Chapter 4

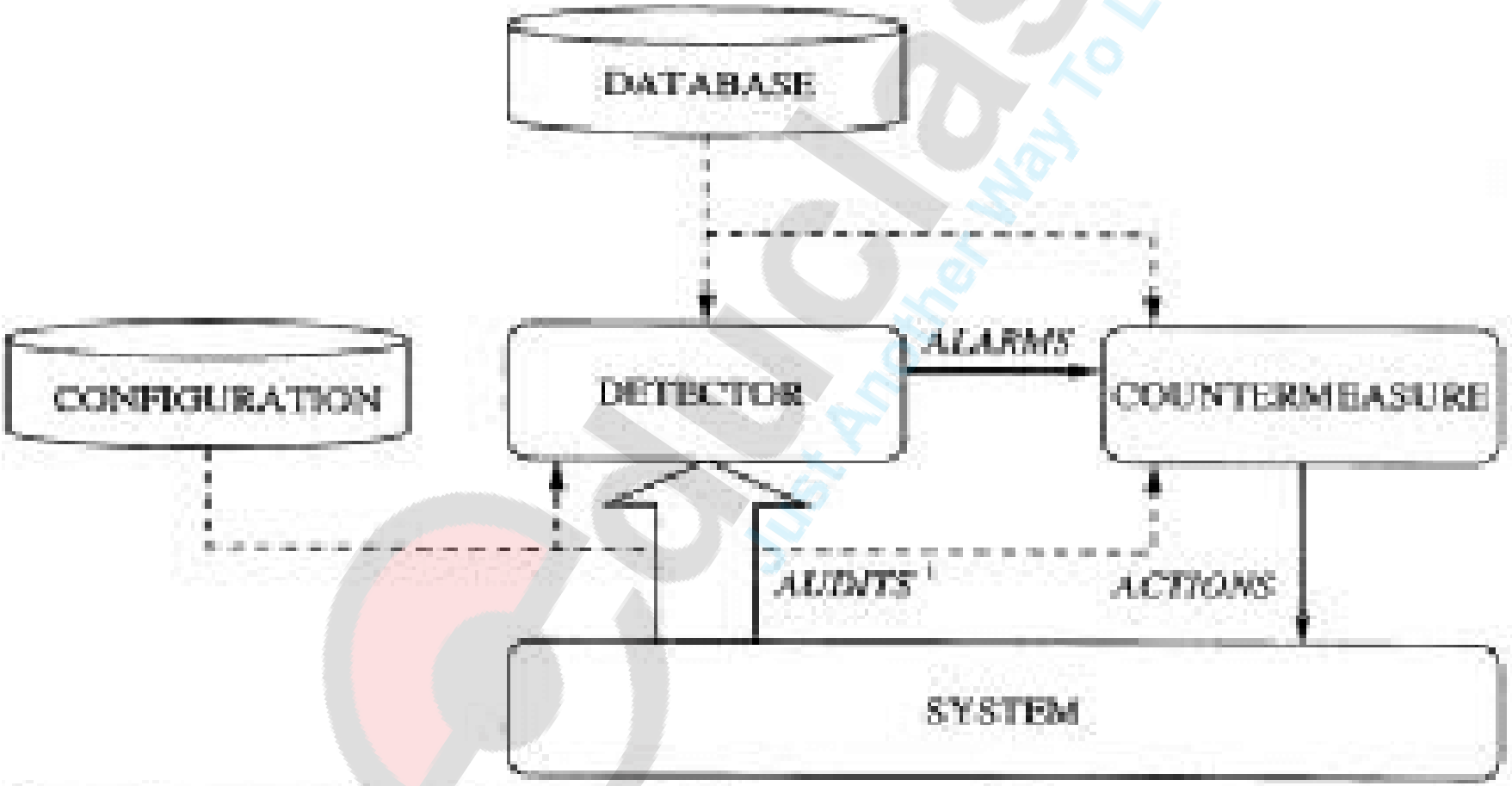
Network Forensic

Network Attack or Intrusion Detection System

The above term can be defined as malicious attacks designed to crash computers and congest networks, even when no actual illegal entry take place with little technical knowledge by cybercriminal.

