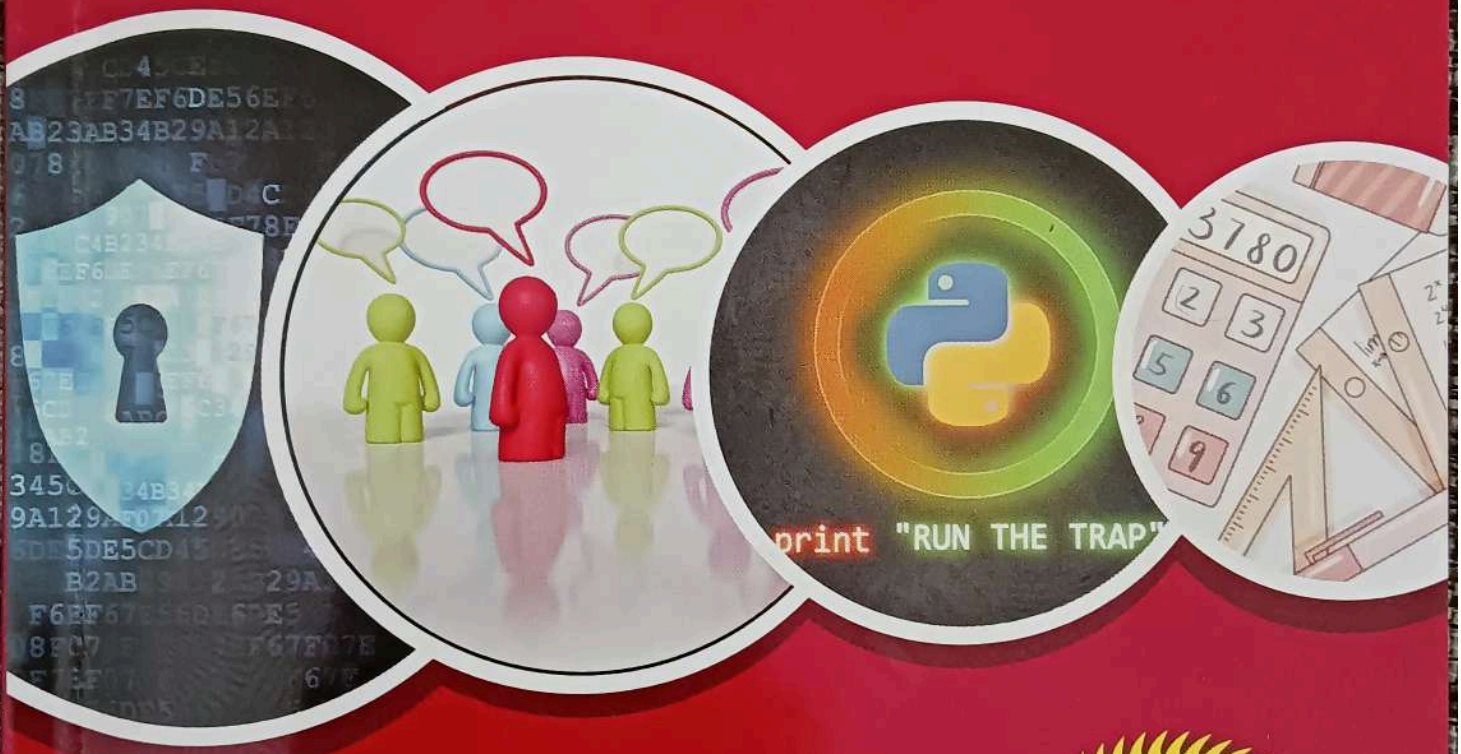
Quantum Series

ENGINEERING

QUANTUM Series

Semester - 3 & 4 Common to All Branches

Cyber Security



- Topic-wise coverage of entire syllabus in Question-Answer form.
- Short Questions (2 Marks)

Session 2023-24 Odd & Even Semester

CONTENTS

BCC301 / BCC401 : Cyber Security

UNIT-4 : UNDERSTANDING COMPUTER FORENSICS

(4–1 W to 4–26 W)

Understanding computer forensics: Introduction, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation.

Forensics and Social Networking Sites: The Security/ Privacy Threats, Challenges in Computer Forensics.

UNIT-5 : INTRODUCTION TO SECURITY POLICIES & CYBER LAWS

(5–1 W to 5–21 W)

Need for an Information Security Policy, Introduction to Indian Cyber Law, Objective and Scope of the Digital Personal Data Protection Act 2023, Intellectual Property Issues, Overview of Intellectual Property Related Legislation in India, Patent, Copyright, Trademarks.

SHORT QUESTIONS

(SQ–1 W to SQ–24 W)

1
UNIT

Introduction to Cyber Crime

CONTENTS

PART-1

Definition and Origins of the Word Cyber Crime and Information Security.

Que 1.1. What is the definition of cyber crime ? Discuss types of attacks prevalent in cyber crime.

Answer

Definition : Cyber crime specifically can be defined in a number of ways; a few definitions are :

1. Cyber crime refers to criminal activities that are carried out using computers, networks, and digital technology.
2. Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.
3. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
4. Any financial dishonesty that takes place in a computer environment.
5. Any threats to the computer itself, such as theft of hardware or software, damage and demands for money.
6. Cyber crime is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.

Types of attacks prevalent in cyber crime : Two types of attacks are prevalent :

1. **Techno-crime :** Techno-crime, also known as technology-enabled crime, refers to criminal activities that are facilitated or significantly enhanced by the use of technology or digital devices. These crimes can encompass a wide range of illegal actions, and they often exploit the capabilities and vulnerabilities of technology to commit offenses.
2. **Techno-vandalism :** Techno-vandalism is a specific subset of techno-crime that involves malicious acts aimed at damaging or defacing digital property or online resources. It often involves unauthorized modifications, deletions, or disruptions of digital content or services.

Que 1.2. Explain the origins of the word "cybercrime".

Answer

1. The term "cybercrime" has its origins in the combination of two words : "cyber" and "crime".

2. **Cyber :** The word "cyber" is derived from the Greek word "kubernetes," which means "steersman" or "pilot". It was later adapted into English to refer to control, communication, and information systems, particularly those related to computers and computer networks.
3. **Crime :** "Crime" is a well-established term that refers to unlawful activities or acts that are in violation of laws and regulations. It encompasses a wide range of illegal behaviors and actions, including theft, fraud, violence, and more.
4. The term "cybercrime" was coined by combining "cyber" and "crime" to describe criminal activities that are conducted in the digital realm using computers, computer networks, and information technology.
5. It became increasingly relevant as technology and the internet gained prominence in the late 20th century.

Que 1.3. How do cyber crimes differ from traditional crimes ?

Answer

S. No.	Aspect	Cybercrimes	Traditional Crimes
1.	Nature of crime	Crimes committed using digital technology and the internet.	Crimes committed through physical means, without digital technology.
2.	Location	Perpetrated in the virtual space, often globally.	Occur in physical locations, such as streets, homes, businesses, etc.
3.	Means of execution	Relies on computers, networks, and online platforms.	Relies on physical actions, weapons, and face-to-face interactions.
4.	Evidence	Digital evidence, including logs, data trails, and IP addresses.	Physical evidence like fingerprints, DNA, and surveillance footage.
5.	Reach	Can target victims worldwide, regardless of geographic location.	Primarily constrained by geography, often local or regional.

Que 1.4. Explain information security. How does information security relate to the prevention of cyber crimes ?

Answer

Information security :

1. Information security is the practice of protecting information by mitigating information risks.
2. It encompasses the strategies, policies, procedures, and technologies that organizations and individuals use to ensure the confidentiality, integrity, and availability of their sensitive data and information.
3. Information security aims to safeguard information from unauthorized access, disclosure, alteration, and destruction.

Information security and prevention of cyber crimes : Here's how information security relates to the prevention of cyber crimes :

1. **Confidentiality :** Information security measures, such as encryption and access controls, help maintain the confidentiality of sensitive data.
2. **Integrity :** Information security mechanisms ensure the integrity of data, which means that data remains accurate and unaltered by unauthorized individuals.
3. **Availability :** Cybercriminals may launch attacks to disrupt online services and make them unavailable. Information security measures help ensure the availability of critical systems and data.
4. **Authentication and authorization :** Information security involves user authentication and authorization. By implementing strong authentication and authorization mechanisms, organizations can reduce the risk of cyber crimes.
5. **Vulnerability management :** Information security practices include vulnerability assessments and patch management. Addressing vulnerabilities promptly reduces the risk of cybercriminals exploiting security flaws.

PART-2

Who are Cybercriminals.

Que 1.5. Who are cybercriminals ? What are their types ?

Answer

Cybercriminals :

1. Cybercriminals are individuals or groups who engage in illegal activities in the digital realm, using technology and the internet to commit various forms of cybercrime.
2. They exploit vulnerabilities in computer systems, networks, and online platforms for financial gain, personal motives, or to disrupt and harm others.

Types of cybercriminals : Following are different types of cybercriminals :

A. Type I : Cybercriminals - Hungry for Recognition :

1. **Hobby hackers :** These are individuals who engage in hacking activities as a pastime. They may not necessarily have malicious intent but can inadvertently cause harm.
2. **IT professionals (social engineering) :** IT professionals with expertise in manipulating people through social engineering techniques can pose a significant threat. They use psychological tactics to trick individuals.
3. **Politically motivated hackers :** These individuals or groups have a specific political agenda and use hacking as a means to advance their causes.
4. **Terrorist organizations :** Some terrorist groups use cyber attacks to further their objectives, including spreading propaganda, recruiting members, or disrupting critical infrastructure.

B. Type II : Cybercriminals - Not Interested in Recognition :

1. **Psychological perverts :** These individuals engage in cybercrimes that involve harassment, cyberbullying, online stalking, or sharing explicit content without consent.
2. **Financially motivated hackers :** This group seeks financial gain through cybercrimes such as corporate espionage. They target organizations to steal sensitive data for monetary profit.
3. **State-sponsored hacking :** Nation-states engage in cyber espionage and sabotage to gather intelligence, disrupt rival nations, or engage in cyber warfare.
4. **Organized criminals :** Organized criminal groups engage in various cybercrimes, such as credit card fraud, ransomware attacks, and identity theft, for financial gain.

C. Type III : Cybercriminals - The Insiders :

1. **Disgruntled or former employees seeking revenge :** These individuals have insider knowledge of an organization's systems and processes, making them potent threats.
2. **Competing companies using employees for economic advantage :** In some cases, rival companies may attempt to gain a competitive edge by recruiting or coercing employees to steal proprietary information.

PART-3

Classifications of Cyber Crimes.

Que 1.6. **What are the different categories or types of cyber crimes ?**

OR

What is the impact of cybercrimes on individuals, property, and government ?

Answer

Following are the different categories or types of cyber crimes :

A. Cybercrime against individuals (persons) :

1. **E-mail spoofing :** E-mail spoofing involves sending emails with a forged sender address to deceive recipients into believing the message is from a legitimate source.
2. **Online frauds :** Online frauds encompass a wide range of scams and deceptive practices conducted on the internet, targeting individuals to trick them into providing money or personal information.
3. **Phishing :** Phishing is a form of cyber crime where perpetrators impersonate trustworthy entities to obtain sensitive information, such as login credentials or credit card details, often through deceptive emails or websites.
4. **Spamming :** Spamming involves sending unsolicited and often irrelevant messages or advertisements to a large number of recipients, typically for commercial purposes.
5. **Cyberstalking and harassment :** Cyberstalking is the use of electronic communication to harass or stalk individuals online. It can include threats, intimidation, or unwanted advances through digital channels.

B. Cybercrime against assets (property) :

1. **Credit card frauds :** Credit card frauds involve the unauthorized use of someone's credit card information to make fraudulent purchases or withdraw funds.
2. **Intellectual property crimes :** These crimes involve the theft or illegal distribution of intellectual property, including copyrighted material, patents, and trade secrets.
3. **Internet time theft :** Internet time theft refers to unauthorized access or manipulation of internet services or resources, such as stealing internet connection bandwidth or using someone else's internet subscription without permission.

C. Cybercrime against organizations (government, business and social) :

1. **Unauthorized accessing of computers :** This involves gaining unauthorized access to computer systems or networks, either to steal sensitive data, disrupt operations, or engage in cyber espionage.

2. **Password sniffing :** Password sniffing is the process of intercepting and recording passwords as they are transmitted over a network.
3. **Denial-of-Service (DoS) attacks :** In DoS attacks, perpetrators overwhelm a target system or network with an excessive volume of traffic, rendering it unavailable to users.
4. **Virus attacks :** Virus attacks involve malicious software (viruses) that can infect computers and compromise their functionality.

D. Cybercrime against society :

1. **Forgery :** In the digital realm, forgery involves creating fake documents, digital signatures, or certificates to deceive others for fraudulent purposes.
2. **Cyberterrorism :** Cyberterrorism involves using cyber attacks to disrupt critical infrastructure, create fear, or advance political or ideological goals.
3. **Web jacking :** Web jacking involves unauthorized access to websites to change their content or display messages for malicious or political purposes.

