, scanners, external devices such as flash drives, hard disks, CD/DVD, tapes, and more.
3. **Preserving integrity of the facts or evidences:** Criminals always remove all the evidences. This is the reason to preserve all the evidences in order to take actions against the offender. Investigation should make exact copy of all the evidences, if possible and should be able to analyze the footprints of attacker/criminal.

4.3.3 Role of Crime Scene Technicians

They are the specialists or experts in computer forensic. They must have a background in the field of computer and its technology with all the computer-related terms like working of file systems, structure of disks, and location of files where data is stored.

Usually, crime scene experts are responsible for:

1. **Preserving temporal evidences to replicating disks:** Temporal data is sometimes known as volatile data located in the computer's memory such as random-access memory. The disk containing evidences should be replicated or copied before shutting down the system, as there might be the possibility of disappearance of evidence after shutting down or rebooting the system.
2. **Shutting down the computer system for transport:** To preserve the integrity of original evidence, shutting down the systems properly is important. All the running programs or applications should be properly closed in order to avoid corruption of files.

   One school of thought says after making sure that there is no fragmentation or disk checking programs is running, power off the system and also unplug the power cable to prevent running of self-destruct programs programmed to run after shut down.

   But in UNIX system should not be shut down in an abrupt manner because it may damage the data files. Some experts in forensic suggest to change the account by "`su`" command or use "`sync; halt`" command to power off the system; but this can only be done if the root password of the system is available.
3. **Marking and recording the evidence:** All the evidences should be noted or marked with time and date of evidence collected, initials of the investigator, case identification number, and other related information. All these tagged or noted evidences should be recorded in evidence log files.
4. **Packaging of the evidence:** All the digital evidences such as hand held, computer, laptops, PDAs, hard disks should be properly packed in antistatic bags for transport.

   Written documents, such as notes, manuals, and books, should be placed in plastic bags in order to protect them from damage.
5. **Transporting evidence:** All the data should be securely transported to a secure evidence locker or room. The evidence should not come directly in contact with magnetic fields during transport nor left in direct contact with sunlight or any other place where temperature increases to 75° F.
6. **Processing the evidence:** The disc image can be reconstructed when the copy of the disk is brought back to the lab. Special tools are used to analyze the data.

4.4 Live Data Collection

Primary step of any digital investigation is to collect information and then deciding the initial response strategy. The steps vary in accordance with the type of incident. For example, there is different response strategy to check whether employee is stealing data present on a share data server. You need to determine the depth of circumstances prior to responding to the target system.

Scanned by CamScanner

There are two ways of initial response: Ensure there is an incident, and after that, obtain system's temporal data that will disappear if you power off the system. The investigator should be able to perform the initial response using very less operation and time and should be authorized to take forensic duplication of the crime scene systems.

4.4.1 Live Data Collection from Windows System

Here, the first step is to determine whether the system was used by the victim or the attacker. We will discuss the preparations made prior to the incident and formation response tool kit.

After discussing tool kits, we will discuss how to collect temporal information so that it reduces the alteration of the system. Finally, we will make a decision about presenting a forensic replication of evidence.

4.4.2 Creating a Response Toolkit

We need to plan a policy to retrieve all the information without messing up with strong evidence. We have to be careful about not destroying or altering the evidence and to do this we need to create a response toolkit.

Do not belittle the significance of creating a response toolkit. There should be an experienced and trusted person to collect files and burn them into CDs. The toolkit should be in proper working condition. Testing toolkit for the first time in "live investigation" will be the biggest risk in the process of investigation.

1. **Collecting the tools:** It is critical to use trusted commands in all incident responses, irrespective of type of incident. An investigator should maintain a CD or a floppy that involves a minimum of the tools described in Table 4.1.

Table 4.1 Response Toolkit tools

Tool	*Description*	*Source*
cmd.exe	The command prompt for Windows NT and Windows 2000	Built in
PsLoggedOn	A utility that shows all users connected locally and remotely	www.foundstone.com
rasusers	A command that shows which users have remote access privileges on the target system	NT Resource Kit (NTRK)
netstat	A system tool that enumerates all listening ports and all current connections to those ports	Built in
Fport	A utility that enumerates all processes that opened and TCP/IP ports on a Windows NT/2000 system	www.foundstone.com
PsList	A utility that enumerates all running processes on the target system	www.foundstone.com
ListDLLs	A utility that lists all running processes, their command-line arguments, and the dynamically linked libraries (DLLs) on which each process depends	www.foundstone.com
nbstat	A system tool that lists the recent NetBIOS connections for approximately the last 10 minutes	Built in

(Continued)

Scanned by CamScanner

Table 4.1 (Continued)

Tool	*Description*	*Source*
Arp	A system tool that shows the MAC addresses of systems that the target system has been communicating with, within the last minute	Built in
Kill	A command that terminates a process	NTRK
md5sum	A utility that creates MD5 hashes for a given file	www.cygwin.com
rmtshare	A command that displays the shares accessible on a remote machine	NTRK
netcat	A utility used to create a communication channel between two different system	www.atstake.com/research/tools/network_utilities
cryptcat	A utility used to create an encrypted channel of communications	http://sourceforge.net/projects/cryptcat
PsLogList	A utility used to dump the contents of the event logs	www.foundstone.com
ipconfig	A system tool that displays interface configuration information	Built in
PsInfo	A utility that collects information about the local system built	www.foundstone.com
PsFile	A utility that shows files that are opened remotely	www.foundstone.com
PsService	A utility that shows information about current processes and threads	www.foundstone.com
auditpol	A utility used to display the current security audit settings	NTRK
doskey	A system tool that displays command history for open cmd.exe shell	Built in

There are two types of applications available in windows:

1. Based on GUI (Graphical User Interface)
2. Based on CUI (Control User Interface)

GUI involves pull-down menus and usually works in the background or "behind the scene" interactions. However, experts advised to avoid GUI for investigation. Table 4.1 contains Response Toolkit tools.