The intrusion detecting system (IDS) help information systems prepare for and deal with attacks. They accomplish this by collecting information from a variety of systems and network sources and then analysing the information for possible security problems

Block Diagram of Intrusion Detection System



*The arrow lines represent the direction of information flowing from one component to the other.

Features of Intrusion Detection System (IDS)

1. Add a superior degree of integrity to the remainder of your infrastructure.
2. Recognize and report modification to knowledge
3. Trace user action from purpose of entry to purpose of impact.
4. Automate a task of observation means finding out the most recent attack accurately.
5. Notice mistakes in your system configuration.
6. Sense once your system is under fire.
7. Make flexible protection management system so that non expert employee can handle.
8. Issue guidelines to system supervisor to building a policy for your computing assets.

Demerits of IDS

1. It can conduct investigation of attacks but not human intervention.
2. Compensate for weak identification and authentication mechanisms.
3. Deal with a number of the trendy network hardware and options.
4. Compensate for flaws in network protocol.
5. Always alter complications involving packet level attacks.
6. Compensate for issues within the excellence or integrity of knowledge the system offers.
7. Analyze all the traffic on a busy network.

Different Types of Attacks in Digital Networks

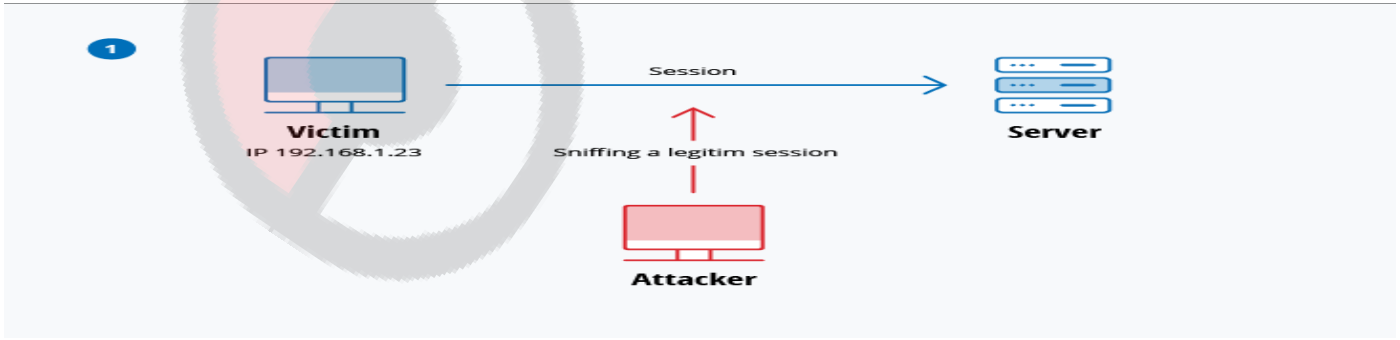
- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

2. Man-in-the-middle (MitM) attack

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.



An attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client. In this case following steps considered:

- A client connects to a server.
- The attacker's computer gains control of the client.
- The attacker's computer disconnects the client from the server.
- The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers.
- The attacker's computer continues dialog with the server and the server believes it is still communicating with the client.

3. Phishing and spear phishing attacks

Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something

Spear phishing is a very targeted type of phishing activity. A spear phishing attack is email spoofing, which is when the information in the “From” section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company

4. Drive-by attack

Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or

PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hacker.