Que 1.7. What is the impact of cyber crimes on individuals, property, and government ?

Answer

Following is a breakdown of the impact of cybercrimes on these three categories :

A. Individuals :

1. **Financial losses :** Individuals can suffer financial losses through various cyber crimes. Cybercriminals may steal money directly from bank accounts or make unauthorized purchases using stolen financial information.
2. **Privacy invasion :** Cybercrimes often involve the unauthorized access or theft of personal information, leading to a breach of privacy. This can result in emotional distress and psychological harm.
3. **Identity theft :** Victims of cybercrimes like identity theft may experience long-term consequences, including damage to their credit scores and difficulties in reclaiming their identities.
4. **Emotional distress :** Being a victim of cyber bullying, online harassment, or cyber stalking can cause significant emotional distress and mental health issues.

B. **Property :**

1. **Data breaches :** Cyber attacks can lead to data breaches, which can result in the theft or exposure of sensitive business or personal information.
2. **Ransomware :** Ransomware attacks can lock individuals or businesses out of their own systems or files until a ransom is paid. Failure to pay can result in the permanent loss of critical data.
3. **Disruption of services :** Cyber attacks on critical infrastructure, such as power grids or transportation systems, can disrupt essential services, leading to economic losses and public inconvenience.

C. **Government :**

1. **National security threats :** Cybercrimes pose a significant threat to national security. State-sponsored cyber attacks, espionage, or sabotage can target government agencies, military institutions, and critical infrastructure.
2. **Economic impact :** Governments can incur substantial economic losses due to cyber attacks on public institutions, as well as the cost of responding to and recovering from cyber incidents.
3. **Data breaches :** Government agencies often store vast amounts of sensitive citizen data. Data breaches can lead to the exposure of personal information, eroding public trust and potentially resulting in legal action.
4. **Intellectual property theft :** Cybercriminals can steal intellectual property from government research institutions, undermining innovation and economic competitiveness.

PART-4

A Global Perspective on Cyber Crimes.

Que 1.8. Write a short note on: global perspective on cyber crimes.

Answer

1. At an international level, cybercrime is defined broadly.
2. The Council of Europe's (CoE's) Cyber Crime Treaty employs the term "cybercrime" as a comprehensive label encompassing a range of criminal activities, including offenses against computer data and systems, computer-related crimes, content offenses, and copyright violations.
3. This expansive definition of cybercrime partially overlaps with general categories of offenses that do not necessarily rely on Information & Communication Technology (ICT), such as white-collar and economic crimes.

4. Significant efforts are required to enhance confidence and security in the use of ICTs and advance the international cooperation agenda.
5. This is because, in the 21st century, there is an increasing reliance on ICTs that span across the globe.
6. The rapid expansion of ICTs and their dependencies altered the perception of cybersecurity threats.
7. The connection between cybersecurity and safeguarding critical infrastructure has emerged as a major concern, with numerous countries assessing threats, vulnerabilities, and exploring methods to address them.
8. Within this context, several notable developments have occurred :
   i. On August 4, 2006, the US Senate ratified the CoE Convention on Cyber Crime, which targets hackers, individuals disseminating destructive computer viruses, those exploiting children or distributing racist material via the Internet, and terrorists attempting to attack infrastructure facilities or financial institutions.
   ii. On August 18, 2006, a news article titled "ISP's Cautious About 'Stringent Obligations' for Web Site Blocking" was published. European Union (EU) officials aimed to block suspicious websites as part of a 6-point plan to enhance joint antiterrorism efforts, particularly those inciting terrorist actions.
   iii. The CoE Cyber Crime Convention, spanning from 1997 to 2001, represented the inaugural international treaty addressing Internet-related crimes by harmonizing national laws, enhancing investigative techniques, and fostering cooperation among nations. To date, over 40 countries have ratified the Convention.

PART-5

Cyber Crime Era : Survival Mantra for the Netizens.

Que 1.9. Discuss the survival mantra for the netizens for online security.

Answer

1. The 5P netizen mantra is the survival mantra for online security.
2. The 5P netizen mantra for online security provides a comprehensive approach to staying safe in the digital world.
3. Each "P" in this mantra represents a key aspect of online security :

A. Precaution :

1. Precaution is the first and fundamental step in online security.
2. It involves being cautious and aware of potential risks and threats when using the internet.

3. Netizens should exercise caution when sharing personal information, clicking on links, or downloading files from unknown sources.
4. This means being skeptical of unsolicited emails or messages, and verifying the legitimacy of websites before providing sensitive information.

B. Prevention :

1. Prevention goes hand in hand with precaution.
2. It entails taking proactive measures to reduce the likelihood of falling victim to online threats.
3. This may include regularly updating software and antivirus programs, using strong and unique passwords, and educating oneself about common online scams and tactics used by cybercriminals.

C. Protection :

1. Protection involves implementing security measures to safeguard personal data and online accounts.
2. This includes using firewalls, encryption, and secure browsing practices.
3. Netizens should also be cautious about the information they share on social media and adjust privacy settings to limit exposure to potential threats.

D. Preservation :

1. Preservation emphasizes the importance of preserving digital assets and records securely.
2. Netizens should regularly back up their data to prevent loss in case of cyber attacks or hardware failures.
3. This includes important documents, photos, and other digital content.
4. Cloud storage and external hard drives can be used for data preservation.

E. Perseverance :

1. Perseverance represents the ongoing commitment to maintaining online security.
2. It's crucial to stay vigilant and adapt to evolving cyber threats.
3. Netizens should keep learning about new security risks and best practices for protection.
4. Regularly reviewing and updating security measures is essential to stay ahead of potential threats.

PART-6

Cyber Offenses : How Criminals Plan the Attacks.

Que 1.10. What do you understand by cyber offenses ? Also explain the terms hackers, crackers and phreakers.

Answer

A. Cyber offenses :

1. Cyber offenses, also known as cyber crimes, are criminal activities committed in the digital realm using computer networks, the internet, or other forms of technology.
2. These offenses involve various illegal activities that exploit vulnerabilities in computer systems, compromise data, or harm individuals or organizations.
3. Cyber offenses are a growing concern due to the increasing reliance on digital technology and the internet in modern society.
4. Law enforcement agencies, cybersecurity experts, and legal authorities work to combat cybercrimes and prosecute offenders to protect individuals, businesses, and governments from the various threats posed by cyber offenses.

B. Hackers : Hackers are individuals with advanced computer skills and knowledge who use their expertise to explore and manipulate computer systems, software, and networks.

C. Crackers : Crackers are individuals who engage in malicious or illegal activities, primarily focused on circumventing software protections (e.g., cracking software licenses or encryption) to gain unauthorized access or manipulate software for personal gain.

D. Phreakers : Phreakers, short for "phone phreaks," are individuals who manipulate or explore the telecommunication systems, often with a focus on gaining free access to phone services or exploring the inner workings of the telephone network.

Que 1.11. Explain how cybercriminals plan the attacks ?

Answer

1. Cybercriminals employ a variety of techniques to identify weaknesses in the security of their target.
2. These methods can include scanning for open ports, searching for unpatched software or outdated operating systems, and exploiting known vulnerabilities.

3. They may also use social engineering to manipulate individuals into revealing sensitive information or credentials.
4. Following phases are involved in planning cyber crime :

A. Reconnaissance (Information gathering) :

1. This initial phase focuses on gathering information about the target.
2. Criminals seek to understand the target's systems, network topology, security measures, and potential vulnerabilities.
3. Reconnaissance activities can include scanning public records, studying social media profiles, and conducting network analysis.
4. Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases :

a. Passive attacks : In passive attacks, criminals gather information without directly interacting with the target's systems. They aim to remain unnoticed while collecting data that may be useful in subsequent attacks. Passive attacks can include activities like monitoring network traffic or profiling potential victims.

b. Active attacks : Active attacks involve direct interaction with the target's systems. Criminals actively exploit vulnerabilities or attempt to gain unauthorized access. These attacks can range from phishing attempts and malware deployment to exploiting software vulnerabilities.

B. Scanning and scrutinizing :

1. Once information is gathered, cybercriminals analyze it to identify valid data and potential vulnerabilities.
2. They may use automated tools to scan for open ports, services, and known weaknesses in the target's systems.
3. The goal is to determine how best to exploit the identified vulnerabilities.

C. Launching an attack (Gaining and maintaining system access) :

1. In this phase, cybercriminals actively initiate their attacks, often by exploiting the vulnerabilities identified in the previous phases.
2. Once they gain access, they work to maintain that access for continued exploitation, data theft, or further attacks.

PART-7

Social Engineering.

Que 1.12. Explain the term "social engineering" in context of cyber security.

Answer

1. "Social engineering" refers to a set of manipulative techniques that cybercriminals use to exploit human psychology and deceive individuals into divulging confidential information.
2. Social engineers exploit a person's natural tendency to trust their word rather than exploiting vulnerabilities in computer security.
3. It is generally agreed that individuals represent the weak link in security, enabling the feasibility of social engineering.
4. Typically, a social engineer employs telecommunications or the internet to convince individuals to violate an organization's security practices or policies.
5. Social engineering revolves around establishing inappropriate trust relationships with insiders to gain access to sensitive information.
6. The objective of a social engineer is to deceive individuals into disclosing valuable information or granting access to it.
7. Social engineers study human behavior to leverage people's willingness to assist, their inclination to trust others, and their fear of facing consequences.
8. The hallmark of highly successful social engineers is their ability to obtain information without raising any suspicions.

Que 1.13. Give classification of social engineering.

Answer

Social engineering is classified as follow :

A. Human-based social engineering : Human-based social engineering refers to person-to-person interaction to get the required/desired information. Following are some of the ways of getting desired information :

1. **Impersonating an employee or valid user :** A social engineer may pretend to be an employee or a legitimate user of a system, gaining trust and access to sensitive information.
2. **Posing as an important user :** The attacker might impersonate a high-ranking official or supervisor to pressure others into complying with their requests.
3. **Using a third person :** A social engineer may enlist the help of a third person, convincing them to vouch for their credibility or act as a reference to gain trust.
4. **Calling technical support :** Pretending to be a user with technical issues, the attacker contacts technical support to gather information or gain unauthorized access.

5. **Shoulder surfing :** Observing someone's computer screen or keypad from a close distance to obtain sensitive data like login credentials.
6. **Dumpster diving :** Physically searching through discarded documents, such as company trash bins, to find confidential information.

B. Computer-based social engineering : Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/internet. Following are some of the ways of getting desired information :

1. **Fake e-mails :** Sending deceptive e-mails that appear to be from a trusted source, often urging recipients to click on links or provide personal information.
2. **E-mail attachments :** Enclosing malicious attachments in e-mails, which, when opened, can infect the recipient's computer with malware.
3. **Pop-up windows :** Generating fake pop-up windows on websites that mimic legitimate login screens or system alerts, tricking users into entering confidential data.

PART-8

Cyber Stalking.

Que 1.14. What do you understand by cyber stalking ? Also give its key characteristics.

Answer

1. Cyber stalking refers to the act of using digital communication tools and online platforms to harass, intimidate, or threaten an individual or group of individuals repeatedly and persistently.
2. It involves unwanted and often obsessive attention, monitoring, or pursuit of a person through electronic means.
3. Cyber stalkers may employ various online methods to carry out their activities, including e-mail, social media, instant messaging, or other forms of online communication.
4. Cyber stalking can have severe consequences, leading to emotional distress, anxiety, depression, and, in some cases, physical harm.
5. It is considered a criminal offense in many jurisdictions, and laws have been enacted to address and punish cyber stalkers.
6. Victims of cyber stalking are encouraged to report incidents to law enforcement agencies and take steps to protect their online privacy and security.

Key characteristics : Key characteristics of cyber stalking include :

1. **Repetitive behavior :** Cyber stalkers engage in repeated and often intrusive actions against their target, causing distress and fear.
2. **Unwanted contact :** They make unsolicited contact with their victims, such as sending threatening e-mails, messages, or posting harmful content about them online.
3. **Anonymity :** Cyber stalkers may hide their true identity or use fake profiles to carry out their activities, making it challenging for victims to identify them.
4. **Monitoring :** They may monitor their victims' online activities, personal information, or location, often with the intent of gathering information to further harass or threaten them.
5. **Threats and harassment :** Cyber stalkers may send explicit threats, engage in hate speech, or engage in character assassination with the aim of causing emotional or psychological harm.
6. **Manipulation :** They may use psychological manipulation tactics to control or manipulate their victims, creating a sense of power and control.

Que 1.15. Mention the types of cyber stalkers.

