CYBER SECURITY

Introduction in Cyber Security	2
Hackers & Cybercrime	16
Ethical Hacking & Social Engineering	41
Cyber Forensics & Auditing	62
Cyber Ethics & Laws	91

NOTE:

MAKAUT course structure and syllabus of 7th semester has been changed from 2021. **CYBER SECURITY** has been introduced as a new subject in present curriculum. Taking special care of this matter we are providing chapterwise model questions and answers, so that students can get an idea about university questions patterns.

INTRODUCTION IN CYBER SECURITY

Multiple Choice Type Questions

1. Programs that multiply like viruses but spread from computer to computer are called as: [MODEL QUESTION]
   a) Worms b) Virus c) Boot d) None of these

Answer: (a)

2. Which of the following is a cybercrime? [MODEL QUESTION]
   a) Hacking b) Cyber bulling c) Virus attack d) All of these

Answer: (d)

3. DLL stands for [MODEL QUESTION]
   a) Dynamic Link Library b) Digital Link Library
   c) Distributed Link Library d) Domain Link Library

Answer: (a)

4. Hackers who release information to the public is [MODEL QUESTION]
   a) a black hat b) a grey hat c) a white hat d) a brown hat

Answer: (b)

5. Which of the following is a social Engineering site? [MODEL QUESTION]
   a) ebay b) facebook c) amazon d) CWB

Answer: (a)

6. Validation of the source of information is known as [MODEL QUESTION]
   a) Confidentiality b) Authentication c) Non-repudiation d) Data integrity

Answer: (b)

7. The Dos attack is one type of [MODEL QUESTION]
   a) Active Attack b) Passive Attack
   c) Brute force attack d) None of these

Answer: (a)

8. Traffic analysis is one type of [MODEL QUESTION]
   a) active attack b) passive attack
   c) brute force attack d) none of these

Answer: (b)

9. Chain & Abel is a popular ..... tool. [MODEL QUESTION]
   a) password cracking b) networking
   c) security d) messenger

Answer: (a)

10. Hacktivism is **[MODEL QUESTION]**
- **a) Activism**
- **b) Hacking for a cause**
- **c) Passive hacking**
- **d) Malicious hacking**

Answer: (b)

11. Banner grabbing is an example of what? **[MODEL QUESTION]**
- **a) Passive operating system fingerprinting**
- **b) Active operating system fingerprinting**
- **c) Footprinting**
- **d) Application analysis**

Answer: (a)

12. What is the full form of CERT/CC? **[MODEL QUESTION]**
- **a) Computer Engineering Response Team Co-ordination Centre**
- **b) Computer Emergency Record Team Co-ordination Centre**
- **c) Computer Emergency Response Team Co-ordination Centre**
- **d) Computer Engineering Record Team Co-ordination Centre**

Answer: (c)

13. LDAP stands for **[MODEL QUESTION]**
- **a) Lightweight Directory Access protocol**
- **b) Lightweight Data Access Protocol**
- **c) Lightweight Domain Access Protocol**
- **d) Lightweight DNS Access protocol**

Answer: (a)

14. What is enumeration? **[MODEL QUESTION]**
- **a) Identifying active systems on the network**
- **b) Cracking passwords**
- **c) Identifying users and machine names**
- **d) Identifying routers and firewalls**

Answer: (c)

Short Answer Type Questions

1. a) Give a brief comparison between a conventional crime and a cyber crime.
b) List the motives and reasons behind cyber crimes. **[MODEL QUESTION]**

Answer:

a) Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment."

Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those crime, where either the computer is an object or subject of the conduct constituting crime. "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime."

There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exists a fine line of demarcation between the conventional and cyber crime. The demarcation lies in the involvement of the medium in cases of cyber crime. The prerequisite for cyber crime is that there should be an involvement of the virtual cyber medium at any stage.

b) The crimes and criminals in the cyber world vary little from their physical world counterparts. Historically, and today, the same laws are used to prosecute both (ie: trespass, fraud, theft, copyright violation).
The motives and profiles of criminals in the virtual world are as varied as in the physical world. Motives include financial benefit, thrill seeking, revenge, knowledge, and beliefs.
Where the two worlds begin to diverge is in the lingo being built for the criminal using the computer in his crimes. A script kiddie is someone with a low technical skill level and of a young age. A hacktivist seeks to further his views by promoting them or striking out at those who hold opposing views. A web defacer targets websites that can be penetrated and changed. Crackers circumvent copy protection mechanisms. Pirates make or distribute unauthorized copies of protected programs or works. Lamers have a low technical skill level and largely reuse the work of others. Phreakers target telephone systems.
The term hacker is primarily used to describe those who participate in the insightful or intuitive exploration of systems. These activities are, in of themselves, benign but the term has also become linked with the cyber criminal. The term cracker is generally reserved for hackers with criminal intentions.
Hackers often align themselves in groups. They exchange details of their exploits on web sites and through Internet Relay Chat (IRC) messages. They contribute technical knowledge to their group and even participate in collaborative attacks.

2. Define strong, weak and random password with examples.

[MODEL QUESTION]

Answer:
A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase.
Weak passwords refer to any passwords that can be easily guessed, either because it's so personal to a person or because it hardly takes any time to find it via the brute-force method, where a hacker (here, a hacker being anyone who's intent on finding your password, be they a criminal in Belarus or your nosey kids) runs through all possible password options.
A random password generator is software program or hardware device that takes input from a random or pseudo-random number generator and automatically generates a password. Random passwords can be generated manually, using simple sources of randomness such as dice or coins, or they can be generated using a computer.

3. Write down the difference between computer virus and worm.
[MODEL QUESTION]

Answer:
A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.
A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

4. What is software piracy? Discuss about the preventive measures against software piracy.
[MODEL QUESTION]

Answer:
1st Part:
Software piracy is the stealing of legally protected software. Under copyright law, software piracy occurs when copyright protected software is copied, distributed, modified or sold. Software piracy is considered direct copyright infringement when it denies copyright holders due compensation for use of their creative works.

2nd Part:
Here are some of the tips to prevent or lessen software piracy:
Code Key - For the past 5 to 7 years, software developers have devised a plan to lessen or prevent software piracy. This is by using a code key. A code key comes with the software that we buy. Before fully installing the software on our computer, we must provide the specific code key that came with the software. After providing the code key, we can run the software on our computer. The code key also locks after it has been used. This is so that the software cannot be installed on other computers after it has been installed on one. We will have to call the manufacturer of the software to be able to use the code key again. This is not good news to people who pirate software.

Open Source - Open source software is described as a free software that anyone can download from the Internet. A lot of different software can are licensed as open source. Open source software are under the license free software license. There are also different upgrades for these open source software that can also be freely downloaded from the Internet. By using open source software, people don't need to worry about spending a lot of money for original copies of software. This will also lessen the number of people who are using pirated software as there are alternative programs that can be used and they do not have to pay fines when they are caught.

Hardware Key - A hardware key is a device that is used for anti-piracy. This tool prevents software vendors to distribute their products or use them without authorization from the copyright owner of the software. The hardware key works when it is attached to a computer. It monitors software licensing and enforces licensing of the protected software those are detected on the computer. This tool will lessen software vendors from illegally distributing the software that they have and is a good prevention measure for piracy.

Anti-Piracy Software - There are different types of anti-piracy software that are available for free. Anti-piracy software is used to prevent illegal duplication or illegal use of copyrighted software. There is also an anti-piracy software that prevents hackers from getting into the software and copying it without consent from the copyright owner. Some of them are also already integrated on the disks of the software that contains the program. This may also be for piracy music. The anti-piracy association is also looking for other ways to prevent software piracy. Reporting anti-piracy may prevent it from happening.

5. Explain the difference between Hackers, Crackers and Phreakers.
[MODEL QUESTION]

Answer:
A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never intentionally damage data.
A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.
Phreaks (or phreakers) are usually motivated more by technical curiosity and the hacker ethos than any criminal intent (although phreaking is most certainly illegal). To bounce a call through a dozen different switching systems around the world, to our friend next door - all for free - is regarded by phreaks as an accomplishment. The fact that they are committing fraud and felonies in the process is regarded as incidental - or perhaps part of the fun.

6. How do cybercriminals plan attack? **[MODEL QUESTION]**

Answer:
Cyber Criminals use many tools and methods to locate vulnerability of their victim. Following are three major phases involved in planning of cyber crime:

1. Reconnaissance: "Reconnaissance" means an act of econnoitring. In this phase attacker try to explore and gain every possible information about target. They use active and passive attacks to get this information.

2. **Scanning and Scrutinizing:** In this phase attacker collects validity of information as well as finds out existing vulnerabilities. It is the key phase before actual attack happens.

- Port scanning: Identify all ports and services (open / closed)
- Network scanning: Verify IP address and network information before cyber attacks.
- Vulnerability scanning: Checking loop hole in system.

3. **Launching an attack:** Using the information gathered in the previous step, they attack the target system to gain confidential information about individuals or organizations. The attack is launched using the following steps:

- Crack the password.
- Exploit the privilege
- Execute malicious command
- Hide the files
- Cover the track.

7. Explain LDAP and RAS security for mobile devices. Discuss the implication for mobile devices. [MODEL QUESTION]

Answer:

1st part:

LDAP: The Lightweight Directory Access Protocol is one of the core protocols that was developed for directory services. LDAP is used to distribute lists of information organized into directory information trees, which are stored within a LDAP database. However, in order to access information stored within an LDAP database, the user must first authenticate their identity. It can deliver LDAP authentication as a cloud based service.

It is a software protocol for enabling anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the public internet. It is a lightweight version of Directory Access Protocol which is part of X.500, a standard for directory services in a network.

RAS security for mobile devices:

RAS provides security features to be ensure that corporate data remains secure even available over the wide area network. In mobile devices;

1. It can robust the system.
2. Protecting corporating data and guarding the network against threats.
3. Highly definable permissions.

8. What do you mean by the term forgery? Explain with example. [MODEL QUESTION]

Answer:

Forgery includes imitation of original paper or online documents for the intent to harm reputation, or cheat, individual or a group by means of telecommunication network is forgery. It includes fraudulent transaction of credit cards, postage stamps, seals, currency,

immigration documents, signatures, bank checks, academic credentials, digital signatures on electronic documents, even medicines.

Example: In year 2008, a cyber crime originated in UK, named as DarkMarket used to sell credit card, login informations to members who used to commit financial crimes and fraudulent transactions.

9. What is the maximum penalty for forgery? **[MODEL QUESTION]**

Answer:

If caught under the act of forgery, defined under Indian Penal Code section 463, 464 an offender will be punished with imprisonment from three to five years or will be charged with a fine upto 2 lakhs or both.

10. What are the classifications of hackers? **[MODEL QUESTION]**

Answer:

Hackers are categorized into three kinds as black hat or crackers, white hat or ethical hackers, and grey hackers. Black hat hackers are normally crackers. They tamper website contents, forward spams, flood the network, and impersonate accounts. They always have malicious intent. White hat persons are ethical hackers who is responsible for finding the loopholes of a system. Industries employ white hats to find security cracks in the system or they are also employed if any attack has taken place. Study reports revealed that most of the industrial attacks are from inside. Someone who knows the security system very well and uses this skill to pose a threat to the organization can be called as grey hat. They behave ethical sometimes and crackers at other times.

11. What are the files that store passwords for Windows and Linux? **[MODEL QUESTION]**

Answer:

Windows stores encrypted files in SAM file under system32 while Linux stores passwords in /etc/shadow file.

12. What are the different types of password hacking method? **[MODEL QUESTION]**

Answer:

There are two different categories for password hacking one is active and another is passive. Passive attack includes sniffing, masquerading, eavesdropping or playing man in the middle attack, dictionary attack, brute force attack. Active attack can include guessing, shoulder surfing, or social engineering.

13. Define the terms social engineering, man in the middle attack. **[MODEL QUESTION]**

Answer:

Social engineering: It is psychological manipulation of persons ultimately gaining their trust to reveal confidential information about the organization or the system. There are different types of social engineering techniques used to lure a victim to reveal secret information. Hackers use people's good nature to make this kind of access into

organization. Pretexting, vishing, tailgating etc. are the normally used as social engineering methods.

Man-in-the middle attack: Attacker acts in between server and client connection. He splits the TCP connection into two and acts as server to the client and a client to the server. Any message is intercepted by the attacker and he is able to manipulate both client and server in his own way.

14. What is eavesdropping and hybrid attack? **[MODEL QUESTION]**

Answer:

- **Eavesdropping:** It is snooping into conversation of unsuspecting parties over telephone lines, instant messages, Wireless LANs, etc. Attacker use tools like Airsnort, Ethereal and sniff around in any forms of communication that is considered to be private. This includes capturing of network packet in the communication medium.
- **Hybrid attack:** It is a password attack which combines the flavor of dictionary attack and brute force attack.

Long Answer Type Questions

1. a) Define Cybercrime? Discuss about various types of Cybercrime.
b) Discuss about email spoofing and email spamming.
c) What is Reconnaissance in the world of Hacking?
d) What is Salami Attack? **[MODEL QUESTION]**

Answer:

a) 1st Part:

Identity theft is a form of stealing someone's personal information and pretending to be that person in order to obtain financial resources or other benefits in that person's name without their consent. Identity theft is considered a cyber crime.

2nd Part:

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.
Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.
Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
Child soliciting and Abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

b) Email spamming refers to sending email to thousands and thousands of users – similar to a chain letter. Spamming is often done deliberately to use network resources. Email spamming may be combined with email spoofing, so that it is very difficult to determine the actual originating email address of the sender. Some email systems, including our Microsoft Exchange, have the ability to block incoming mail from a specific address. However, because these individuals change their email addresses frequently, it is difficult to prevent some spam from reaching your email inbox.
Email spoofing refers to email that appears to have originated from one source when it was actually sent from another source. Individuals, who are sending "junk" email or "spam", typically want the email to appear to be from an email address that may not exist. This way the email cannot be traced back to the originator.

c) Reconnaissance is considered the first pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. The hacker seeks to find out as much information as possible about the victim. This first step is considered a *passive information gathering*. As an example, many have probably seen a detective movie in which the policeman waits outside a suspect's house all night and then follows him from a distance when he leaves in the car. That's reconnaissance; it is passive in nature, and, if done correctly, the victim never even knows it is occurring.

d) Salami attack: A salami attack is a collection of small attacks that result in a larger attack when combined. For example, if an attacker has a collection of stolen credit card numbers, the attacker could withdraw small amounts of money from each credit card (possibly unnoticed by the credit card holders). Although each withdrawal is small, the combination of the multiple withdrawals results in a significant sum for the attacker.

2. Explain the difference between passive and active attacks. [MODEL QUESTION]

Answer:

Refer to Question No. 6(c) of Long Answer Type Questions.

3. What is forgery? [MODEL QUESTION]

Answer:

Forgery includes imitation of original paper or online documents for the intent to harm reputation, or cheat, individual or a group by means of telecommunication network is forgery. It includes fraudulent transaction of credit cards, postage stamps, seals, currency, immigration documents, signatures, bank checks, academic credentials, digital signatures on electronic documents, even medicines.

Example: In year 2008, a cyber crime originated in UK, named as DarkMarket used to sell credit card, login informations to members who used to commit financial crimes and fraudulent transactions.

4. a) Who are cyber criminals? Discuss about various types of Cybercrime.
b) Discuss the role of Cloud computing in cyber security. [MODEL QUESTION]

Answer:

a) 1st Part:

A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.

Cybercriminals use computers in three broad ways:

- **Select computer as their target:** These criminals attack other people's computers to perform malicious activities, such as spreading viruses, data theft, identity theft etc.
- **Uses computer as their weapon:** They use the computer to carry out "conventional crime", such as spam, fraud, illegal gambling, etc.
- **Uses computer as their accessory:** They use the computer to save stolen or illegal data.

2nd Part: ***Refer to Question No. 1(a) (2nd Part) of Long Answer Type Questions.***

b) Cloud computing and cyber security are the two advanced sectors in IT world making huge changes of working pattern in the field. When these two merge it opens a wide range of possibilities. The cloud computing security provides companies with the availability, reliability, and security they need to conduct business in a global marketplace. Advanced cyber security features combine with physical infrastructure to create a comprehensive, secure solution to your cloud computing needs.

As companies migrate more and more of their data and infrastructure to the cloud, the question of cloud computing security becomes paramount. Cloud security provides multiple levels of control in a network infrastructure to afford continuity and protection. It's an essential ingredient in creating an environment that works for companies around the world. The benefits of cloud computing can be affordably attained by partnering with

advanced private cloud computing providers in a way that doesn't jeopardize your company's security.

At a time when cyber attacks are growing worldwide, and high-profile cybercrime such as data theft, ransomware and computer hacks have become the order of the day, experts believe that cloud computing may provide the security against cyber threats that companies need. They reason that Cloud helps security operations respond quicker to threats and focus on business risk as opposed to spending countless hours researching threats and trouble-shooting aging on-premises systems. It also saves a substantial cost for organizations in the long run.

5. "Social Networking is increasingly becoming a source of cybercrime." Explain. **[MODEL QUESTION]**

Answer:

As social networking becomes more a part of our daily lives, individuals find this technology an attractive vehicle to perpetrate cyber crimes. Anonymity provided via social networks allows a person to easily portray another user's identity. Cyber criminals exploit such vulnerabilities to steal user credentials, which in turn can be used to breach a company's network infrastructure.

The term cyber crime is confirmed as the official crime term as criminals started getting more aggressive over the online and becoming a threat for millions of Internet users. Identity theft is the key threat to many social media users, as millions of online users use their personal information in order to getting registered with one or more social media platforms. Such huge information with personal data of so many people is one of the easiest targets for many cyber criminals. Many users also use their credit or debit card to purchase different products, items or services through these social networking sites. This is why the cyber criminals around the world continuously try to get inside the personal details of many users from those social media platforms.

We can minimize the threat of cyber attack or cyber crime by getting a little aware and conscious while using social networking sites.

6. Write short note on the following: **[MODEL QUESTION]**

a) Computer Network Intrusion

b) Forgery

c) Passive attack vs. Active attack

Answer:

a) Computer Network Intrusion:

A network intrusion is any unauthorized activity on a computer network. Detecting an intrusion depends on the defenders having a clear understanding of how attacks work.

In most cases, such unwanted activity absorbs network resources intended for other uses, and nearly always threatens the security of the network and/or its data. Properly designing and deploying a network intrusion detection system will help block the intruders.

As a first step of defence, here's a brief rundown of popular attack vectors.

Asymmetric Routing

In this method, the attacker attempts to utilize more than one route to the targeted network device. The idea is to have the overall attack evade detection by having a significant portion of the offending packets bypass certain network segments and their network intrusion sensors. Networks that are not set up for asymmetric routing are impervious to this attack methodology.

Buffer Overflow Attacks

This approach attempts to overwrite specific sections of computer memory within a network, replacing normal data in those memory locations with a set of commands that will later be executed as part of the attack. In most cases, the goal is to initiate a denial of service (DoS) situation, or to set up a channel through which the attacker can gain remote access to the network. Accomplishing such attacks is more difficult when network designers keep buffer sizes relatively small, and/or install boundary-checking logic that identifies executable code or lengthy URL strings before it can be written to the buffer.

Gateway Interface Scripts

The Common Gateway Interface (CGI) is routinely used in networks to support interaction between servers and clients on the Web. But it also provides easy openings—such as "backtracking"—through which attackers can access supposedly secure network system files. When systems fail to include input verification or check for backtrack characters, a covert CGI script can easily add the directory label ".." or the pipe "|" character to any file path name and thereby access files that should not be available via the Web.

Protocol-Specific Attacks

When performing network activities, devices obey specific rules and procedures. These protocols—such as ARP, IP, TCP, UDP, ICMP, and various application protocols—may inadvertently leave openings for network intrusions via protocol impersonation ("spoofing") or malformed protocol messages. For example, Address Resolution Protocol (ARP) does not perform authentication on messages, allowing attackers to execute "man-in-the-middle" attacks. Protocol-specific attacks can easily compromise or even crash targeted devices on a network.

Traffic Flooding

An ingenious method of network intrusion simply targets network intrusion detection systems by creating traffic loads too heavy for the system to adequately screen. In the resulting congested and chaotic network environment, attackers can sometimes execute an undetected attack and even trigger an undetected "fail-open" condition.

Trojans

These programs present themselves as benign and do not replicate like a virus or a worm. Instead, they instigate DoS attacks, erase stored data, or open channels to permit system control by outside attackers. Trojans can be introduced into a network from unsuspected online archives and file repositories, most particularly including peer-to-peer file exchanges.

Worms

A common form of standalone computer virus, worms are any computer code intended to replicate itself without altering authorized program files. Worms often spread through

email attachments or the Internet Relay Chat (IRC) protocol. Undetected worms eventually consume so many network resources, such as processor cycles or bandwidth that authorized activity is simply squeezed out. Some worms actively seek out confidential information—such as files containing the word "finance" or "SSN"—and communicate such data to attackers lying in wait outside the network.

b) Forgery:

Offences of computer forgery and counterfeiting have become rampant as it is very easy to counterfeit a document like birth certificate and use the same to perpetuate any crime. The authenticity of electronic documents hence needs to be safeguarded by making forgery with the help of computers abs explicit offence punishable by law.

When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. In this instance, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery. A new generation of fraudulent alteration or counterfeiting emerged when computerized color laser copiers became available. These copiers are capable of high-resolution copying, modification of documents, and even the creation of false documents without benefit of an original, and they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.

These schemes take very little computer knowledge to perpetrate. Counterfeit checks, invoices and stationery can be produced using scanners, color printers, and graphics software. Such forgeries are difficult to detect for the untrained eye. It is relatively easy to scan a logo into a computer system and go from there.

c) Passive attack vs. Active attack:

Active attacks alter the system or network operations while passive attack gathers information about the system without altering the system. Active attack can involve infecting the system with virus or worms or can span upto deleting the entire hard drive. Normally passive attacks remain undetected. Active attack can flood the entire network with unnecessary packets and can render it slow while passive attack can sniff network packets without changing them. Passive attackers can know the presence of certain user accounts along with their password while active attackers use this information to render the system useless to the owner.

7. What are the different types of software piracy? What are the risks involved in using pirated software? [MODEL QUESTION]

Answer:

1st Part:

According to some people "Software piracy is copying and use of Software without proper license from the developer. Similarly, simultaneous use of single user license software by multiple users or loading of a single user license software at multiple sites, also amounts to software piracy. Using trial version software for commercial gains is also piracy, Piracy is also can be punishable if you install an pirated software do your work and then delete this software from the machine with enough evidences to show the

activity. Any Copyright infringement is the unauthorized use of copyrighted material in a manner that violates one of the copyright owner's exclusive rights, such as, the right to reproduce or to make derivative works that build upon it. For electronic and audio-visual media, such unauthorized reproduction and distribution of a copyrighted work is often referred to as piracy (however there is no legal basis for the term 'piracy')". There are different types of software piracy such as copying of copyrighted materials and using multiple copies of the same without license. Even if a person installs and uses the copy of the material and then removes it from the system, it will also be reported as software piracy. It includes installation on hard drive or on servers and clients with same version and no license. If a company illegally sells the product of another company without their permission or authorization with or without alteration of the original product can be considered as piracy.

2nd Part:

Apart from getting caught and termed a three years of imprisonment, an offender can be charged with fine of Rs 50,000 to Rs 2 lakhs or both. The software can be corrupted or can be of low or degraded quality. The software can contain malwares or Trojans that can cause data theft or may lead to disabled system or infected network. Pirated software can cause reputation loss in a business and can end contracts with the clients.

HACKERS & CYBERCRIME

Multiple Choice Type Questions

1. The use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization is termed: [MODEL QUESTION]
   a) Cyberspace b) Cyber Stalking c) Pornography d) None of these
Answer: (b)

2. Changing of raw data is known as [MODEL QUESTION]
   a) Salami attack b) Data diddling c) Forgery d) Web Jacking
Answer: (b)

3. Sniffing is a technique used for [MODEL QUESTION]
   a) attacks on computer hardware b) attacks on computer software
   c) attacks on operating system d) attacks on wireless network
Answer: (d)

4. Pharming is used for [MODEL QUESTION]
   a) Data hiding b) Data alteration
   c) Hosts of file poisoning d) File overriding 15 digits
Answer: (b)

5. Skimming means [MODEL QUESTION]
   a) Stealing ATM PIN information b) Stealing telephonic information
   c) Stealing identity d) None of these
Answer: (a)

6. A planned act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system is [MODEL QUESTION]
   a) Techno crime b) Techno vandalism
Answer: (a)

7. The practice of buying 'domain names' that have existing business names and selling it back to the rightful owner at much higher price is [MODEL QUESTION]
   a) cyberterrorism b) cybersquatting c) cyberwarfare d) forgery
Answer: (b)

8. Credit card fraud is a cybercrime against [MODEL QUESTION]
   a) individual b) property c) organization d) society
Answer: (b)

9. Which of the following is a type of intellectual property theft? **[MODEL QUESTION]**

a) Business **b) Financial** **c) Medical** **d) None of these**

Answer: (d)

10. Trying every possible key until an intelligent translation of the CT into PT is known as **[MODEL QUESTION]**

a) Trojan horse **b) Virus** **c) Brute force attack** **d) Worm**

Answer: (c)

11. Public key cryptography is also known as **[MODEL QUESTION]**

a) symmetric key cryptography **b) asymmetric key cryptography**
c) both (a) & (b) **d) none of these**

Answer: (b)

Short Answer Type Questions

1. Write down the different types of Credit Card frauds. **[MODEL QUESTION]**

Answer:

Different credit card frauds are as follows:

Manual or Electronic Credit Card Imprints

Data from a legitimate card is imprinted or the magnetic strip is skimmed. The information from the card is then later used for fraudulent transactions or for encoding fake cards.