5. Password attack

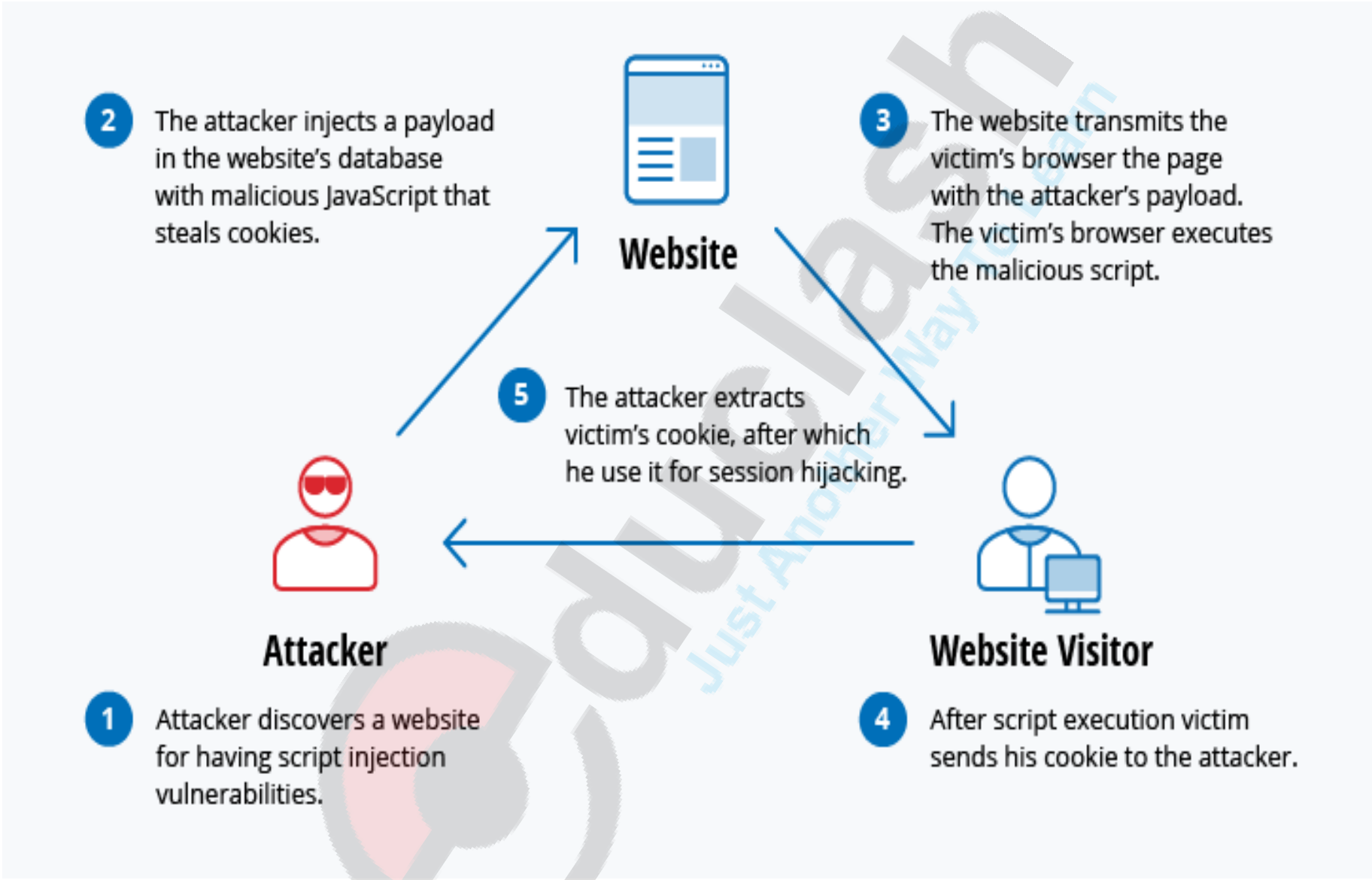
Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, "sniffing" the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing.

6. SQL injection attack

SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands

7. Cross-site scripting (XSS) attack

XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application.When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script.