2. **Preparing the response toolkit:** We must assure that the toolkit will work exactly as intended and it should not alter the target system. There are several stages to prepare toolkit for initial response:
   (a) ***Tag a response toolkit media:*** Documenting the collection itself is the first step in evidence collection process. CD or floppies should be tagged, to identify that this is your part of investigation. The tag may contain information such as case identification number, time and date of the investigation, name of the investigator who created response media, and name of the investigator who used that response media.
   (b) ***Check the dependencies:*** It is necessary to identify which files the response tool is to depend on. Film can be used to determine all the files used and affected by each of the utility in the toolkit.

Scanned by CamScanner

There should not be a tool which will alter information of the target system, although knowing which tool changes the access time on files of the target system is beneficial.

(c) ***Creating checksum for the response toolkit:*** There is always a file which contains the checksum of all the commands. This file is usually a text file.

Figure 4.1 shows the md5sum commands used to generate the text file (named commandsums.txt).

```
F:\WINNT\System32\cmd.exe
E:\IRResponse>md5sum *.* > commandsums.txt

E:\IRResponse>type commandsums.txt
d2e269e42163363e45e5a2390a09beaa  AFind.exe
314d58ed93a4c22f84e740e61d305cde  ARP.EXE
4becb7753b7a3c9dd6b5ec827ef3e39a  CMD.EXE
5cf6dbd25e9fd49e9de1ed2497be7166  KILL.EXE
2c96269985ee63d8a590f9019663d749  LOGGEDON.EXE
ddfdb9bad8af665da194fbc655157dca  NBTSTAT.EXE
dfc527e6d77d321e0dfc2e40faef32eb  NC.EXE
e73c70de4bc211b5fbc5eb9cf69ca785  NET.EXE
d6221ae6aab3bb87a05dab726e1124ff  NETSTAT.EXE
272af92c8ca586105562c435049d9bef  NTLast.exe
e5945b08bb75f49d2a5957d5a0db0e94  PSAPI.DLL
b612005f2d2964308d78dfb7bea2882d  PSLIST.EXE
fa527efa4517f59612f8f01a7fac1fb0  SFind.exe
aeb4654e1cc1a6d97b39cec934f9892b  commandsums.txt
2da73b427585afea2e3e457b7c3157fb  cygwin1.dll
5078eff0d95ae3d935b2ebfdab082dcd  fport.exe
8da470b2e93697da0745dcd075bdc9d7  listdlls.exe
208ed5a29c4a58cb7a8c3fcc70be89bb  md5sum.exe
563b25aaf7b86b0df2d1f20b7b898fb7  pulist.exe

E:\IRResponse>
```

Figure 4.1 md5sum to create a checksum for the response toolkit.

3. **Preparing the response toolkit:** We assure that the toolkit will work exactly as intended and it should not alter the target system. There are several stages to prepare toolkit for initial response:
   (a) ***Tag a response toolkit media:*** Documenting the collection itself is the first step in evidence collection process. CD or floppies should be tagged, to identify that this is your part of investigation. The tag may contain information such as case identification number, time and date of the investigation, name of the investigator who created response media, and name of the investigator who used that response media.
   (b) ***Check the dependencies:*** It is necessary to identify which files the response tool is to depend on. Film can be used to determine all the files used and affected by each of the utility in the toolkit. There should not be a tool which will alter information of the target system, although knowing which tool changes the access time on files of the target system is beneficial.
   (c) ***Creating checksum for the response toolkit:*** There is always a file which contains the checksum of all the commands. This file is usually a text file.

4.4.3 Saving Information Collected During Initial Response

We can collect a lot of information from the live system at the time of initial response. Live term describes that the system used for investigation is significant, whether it is victim or the attacking system, and is powered on at this moment.

Scanned by CamScanner

There are four options available when the information has been retrieved from the live system:

1. The information obtained from the hard drive of the target system should be saved.
2. The obtained data should be noted by hand.
3. The data obtained from the floppy disks or other external devices should be saved.
4. The obtained data should be stored from forensic system by using cryptcat or netcat.

It is not advisable to save the data to the hard drives because it alters the system. Storing the data manually by hand is not possible as the volume of data could be larger. Use of floppy drives are out because the storage capacity of the floppy is less compared to recent storage devices which are compact in size such as removable USB drives. It is the best solution in the place of floppy drives.

The storage capabilities of these compact devices are fascinating. It provides the range of gigabytes having the capacity of storing toolkit as well as the collected data. These devices will work with any computer having USB ports. Experts suggest that one should obtain a few of these devices for the response toolkit. Even if these devices are good to store large amount of information related to an investigation, there is still a need of network to save the information. Netcat is a widely used tool to transfer the data from target system to remote forensic workstations.

Moving of Data Using Netcat

Netcat is a freely available tool that can be used to establish a communication channel between hosts. We can use this at the time of initial response to establish a TCP connection between the forensic workstations and the target system. Netcat is easy to use. To use Netcat, we need an IP address of the target system and sufficient storage capacity laptop to keep the information we have collected. Netcat helps to transfer all the significant system information and data that is required to confirm whether an event has occurred or not. There are two practices promoted by this technique:

1. It helps to quickly get on and off the target system.
2. It also provides offline feature of reviewing the information which was previously attained.