Card-not-present (CNP) fraud

Credit card fraud can be perpetrated against you if the account number and expiry date of your card are known. The fraud may be by way of mail, phone or internet and does not require your physical card to be present unless the merchant requests the card verification code.

Counterfeit card fraud

This fraud usually involves skimming. The data is then transferred onto a fake magnetic stripe card. A skimmed counterfeit is used to produce a fully functional counterfeit card. There is an exact copy of the magnetic stripe.

Lost and stolen card fraud

This occurs when your card is physically stolen or lost and then used by a criminal, posing as you, to make unauthorized charges on your account.

Card ID theft

This occurs when a criminal has managed to obtain details about your card and uses the information to open or take over a card account in your name.

Mail non-receipt card fraud aka intercept fraud aka never received issue

Doctored Cards

The metallic stripe on a card can be erased using a strong magnet. A criminal will do this and then alter details on the card to match those of a valid card. The card will not work and the criminal will then con the merchant into punching in the card details manually.

Fake Cards

Producing fake cards takes a lot of time, effort and skill. There are many security features particularly difficult to reproduce, for example, holograms.

Account Takeover

This can happen when a criminal, having gathered Manual or Electronic Credit Card Imprints.

Data from a legitimate card is imprinted or the magnetic strip is skimmed. The information from the card is then later used for fraudulent transactions or for encoding fake cards.

Card-not-present (CNP) fraud

Credit card fraud can be perpetrated against you if the account number and expiry date of your card are known. The fraud may be by way of mail, phone or internet and does not require your physical card to be present unless the merchant requests the card verification code.

2. Differentiate between Inside and Outside attack. [MODEL QUESTION]

Answer:

Inside attack takes place from inside of secured perimeters of an organization. Normally, Insider has more access to resources of the organization. This may include selling of confidential information of an organization to any competitor. Also time taken by an inside attacker is always less than an outside intruder. Outside attack takes place from remote site or from Internet. Resources gathered by the attacker is less than the previous case. Outside attack may bypass firewall and NAT.

3. Who are the crackers? [MODEL QUESTION]

Answer:

A computer cracker is an outdated term used to describe someone who broke into computer systems, bypassed passwords or licenses in computer programs, or in other ways intentionally breached computer security. Computer crackers were motivated by malicious intent, for profit or just because the challenge is there.

4. Compare between cracker and hacker. [MODEL QUESTION]

Answer:

The antiquated phrase *computer cracker* is not used anymore. It was originally proposed as an antonym, or the opposite, of the term *hacker*. Hacker initially applied to only those who used their computing skills *without* malicious intent -- they broke into systems to identify or solve technical issues. Skillful technologists with altruistic motives were called *hackers*; those with bad intent were called *computer crackers*. This distinction never gained much traction, however.

In 1993, the Internet Users' Glossary defined hacker as "a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where 'cracker' would be the correct term."

The Glossary defined a computer cracker as "an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system."
The term *computer cracker* was subsequently subsumed by the term black hat, another outdated term for threat actor.
It should be noted, however, that people today rarely distinguish between ethical hackers and malicious hackers. Although hackers, by definition, do not have malicious intent, some people assume malicious intent when the word is used in everyday context.

5. What is a cyber security vulnerability? [MODEL QUESTION]

Answer:

In order to define a cyber security vulnerability, first, we need to understand what a vulnerability is. A vulnerability, in broad terms, is a weak spot in your defense.
Every organization has multiple security measures that keep intruders out and important data in.
Through security vulnerabilities, an attacker can find their way into your systems and network, and even extract sensitive information. Bearing in mind that a chain is as strong as its weakest link, we can assume that the security posture of your organization is as strong as its vulnerable spots.
Now having defined a vulnerability, we can narrow down our definition to cover cyber security vulnerabilities. **The term cyber security vulnerability refers to any kind of exploitable weak spot that threatens the cyber security of your organization.**
For instance, if your organization does not have a lock on its front door, this poses a security vulnerability, since one can easily come in and steal anything valuable.
Similarly, if your organization does not have proper firewalls, an intruder can easily break into your networks and network assets and steal important data. Since the assets under threat are digital, not having proper firewalls poses a cyber security vulnerability.

6. What are different types of cyber security vulnerabilities? [MODEL QUESTION]

Answer:

There are specific cyber security vulnerabilities that are targeted by attackers more often, especially computer software vulnerabilities. Below you can find a list of the top three cyber security vulnerabilities that have caused the most harm to organizations in this decade.

Broken Authentication:

In order to pose as the original user, malicious attackers can hack user sessions and identities by compromising authentication credentials. In the past, multi-factor authentication was vastly popular, but due to its difficulties in use, password authentication prevailed.
Two-factor authentication, on the other hand, is still a widely implemented security process that involves two methods of verification. One method is usually password verification. Frequently used types of authentication technology are username/password, one-time password and biometric authentication.

Injection:
An injection flaw is a vulnerability which allows an attacker to relay malicious code through an application to another system. This can include compromising both backend systems as well as other clients connected to the vulnerable application.

Security Misconfiguration:
Security misconfiguration gives attackers a chance to gain unauthorized access to some system data or functionality. Generally, such flaws evolve into a complete system compromise. The business impact depends on the protection needs of the application and data.

7. What are the types of security vulnerabilities? **[MODEL QUESTION]**

Answer:
There are three main types of security vulnerabilities:

- Faulty defenses
- Poor resource management
- Insecure connection between elements

Faulty Defenses:
Faulty defenses refer to porous defense measures that fail to protect your organization from intruders. There are various defense techniques including authorization, encryption and authentication.
When employed properly, these techniques have the ability to protect your organization from a great deal of cyber attacks. On the other hand, with poor implementation, they create an illusion of security while exposing your organization to grave risks.

Poor Resource Management:
Resource management practices include transferring, using, creating and even destroying the resources within a system. When management of resources is poor or risky, your organization is prone to have vulnerabilities like path traversal, use of potentially dangerous functions, buffer overflow, and much more.

Insecure Connection Between Elements:
When the interaction between components of your system and/or network is insecure, your organization is exposed to many threats including SQL injection, open redirect, cross-site scripting, and much more.
In order to ensure that your organization is free from such vulnerabilities, it is critical to pay the utmost attention to how data circulates across your networks and systems. If you can secure the circulation of data, most aforementioned vulnerabilities and threats can be considered solved. Yet you must also consider unique vulnerabilities and develop appropriate solutions for each.

8. What is malware threat? **[MODEL QUESTION]**

Answer:
Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software." Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.
Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems. Though varied in type and capabilities, malware usually has one of the following objectives:

- Provide remote control for an attacker to use an infected machine.
- Send spam from the infected machine to unsuspecting targets.
- Investigate the infected user's local network.
- Steal sensitive data.

9. What are different types of Malware Attacks? [MODEL QUESTION]
Answer:
Malware also uses a variety of methods to spread itself to other computer systems beyond an initial attack vector. Malware attack definitions can include:

- Email attachments containing malicious code can be opened, and therefore executed by unsuspecting users. If those emails are forwarded, the malware can spread even deeper into an organization, further compromising a network.
- File servers, such as those based on common Internet file system (SMB/CIFS) and network file system (NFS), can enable malware to spread quickly as users access and download infected files.
- File-sharing software can allow malware to replicate itself onto removable media and then on to computer systems and networks.
- Peer to peer (P2P) file sharing can introduce malware by sharing files as seemingly harmless as music or pictures.
- Remotely exploitable vulnerabilities can enable a hacker to access systems regardless of geographic location with little or no need for involvement by a computer user.

10. How to prevent malware? [MODEL QUESTION]
Answer:
A variety of security solutions are used to detect and prevent malware. These include firewalls, next-generation firewalls, network intrusion prevention systems (IPS), deep packet inspection (DPI) capabilities, unified threat management systems, antivirus and anti-spam gateways, virtual private networks, content filtering and data leak prevention systems. In order to prevent malware, all security solutions should be tested using a wide range of malware-based attacks to ensure they are working properly. A robust, up-to-date library of malware signatures must be used to ensure testing is completed against the latest attacks

The Cortex XDR agent combines multiple methods of prevention at critical phases within the attack lifecycle to halt the execution of malicious programs and stop the exploitation of legitimate applications, regardless of operating system, the endpoint's online or offline status, and whether it is connected to an organization's network or roaming. Because the Cortex XDR agent does not depend on signatures, it can prevent zero-day malware and unknown exploits through a combination of prevention methods.

Malware Detection:
Advanced malware analysis and detection tools exist such as firewalls, Intrusion Prevention Systems (IPS), and sandboxing solutions. Some malware types are easier to detect, such as ransomware, which makes itself known immediately upon encrypting your files. Other malware like spyware, may remain on a target system silently to allow an adversary to maintain access to the system. Regardless of the malware type or malware meaning, its detectability or the person deploying it, the intent of malware use is always malicious.
When you enable behavioral threat protection in your endpoint security policy, the Cortex XDR agent can also continuously monitor endpoint activity for malicious event chains identified by Palo Alto Networks.

Malware Removal:
Antivirus software can remove most standard infection types and many options exist for off-the-shelf solutions. Cortex XDR enables remediation on the endpoint following an alert or investigation giving administrators the option to begin a variety of mitigation steps starting with isolating endpoints by disabling all network access on compromised endpoints except for traffic to the Cortex XDR console, terminating processes to stop any running malware from continuing to perform malicious activity on the endpoint, and blocking additional executions, before quarantining malicious files and removing them from their working directories if the Cortex XDR agent has not already done so.

Malware Protection:
To protect your organization against malware, you need a holistic, enterprise-wide malware protection strategy. Commodity threats are exploits that are less sophisticated and more easily detected and prevented using a combination of antivirus, anti-spyware, and vulnerability protection features along with URL filtering and Application identification capabilities on the firewall.

11. What is sniffing technique? **[MODEL QUESTION]**

Answer:
Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.
There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical

location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

One can sniff the following sensitive information from a network –

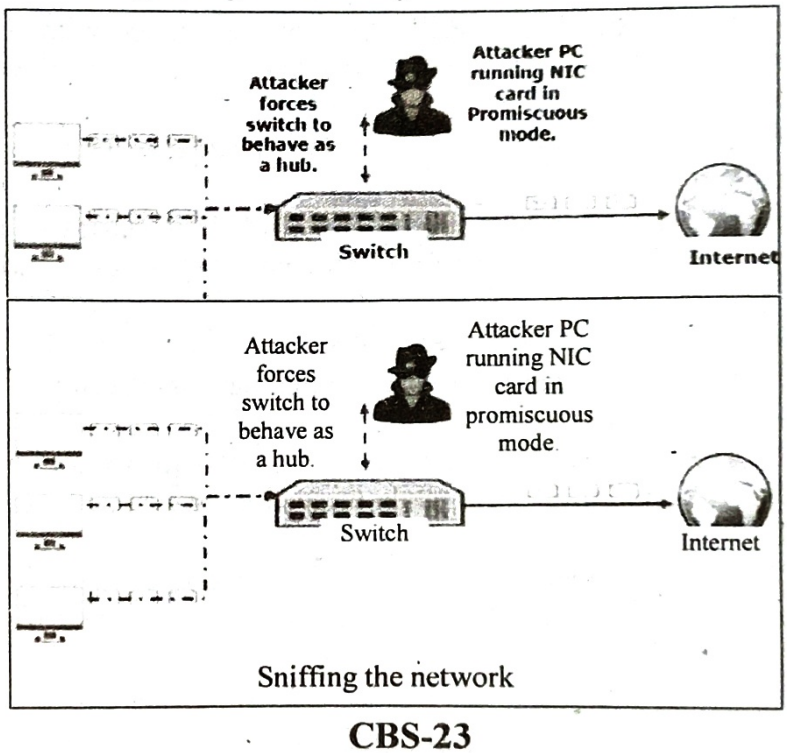
- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

12. How does sniffing work? **[MODEL QUESTION]**

Answer:

A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.



Sniffing the network

A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

13. What are different types of sniffing? **[MODEL QUESTION]**

Answer:

Sniffing can be either Active or Passive in nature.

Passive Sniffing:

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing:

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques –

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

Protocols which are affected:

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing –

- **HTTP** – It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP** (Simple Mail Transfer Protocol) – SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
- **NNTP** (Network News Transfer Protocol)– It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
- **POP** (Post Office Protocol) – POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- **FTP** (File Transfer Protocol) – FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.

- **IMAP** (Internet Message Access Protocol) – IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** – Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

14. What is gaining access attack? **[MODEL QUESTION]**

Answer:

Gaining access attack is the second part of the network penetration testing. In this section, we will connect to the network. This will allow us to launch more powerful attacks and get more accurate information. If a network doesn't use encryption, we can just connect to it and sniff out unencrypted data. If a network is wired, we can use a cable and connect to it, perhaps through changing our MAC address. The only problem is when the target use encryption like WEP, WPA, WPA2. If we do encounter encrypted data, we need to know the key to decrypt it.

15. What is privilege escalation? **[MODEL QUESTION]**

Answer:

Privilege escalation is a common way for attackers to gain unauthorized access to systems within a security perimeter.

Attackers start by finding weak points in an organization's defenses and gaining access to a system. In many cases that first point of penetration will not grant attackers with the level of access or data they need. They will then attempt privilege escalation to gain more permissions or obtain access to additional, more sensitive systems.

In some cases, attackers attempting privilege escalation find the "doors are wide open" – inadequate security controls, or failure to follow the principle of least privilege, with users having more privileges than they actually need. In other cases, attackers exploit software vulnerabilities, or use specific techniques to overcome an operating system's permissions mechanism.

There are two types of privilege escalation:

- **Horizontal privilege escalation**—an attacker expands their privileges by taking over another account and misusing the legitimate privileges granted to the other user. To learn more about horizontal privilege escalation see our guide on lateral movement.
- **Vertical privilege escalation**—an attacker attempts to gain more permissions or access with an existing account they have compromised. For example, an attacker takes over a regular user account on a network and attempts to gain administrative permissions. This requires more sophistication and may take the shape of an Advanced Persistent Threat.

16. What are computer Viruses? **[MODEL QUESTION]**

Answer:

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

17. How does a computer virus attack? **[MODEL QUESTION]**

Answer:

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.

This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.

While some viruses can be playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk. Worse yet, some viruses are designed with financial gains in mind.

18. How do computer viruses spread? **[MODEL QUESTION]**

Answer:

In a constantly connected world, you can contract a computer virus in many ways, some more obvious than others. Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Your mobile devices and smartphones can become infected with mobile viruses through shady app downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files.

To avoid contact with a virus, it's important to exercise caution when surfing the web, downloading files, and opening links or attachments. To help stay safe, never download text or email attachments that you're not expecting, or files from websites you don't trust.

19. What are the signs of a computer virus? **[MODEL QUESTION]**

Answer:

A computer virus attack can produce a variety of symptoms. Here are some of them:

- **Frequent pop-up windows.** Pop-ups might encourage you to visit unusual sites. Or they might prod you to download antivirus or other software programs.
- **Changes to your homepage.** Your usual homepage may change to another website, for instance. Plus, you may be unable to reset it.
- **Mass emails being sent from your email account.** A criminal may take control of your account or send emails in your name from another infected computer.

- **Frequent crashes.** A virus can inflict major damage on your hard drive. This may cause your device to freeze or crash. It may also prevent your device from coming back on.
- **Unusually slow computer performance.** A sudden change of processing speed could signal that your computer has a virus.
- **Unknown programs that start up when you turn on your computer.** You may become aware of the unfamiliar program when you start your computer. Or you might notice it by checking your computer's list of active applications.
- **Unusual activities like password changes.** This could prevent you from logging into your computer.

20. How to help protect against computer viruses? **[MODEL QUESTION]**

Answer:

How can you help protect your devices against computer viruses? Here are some of the things you can do to help keep your computer safe.

- Use a trusted antivirus product, such as Norton AntiVirus Basic, and keep it updated with the latest virus definitions. Norton Security Premium offers additional protection for even more devices, plus backup.
- Avoid clicking on any pop-up advertisements.
- Always scan your email attachments before opening them.
- Always scan the files that you download using file sharing programs.

21. What are the different types of computer viruses? **[MODEL QUESTION]**

Answer:

1. Boot sector virus:

This type of virus can take control when you start — or boot — your computer. One way it can spread is by plugging an infected USB drive into your computer.

2. Web scripting virus:

This type of virus exploits the code of web browsers and web pages. If you access such a web page, the virus can infect your computer.

3. Browser hijacker:

This type of virus "hijacks" certain web browser functions, and you may be automatically directed to an unintended website.

4. Resident virus:

This is a general term for any virus that inserts itself in a computer system's memory. A resident virus can execute anytime when an operating system loads.

5. Direct action virus:

This type of virus comes into action when you execute a file containing a virus. Otherwise, it remains dormant.

6. Polymorphic virus:

A polymorphic virus changes its code each time an infected file is executed. It does this to evade antivirus programs.

7. File infector virus:
This common virus inserts malicious code into executable files — files used to perform certain functions or operations on a system.
8. Multipartite virus:
This kind of virus infects and spreads in multiple ways. It can infect both program files and system sectors.
9. Macro virus:
Macro viruses are written in the same macro language used for software applications. Such viruses spread when you open an infected document, often through email attachments.

22. How to remove computer viruses? **[MODEL QUESTION]**
Answer:
You can take two approaches to removing a computer virus. One is the manual do-it-yourself approach. The other is by enlisting the help of a reputable antivirus program.
Want to do it yourself? There can be a lot of variables when it comes to removing a computer virus. This process usually begins by doing a web search. You may be asked to perform a long list of steps. You'll need time and probably some expertise to complete the process.
If you prefer a simpler approach, you can usually remove a computer virus by using an antivirus software program. For instance, Norton AntiVirus Basic can remove many infections that are on your computer. The product can also help protect you from future threats.
Separately, Norton also offers a free, three-step virus clean-up plan. Here's how it works.
1. Run a free Norton Security Scan to check for viruses and malware on your devices. Note: It does not run on Mac OS.
2. Use Norton Power Eraser's free virus and malware removal tool to destroy existing viruses. A Norton tech can assist by remotely accessing your computer to track down and eliminate most viruses.
3. Install up-to-date security software to help prevent future malware and virus threats.

Long Answer Type Questions

1. What is buffer overflow? Explain various types of buffer overflow. How to minimize buffer overflow? **[MODEL QUESTION]**
Answer:
1st Part:
A buffer overflow occurs when more data are written to a buffer than it can hold. The excess data is written to the adjacent memory, overwriting the contents of that location and causing unpredictable results in a program. Buffer overflows happen when there is improper validation (no bounds prior to the data being written). It is considered a bug or weakness in the software.

2nd Part:

A buffer overflow is an exploit that takes advantage of a program that is waiting on a user's input. There are two main types of buffer overflow attacks: stack based and heap based. Heap-based attacks flood the memory space reserved for a program, but the difficulty involved with performing such an attack makes them rare. Stack-based buffer overflows are by far the most common.

In a stack-based buffer overrun, the program being exploited uses a memory object known as a stack to store user input. Normally, the stack is empty until the program requires user input. At that point, the program writes a return memory address to the stack and then the user's input is placed on top of it. When the stack is processed, the user's input gets sent to the return address specified by the program.

3rd Part:

A buffer overflow attack requires two things. First, a buffer overflow must occur in the program. Second, the attacker must be able to use the buffer overflow to overwrite a security sensitive piece of data (a security flag, function pointer, return address, etc).

If we want to prevent buffer overflows completely we must stop one of these two things, i. e. either:

1. Prevent all buffer overflows or
2. Prevent all sensitive information from being overwritten

Both these solutions are costly in terms of efficiency and many programs therefore settle for a partial goal, such as:

- Prevent use of dangerous functions: gets, strcpy, etc.
- Prevent return addresses from being overwritten
- Prevent data supplied by the attacker from being executed (stops the attacker from jumping into his own buffer)

There are several possible levels where a defense mechanism can be inserted. At the language level we can make changes to the C language itself to reduce the risk of buffer overflows. At the source code level we can use static or dynamic source code analyzers to check our code for buffer overflow problems. At the compiler level we can change the compiler so that it does bounds checking or protects certain addresses from overwriting. At the operating system level we can change the rules for which memory pages that should be allowed to hold executable content.

2. a) Define Cyberstalking. How stalking works? [MODEL QUESTION]

Answer:

1st part:

Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyberstalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. Cyberstalking messages differ from ordinary spam in that a cyberstalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

2nd part:

Cyber stalking works in many ways, depending on the technological capabilities of the cyber stalker.

- Multiple stalker utilize the services provided on the internet.
- Through Datafurnishing companies that provide information on a person's capability to function in a society.
- There are several other methods used by the cyber stalkers to stalk their victims
  - Spyware software
  - Phising
  - Juice Jacking
  - Wi-Fi interface (Jacking)
  - Caller ID Spoofing

b) Explain the different attacks launched with attack vector. [MODEL QUESTION]

Answer:

An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Just like we don't know whom we're up against, we don't always know what we're up against. There are different attack vectors, and we must have protection against any and all of them, before we can be secure. Here are some examples.

- **Social engineering** involves using social skills to obtain or compromise information. For instance, an attack can involve claiming to be a new employee, a friend stranded on vacation in need of money, a researcher or an acquaintance. Many times, they offer credentials and other information to make themselves appear more legitimate and support their identity. Phishing attacks are a form of social engineering attacks.
- **Brute force attacks** involve a trial-and-error method used to get information such as a PIN or password. In this type of attack, an automated software generates several consecutive guesses to try to isolate the correct solution. These attacks can be used by hackers to decrypt data, or by a security analysis team to test network security. These attacks are both time and resource consuming. When successful, they are usually based on computer power and the number of combinations tried, rather than an algorithm.
- **Distributed Denial of Service (DDoS)** involves using multiple compromised systems, typically infected with a Trojan to target a single system to cause a denial of service, or DDoS, attack. It floods the server with incoming traffic, which overwhelms it, shuts it down, and renders the website or online service useless for visitors. Since the flood of traffic comes from multiple sources, solving it is not as simple as blocking an IP address.
- **Cross-site scripting (XSS)** is a type of code injection attack. This happens by incorrectly validating user data, inserted on a page via an altered link or web form. The code can be injected can be any malicious client-side code, such as Flash, CSS, HTML, JavaScript, VBScript, and the like. These happen when

developers don't take proper measures to secure their code. PHP developers must be diligent in knowing how attacks can be carried out to ensure they address potential vulnerabilities.

c) What is Cyberbullying? **[MODEL QUESTION]**

Answer:

Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

Examples of cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

3. What are the phases of hacking? **[MODEL QUESTION]**

Answer:

Hacking can be organized into five phases reconnaissance, scanning, gaining access, maintaining access and covering tracks.

Reconnaissance means gathering of information without the knowledge of the person. It involves active and passive reconnaissance of the target machine. Gathering account information, identifying operating system, name and version of OS, getting IP and hostname of the machine. Passive information gathering may involve sniffing network traffic and filtering information from messages. Active reconnaissance is finding open ports, names by asking information from network although chances of getting caught are more.

Reconnaissance phase is elaborated in scanning. The information gathered during first phase is used extensively here. User accounts, IP, hostnames, installed applications etc are obtained in this phase. There are three types of scanning like port scanning, network scanning, and vulnerability scanning. In port scanning open ports and services are checked. In network scanning IP addresses are obtained. In vulnerability scanning, names and versions of OS and installed applications and their weaknesses are scanned. All starts with probing into network and looking for active hosts, once they are found IP address, hostname is obtained. Then OS finger printing is carried out looking for version and type of OS. Once it is determined installed applications and open ports are scanned. This can be done actively and passively. Scanning tools like TCP scan, TCP ping, UDP scan, SYN, XMAS tree scan tools use port scanning mechanism by setting FLAGS for normal communication and easily capture any open port. Hackers use these tools to find any response from open ports of unsuspecting hosts and establish connection like a normal machine. Properly installed and configured firewalls and intrusion detection system (IDS) can check active port scanning. One such scanning method is war dialing technique which is used to gain access to a remote modem and network. Hackers starts enumeration for obtaining user names, groups, services, network resources, NETBIOS names, file ownerships and permissions after scanning and gathering information.