8. Eavesdropping attack

Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. Eavesdropping can be passive or active:

Passive eavesdropping — A hacker detects the information by listening to the message transmission in the network.

Active eavesdropping — A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

9. Birthday attack

Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message

The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.

10. Malware attack

Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet.

This kinds of Malware attack also known as Automated attacks. The most of the tools would initiate only one attack sequence, launching complementary attack sequences which demand the interference of the human attacker. The internet protocol like HTTP and Internet Relay Chat(IRC) mask the packets by making them look as normal Internet traffic and hack pattern to recognition authenticated information.

11. Accidental Attacks

Sometimes unintentionally intrusions and attack are perform by inducing Trojan horse and worms into victims address book and sending infected e-mail to all the address found there.

The criminal code commonly refers to a default level of responsibility that applies , if no level of responsibility is specified.

Intrusions *Vs* Attacks

The attacker never gains access to any computer on the network, as these attacks overload network resources to make the network inaccessible to genuine users.

And in case of intrusions , the intruders gains access into systems and then abolish information or plant viruses.

Direct Vs Distributed Attacks

A Direct Attack is launched from a computer used by the attacker (often after pre-intrusion / attack tool , such as port scanners, are used to find potential victims)

The Distributed Attacks is more complex because of it include multiple victims and intermediary devices over network as well. In this attack , the attackers uses the some other individual system to target specific systems as well as intermediaries devices simultaneously using distributed methods.

Distributed Attack Process

Step	Component	Action
1	Daemon (Agent)	Announces itself to the “master” that have been predefined
2	Master	Lists daemon as “ready and willing” to be used for attack
3	Attacker	Issues command to masters to launch attack
4	Master	Issues command to daemons on agents to launch attack(with specific parameters such as identity of target and duration attack)
5	Daemon	Launches attack on specified victim.

To overcome such types of attack , arranging all system components into pyramid form. But sometimes attackers controls various other daemon or agents through this model.

Main advantages of this model is that it is easier to disable or deactivate the system attack which is nearer to the top of the pyramid.

If masters are deactivate , the agents and their guiding force software will not be able to function.

This model's components are arranged in pyramid form. So that master deactivated then all agents can not be access. If Master is attacks then attacker gain access to all agents into Model.

Preventing Intentional Internal Security Breaches

Security Breaches is an event that affects unauthorized access of data, application, services, network or devices by avoiding their core security mechanism.

The Internal attackers are more dangerous because

1. They can easily to gain access without reorganization because they all system structure and configuration very well.
2. They easily find out password and fleapits in the current security system.
3. Internal attacks knows about internal information and activities to manipulates secured contents.

To overcome over internal security breaches following points must be considered

1. Install totally diskless workstation or computer.
2. Apply system or group strategy that avoid users from installing software.
3. Lock PC case and cover physical access to serial ports, USB ports and other connection points so that removable media devices cannot be connected.

Preventing Unauthorized External Intrusions

Unauthorized intrusion can also be defined as attacks in which attacker gets access into the system by means of different hacking or cracking technique. This types of activity performed by some outsider to access system in order to use negative purpose.

Firewall Failures

Firewall system in the organization must be audit within proper time period so that it can be customize according to current scenarios. If this system is outdated , then intrusion can easily breach the system and damage more data.

External Intruders with Internal Access

External intruders who physically breaks into organization internal system and login as a internal user. For this kind of attack, security threat assessment must be based on technical aspects so that initially we can analysis motive behind attackers. In high security environment these task should be the responsibility of an incident team.

Recognizing the "Fact of the Attack"

The Network Administrator follows reactive mode if IDS system not working properly , try to minimize damages.

IDS use following two methods.

1. **Pattern recognition** : Investigating files, network traffic, series in RAM or other data for recurrent or identifiable marks of attack like mysterious increases in file size or particular characters strings.
2. **Effect recognition** : Recognition the results of an attack like system crash triggered by overload or unexpected reboot for no reasons. For this IDS fixed specific criteria to recognize attacks.