Answer

There are primarily two types of cyber stalkers :

A. **Online stalkers :** Online stalkers are individuals who engage in cyberstalking primarily through digital means and within the virtual realm. They use the internet and various online platforms to harass, intimidate, or threaten their victims. Following are some key characteristics and behaviors associated with online stalkers :

1. **Digital communication :** Online stalkers use electronic communication channels to carry out their activities. This may include sending threatening emails, text messages, or making harmful comments on social media platforms.
2. **Anonymity :** Many online stalkers take advantage of the relative anonymity provided by the internet. They may use pseudonyms or fake profiles to conceal their true identities, making it difficult for victims to identify them.
3. **Monitoring :** Online stalkers often closely monitor their victims' online activities. They may track social media posts, comments, and interactions, as well as gather personal information from public profiles.
4. **Harassment :** These individuals engage in repetitive and unwanted contact with their victims. They may post defamatory content, share private information, or engage in hate speech directed at their targets.

5. **Cyber bullying :** Online stalkers may also engage in cyber bullying, especially when their victims are younger individuals, such as teenagers.
6. **Obsession :** Online stalkers may become obsessed with their victims, often fixating on them and engaging in persistent online harassment over an extended period.

B. **Offline stalkers :** Offline stalkers, on the other hand, are individuals who initially establish their obsession or harassment in the physical world but may use online tools or information to further their stalking activities. Following are some characteristics and behaviors associated with offline stalkers :

1. **Physical presence :** Offline stalkers may physically follow, surveil, or confront their victims in real life. They might appear at their homes, workplaces, or other locations.
2. **Gathering information :** While offline stalkers may start their activities in the physical world, they may also use online resources to gather more information about their victims. This can include researching personal details, social media profiles, or online posts.
3. **Intimidation :** Offline stalkers often use tactics like sending threatening letters or making harassing phone calls to instill fear in their victims.
4. **Trespassing :** In extreme cases, offline stalkers may trespass on their victims property, leaving behind evidence of their presence.
5. **Escalation :** Offline stalking can escalate to dangerous levels, including physical harm or violence against the victim.

PART-9

Cybercafe and Cyber Crimes.

Que 1.16. What do you mean by cybercafe ? How cybercafes are associated with cyber crimes in India ?

Answer

1. A cybercafe is a physical establishment or business where customers can access computers, the internet, and various online services for a fee.
2. These cafes typically provide public access to computers and the internet to individuals for a specified period.
3. Cybercafes have played a significant role in India's digital revolution, providing access to the internet and online services for millions of people.
4. Here's a brief overview of role of cybercafes :

i. **Digital inclusion :** Cybercafes have played a crucial role in bridging the digital divide, allowing individuals, especially those without personal internet access, to connect online, search for information, and complete various tasks.

ii. **Youth and education :** Many students rely on cybercafes for research, online exams, and educational resources. They have become essential for students who lack personal computers or internet connectivity at home.

iii. **Business and communication :** People use cybercafes for online job applications, communication, and even running small businesses, making them vital for economic activities.

Association of cybercafes with cyber crimes in India :

1. **Terrorist communication :** Cybercafes have been linked to instances of terrorist communication and recruitment, prompting concerns about national security.
2. **Cyberfraud :** Cybercrimes such as phishing, identity theft, and online financial fraud have occurred through cybercafes, often targeting unsuspecting users.
3. **Obscene content :** Cybercafes have been used to access and distribute obscene or illegal content, leading to harassment and distress for victims.
4. **Malware distribution :** Some cybercafes have unknowingly become hubs for malware distribution due to the use of pirated software and lack of proper security measures.
5. **Lack of IT governance :** Many cybercafes in India lack awareness about IT security and governance. They often use outdated software, fail to block inappropriate websites, and may not cooperate with authorities during cyber crime investigations.

Que 1.17. What is Indian government response to combat cybercrimes using cybercafes ?

Answer

1. Indian authorities have taken steps to regulate cybercafes and combat cybercrimes.
2. They have issued guidelines for cybercafes, emphasizing the need for proper record-keeping, user identification, and IT security measures.
3. The government has established cybercrime cells and cyber forensic laboratories to investigate and prosecute cybercrimes effectively.
4. There is an ongoing effort to raise awareness about cybersecurity among cybercafe owners and the general public to mitigate cyber threats.

Que 1.18. **What are the measure an individual should take while using the computer in a cybercafe ?**

Answer

Following are a few tips for safety and security while using the computer in a cybercafe :

1. **Always logout :** Ensure that you log out of all your accounts and applications before leaving the computer.
2. **Stay with the computer :** While using a cybercafe computer, avoid leaving it unattended, even for a short time. Others may tamper with your session or gain unauthorized access to your accounts if you're not present.
3. **Clear history and temporary files :** After your session, clear your browsing history, cookies, and temporary files. This helps protect your privacy by removing traces of your online activities from the computer.
4. **Be alert :** Be aware of your surroundings and the people near you.
5. **Avoid online financial transactions :** It's generally advisable to avoid conducting sensitive financial transactions on public computers. Public computers may not have adequate security measures, and your financial information could be at risk.
6. **Change passwords :** If you've used a cybercafe computer to access sensitive accounts, consider changing your passwords afterward.
7. **Use virtual keyboard :** If you need to enter sensitive information like passwords, consider using the virtual keyboard provided by the operating system.
8. **Security warnings :** Pay attention to security warnings from your browser or operating system.

PART-10

Botnets : The Fuel for Cybercrime.

Que 1.19. **Write a short note on: Botnets.**

OR

What are Botnets ? Why are they considered "The Fuel for Cybercrime" ?

Answer

Botnets :

1. Botnets are networks of compromised computers (bots) that are remotely controlled by a cybercriminal or a group of cybercriminals known as "bot herders" or "botmasters."

2. These compromised computers are typically infected with malicious software or malware, allowing the attacker to gain control over them.
3. Once under the attacker's command, these infected computers can be used for various malicious activities, making botnets a significant threat.

Fuel for Cybercrime : Here's why botnets are considered "The Fuel for Cybercrime":

1. **Massive computing power :** Botnets consist of a large number of compromised computers, sometimes numbering in the thousands. This massive computing power can be harnessed by cybercriminals.
2. **Anonymity :** Bot herders can operate botnets remotely. This anonymity makes it challenging for law enforcement agencies to track down the perpetrators.
3. **Distributed attacks :** Botnets enable cybercriminals to launch distributed attacks.
4. **Spreading malware :** Botnets can be used to propagate and distribute malware.
5. **Data theft and espionage :** Botnets can be used to steal sensitive information. Compromised computers can be used to exfiltrate data, spy on users, or log keystrokes.
6. **Ad fraud :** Botnets are used in click fraud schemes, where automated bots click on online ads to generate revenue for cybercriminals.
7. **Cryptocurrency mining :** Cybercriminals can use botnets to mine cryptocurrencies by harnessing the computational power of the infected computers.

Que 1.20. What measures should an individual take to secure his system from botnets ?

Answer

Following measures should be taken to secure the system from botnets :

1. Use antivirus and anti-spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer.
5. Downloading the freeware only from websites that are known and trustworthy.
6. Check regularly the folders in the mail box - "sent items" or "outgoing" - for those messages you did not send.
7. Take an immediate action if your system is infected.

PART-11

Attack Vector.

Que 1.21. What do you mean by "attack vector" ? How are attack vectors launched ?

Answer

1. An attack vector is a path or a means by which a cyber attack can be carried out against a computer system, network, or organization.
2. It represents the specific method or avenue that a malicious actor or hacker can use to exploit vulnerabilities and compromise the security of a target.
3. Attack vectors can vary widely and may include various techniques, tactics, or strategies employed by attackers to achieve their objectives.
4. Understanding attack vectors is crucial for cybersecurity professionals and organizations to anticipate and prevent potential threats.
5. Effective cybersecurity measures often involve addressing known attack vectors, applying patches and updates, implementing security controls, and educating users.

Launching attack vectors : The attack vectors are launched by following means :

1. **Attack by e-mail :** Cybercriminals send deceptive emails that appear legitimate, often with enticing subject lines or claims, to trick recipients into taking malicious actions, such as clicking on links or downloading attachments.
2. **Attachments (and other files) :** Attackers often send malicious attachments, such as infected documents or executables, via email or other communication channels.
3. **Attack by deception :** Deception-based attacks involve tricking individuals or organizations into taking actions that compromise security. This can include social engineering techniques like impersonation, pretexting, or baiting.
4. **Hackers :** Hackers with advanced technical skills can exploit software vulnerabilities, use brute force methods, or employ other techniques to gain unauthorized access to systems.
5. **Attack of the worms :** Worms are self-replicating malware that spread independently across networks or systems. They exploit vulnerabilities to infect computers and propagate to other devices.

6. **Malicious macros :** Malicious macros are scripts embedded within documents, such as Microsoft Word or Excel files. When enabled, these macros can execute malicious code, leading to malware infection or data theft.

7. **Viruses :** Viruses are malicious software programs that attach themselves to legitimate files or applications. When the infected file is executed, the virus replicates and spreads to other files.

☺☺☺

2 UNIT

Cyber Crime

CONTENTS

PART-1

Mobile and Wireless Devices Introduction.

Que 2.1. Explain the rising importance of mobile and wireless devices.

Answer

1. In the modern era, electronic gadgets, specifically mobile hand-held devices, have become crucial for businesses, providing internet connectivity beyond the office environment.
2. The widespread adoption of laptops, personal digital assistants (PDAs), and mobile phones has evolved from limited user groups to extensive use.
3. According to GSMA real-time intelligence data, there are now over 11.856 billion mobile connections worldwide in 2023, and a growing portion of these devices were internet-enabled.
4. Managing these devices outside the office poses complex challenges that information technology (IT) departments within organizations must tackle.
5. Remote connections have evolved from fixed location dial-in to wireless-on-the-move, and PDAs have become networked, converging with mobile phones.
6. The development of PDAs and advancements in cellular phone technology has given rise to a new category of mobile devices known as Smartphones, which integrate mobile and wireless technologies for business purposes.
7. Now-a-days many employees bring their personal Smartphones to the office, adding to the diversity of mobile users and devices.
8. This expanded user base and device variety place increased demands on IT departments to ensure device, data, and network security while maintaining control over corporate assets and supporting mobile user productivity.
9. These technological advancements introduce a fresh set of security challenges for global organizations.

PART-2

Proliferation of Mobile and Wireless Devices.

Que 2.2. **Write a short note on: proliferation of mobile and wireless devices.**

Answer

1. Presently, remarkable advancements are occurring in the realm of mobile devices.
2. The prevailing trend involves reducing device size while increasing processing capabilities.
3. Just a few years ago, consumers had to decide between a wireless phone and a basic PDA.
4. However, today's consumers have a lot of options for compact Smartphones with wireless internet browsing capabilities.
5. Simple handheld mobile devices offer sufficient computing power to run small applications, play games and music, and facilitate voice calls.
6. The term "mobile device" encompasses a wide range of products and technologies.
7. Mobile computing can be defined as the practice of taking a computer, along with all the necessary files and software, into various field-based environments.
8. Many types of mobile computers have been introduced since 1990s. They are as follows :
   - i. **Portable Computer :** Portable computers are essentially laptops or notebook computers that are designed to be carried around easily. They typically feature a foldable design with a built-in keyboard and display.
   - ii. **Tablet PC :** Tablet PCs are a class of mobile devices that typically consist of a touchscreen interface. They often come with a stylus or digital pen for input, allowing users to write or draw directly on the screen.
   - iii. **Internet Tablet :** Internet tablets are compact, portable devices primarily focused on internet browsing and media consumption. They typically feature larger screens than smartphones but lack the full functionality of traditional laptops.
   - iv. **Personal Digital Assistant (PDA) :** PDAs were designed for personal organization and included features like calendars, address books, and note-taking apps. PDAs paved the way for modern smartphones by introducing the concept of a pocket-sized personal organizer.
   - v. **Ultramobile PC (UMPC) :** UMPCs are a class of small, lightweight computers designed for portability and versatility. They often have a compact form factor, with screens ranging from 5 to 7 inches. UMPCs are suitable for light computing tasks and are known for their mobility.

vi. **Smartphone :** Smartphones are handheld devices that combine the functions of a mobile phone with those of a computer. They typically feature touchscreens, powerful processors, and access to a wide range of mobile apps.

Que 2.3. Give distinction among the key terms: mobile computing, wireless computing and hand-held devices.

Answer

S. No.	Term	Description	Key Characteristics
1.	Mobile Computing	Using computers or devices on the go, often involving wireless connectivity for remote access.	Mobile settings, Wireless connectivity
2.	Wireless Computing	Utilizing wireless communication for data transmission across various computing contexts.	Wireless data transmission - Mobile and non-mobile scenarios
3.	Hand-Held Devices	Compact, portable devices designed for one-handed operation, serving specific functions.	One-handed operation - Task-specific design

PART-3

Trends in Mobility.

Que 2.4. Discuss the present trends in mobility. What are mobility types and its implications ?

Answer

Present trends in mobility :

1. Mobile computing is entering a new phase offering enhanced usability, faster networking, and a wider range of applications.
2. Prominent examples of this trend include Apple's "iPhone" and the Google-driven "Android" phones, with numerous other advancements reinforcing this direction.
3. The growing popularity of this intelligent mobile technology has also attracted the attention of attackers, including hackers and crackers.
4. It is essential to pay attention to the evolving trends in mobile computing to appreciate the significance of cybersecurity concerns within this domain.