In the third phase hackers uses this account information to gain access to the system. Gaining access includes Denial of Service attack (DOS), brute force attack etc. First they crack passwords either manually or using password cracking tools. Then they exploit the applications. Finally they hide the applications, create backdoors to maintain access to the system anonymously. Last phase of maintaining continued access is by covering all the tracks and disabling the firewall. They normally delete the system log files and any related information that can grow any suspicion.

4. What are the different types of hackers? **[MODEL QUESTION]**

Answer:

Computers and the Internet have changed the work environment of the world beyond imagination. Computers on taking over a major part of our lives, all our data has got transferred from records and ledgers to computers. Though this kind of shift in working has reduced the physical burden on workers it has also increased the chances of data theft. People involved in stealing data or harming the systems are knowledgeable people with wrong intentions known as Hackers. There are different types of hackers. Let's take a look at how many types of hackers are there and the types of hacker attacks and techniques.

1. **White Hat Hackers**
2. **Black Hat Hackers**
3. **Gray Hat Hackers**
4. **Script Kiddies**
5. **Green Hat Hackers**
6. **Blue Hat Hackers**
7. **Red Hat Hackers**
8. **State/Nation Sponsored Hackers**
9. **Hacktivist**
10. **Malicious insider or Whistleblower**

1) White Hat Hackers: White hat hackers are types of hackers who're professionals with expertise in cyber security. They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system. They hack the system from the loopholes in the cyber security of the organization. This hacking is done to test the level of cyber security in their organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. White hat hackers work as per the rules and regulations set by the government. White hat hackers are also known as ethical hackers.

Motives & Aims: The goals of these types of hackers are helping businesses and an appetite for detecting gaps in networks' security. They aim to protect and assist companies in the ongoing battle against cyber threats. A White Hat hacker is any individual who will help protect the company from raising cyber crimes. They help enterprises create defences, detect vulnerabilities, and solve them before other cybercriminals can find them.

2) Black Hat Hackers: Black hat hackers are also knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry. On gaining entry they might steal the data or destroy the system. The hacking practices used by these types of hackers depend on the individual's hacking capacity and knowledge. As the intentions of the hacker make the hacker a criminal. The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking.
Motives & Aims: To hack into organizations' networks and steal bank data, funds or sensitive information. Normally, they use the stolen resources to profit themselves, sell them on the black market or harass their target company.

3) Gray Hat Hackers: The intention behind the hacking is considered while categorizing the hacker. The Gray hat hacker falls in between the black hat hackers and white hat hackers. They are not certified, hackers. These types of hackers work with either good or bad intentions. The hacking might be for their gain. The intention behind hacking decides the type of hacker. If the intention is for personal gain then the hacker is considered to be a gray hat hacker.
Motives & Aims: The difference is, they don't want to rob people nor want to help people in particular. Rather, they enjoy experimenting with systems to find loopholes, crack defenses, and generally find a fun hacking experience.

4) Script Kiddies: It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateurs types of hackers in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites. The intention behind the hacking is just to get attention from their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.
Motives & Aims: One standard Kiddie Script attack is a DoS (Denial of Service) or DDoS attack (Distributed Denial of Service). This simply means that an IP address is flooded with too many excessive traffic that it collapses. Consider several Black Friday shopping websites, for instance. It creates confusion and prevents someone else uses the service.

5) Green Hat Hackers: Green hat hackers are types of hackers who're learning the ropes of hacking. They are slightly different from the Script Kiddies due to their intention. The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.

6) Blue Hat Hackers: Blue Hat Hackers are types of hackers who're similar to Script Kiddies. The intent to learn is missing. They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries. Blue Hat Hackers are dangerous due to the intent behind the hacking rather than their knowledge.

7) Red Hat Hackers: Red Hat Hackers are synonymous with Eagle-Eyed Hackers. They are the types of hackers who're similar to white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is in the process of hacking through intention remains the same. Red hat hackers are quite ruthless while dealing with black hat hackers or counteracting with malware. The red hat hackers continue to attack and may end up having to replace the entire system set up.

Above are 7 types of hackers broadly referred to in the cybersecurity world.

The three types of hackers listed below work in different capacities.

8) State/Nation Sponsored Hackers: Government appoints hackers to gain information about other countries. These types of hackers are known as State/Nation sponsored hackers. They use their knowledge to gain confidential information from other countries to be well prepared for any upcoming danger to their country. The sensitive information aids to be on top of every situation but also to avoid upcoming danger. They report only to their governments.

9) Hacktivist: These types of hackers intend to hack government websites. They pose themselves as activists, so known as a hacktivist. Hacktivist can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks. The data gained from government files accessed are used for personal political or social gain.

10) Malicious insider or Whistleblower: These types of hackers include individuals working in an organization who can expose confidential information. The intent behind the exposure might be a personal grudge with the organization or the individual might have come across the illegal activities within the organization. The reason for expose defines the intent behind the exposure. These individuals are known as whistleblowers.

5. What are different types of cyber security threat? [MODEL QUESTION]

Answer:

Just as some germs and diseases can attack the human body, numerous threats can affect hardware, software, and the information you store. Some of the major ones include the following:

- **Viruses** are designed so that they can be easily transmitted from one computer or system to another. Often sent as email attachments, viruses corrupt and co-opt data, interfere with your security settings, generate spam, and may even delete content.
- **Computer worms** are similar; they spread from one computer to the next by sending themselves to all of the user's contacts and subsequently to all contacts' contacts.
- **Trojans** are malicious pieces of software insert themselves into a legitimate program. Often, people voluntarily let trojans into their systems in email messages from a person or an advertiser they trust. As soon as the accompanying attachment is open, your system becomes vulnerable to the malware within.

- **Bogus security software** that tricks users into believing that their system has been infected with a virus. The accompanying security software that the threat actor provides to fix the problem causes it.
- **The adware** tracks your browsing habits and causes particular advertisements to pop up. Although this is common and often something you may even agree to, adware is sometimes imposed upon you without your consent.
- **Spyware** is an intrusion that may steal sensitive data such as passwords and credit card numbers from your internal systems.
- **A denial of service (DOS) attack** occurs when hackers deluge a website with traffic, making it impossible to access its content. A distributed denial of service (DDOS) attack is more forceful and aggressive since it is initiated from several servers simultaneously. As a result, a DDOS attack is harder to mount defenses against it.
- **Phishing attacks** are social engineering infiltrations whose goal is to obtain sensitive data: passwords and credit card numbers incorrectly. Via emails or links coming from trusted companies and financial institutions, the hacker causes malware to be downloaded and installed.
- **SQL injections** are network threats that involve using malicious code to infiltrate cyber vulnerabilities in data systems. As a result, data can be stolen, changed, or destroyed.
- **Man-in-the-middle attacks** involve a third party intercepting and exploiting communications between two entities that should remain private. Eavesdropping occurs, but information can be changed or misrepresented by the intruder, causing inaccuracy and even security breaches.
- **Rootkit tools** gain remote access to systems without permission and can lead to the installation of malware and the stealing of passwords and other data.

6. What are different types of malware? **[MODEL QUESTION]**

Answer:

Malware is an inclusive term for all types of malicious software. Malware examples, malware attack definitions and methods for spreading malware include:

Adware – While some forms of adware may be considered legitimate, others make unauthorized access to computer systems and greatly disrupt users.

Botnets – Short for "robot network," these are networks of infected computers under the control of single attacking parties using command-and-control servers. Botnets are highly versatile and adaptable, able to maintain resilience through redundant servers and by using infected computers to relay traffic. Botnets are often the armies behind today's distributed denial-of-service (DDoS) attacks.

Cryptojacking – is malicious cryptomining (the process of using computing power to verify transactions on a blockchain network and earning cryptocurrency for providing that service) that happens when cybercriminals hack into both business and personal computers, laptops, and mobile devices to install software.

Malvertising – Malvertising is a portmanteau of "malware + advertising" describing the practice of online advertising to spread malware. It typically involves injecting malicious code or malware-laden advertisements into legitimate online advertising networks and webpages.

Polymorphic malware – Any of the above types of malware with the capacity to "morph" regularly, altering the appearance of the code while retaining the algorithm within. The alteration of the surface appearance of the software subverts detection via traditional virus signatures.

Ransomware – Is a criminal business model that uses malicious software to hold valuable files, data or information for ransom. Victims of a ransomware attack may have their operations severely degraded or shut down entirely.

Remote Administration Tools (RATs) – Software that allows a remote operator to control a system. These tools were originally built for legitimate use, but are now used by threat actors. RATs enable administrative control, allowing an attacker to do almost anything on an infected computer. They are difficult to detect, as they don't typically show up in lists of running programs or tasks, and their actions are often mistaken for the actions of legitimate programs.

Rootkits – Programs that provide privileged (root-level) access to a computer. Rootkits vary and hide themselves in the operating system.

Spyware – Malware that collects information about the usage of the infected computer and communicates it back to the attacker. The term includes botnets, adware, backdoor behavior, keyloggers, data theft and net-worms.

Trojans Malware – Malware disguised in what appears to be legitimate software. Once activated, malware Trojans will conduct whatever action they have been programmed to carry out. Unlike viruses and worms, Trojans do not replicate or reproduce through infection. "Trojan" alludes to the mythological story of Greek soldiers hidden inside a wooden horse that was given to the enemy city of Troy.

Virus Malware – Programs that copy themselves throughout a computer or network. Malware viruses piggyback on existing programs and can only be activated when a user opens the program. At their worst, viruses can corrupt or delete data, use the user's email to spread, or erase everything on a hard disk.

Worm Malware – Self-replicating viruses that exploit security vulnerabilities to automatically spread themselves across computers and networks. Unlike many viruses, malware worms do not attach to existing programs or alter files. They typically go unnoticed until replication reaches a scale that consumes significant system resources or network bandwidth.

7. Write short notes on the following: **[MODEL QUESTION]**

a) Active attacks
b) Hacking Cybercrime
c) Cyber stalking
d) Worms
e) Trojans
f) Backdoors

Answer:

a) Active attacks:

An active attack is an attempt "to alter system resources or affect their operation." It includes the falsification of data and transactions through such means as: (1) alteration, deletion, or addition; (2) changing the apparent origin of the message; (3) changing the actual destination of the message; (4) altering the sequence of blocks of data or items in

the message; (5) replaying previously transmitted or stored data to create a new false message; or (6) falsifying an acknowledgement for a genuine message.
An active attack is "[a]n attack on the authentication protocol where the attacker transmits data to the claimant or verifier. Examples of active attacks include a man-in-the-middle, impersonation, and session hijacking."

b) Hacking Cybercrime:
In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking. The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks.
There are many definitions of hacking. Here we will define hacking as identifying weakness in computer systems and/or networks and exploiting the weaknesses to gain access. An example of hacking is using by passing the login algorithm to gain access to a system. A hacker is a person who finds and exploits weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.
Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

c) Cyber stalking:
Cyber stalking is the means by which a person is harassed over Internet, mobile phone, SMS, email. This can range from mere annoyance to serious crimes. According to some" Cyber stalking involves a disturbed obsession with the target, and a perverse desire to control that target in some way, even by attacking the target's family members." Cyber stalkers can interfere into someone's life by means of modern telecommunication medium. They choose any persons at random. Most of the potential target belong s to women, children, teenagers. Cyber stalkers can target an individual or a group. These kind of stalkers want ultimate submission from their victims. By hacking into someone's Internet activity such as email, Facebook or any social media they can even threat or blackmail to the victims existence. These cyber bullies can even use children for offensive actions. Cyber stalking uses same techniques as the hackers but researches about victims likes and dislikes and uses against them. In India Criminal Law (Ammendment) Bill of 2013 includes law for handling cyber stalking. Section 66A of IT act deals with such kind of offenses. In section 354D - "anyone who monitors an individual's electronic communication and causes fear or distress is guilty of stalking, just as they are if they follow or attempt to contact them in the real world. The offender could get a fine and three years in jail. "Although there is no organized law against cyber stalking still it is considered as a serious offense.

d) Worms:

A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.

Worms can be transmitted via software vulnerabilities. Or computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it's installed, the worm silently goes to work and infects the machine without the user's knowledge.

Worms can modify and delete files, and they can even inject additional malicious software onto a computer. Sometimes a computer worm's purpose is only to make copies of itself over and over — depleting system resources, such as hard drive space or bandwidth, by overloading a shared network. In addition to wreaking havoc on a computer's resources, worms can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings.

If you suspect your devices are infected with a computer worm, run a virus scan immediately. Even if the scan comes up negative, continue to be proactive by following these steps.

1. **Keep an eye on your hard drive space.** When worms repeatedly replicate themselves, they start to use up the free space on your computer.
2. **Monitor speed and performance.** Has your computer seemed a little sluggish lately? Are some of your programs crashing or not running properly? That could be a red flag that a worm is eating up your processing power.
3. **Be on the lookout for missing or new files.** One function of a computer worm is to delete and replace files on a computer.

e) Trojans:

The name of the **Trojan Horse** is taken from a classical story of the Trojan War. It is a code that is malicious in nature and has the capacity to take control of the computer. It is designed to steal, damage, or some harmful actions in the computer. It tries to deceive the user to load and execute the files on the device. After it executes, this allows cyber criminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more. Now like many viruses or worms, Trojan Horse does not have the ability to replicate itself.

For example:

There was a Trojan that disguised itself as a game. Many users have downloaded this game and that secretly turned into a self-replicating virus. The game was a simple theme based game, but it started to back up all the files of the drive where the user would access them. The Trojan turned to be harmless, and it was easy for them to fix. So this was identified as Trojan because it did not disclose the virus.

Now after this many Trojan viruses or Malware came which turned out to be a threat or the most popular malware attack. As these Trojans can be found as versatile, this is used by many Online Criminals for malware attacks. The Trojans are a bit tougher to be identified. Trojans can be found in MP3 songs that the user may have downloaded, or

downloading games from an unsecured website, or the advertisement that pops up when the user is browsing the page.
Many people have been infected by Trojans without realizing it. This type of Trojans is called Direct-Action-Trojans. It can't spread to any user because when a virus infects the system show some indications that it has been affected by the virus.
For example:, there is a direct action Trojan name Js. ExitW. It can be downloaded from many malicious sites. The effect of the Js. ExitW is to make the computer fall in a never-ending loop of start and shutdown. The Trojan does not do any damage which could be considered dangerous. But we should be aware that there are many Trojans that are far more dangerous.

Some features of the Trojan horse are as follows:

- It steals information like a password and more.
- It can be used to allow remote access to a computer.
- It can be used to delete data and more on the user's computers.

There are many ways that it can be used:
1. Spy – Some Trojans act as spyware. It is designed to take the data from the victim like social networking(username and the passwords), credit card details, and more.
2. Creating backdoors – The Trojan makes some changes in the system or the device of the victim, So this is done to let other malware or any cyber criminals get into your device or the system.
3. Zombie – There are many times that the hacker is not at all interested in the victim's computer, but they want to use it under their control.

Now there are many Trojans which is designed to perform specific functions. Some of them are: –
1. Trojan-Banker – It is designed to steal the account data for online banking, credit and debit cards, etc.
2. Trojan_Downloader – It is designed to download many malicious files like the new versions of Trojan and Adware into the computer of the victims.
3. Trojan-Dropper – It is designed to prevent the detection of malicious files in the system. It can be used by hackers for installing Trojans or viruses in the victim's computers.
4. Trojan-GameTheif – It is designed to steal data from Online Gamers.
5. Trojan-I's – It is designed to steal the data of login and passwords like: -a. skype b. yahoo pager and more.
Other Trojans can be also be used like: -Trojan-notifier, Trojan-clicker, and more.

Indications that the system has been affected by the virus:

- First the system or the device where it has been affected will be slow.
- The user will experience the files to be opening much slower.
- The user can also experience a direct shutdown of the pc.

Advantage of the Trojan Horse:

- It can be sent as an attachment in an email.
- It can be in some pop-up ads that we find on the web page.

Disadvantages of the Trojan Horse:

- It can't manifest by itself. It requires the implementation of the .exe files.
- It remains undetected and starts its execution when the user is doing any online transaction activity.

f) Backdoors:

The backdoor attack is a type of malware that is used to get unauthorized access to a website by the cybercriminals. The cybercriminals spread the malware in the system through unsecured points of entry, such as outdated plug-ins or input fields. The malware is entered in the system through the backdoor and it makes it ways to the company's sensitive data including customer personally identifiable information.

Smaller and middle-sized businesses are usually attacked by the backdoor attack as they have fewer resources to close off entry points and identify successful attacks. SMBs often lack resources like budget and security experts to prevent and mitigate attacks. In backdoor attacks, the business usually remains unaware of the attack as the name suggests the attack is made from the backdoor.

- **The Consequences of Backdoor Attacks on Small Businesses**

Small businesses are always at high risk of security breaches or attacks. They need to take proactive measures to secure their websites and prevent backdoor attacks to avoid the financial fallout of successful breaches. A data breach cost may exceed $100,000 for smaller businesses that do not include a high price tag with repairing reputation and rebuilding customer trust.

Backdoor attacks have been increased in the last two years as the problem is getting worse as detecting it is becoming more difficult. Cybercriminals are using different new techniques and strains of malware that can bypass malware scanners easily without detection. The more a malware remains undetected in a system the more damage it causes to the business.

- **How to Prevent Backdoor Attacks**

Business owners can use website scanners to defend themselves against backdoor attacks. The website scanners mitigate malware, patch vulnerabilities and alert the administrator against threats.

Make sure your cybersecurity team performs adequate research to detect and review new types of malware daily. They are using updated tools to detect malware. Install a web application firewall to protect your website from malicious actors.

- **What to Do If You Suspect a Backdoor Attack**

Firms should take some immediate action if they suspect a backdoor attack to keep costs and reputational damage.

- Make sure the cybersecurity team reviews the site access logs for everything out of ordinary.
- Keep the plug-ins and themes on the websites updated and reinstall the core files to your CMS.
- Audit your CMS and uninstall all the plug-ins from the file manager.

ETHICAL HACKING & SOCIAL ENGINEERING

Multiple Choice Type Questions

1. What is the ethics behind training how to hack a system? [MODEL QUESTION]
   a) To think like hackers and know how to defend such attacks
   b) To hack a system without the permission
   c) To hack a network that is vulnerable
   d) To corrupt software or service using malware

Answer: (a)

2. Performing a shoulder surfing in order to check other's password is _____ ethical practice. [MODEL QUESTION]
   a) a good
   b) not so good
   c) very good social engineering practice
   d) a bad

Answer: (d)

3. _____ has now evolved to be one of the most popular automated tools for unethical hacking. [MODEL QUESTION]
   a) Automated apps
   b) Database software
   c) Malware
   d) Worms

Answer: (c)

4. _____ is the technique used in business organizations and firms to protect IT assets. [MODEL QUESTION]
   a) Ethical hacking
   b) Unethical hacking
   c) Fixing bugs
   d) Internal data-breach

Answer: (a)

5. The legal risks of ethical hacking include lawsuits due to _____ of personal data. [MODEL QUESTION]
   a) stealing
   b) disclosure
   c) deleting
   d) hacking

Answer: (b)

6. Before performing any penetration test, through legal procedure, which key points listed below is not mandatory? [MODEL QUESTION]
   a) Know the nature of the organization
   b) Characteristics of work done in the firm
   c) System and network
   d) Type of broadband company used by the firm

Answer: (d)

7. After performing _____ the ethical hacker should never disclose client information to other parties. [MODEL QUESTION]
   a) hacking
   b) cracking
   c) penetration testing
   d) exploiting

Answer: (d)

8. _____ is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong. [MODEL QUESTION]

a) Social ethics
b) Ethics in cyber-security
c) Corporate ethics
d) Ethics in black hat hacking

Answer: (d)

9. _____ helps to classify arguments and situations, better understand a cyber-crime and helps to determine appropriate actions. [MODEL QUESTION]

a) Cyber-ethics
b) Social ethics
c) Cyber-bullying
d) Corporate behavior

Answer: (a)

10. A penetration tester must identify and keep in mind the _____ & _____ requirements of a firm while evaluating the security postures. [MODEL QUESTION]

a) privacy and security
b) rules and regulations
c) hacking techniques
d) ethics to talk to seniors

Answer: (a)

11. Which of the following do not comes under Social Engineering? [MODEL QUESTION]

a) Tailgating
b) Phishing
c) Pretexting
d) Spamming

Answer: (d)

12. In a phishing, attackers target the _____ technology to so social engineering. [MODEL QUESTION]

a) Emails
b) WI-FI network
c) Operating systems
d) Surveillance camera

Answer: (a)

13. Which of the following is not an example of social engineering? [MODEL QUESTION]

a) Dumpster diving
b) Shoulder surfing
c) Carding
d) Spear phishing

Answer: (c)

14. Social engineering can be thwarted using what kinds of controls? [MODEL QUESTION]

a)Technical
b) Administrative
c) Physical
d) Proactive controls

Answer: (a,b,c)

15. Social engineering preys on many weakness, including **[MODEL QUESTION]**
a) Technology **b) People** **c) Human Nature** **d) Physical**
Answer: (a,b,c,d)

16. Social engineering can use all the following except **[MODEL QUESTION]**
a) Mobile phones **b) Instant messaging**
c) Trojan horses **d) viruses**
Answer: (d)

17. Social engineering is designed to _____ **[MODEL QUESTION]**
a) Manipulate human behaviour **b) Make people distrustful**
c) Infect a system **d) Gain a physical advantage**
Answer: (a)

18. What is the best option for thwarting social-engineering attacks? **[MODEL QUESTION]**
a) Technology **b) Training** **c) Policies** **d) Physical controls**
Answer: (b)

19. In social engineering a proxy is used to **[MODEL QUESTION]**
a) Assist in scanning
b) Perform a scan
c) Keep an attacker's origin hidden
d) Automate the discovery of vulnerabilities
Answer: (c)

20. Social engineering can be used to carry out email campaigns known as _____ **[MODEL QUESTION]**
a) Spamming **b) Phishing** **c) Vishing** **d) Splashing**
Answer: (b)

21. Now a days Phishing has become a criminal practice of using social engineering over which of the following? **[MODEL QUESTION]**
a) Social networking sites **b) Mobile Phones**
c) E-mail **d) Cyber cafes**
Answer: (b)

Short Answer Type Questions

1. What is purpose of ethical hacking? **[MODEL QUESTION]**
Answer:
Ethical Hacking is also called as penetration Testing. It is an act of penetrating networks or systems to find out threats and vulnerabilities in that system which the attacker would have exploited and caused the loss of data, financial loss or other major damages to a business.

The purpose of Ethical hacking is to build the security of the system or network by settling the vulnerabilities which are detected while testing. Ethical hackers may use the same techniques and mechanisms used by malicious hackers but with the permission of the authorized person, the Ethical hackers help to develop the security and defend the systems from attacks.

2. Why Ethical Hacking is important? **[MODEL QUESTION]**

Answer:

When the Ethical hacker finds a vulnerability, he will inform the issues and advise how to fix the problem. The company employs an Ethical hacker to protect and secure their data. The Ethical hacker's tests do not always mean a system is attacked by malicious attackers. Sometimes, it means the hacker is preparing and protecting their data in precaution. Some of the advanced attacks caused by hackers include:-

- Piracy
- Vandalism
- Credit card theft
- Theft of service
- Identity theft
- Manipulation of data
- Denial-of-service Attacks

These types of cyber attacks, hacking cases are increased because of the huge usage of online services and online transactions in the last decade.

3. What are skills of an ethical hacking? **[MODEL QUESTION]**

Answer:

A skilled Ethical Hacker should hold a collection of technical and non-technical skills.

Technical Skills:

- The Ethical Hackers must have strong knowledge in all Operating Systems like Windows, Linux, and Mac.
- The Ethical Hackers should be skilled with Networking and have a strong knowledge of basic and detailed concepts in technologies, software, and hardware applications.
- Ethical Hackers must know all kinds of attacks.

Non-Technical Skills:

- Communication Skills
- Learning Ability
- Problem-solving skills
- Proficient in the security policies
- Awareness of laws, standards, and regulations.

4. What is Scope of Ethical Hacking? **[MODEL QUESTION]**

Answer:
Ethical hacking is generally used as penetration testing to detect vulnerabilities, risk and identify the loopholes in a security system and to take corrective measures against those attacks.
Ethical hacking is a key component of risk evaluation, auditing, and counter-frauds. The scope for the Ethical Hackers is high and it is one of the rapidly growing careers at present as many malicious attackers cause a threat to the business and its networks. Industries like Information Technology and Banking Sectors hire several Ethical hackers to protect their data and infrastructure. Also, in the upcoming days, the demand for this profile is going to be high compared to other profiles due to an increased threat of vulnerabilities.