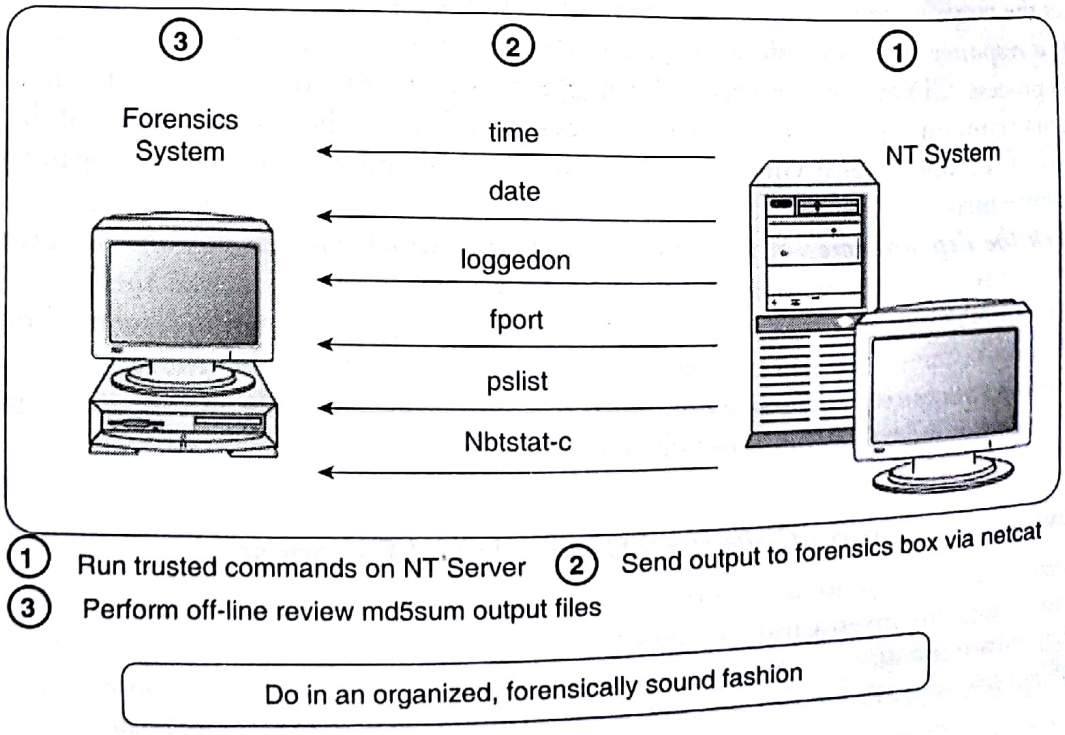

Figure 4.2 Use of Netcat at the time of initial response.

Scanned by CamScanner

We need to initialize a Netcat listener on the forensic work station. We also need to redirect all the incoming data. Figure 4.2 shows the incoming connection on port 2222. The file called pslist will contain all the information received on the port 2222. The output to the response command is provided to the forensic workstations by using Netcat on the target system. Figure 4.3 runs the command for pslist, by sending the output to the forensic workstation with the IP address 192.168.0.20.

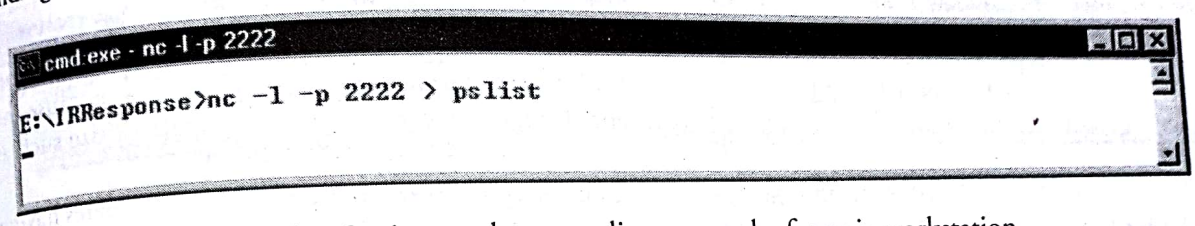

Figure 4.3 Setting up the netcat listener on the forensic workstation.

The Netcat is unaware of completion of data transfer while transferring the files in this manner. We need to disconnect the connection after the completion of data transfer by pressing CTRL-C on the forensic workstation. The stopping of the spine on target system or no growth of the file size will indicate that the data transfer is completed.

4.4.4 Obtaining Volatile Data

Exactly which data is to be collected is determined in this section. Here, we need to retrieve temporal data from windows NT/2000 system before powering off the system. We collect the following temporal/volatile data before forensic duplication:

1. The date and the time of the system.
2. List of users that are currently logged on.
3. Entire file system's time and date stamp.
4. List of processes that are currently running.
5. List of sockets that are open currently.
6. Applications that are listening on the open sockets.
7. List of systems that have current or had recent connections to the system.

If you are aware of the investigation that is improbable to require forensic duplication, you need to collect a lot of information. Here are some steps that are important to retrieve as soon as possible, because it may disappear on turning off the system and perform forensic replication.

4.4.5 Documenting and Managing the Investigation

For accurate incident response, it is necessary to have technical skills. Practices that are documented and organized are important. There are two main reasons for documenting the actions while responding to the victim system:

1. To protect an organization to which you belong.
2. To collect the data that may become evidence against the offender or criminal.

What if the server, from which the information has been received, crashes? A solution for this is—we have to note steps that we took on the system. We should have MD5 checksum file of each tool used, before starting to collect the information. We will also use binaries with their path name known to us.