Mobility types and its implications :

1. **User mobility :** User mobility refers to the ability of individuals to move physically while maintaining network connectivity and access to services. It involves users accessing network resources from different locations or devices.

   Implications :

   i. **Flexibility :** User mobility allows individuals to work or access services from various locations, which can increase flexibility and productivity.

   ii. **Challenges :** Managing security and authentication becomes crucial to ensure that users are granted access only from authorized locations or devices.

   iii. **Data synchronization :** Ensuring that users have access to the same data and services regardless of their location or device requires efficient data synchronization methods.

2. **Device mobility :** Device mobility refers to the ability of devices (e.g., smartphones, laptops, tablets) to move between different access points or networks while maintaining uninterrupted connectivity.

   Implications :

   i. **Seamless connectivity :** Device mobility ensures that users experience continuous network connectivity, even when moving between Wi-Fi networks, cellular networks, or other access points.

   ii. **Handoff mechanisms :** Implementing efficient handoff mechanisms is essential to ensure a smooth transition between different access points.

   iii. **Quality of Service (QoS) :** Maintaining QoS is a challenge, as devices may switch between networks with varying bandwidth and reliability.

3. **Session mobility :** Session mobility refers to the capability to transfer an ongoing network session from one device or network to another without interruption.

   Implications :

   i. **Seamless handover :** Users can switch devices or networks without losing their active sessions, which is essential for applications like video conferencing.

   ii. **Protocol support :** Implementing protocols like Mobile IP or SIP (Session Initiation Protocol) is necessary to support session mobility.

   iii. **Resource management :** Managing resources, such as IP addresses or server connections, during session handovers is crucial for maintaining the user experience.

4. **Service mobility :** Service mobility involves the ability to access the same services or applications from different devices or locations.

Implications :

i. **Cross-platform compatibility :** Services must be designed to work seamlessly across various devices and platforms to accommodate service mobility.

ii. **Data accessibility :** Ensuring that users have access to their data and services regardless of the device they use is a key consideration.

iii. **Cloud-based solutions :** Many services leverage cloud computing to provide consistent access and functionality across different devices and locations.

Que 2.5. **Describe the popular types of attacks against 3G mobile networks.**

Answer

Popular types of attacks against 3G mobile networks are as follows :

1. **Malwares, viruses and worms :** Malware, viruses, and worms are malicious software programs that can infect mobile devices within a 3G network. They are typically designed to compromise device security, steal sensitive data, or disrupt network operations.
2. **Denial-of-Service (DoS) :** Denial-of-Service attacks aim to overwhelm 3G network resources, rendering them unavailable to legitimate users. Attackers flood the network with traffic or exploit vulnerabilities to disrupt services.
3. **Overbilling attack :** Overbilling attacks involve manipulating 3G network protocols or exploiting vulnerabilities to generate fraudulent billing for data or services, leading to financial losses for users.
4. **Spoofed Policy Development Process (PDP) :** In a spoofed PDP attack, malicious entities impersonate a legitimate device to establish a policy context in a 3G network. This allows unauthorized access to network resources.
5. **Signaling-level attacks :** Signaling-level attacks target the communication protocols used in 3G networks to establish and manage connections. Attackers manipulate these protocols to disrupt services or intercept communication.

PART-4

Credit Card Frauds in Mobile and Wireless Computing Era.

Que 2.6. **What do you mean by credit card frauds in context of mobile and wireless computing ?**

Answer

1. In the context of mobile and wireless computing, credit card fraud refers to fraudulent activities that involve the unauthorized use of credit card information in mobile or wireless transactions.
2. These frauds exploit vulnerabilities or weaknesses in the mobile and wireless technologies and systems used for processing credit card transactions.
3. Mobile and wireless computing have introduced new conveniences and capabilities for consumers, but they have also created new opportunities for credit card fraud.
4. As a result, mobile and wireless security measures, such as encryption, secure authentication methods, and fraud detection algorithms, are essential to protect both consumers and businesses from these types of fraudulent activities.
5. Additionally, individuals should remain vigilant about the security of their mobile devices and credit card information when engaging in mobile and wireless transactions.

Que 2.7. Discuss credit card frauds in mobile and wireless computing era. Give some tips to prevent credit card frauds.

Answer

Credit card frauds in mobile and wireless computing era :

1. Emerging trends in cybercrime related to mobile computing include mobile commerce (M-Commerce) and mobile banking (M-Banking).
2. The prevalence of credit card fraud is on the rise due to the increasing power and decreasing prices of mobile hand-held devices, making these gadgets readily available to almost anyone.
3. Mobile credit card transactions have become commonplace, with new technologies merging affordable mobile phone capabilities and point-of-sale (POS) terminal functionalities.
4. The contemporary era is characterized by "mobile computing," emphasizing the ability to compute anywhere and anytime.
5. Credit card companies typically assist consumers in resolving identity (ID) theft issues after they occur, but they could further reduce ID fraud by providing consumers with enhanced tools to monitor their accounts and restrict high-risk transactions.

Tips to prevent credit card frauds :

A. Do's :

1. Sign your card as soon as you receive it.

2. Make photocopies of both sides of your card and store them securely to retain the card number and expiration date in case of card loss.
3. Change the default Personal Identification Number (PIN) received from the bank before initiating any transactions.
4. Maintain vigilance over your card during transactions and ensure its immediate return.
5. Safeguard all receipts for later comparison with your credit card statement.
6. Verify the authenticity of a website before providing your card details.
7. Notify your bank promptly in the event of card loss and report it to the police if necessary.

B. Don'ts :

1. Avoid storing your card number and PINs in your cellphone.
2. Refrain from lending your cards to anyone.
3. Never leave cards or transaction receipts lying unattended.
4. Do not sign a blank receipt; if the transaction details are unclear, request another receipt to verify the amount.
5. Avoid writing your card number or PIN on a postcard or the outside of an envelope.
6. Do not disclose your account number over the phone immediately, unless you are calling a trusted company or your bank.
7. Do not dispose of credit card receipts by simply discarding them into a garbage box or dustbin.

Que 2.8. What are different types and techniques of credit card frauds ?

Answer

Following are different types and techniques of credit card frauds :

1. Traditional Techniques :

i. **ID theft :** Identity theft involves fraudsters stealing personal information, such as a person's name, address, and credit card details, to impersonate the victim and make unauthorized transactions.

ii. **Financial fraud :** Financial fraud includes a range of fraudulent activities where criminals use stolen credit card information to make unauthorized purchases, cash advances, or transfers of funds. It can involve card-present or card-not-present transactions.

2. **Modern Techniques :**
   i. **Triangulation :** Triangulation fraud involves fraudsters creating a complex network of online transactions. They use a stolen credit card to purchase goods from one online store, have those goods shipped to another address, and then resell them through a third-party marketplace.
   ii. **Credit card generators :** Credit card generators are software programs or tools that create fake credit card numbers that may pass initial validation checks. Criminals use these fake numbers to attempt unauthorized transactions.

PART-5

Security Challenges Posed by Mobile Devices.

Que 2.9. What are the security challenges posed by mobile devices to cybersecurity ?

Answer

Mobility brings two main challenges to cybersecurity :

1. **On the hand-held devices, information is being taken outside the physically controlled environment :** This challenge refers to the fact that mobile and hand-held devices, such as smartphones, tablets, and laptops, are inherently portable. Users carry them outside the physically controlled and secure environments typically found in office or home settings.
2. **Remote access back to the protected environment is being granted :** This challenge relates to the need to provide remote access to corporate networks or protected environments from mobile devices. Users require this access to work and access resources while not physically present in the controlled network environment.

Que 2.10. What are the technical challenges associated with mobile security ?

Answer

Some well-known technical challenges in mobile security are :

1. **Managing the registry settings and configurations :** Mobile devices often rely on configuration settings stored in the registry. Managing these settings securely is a challenge, as unauthorized access to or tampering with registry entries can compromise device security.

2. **Managing the authentication service security :** Ensuring secure authentication services on mobile devices is crucial. Authentication mechanisms, such as biometrics, PINs, and passwords, must be protected to prevent unauthorized access to the device and associated services.
3. **Cryptography security :** Cryptography is essential for securing data on mobile devices, particularly during data transmission and storage.
4. **Lightweight Directory Access Protocol (LDAP) security :** LDAP is often used for directory services in mobile applications. Ensuring the security of LDAP directories is vital to protect user identities and access control.
5. **Remote Access Server (RAS) security :** RAS systems enable remote access to corporate networks. Securing RAS is crucial to prevent unauthorized access, data breaches, and attacks.
6. **Media player control security :** Mobile devices often include media players that can access streaming content or local media files. Securing media player controls is essential to prevent vulnerabilities that could be exploited for malicious purposes.
7. **Networking application program interface (API) security :** Mobile applications rely on networking APIs to communicate with servers and services. Securing these APIs is essential to prevent data leaks, unauthorized access, and API abuse.

PART-6

Registry Settings for Mobile Devices.

Que 2.11. Write a short note on: registry settings for Windows mobile-powered devices.

Answer

Registry settings on mobile devices can be understood through following example :

1. Microsoft ActiveSync is designed for syncing with Windows-powered personal computers (PCs) and Microsoft Outlook.
2. ActiveSync serves as the intermediary between Windows-powered PCs and Windows mobile-powered devices, facilitating the transfer of applications like Outlook data, Microsoft Office documents, photos, music, videos, and apps from a user's desktop to their device.
3. In addition to PC synchronization, ActiveSync can directly sync with the Microsoft Exchange server, allowing users to wirelessly update their emails, calendars, notes, and contacts when they are away from their PCs.

4. Given the ease with which various applications allow the free flow of information, registry settings become crucial in this context for establishing trusted groups, especially within "group policy," a core function performed by Windows Active Directory.
5. Mobile device security also involves dealing with new mobile applications that continuously emerge to combat threats like spyware, viruses, worms, malware, and other malicious codes traversing networks and the internet.
6. In Windows platforms, one issue with mobile security is that the baseline security settings may not be configured correctly when a computer or mobile device is first used or installed.
7. Achieving a high level of security on a Windows computer often requires making additional registry changes that are not exposed through any user interface.
8. While there are various methods to implement these registry changes on each computer, some approaches are more efficient than others for achieving the desired baseline security.

PART-7

Authentication Service Security.

Que 2.12. What do you understand by authentication services security ? Discuss the types of attacks to which mobile devices are subjected to.

Answer

Authentication services security :

1. Authentication services security refers to the measures and practices put in place to ensure that users and devices attempting to access a network, application, or service are legitimate and authorized.
2. It is a fundamental aspect of mobile and wireless security aimed at verifying the identity of users and devices to prevent unauthorized access and protect sensitive information.
3. Authentication services security is crucial for safeguarding sensitive data, protecting networks, and ensuring that only authorized users and trusted devices can access resources and services.
4. It is an essential component of a robust mobile and wireless security strategy.

Types of attacks : Mobile devices are subject to following types of attacks :

1. **Push attacks :** Push attacks are malicious actions initiated by external entities or applications to exploit vulnerabilities in a mobile device. These attacks often involve the unauthorized installation of malware, malicious apps, or files onto the device without the user's consent or knowledge.
2. **Pull attacks :** Pull attacks involve the mobile device actively seeking and downloading malicious content or software from untrusted sources, often without the user's awareness. These attacks occur when a user unknowingly initiates actions that lead to the compromise of their device.
3. **Crash attacks :** Crash attacks aim to destabilize a mobile device by exploiting software vulnerabilities. Attackers deliberately send malformed or malicious data to the device, causing applications, services, or even the entire operating system to crash.

Que 2.13. Discuss cryptographic security for mobile devices.

Answer

1. To secure a mobile device we use a technique known as cryptographically generated addresses (CGA).
2. CGA generates addresses with up to 64 bits by hashing the owner's public-key address.
3. The owner employs the corresponding private key to assert address ownership and sign messages sent from the address, all without the need for a public-key infrastructure (PKI) or other security infrastructure.
4. Implementing a PKI offers numerous advantages for users seeking to secure their financial transactions originating from mobile devices.
5. CGA-based authentication can serve as a protective measure for IP-layer signaling protocols, including neighbor discovery and mobility protocols.
6. Additionally, it can be utilized for key exchange within opportunistic Internet Protocol Security (IPSec).
7. Smartphones stand out as one of the most prevalent hand-held devices in mobile computing.
8. These devices are equipped with cryptographic security controls to bolster their security.

Que 2.14. Explain RAS Security for Mobile Devices :

Answer

1. Safeguarding business-sensitive data stored on employees' mobile devices underscores the importance of Remote Access Servers (RAS).
2. From a cyber security perspective, mobile devices are highly susceptible.
3. Mobile devices not only have their vulnerabilities to unauthorized access but also serve as potential entry points to connected systems.