5. What is an attack vector? **[MODEL QUESTION]**
Answer:
An attack vector is a path or means by which an attacker or hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
Common cyber attack vectors include viruses and malware, email attachments, webpages, pop-up windows, instant messages (IMs), chatrooms and deception. Except for deception, all of these methods involve programming or, in a few cases, hardware. Deception is when a human operator is fooled into removing or weakening system defenses.
To some extent, firewalls and antivirus software can block attack vectors. But no protection method is totally attack-proof. A defense method can quickly become obsolete, as hackers are constantly updating attack vectors and seeking new ones in their quest to gain unauthorized access to computers and servers.
The most common malicious payloads are viruses, which can function as their own attack vectors, Trojan horses, worms and spyware. Third-party vendors and service providers can also be considered attack vectors, as they are a risk to an organization if they have access to its sensitive data.

6. What is Threat Modeling? **[MODEL QUESTION]**
Answer:
Threat modeling is a method of optimizing network security by locating vulnerabilities, identifying objectives, and developing countermeasures to either prevent or mitigate the effects of cyber-attacks against the system.
While security teams can conduct threat modeling at any point during development, doing it at the start of the project is best practice. This way, threats can be identified sooner and dealt with before they become an issue.

7. What is insider threat? **[MODEL QUESTION]**

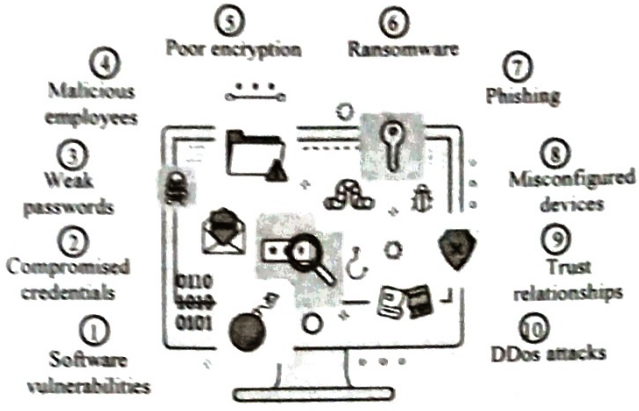
Answer:
An insider threat is a malicious activity against an organization that comes from users with legitimate access to an organization's network, applications or databases. These users can be current employees, former employees, or third parties like partners, contractors, or temporary workers with access to the organization's physical or digital assets. While the term is most commonly used to describe illicit or malicious activity, it can also refer to users who unintentionally cause harm to the business.
There are several types of insider threats:

- **Malicious Insider**—an employee or contractor who knowingly looks to steal information or disrupt operations. This may be an opportunist looking for ways to steal information that they can sell or which can help them in their career, or a disgruntled employee looking for ways to hurt an organization, punish or embarrass their employer. An example of a malicious insider are the various Apple engineers who were charged with data theft for stealing driverless car secrets for a China-based company.
- **Negligent Insider**—an employee who does not follow proper IT procedures. For example, someone who leaves their computer without logging out, or an administrator who did not change a default password or failed to apply a security patch. An example of a negligent insider is the data analyst who, without authorization, took home a hard drive with personal data from 26.5 million U.S. military veterans, that was stolen in a home burglary.
- **Compromised Insider**—a common example is an employee whose computer has been infected with malware. This typically happens via phishing scams or by clicking on links that cause malware downloads. Compromised insider machines can be used as a "home base" for cybercriminals, from which they can scan file shares, escalate privileges, infect other systems, and more. As is the case of the recent Twitter breach where attackers used a phone spear phishing attack to gain access to employee credentials and their internal network. The attackers managed to gain information about Twitter's processes and target employees with access to account support tools to hack high-profile accounts and spread a crypto currency scam that earned $120,000.

Long Answer Type Questions

1. What are most common attack vectors? **[MODEL QUESTION]**

Answer:



10 common attack vectors

Intruders are continuously seeking out new attack vectors. The most common attack vectors include the following:

1. Software vulnerabilities: If a network, OS, computer system or application has an unpatched security vulnerability, an attacker can use a threat vector, such as malware, to gain unauthorized access.

2. Compromised user credentials: Users can knowingly or inadvertently share their user IDs and passwords. This can be done verbally, but cyber attackers can also gain access to credentials through a brute-force attack that tries different combinations of user IDs and passwords until an authorized set of credentials is uncovered. The hacker then uses these credentials to hack a network, system or application.

3. Weak passwords and credentials: In brute-force attacks, cyber attackers focus their efforts on hacking user IDs and passwords that are weak or can be easily guessed. But hackers also steal credentials by using programs that monitor public Wi-Fi networks for when users input their access credentials. For example, a hacker could install keylogging software on a user's workstation through an infected website or email. The keylogging program logs user keyboard activity, including the entry of the user's ID and password. Hackers can also gain access by enticing users to open unsolicited email attachments that contain malicious links to bogus websites that convince them to surrender personally identifiable information (PII).

4. Malicious employees: Malicious or disgruntled employees can hack into networks and systems using their security clearances to extract sensitive information, such as customer lists and intellectual property (IP) that they either demand ransom for or sell to others for nefarious purposes.

5. Poor or missing encryption: In some cases, employees -- or IT -- may forget to encrypt sensitive information stored on laptops and smartphones out in the field. In other cases, encryption techniques have known design flaws or only use limited keys to encrypt and protect data.

6. Ransomware: Ransomware is a type of malware that locks the data on the victim's computer, and the attacker either threatens to publish the victim's data or block access to it unless a ransom is paid. Ransomware can lock a user's files, often demanding a cash sum from the user in order to unlock the files. Most ransomware is inadvertently downloaded onto a computer or network by a user. It can come in the form of a file that a user opens that contains a worm, which is malware that spreads itself throughout a network, or a Trojan, which embeds malicious software code in a downloaded file that locks up the user's computer or data and then demands payment.

7. Phishing: Phishing is the deceptive practice of sending emails in which the attacker purports to be from a reputable company in order to lure individuals into revealing personal information, such as passwords or credit card numbers. Spear phishing is a highly targeted attack that targets a single recipient, seeking unauthorized access to sensitive company information.

8. Misconfigured devices: Companies can misconfigure their software and hardware security, which leaves them vulnerable to hackers. Vendor security presets on equipment are lax, and if IT doesn't reconfigure this equipment before installing it on networks, security hacks can occur. In still other cases, companies purchase equipment and forget to fully configure security.

9. Trust relationships: In many cases, companies entrust their security to outside system and network vendors, cloud providers and business partners. When the systems of these third parties are breached, the information the hackers obtain may also contain sensitive information from the companies these providers service. Examples include when a major credit card carrier's network is breached or when a healthcare system is breached and sensitive data from patients is stolen.

10. Distributed denial-of-service (DDoS) attacks: DDoS attacks flood victims with bogus emails, rendering their system or network unusable and services unavailable to their intended recipients. These attacks often target the web servers of finance, commerce and government organizations and are often used to distract an organization from other network attacks.

2. Explain Information Assurance Model in Cyber Security. [MODEL QUESTION]

Answer:

Information Assurance concerns implementation of methods that focused on protecting and safeguarding critical information and relevant information systems by assuring confidentiality, integrity, availability, and non-repudiation. It is strategic approach focused which focuses more on deployment of policies rather than building infrastructures.

Information Assurance Model:

The security model is multidimensional model based on four dimensions:

1. Information States –

Information is referred to as interpretation of data which can be found in three states stored, processed, or transmitted.

2. Security Services –

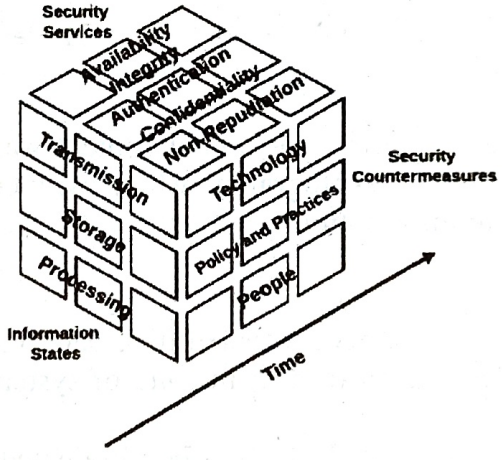
It is fundamental pillar of the model which provides security to system and consists of five services namely availability, integrity, confidentiality, authentication, and non-repudiation.

3. Security Countermeasures –

This dimension has functionalities to save system from immediate vulnerability by accounting for technology, policy & practice, and people.

4. Time –

This dimension can be viewed in many ways. At any given time data may be available offline or online, information and system might be in flux thus, introducing risk of unauthorized access. Therefore, in every phase of System Development Cycle, every aspect of Information Assurance model must be well defined and well implemented in order to minimize risk of unauthorized access.



Information States:

1. Transmission –

It defines time wherein data is between processing steps.

Example:

In transit over networks when user sends email to reader, including memory and storage encountered during delivery.

2. Storage –

It defines time during which data is saved on medium such as hard drive. Example: Saving document on file server's disk by user.

3. Processing –

It defines time during which data is in processing state.

Example:

Data is processed in random access memory (RAM) of workstation.

Security Services:

1. Confidentiality –

It assures that information of system is not disclosed to unauthorized access and is read and interpreted only by persons authorized to do so. Protection of confidentiality prevents malicious access and accidental disclosure of information. Information that is considered to be confidential is called as **sensitive information**.

To ensure confidentiality data is categorized into different categories according to damage severity and then accordingly strict measures are taken.

Example:

Protecting email content to read by only desired set of users. This can be insured by data encryption. Two-factor authentication, strong passwords, security tokens, and biometric verification are some popular norms for authentication users to access sensitive data.

2. Integrity –

It ensures that sensitive data is accurate and trustworthy and cannot be created, changed, or deleted without proper authorization. Maintaining integrity involves modification or destruction of information by unauthorized access.

To ensure integrity backups should be planned and implemented in order to restore any affected data in case of security breach. Besides this cryptographic checksum can also be used for verification of data.

Example:

Implementation of measures to verify that e-mail content was not modified in transit. This can be achieved by using cryptography which will ensure that intended user receives correct and accurate information.

3. Availability –

It guarantees reliable and constant access to sensitive data only by authorized users. It involves measures to sustain access to data in spite of system failures and sources of interference.

To ensure availability of corrupted data must be eliminated, recovery time must be speed up and physical infrastructure must be improved.

Example:

Accessing and throughput of e-mail service.

4. Authentication –

It is security service that is designed to establish validity of transmission of message by verification of individual's identity to receive specific category of information.

To ensure availability of various single factors and multi-factor authentication methods are used. A single factor authentication method uses single parameter to verify users' identity whereas two-factor authentication uses multiple factors to verify user's identity.

Example:
Entering username and password when we log in to website is example of authentication. Entering correct login information lets website verify our identity and ensures that only we access sensitive information.

5. Non-Repudiation –
It is mechanism to ensure sender or receiver cannot deny fact that they are part of data transmission. When sender sends data to receiver, it receives delivery confirmation. When receiver receives message it has all information attached within message regarding sender.
Example:
A common example is sending SMS from one mobile phone to another. After message is received confirmation message is displayed that receiver has received message. In return, message received by receiver contains all information about sender.

Security Counter measures:
1. People –
People are heart of information system. Administrators and users of information systems must follow policies and practice for designing good system. They must be informed regularly regarding information system and ready to act appropriately to safeguard system.
2. Policy & Practice –
Every organization has some set of rules defined in form of policies that must be followed by every individual working in organization. These policies must be practiced in order to properly handle sensitive information whenever system gets compromised.
3. Technology –
Appropriate technology such as firewalls, routers, and intrusion detection must be used in order to defend system from vulnerabilities, threats. The technology used must facilitate quick response whenever information security gets compromised.

3. What are different threat modelling methodologies? [MODEL QUESTION]
Answer:
There are as many ways to fight cybercrime as there are types of cyber-attacks. For instance, here are ten popular threat modeling methodologies used today.
1. STRIDE
A methodology developed by Microsoft for threat modeling, it offers a mnemonic for identifying security threats in six categories:

- Spoofing: An intruder posing as another user, component, or other system feature that contains an identity in the modeled system.
- Tampering: The altering of data within a system to achieve a malicious goal.
- Repudiation: The ability of an intruder to deny that they performed some malicious activity, due to the absence of enough proof.
- Information Disclosure: Exposing protected data to a user that isn't authorized to see it.

- Denial of Service: An adversary uses illegitimate means to exhaust services needed to provide service to users.
- Elevation of Privilege: Allowing an intruder to execute commands and functions that they aren't allowed to.

2. DREAD

Proposed for threat modeling, but Microsoft dropped it in 2008 due to inconsistent ratings. OpenStack and many other organizations currently use DREAD. It's essentially a way to rank and assess security risks in five categories:

- Damage Potential: Ranks the extent of damage resulting from an exploited weakness.
- Reproducibility: Ranks the ease of reproducing an attack
- Exploitability: Assigns a numerical rating to the effort needed to launch the attack.
- Affected Users: A value representing how many users get impacted if an exploit becomes widely available.
- Discoverability: Measures how easy it is to discover the threat.

3. P.A.S.T.A

This stands for Process for Attack Simulation and Threat Analysis, a seven-step, risk-centric methodology. It offers a dynamic threat identification, enumeration, and scoring process. Once experts create a detailed analysis of identified threats, developers can develop an asset-centric mitigation strategy by analyzing the application through an attacker-centric view.

4. Trike

Trike focuses on using threat models as a risk management tool. Threat models, based on requirement models, establish the stakeholder-defined "acceptable" level of risk assigned to each asset class. Requirements model analysis yields a threat model where threats are identified and given risk values. The completed threat model is then used to build a risk model, factoring in actions, assets, roles, and calculated risk exposure.

5. VAST

Standing for Visual, Agile, and Simple Threat modeling, it provides actionable outputs for the specific needs of various stakeholders such as application architects and developers, cybersecurity personnel, etc. VAST offers a unique application and infrastructure visualization plan so that the creation and use of threat models don't require any specialized expertise in security subject matters.

6. Attack Tree

The tree is a conceptual diagram showing how an asset, or target, could be attacked, consisting of a root node, with leaves and children nodes added in. Child nodes are conditions that must be met to make the direct parent node true. Each node is satisfied

only by its direct child nodes. It also has "AND" and "OR" options, which represent alternative steps taken to achieve these goals.

7. Common Vulnerability Scoring System (CVSS)

This method provides a way to capture a vulnerability's principal characteristics and assigning a numerical score (ranging from 0-10, with 10 being the worst) showing its severity. The score is then translated into a qualitative representation (e.g., Low, Medium, High, and Critical). This representation helps organizations effectively assess and prioritize their unique vulnerability management processes.

8. T-MAP

T-MAP is an approach commonly used in Commercial Off the Shelf (COTS) systems to calculate attack path weights. The model incorporates UML class diagrams, including access class, vulnerability, target assets, and affected value.

9. OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) process is a risk-based strategic assessment and planning method. OCTAVE focuses on assessing organizational risks only and does not address technological risks. OCTAVE has three phases:

- Building asset-based threat profiles. (Organizational evaluation)
- Identifying infrastructure vulnerabilities. (Information infrastructure evaluation)
- Developing and planning a security strategy. (Evaluation of risks to the company's critical assets and decision making.)

10. Quantitative Threat Modeling Method

This hybrid method combines attack trees, STRIDE, and CVSS methods. It addresses several pressing issues with threat modeling for cyber-physical systems that contain complex interdependencies in their components. The first step is building components attack trees for the STRIDE categories. These trees illustrate the dependencies in the attack categories and low-level component attributes. Then the CVSS method is applied, calculating the scores for all the tree's components.

4. Explain Enterprise Information Security Architecture. [MODEL QUESTION]

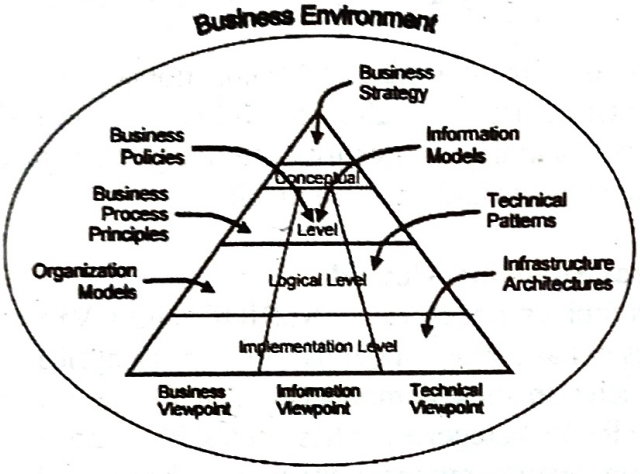
Answer:

Enterprise Information Security Architecture (EISA) is a key component of an information security program. The primary function of EISA is to document and communicate the artifacts of the security program in a consistent manner. As such, the primary deliverable of EISA is a set of documents connecting business drivers with technical implementation guidance. These documents are developed iteratively through multiple levels of abstraction.

Information security should define three dimensions, or viewpoints, into the architecture framework:

- A "**business**" viewpoint that represents the information security organization and process dimensions. This viewpoint reflects the "business of security," in the sense that it represents the way information security is practiced in the organization, as well as how the "security business" interrelates with the rest of the enterprise via processes, roles, responsibilities and organizational structures.
- An "**information**" viewpoint that represents the information required to run the information security function. It represents the information models used by the security team, as well as the models used to capture the security requirements for enterprise information.
- A "**technical**" viewpoint that represents the security infrastructure architectures. It captures the models that are used to abstract varying requirements for security into guidance for required hardware and software configurations.

Security architecture should describe how security is woven into the fabric of the business. For this reason, the EISA should be integrated with the organization's EA. The EISA process must allow inputs from and interface points with design components from other planning disciplines (Figure1). Many of these inputs can be obtained from the EA. Then, as the architecture and security processes mature, the relationship between the EISA and EA should become increasingly symbiotic and integrated.



Contents of EISA

EISA consists of three levels of documents:

1) **Requirements**: Documents that define what the architecture is trying to achieve. At the conceptual layer, this could represent business requirements, such as strategic product plans or regulatory requirements. At the implementation layer, it could represent technology product specifications.

2) **Principles**: Documents containing statements that guide decision making during the architecture process.

3) **Models**: Representations of alternative patterns, or of current and future states. Pattern-based models represent recurring characteristics in business process and applications, and are used as decision making tools. Current- and future-state models are used to improve a shared understanding among stakeholders and in gap analysis for project planning and prioritization.

Different approaches used to implement Security Architecture

The term "security architecture" is used interchangeably to describe a process, a set of deliverables and occasionally also the solutions implemented as a consequence of the process. Enterprise information security architecture (EISA) is the process that delivers planning, design and implementation documentation (artifacts) in support of the information security program.

The EISA process is a dynamic set of planning and design activities. The exact nature of these activities depends on the approach that the organization takes to security architecture. There are three different strategic approaches:

- The **strategic refresh approach**, where the primary function of the architecture is to guide a complete renewal of the enterprise security environment.
- The **opportunistic approach**, where architecture is only used to develop the security requirements for ad hoc projects and initiatives.
- The **hybrid approach**, where architecture is predominantly used in an opportunistic manner, but also selectively for more strategic planning purposes.

5. What is vulnerability testing? Explain the process of vulnerability assessment process. **[MODEL QUESTION]**

Answer:

1st part:

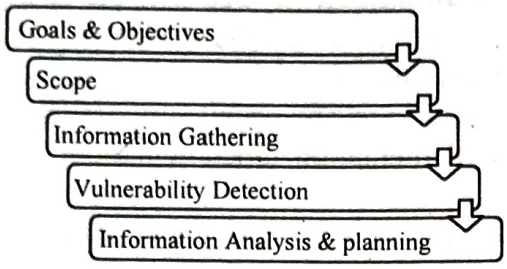
Vulnerability Testing also called Vulnerability Assessment is a process of evaluating security risks in software systems to reduce the probability of threats. The purpose of vulnerability testing is reducing the possibility for intruders/hackers to get unauthorized access of systems. It depends on the mechanism named Vulnerability Assessment and Penetration Testing (VAPT) or VAPT testing.

A vulnerability is any mistake or weakness in the system's security procedures, design, implementation or any internal control that may result in the violation of the system's security policy.

- It is important for the security of the organization.
- The process of locating and reporting the vulnerabilities, which provide a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process Operating systems, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities, which include inappropriate software design, insecure authentication, etc.

2nd part:

Here is the step by step **Vulnerability Assessment Process** to identify the system vulnerabilities.



Step 1) Goals & Objectives – Define goals and objectives of Vulnerability Analysis.
Step 2) Scope – While performing the Assessment and Test, Scope of the Assignment needs to be clearly defined.
The following are the three possible scopes that exist:

- **Black Box Testing** – Testing from an external network with no prior knowledge of the internal network and systems.
- **Grey Box Testing** – Testing from either external or internal networks with the knowledge of the internal network and system. It's the combination of both Black Box Testing and White Box Testing.
- **White Box Testing** – Testing within the internal network with the knowledge of the internal network and system. Also known as Internal Testing.

Step 3) Information Gathering – Obtaining as much information about IT environment such as Networks, IP Address, Operating System Version, etc. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing and White Box Testing.

Step 4) Vulnerability Detection – In this process, vulnerability scanners are used to scan the IT environment and identify the vulnerabilities.

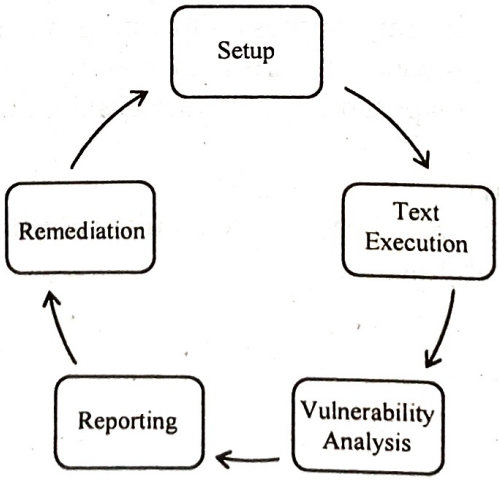
Step 5) Information Analysis and Planning – It will analyze the identified vulnerabilities to devise a plan for penetrating into the network and systems.

6. How to do Vulnerability Assessment? **[MODEL QUESTION]**

Answer:

Step 1) Setup:

- Begin Documentation
- Secure Permissions
- Update Tools
- Configure Tools



Step 2) Test Execution:

- Run the Tools
- Run the captured data packet (A packet is the unit of data that is routed between an origin and the destination. When any file, for example, e-mail message, HTML file, Uniform Resource Locator (URL) request, etc. is sent from one place to another on the internet, the TCP layer of TCP/IP divides the file into a number of "chunks" for efficient routing, and each of these chunks will be uniquely numbered and will include the Internet address of the destination. These chunks are called packets. When all the packets are arrived, they will be reassembled into the original file by the TCP layer at the receiving end while running the assessment tools

Step 3) Vulnerability Analysis:

- Defining and classifying network or System resources.
- Assigning priority to the resources(Ex: – High, Medium, Low)
- Identifying potential threats to each resource.
- Developing a strategy to deal with the most prioritized problems first.
- Defining and implementing ways to minimize the consequences if an attack occurs.

Step 4) Reporting

Step 5) Remediation:

- The process of fixing the vulnerabilities.
- Performed for every vulnerability

7. What is penetration testing? What are common penetration testing strategies? [MODEL QUESTION]

Answer:

1st part:

Penetration testing, also known as pen testing, security pen testing, and security testing, is a form of either hacking. It describes the intentional launching of simulated cyberattacks by "white hat" penetration testers using strategies and tools designed to access or exploit computer systems, networks, websites, and applications. Although the main objective of pen testing is to identify expoitable issues so that effective security controls can be implemented, security professionals can also use penetration testing is to identify exploitable issues so that effective security controls can be implemented, security professionals can also use penetration testing techniques, along with specialized testing tools, to test the robustness of an organization's security policies, its regulatory compliance, its employees' security awareness, and the organization's ability to identify and respond to security issues and incidents such as unauthorized access, as they occur.

As a simulated cyberattack, ethical hacking techniques help security professionals evaluate the effectiveness of information security measures within their organizations. The pen test attempts to pierce the armor of an organization's cyber defenses, checking

for exploitable vulnerabilities in networks, web apps, and user security.The objective is to fine weakness in systems before attackers do.

- In the case of networks, the high-level goal is to strengthen security posture by closing unused ports, troubleshooting services, calibrating firewall rules, and eliminating all security loopholes.
- In the case of web applications, pen testing is designed to identity, analyze, and report on common web application vulnerabilities such as buffer overflow, SQL injection, cross-site scripting, to name just a few.
- Pen testing can also be used to attempt to gain privileged access to sensitive systems or to steal data from a system that is believed to be secure.