Scanned by CamScanner

In the process of investigation, start time of command being executed and the command line entered should also be recorded. There should be a document about which binary we are using, trusted to untrusted. Then, we create MD5 sum of data retrieved by each command and significant comments are also added. An example of this form is illustrated in the following table:

Start Time	*Command Line*	*Trusted*	*Untrusted*	*MD5 Sum of Output*	*Comments*
12:15:22	type lmhosts | nc 192.168.0.1 2222	X		3d2e531d.6553ee93 e0890091.3857eef3	Contents of lmhosts file
12:15:27	pslist | nc 192.168.0.1 2222	X		1ded672ba8b2ebf5be ef672201003fe8	
12:15:32	netstat –an | nc 192.168.0.1 2222	X		52285a2311332453 efe202343857eef3	

Using this form will help us get information in the future references. This method helps in ensuring that the investigators plan ahead.

4.4.6 Collecting Temporal Data

After knowing what data should be collected and how to document the response, it is time to retrieve the temporal data. Following are the steps used for collecting the data:

1. **Run a Trusted cmd.exe:** As discussed earlier, investigators should be careful about the traps that have been implemented by an attacker, which will mislead the investigator to place wrong incident response.

   There might be a need to run cmd.exe on victim system, only to find that you actually del *.* in the \winnt\system32 directory, illustrating the system virtually inoperable.

   Running trusted version of cmd.exe from your own toolkit will be the best solution for this problem. To open trusted cmd.exe on floppy drive of Windows system, Figure 4.4 shows the run command.

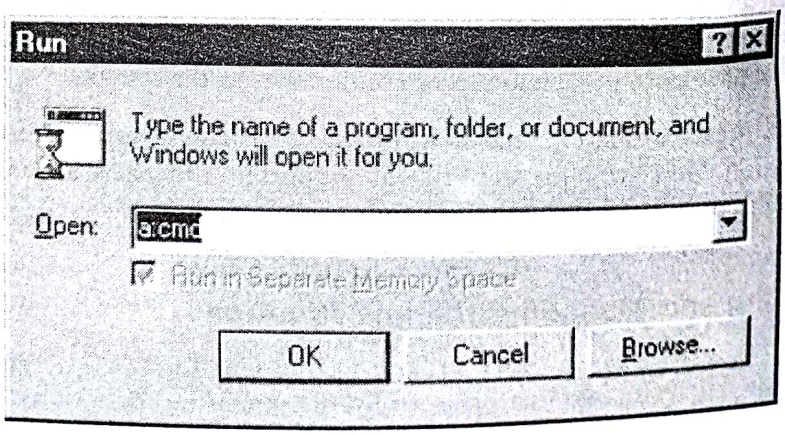

Figure 4.4 Running the trusted version of cmd.exe.

2. **Recording the system time and date:** After executing the trusted command shell, it is a good idea to capture the local system date and time settings. This is important to correlate the system logs, as well as to mark the times at which you performed your response. The time and date commands are a part of the cmd.exe application. Figure 4.5 illustrates the execution of the date command, redirecting the output to a file called date.txt on the floppy drive. The second command in the figure uses the append operator (>>) to add the output to the time command to the date.txt file.

Scanned by CamScanner

```
A:\cmd.exe
A:\>date > date.txt

A:\>time >> date.txt

A:\>type date.txt
The current date is: Fri 02/02/2001
Enter the new date: (mm-dd-yy) The current time is:  9:01:53.11
Enter the new time:
A:\>_
```

Figure 4.5 Obtaining the date and time of the system.

To indicate that you do not want to change the setting, press the "enter" key.

3. **Identify who has logged on to the system and who are the remote access users:** Identifying the active connections of the user accounts is the next step. As shown in Figure 4.6, Russinovich created a utility which provides the information about the local and remote users.

   It is necessary to identify which user accounts have remote access rights on the target system, in order to respond to a system that offers remote access via modem. You need to decide if you want to pull the telephone lines from the system at the time of response, if several accounts access systems via Remote Access Services (RAS).

```
A:\cmd.exe
A:\>loggedon

LoggedOn v1.1 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
     WEBTARGET\batman

No one is logged on via resource shares.

A:\>loggedon

LoggedOn v1.1 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
     WEBTARGET\batman

Users logged on via resource shares:
     (null)\doe
A:\>
```

Figure 4.6 Use of PsLoggedOn to list the users that are currently logged on to the system.

You may not want to allow any access to the target system while you are responding.

The commands to determine the number of the users who logged into the system (via RAS) is called rasusers.

Scanned by CamScanner

4. **Record creation, access time, and all the modifications made to the files:** To get the list of all the directory files on the target machine, "dir" command is used. It includes the size, access, and alteration and creation time. The time and date stamps become the evidence, if the significant information about the time frame when an event occurred is identified. Windows system performs the task of collecting time and date stamps very quickly.