4. By using a mobile device to impersonate a registered user, a potential attacker gains the ability to steal data or compromise corporate systems in various ways.
5. Another security concern arises from the practice of conducting port scans.
6. Protection against port scanning necessitates software capable of intercepting unauthorized incoming data packets and preventing a mobile device from disclosing its presence and identity.
7. When connecting through a direct Internet or RAS connection, a personal firewall on a Smartphone device can serve as an effective protective barrier against this type of attack for users.

PART-8

Attacks on Mobile / Cell Phones.

Que 2.15. Describe the various types of attacks against mobile/ cell phones.

Answer

Following the various types of attacks against mobile/cell phones :

1. **Mobile phone theft :** Mobile phone theft occurs when a mobile device is physically stolen by a perpetrator. The theft can happen through snatching, pickpocketing, or burglary. The thief gains unauthorized access to the victim's personal data, contacts, messages, photos, and potentially sensitive information. Stolen phones are often resold or used for fraudulent activities.
2. **Mobile viruses :** Mobile viruses are malicious software programs specifically designed to infect and disrupt the operation of mobile devices. These viruses can spread through infected apps, downloads, or malicious links. Mobile viruses can compromise device security, steal personal information, send unauthorized messages, or render the device unusable.
3. **Mishing :** Mishing (Mobile Phishing) is a cyber attack where attackers use text messages (SMS) to trick users into divulging sensitive information, such as login credentials, account numbers, or personal details. Mishing attacks can lead to identity theft, unauthorized access to accounts, and financial fraud.
4. **Vishing :** Vishing (Voice Phishing) involves attackers using phone calls to impersonate legitimate entities, such as banks or government agencies, to manipulate victims into revealing confidential information or performing certain actions. Victims of vishing can experience financial losses, identity theft, or unauthorized access to their accounts.

5. **Smishing :** Smishing (SMS Phishing) is a form of phishing where attackers send deceptive SMS messages containing malicious links or prompts to trick users into revealing personal information or installing malware. Smishing can lead to malware infections, identity theft, or unauthorized access to sensitive accounts.

6. **Hacking Bluetooth :** Hacking Bluetooth involves unauthorized access to a device's Bluetooth connection. Attackers can exploit vulnerabilities to gain control of the device, eavesdrop on communications, or transmit malicious content. Bluetooth hacking can lead to data breaches, unauthorized access to paired devices, or the distribution of malware.

PART-9

Mobile Devices : Security Implications for organizations.

Que 2.16. What are the various security implications for organizations related to mobile devices ?

Answer

Following are various security implications for organizations related to mobile devices :

A. Managing diversity and proliferation of hand-held devices :

1. For most organizations, cyber security remains a primary concern.
2. Many organizations overlook the long-term importance of maintaining records of mobile device ownership.
3. Regardless of whether employees receive devices from the organization, their mobile devices should be registered in the corporate asset register.
4. Furthermore, diligent monitoring of these devices is necessary in terms of their usage.
5. Upon an employee's departure, it is crucial to revoke both logical and physical access to organizational networks.
6. Consequently, company-owned mobile devices should be surrendered to the IT department and, at a minimum, deactivated and thoroughly cleansed.

B. Unconventional/Stealth storage devices :

1. Secondary storage devices, like USB drives, used by employees pose a potential cyber security risk.
2. Advancing technology leads to the continual reduction in the size and diversification of these devices.
3. Modern storage devices are challenging to detect, presenting a significant security concern for organizations.

4. Their compact dimensions enable inconspicuous concealment within bags or on one's person.
5. Advisable measures include prohibiting employee usage of these devices, as they can introduce viruses, worms, and Trojans into the organizational network, potentially causing data loss.

C. Threats through lost and stolen devices :

1. This presents a newly emerging cyber security concern.
2. Mobile handheld devices are frequently misplaced during people's travels.
3. Misplaced mobile devices pose an even greater security threat to corporations.
4. The cyber security threat in this scenario is concerning due to the generally inadequate security on mobile devices.
5. The value of the handheld device itself is often insignificant compared to the critical content it holds; its loss or theft can jeopardize a company's professional integrity, subjecting it to sabotage, exploitation, or damage.
6. Many of these lost devices have wireless access to corporate networks and minimal security, making them a vulnerable point and a significant challenge for security administrators.

PART-10

Organizational Measures for Handling Mobile.

Que 2.17. Discuss what organizations can do toward safeguarding their information systems in the mobile computing paradigm.

Answer

Organizations can do following to safeguard their information systems :

A. Encrypting organizational databases :

1. Hand-held devices now offer access to critical and sensitive data stored in databases, thanks to technological advancements.
2. Protecting the organization's data from loss necessitates encrypting such databases.
3. Typically, two algorithms are employed to implement strong encryption of database files :
   i. The Rijndael algorithm
   ii. The Multi-Dimensional Space Rotation (MDSR) algorithm

4. In this context, "strong encryption" implies greater resistance to decryption attempts that can impact performance significantly.
5. Employing either AES or MDSR algorithms for database file encryption renders the database unusable without the key (password).
6. When implementing strong encryption, it's crucial not to store the key on mobile devices.
7. The key is case-sensitive and must be accurately entered to access the database.
8. For enhanced security, there's an option to prompt the user to enter the encryption key via a dialog box displayed by the database server.
9. To safeguard against information theft through mobile devices connecting to corporate databases, additional security measures can be implemented, including a server-controlled self-destruct policy.

B. Including mobile devices in security strategy :

1. The responsibility for addressing cyber security threats stemming from improper access to organizational data by mobile-device-using employees falls squarely on the shoulders of IT departments.
2. Encrypting corporate databases doesn't mark the conclusion of security measures.
3. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse.
4. There exist technologies capable of adequately securing mobile devices, which suffice for the majority of organizations.
5. While mobile devices do present distinct cyber security challenges, there are general steps users can take to tackle them.
6. Some measures organizations can adopt include :

i. Implementing robust asset management, virus scanning, loss prevention, and other controls for mobile systems to prevent unauthorized access and data corruption.
ii. Exploring secure access alternatives like mobile VPNs for company information through firewalls.
iii. Establishing a more frequent and comprehensive system of security audits for mobile devices.
iv. Integrating security awareness into mobile training and support programs, emphasizing its significance in the overall IT strategy.
v. Promptly notifying the relevant law enforcement agency and change passwords.

PART-11

Organizational Security Policies and Measures in Mobile Computing Era.

Que 2.18. Discuss the importance of security policies relating to mobile computing devices.

Answer

1. The proliferation of mobile devices amplifies the complexity of the cyber security challenge, surpassing common perception.
2. Individuals, particularly the younger generation, have become so accustomed to their handheld devices that they store a plethora of confidential information on them.
3. They store credit card and bank account details, passwords, confidential emails, and strategic organizational data on mobile devices.
4. Contemplate the potential business repercussions if an employee's mobile device were lost or stolen, exposing sensitive customer information.
5. This scenario not only poses a public relations catastrophe but also raises concerns about legal compliance.
6. When safeguards cannot be established to protect data in the event of theft, the most straightforward solution is to prohibit users from storing proprietary information on insecure platforms.
7. Although enforcing such a policy may prove challenging, increasing user awareness can yield reasonable effectiveness.
8. An information classification and handling policy should unambiguously outline which types of data are permissible for storage on mobile devices.
9. In the absence of alternative safeguards, refraining from storing confidential data on vulnerable platforms effectively mitigates the risk of theft or loss.

Que 2.19. Give the operating guidelines for implementing mobile device security policies.

Answer

Following are the operating guidelines for implementing mobile device security policies :

1. Assess whether organizational employees require the use of mobile computing devices.
2. Deploy additional security technologies such as robust encryption, device passcodes, and physical locks.
3. Standardize both the mobile computing devices and the associated security tools used in conjunction with them.
4. Formulate a dedicated framework for the utilization of mobile computing devices.
5. Maintain an inventory to track who is using which types of devices.

6. Institute patching protocols for software on mobile devices.
7. Label the devices and register them with an appropriate service.
8. Establish procedures for disabling remote access to any mobile device.
9. Eradicate data from computing devices that are not in active use.
10. Offer education and awareness training to personnel utilizing mobile devices.

Que 2.20. What are different ways to create policy for mobile devices ?

Answer

Following are different ways to create policy for mobile devices :

1. **Creating a distinct mobile computing policy :** In this approach, organizations develop a separate and dedicated policy exclusively focused on mobile computing devices. This policy is crafted to address the unique challenges and considerations associated with mobile devices, such as smartphones and tablets.

   Advantages : It allows for comprehensive coverage of mobile-specific issues, tailoring guidelines, security measures, and acceptable usage rules to the specific needs and risks posed by mobile devices.

   Challenges : Managing an additional policy may add complexity to policy administration, and employees might need to familiarize themselves with multiple policies.

2. **Including mobile devices under existing policy :** In this approach, mobile devices are integrated into the organization's existing policies, particularly those related to information security, acceptable use, and data protection. Mobile devices are treated as extensions of the existing policies.

   Advantages : This streamlines policy management by keeping mobile devices under the umbrella of existing governance structures, simplifying policy enforcement, and ensuring consistency.

   Challenges : The existing policies may not comprehensively address all mobile-specific risks, necessitating adaptations and updates. This approach might require policy revisions to accommodate the unique characteristics of mobile devices.

3. **Hybrid approach (mobile devices fall under both existing general policies and a new one) :** In this approach, mobile devices are subject to a dual policy framework. They are covered by both the organization's existing general policies (e.g., IT security, data protection) and a newly created mobile computing policy.

Advantages : It combines the strengths of both approaches by ensuring that mobile devices are integrated into overarching governance structures while also addressing their specific needs.

Challenges : Managing and coordinating policies in a hybrid fashion can be complex. Organizations must ensure that policies are consistent and do not conflict with each other. It may also require employees to adhere to multiple sets of guidelines, potentially leading to confusion.

☺☺☺

3 UNIT

Tools and Methods Used in Cybercrime

CONTENTS

PART-1

Introduction.

Que 3.1. Describe the basic stages of attack through which attacker can compromise a network.

Answer

Following are the basic stages of attack through which attacker can compromise a network :

1. **Initial uncovering :** This stage encompasses two key steps :
   i. In the first step, known as reconnaissance, the attacker collects information about the target from internet sources.
   ii. In the second step, the attacker identifies the company's internal network details, including internet domain, machine names, and IP address ranges, for potential data theft.
2. **Network probe (investigation) :**
   i. During the network investigation phase, the attacker conducts a "ping sweep" to scan the organization's IP addresses.
   ii. Subsequently, a "port scanning" tool is utilized to pinpoint the services running on the target system.
   iii. At this juncture, the attacker has not engaged in any activity deemed abnormal or classifiable as intrusion.
3. **Progressing toward electronic crime (E-crime) :**
   i. The attacker now begins to venture into electronic crime territory by exploiting potential vulnerabilities on the target system.
   ii. Typically, the attacker proceeds through various exploit stages to gain access to the system.
   iii. Once access to a user account is secured, further attempts are made to attain administrator or "root" access.
   iv. "Root" access grants the attacker extensive privileges within the system.
4. **Capturing the network :**
   i. In this stage, the attacker endeavors to assume control of the network, swiftly infiltrating internal systems.
   ii. The next step involves erasing any traces of the attack. The attacker often deploys tools that replace existing files and services with Trojan versions, equipped with backdoor passwords.

5. **Grab the data :**
   i. Having successfully "captured the network," the attacker exploits their position to pilfer confidential data.
6. **Covering tracks :**
   i. The final phase of any cyber attack entails actions taken by the attacker to prolong unauthorized system use while avoiding detection.
   ii. The attacker may remain concealed for extended periods.
   iii. Throughout this entire process, the attacker is meticulous in concealing their identity, starting from the initial stage.

PART-2

Proxy Servers and Anonymizers.

Que 3.2. Briefly explain proxy servers.

Answer

1. A proxy server, situated within a network, serves as an intermediary for connecting with other computers on that same network.
2. To initiate contact with a target system, the attacker initially connects to a proxy server, establishing a connection through an existing link with the proxy.
3. This capability empowers an attacker to navigate the internet incognito and/or conceal the attack's source.
4. When a client seeks specific services (e.g., a file or webpage) from a different server, it connects to the proxy server.
5. The proxy server assesses the request, securing the resource by establishing a connection with the appropriate server and/or soliciting the required service on behalf of the client.
6. Utilizing a proxy server allows an attacker to obscure their identity, achieving anonymity on the network.
7. A proxy server serves several purposes, including :
   i. Concealing systems behind the scenes, primarily for security reasons.
   ii. Accelerating resource access through caching, typically involving the storage of web pages from a web server.
   iii. Employing specialized proxy servers to filter out undesired content, such as advertisements.
   iv. Multiplexing IP addresses, enabling multiple computers to connect to the internet when only one IP address is available.

Que 3.3. **Briefly explain anonymizer.**

Answer

1. An anonymizer, also known as an anonymous proxy, is a tool designed to enhance online privacy by rendering internet activity untraceable.
2. It achieves this by acting as an intermediary between a user and the internet, safeguarding personal information and concealing the identifying details of the user's source computer.
3. Anonymizers are typically web-based services that facilitate anonymous web surfing.
4. Users access these services by visiting a website that acts as the proxy server for their web client.
5. Anonymizers are particularly useful when users want to prevent websites, advertisers, or even malicious entities from tracking their online behavior.
6. While anonymizers offer anonymity to a certain extent, it's essential to recognize that they may not guarantee complete privacy.
7. Users should also exercise caution and verify the trustworthiness of anonymizer services to avoid potential security risks.