2nd part:

Based on the objectives of the organization, here are some commonly used penetration testing strategies:

- External testing: This involves attacks on the organization's network perimeter using procedures performed from outside the organization's systems, e.g., the Extranet and Internet.
- Internal testing: Performed from within the organization's environment, this test attempts to understand what could happen if the network perimeter were successfully penetrated or what an authorized used could do to penetrate specific information resources within the organization's network.
- Blind testing: In this case, the tester tries to simulate the actions of a real hacker. The testing team has little or no information about the organization but instead must rely on publicly available information (such as corporate website, domain name registry, etc.) to gather information about the target and conduct its penetration tests.
- Double blind testing: In this exercise, only a few people within the organization are made aware of the testing. The IT and security staff are not notified or informed beforehand, and as such, they are "blind" to the planned testing activities. Double-blind testing helps test an organization's security monitoring and incident identification processes, as well as its escalation and response procedures.
- Targeted testing: Also known as the lights-turned-on approach, target testing involves both IT and penetration testing teams. Testing activities and information concerning the target and the network design are known going in. Targeted tests require less time and effort than a blind test, but typically don't provide as complete a picture of an organization's security vulnerabilities and response capabilities as other testing strategies.

8. What are different types of social engineering attacks? [MODEL QUESTION]

Answer:

By definition, social engineering is an attack vector used to gain access to gain access to networks, systems, or physical locations, or for financial gain by using human psychology, rather than using technical hacking methods. It relies on social interaction to manipulate people into circumventing security best practices and protocols.

Social engineering is the new preferred tactic among the hacker community. It is easier to exploit users' flaws than to discover a vulnerability in networks or systems.
Understanding **different types of social engineering attacks** is an essential aspect of protection.

Common Types of social engineering attacks:

- **Phishing attacks**

Phishing is a leading form of social engineering attack that is typically delivered in the form of an email, chat, web ad or website that has been designed to impersonate a real system, person, or organization. Phishing messages are crafted to deliver a sense of urgency or fear with the end goal of capturing an end user's sensitive data. A phishing message might come from a bank, the government or a major corporation.
The call to actions vary. Some ask the end user to "verify" their login information of an account and include a mocked-up login page complete with logos and branding to look legitimate. Some claim the end user is the "winner" of a grand prize or lottery and request access to a bank account in which to deliver the winnings. Some ask for charitable donations (and provide wiring instructions) after a natural disaster or tragedy. A successful attack often culminates in access to systems and lost data. Organizations of all sizes should consider backing up business-critical data with a business continuity and disaster recovery solution to recover from such situations.

- **Baiting attacks**

Baiting, similar to phishing, involves offering something enticing to an end user, in exchange for login information or private data. The "bait" comes in many forms, both digital, such as a music or movie download on a peer-to-peer site, and physical, such as a corporate branded flash drive labeled "Executive Salary Summary Q3" that is left out on a desk for an end user to find. Once the bait is downloaded or used, malicious software is delivered directly into the end users system and the hacker is able to get to work.

- **Quid Pro Quo**

Similar to baiting, quid pro quo involves a hacker requesting the exchange of critical data or login credentials in exchange for a service. For example, an end user might receive a phone call from the hacker who, posed as a technology expert, offers free IT assistance or technology improvements in exchange for login credentials. Another common example is a hacker, posing as a researcher, asks for access to the company's network as part of an experiment in exchange for $100. If an offer sounds too good to be true, it probably is quid pro quo.

- **Piggybacking attacks**

Piggybacking, also called tailgating, is when an unauthorized person physically follows an authorized person into a restricted corporate area or system. One tried-and-true method of piggybacking is when a hacker calls out to an employee to hold a door open for them as they've forgotten their ID card. Another method involves a person asking an employee to "borrow" his or her laptop for a few minutes, during which the criminal is able to quickly install malicious software.

- **Pretexting attacks**

Pretexting, the human equivalent of phishing, is when a hacker creates a false sense of trust between themselves and the end user by impersonating a co-worker or a figure of authority well known to an end user in order to gain access to login information. An example of this type of scam is an email to an employee from what appears to be the head of IT support or a chat message from an investigator who claims to be performing a corporate audit. Pretexting is highly effective as it reduces human defenses to phishing by creating the expectation that something is legitimate and safe to interact with. Pretexting emails are particularly successful in gaining access to passwords and business data as impersonators can seem legitimate, so it's important to have a third-party backup provider.

9. How we can prevent insider threat? **[MODEL QUESTION]**

Answer:

- **Ransomware attacks**

Like phishing emails, ransomware, or malware may be unwittingly added by an employee to your network.

These attacks usually lead to a company device locked by a virus, and hackers have to get paid for this before the systems can be retrieved.

- **Hacking Internally**

This is a deliberate act for doing stuff such as robbing data, leaks, or corrupting data sensitive to your network.

- **Cloud and mobile storage attacks**

A rise in remote operations has made mobile and cloud-based storage much more dependent. Both technologies are safeguarded but workers who download cloud data on their own devices are dangerous.

- **Attacks via Email**

Phishing emails are a common way for people to access your information. Emails are designed to get a malicious connection from the receiver to access your network.

- **Insider Threats Types**

It is important to understand what insider threats look like, defend the organization from insider threats. Pawn and turncloaks.

- **Pawn**

In a pawn insider attack, the victim is unaware that they are being exploited or that they are the source of the issue. When an employee is the target of an insider attack, this is the most likely scenario.

Phishing or social engineering attempts are often made against them. The external threat would need to gain access to the 'pawns' credentials in order for this to happen, rendering your employee a compromised insider.

- **Turn cloaks**

Insiders who steal data maliciously are known as turncloaks. Most of the time, it's an employee or contractor who is supposed to be on the network, and has valid credentials but is exploiting their access for fun or profit. We've seen a wide range of reasons for this

form of conduct, from selling secrets to foreign governments to simply hand over a few documents to an opponent when resigning.

10. How to defend the organization from insider attacks? [MODEL QUESTION]

Answer:

- **Access Control**

Limiting the effect and potential of an insider to commit an attack requires applying the Principle of Least Privilege. The Principle of Least Privilege ensures that employees have the least amount of access necessary for their employment. This essentially means that employees don't have access to anything on the network that isn't necessary for their job. To keep your data secure, you must know where it is stored and who has access to it. The first step in assessing and managing your data protection is access control. By restricting who has access to your data and certain parts of your network, you will reduce the risk of it being hacked.

- **Limit the amount of data that can be copied or transferred.**

It may be important to prevent users from transmitting data to external sources (USBs, outside email addresses, etc.) or copying files, depending on the type of data your company has, such as patient files. Disgruntled workers may find it more difficult to steal information or accidentally share sensitive information with others as a consequence of this.

- **Educate the employees**

Unauthorized actors were involved in one-third of all insider attacks, meaning an insider unknowingly authorized or facilitated an attack. This can happen if employees insert an infected USB drive into their work machine, open a phishing email, or download a suspicious file. The only way to avoid such threats is to ensure that your employees are well-versed in data security best practices. Phishing, social engineering, ransomware, passwords, use of portable devices, physical access, data destruction, encryption, data breaches, and how workers can react if a security threat is discovered should all be covered in annual security training. Your first line of defence should be well-trained employees.

- **Third-party vendors should be avoided if possible.**

According to a recent report on third-party risk management, third-party vendors were responsible for 63 percent of all data breaches. Many third-party providers have access to an organization's internal networks, increasing the network's vulnerability to security breaches.

- **Behaviour Analysis**

Monitoring the actions of users on your network will help you stop an attack in its path and mitigate the harm. Organizations can mitigate disruption to their enterprise by analyzing patterns of activity using User and Entity Behavior Analytics Software (UEBA). Is a member of your team by logging in at odd hours or downloading or uploading unusually large amounts of data? This may be indicators of an impending assault or breach.

CYBER FORENSICS & AUDITING

Multiple Choice Type Questions

1. Computer forensics also known as? [MODEL QUESTION]
   a) digital forensic science b) computer crime
   c) computer forensic science d) computer forensics investigations

Answer: (c)

2. Which method used stochastic properties of the computer system to investigate activities lacking digital artifacts? [MODEL QUESTION]
   a) Steganography b) Stochastic forensics c) Both d) None of these

Answer: (b)

3. Computer forensics also be used in civil proceedings. [MODEL QUESTION]
   a) Yes b) No c) Can be yes or no d) Can not say

Answer: (a)

4. Which of the following techniques are used during computer forensics investigations? [MODEL QUESTION]
   a) Cross-drive analysis b) Live analysis
   c) Deleted files d) All of these

Answer: (d)

5. CCFP stands for? [MODEL QUESTION]
   a) Cyber Certified Forensics Professional
   b) Certified Cyber Forensics Professional
   c) Certified Cyber Forensics Program
   b) Certified Cyber Forensics Product

Answer: (b)

6. How many c's in computer forensics? [MODEL QUESTION]
   a) 1 b) 2 c) 3 d) 4

Answer: (c)

Short Answer Type Questions

1. What do you understand by cyber forensics? [MODEL QUESTION]

Answer:

Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user.

In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.

2. Why is computer forensics important? **[MODEL QUESTION]**

Answer:

In the civil and criminal justice system, computer forensics helps ensure the integrity of digital evidence presented in court cases. As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence -- and the forensic process used to collect, preserve and investigate it -- has become more important in solving crimes and other legal issues.

The average person never sees much of the information modern devices collect. For instance, the computers in cars continually collect information on when a driver brakes, shifts and changes speed without the driver being aware. However, this information can prove critical in solving a legal matter or a crime, and computer forensics often plays a role in identifying and preserving that information.

Digital evidence isn't just useful in solving digital-world crimes, such as data theft, network breaches and illicit online transactions. It's also used to solve physical-world crimes, such as burglary, assault, hit-and-run accidents and murder.

Businesses often use a multilayered data management, data governance and network security strategy to keep proprietary information secure. Having data that's well managed and safe can help streamline the forensic process should that data ever come under investigation.

Businesses also use computer forensics to track information related to a system or network compromise, which can be used to identify and prosecute cyber attackers. Businesses can also use digital forensic experts and processes to help them with data recovery in the event of a system or network failure caused by a natural or other disaster.

As the world becomes more reliant on digital technology for the core functions of life, cybercrime is rising. As such, computer forensic specialists no longer have a monopoly on the field. See how the police in the U.K. are adopting computer forensic techniques to keep up with increasing rates of cybercrime.

3. What are types of computer forensics? **[MODEL QUESTION]**

Answer:

There are various types of computer forensic examinations. Each deals with a specific aspect of information technology. Some of the main types include the following:

- **Database forensics.** The examination of information contained in databases, both data and related metadata.
- **Email forensics.** The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.
- **Malware forensics.** Sifting through code to identify possible malicious programs and analyzing their payload. Such programs may include Trojan horses, ransomware or various viruses.
- **Memory forensics.** Collecting information stored in a computer's random access memory (RAM) and cache.

- **Mobile forensics.** The examination of mobile devices to retrieve and analyze the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.
- **Network forensics.** Looking for evidence by monitoring network traffic, using tools such as a firewall or intrusion detection system.

4. How is computer forensics used as evidence? **[MODEL QUESTION]**

Answer:

Computer forensics has been used as evidence by law enforcement agencies and in criminal and civil law since the 1980s. Some notable cases include the following:

- **Apple trade secret theft:** An engineer named Xiaolang Zhang at Apple's autonomous car division announced his retirement and said he would be moving back to China to take care of his elderly mother. He told his manager he planned to work at an electronic car manufacturer in China, raising suspicion. According to a Federal Bureau of Investigation (FBI) affidavit, Apple's security team reviewed Zhang's activity on the company network and found, in the days prior to his resignation, he downloaded trade secrets from confidential company databases to which he had access. He was indicted by the FBI in 2018.
- **Enron:** In one of the most commonly cited accounting fraud scandals, Enron, a U.S. energy, commodities and services company, falsely reported billions of dollars in revenue before going bankrupt in 2001, causing financial harm to many employees and other people who had invested in the company. Computer forensic analysts examined terabytes of data to understand the complex fraud scheme. The scandal was a significant factor in the passing of the Sarbanes-Oxley Act of 2002, which set new accounting compliance requirements for public companies. The company declared bankruptcy in 2001.
- **Google trade secret theft:** Anthony Scott Levandowski, a former executive of both Uber and Google, was charged with 33 counts of trade secret theft in 2019. From 2009 to 2016, Levandowski worked in Google's self-driving car program, where he downloaded thousands of files related to the program from a password-protected corporate server. He departed from Google and created Otto, a self-driving truck company, which Uber bought in 2016, according to *The New York Times*. Levandowski plead guilty to one count of trade secrets theft and was sentenced to 18 months in prison and $851,499 in fines and restitution. Levandowski received a presidential pardon in January 2021.
- **Larry Thomas:** Thomas shot and killed Rito Llamas-Juarez in 2016 Thomas was later convicted with the help of hundreds of Facebook posts he made under the fake name of Slaughtaboi Larro. One of the posts included a picture of him wearing a bracelet that was found at the crime scene.
- **Michael Jackson:** Investigators used metadata and medical documents from Michael Jackson's doctor's iPhone that showed the doctor, Conrad Murray, prescribed lethal amounts of medication to Jackson, who died in 2009.

- **Mikayla Munn:** Munn drowned her newborn baby in the bathtub of her Manchester University dorm room in 2016. Investigators found Google searches on her computer containing the phrase "at home abortion," which were used to convict her.

5. What are the advantages of Cyber Forensics? **[MODEL QUESTION]**

Answer:

Below are some of the advantages given.

- Similar types of data and relevant data can be compared from different source systems to get a complete understanding of the scenario.
- Those data over a period that is relevant can be made trending using cyber forensics.
- The entire data can be scanned to identify and extract specific risks for future analysis.
- The efficiency of the control environment and policies can be tested by determining the attributes that violate the rules.
- It is used to set the trends of identification which the company people, consultants and forensic analysts are not aware of.

6. Who can use computer forensic evidence? **[MODEL QUESTION]**

Answer:

1. Criminal prosecutors use computer evidence in a variety of crimes where incriminating documents can be found, including homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
2. Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.
3. Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
4. Corporations often hire computer forensics specialists to find evidence relating to sexual harassment, embezzlement, and theft or misappropriation of trade secrets, and other internal and confidential information.
5. Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment.
6. Individuals sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination.

7. Who are forensic investigator? **[MODEL QUESTION]**

Answer:

Forensic investigators are those with the ability to ensure that the statements, recording, and/or evidence they collect will be sufficiently reliable for the forensic examiner to analyze. They attend all the details necessary to provide what the scientific community refers to as data integrity.

Subsequently the forensic investigator ensures their evidence and eventual analytical findings will be admissible in court. They provide what the forensic scientists need to conduct their examinations in good faith. The scientific community calls it data integrity, but it is referred to in the forensics as a chain of custody.

8. What is the difference between forensic investigation and intrusion detection? **[MODEL QUESTION]**

Answer:

The following are some of the elements of an end-to-end forensic trace:

- **The end-to-end concept:** An end-to-end investigation tracks all elements of an attack, including how the attack began, what intermediate devices were used during the attack, and who eas attacked.
- **Local evidence:** Once an investigator knows what devices were used during the attack, he or she can search for evidence on those devices. The investigator can then analyse that evidence to learn more about the attack and the attacker.
- **Pitfalls of network evidence collection:** Evidence can be lost in a few seconds during log analysis because logs change rapidly. Sometimes, permission is required to get evidence from certain sources, such as ISPs. This process can take time, which increases the chances of evidence less. Other pitfalls include the following:
  - An investigator or network administrator may mistake normal computer or network activity for attack activity.
  - There may be gaps in the chain of evidence.
  - Logs may be ambiguous, incomplete, or missing.
  - Since the Internet spans the globe, other nations may be involved in the investigation. This can create legal and political issues for the investigation.
- **Event analysis:** After an investigator examines all the information, he or she correlates all of the events and all of the data from the various sources to get the whole picture.

Investigation of a security alert does not necessarily have the goal to prosecute; however, legal action may still be the consequence of the investigation. For example, termination of employees(as a result of an investigation) may lead to an unfair dismissal suit. In a case of personally identifiable information (PII) theft, the victim will need to present evidence that it fulfilled it's regulatory obligations. It is therefore advisable to treat the evidence as if it is going to be used in court.

Long Answer Type Questions

1. How do Cyber Forensics Experts Work? **[MODEL QUESTION]**

Answer:

Let us now discuss the 7 steps how does it work.

1. **Copying the hard drive of the system under investigation:** Copying or imaging the hard drive means making a copy of the files and folders present on the hard drive. The replica of the drive is created on another drive-by copying every bit of data on the drive from the system under investigation.
2. **Verification of the copied data:** After the data is copied from the hard drive of the system under investigation to another hard drive, the forensic experts make sure if the copied data is exactly the same as the original data.

3. **Ensuring the copied data is forensically sound:** Based on the operating system used in the computer, the data written to the hard drive is in a format compatible with the operating system. Hence the forensic experts must make sure the data while being copied from the drive of the system under investigation into another drive is not altered in any way. That is, the data is copied using a write-blocking device in a forensically sound manner.
4. **Deleted files recovery:** The files deleted by the user on the computer can be recovered by forensic experts. The files are not deleted permanently by the computer and forensic experts know how to recover the deleted files.
5. **Finding data in free space:** The operating system sees the free space in the hard drive as space available to store the new files and folders but temporary files and files that were deleted years ago are stored here until the time new data is written into the free space. Forensic experts search through this free space to recreate those files.
6. **Performing keyword search:** Forensic experts make use of software that can go through the entire data for the given keywords and output the relevant data.
7. **The technical report:** The technical report must be an easy to understand document for anyone irrespective of the background. It should mainly focus on what is the offense, who is the offender and how did he commit the crime along with all the technicalities.

2. What are types of computer forensic systems? **[MODEL QUESTION]**

Answer:

i) Internet security systems
ii) Intrusion detection systems
iii) Firewall security systems
iv) Storage area network security systems
v) Network disaster recovery systems
vi) Public key infrastructure security systems
vii) Wireless network security systems
viii) Satellite encryption security systems
ix) Instant messaging (IM) security systems
x) Net privacy systems
xi) Identity management security systems
xii) Identity theft prevention systems

Internet security systems: Internet and network security are topics that many executives and managers avoid talking about. Many feel that discussing their security implementations and policies will cause their companies to become vulnerable to attack. Ironically, Internet security can provide a more secure solution, as well as one that is faster and less expensive than traditional solutions to security problems of employees photocopying proprietary information, faxing or mailing purchase orders, or placing orders by phone.

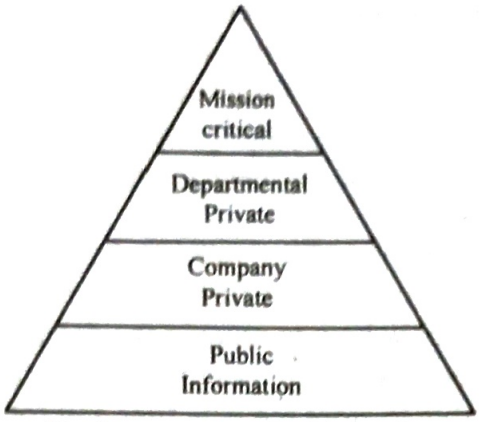


Fig Internet security hierarchy

Intrusion Detection Systems: Intrusion detection systems help computer systems prepare for and deal with attacks. They collect information from a variety of vantage points within computer systems and networks and analyze this information for symptoms of security problems. Vulnerability assessment systems check systems and networks for system problems and configuration errors that represent security vulnerabilities

- ✓ Monitoring and analysis of user and system activity
- ✓ Auditing of system configurations and vulnerabilities
- ✓ Assessing the integrity of critical system and data files
- ✓ Recognition of activity patterns reflecting known attacks
- ✓ Statistical analysis of abnormal activity patterns

Firewall Security Systems: For most organizations now connecting to the Internet and big business and big money moving toward electronic commerce at warp speed, the motive for mischief from outside is growing rapidly and creating a major security risk to enterprise networks. Reacting to this threat, an increasing number of network administrators are installing the latest firewall technology as a first line of defense in the form of a barrier against outside attacks. These firewall gateways provide a choke point at which security and auditing can be imposed. They allow access to resources on the Internet from within the organization while providing controlled access from the Internet to hosts inside the virtual private network (VPN).

Storage area network security systems: SANs are a relatively new methodology for attaching storage, whereby a separate network (separate from the traditional LAN) connects all storage and servers. This network would be a high-performance implementation, such as a fiber channel, that encapsulates protocols such as a small computer system interface (SCSI). These are more efficient at transferring data blocks from storage and have hardware implementations offering buffering and delivery guarantees. This is not available using TCP/IP. The SAN development areas have not yet been realized, but there is great potential with regard to centralized storage SAN management and storage abstraction. Storage abstraction refers to an indirect representation of storage that has also been called virtualization. Together with these

potential enhancements, SANs should be able to generate greater functionality than has been possible previously. Thus, most system vendors have ambitious strategies to change the way enterprise operations store and manage data with new capabilities based on SANs.

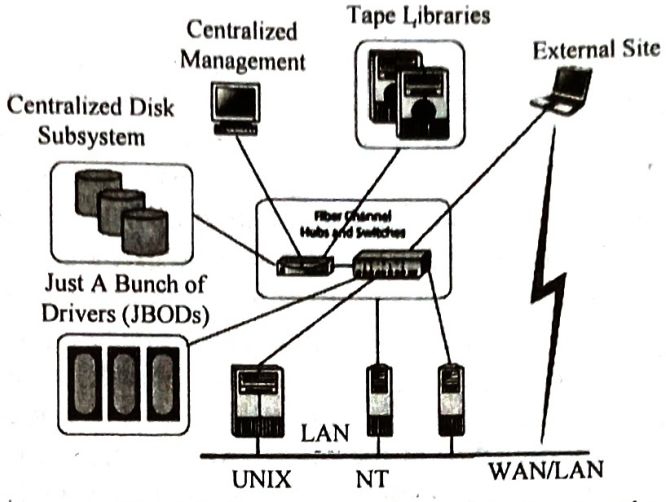


Fig. (a): Storage-centric model of computing

Network Disaster Recovery Systems: The high availability of mission critical systems and communications is a major requirement for the viability of the modern organization. A network disaster could negate the capability of the organization to provide uninterrupted service to its internal and external customers. How would your company respond in the event of a network disaster or emergency? Network disaster recovery (NDR) is the ability to respond to an interruption in network services by implementing a disaster recovery plan to restore an organization's critical business functions. NDR is not a new idea. In recent years, data has become a vitally important corporate asset essential to business continuity. A fundamental requirement of economic viability is the ability to recover crucial data quickly after a disaster. Many companies see their disaster recovery efforts as being focused primarily on their IT departments. IT people are in the lead in sponsoring and managing their disaster recovery plans, and relatively few companies involve line-of-business staff and partners in designing and testing such plans at all. Not surprisingly, the person most frequently cited as being responsible for the management of an NDR plan is the company's chief information officer (CIO) or another IT manager.

Public Key Infrastructure Systems: The PKI assumes the use of public key cryptography, which is the most common method on the Internet for authentication of a message sender or encryption of a message. Traditional cryptography involves the creation and sharing of a secret key for the encryption and decryption of messages. This secret key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the PKI is the preferred approach on the Internet.

A PKI consists of

✓ A certificate authority that issues and verifies digital certificates

✓ A registration authority that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
✓ One or more directories where the certificates (with their public keys) are held
✓ A certificate management system

Wireless Network Security Systems: The only reason the wireless viruses of today have not been more damaging is that there's a lack of functionality and a lack of mature infrastructure globally. That's about to change. Industry analysts predict dramatic increases in wireless handheld use and the proliferation of new mobile capabilities. The wireless world, with its often-incompatible alphabet soup of standards, may be new territory for many IT managers. Many enterprises have felt that protecting their wireless processes against viruses is one piece of the complicated puzzle they can afford to omit. They'll soon need to think again or face threats that could wreak havoc. The good news is wireless network security vendors (even giants like IBM) are busy developing products to fight the viruses and security breaches of the future. Among them are those that head off problems on a wireless network level, within applications and on devices.

