VENDOR AND COMPUTER FORENSICS SERVICES:-

As information technology and the internet become more integrated into today's workplaces, organizations must consider the misuse of technology as a real threat and plan for its eventuality.

Computer forensic services:-

- ✓ **Forensic incident response**
- ✓ **Evidence collection**
- ✓ **Forensic analysis**
- ✓ **Expert witness**
- ✓ **Forensic litigation and insurance claims support**
- ✓ **Training**
- ✓ **Forensic process improvement**

Occurrence of Cyber Crime:-

Cybercrime occurs when information technology is used to commit or conceal an offense. Computer crimes include:

- ✓ **Financial fraud**
- ✓ **Sabotage (damage) of data or networks**
- ✓ **Theft of proprietary information**
- ✓ **System penetration from the outside and denial of service**
- ✓ **Unauthorized access by insiders and employee misuse of Internet access privileges**
- ✓ **Viruses, which are the leading cause of unauthorized users gaining access to systems and networks through the Internet**

Cyber Detectives

Forensic investigators detect the extent of a security breach, recover lost data, determine how an intruder got past security mechanisms, and, possibly, identify the culprit.

A Forensic expert need to be qualified in both investigative and technical fields and trained in countering cybercrime. They should also be knowledgeable in the law, particularly legal jurisdictions, court requirements, and the laws on admissible evidence and production.

In many cases, forensic investigations lead to calling in law enforcement agencies and building a case for potential prosecution, which could lead to a criminal trial. The alternative is pursuing civil remedies, for instance, pursuing breach of trust and loss of intellectual property rights.

Fighting Cyber Crime with Risk-Management Techniques:-

The best approach for organizations want to counter cybercrime is to apply riskmanagement techniques. The basic steps for minimizing cybercrime damage are creating well-communicated IT and staff policies, applying effective detection tools, ensuring procedures are in place to deal with incidents, and having a forensic response capability.

✓ Effective IT and Staff Policies

The goal of these policies is to create a security solution that is owned by all staff, not only by those in the IT division.

✓ Vendor Tools of the Trade

The right vendor tools will detect an external attack and alert the organization to the threat. These tools are programs that either analyzes a computer system to detect anomalies, which may locate data that can be used as evidence supporting a crime or network intrusion.

Computer Forensics Investigative Services:-

In many companies, forensic computer examiners are great because they have more knowledge of the subject than their peers. However, they are still subject to management pressures to produce results, and at times this can color their judgment. Time restrictions can cause them to take short cuts that invalidate the very evidence they are trying to gather, and when they do not find the evidence that people are demanding (even if it isn't there), they are subject to criticism and undue pressure.

Many of these specialists are well meaning, but they tend to work in isolation or as part of a hierarchical structure where they are the computer expert. It takes a very strong-minded person to resist the sort of pressure, and it is obvious that this has had an adverse effect in a number of cases.

Computer Intrusion Detection Services:-

Intrusion detection is the latest security service to be offered on an outsourced basis, usually by the types of Internet service providers (ISPs) or specialized security firms that have been eager to manage your firewall and authentication. Although outsourcing security means divulging sensitive information about your network and corporate business practices, some companies say they have little choice but to get outside help, given the difficulty of hiring security experts.

Ex:- the Yankee Group reports that managed-security services (of which intrusion detection is the latest phenomenon) more than tripled, from $450 million in 2000 to $1.5 billion in 2003. By 2009, the market is expected to reach $7.4 billion, fueled by the trend toward outsourcing internal local area network (LAN) security to professional security firms as virtual employees.

Digital Evidence Collection:-

The following are some helpful tips that you can follow to help preserve the data for future computer forensic examination:

1. Do not turn on or attempt to examine the suspect computer. This could result in destruction of evidence.

2. Identify all devices that may contain evidence:

- **Workstation computers**
- **Off-site computers**
- **Removable storage devices**
- **Network storage devices (redundant array of independent disks [RAIDs], servers, storage area networks [SANs], network attached storage [NAS], spanned, remote network hard drives, back-up tapes, etc.)**

3. Quarantine all in-house computers:

• Do not permit anyone to use the computers.

• Secure all removable media.

• Turn off the computers.

• Disconnect the computers from the network.