PART-3

Phishing.

Que 3.4. **What is phishing ? How phishing works ?**

Answer

Phishing :

1. "Phishing" is a term denoting a cyber attack tactic that involves the use of email programs to trick internet users into divulging confidential information.
2. While reviewing their email, a user comes across a message allegedly from the bank, warning of potential account closure unless an immediate response is provided.
3. Despite the message raising suspicions due to its content, arriving at the conclusion that it is indeed a fraudulent email can be challenging.
4. This message serve as examples of phishing.
5. Apart from the theft of personal and financial data, they also pose the risk of infecting systems with viruses and are employed as a method for online identity theft in various cases.

6. These deceptive messages are meticulously crafted to appear genuine and aim to get users into divulging their personal information.

How phishing works ? Phishers work in the following ways :

1. **Planning :** Phishing attacks begin with meticulous planning. Phishers select their targets, which can be individuals, businesses, or institutions. They research their targets, often gathering information from publicly available sources and online platforms to personalize their attacks.
2. **Setup :** In this stage, phishers establish the infrastructure required for their phishing campaign. This typically involves creating a fake website, email account, or other communication channels that mimic legitimate entities or organizations.
3. **Attack :** Once the setup is complete, phishers initiate the attack. This usually involves sending deceptive emails or text messages. These messages often contain urgent or alarming content, such as fake security alerts, account suspension notices, or offers that seem too good to be true, enticing recipients to take action.
4. **Collection :** As recipients fall for the deception and respond to the phishing messages, phishers collect sensitive information. This can include login credentials, personal identification details, financial information, or credit card numbers.
5. **Identity theft and fraud :** With the collected information, phishers proceed to carry out identity theft and fraudulent activities. They may gain unauthorized access to online accounts, make unauthorized transactions, or even impersonate victims for further phishing attacks.

PART-4

Password Cracking.

Que 3.5. **What do you mean by password cracking ? What is the purpose of password cracking ?**

Answer

Password cracking : Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

Purpose of password cracking : The purpose of password cracking is as follows :

1. **To recover a forgotten password :**
   i. One of the primary and legitimate purposes of password cracking is to recover a forgotten or lost password.

ii. Individuals may find themselves locked out of their accounts due to memory lapses or password changes.

iii. In such cases, they may attempt to crack their own passwords to regain access to their accounts, files, or data.

2. **As a preventive measure by system administrators to check for easily crackable passwords :**
   i. System administrators and security professionals may use password cracking tools proactively as part of security assessments.
   ii. They perform this to identify and rectify security weaknesses in their systems.
   iii. The goal is to find and address vulnerabilities before malicious actors can exploit them.

3. **To gain unauthorized access to a system :**
   i. On the malicious side, cybercriminals and hackers use password cracking techniques to gain unauthorized access to computer systems, user accounts, or sensitive data.
   ii. These attackers may employ various methods, such as brute force attacks, dictionary attacks, or social engineering, to crack passwords and compromise systems.
   iii. Once they gain access, they can engage in activities like data theft, unauthorized transactions, espionage, or vandalism.

Que 3.6. **Discuss the categories of password cracking attacks.**

Answer

Password cracking attacks can be classified under three categories as follows :

A. **Online attacks :**
   1. A potential attacker can create a script file to systematically attempt each password from a list, and when a match is found, they can gain access to the system.
   2. The most prevalent online attack is the man-in-the-middle (MITM) attack, also referred to as the "bucket-brigade attack".
   3. It involves actively stealing information, where the attacker establishes a connection between the victim and the server to which the victim is connected.
   4. Upon a victim client connecting to the fraudulent server, the MITM server intercepts the communication, hashes the password, and then forwards the connection to the victim server.
   5. This form of attack is employed to acquire passwords for email accounts on public websites like Yahoo, Hotmail, and Gmail. It can also be used to obtain passwords for financial websites with the intention of gaining access to banking portals.

B. **Offline attacks :**
   1. Typically, offline attacks are conducted from a location separate from where the passwords are stored or utilized, such as a different computer system or while connected to the network.
   2. Offline attacks typically necessitate physical access to the computer, involving the extraction of the password file from the system onto removable media.

C. **Non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving) :** Refer Q. 1.13, Page 1–13W, Unit-1.

Que 3.7. **Give the password guidelines to be practiced by netizens to avoid being the victim of cyber attack.**

Answer

Following password guidelines should be practiced by netizens to avoid being the victim of cyber attack :

1. It is advisable to maintain separate passwords for business email accounts, personal email accounts, and banking/financial user accounts.
2. Passwords should consist of a minimum of eight alphanumeric characters, avoiding common names or phrases.
3. It is recommended to change passwords every 30 to 45 days.
4. Passwords should not be shared with family members or friends.
5. When renewing a password, refrain from using any previously used passwords.
6. For personal email and banking/financial accounts, change passwords within a few days if these accounts have been accessed from public internet facilities like cybercafes, hotels, or libraries.
7. Avoid storing passwords on mobile phones or PDAs, as these devices are susceptible to cyber attacks.
8. If email or user accounts are compromised, it is essential to promptly contact the relevant agencies or institutions.

PART-5

Keyloggers and Spywares.

Que 3.8. **What do you mean by keylogging (keystroke logging) ? Discuss keylogger and give its classification.**

Answer

Keylogging : Keylogging involves the practice of recording keystrokes on a keyboard, typically done discreetly so that the keyboard user remains unaware of the monitoring.

Keylogger : A keylogger provides a faster and more straightforward method for capturing passwords and observing the digital behavior of victims.

Classification of keylogger : It can be classified as :

A. Software keylogger :

1. Software keyloggers are software programs installed on computer systems, often positioned between the operating system and the keyboard hardware, recording every keystroke.
2. These software keyloggers are typically installed on a computer system without the user's knowledge, often via Trojans or viruses.
3. Cybercriminals frequently deploy such tools on vulnerable computer systems found in public places like cybercafés, making it easy to gather information about their targets.
4. A typical keylogger consists of two files within the same directory : a dynamic link library (DLL) file and an executable (EXE) file. The DLL file is responsible for recording keystrokes.

B. Hardware keylogger :

1. Hardware keyloggers are compact physical devices.
2. They are connected to the PC and/or the keyboard, recording each keystroke either in a file or in the device's memory.
3. Cybercriminals may install these devices on ATM machines to capture ATM card PINs.
4. Every keypress on the ATM's keyboard is registered by these keyloggers.
5. These keyloggers blend seamlessly into the system's architecture, making bank customers unaware of their presence.

Que 3.9. What do you understand by antikeylogger ? Give its advantages.

Answer

An antikeylogger is a tool designed to identify and remove keyloggers that have been installed on a computer system.

Advantages of antikeylogger are as follows :

1. **Detection and removal :** Antikeyloggers are specifically designed to identify the presence of keyloggers on a system. They can detect keylogging software or hardware and help remove it.

2. **Protection from unauthorized surveillance :** By detecting and preventing keyloggers, antikeylogger software ensures that your keystrokes and sensitive data remain private.
3. **Preventing identity theft :** Antikeyloggers are a valuable defense against identity theft.
4. **Preservation of online security :** By safeguarding login credentials and personal information, antikeyloggers help maintain the security of online accounts.
5. **Protecting business and financial data :** For businesses, antikeyloggers are a crucial defense against data breaches and financial losses.

Que 3.10. What do you mean by spyware ?

Answer

1. Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.
2. Spyware can collect sensitive personal information posing a severe threat to users' privacy and security.
3. Spyware operates discreetly in the background, making it challenging for users to detect its presence or activities.
4. In the corporate environment, some individuals may install spyware to gain unauthorized access to sensitive business information.
5. Public computers, such as those in libraries or cybercafes, can be targeted for spyware installation.
6. Spyware can lead to data theft, identity theft, and financial losses for users.
7. The deployment of spyware represents a severe violation of privacy, as it involves monitoring individuals without their consent or knowledge.

PART-6

Virus and Worms.

Que 3.11. What is a computer virus ? List various types of viruses.

Answer

1. A computer virus is a program that can "infect" legitimate software by altering it to incorporate a potentially "mutated" version of itself.
2. Viruses autonomously propagate to potentially numerous programs on various machines without the users' knowledge or consent.

3. The transmission of a computer virus from one system to another closely resembles how a biological virus spreads from one person to another.
4. Viruses may also include malicious instructions that can result in damage or annoyance.
5. The fusion of potential malicious code with the ability to disseminate makes viruses a significant concern.
6. Viruses often have the capacity to spread silently, without displaying obvious symptoms.
7. A virus can initiate based on event-triggered occurrences, time-based triggers, or even randomly occur.
8. A true virus can only spread from one system to another when its host is taken to the target computer; for instance, when a user sent it over the internet or carried it on a removable media such as USB drive.

Types of Viruses :

1. **Boot sector viruses :** These viruses typically infect the master boot record (MBR) of a computer's hard drive or removable media, like USB drives. They are activated when the infected system boots up, making them an early-stage infection.
2. **Program viruses :** Program viruses attach themselves to executable files or applications. When an infected program is run, the virus code executes, potentially damaging the file and spreading to other programs.
3. **Multipartite viruses :** These viruses combine characteristics of both boot sector and program viruses. They can infect both the boot sector and executable files. This dual infection capability makes them resilient and more challenging to remove.
4. **Stealth viruses :** Stealth viruses are adept at concealing their presence from antivirus software and detection methods. They achieve stealthiness by actively altering their code and behavior, making them elusive. These viruses often use rootkit techniques to hide their activities from the operating system.
5. **Polymorphic viruses :** Polymorphic viruses continually change their code's appearance while maintaining their core functionality. This shape-shifting ability allows them to evade signature-based detection mechanisms used by antivirus software.
6. **Macro viruses :** Macro viruses target the macro programming language found in applications like Microsoft Word and Excel. They attach to documents and spreadsheets, and when the document is opened, the macro code executes.

Que 3.12. What is a computer worm ?

Answer

1. A computer worm is a type of malware computer program that possesses the ability to replicate itself.
2. It leverages a computer network to distribute copies of itself to other nodes, or computers, within the network, often accomplishing this without requiring any user involvement.
3. This capability stems from security weaknesses in the target computer's defenses.
4. Worms automatically propagate to other computers via networks by taking advantage of security vulnerabilities.
5. In contrast to viruses, worms do not need to attach themselves to existing programs.
6. Worms typically have some impact on the network, such as consuming bandwidth, whereas viruses usually cause damage by corrupting or altering files on the targeted computer.

Que 3.13. Differentiate between computer virus and worm.

Answer

S. No.	Aspect	Computer Virus	Computer Worm
1.	Definition	A computer program that attaches itself to other executable files or programs and requires a host program to propagate.	A self-replicating malware program that can spread independently and does not need a host program.
2.	Propagation	Requires a host program or file to attach to.	Spreads independently through network connections or other means.
3.	User Involvement	Typically requires user action to execute an infected program.	Can spread without user intervention.
4.	Typical Impact	Can cause damage to files, applications, or the system when activated.	Often consumes network bandwidth and can overload systems.
5.	Examples	CIH virus (Chernobyl virus), Melissa virus.	Conficker worm, ILOVEYOU worm.

PART-7

Trojan-horses and Backdoors.

Que 3.14. What do you mean by Trojan Horse ? Give some typical threats of Trojan Horse.

Answer

1. A Trojan Horse is a program that conceals malicious or harmful code within seemingly harmless software or data, allowing it to take control and inflict damage.
2. Trojan Horses may be widely redistributed as part of a computer virus.
3. Similar to Spyware and Adware, Trojans can infiltrate a system through various means, such as web browsers and email.
4. It might be necessary to format a USB flash drive or another portable device to eliminate an infection and prevent its transfer to other machines.
5. Unlike viruses or worms, Trojans don't replicate themselves, but they can be just as destructive.
6. Trojans initially appear benign and harmless, but once the infected code is executed, they activate and carry out malicious actions that harm the computer system without the user's awareness.

Typical threats of Trojan Horse : Common threats associated with Trojan Horses include :

1. Data deletion, overwriting, or corruption on a computer.
2. Facilitating the dissemination of other malware, such as viruses.
3. Disabling or interfering with antivirus and firewall programs.
4. Granting remote access to your computer.
5. Unauthorized uploading and downloading of files without your knowledge.
6. Compiling email addresses for spam distribution.
7. Recording keystrokes to steal sensitive information like passwords and credit card numbers.
8. Replicating fake links to fraudulent websites, displaying explicit content, playing multimedia, and showing images.
9. Slowing down, restarting, or shutting down the system.
10. Reinstalling themselves even after being disabled.
11. Disabling the task manager.
12. Disabling the control panel.