Satellite Encryption Security Systems:

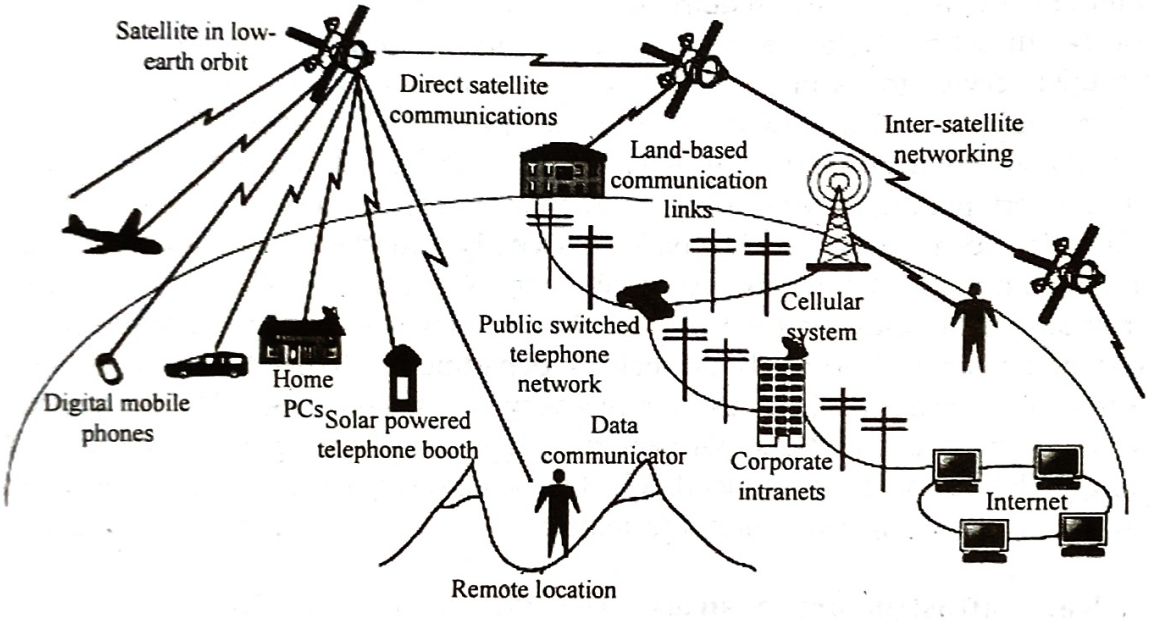


Fig. (b): The low Earth orbit (LED) network

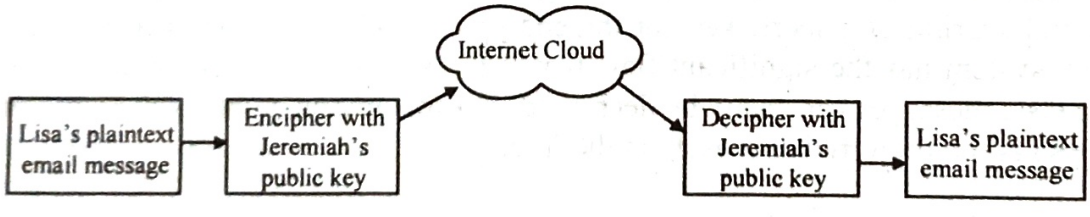


Fig. (c): The path of a public-key-encrypted message

Instant messaging (IM) security systems: The security threats from IM are straightforward. Since deployment isn't controlled, the enterprise can't keep a rein on how the systems are used. With the public IM networks, the individual employee registers for service. If the employee leaves a company, the firm has no (technology-based) way to prevent him from continuing to use the account, or from continuing to represent himself as still working for the company. Furthermore, without additional tools, the company has no way of archiving IM messages for legal or regulatory purposes, or of monitoring and controlling the content of messages to filter for inappropriate communications.

There are the obvious holes that IM opens up on the corporate network. Each of the IM networks uses a well-known port that must either be left open on the corporate firewall to allow traffic in or closed, which, at least in theory, bans that service to end users.

3. Explain big picture of forensic investigation. **[MODEL QUESTION]**

Answer:

A forensic investigation is one that is conducted to address case-related questions about the evidence, and then meet the challenges of courtroom admissibility. The forensic investigation is every part of the inquiry; it includes the work of all forensic professionals, including investigators and examiners alike. It includes the following component parts:

1. Crime scene investigation (evidence collection, examination and reconstruction)
2. Forensic interviews
3. Forensic victimology
4. Medicolegal investigation (e.g., sexual assault examination, toxicology, and/or autopsy)
5. Crime lab analysis (e.g., criminalistics)
6. Forensic mental health assessments

Forensic investigators recognize, document, collect, preserve, and even transport evidence to forensic examiners so they can do the work of examination and interpretation. That is the nature of the relationship. The quality and reliability of one depends entirely on that of the other.

As described in Edwards and Gotsonis (2009, p. 55):

Forensic investigations involve intelligence and information gathering, crime scene investigation, laboratory analysis, interpretation of tests and results, and reporting and communication with members of law enforcement and the judical system. Law enforcement agencies within the United States vary in organizational structure regarding how forensic science examinations are conducted and evidence is admitted into court. Variations are attributable to the geographical size and population served by the jurisdictional authority, the types and level of crimes encountered, the funding cource, and local tradition. In general, however, the forensic science community includes crime scene investigators; state and local crime laboratories; medical examiners; private forensic laboratories; law enforcement inentification units; resources such as registries and databases; professional organizations; prosecutors and defense attorneys; quality

system providers and federal agencies that conduct or support research as well as provide forensic science services and training.

For example, a medical examiner's office will employ forensic investigators. These investigators are charged with attending the death scene on behalf of the medical examiner taking photographs and recording their observations. They do this on behalf of the medical examiner; so the medical examiner does not have to do it themselves; so that the medical examiner can focus on the larger picture. The forensic investigator gathers information and evidence; the medical examiner examines everything together, including autopsy-related findings and provides interpretations. Both may be called to testify in court, to verify the nature and quality of their work.

4. What do you understand by network forensic? What are challenges of network forensics? [MODEL QUESTION]

Answer:

1st part:

Network Forensics is the process of capturing, recording and conducting analysis of the various network events in order to identify the origin of the security attacks and other problems. This helps in figuring out the unauthorized access to the computer system and conducts search for the evidence in such occurrences. Network Forensics has the capability to conduct investigation at a network level as well as the events that take place across an IT system.

- Intrusion detection,
- logging and
- Correlating intrusion detection and logging are the three parts of a network forensics.

The main aim of this network forensics is to make available the sufficient evidence in order to impose punishment on the criminal offenders. Network Forensics is applied in the major areas of hacking, fraud, insurance companies, theft of data, defamation, obscene publication, credit card cloning, software piracy, etc.

2nd part:

One of the greatest challenges faced in conducting network forensics is the enormous quantity of data created by the network which amounts to gigabytes per day. It is a tiresome process to search for the evidence and in some cases, it is almost impossible to find it if the event is brought to notice after a prolonged period of time. Another such challenge is in the constant unknown identities of the Internet protocols. Each of the internet layer such as the IP addresses, e-mail addresses and the MAC addresses uses a particular form of addressing which can fall prey to spoofing. However, the various high-powered software available makes it possible to conduct analysis of the internet activity and solve these cases.

Network forensic duties that can be made easier through the software comprises the collection, normalizing, filtering, labeling, stream reassembly, correlation and analysis of numerous sources of vast market data. Even though there are tools used for a single purpose which aims at fulfilling each of these tasks, feature creep is less distinct among the categories. It results in tools that are useful in addressing a growing number of things

that can go wrong on the network. Prior to the performance of the foreign task by the investigator, suitable network activity data must be collected. The raw network packets which comprises of the highest possible level of traffic details supplement the often-sparse log data available from applications, authentication systems, routers and firewalls. Sniffing also collects such network data.

Stream reassembly is the gathering and packaging of raw network traffic from a single source in such a way where all the data within a connection session is presented as a complete stream. Stream reassembly is performed by the protocol analysis tools, which isolate the specific communications that took place between two or more of the apparent endpoints or relay points. Such an examination or investigation is the foremost step in identifying who communicated when and what messages was transmitted. Majority of the protocol analysis tools are made use of within the sessions and they provide a tree-oriented view of sessions. Suchlike a visual presentation of network traffic makes it easier to figure out or realize as to what exactly happened on the network.

5. What is network based digital evidence? **[MODEL QUESTION]**

Answer:

Network-based digital evidence is a type of digital evidence which arises as product of the communications over a network. The primary and the secondary storage media of computers (such as the RAM and hard drives) tend to be productive elements for the forensic analysis and investigation. As a result of all the fragments of data, constant storage can maintain forensically recoverable and appropriate evidence for hours, days and years beyond the file deletion and storage reuse. Network-based digital evidence can be exceedingly unpredictable in variance to this. Within the milliseconds of the blinking of an eye, the packets move swiftly and lightly across the wire and disappear from the switches. Web sites keep changing from when and where they're viewed.

Network-based evidences lays down certain specific and prominent challenges in various areas, some of the most common challenges which are related to the Network-based digital evidence are as follows:

- **Acquisition:** To find or locate a specific evidence in a network environment can be a hard task. There are multiple sources of evidence commencing from the wireless access points to the web proxies to the central log servers which makes it often difficult to point out the exact location of an evidence. In certain cases, where we are still aware of a specific evidence and as to where it resides, obtaining an access to it can often become complex at times due to the political or technical reasons.
- **Content:** Apart from the file systems, which are mainly designed to contain all the contents of files and their metadata, network devices may or may not store evidence with the level of granularity desired. The storage limit capacity of the network devices is often very limited. Most of the time, only the selected metadata about the data transfer or transaction is maintained as compared to entire records of the data that traversed the network.
- **Storage:** Secondary or persistent storage are usually not engaged as part of network devices. As a result of this consequence a device may not be able to survive a reset because the data contained in these network devices are unstable and uncertain.

- **Privacy:** Depending on the jurisdiction, legal issues could arise which may include personal privacy issues that are unique to network-based acquisition techniques.
- **Seizure:** Seizing of a hard drive can cause trouble and disruption to an individual or organization. However, a copy of the original hard drive can be constructed and deployed where the grave operations can continue with limited disturbance.
  Seizure done to a network device are most often way more disruptive. In the most serious cases, an entire network segment may be brought down perpetually. In most of the circumstances, investigators have the ability to minimize the impact on network operations.
- **Admissibility:** File system-based evidence is being admitted consistently both in criminal and civil proceedings. As long as the file system-based evidence is relevant to the case, lawfully acquired & properly handle there is a clear precedent for validating or verifying the evidence and admitting it in court. In variance, the network forensics is one of the newest approaches to digital investigations. Often there arise conflicting or even non-existing legal precedents for the admission of various types of network-based digital evidence. With time the network-based digital evidence may become more widespread and the case precedents will be set and standardized.

6. How to collect network based evidence? **[MODEL QUESTION]**

Answer:

Depending on the technical means available, as well as legal and regulatory requirements, it will not always be possible to wiretao everything and keep a full log of all data sent.

The task of acquiring network evidence can be divided into active aquisition. Passive acquisition happens when data is gathered without emitting data at OSI Layer 2 or above. Traffic acquisition, or capturing, or sniffing falls into this field. In contrast, active acquisition happens when evidence is gathered by interacting with systems on the network, i.e. by sending queries to them, or system loggign to a log host, SIEM or management station. This may even including scanning the network ports of determine their current state.

To preserve as much of the evidence as possible, acquisition should not change the packets, send out additional packets or alter the network configuration (thus observing the data integrity principle). Quoting Jones (2013, p.45):

"Ideally, we would like to obtain perfect-fidelity evidence, with zero impact the environment. For copper wires, this would mean only observing changes in voltages without ever modifying them. For fibre cables, this would mean observing the quanta without ever injecting any. For radio frequency, this would mean observing RF waveswithout ever emitting any. In the real world, this would be equivalent to a murder investigator collecting evidence from a crime scene without leaving any new footprints." (Davidoff and Ham, 2012, p. 45).

Network forensic investigators can passively acquire network traffic by intercepting it as it is sent across cables, through the air, or through network equipment such as hubs and switches.

One word of advice: If investigators can capture traffic, so adversaries. A compromised system could trivially act as a passive listener and eavesdrop on any data transfers or communications. Any evidence sent across the network,or normal traffic sent by the investigator's operating system, may be trivially captured by anyone else on the local network.

Aquiring traffic in cables

Cables allow for point-to-point connections between stations. The most common cabling types are copper cables with the twisted-pair and coaxial subtype, where information is transferred in form of electrical signals, and (glass) fibres where information takes the form of optical signals. Both sorts of cables can be sniffed, but the equipment and side effects vary.

- Coaxial cable, shorthand "coax," consists of a single inner wire wrapped in insulation and covered with an additional outer metal layer shield. Another insulation layer and an outer protective layer. The term coaxialcomes from the inner conductor and the outer shield sharing a geometric axis. The advantage of coaxial cablesis that the core and thus the transmission is shielded from electromagnetic interence. If the inner core is tapped, the traffic to and from all stations that share the physical medium can be captured by investigator

  The main use of coaxial cable is as a transmission line for radio frequency signals. Applicationinclude antenna cables, digital audio (S/PDIF) and computer networks, mostly in the form of 10Base5 ("thick" Ethernet or "Yellow Cable") or 10Base2 ("thin" Ethernal, "Cheapernet"). They have fallen out of use and been replaced by cheaper and more performant network technologies (Fast or Gigabit Ethernet) based on twisted pair cabling, although there will be some legacy installations that still might use it.
- Twisted Pair (TP) cabling is a wiring in which two conductors of a single circuit are twisted together to negate electromagnetic interference. Multiple circuits will be combined into a cable with an optional outer shielding layer. In the latter case, this is called Shielded Twisted Pair (STP) and the other case Unshielded Twisted Pair (UTP). Typical deployments in computer networks consist of 4 pairs of wires in one cable.

  TP cabling is typically deployed in star network topologies where stations are connected to a switch or hub, in contrast, direct connection (so called ccross-cables) are relatively rare. By tapping one pair of TP wires on a switched network, only traffic relating relating to only one end station may be received. Standard network taps allow tapping into two or all wire pairs in a receive T least bi-directional traffic.
- Fibre optic cables consist of thin strands of glass (or sometimes plastic) which are bundled together to send signals across a distance. Light is beamed into the fibre at one end and travels along an optic fibre, reflecting constantly against the walls until it reaches an optical receiver at the other end.

Network taps

Inline network taps are OSI layer 1 devices (see Fig. a), which can be inserted inline between two physically connected network devices. The network tap will pass along the packets and physically replicate copies to one or morre monitoring ports. Network taps (like the one in figure below) commonly have four ports: two connected inline to facilitate normal traffic, and two sniffing ports, which mirroe that traffic (one for each direction). Insertion of an inline network tap typically causes a brief descruption, since the cable must be seperated to connect the network tap inline.

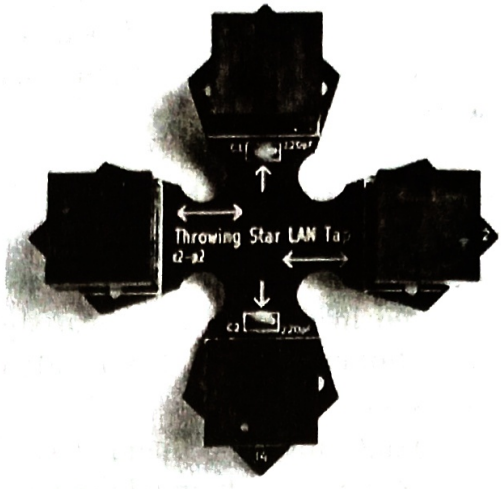


Fig. (a) Inline network tap

They are commonly designed to repaire no power for passively pasing packets. This reduces the risk of a network outage cause by the tap. This does not cover the power requirements of the monitoring station though.

Fully passive tapping is not possible with Gigabit Ethernet as each cable pair transports 5 bits simultaneously in both directions. The Layer 1 (PHY) chips at each end of the cable they must separate the two signals from each other. This is only possible because they know their own signal, so they can direct their own send signals from the mixed signals on the line and then interpret the information sent by their link partners.

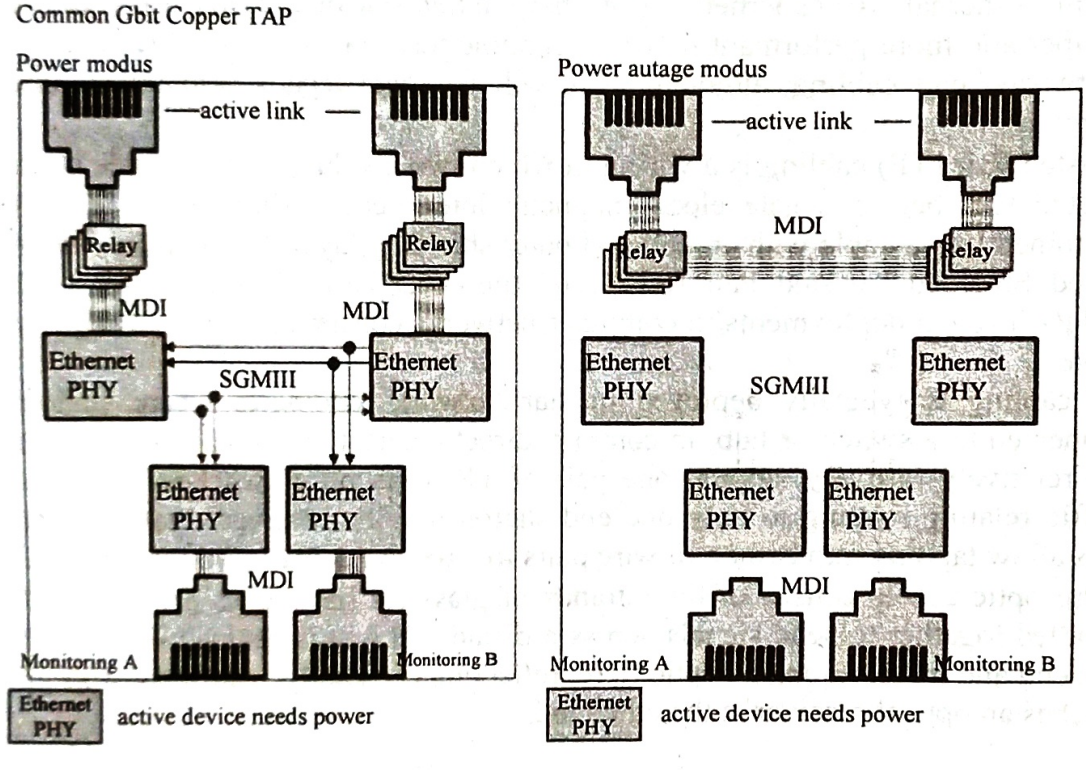


Fig. (b): Gigabit Ethernet network tap function schema

The only way to terminate the signal (as shown in Fig b) is to use a PHY chip to separate the signal and then send the signal on to the link partner. However, it is not passive any longer, so in case of a failure the link can go down and the servers on the link are interrupted. To minimize this problem each copper tap has a bypass switch (relays), which closes in s power down situation (as shown in the picture), to bring the link backup.

Vampire taps (Fig c) are deveices that piece the shielding of coaxial cables to provide access to the signal within. The device clamps onto and "bites" into the cable (hence the term "vampire", see Figure d), inserting a probe through a hole drilled using a special tool through th outer shilding to contact the inner conductor, while another spikes bite into the outer conductor. Unlike inline network taps, the cable does not need to be severed or disconnected for a vampire tap to be installed. Great carre must be taken when drilling into the cable, since the inner conductor is only a few millimeteres thick at best, the conductor can be broken when drilling too far.

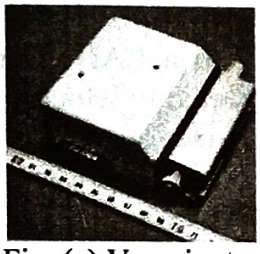


Fig. (c) Vampire tap

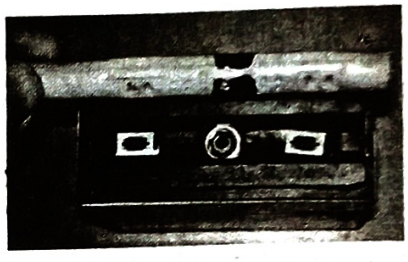


Fig. (d) Vampire tap internals

Fibre Optic network taps (Fig e) work similarly to inline taps for copper cables. The investigators will splice the optic cable and connect it to each port of a tap or insert a pre-fabricated tap at a point where the optical cable is terminating, like before a switch or patch panel.

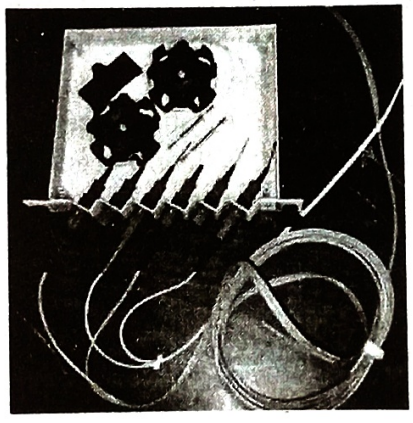


Fig. (e) Passive fibre optic tap

Attaching the tap to network will disrupt the network at the point of insertion and cause some additional signal attenuation, although taps that are more complex may amplify the signal back to its original level, but this will require some kind of power supply.

Hubs

A network hub is an OSI Layer 1 device that physically connects all stations on a local subnet to one circuit. It maintains no knowledge of what devices are connected to what ports. It is merely a physical device designed to implement baseband (or "shared") connectivity. When the hub receives a frame, it forwords it to all other ports. Therefore, every device connected to the hub physically receives all traffic destined to every other device attached to the hub. Thus, all traffic on the segment can be travially captured by connecting to any unused port on a hub.

Many devices that are labelled as "hubs" are in fact switches. A reliable way to determine if a device is actually a hub is to connect a station to it, put the network interface into promiscuous mode, and observe the traffic. If only packets destined for the monitoring station and broadcast traffic can be seen, then the device is a switch. If it is a hub, traffic to all other connected stations should be seen.

Switches

Like hubs, switches connect multiple stations' together to form a LAN. Unlike hubs, switches use software to keep track of which stations are connected to which ports, in its CAM (Content Addressable Memory) table. When a switch receives a packet, it forwards it only to the destination station's port. Individual stations do not physically receive each other's traffic. This means that every port on a switch is its own collision domain. Depending on the OSI layer a switch operates at it is referred to as a layer 2 switch when operating at the data-link layer 3 switch when operating at the network layer, which is also called routing.

A switches CAM table stores MAC addresses with corresponding switch ports. The purpose of the CAM table is to allow the switch to minimize traffic per port so that each individual station only receives traffic that is destined for it.

Switches can often be configured to replicate traffic from one or more ports to some other port for aggregation and analysis. The most vender-neutral term for this is "port mirroring." Investigators will need administrative access to the switch's operating system to configure port mirroring. A monitoring station needs to be connected to the mirroring port to vapture the traffic. Investigators must consider the bandwidth mirroring port in comparison to the traffic on the monitored ports, not to drop packets.

Active acquisition

Without administrative access, there are still methods to sniff traffic in switched networks. In cases when the network administrators themselves are not trusted, investigators may need to use the same techniques as attackers. This is not recommended and should be seen only as a measure of last resort, as they cause the switch to operate outside normal parameters and will likely trigger intrusion detection mechanisms in the network.

First, the attacker can flood the CAM table of the switch with information (by sending packets with different MAC addresses). This atttack is referred to as "Mac flooding" or "CAM table overflow". When the CAM table overflows, switches by default will "fail

open" to a hub mode of operation and send traffic for systems not in the CAM table out to every port.

For each protocol, there are several frequency bands over which data can be transmitted, with each band subdivided into smaller bands, called channels. Not all frequency bands or all channels are in use everywhere in the world. Most countries limit what frequency and channels are used within their jurisdiction. The consequence is that network equipment made for one country may operate on different frequencies and channels than one made for another country. Thus, advarsaries using wireless technology from a different country which may not be detected by that countries network equipment.

Spectrum analysers are designed to monitor RF frequencies and report on usage. They can be very helpful for identifying rogue wireless devices and channels in use.

Second, an "ARP spoofing", or "ARP (cache) poisoning" attack can be conducted. The address Resolution Protocol(ARP) is used bu stations on a LAN to dynamically map IPv4 addresses (Layer 3) to corresponding MAC addresses (for IPv6 this dunction is carried out within ICMPv6, but the principle is otherwise identical). The attacker broadcasts bogus ARP packets, which link the attacker's MAC address to the victim's IP address. Other stations on the LAN add this bogus information to their ARP tables, and send traffic for the roughter's IP address to the attacker's MAC address instead. This causes all IP packets destined for the victin station to be sent instead to the attacker (who can then copy, change, and/or forword them on to the victim).

Acquiring traffic in ratio networks

There are some additional complexities involved in capturing traffic in wireless network. In this section, a few significant notes for capturing and analysing such wireless traffic are given.

There are many protocols in use today that enable wireless networking. To name the more common onec:

- WLAN: this refers to Wireless Local Area Networks as specified in IEEE 802.11-2016.
- Mobile telephone: with a wide variety of protocols being currently in use.
- Bluetooth: Also called EIreless Personal Area Networks they are specified in IEEE 802.15.1. Depending on the class to the device, ranges vary from 0.5 m up to 100 m.
- IEEE 802.15.1: This will refer to lower layers of protocols like ZigBee or LoPWAN[14] with ranges being similar to Bluetoooth. Power requirements and data ranges are generally lower than 802.15.1, except for Bluetooth LE (lower energy).