4. Forensically image all suspect media.

Forensic Process Improvement:-

Most system administrators are rightly concerned with first securing their hosts and networks from attack. The techniques covered in this section will help you to determine possible actions and possible motivations of the attacker. If you can understand your attacker, than you can better defend against and respond to attacks against your network. Of course, it is important to understand that hackers will loop through several systems during the attack phase.

The first steps in the threat identification process are simply to know who owns the IP used in the attack.

The tools that are used in the threat identification process are:

- ✓ **Dig –x /nslookup**
- ✓ **Who is**
- ✓ **Ping**
- ✓ **Traceroute**
- ✓ **Finger**
- ✓ **Anonymous Surfing**
- ✓ **USENET**

Dig –x /nslookup:

The first step in the process is to reverse the offending (criminal) IP address. The"dig-x ip"command will perform a reverse lookup on an IP address from its domain name server. The "-x" operation will ensure that you receive all records possible about your host. This might include name servers, e-mail servers. The "nslookup" and "nslookup ip" will perform a reverse lookup of the host IP address.

Whois

The next step in the process is to perform a "whois" lookup on the IP address to see who owns or at least who the offending IP is registered to.

Ping

Conduct the "ping ip" command to determine if your attacking IP is currently online.

Traceroute

The next step in the process is to conduct a "traceroute ip" to determine possible paths from your proxy site to the target system. Traceroute may help you in two ways. One is if your IP does not resolve possible paths from your proxy site to the target system, there may be a clue. Second is traceroute may give you an important clue as to the physical location of the attacking box.

Finger

Conduct a "finger @ip" command to determine who is currently logged on to the system that attacked you.

Anonymous Surfing

Surfing anonymously to the domain from where you're attacking IP is hosted, is the next step in the threat identification process. You will know this domain name by looking at the resolved name of the host and "who is" data. One technique that is useful is to use a search engine such as http://www.altavista.com with the specialized advanced search option of "+host:domain name and hack*." This query will return the web links of possible hackers who operate from the domain name you queried.

USENET

The last step in the process of threat identification is to conduct a USENET traffic search on your domain. Sites such as http://www.deja.com are excellent for this.

Putting It All Together

Once you have completed the process previously outlined and gathered all the information from these tools, you should be able to make an educated guess about the threat level from the domain you are analyzing. An excellent site to check for archived postings of recently seen attacks is both http://www.sans.org and http://www.securityfocus.com.

Training

As previously explained, computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data). Often the computer evidence was created transparently by the computer's operating system and without the knowledge of the computer operator. Such information may actually be hidden from view and, thus, special forensic software tools and techniques are required to preserve, identify, extract, and document the related

computer evidence. It is this information that benefits law enforcement and military agencies in intelligence gathering and in the conduct of investigations.

Understanding terms in computer forensics

Each participant in a computer forensics course, who successfully completes the course, should receive some sort of a Certificate of completion that is suitable to framing. They should also leave the course with a good understanding of the following:

Computer-Evidence-Processing Procedures

The processing procedures and methodologies taught in a computer forensics course should conform (follow) to federal computer-evidence-processing standards. The tools that are used in the course, as well as the methods and procedures taught, should work with any computer forensics tools. The methods and many of the software tools should conform specifically to the computer-evidence-processing procedures followed by the FBI, U.S. Department of Defense and the U.S. Drug Enforcement Administration.

Preservation of Evidence

- ✓ **Computer evidence is fragile and susceptible to alteration or erasure by any number of occurrences.**
- ✓ **Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.**
- ✓ **Black box computer forensics software tools are good for some basic investigation tasks, but they do not offer a full computer forensics solution.**
- ✓ **SafeBack software overcomes some of the evidence weaknesses inherent in black box computer forensics approaches.**

- ✓ SafeBack technology has become a worldwide standard in making mirror image backups since 1990.

TROJAN HORSE PROGRAMS

- ✓ The computer forensic expert should be able to demonstrate his or her ability to avoid destructive programs and traps that can be planted by computer users bent on destroying data and evidence.
- ✓ Such programs can also be used to covertly capture sensitive information, passwords, and network logons.