Que 3.15. What do you understand by Backdoor ? Give its functions.

Answer

1. A backdoor provides a means of accessing a computer program while bypassing its security mechanisms.
2. Occasionally, a programmer may intentionally introduce a backdoor into a program to enable access for troubleshooting or other legitimate purposes.
3. However, attackers frequently exploit or implant backdoors themselves as part of a malicious scheme.
4. In some instances, a worm is specifically designed to exploit a backdoor created by a prior attack.
5. Operating silently in the background, a backdoor remains concealed from the user.
6. Due to its resemblance to a virus, detecting and completely disabling a backdoor can be exceptionally challenging.
7. A backdoor grants malicious individuals the capability to execute any conceivable action on a compromised system.

Functions of backdoor : Following are some functions of backdoor :

1. It grants an attacker the ability to perform actions such as creating, deleting, renaming, copying, or modifying files; executing various commands; adjusting system configurations; and making changes to the Windows registry.
2. It provides an attacker with control over computer hardware devices, enabling them to manipulate associated settings without seeking user authorization.
3. It covertly acquires sensitive personal information, valuable documents, login credentials, passwords, identification details, logs user activities, and monitors internet browsing patterns.
4. It captures keystrokes entered on a computer's keyboard and takes screenshots of the user's activity.
5. It transmits all gathered data to a predetermined email address, uploads it to a predefined FTP server, or transfers it through a concealed internet connection to a remote host.
6. It contaminates files, disrupts installed applications, and inflicts damage on the entire operating system.

Que 3.16. How to protect your systems from Trojan Horses and backdoors ?

Answer

Follow the given steps to protect your systems from Trojan Horses and backdoors :

1. **Stay away from suspect websites/weblinks :** Avoid visiting websites or clicking on web links that appear suspicious or untrustworthy. Be cautious of pop-up ads and links in unsolicited emails, especially those promising free downloads or prizes. Stick to reputable and well-known websites, and ensure the URLs are spelled correctly to avoid phishing attempts.
2. **Surf on the Web cautiously :** Exercise caution when downloading files or software from the internet. Only download from trusted sources, such as official websites or app stores. Be wary of email attachments, especially from unknown senders. Do not open attachments unless you are certain of their legitimacy.
3. **Install antivirus/Trojan remover software :** Install reputable antivirus software on your computer and keep it up to date. Antivirus programs can detect and remove various types of malware, including Trojans and backdoors. Schedule regular system scans to proactively identify and remove any potential threats that may have entered your system.

Que 3.17. What is the difference between Trojan Horses and backdoors ?

Answer

S. No.	Aspect	Trojan Horse	Backdoor
1.	Purpose	Deceptive, appears legitimate.	Covert access and control.
2.	Delivery	Trick users into unknowingly installing.	Can be intentional or left behind.
3.	Visibility	Victim is aware of the program.	Often hidden from the user.
4.	Functionality	Performs specific malicious tasks.	Provides unauthorized access.
5.	Detection	Can be challenging due to deception.	Can be detected through monitoring.
6.	Example	Zeus (banking Trojan).	Netcat (network utility).

PART-8

Steganography.

Que 3.18. Write a short note on: steganography and steganalysis.

Answer

Steganography :

1. Steganography involves the act of hiding a file, message, image, or video within another file, message, image, or video.
2. The term "steganography" is derived from two Greek words : "steganos," which means "covered, concealed, or protected," and "graphein," which means "writing."
3. Steganography is known by various names, including data hiding, information hiding, and digital watermarking.
4. Steganography has the potential to create a digital watermark for identifying unauthorized duplication of digital images.
5. Consequently, it contributes to preserving the confidentiality and integrity of data.

Steganalysis :

1. Steganalysis is the practice of identifying concealed messages within images, audio, or video files that have been encoded using steganography.
2. The primary objective of steganalysis is to detect potentially concealed data packages and ascertain whether they contain encoded payloads, with the ultimate goal of potential recovery.
3. Automated software tools are employed to uncover steganographically hidden data or information within image, audio, and video files.

Que 3.19. Give difference between steganography and cryptography.

Answer

S. No.	Aspect	Steganography	Cryptography
1.	Objective	Hides the message itself within something else.	Converts the message into a secret code.
2.	Visibility	Keeps the fact that a message is hidden discreet.	Makes the message unreadable without a key.

3.	Concealment	Hides the message in plain sight within a medium.	Encodes the message into a secret format.
4.	Detection	Detecting hidden information can be tricky.	Decrypting without the key is tough.
5.	Purpose	Focuses on privacy and keeping messages hidden.	Focuses on security and protecting message content.

PART-9

DoS and DDoS Attacks.

Que 3.20. What is denial-of-service (DoS) attack ? Give its classification.

Answer

1. A DoS attack is an attempt to make a computer resource unavailable to its intended users.
2. In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his e-mail box with Spam mail, making it hard for them to use their services.
3. A technique called Buffer overflow is used to do this criminal attack, which is called Spoofing.
4. IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of hiding the ID of the sender.
5. The attacker spoofs the IP address and floods the network of the victim with repeated requests.
6. Because the IP address is fake, the victim's computer keeps waiting for response from the attacker's machine for each request.
7. This uses up all the bandwidth of the network which then fails to serve real requests and ultimately stops working.

Classification of DoS attack :

1. **Bandwidth attacks :** Bandwidth-based DoS attacks focus on overwhelming a victim's network or server by consuming its available bandwidth with a massive volume of data. This causes legitimate users to experience slow or no access to the targeted resource.

Example : A simple bandwidth attack might involve sending an enormous amount of traffic to a website, making it slow or entirely inaccessible for regular users.

2. **Logic attacks :** Logic-based DoS attacks exploit vulnerabilities in the software or application logic to disrupt services. These attacks do not necessarily require a high volume of traffic but focus on exploiting weaknesses in the target system's logic or functionality.

   Example : An attacker might send specially crafted requests to a web application, causing it to crash or become unresponsive due to a software vulnerability.

3. **Protocol attacks :** Protocol-based DoS attacks exploit weaknesses in network protocols to disrupt communication between devices or services. These attacks often involve exploiting flaws in how systems handle network protocols, leading to service disruptions.

   Example : An attacker might send a flood of malformed or malicious network packets to exploit vulnerabilities in the target's network protocol stack, leading to service disruption.

4. **Unintentional DoS attack :** Unintentional DoS attacks occur without malicious intent. Instead, they result from genuine user actions or system misconfigurations that inadvertently disrupt services or resources.

   Example : A website may experience an unintentional DoS attack during a product launch when a large number of users simultaneously try to access the site, causing it to slow down or become temporarily unavailable.

Que 3.21. What are different types or levels of DoS attacks ?

Answer

Following are different types or levels of DoS attacks :

1. **Flood attack :** A flood attack is a straightforward form of DoS attack where the attacker overwhelms the target system with an excessive volume of traffic, such as a flood of data packets or connection requests.
2. **Ping of death attack :** The ping of death attack exploits vulnerabilities in the way some systems handle oversized ICMP packets (ping requests) to crash or freeze the target system.
3. **SYN attack :** SYN attacks target the TCP (Transmission Control Protocol) handshake process, which establishes a connection between two devices. Attackers send a large number of SYN (synchronize) requests without completing the handshake, tying up the target's resources.
4. **Teardrop attack :** A teardrop attack exploits vulnerabilities in the reassembly of fragmented IP packets. Attackers send overlapping, fragmented packets to the target, causing it to crash or become unstable when attempting to reassemble them.

5. **Smurf attack :** A Smurf attack abuses network broadcast addresses to amplify a DoS attack. Attackers send ICMP echo requests (pings) with a spoofed source IP address to a network's broadcast address, causing all devices on the network to respond to the victim's IP address.
6. **Nuke :** Nuke attacks target the vulnerabilities in older operating systems (such as Windows 95 and Windows 98). Attackers send malicious packets designed to exploit these vulnerabilities, causing the target system to crash or freeze.

Que 3.22. What is distributed denial-of-service (DDoS) attack ?

Answer

1. DDoS attack is a malicious attempt to disrupt networks or websites by flooding them with massive traffic from multiple sources.
2. DDoS differs from traditional DoS as it uses multiple compromised devices, forming botnets, for a coordinated attack.
3. In a DDoS attack, your computer might be used by an attacker to target another computer.
4. By exploiting security vulnerabilities or weaknesses, an attacker could gain control over your computer.
5. Subsequently, they could compel your computer to send substantial volumes of data to a website or dispatch spam to specific e-mail addresses.
6. The term "distributed" in this context refers to the attacker utilizing multiple computers for launching the DoS attack.
7. A DDoS attack is essentially a distributed form of DoS where a considerable number of zombie systems are synchronized to attack a specific target.
8. Presently, botnets are the prevalent means for initiating DoS/DDoS attacks.

Que 3.23. How to protect from being a victim of DoS/DDoS attacks ?

Answer

To avoid falling victim to DoS/DDoS attacks, you can take the following preventative measures :

1. Apply router filters to reduce vulnerability to specific DoS attacks.
2. If your system supports them, apply patches to protect against TCP SYN flooding.
3. Deactivate any unnecessary or unused network services.
4. If available, enable quota systems on your operating system.
5. Monitor your system's performance and create benchmarks for normal activities.

6. Regularly assess your physical security in alignment with your current requirements.
7. Employ tools like Tripwire or similar software to detect alterations in configuration data or other files.
8. Invest in and maintain "hot spares" - machines that can be swiftly deployed if a similar machine fails.
9. Establish redundant and fault-tolerant network setups for added resilience.
10. Set up and adhere to routine backup schedules.
11. Implement and uphold appropriate password policies.

Que 3.24. What is the difference between DoS and DDoS ?

Answer

S. No.	Aspect	DoS (Denial of Service)	DDoS (Distributed Denial of Service)
1.	Attack Source	Single source or a few systems	Multiple sources, often a botnet network
2.	Traffic Volume	Moderate to low	High, often overwhelming
3.	Complexity	Relatively simple to execute	Requires coordination and resources
4.	Detection	Easier to detect and mitigate	Harder to detect and mitigate
5.	Resource Usage	Minimal resource usage	Significant resource consumption
6.	Impact	Can disrupt services briefly	Can cause prolonged outages
7.	Example	Sending excessive requests	Coordinated attack from a botnet

PART-10

SQL Injection.

Que 3.25. What is SQL Injection and what are the different countermeasures to prevent the attack ?

Answer

SQL Injection :

1. SQL injection is a method of injecting code that takes advantage of a security weakness occurring in the database layer of an application.
2. SQL injection attacks can also be referred to as SQL insertion attacks.
3. SQL servers, which are commonly used by many organizations to store sensitive data, are the primary targets of these attackers.
4. The primary goal of an SQL injection attack is to retrieve information from a database table that might include personal data like credit card numbers, social security numbers, or passwords.
5. Malicious code is inserted into either a web form field or the website's code during an SQL injection attack.
6. For instance, when a user logs in with a username and password, the database is queried using an SQL query to verify if the user has a valid name and password.
7. SQL injection enables an attacker to potentially alter the SQL query by sending a carefully crafted username and/or password field.

Countermeasures to prevent SQL Injection attack : The following steps can be taken to prevent SQL injection attack :

1. **Input validation :**
   - i. Input validation is the process of verifying and sanitizing user inputs before they are used in SQL queries.
   - ii. It involves checking the data type, length, and format of inputs to ensure they adhere to expected patterns.
2. **Modify error reports :** Error messages generated by your application should not reveal sensitive information about the database structure or SQL queries. Attackers can exploit detailed error messages to gain insights into your database and its vulnerabilities.

   Example : Instead of an error message like "SQL Syntax Error : You have an error in your SQL query near 'SELECT* FROM users WHERE username = 'admin' –", display a generic message like "An error occurred. Please try again later."
3. **Other preventions :**
   - i. The default system accounts for SQL server 2000 should never be used.
   - ii. Isolate database server and web server.
   - iii. Implement a web application firewall to filter and monitor incoming traffic for suspicious patterns and known attack signatures.
   - iv. Keep your database management system (DBMS) and application framework up to date with security patches.

Que 3.26. What is Blind SQL Injection attack ? Can it be prevented ?

Answer

Blind SQL Injection attack :

1. Blind SQL injection is employed when a web application has a vulnerability to SQL injection, but the attacker cannot directly see the outcomes of the injection.
2. The vulnerable page might not be responsible for showing data, but its response varies based on the results of a logical statement injected into the legitimate SQL statement executed on that page.
3. This form of attack can be time-consuming as it requires the creation of a new statement for each recovered bit of information.
4. Numerous tools are available for automating these attacks once the vulnerability's location and the target information have been identified.

Prevention of Blind SQL Injection :

1. Blind SQL Injection attacks can be prevented through a combination of secure coding practices and following input validation techniques :
   - i. **Input validation :** Validate and sanitize user inputs to reject malicious characters.
   - ii. **Prepared statements :** Use parameterized queries to automatically prevent SQL injection.
   - iii. **Least privilege :** Limit database user permissions to minimize potential damage.
   - iv. **Error handling :** Mask sensitive database details in error messages.
   - v. **Regular updates :** Keep software and frameworks up to date.
2. By implementing these preventive measures, you can significantly reduce the risk of Blind SQL Injection attacks.