For each protocol, there are several frequency bands over which data can be transmitted, with each band subdivided into smaller bands, called channels. Not all frequency bands or all channels are in use everywhere in the world. Most countries limit what frequency and channels are used within their jurisdiction. The consequence is that network equipment made for one country may operate on different frequencies and channels than one made for another country. Thus, advarsaries using wireless technology from a different country which may not be detected by that countries network equipment.

Spectrum analysers are designed to monitor RF frequencies and report on usage. They can be very helpful for identifying rogue wireless devices and channels in use.

WLAN passsive evidence acquisition

TO capture WLAN traffic, investigators need an 802.11 wireless card capable of running in Monitor mode; a mode that many WLAN cards do not support. There is a difference between Monitor mode and Promiscuous mode that can be summed up as follows:

- Monitor mode: Packets are captured without associating to an access point. Traffic from (and to) all access points and stations in ratio range will be captured, indepent of SSID. This can be thought of an analogue to standing in a room and listening to people's converstions.
- Promiscuous mode: Packets are captured after associating with an access point and the system will be listening to all packets, even those not addressed to it. "All packets" in promiscuous mode means packets form all stations being associated with the AP. This can be throught of an analogue to joining a group of people in a conversation, and hearing sentences not related to you.

An important difference between Monitor mode and promiscous mode the packets are captured in 802.11 formet while in promiscuous mode they are presented in Ethernet (802.3) formet. From a forensic standpoint, monitor mode is preferable as it is completely passive and conveys more information. It is recommended to use a special-purpose WiFi monitoring card that can be configured to operate completely passively. Similar considerations must be mode with 802.15.4 traffic. Equipment to capture mobile telephone traffic is typically not available to investigators not belonging to lay enforcement.

Rgardless of whether a WLANs traffic is encrypted, investigators can gain a great deal of information by capturing and analysing 802.111 management traffic. This information commomly includes:

- Broadcast SSIDs (and sometimes even non-broadcast ones).
- WAP MAC addresses.
- Supported encryption/authentication algorithms.
- Associated client MAC addresses.

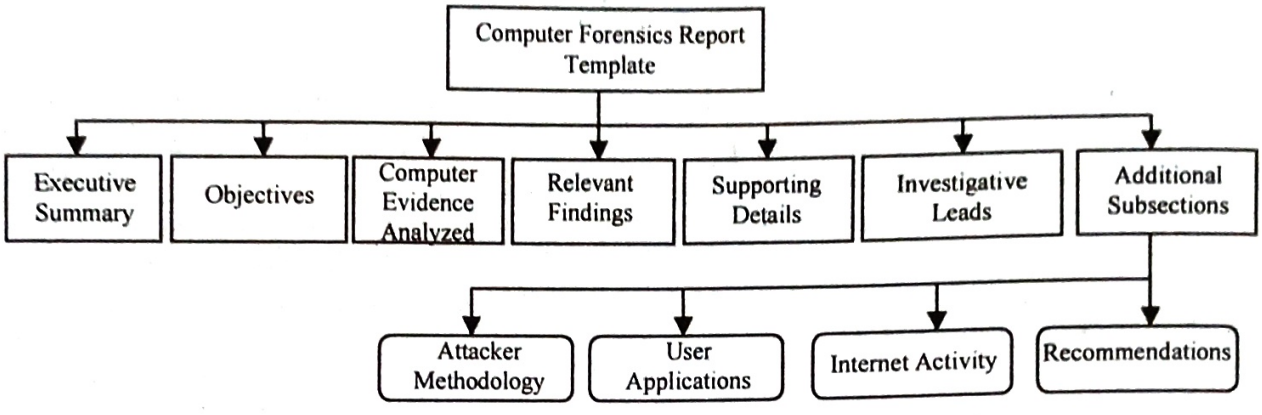
Even when a WLAN's traffic is encrypted, there is a single shared key for all stations. This means that anyone who gains access to the encryption key can listen to all traffic relating to all stations (as with physical hubs)[15].For investigators, this is helpful because local IT staff can provide authentication credentials, which facilitate monitoring of all WLANs traffic. Furthermore, there are well-known flaws in common WLAN encryption algorithms such as WEP, which can allow investigators to circumvent or crack unknown encryption keys.

Once an investigator has gained full access to unencrypted 802.11 traffic contents, this data can be analysed in the same manner as any other unencrypted network traffic.

7. Explain computer forensic report format. **[MODEL QUESTION]**

Answer:

The main goal of Computer forensics is to perform a structured investigation on a computing device to find out what happened or who was responsible for what happened, while maintaining a proper documented chain of evidence in a formal report. Syntax or template of a Computer Forensic Report is as follows:



1. Executive Summary:

Executive Summary section of computer forensics report template provides background data of conditions that needs a requirement for investigation. Executive Summary or the Translation Summary is read by Senior Management as they do not read detailed report. This section must contain short description, details and important pointers. This section could be one page long. Executive Summary Section consists of following:

- Taking account of who authorized the forensic examination.
- List of the significant evidences in a short detail.
- Explaining why a forensic examination of computing device was necessary.
- Including a signature block for the examiners who performed the work.
- Full, legitimate and proper name of all people who are related or involved in case, Job Titles, dates of initial contacts or communications.

2. Objectives:

Objectives section is used to outline all tasks that an investigation has planned to complete. In some cases, it might happen that forensics examination may not do a full fledged investigation when reviewing contents of media. The prepared plan list must be discussed and approved by legal council, decision makers and client before any forensic analysis. This list should consist tasks undertaken and method undertaken by an examiner for each task and status of each task at the end of report.

3. Computer Evidence Analyzed:

The Computer Evidence Analyzed section is where all gathered evidences and its interpretations are introduced. It provides detailed information regarding assignment of evidence's tag numbers, description of evidence and media serial numbers.

4. Relevant Findings:
This section of Relevant Findings gives summary of evidences found of **probative Value.** When a match is found between forensic science material recovered from a crime scene e.g., a fingerprint, a strand of hair, a shoe print, etc. and a reference sample provided by a suspect of case, match is widely considered as strong evidence that suspect is source of recovered material.

5. Supporting Details:
Supporting Details is section where in-depth analysis of relevant findings is done. 'How we found conclusions outlined in Relevant Findings?', is outlined by this section. It contains table of vital files with a full path name, results of string searches, Emails/URLs reviewed, number of files reviewed and any other relevant data. All tasks undertaken to meet objectives is outlined by this section. In Supporting Details we focus more on technical depth. It includes charts, tables and illustrations as it conveys much more than written texts.

6. Investigative Leads:
Investigative Leads performs action items that could help to discover additional information related to the investigation of case. The investigators perform all outstanding tasks to find extra information if more time is left. Investigative Lead section is very critical to law enforcement. This section suggests extra tasks that discovers information needed to move on case. e.g. finding out if there are any firewall logs that date any far enough into past to give a correct picture of any attacks that might have taken place. This section is important for a hired forensic consultant.

8. What is the meaning of forensic audit? What is the significance of forensic audit? [MODEL QUESTION]

Answer:

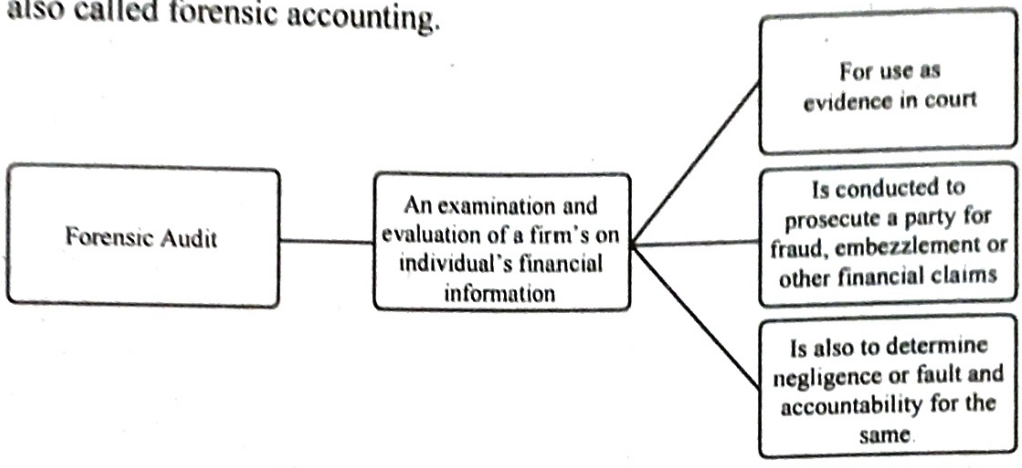
1st part:

Forensic audit is, in general, referred to as an examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court.

As per the definition given in Investopedia, Forensic Audit is an examination and evaluation of a firm's or individual's financial information for use as evidence in court. A Forensic Audit can be conducted in order to prosecute a party for fraud, embezzlement or other financial claims. In addition, an audit may be conducted to determine negligence or even to determine how much spousal or child support an individual will have to pay.

Jack Bologna and Robert defined Forensic Audit as the application of financial skills and an investigative mentality to unresolved issues, conducted within the context of the rules of evidence. As a discipline, it encompasses financial expertise, fraud knowledge, and a strong knowledge and understanding of business reality and the working of the legal system.

Collin Greenland defines that forensic accounting (or auditing) is the integration of accounting, auditing and investigative skills in order to provide an accounting analysis suitable for the resolution of disputes (usually but not exclusively) in the courts.
Business Dictionary defines Forensic Audit as the application of accounting methods to the tracking and collection of foremsic evidence, usually for investigation and prosecution of criminal acts such as embezzlement or fraud. It further states that forensic audit is also called forensic accounting.



2nd part:

Forensic auditing has takenn an important role in both private and public organizations since the down of the 21st century especially in the advance economies. The catastrophe of some formerly prominent public companies such as Enrol and WorldCom (MCI Inc.) in the late 1990s, coupled with the terrorist attacks of september 11,2001 and the recent incident incidence of frauds taken place in the corporates inluding the one in the leading public bank of Indian economy, have fueled the prominence of forensic auditing/ accounting, creating a new important and lucreative specially. Forensic auditing procedures target mostly financial and operational fraud, discovery of hidden assets, and adherence to federal regulations.
Cressy (2012) in his paper explained that in forensic auditing specific procedures are carried out in order to produce evidence. Audit techniques and procedures are used to identify and to gather evidence to prove, for example, how long have fraudulent activities existed and carried out in the organization, and how it was conducted and concealed by the perpetrators. Evidence may also be gathered to support ather issues which would be relevant in the event of a court of a court case.
Further, with the increase in the financial frauds popularly known as while coller crimes, forensic auditing and accounting have risen to prominence for ensuring the directed growth of the corporates and inclusive growth of economy.
Forensic audit is becoming increasingly frequent for top leadership searches as stringent corporate governance norms and increasing stakes are prompting Indian and multinational companies to make sure that the people they take on board have no blotches on their track record. This realizes the significance of Forensic Audit in the contemporary time for the corporates to rationalize premier principles of Good Governance.
A Ready Reference to the Significance of Forensic Audit could be rationalized as below:

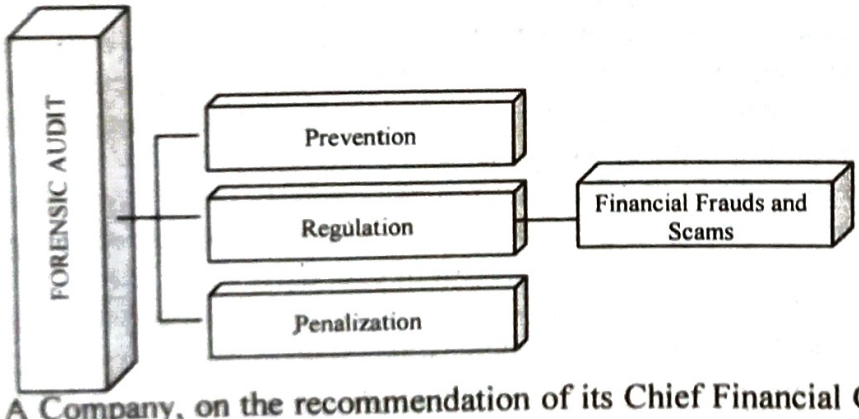
- In general, forensic auditing, which is described as a specialized field of accountancy investigates fraud and analyses financial information to be used in legal proceedings.
- In Forensic Audit, a systematic and independent examination of books, accounts statutory records, documents and vouchers of an organization is held to ascertain fraud or probability of fraud.
- Much beyond the official documents of the company, the Forensic audit involves lot of field work, trying to talk to multiple stake holders to gather information and then look for evidence to corroborate it and alike.
- It also attempts to identify or to corroborate the culprit behind the fraud.
- It arranges and collects the evidences of the fraud and the person accused of fraud.
- The collected evidences and reviewed facts are used in the legal proceedings which assist the court in granting punishment to the real accused of the fraud.
- Forensic auditing uses accounting, auditing and investigative skills to conduct investigations into theft and fraud. It encompasses both Litigation Support and Investigative Accounting.

This makes forensic audit an apt tool in the contemporary times, ensuring financial health of the companies through aiding in the Prevention, Regulation and Penalization of financial frauds and scams.

9. What are key benefits of forensic audit? **[MODEL QUESTION]**

Answer:

Forensic Audit is an examination of a company's financial records to derive evidence which can be used in a court of law or legal proceeding. In the contemporary times, when the Government is looking forward for a robust economy and nation building at par, financial stability is a must corporate. Forensic audit submits various recompenses in ensuring commercial health of the companies through aiding in the Prevention, Regulation and Penalization of financial frauds and scams.



For example, A Company, on the recommendation of its Chief Financial Officer (CFO), entered into a contract with ABC Inc for the supply of carts. At the time, ABC Inc was not authorized to conduct business, as its license was suspended due to certain irregularities in taxes paid. The CFO had knowledge of this fact, but still recommended

the company to enter into a contract with ABC Inc because he was secretly receiving compensation from ABC Inc for doing so. A forensic audit cannot reveal such cases of fraud, but could also create bunch of evidenced for the production the court of Law. This way forensic audit ensures the healthy conduct of the organization and stability and growth to the economy as a whole.

Key Advantages:
In the context, few key benefits of Forensic Audit are listed below:
1. Detection and Responsibility of Corruption: In a Forensic Audit, while investigating fraud, an auditor would look out for:

- Conflicts of interest - When fraudster uses his/her influence for personal gains detrimental to the company. For example, if a manager allows and approves inaccurate expenses of an employee with whom he has personal relations. Even though the manager is not directly financially benefitted from this approval, he is deemed likely to receive personal benefits after making such inappropriate approvals.
- Bribery- As the name suggests, offering money to get things done or influence a situation in one's favor is bribery. For example, ABC bribing an employee of B2C company to provide certain data to aid ABC in preparing a tender offer to B2C.
- Extortion- If B2C demands money in order to award a contract to ABC, then that would amount to extortion.

In this process, Forensic Adult aids in detecting the corruption in the corporate and also determines responsibility of the person liable for the corruption and its practices.

2. Detection of Asset Misappropriation: This is the most common and prevalent form of fraud Misappropriation of cash, raising fake invoices made to non-existing supplies or employees, misuse of assets, or theft of Inventory are a few examples of such asset misappropriation.

3. Detection of Financial Statement Fraud: Companies get into this type of fraud to try to show the company's financial performance as better than what it actually is. The goal of presenting fraudulent numbers may be to improve liquidity, ensure top management continue receiving bonuses, or to deal with pressure for market performance. Some examples of the form that financial statement fraud takes are the intentional forgery of accounting records, omitting transactions- either revenue or expenses, non-disclosure of relevant details from the financial statements, or not applying the requisite financial reporting standards.

4. Fraud Identification and Prevention: Fraud is quite common in big organizations where the number of daily financial transactions is huge. In such an environment, an employee can easily undertake fraudulent activities without being caught. Forensic accounting helps in analyzing whether the company's accounting policies are followed or

not, and whether all the transactions are clearly stated in the books of accounts. Any deviation observed in the books of accounts can help in identifying fraud, and necessary measures can be taken to prevent it in the future.

5. Making Sound Investment Decisions: As forensic accounting helps in analyzing the financial standing and weaknesses of a business, it provides a path for investors to make thoughtful investment decisions. A company engaged in fraud is definitely not a good option for investment. Therefore, the reports of forensic accountants act as a guide for potential investors of a company. Many organizations also apply for loans from various financial institutions. By performing an analysis, such institutions can come to a decision on whether they would like to fund a company or not.

6. Formulation of Economic Policies: Various cases of fraud that becomes evident after forensic analysis act as a reference for the government to formulate improved economic policies that would be able to curb such fraudulent activities in the future. By doing so, the government can strengthen the economy and prevent such illegal activities in the country.

7. Rewarding Career Opportunity: As a career, forensic auditing is extremely rewarding, as it not only involves regular auditing and accounting activities, but also involves identification, analysis, and reporting of the findings during an audit. The acceptance of reports generated by a forensic auditors by the court of law, gives them an upper hand as compared to other accountants. Good forensic auditors are in high demand and can easily draw a striking starting salaries around the globe.

Other Advantages

- **Objectivity and Credibility:** An external party as a forensic auditor would be far more independent and objective than an internal auditor or company accountant who ultimately reports to management on his findings. An established firm og forensic auditors and its team would also have credibility stemming from the firm's reputation, network and track record.
- **Accounting Expertise and Industry Knowledge-** An external forensic auditor would add to the organization's investigation team with breadth and depth of experience and deep industry expertise in handling frauds of the nature encountered by the organization.
- **Provision of Valuable Manpower Resources-**An organization on the midst of reorganization and restructuring following a major fraud would hardly have the full-time resources to handle a broad-based exhaustive investigation. The forensic audit and his team of assistants would provide the much needed experiences resources, thereby freeing the organization's staff for other more immediate management demands. This is all the more critical when the nature of the fraud calls for management to move quickly to contain the problem and when resources cannot be mobilized in time.

- **Enhanced Effectiveness and Efficiency-** This arises from the additional dimension and depth which experienced individuals in fraud investigation bring with them to focus on the issues at hand. Such individuals are specialists in rooting out draud and would recognize transactions normally passed over by the organization's accountants or auditors.

10. What is need and benefits of forensic audit? [MODEL QUESTION]

Answer:

Time and again, it has been established thta corporate frauds are one of the major hindrances to the inclusive growth of the economy the rise in corporate frauds is directly proportionate to the fall of economy. Corporate fraud schemes go beyond the scope of an employee's stated position, and are marked by their complexity and economic impact on the business, other employees and outside parties.

As per the report submitted by Goldman Sachs on the Impact of PNB Scam on indian Economy, it is stated that "To global investors, India's economy may seem a bit like a raw mango these days-enticing from a distance but bitter to taste; good for pickles, and not much seem a bit like a raw mango these days-enticing from a distance but bitter to taste; good for pickles, and not much more. That Goldman Sachs cut India's economic growth estimate from 8% to 7.6% for financial year 2019 may not be a surprise after the swell of back scams that have washed over handlines in the last few weeks. The globalinvestment bank has cited tha $2 billion fraud at the state-run Punjab National Bank(PNB) among the reasons for slashing the projections for the world's fastest-growing major economy. It is feared that the fraud is just the beginning of a prolonged period of pain for the Indian economy. "Markets and investors are questioning wheather the problem is more systemic, "the analysts wrote in the mote to clients.

Indeed, in the days following the revelation that billionaire jewellers, Nirav Modi and Mehul Choksi, duped India's second-largest government bank, the PNB stock has lost more than a quarter of its market value. Other public sector bank scrips have tumbled, too."

In the previous years too, India has witnessed financial francial frauds which affected the golden growth of India's economy. The Investigations and risk consulting firm Kroll unearthed in there survey that 69% of companies studied were affected by fraud in Financial Year of 2013, up from 68% in the previous year. The value of fraud, the study found, rose, to 71% from 67%. Insider fraud was particularly rife in India, with 89% of respondents indicating the perpetrator was an insider of some sort – a junior, middle management or senior employee, or an agent. That's the reason that a team of Deloitte Forensic (India) pointed out,forensic audit practices have evolved significantly over the last 10-15 years. He added that "earlier the investigations were restricted to books and records but now there is a significant of intelligence gathering. The technology, analytics and professional expertise have a greater play in every aspect of forensic auditing"

Indeed, the recent upswin in the financial frauds in India, compelling more management to conduct forensic audits in the interest of our growing economy. Experts on white-collar crimes say forensic auditing is not just gaining prominence, the methods are changing fast.

From all the past incidences, it has been found that Crimes are of all hues, seven in particular:

i) Theft of physical assets, ii) Theft of information, iii) Corruption and Briberry, iv) Internal financial fraud, v) Vendor fraud, vi) Management conflict of interest and v) Regulatory breach, are high in their perspectives of corporate fraud.

That's not surprising given how the incidence of corporate fraud is on the rise. But other spaces too are exposed to fraud, which is why the scope and need of forrnsic auditing is getting wider.

Kroll observed that there are other reasons like ensuing financial stability, holding accountability of the accused and deterring the future fraudsters alike are also giving rise to the need and significance of Forensic Audit.

Further, provisions of the new Companies Act mean that every company now has to have proactive fraud risk management policies. The Act requires independent directors to increase safeguards against fraud and reminds them of their whistle blowing responsibilities. Objections must be documented, and now that the Act defines fraud and safeguards explicitly, ignorance of the parameters of either will no longer be a defense.

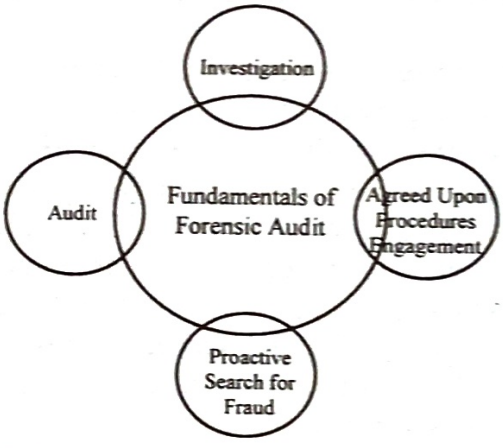
Companies Act, 2013
— A big leap to prevent and punish fraud

11. What are fundamentals of forensic audit? **[MODEL QUESTION]**

Answer:

Forensic Auditing is a discipline of detecting frauds in the organizations and gathering and presenting financial information in a form of evidences that will be accepted by a court of jurisprudence against perpetrators of economic crimes.

The integration of accounting, auditing and investigative skills and evidences yields the specialty known as Forensic Auditing which focuses very closely on detecting or preventing financial fraud.



"Forensic", according to the Webster's Dictionary means, "Belonging to, used in or suitable to courts of judicature or to public discussion and debate".

The word "Auding " is defined as the examination or inspection of various books of accounts by an auditor followed by physical checking to make sure that all departments are following documented system of recording transactions. It is done to ascrtain the accuracy of financial statements provided by the organization.

With India being ranked as the 78th in Global Corruption Perception Index, the needs audit become all the more profound to strength the corporate culture with the vibes of good governance in the country.

The term forensic auditing' refers to financial fraud investigation which includes the analysis of various books of accounts to prove or disprove financial fraud and serving as an expert witness in Court to prove or disprove the same.
Thus basically, forensic auditing is the use of accounting or secretarial skills for legal purposes.

Major fundamentals of Forensic Audit involves:
1. An audit
2. An investigatiion
3. An agreed-upon procedures engagement
4. A proactive search for fraud

1. Forensic Audit: An examination of evidence ragerding an assertion to review its trail for reporting in a manner regarded suitable by the court of law.

2. Forensic Investigatiion: The utilization of specialized investigative skills in carrying out an inquiry conducted in such a manner that the outcome will have application to a court of law. A Forensic Investigation may be grounded in accounting, medicine, engineering or some other discipline.

3. Agreed-upon procedural engagement: As the purpose of the forensic audit is to ensure that there is no financial deception in the organizations and it collects evidences after the examination of accounts and its records, therefore, it is required that forensic audit is done under the agreed procedures of Audit and Evidences. For instance for Company Audit, the auditor is required to prepare the audit report in accordance with the Company, such as fixed assets, inventories, internal audit standards, internal controls, statutory dues, among others. Besides, the agency or entity directing the engagement should have locus standi on the matter.

4. Predicting the Unpredictable - A Proactive Search: A proactive search for fraud comprises a Forensic Audit Thinking. Forensic Audit Thinking involves-

- The critical assessment throughout the audit
- Of all evidential matter and
- Maintaining a higher degree of professional skepticism
- That fraud may have occurred, is occurring, or will occur in the future.