Identifying and Categorizing Attack Types

The following types of attacks,

1. Pre-intrusion / attack activities
2. Password – cracking methods
3. Technical exploits
4. Malicious code attacks

By analyzing above attack type , the administrator will equip with various measures

Digital Evidence Collection

The information of value to a criminal case that is stored or transmitted in a digital form is called as Digital Evidence.

The different standards have been created which are used to find out and preserve digital evidence are as follows:

1. If evidence is not collected and handled according to the proper standards, the judge or jury members will never evaluated in accordance with their understanding and marks it as inadmissible.
2. If the proof is admitted , the opposing lawyer can attack its quality by questioning the witnesses and produces doubt in jury members mind to create bad impact in decision making.

Evidence Admissibility

Legal process of searching ,examining , preserving and exhibiting facts or evidence is generally governed by the law of authority of the court or jurisdiction area.

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

1.Evidence should be competent.

2.Evidencce should be relevant.

3.Evidence should be material.

4.Evidence should be obtained legally.

Apart from above a) The originality of the evidence should be preserved .

b) There should be an exact copy of the original in order to maintain integrity of the evidence.

c) The copies should be preserved on a disk with no other documents available on the disk and disk should be cleaned before placing copies in it.

People involved in Data Collection Techniques

There are several people involved in evidence collection technique

1. First respondent (usually an officer or a security person)
2. Investigators (usually a senior investigator)
3. The crime scene technician (usually a person who is an expert in Computer forensic)

A) First Respondent

He is first person arrives at crime location hence he must follow following procedures.

i) Identifying the crime location: - He restrict the crime area to access anybody and make a list of digital equipment might have been involved in the

crime in all possible area of crime.

ii) Protecting the crime scene : The first respondent must freeze all digital devices use in crime and wait for IT incident response team or investigator in-charge to decide if any equipment can be excluded.

iii) 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.

B) Role of investigators

i) A chain of order : - It means flow of investigation process. All the system and order of equipment at the crime scene should not be touched,replaced,accessed or unplugged without permission of senior investigator

ii) Conducting the crime scene search:- Officers should seek all the system like hardware equipment's, written documents and notes, manuals and log files related to the crime.

iii) Preserving integrity of the facts or evidence : -

The investigator should take precaution whether criminal will remove all evidences. So that he make exact duplicate copies of all the evidence and fingerprints and footprints as well.

C) Role of Crime Scene Technicians

They are specialists in computer forensics like hardware configuration and different software file system and structures.

i) Preserving temporal evidences to replicate disks:- The disk containing evidences should be replicated

Or copied before shutting down the system because there might be possibilities that evidence should erase out from temporary computer memory.

ii) Shutting down the computer system for transport :
- To preserve the integrity of original evidences , the computer should be close down properly so that original file system should not be corrupted.

iii) Marking and recording the evidences : - All the evidences should be noted or mark with time and date of evidence collection, initial of the investigators ,case identification number in the recorded evidence log files.

iv) Packaging of the evidence : All digital devices use in evidence and papers should be packed in antistatic bags during transport.

v) Transporting and Processing the evidence :- All the data should be securely transported to a secure evidence locker or room or special tools to avoid damages.

Investigating Evidence in Windows Systems

Following steps involve in windows system for collecting evidences

a) Review all pertinent logs
b) Perform keyword searches
c) Review relevant files
d) Identify unauthorized user accounts or groups
e) Identify rogue process and services
f) Look for unusual or hidden files/directories
g) Check for illegal entry points
h) Inspect jobs run by the Scheduler service
i) Analyze trust relationship
j) Review security identifiers

Location of Evidences in Windows Systems

1) Volatile data in kernel structure
2) Slack space means from where we can recover deleted file information
3) Free or unallocated space after deleting files
4) The logical file system
5) The event logs
6) The registry which you should think of as enormous log file
7) Application logs not managed by the windows Event Log Services
8) The printer spool
9) Sent or received email such as the .pst files for Outlook mail.