   An example of using "`dir`" command to gain access, modification, and time of creation:

`dir/t:a/a/s/o:dc:\`	Provides a recursive directory listing of all the access times on the C: drive
`dir/t:w/a/s/o:dd:\`	Provides a recursive directory listing of all the modification times on the D: drive
`dir/t:c/a/s/o:de:\`	Provides a recursive directory listing of all the creation times on the E: drive

5. **Identifying open ports:** There are several networking commands available, out of which Netstat can be used to determine which ports are open. It also enlists all listening port and currents connections to those ports. Volatile data, such as recently terminated connections and current connections, can be recorded using Netstat. Figure 4.7 illustrates the execution of `Netstat` command on NT server machine. There are several local host connections in the output. The applications on the local host 127.0.0.1 will always be displayed by `Netstat` command.

```
A:\cmd.exe
A:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:465            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3970           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1026         127.0.0.1:1026         ESTABLISHED
  TCP    127.0.0.1:1027         127.0.0.1:1025         ESTABLISHED
  TCP    127.0.0.1:1027         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1029         127.0.0.1:1029         ESTABLISHED
  TCP    127.0.0.1:1030         127.0.0.1:1027         ESTABLISHED
  TCP    192.168.0.100:137      0.0.0.0:0              LISTENING
  TCP    192.168.0.100:138      0.0.0.0:0              LISTENING
  TCP    192.168.0.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.0.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.0.100:1152     192.168.0.20:1054      ESTABLISHED
  UDP    0.0.0.0:135            0.0.0.0:0              LISTENING
  UDP    192.168.0.100:137      192.168.0.20:139       ESTABLISHED
  UDP    192.168.0.100:138      *:*
                                *:*
A:\>_
```

Figure 4.7 View of `Netstat` command.

Scanned by CamScanner

6. **List of applications that are associated with those ports:** Knowing which services listen on which ports is helpful. A free tool fport is used to enlist listening ports for all the processes. Figure 4.8 shows the fport syntax and its corresponding output.

```
A:\cmd.exe
A:\>fport
FPort v1.31 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Securing the dot com world
Pid   Process          Port  Proto Path
2     System       ->  25    TCP
160   inetinfo     ->  25    TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
2     System       ->  80    TCP
160   inetinfo     ->  80    TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
79    RpcSs        ->  135   TCP   D:\WINNT\system32\RpcSs.exe
2     System       ->  135   TCP
2     System       ->  139   TCP
2     System       ->  443   TCP
160   inetinfo     ->  443   TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
2     System       ->  465   TCP
160   inetinfo     ->  465   TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
79    RpcSs        ->  1025  TCP   D:\WINNT\system32\RpcSs.exe
2     System       ->  1025  TCP
79    RpcSs        ->  1026  TCP   D:\WINNT\system32\RpcSs.exe
2     System       ->  1026  TCP
2     System       ->  1027  TCP
91    msdtc        ->  1027  TCP   D:\WINNT\System32\msdtc.exe
2     System       ->  1028  TCP
91    msdtc        ->  1028  TCP   D:\WINNT\System32\msdtc.exe
2     System       ->  1029  TCP
91    msdtc        ->  1029  TCP   D:\WINNT\System32\msdtc.exe
2     System       ->  1030  TCP
160   inetinfo     ->  1030  TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
2     System       ->  1031  TCP
160   inetinfo     ->  1031  TCP   D:\WINNT\System32\inetsrv\inetinfo.exe
2     System       ->  1151  TCP
2     System       ->  3970  TCP
160   inetinfo     ->  3970  TCP   D:\WINNT\System32\inetsrv\inetinfo.exe

79    RpcSs        ->  135   UDP   D:\WINNT\system32\RpcSs.exe
2     System       ->  135   UDP
2     System       ->  137   UDP
2     System       ->  138   UDP

A:\>
```

Figure 4.8 View of `fport` command.

7. **List of all running processes:** It is necessary to record all the processes that are currently executing on the system before turning off the target system. Unplugging the power cable will destroy this information. The executable code that resides in address space has been created when a process is created on the Windows system. To manage the process and maintain statistical information about the process, the kernel object is created by the operating system.
8. **List of current and recent connections:** To know who is connected or who has connected recently, the networking commands like `Netstat`, `ARP`, and `Nbstat` are useful. For many Windows system, these utilities might be the only way to determine a remote system connecting to workstation. Many experts refer `Netstat` command to enlist the ports that are opened on a system. As previously discussed, fport lists open ports and application listening to them, so also can Netstat be used to identify IP address of remote system and current connections of the systems. `ARP` networking command is used to map IP address to the MAC address. The utility named nbtstat is used to access the remote

Scanned by CamScanner

NetBIOS name cache, listing the recent NetBIOS connections for approximately the last 10 minutes. The example of NetBIOS is shown in Figure 4.9.

```
A:\cmd.exe
A:\>nbtstat -c
Node IpAddress: [192.168.0.100] Scope Id: []

                NetBIOS Remote Cache Name Table

    Name               Type         Host Address     Life [sec]
GENGIS          <00>  UNIQUE       192.168.0.20          60
GENGIS          <20>  UNIQUE       192.168.0.20         660

A:\>nbtstat -c
Node IpAddress: [192.168.0.100] Scope Id: []

                NetBIOS Remote Cache Name Table

    Name               Type         Host Address     Life [sec]
GENGIS          <20>  UNIQUE       192.168.0.20         600

A:\>
```

Figure 4.9 Using Nbtstat to view recent NetBIOS connections.

9. **Record date and time of target system:** Recording date and time of the target system ensures that you have a record of when you were logged on to that system. It can be used as an evidence, if anything changed on the system outside the timeframe you have recorded; you are not responsible for that alteration.
10. **Commands accessed at the time of initial response:** We can use doskey/history command to show the history of the commands that was currently accessed on the system. Figure 4.10 shows the use of doskey/history command.

```
A:\cmd.exe
A:\>doskey /history
date
time
pslist
netstat -an
ntlast
ntlast -f -r
fport
cls
doskey /history
```

Figure 4.10 Use of doskey to record the steps taken during initial response.