COMPUTER FORENSICS DOCUMENTATION

- ✓ Without proper documentation, it is difficult to present findings.
- ✓ If the security or audit findings become the object of a lawsuit or a criminal investigation, then documentation becomes even more important.

FILE SLACK

- ✓ Slack space in a file is the remnant area at the end of a file in the last assigned disk cluster, that is unused by current file data, but once again, may be a possible site for previously created and relevant evidence.
- ✓ Techniques and automated tools that are used by the experts to capture and evaluate file slack.

DATA-HIDING TECHNIQUES

Trade secret information and other sensitive data can easily be secreted using any number of techniques. It is possible to

hide diskettes within diskettes and to hide entire computer hard disk drive partitions. Computer forensic experts should understand such issues and tools that help in the identification of such anomalies.

Internet-Related Investigations:-

Issues and techniques related to the investigation of Internet-related matters should be covered in the course. This should include a demonstration of how Internet related evidence differs from more traditional computer evidence. Emphasis should be placed on the investigation of Internet-based terrorist leads.

Dual-Purpose Programs:-

Programs can be designed to perform multiple processes and tasks at the same time. They can also be designed for delayed tasks and processes. These concepts should be demonstrated to the participants during the course through the use of specialized software. The participants should also have hands-on experience with such programs.

Text Search Techniques:-

Specialized search techniques and tools should be developed that can be used to find targeted strings of text in files, file slack, unallocated file space, and Windows swap files. Each participant should leave the class with the necessary knowledge to conduct computer security reviews and computer-related investigations. Because of the need to search for non-Latin words and word patterns tied to foreign languages, the course should also cover the search of such data tied to foreign languages Fuzzy Logic

Tools Used to Identify Previously Unknown Text:-

A methodology and special computer forensics tools should be developed that aid in the identification of relevant evidence and unknown strings of text.

Traditional computer evidence searches require that the computer specialist knows what is being searched for. However, many times not all is known in investigations. Thus, not all is known about what may be stored on a targeted computer system. In such cases, fuzzy logic tools can assist and can provide valuable leads as to how the subject computer was used. The participants should fully understand these methods and techniques. They should also be able to demonstrate their ability to use them to identify leads in file slack, unallocated file space, and Windows swap files.

Disk Structure:-

Participants should leave the course with a solid understanding of how computer hard disks and floppy diskettes are structured and how computer evidence can reside at various levels within the structure of the disk. They should also leave the class with a good understanding of how easy it is to modify the disk structure and to hide computer data in obscure places on floppy diskettes and hard disk drives.

Data Encryption:-

A computer forensics training course should also cover how data is encrypted and illustrate the differences between good encryption and bad encryption. The participants should become familiar with the use of software to crack security associated with these different encryption file structures.

Matching a Floppy Diskette to a Computer:-

Specialized computer forensics techniques and computer forensics tools should also be developed that make it possible to conclusively tie a floppy diskette to a computer hard disk drive. Each participant should also be taught how to use special software tools to complete a unique computer storage data-matching process. Some computer forensics experts believe floppy diskettes are no longer popular. They are wrong. Floppy diskettes are found to be a valuable source of computer evidence in some civil litigation cases that involve the theft of trade secrets.

Data Compression:-

The participant should be shown how data compression programs can be used to hide and disguise critical computer data. Furthermore, the participant should learn how password-protected compressed files can be broken.

Erased Files:-

Participants should be shown how previously erased files can be recovered using computer forensics processes and methods. Documentation of the process should also be covered in detail.

Internet Abuse Identification and Detection:-

The participant should be shown how to use specialized software to identify how a targeted computer has been used on the Internet. This process should focus on computer forensics issues tied to data that the computer user probably doesn't realize exists (file slack, unallocated file space, and Windows swap files). Participants should get hands-on experience in using this unique technology and they should be given the opportunity to purchase the software for a nominal charge. Nevertheless, it should be provided free of charge to law enforcement computer crime specialists who attend the course. Law enforcement agencies are typically underfunded.

The Boot Process and Memory Resident Programs:-

Participants should be able to see how easy it is to modify the operating system to capture data and to destroy computer evidence. Such techniques could be used to covertly capture keyboard activity from corporate executives, government computers, and the like. For this reason, it is important that the participants understand these potential risks and how to identify them