A) Reviewing All Pertinent Logs

The System log, application log and security log are the three files that Windows NT , 2000 and XP operating system maintain. Using this files following information will be review

i) Determine which users have been accessing specific files
ii) Determine who has been successfully logging on to a system
iii) Determine who has been trying unsuccessfully to log on to a system
iv) Track usage of specific application
v) Track alterations to the audit policy
vi) Track changes to user permission

System log records System process and device driver activates. Windows includes device drivers that fail to start properly, hardware failures, duplicate IP address and starting, pausing and stopping of services are audited by system events.

Application log having activities related to user programs and commercial off the shelf application.

Security log having system auditing and security process used by windows.

Security log can be read by administrators only but system log and application log can be viewed by any users

B) Performing Keyword Searches : - It is important to perform string searches of the subject's hard drive during in investigation into possession of intellectual property or proprietary information, sex offenses and practically any case involving text based communication. To examine the contents of entire drive string searches can be conducted on the logical files structure or at physical level to examine the contents of an entire drive.

C) Reviewing Relevant Files :- Using third party software like antivirus and firewall , we can augment the monitoring and records keeping that a windows system. Windows contains temp files, cache files and other location where runtime data is stored.

D) Identifying Unauthorised user accounts or groups : User accounts and user groups on a live system can be audited in several ways.

i) For unauthorised user accounts, look in the User Manager

ii) To view all domain accounts on a domain controller and for suspicious entries, use userstat from NTRK.

iii) Examine the Security log using Event Viewer filtering for events.

iv) Check the \%systemroot%\Profiles\<user account> directory for User managers or registry.

E) Looking for Unusual or hidden files :- Using NTFS file system we have to view hidden file in windows system.

F) Checking for Unauthorised Access Points : An entry point to unwanted intruders could be provided by any services that allows some degree of remote access by using Trojan.

G) Examining Jobs Run by the scheduler Services:- The <hostname> is the NetBIOS name of the remote system and batman5 is the key pharse to connect. Using at command we can see any job that have been scheduled.

H) Analyzing Trust Relationship : - Sometimes attacker hack internal user username and password and access to system and make relationship with other entity in system and retrive all information. Hence we have to find all chain of relationship for all user login and accessibilty.

I) Reviewing Security Identifiers (SID) :- Investigators need to compare security identifiers (SID) found in the victim machine with those at central authentication authority to establish the actions of a specific user ID. Using SID user gets access to remote server with unique sequence number available in workstation registry.

Therefore SID can be digital fingerprints that prove that a remote system was used to log on to a machine and access domain.

Investigating Evidence in Unix Operating System

To investigate Unix OS , user needs to fetch and respond to a computer security incident. Unix offer some effective safety features such as login and user accounts which are stored in the /etc/passwd file , access control with a granularity of owner,cumentgroup and world and save record file :usr/adm/lastlog,/var/adm/utmp,/var/adm/wtmp,and /var/adm/acct.

Unix system directly connected to the internet are often subject to hacking attempts.

Some of the methods for UNIX investigation are :

1.Studying relevant logs.
2.Carrying out keyword searches
3.Go through relevant files
4.Recognizing illegal user accounts or groups
5.Classifying rogue process.
6.Checking for illegal access points
7.Examining trust relationship
8.Noticing Trojan loadable kernel modules

If attacker access root of the system, then he can modifying anything on operating system, including the evidence that you are reviewing.

Unix is a fully functional robust operating system. It continually added functionality over the course of its long history including network service. Along with Network File System(NFS),telnet,finger,rlogin and many others. A default installation of Unix offers a dazzling array of network services. Any one of the network services on UNIX systems can potentially allow some degree of remote access to unwanted intruders, as can a phone line connected to a mode.