4.5 Live Data Collection from UNIX System

The initial response for incidents is similar for both—Windows system and UNIX system. The main goal of live data collection is to obtain temporal or volatile data before forensic duplication. The scope of initial response can be expanded by obtaining configuration files, system files, files that contain attacker's tools and suspicious programs, and log files to confirm quickly whether the event has occurred or not.

Scanned by CamScanner

Recovering deleted files in the UNIX system becomes a major difference in working with UNIX and Windows. In Windows, files that correspond to the running process from the hard drive cannot be deleted, whereas in UNIX, programs files can be deleted even if the process is running. In this section, we will see live data collection from UNIX system by recovering files before turning off the system, creating response toolkit, obtaining temporal data, and finally conducting live data.

4.5.1 Creating a Response Toolkit

It is difficult to create a trusted toolkit as it takes a lot time; the reason behind this is that every variable in UNIX requires a UNIX toolkit. In some cases, you may need to compile a source code on your own because some recommended tools are not included with the official UNIX system.

Before going further, many versions of UNIX system are not forward or backward compatible. For example, programs compiled on Solaris 2.7 system may not work properly on Solaris 2.6 and vice versa. These issues make your response toolkit time consuming. The number of resources is also increased because of this issue.

4.5.2 Saving Information Obtained at the Time of Initial Response

You must choose where to save information retrieved at the time of initial response. The storage options are:

1. Save the data on local hard drive.
2. Save the data on external devices such as USB or tape drives.
3. Record the information manually (i.e., by hand).
4. To transfer the retrieved data to the forensic workstations, use Netcat or cryptcat.

When possible, saving the data on local drives should be avoided. The information you save on the local hard drive will destroy the deleted data that was in a not allotted space; this may be of investigative value when data recovery or forensic analysis is required.

Newer versions of Linux support USB drive connections, and they are also useful for information collection by direct physical connection. But there is a solution for this limitation—use of Netcat to transfer the data over a network to forensic workstation. Use of Linux in forensic workstation provides a faster response. This helps to overcome the limitation of storage space. We use netcat to transfer the information across the network, and "pipe" the netcat stream through *des* to encrypt the transfer. The cryptcat command offers an encrypted TCP channel in a single step.

The best time to respond should be considered after selecting how to retrieve information from the target system. There should be a need for determining the network connectivity of the target system. After determining the network connectivity, you can now respond at the console of the target system.

4.5.3 Obtaining Volatile Data before Forensic Duplication

After collecting temporal data, you need to respond to the target system console rather than accessing it over a network. This reduces the possibility of the attacker stalking the response and also ensures that you are running a trusted command. You should focus on gathering the temporal data of the system before shutting down the system, if you are certain that you will be creating a forensic duplication of the target system.

Temporal data may involve running processes, system RAM's content, the location of files that are unlinked, and also the sockets that are currently open.

The files marked for deletion, when processes that access it are terminated, are called unlinked files. Marked files for deletion will vanish when the system is turned off. That is why the initial response should be created in such a way that it will recover each type of volatile evidence with the files that are marked for deletion.

Scanned by CamScanner

Collecting the data

The following information should be collected:

1. Date and time of the system.
2. A list of users who are currently logged on.
3. Entire file system's time and date stamps.
4. List of processes that are currently in running state.
5. List of currently open socket.
6. List of application that is listening to those open ports.
7. List of systems that have current or recent connections to the system.

For obtaining live data, following steps should be followed:

1. **Run a trusted shell:** One of the two scenarios you get when you respond to the target system running UNIX—the machine executing in console mode and the machine executing X Windows.

   X Windows should be closed before initiating a response, in order to avoid common X Windows-based vulnerabilities that allow the attacker to log keystrokes. You should be able to switch to another virtual console by pressing ALT (F2).

   To avoid generating network jamming, log on at the victim console with root-level privileges. You need to implement your trusted toolkit and respond with the trusted tools. This command—`mount/dev/fd0/mnt/floppy`—will mount the trusted toolkit on the mount point/mnt/floppy. You will be able to access the trusted files when you change the directory to/mnt/floppy.

   To be certain about execution of trusted command shell is the first step in all response. Attacker attacks the UNIX shell to log all the commands executed on the system or to perform criminal activities hidden to the investigator. This is the reason to run your trusted own shell. Bash shell can be used for this purpose. Set path environment variable equal to dot (.) after executing your trusted shell. The possibility of executing untrusted commands that are in the target system's PATH will be reduced.
2. **Record the time and date of the system:** Recording local time and date is necessary for future reference. It will also display when you were on the system. The following command can be used to capture this information:

```
[root@conan /root]# date
Tue Dec 17 16:12:43 UTC 2003
```

3. **Identify who is currently logged on to the system:** It is easy to identify who is logged on. We just need to execute the w command. The user IDs of logged on users, the system they logged on from, and what they are currently executing can be displayed by using this w command.

   Following shows the example of w command:

```
[root@conan /root]# w
 11:39pm up 3:11, 3 users, load average: 1.27, 1.43, 1.84
USER     TTY     FROM                LOGIN@   IDLE    JCPU    PCPU    WHAT
nada     ttyp0   jitter.rahul.net    8:30pm   3:02m   1:08    0.14s
telnet bothosti
bovine   ttyp1   shell1.bothostin    8:35pm   3:02m   1:01    0.12s   -bash
mandiak  ttyp2   adsl-225-75.poto    11:38pm  0.00s   0.25s   0.11s   w
root@conan /root]#
```

   The header line in the output shows the current time of the system, how long the system has been in the running state, number of users that are currently logged in, and the system load averages for the past 1, 5, or 15 minutes.