It further involves deciphering pattern, evaluating reports with figures to study their number patterns and comparing them with standards established looking for prima facie area of suspicion.
In this scenario, Forensic auditing aids in detecting, investigating and preventing frauds. Whether it is stock market fraud or bank fraud; forensic auditing seems to be an essential tool for investigation and defining evidences against perpetrators.

12. Write a short note on ISO-27001:2013. **[MODEL QUESTION]**

Answer:

ISO 27001:2013 is an international security standard that lays out best practices for how organizations should manage their data. It outlines how companies should manage information security risk by creating an information security management system (ISMS). This approach demands executive leadership while embedding data security at all organizational levels. The standard is voluntary, but organizations that follow its guidelines can seek ISO 27001 certification.

ISO 27001 was developed in tandem by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). It was originally released in 2005 and revised in 2013, thus its full title: ISO/IEC 27001:2013.

For companies that earn ISO 27001 certification, it's a sign of their commitment to data security. But even companies not seeking certification should pay attention to ISO 27001's lessons.

Essentially, all the guidelines in ISO 27001 add up to one thing: a guide for creating an ISMS. An ISMS describes the structures an organization has in place to manage data, including technology, physical security, personnel policies, and organizational hierarchy that delegates responsibility for these issues.

ISO 27001:2013 certification is an important thing to look for in any cyber security partner because it indicates an organization-wide commitment to security. Working with such a partner can benefit your own organization's security. As Clause 6 states, sometimes the most effective way to deal with data security risk is to either eliminate it or outsource it to a third-party.

For example, by choosing an identity and access management (IAM) partner to manage your user passwords, you offload some risk by not storing sensitive data on your own servers. And using an ISO 27001-certified IAM provider (as Auth0 has done since 2018) sends a message to your own users and partners that your data is secure.

ISO 27001 is also the cornerstone of a growing international consensus about data security best practices. Australia based its federal Digital Security Policy on ISO 27001. Likewise, ISO 27001 can provide guidance on how to meet the standards of other data privacy laws, such as the GDPR, which often direct companies to it as an example of universal best practices. So if you abide by ISO 27001's recommendations, you're on the right track for legal compliance, not to mention improved data security.

CYBER ETHICS & LAWS

Multiple Choice Type Questions

1. Many Cyber Crimes comes under Indian Penal Code Which one of the following is example? [MODEL QUESTION]
   a) Sending Threatening message by Email
   b) Forgery of Electronic Record
   c) Bogus Website
   d) All of above

Answer: (d)

2. The Information Technology Act 2000 is an Act of Indian Parliament notified on [MODEL QUESTION]
   a) 27th October 2000
   b) 15th December 2000
   c) 17th November 2000
   d) 17th October 2000

Answer: (d)

3. Digital Signature Certificate is _____ requirement under various applications. [MODEL QUESTION]
   a) Statutory
   b) Legislative
   c) Govenmental
   d) Voluntary

Answer: (a)

4. Assessing Computer without prior authorization is a cyber crime that comes under [MODEL QUESTION]
   a) Section 65
   b) Section 66
   c) Section 68
   d) Section 70

Answer: (b)

5. _____ means a person who has been granted a licence to issue a electronic signature Certificate. [MODEL QUESTION]
   a) Certifying Authority
   b) Certifying private key Authority
   c) Certifying system controller
   d) Appropriate Authority

Answer: (a)

6. _____ is a data that has been organized or presented in a meaningful manner. [MODEL QUESTION]
   a) A process
   b) Software
   c) Storage
   d) Information

Answer: (d)

7. _____ is an application of information and communication technology (ICT) for delivering Government Service. [MODEL QUESTION]
   a) Governance
   b) Electronic Governance
   c) Governance and ethics
   d) Risk and Governance

Answer: (b)

8. The Altering of data so that it is not usable unless the changes are undone is **[MODEL QUESTION]**

a) Biometrics **b) Encryption** **c) Ergonomics** **d) Compression**

Answer: (b)

9. Authentication is _____ **[MODEL QUESTION]**

a) To assure identity of user on a remote system **b) Insertion**

c) Modification **d) Integration**

Answer: (a)

10. The following cannot be exploited by assigning or by licensing the rights of others **[MODEL QUESTION]**

a) Patent **b) Design** **c) Trademark** **d) All of these**

Answer: (c)

Short Answer Type Questions

1. What is the need of cyber law? Write about cyber laws in India? **[MODEL QUESTION]**

Answer:

1st part:

In today's techno-sawy environment the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

In today's highly digitalized world, almost everyone is affected by cyber law.

For example:

Almost all transactions in shares are in demat form.

Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.

Government forms including income tax returns, company law forms etc. are now filled in electronic form.

Consumers are increasingly using credit/debit cards for shopping.

Most people are using email phones and SMS messages for communication.

Even in "non-cyber crime" cases, important evidence is found in computers/cell phones eg: in cases of murder, divorce, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.

Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.

Digital signatures and e-contracts are fast replacing conventional method of transacting business.

2nd part:

In India cyber laws are contained in the Information technology Act, 2000("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgement found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the need for enactment of relevant cyber laws.

None of the existing laws gave any legal validity or sanction to the activities in cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email id not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the parliament. As such the need has arisen for cyber law.

2. What is commerce? What is E-commerce? [MODEL QUESTION]

Answer:

Commerce is an important part of a business. It is nothing but buying and selling of goods, which means when we buy a product or service to others, and then it is called as commerce.

E-commerce can be broadly defined as the process of buying and selling of goods or services using an electronic medium such as the Internet. It is also referred as a paperless exchange of business information using EDI, E-mail, electronic fund transfer, etc.

3. Name some advantages of E-Commerce. [MODEL QUESTION]

Answer:

1. Global scope: It provides the sellers with a global reach. Now sellers and buyers can meet in the virtual world, without a geographical barrier.

2. Electronic transaction: E-commerce reduces the paper work and significantly lowers the transaction cost. It enables the use of credit cards, debit cards, smart cards, electronic fund transfer via bank's website and other modes of electronic payment.

3. Cost saving: E-commerce application provides users with more options to compare and select the cheaper and better option. It helps in reducing services such as healthcare, the cost of searching a product, etc. E-commerce has enabled rural areas to access services and products, which are otherwise not available to them.

4. Anytime shopping: One other great advantage is the convenience. A customer can shop 24×7. The website is functional at all times; it does not have working hours like a shop.

5. No intermediaries: Electronic commerce also allows the customer and the business to be in touch directly, without any intermediaries. This allows for quick communication and transactions.

6. Public services: E-commerce helps the government to deliver public e education, social services at a reduced cost and in an improved manner.

4. List the differences between Traditional commerce and E-commerce. **[MODEL QUESTION]**

Answer:

Traditional commerce	E-commerce
It focuses on the exchange of products and services through personal interactions, so it is manual.	Trading activities are online via the internet and can be considered automatic.
Traditional commerce is limited to business hours i.e. during the day	It is 24×7; it can be done anytime day and night.
Traditional commerce provides face to face customer interaction.	It can be termed as screen to face interaction.
It is limited to a particular geographic location.	It is global and has no physical limitation.
Modes of payment: cash, cheques and credit cards.	Modes of payment: bank transfer, credit cards, e-wallet, mobile payment and many more.
Delivery of goods or services is instant.	Delivery of goods or services takes some time.
Its scope is local.	Its scope is global.

5. List disadvantages of E-Commerce. **[MODEL QUESTION]**

Answer:

1. Setup cost: The setup of the hardware and the software, the training cost of employees, the constant maintenance and upkeep are all quite expensive

2. Physical presence: This lack of a personal touch can be a disadvantage for many types of services and products like interior designing or business.

3. Security: Security is another area of concern. Credit card theft, identity theft etc. remain big concerns with the customers.

4. Goods delivery: There may arrive some problem with fulfilment of order. Even after the order is placed there can be problems with shipping, delivery, mix-ups etc. This leaves the customers unhappy and dissatisfied.

6. What are the types of E-Commerce? **[MODEL QUESTION]**

Answer:

i) Business – to – Consumer (B2C):

In B2C model, business sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same.

The website will then send a notification to the business organization via email and the organization will dispatch the product/ goods to the customer. These B2C businesses are online retailers. Example: Amazon, Flipchart, etc.

ii) Business – to – Business (B2B):
In B2B model, business sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the product to the final customer who comes to buy the product at one of its retail outlets. Example: Tata communications (network provider).

iii) Consumer – to – Consumer (C2C):
In C2C model, consumer helps consumer to sell their assets like residential property, cars, motorcycles , or rent a room by publishing their information on the website. Website may or may not charge the consumer for its services. Example - OLX, Quirk, online auction.

iv) Consumer – to – Business (C2B):
In this model, consumers have products or services of value that can be consumed by businesses. For example, the comparison of interest rates of personal loan/car loan provided by various banks via websites. A business organization that fulfills the consumer's requirement within the specified budget approaches the customer and provides its services.

7. What is E-Governance? Enlist the types of E-Governance. List the advantages of E-Governance. [MODEL QUESTION]

Answer:

E-Governance: It signifies the implementation of information technology in the government processes and functions so as to cause simple, moral, accountable and transparent governance. The basic purpose of e-governance is to simplify processes for all, i.e. government, citizens, businesses etc. at National, State and local levels.
Hence, E-governance delivers SMART government. (S- Simple, M-Moral, A-Accessible, R-Responsive, T-Transparent Government)

Types of E-Governance:
i) Government-to-Citizen (G2C)
ii) Government-to-Business (G2B)
iii) Government-to-Government (G2G)
iv) Government-to-Employee (G2E)

Advantages of E-Governance:
i) Reduced corruption
ii) High transparency
iii) Increased convenience

iv) Direct participation of constituents
v) Reduction in overall cost.
vi) Expanded reach of government

8. What is Government-to-Citizen E-Governance? [MODEL QUESTION]

Answer:

This refers to the government services which enable citizens to get access to wide variety of public services. Most of the government services fall under G2C. It helps the ordinary people reduce the time and cost to conduct a transaction. A citizen can have access to the services anytime from anywhere. Many services like license renewals and paying tax are essential in G2C. It also focuses on geographic land barriers.

9. Explain Government-to-Business (G2B) type E-Governance. [MODEL QUESTION]

Answer:

The Government to business is the exchange of services between Government and Business organizations. G2B provides access to relevant forms needed to comply. The G2B also consists of many services exchanged between business sectors and government. It aims at eliminating paper work, saving time, cost and establish transparency in the business environment, while interacting with government.

10. What is Government-to-Government (G2G)? [MODEL QUESTION]

Answer:

The Government-to-Government refers to the interaction between different government departments, organizations and agencies. In G2G, government agencies can share the same database using online communication. The government departments can work together. G2G services can be at the local level or the international level. Likewise, it provides safe and secure inter-relationship between domestic or foreign government.

11. Write a note on Government-to-Employee (G2E). [MODEL QUESTION]

Answer:

The Government-to-Employee is the internal part of G2G sector. G2E aims to bring employees together and improvise knowledge sharing. It provides online facilities to the employees like applying for leave, reviewing salary payment record and checking the balance of holiday. The G2E sector provides human resource training and development. G2E is also the relationship between employees, government institutions and their management.

12. List some effective examples of successful implementation of E-Governance projects. [MODEL QUESTION]

Answer:

1. e-Mitra project (Rajasthan)
2. e-Seva project (Andhra Pradesh)
3. CET (Common Entrance Test)
4. AADHAAR card

5. DigiLocker
6. Bharat Bill Payment System
7. PAN
8. EPFO services
9. PMKVY services

Long Answer Type Questions

1. What is Controller of Certifying Authorities (CCA)? Mention role of Certifying Authorities. [MODEL QUESTION]

Answer:

1st part:

The IT Act accommodates the Controller of Certifying Authorities (CCA) to permit and direct the working of Certifying Authorities. The Certifying Authorities (CAs) issue computerized signature testaments for electronic confirmation of clients. The Controller of Certifying Authorities (CCA) has been named by the Central Government under Section 17 of the Act for reasons for the IT Act. The Office of the CCA appeared on November 1, 2000. It targets advancing the development of E-Commerce and E-Governance through the wide utilization of computerized marks.

The Controller of Certifying Authorities (CCA) has set up the Root Certifying Authority (RCAI) of India under segment 18(b) of the IT Act to carefully sign the open keys of Certifying Authorities (CA) in the nation. The RCAI is worked according to the gauges set down under the Act. The CCA guarantees the open keys of CAs utilizing its own private key, which empowers clients in the internet to confirm that a given testament is given by an authorized CA. For this reason it works, the Root Certifying Authority of India (RCAI). The CCA likewise keeps up the Repository of Digital Certificates, which contains all the authentications gave to the CAs in the nation.

2nd part:

Certificate Authority (CA) is a confided in substance that issues Digital Certificates and open private key sets. The job of the Certificate Authority (CA) is to ensure that the individual allowed the extraordinary authentication is, truth be told, who the individual in question professes to be.

The Certificate Authority (CA) checks that the proprietor of the declaration is who he says he is. A Certificate Authority (CA) can be a confided in outsider which is answerable for genuinely confirming the authenticity of the personality of an individual or association before giving an advanced authentication. A Certificate Authority (CA) can be an outer (open) Certificate Authority (CA) like sign, or an inward (private) Certificate Authority (CA) arranged inside our system. Certificate Authority (CA) is a basic security administration in a system. A Certificate Authority (CA) plays out the accompanying capacities. A Controller plays out a few or the entirety of the following roles:

1. Administer the exercises of the Certifying Authorities and furthermore confirm their open keys.

2. Set out the guidelines that the Certifying Authorities follow.
3. Determine the accompanying capabilities and furthermore experience necessities of the workers of all Certifying Authorities conditions that the Certifying Authorities must follow for directing business the substance of the printed, composed, and furthermore visual materials and ads in regard of the advanced mark and the open key the structure and substance of an advanced mark declaration and the key the structure and way where the Certifying Authorities look after records terms and conditions for the arrangement of examiners and their compensation.
4. Encourage the Certifying Authority to set up an electronic framework, either exclusively or together with other Certifying Authorities and its guideline.
5. Indicate the way where the Certifying Authorities manage the endorsers.
6. Resolve any irreconcilable situation between the Certifying Authorities and the endorsers.
7. Set out the obligations of the Certifying Authorities.
8. Keep up a database containing the revelation record of each Certifying Authority with all the subtleties according to guidelines. Further, this database is open to the general population.

Certificate Authority (CA) Verifies the personality: The Certificate Authority (CA) must approve the character of the element who mentioned a computerized authentication before giving it. Certificate Authority (CA) issues computerized testaments: Once the approval procedure is finished, the Certificate Authority (CA) gives the advanced authentication to the element who requested it. Computerized declarations can be utilized for encryption (Example: Encrypting web traffic), code marking, authentication and so on. Certificate Authority (CA) keeps up Certificate Revocation List (CRL): The Certificate Authority (CA) keeps up Certificate Revocation List (CRL).

An authentication repudiation list (CRL) is a rundown of computerized testaments which are not, at this point legitimate and have been disavowed and subsequently ought not be depended by anybody. A Certificate Authority (CA) is a selective element which issues and signs SSL endorsements, confirming and guaranteeing the reliability of their proprietors. All CAs are individuals from the CA/B Forum (Certificate Authority and Browser Forum), being subjects to industry guidelines, principles, and prerequisites, and are every year examined to guarantee their consistence. The CA is a basic component when talking about SSL Certificates. The CA recognizes and verifies the character of the SSL Certificate's proprietor when giving and marking the SSL Certificate. In view of the SSL Certificate's sort, the CA completely checks the candidate's area name, business and individual data, and different qualifications before giving the testament.

2. What do you understand by intellectual property in cyberspace?

[MODEL QUESTION]

Answer:

Intellectual Property (IP) simply refers to the creation of the mind. It refers to the possession of thought or design by the one who came up with it. It offers the owner of any inventive design or any form of distinct work some exclusive rights, that make it unlawful to copy or reuse that work without the owner's permission. It is a part of

property law. People associated with literature, music, invention, etc. can use it in business practices.
There are numerous types of tools of protection that come under the term "intellectual property".

Cyberspace is the non-physical domain where numerous computers are connected through computer networks to establish communication between them. With the expansion of technology, cyberspace has come within reach of every individual. This fact led to the emergence of cyberspace as a business platform and hence increases pressure on Intellectual Property. Nowadays, cyber crimes do not solely limit themselves to fraud, cyberbullying, identity thefts but also an infringement of copyrights and trademarks of various businesses and other organizations. Online content needs to be protected and hence Intellectual Property Rights and Cyber laws cannot be separated.
In cyberspace, sometimes one person makes a profit by using another person's creation without the owner's consent. This is a violation of privacy, and it is protected by IPR. We have certain laws to avoid violation of Intellectual Property Rights in cyberspace and when it is violated, then additionally we have several remedies in law.

Copyright Infringement:
Copyright protection is given to the owner of any published artistic, literary, or scientific work over his work to prohibit everyone else from exploiting that work in his name and thereby gain profit from it.
When these proprietary creations are utilized by anyone without the permission of the owner, it leads to copyright infringement. If copies of any software are made and sold on the internet without the permission of the owner or even copying the content from any online source, these all are examples of copyright infringement.

Copyright Issues in Cyberspace:
1. Linking –
It permits a Website user to visit another location on the Internet. By simply clicking on a word or image on one Web page, the user can view another Web page elsewhere in the world, or simply elsewhere on the same server as the original page.
Linking damages the rights or interests of the owner of the Linked webpage. It may create the supposition that the two linked sites are the same and promote the same idea. In this way, the linked sites can lose their income as it is often equal to the number of persons who visit their page.

2. Software Piracy –
Software piracy refers to the act of stealing software that is lawfully shielded. This stealing comprises various actions like copying, spreading, altering, or trading the software. It also comes under the Indian copyright act.

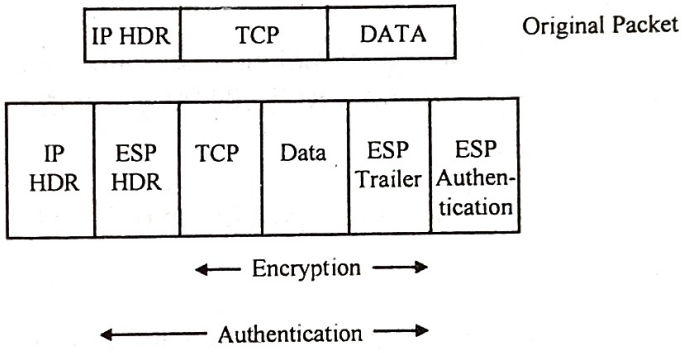
Components of IP Security –
It has the following components:

A. Encapsulating Security Payload (ESP) –
It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

B. Authentication Header (AH) –
It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

IP HDR	AH	TCP	DATA

C. Internet Key Exchange (IKE) –
It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.
Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts (using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.

Components of IP Security –

It has the following components:

A. Encapsulating Security Payload (ESP) –

It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

B. Authentication Header (AH) –

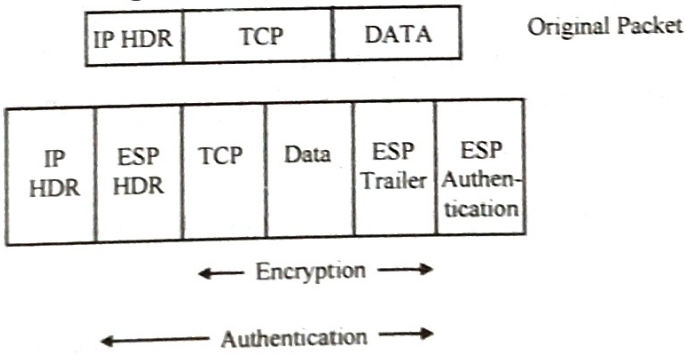
It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

IP HDR	AH	TCP	DATA

C. Internet Key Exchange (IKE) –

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts (using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.

4. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

4. What are offences under IT act 2000? **[MODEL QUESTION]**

Answer:

Section 43: Where a person without the permission of owner or any other person in charge damage the computer, or Computer System, or Computer Network, The he shall be liable for Penalty and Compensation to such person so affected.

Section 44: Where a person fails to furnish any document, return, report to the controller, or certifying authority, then he shall be liable to pay penalty up to Rs. 1,50,000/- per failure. Further where a person fails to furnish any information, books or other documents within the time specified, then he shall be liable to pay penalty upto Rs.5,000/- per day. Further provided that where a person fails to maintain books of accounts or other records, then he shall be liable to pay penalty upto Rs.10,000/- per day.

Section 65: Any person tamper, conceal, destroy, or alter any computer source document intentionally, then he shall be liable to pay penalty upto Rs.2,00,000/-, or imprisonment upto 3 years, or both.

Section 66: Any person dishonestly, or fraudlently does any act as referred in Section 43, then he shall be liable to pay penalty upto Rs.5,00,000/-, or imprisonment upto 3 years, or both.

Section 43: then he shall be liable to pay penalty upto Rs. 5,00,000/- or Imprisonment upto 3 years, or both.

Section 66B: Any person dishonestly, or Fraudulently receives or retains any stolen computer resource or communication device, then he shall be liable to pay penalty upto Rs.1,00,000/-, or imprisonment upto 3 years, or both.

Section 66F: Any person dishonestly or fraudulently make use of Electronic signature, password or any other unique identification feature of any other person, then he shall be liable to pay penalty upto 3 years or both.

Section 67: Any person publishes or transmits in electronic from any material which appeals to prurient interest, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see, or hear matter contained in it, then he shall be liable to pay penalty upto Rs.5,00,000/-, or imprisonment upto 3 years, or both and in the event

of second or subsequent conviction, he shall be liable to pay penalty upto Rs.10,00,000/-, or imprisonment upto 5 years, or both.

Section 67A: Any person publishes or transmits in electronic from any materia which contains sexually explicit act, or conduct, then he shall be liable to pay penalty upto Rs.10,00,000/-, or imprisonment upto 5 years, or both and in the event of second or subsequent conviction, he shall be liable to pay penalty upto Rs.10,00,000/-, or imprisonment upto 7 years, or both.

Section 66E: Any person intentionally captures, publishes, or transmit image of private area of any person without consent, then he shall be liable to pay penalty upto Rs.2,00,000/-, or imprisonment of 3 years or both.

Sectoion 66F: Any person does any act electronically, or with use of intent to threanten unity, integrity, security, or sovereignty of India, then he shall punishable with imprisonment for life.

Section 68: The controller may, by order, direct a certifying authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under and if any person who intentionally or knowingly fails to comply with the order, then he shall be liable to pay penalty upto Rs.1,00,000/-, or imprisonment upto 2 years, or both.

Section 69: Where the Central Government or a state Government or any of its officers specially authorized by the Central Government or the state Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence Of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence recorded in writing, by order, direct any agency of the appropriate government to intercept ,monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted , received or stored in any computer resource , any person who fails to comply with the order ,then he shall be liable to imprisonment of 7 years , along with the fine (amount of fine is not specified in the act).

Section 70: The appropriate government may be notification in the official Gazette, declare any computer resource which directly or indirectly affects the facility to critical information infrastructure, to be a protected system, any person who fails to comply with the notification, then he shall be liable to imprisonment of 10 years, along with the fine(amount of the fine is not specified).

Section 71: Whoever makes any misrepresentation to or suppresses any material fact from the controller or the certifying Authority for obtaining any License or Electronic

Signature certificate, the case may be then he shall be liable to pay penalty upto Rs.1,00,000/- , or imprisonment upto 2 years or both.

Section 72: If any person who has secured access to any electronic record book, register, correspondence, information, document or other material without the consent of the person concerned disclosed such electronic record book, register, correspondence, information, document or other material to any other person, then he shall be liable to pay upto Rs.1,00,000/- , or imprisonment upto 2 years or both.

Section 72A: If any person who has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, then he shall be liable to pay penalty upto Rs.5,00,000/-, or imprisonment upto 3 years , or both.

Section 73: If a person publishes a electronic signature certificate, or make it available to any other person with the knowledge that

- Certifying authority has not issued it , or
- Subscriber has not accepted it, or
- Certificate has been revoked or suspended

then he shall be liable to pay penalty upto Rs.1,00,000/- , or imprisonment upto 2 years , or both.

Section 74: If any person knowingly creates, publishes or otherwise makes available electronic signature certificate for any fraudulent or unlawful purpose, then he shall be liable to pay penalty upto Rs.1,00,000/- , or imprisonment upto 2 years or both.

Section 75: If any person committed an offence or contravention committed outside India, and if the actor conduct constituting the offence or contravention involves a computer, computer system or computer network located in India , then the provisions of this act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

Section 76: Any computer , computer system, floppies, compact disks , tape drives or any other accessories related thereto , in respect of which any provision of this Act, rules, orders or regulations ,made there under has been or is being contravened , shall be liable to confiscation. However, if it is proved that such resources were not used in committing fraud then only person in default will be arrested.