If you want to investigate UNIX system, then you will need to examine all network services as potential access points.

E-mail Forensics for standard Protocols

Importance of E-mail as Evidence

1. E-mail can be pivotal evidence in a case.
2. Due to its informal nature, it does not always represent corporate policy.
3. E-mail itself is evidence as it left in arrears as it travels from sender to recipient like contain various logs and maintain system administrator
4. Law enforcement can use a writ issued by a government agency to collect e-mails.
5. There are two standard methods for sending & receiving e-mails (A) Client/Server application (B)Webmail.
6. After configuring server, user across globe

Register to these e-mail server and setup accounts and start communicating over internet with help of networking protocol like SMTP,POP3, HTTP,MAPI

SMTP is used in E-mail delivering and sending between client and server with port no. 25 on server.

POP3 is use to download email from server memory to client machine. IMAP stands for Internet Message Access Protocol use for downloading email from server and allow to store email content on server by utilizing proper memory and processing on server side.

E-mail fraud over Internet

1. E-mail Spoofing : - Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. The spoofer is trying to phish your passwords and login names. Phishing occurs when the dishonest sender tries to lure you into trusting the email. A false (spoofed) website may be waiting off to the side, cleverly disguised to appear to be a legitimate online bank website or paid web service

Steps to be taken if your mail Identity has been spoofed

- Report about the Spoofed mails to your Internet Service provider and notify them through Email.
- Change your password immediately for all your other email accounts.
- Enable Sender filtering
- Enable recipient filtering
- Further do not respond to any mails which have personal information from the forged Mail ID
- Add and update the block list regularly with the spammers, either their domain name or their email addresses
- Download Exchange tools and RUN it to make sure your server is safe and healthy

2. E-mail Spamming : - Email spam, also known as junk email, is unsolicited **bulk** messages sent through email. The use of spam has been growing in popularity since the early 1990s and is a problem faced by most email users.

How to stop spam emails

While receiving some spam may be unavoidable, users can reduce the amount that makes it into their inbox. Most email clients already have spam filtering in place, which will move suspicious email to a separate junk folder. By reporting, blocking and deleting instances of spam email that do make it into their inboxes, users can train the client to prevent further messages from those particular spam addresses or messages displaying similar content.

3. E-mail Tracing : - It means locating the original sender and getting to know IP address of the network from which the e-mail was actually generated, gets its all information regarding it's email routing and sender and receiver information..

4. Keystroke Loggers : - It capture the target's keystroke either saves them in a file to be read and communicate them to prearranged end point available to the hacker. Since keystroke logging program record every single keystroke in through the keywords, they can capture a widespread diversity of private information.

Securing E-mail account

1. Use a strong password.
2. Beware of Public PC.
3. Protect your email address and don’t publish it publically
4. Lock your PC always after working
5. Do not be fooled by e-commerce site etc. by disclosing all your personal information.
6. Use the encryption technique to send important data over email.

E-mail Recovery

1. Check the trash section
2. Search your inbox
3. Check any folder or label you have created
4. Check your archived message in Gmail
5. Contact Email services and with help of email recovery software recover email
6. Check the trash and other location
7. Check wen services that your client connects.
8. Check with the server administrator

E-mail Forensics Analysis steps and Methods

1. Header Analysis : With the help of header information of email, we can track sender information with respect to server or persons
2. Bait Tactics : - Using this technique we have to read log files on server and client , then we can gets all information's at both ends like IP address.
3. Server Investigation : - Over the sever we can get source of email and date and time as well as content.
4. Network Device Investigation : - Network devices keeps the records of log in which we can trace the e-mail routing path.

5. Software Embedded Identifiers : using this we can trace PST file,username,MCA address etc.
6. Sender e-mail fingerprints : - In header field of email we can allow to store face recognition and finger prints.