Scanned by CamScanner

4. **Record creation, alteration, and access time of each file:** You have to obtain all the time and date stamps on the file system. There are three time/date stamps available for each file in Windows and UNIX system—atime (i.e., access time), mtime (i.e., modification time), and ctime (i.e., inode change time). With the use of proper command line arguments to obtain these times for each file, you can use the trusted command `ls`. Following shows the demonstration of obtaining time/date stamps and saving the output on trusted floppy disk:

```
ls -alRu / > /floppy/atime
ls -alRc / > /floppy/ctime
ls -alR / > /floppy/mtime
```

R option in the `ls` command forces a recursive listing for which it takes some time. Sometimes you may be forced to use other media or cryptcat/Netcat because this data may not fit on 1.55 mb floppy drive.

5. **Identify open ports:** The most widely used command for listing open ports on a UNIX system is Netstat. Determining which applications are responsible for the open network sockets are difficult. To view all the open ports, use -an command. To tell the `Netstat` command not to resolve the host name, which reduces the impact on the system and speed up the execution of the command, -n option is used.

```
[root@conan /root]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address          State
tcp        0      176 66.192.0.66:22       66.192.0.26:20819
ESTABLISHED

tcp        0        0 0.0.0.0:80           0.0.0.0:*                LISTEN
tcp        0        0 0.0.0.0:21           0.0.0.0:*                LISTEN
tcp        0        0 0.0.0.0:22           0.0.0.0:*                LISTEN
udp        0        0 0.0.0.0:69           0.0.0.0:*
```

6. **Enlist applications associated with open ports:** -p option of `Netstat` command used to map the name of the application and its process identification number (i.e., PID) to the open ports.

```
[root@conan /root]# netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q    Local Address   Foreign Address   State
PID/Program name
1)  tcp    0      0 0.0.0.0:143   0.0.0.0:*    LISTEN    385/inetd
2)  tcp    0      0 0.0.0.0:22    0.0.0.0:*    LISTEN    395/sshd
3)  tcp    0      0 0.0.0.0:512   0.0.0.0:*    LISTEN    385/inetd
4)  tcp    0      0 0.0.0.0:513   0.0.0.0:*    LISTEN    385/inetd
5)  tcp    0      0 0.0.0.0:514   0.0.0.0:*    LISTEN    385/inetd
6)  tcp    0      0 0.0.0.0:23    0.0.0.0:*    LISTEN    385/inetd
7)  tcp    0      0 0.0.0.0:21    0.0.0.0:*    LISTEN    385/inetd
8)  udp    0      0 0.0.0.0:69    0.0.0.0:*              385/inetd
9)  raw    0      0 0.0.0.0:1     0.0.0.0:*              7
    -
10) raw    0      0 0.0.0.0:6     0.0.0.0:*              7
    -
```

Scanned by CamScanner

This output displays seven open TCP sockets and one open UDP socket. If you examine line 2, you can see that the secure shell daemon, sshd, with a PID of 395, is listening for connections on TCP port 22. Line 9 indicates a raw socket is listening for ICMP, and line 10 reveals that the kernel is also listening for TCP packets. Lines 1, 3, 4, 5, 6, and 7 show that the inetd, with a PID of 385, is listening on TCP ports 143, 512, 513, 514, 23, and 21. You now can discern which processes are responsible for opening the specific Internet ports.

7. **Identify the running processes:** Taking snapshots of ps command, the processes that are running during the initial response is difficult; but by using ps command we can achieve this. Output will be different on different UNIX flavors. The result of ps command is illustrated as follows:

```
[root@conan]# ps -aux
USER     PID  %CPU  %MEM  VSZ   RSS   TTY    STAT  START  TIME   COMMAND
root     1    0.1   0.7   1060  480   ?      S     17:52  0:03   init [3]
root     2    0.0   0.0   0     0     ?      SW    17:52  0:00   [kflushd]
root     3    0.0   0.0   0     0     ?      SW    17:52  0:00   [kupdate]
root     4    0.0   0.0   0     0     ?      SW    17:52  0:00   [kpiod]
root     5    0.0   0.0   0     0     ?      SW    17:52  0:00   [kswapd]
root     6    0.0   0.0   0     0     ?      SW<   17:52  0:00   [mdrecoveryd]
root     259  0.0   0.2   348   136   ?      S     17:52  0:00   /sbin/dhcpcd eth0
root     316  0.0   0.8   1112  556   ?      S     17:52  0:00   syslogd -m 0
root     326  0.0   1.1   1360  756   ?      S     17:52  0:00   klogd
daemon   341  0.0   0.7   1084  492   ?      S     17:52  0:00   /usr/sbin/atd
root     356  0.0   0.9   1272  608   ?      S     17:53  0:00   crond

root     385  0.0   0.7   1080  488   ?      S     17:53  0:00   inetd
root     395  0.0   1.5   2032  980   ?      S     17:53  0:00   /usr/sbin/sshd
xfs      422  0.0   5.0   4292  3172  ?      s     17:53  0:00   xfs -port -1 -dae
root     438  0.0   1.7   2188  1072  ttyl   s     17:53  0:00   login - root
root     439  0.0   0.6   1028  404   tty2   s     17:53  0:00   /sbin/mingetty tt
root     440  0.0   0.6   1028  404   tty3   s     17:53  0:00   /sbin/mingetty tt
root     441  0.0   0.6   1028  404   tty4   s     17:53  0:00   /sbin/mingetty tt
root     442  0.0   0.6   1028  404   tty5   s     17:53  0:00   /sbin/mingetty tt
root     443  0.0   0.6   1028  404   tty6   s     17:53  0:00   /sbin/mingetty tt
root     446  0.0   2.1   2108  1328  ttyl   s     17:55  0:00   -bash
root     499  0.0   0.7   1112  480   ttyl   s     18:41  0:00   script
root     500  0.5   0.8   1116  508   ttyl   s     18:41  0:00   script
root     501  1.7   2.0   2084  1292  pts/0  s     18:41  0:00   bash -I
root     513  0.0   1.5   2636  984   pts/0  R     18:42  0:00   ps -aux
```

From the snapshot, we can say that the UNIX system has more running processes than Windows servers. An attacker will take advantage of this to hide evil processes. When looking for such evil processes, a system admin should go through each of the hundreds of executing processes. The start field in ps command output is important, as it shows when a process has started. You can easily determine the suspect processes entirely by the time they are executed.

Scanned by CamScanner

8. **List the current and recent connections:** We have already discussed about the use of Netstat command. It provides the information about current and recent connections made to the system.
9. **Record the time of the system:** Date command can be used to record the current systems time. It will help to know the exact time frame when you altered or manipulated the system. It will help to know that any modifications made outside this time frame are not due to your investigation.
10. **Record the steps taken:** The commands that you have accessed should be recorded. Possibilities can be: use of script, history, or vi if live response is performed from the editor. As you have retrieved all the commands from the trusted shell, the use of history command will make a record of commands that have been executed. Still, experts recommend using script command which records the output and the keystrokes made by you. This command should be executed before performing live response.
11. **Record cryptographic checksum:** Md5sum can be used against all the files in data directory to record cryptographic checksum of all collected information:

```
[root@conan /root]# md5sum * > md5sums.txt
```

Storing Information Obtained During Initial Response

Most of the UNIX variants place their log files in /var/adm. To know where the logs are stored, you need to be familiar with each variants of the UNIX system. Now, we discuss how retrieval of log files is carried out. To retrieve the log files from the system, we can use several combinations of `Netcat`, `crypcat`, `dd`, `des` commands. You should acquire at least three binary log files and command ASCII text log file. Following shows the binary log files of particular interest:

1. Utmp file accessed with w command.
2. Wtmp file accessed with last utility.
3. Last log file accessed with last log utility.
4. Process accounting logs accessed with lastcomm utility.

Some ASCII text log files are as follows:

1. Xferlog
2. Web access logs
3. History files

Obtaining Important Configuration Files

The configuration files commonly accessed or modified by attackers are maintained by UNIX. To locate unauthorized user IDs and unauthorized trusted relationships of these configuration files are important to be reviewed. Here is the list about which file should be obtained during initial response:

1. To look for unauthorized user accounts: /etc/passwd.
2. To ensure about password authentication of every account: /etc/shadow.
3. To look for escalation in scope of access and privileges: /etc/groups.
4. To list the DNS (Domain Name System) entries: /etc/hosts.
5. To review trusted relationships: /etc/hosts.equiv.
6. To look in the start-up files: /etc/rc.
7. To list scheduled events: crontab files.

Dumping System RAM

There is no proper way to dump the system RAM on the UNIX system. We normally transfer /proc/kmem or /proc/kcore file from the target system. These files contain the files of system RAM in discontinuous manner. Core dump type of analysis can be done by very few people.

Scanned by CamScanner

Summary

Incident response (during early response) is a phase of initial information meeting to regulate whether or not illegal, unofficial, or intolerable activity occurred, and the information gathered during your initial response forms the basis for your level of response. During the initial response, it may be necessary to capture live data—volatile evidence—before it is lost through actions such as rebooting or shutting down a system. When live data collection is necessary, it is critical to adhere to sound forensic principles and alter the state of the system as little as possible. The information you obtain during the response may lead to administrative or legal proceedings.

Key Terms

- **Recovery certificate:** A method NTFS uses, so that a network administrator can recover encrypted files if the file's user/creator loses the private key encryption code.
- **Registry:** A Windows database containing information about hardware and software configurations, network connections, user preferences, setup information, and other critical information.
- **Sector:** A section on a track typically made up of 512 bytes.
- **Track density:** The space between tracks on a disk. The smaller the space between tracks, the more tracks on a disk. Older drives with wider track densities allowed the heads to wander.
- **Tracks:** Concentric circles on a disk platter where data is stored.
- **Trusted Computing Group (TCG):** A nonprofit organization that develops support standards for trusted computer access across multiple platforms.
- **Trusted Platform Module (TPM):** A microchip that stores encryption key data used to encrypt and decrypt drive data.
- **Inodes:** A key part of the Linux file system, these information nodes contain descriptive file or directory data such as UIDs, GIDs, modification times, access times, creation times, and file locations.
- **International Organization of Standardization (ISO):** An organization set up by the United Nations to ensure compatibility in a variety of fields, including engineering, electricity, and computers. The acronym ISO is the Greek word for "equal."
- **Leaf nodes:** The bottom-level nodes of the B*-tree that contain actual file data in the Macintosh file system.
- **Logical blocks:** In the Macintosh file system, a collection of data that cannot exceed 512 bytes.
- **Logical blocks:** These are assembled in allocation blocks to store files in a volume.
- **Logical EOF:** In the Macintosh file system, the number of bytes in a file containing data.
- **Master Directory Block (MDB):** On older Macintosh systems, the location where all volume information is stored. A copy of the MDB is kept in the next-to-last block on the volume. Called the Volume Information Block (VIB) in HFS+.

Review Questions

1. What are the different ways to organize and document an investigation?
2. How do you store information obtained during initial response in the UNIX system?
3. Explain response tool kit. How do you create response tool kit for Windows system?

Scanned by CamScanner