PART-11

Buffer Overflow.

Que 3.27. What is buffer overflow ? What are different buffer overflow attacks ?

Answer

Buffer overflow :

1. A buffer overflow, also known as a buffer overrun, occurs when a process stores data in a buffer beyond the memory allocated for it by the programmer.

2. This can lead to unreliable program behavior, such as memory access errors, incorrect results, program crashes, or even a compromise of system security.
3. Buffer overflows can be triggered by inputs intended to execute code or modify the program's behavior.
4. Consequently, they serve as the foundation for numerous software vulnerabilities and can be maliciously exploited.
5. The implementation of bounds checking is an effective way to prevent buffer overflows.
6. Programming languages commonly linked with buffer overflows, such as C and C++, lack built-in protections against unauthorized data access or memory overwrites.

Buffer overflow attacks :

1. **Stack-based buffer overflow :**

   Description : In a stack-based buffer overflow, the attacker exploits a vulnerability in a program by overflowing a buffer located on the call stack. The call stack is a region of memory used to manage function calls and local variables.

   How it works : The attacker supplies more data than the buffer can hold, causing the excess data to overwrite adjacent memory locations, including function return addresses.

2. **NOPs :**

   Description : NOPs, or no-operation instructions, are used as padding in buffer overflow exploits. They serve to create space between the injected shellcode and the return address, making it easier for the attacker to hit the correct memory address.

   How it works : By inserting NOPs into the payload, the attacker increases the likelihood of the CPU executing the shellcode correctly. Even if the exact memory location is not known, the NOP sled increases the chances of landing in the vicinity of the shellcode.

3. **Heap buffer overflow :**

   Description : In a heap-based buffer overflow, the attacker targets data stored in the program's heap memory, which is used for dynamically allocated data.

   How it works : The attacker manipulates the program in such a way that it writes data beyond the boundaries of a heap-allocated buffer. This can corrupt heap metadata or overwrite other heap objects.

Que 3.28. How to minimize buffer overflow attacks ?

Answer

Following methods help to minimize buffer overflow attacks :

1. **Assessment of secure code manually :** Manual code review and assessment involve scrutinizing the source code by human experts to identify and rectify potential vulnerabilities, including buffer overflows.

   How it works : Skilled developers and security experts examine the code line by line to identify insecure coding practices, such as improper bounds checking or unvalidated input handling, which can lead to buffer overflows.

2. **Disable stack execution :** Disabling stack execution is a security mechanism that prevents code from being executed on the stack, making it more challenging for attackers to exploit stack-based buffer overflows.

   How it works : By configuring the system to mark the stack memory as non-executable (using features like NX or DEP, depending on the operating system), the CPU prevents execution of code residing on the stack.

3. **Compiler tools :** Modern compilers often include security features and flags to mitigate buffer overflow vulnerabilities during the compilation process.

   How it works : Compiler tools can perform various tasks, such as bounds checking, stack canaries (random values placed between buffers and return addresses), and other optimizations to enhance code security.

4. **Dynamic run-time checks :** Dynamic run-time checks involve monitoring a program's execution during runtime to identify and respond to unexpected behavior, such as buffer overflows.

   How it works : Intrusion detection systems (IDS), runtime security monitors, and tools like AddressSanitizer can dynamically detect buffer overflow attempts while the program is running.

PART-12

Attacks on Wireless Networks.

Que 3.29. What are different components of wireless network ?

Answer

Following are different components of wireless network :

1. **802.11 networking standards :** These are a set of standards established by the IEEE that define the specifications for wireless local area networks (Wi-Fi). Examples include 802.11b, 802.11g, 802.11n, and 802.11ac.
2. **Access points :** Access points (APs) are devices that bridge wireless clients (like laptops and smartphones) to a wired network. They create a wireless local area network (WLAN) by broadcasting a Wi-Fi signal.
3. **Wi-Fi hotspots :** Wi-Fi hotspots are locations where wireless access to the internet is available, often provided by public establishments such as cafes, airports, and hotels.

4. **Service Set Identifier (SSID) :** The SSID is a unique name assigned to a wireless network. It acts as an identifier for wireless clients to distinguish one network from another.
5. **Wired equivalence privacy (WEP) :** WEP is an early security protocol used in Wi-Fi networks to encrypt data transmitted over the network.
6. **Wi-Fi protected access (WPA and WPA2) :** WPA and WPA2 are improved and more secure encryption and security protocols for Wi-Fi networks.
7. **Media access control (MAC) :** The MAC address is a unique hardware identifier assigned to each network device, such as network adapters or wireless cards.

Que 3.30. **Discuss some of the traditional techniques of attacks on wireless networks.**

OR

How can wireless networks be compromised ?

Answer

Following are some of the traditional techniques of attacks on wireless networks :

1. **Sniffing :** Sniffing, also known as packet sniffing or network sniffing, involves intercepting and monitoring data packets transmitted over a wireless network.

   Function : Attackers capture network traffic to eavesdrop on sensitive information, such as login credentials, emails, or financial data. Sniffing attacks exploit the lack of encryption or weak encryption in network communication.
2. **Spoofing :** Spoofing attacks involve impersonating a legitimate entity or device on a wireless network by falsifying identifying information.

   Function : Attackers can perform various spoofing attacks, such as MAC address spoofing or ARP spoofing, to deceive network devices into accepting them as trusted entities. This can lead to unauthorized access or interception of data.
3. **Denial of service (DoS) :** Denial of Service attacks aim to disrupt the normal functioning of a wireless network or the services it provides by overwhelming it with excessive traffic or requests.

   Function : Attackers flood the network or its resources, making them unavailable to legitimate users. This can result in network downtime, rendering it unusable.
4. **Man-in-the-middle attack (MITM) :** In a Man-in-the-Middle attack, an attacker intercepts and possibly alters communication between two parties without their knowledge.

Function : Attackers position themselves between the communicating parties, allowing them to capture, modify, or inject data into the communication flow. MITM attacks can lead to data interception, eavesdropping, or the insertion of malicious content.

5. **Encryption cracking :** Encryption cracking involves attempting to decrypt encrypted data transmitted over a wireless network by exploiting vulnerabilities or using brute force methods.

   Function : Attackers target encrypted data, such as Wi-Fi passwords, using techniques like dictionary attacks or cryptographic weaknesses. Successful decryption provides unauthorized access to the network.

PART-13

Phishing and Identity Theft : Introduction to Phishing, Identity Theft (ID Theft).

Que 3.31. **What is phishing ? Explain with examples.**

Answer

1. Phishing is a cyber attack technique in which attackers impersonate legitimate individuals, organizations, or entities to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal data.
2. Phishing attacks typically occur through email, but they can also take place via text messages, social media, or other communication channels.

Examples of Phishing :

1. **Email phishing :** You receive an email that appears to be from your bank, asking you to verify your account details urgently. The email contains a link that takes you to a website that looks identical to your bank's official site. If you enter your login credentials on this fake site, the attackers capture your information.
2. **Vishing (voice phishing) :** You receive a phone call from someone claiming to be from a trusted organization, like a bank or tech support. They inform you of a security issue and ask for sensitive information, such as your credit card details.
3. **Smishing (SMS phishing) :** You receive a text message claiming to be from a reputable service or organization. It informs you of an urgent matter and includes a link or phone number to resolve the issue. Clicking the link may lead to a fraudulent website or result in a phone call with a scammer.
4. **Social media phishing :** Attackers create fake social media profiles impersonating friends, family members, or known organizations. They send messages or friend requests to gather personal information or spread malware.

Que 3.32. **Discuss spam and hoax e-mails. Give difference between them.**

Answer

1. Spam and Hoax emails are both types of unsolicited or deceptive emails, but they serve different purposes and often have distinct characteristics.
2. Spam emails are typically commercial or promotional in nature, seeking profit or engagement with recipients.
3. Hoax emails, on the other hand, aim to deceive or misinform recipients with fabricated stories, warnings, or false information.

Difference :

S. No.	Aspect	Spam Emails	Hoax Emails
1.	Purpose	Promotional or commercial.	Spread false information.
2.	Content	Ads, offers, product links.	Fabricated stories, warnings.
3.	Origin	Marketers, businesses, cybercriminals.	Individuals, groups.
4.	Response	Prompt action (clicks, purchases).	Elicit emotional responses.
5.	Examples	Product ads, phishing, scams.	Chain letters, false alerts.

Que 3.33. **What are different methods of phishing attacks ?**

Answer

Following are different methods of phishing attacks :

1. **Dragnet :** Dragnet phishing is a mass email phishing technique where cybercriminals send a large number of generic phishing emails to a wide audience.

   How it works : Attackers cast a wide net, sending phishing emails without specific targeting. These emails often contain generic messages and fake links or attachments designed to trick recipients into providing personal information or credentials.

2. **Rod-and-reel :** Rod-and-reel phishing is a more targeted approach in which attackers select specific individuals or organizations as their victims.

   How it works : Unlike dragnet phishing, which casts a wide net, rod-and-reel phishing involves carefully selecting and researching potential victims. Attackers tailor their phishing emails to appear highly relevant to the targeted individuals, increasing the likelihood of success.

3. **Lobsterpot :** In lobsterpot phishing attackers focus on high-value individuals or entities.

   How it works : Cybercriminals gather extensive information about their intended targets, including personal and professional details. They craft highly personalized and convincing phishing emails, often posing as trusted contacts or organizations the targets are familiar with.

4. **Gillnet :** Gillnet phishing is a method that combines elements of both dragnet and rod-and-reel phishing. It targets a larger group of individuals or organizations than rod-and-reel, but with a more focused approach than dragnet.

   How it works : Attackers select a specific group or category of potential victims who share certain characteristics. They send phishing emails tailored to the interests or needs of this group.

Que 3.34. **What is identity theft (ID theft) ? Explain types of identity theft.**

Answer

1. Identity theft (ID theft) is a type of cybercrime where an individual's personal, financial, or confidential information is stolen by malicious actors with the intent of impersonating the victim for various fraudulent purposes.
2. Identity thieves often use this stolen information to commit financial fraud, gain unauthorized access to accounts, or engage in other criminal activities under the victim's identity.

Types of identity theft :

1. **Financial identity theft :** Financial identity theft occurs when an individual's personal and financial information, such as credit card numbers, or bank account details, is stolen with the intent to commit financial fraud.
2. **Criminal identity theft :** Criminal identity theft involves an identity thief using the victim's identity to evade law enforcement, typically when they are facing criminal charges or arrest.
3. **Identity cloning :** It is a comprehensive form of identity theft where the attacker duplicates the victim's entire identity, including personal, financial, and biographical information.
4. **Business identity theft :** In business identity theft, fraudsters target businesses, often small ones, to steal their identities. This allows them to exploit the business's credit, finances, or reputation.

5. **Medical identity theft :** It occurs when an attacker gains access to an individual's healthcare information, including medical insurance details and medical history, for fraudulent purposes.
6. **Synthetic identity theft :** It involves creating a new identity by combining real and fake information. Attackers use this identity to establish credit or engage in fraudulent activities.
7. **Child identity theft :** Child identity theft targets minors who have clean credit histories. Criminals obtain and misuse the child's personal information, often going undetected for years.

Que 3.35. **What are different techniques of identity theft (ID theft) ?**

Answer

Techniques of ID theft :

A. Human-based methods :

1. **Direct access to information :** Attackers gain access to personal information through social engineering or deception, often by impersonating trusted individuals or services.
2. **Dumpster diving :** Identity thieves sift through trash, looking for discarded documents containing sensitive information, such as bank statements or credit card offers.
3. **Theft of a purse or wallet :** Criminals physically steal purses or wallets to obtain IDs, credit cards, and personal information to commit identity fraud.
4. **Mail theft and rerouting :** Attackers intercept or reroute victims' mail to gain access to financial statements, checks, and other personal data.
5. **Shoulder surfing :** Thieves watch over victims' shoulders as they enter PINs or passwords, gaining unauthorized access to accounts.
6. **Dishonest or mistreated employees :** Insiders with access to personal data may misuse or steal this information for financial gain.
7. **Telemarketing and fake telephone calls :** Scammers use phone calls to trick victims into revealing personal or financial information, often posing as legitimate entities.

B. Computer-based technique :

1. **Backup theft :** Attackers steal physical or digital backups containing sensitive information, allowing them access to victim data.
2. **Hacking :** Cybercriminals exploit vulnerabilities to gain unauthorized access to computer systems and databases, stealing personal and financial data.
3. **Phishing :** Attackers send deceptive emails or messages, impersonating trusted entities to trick recipients into revealing sensitive information.

4. **Pharming :** Cybercriminals redirect victims to fraudulent websites to capture login credentials or personal information, often through DNS manipulation.
5. **Hardware :** Attackers may compromise hardware, such as ATM skimmers or compromised point-of-sale (POS) systems, to steal card data or personal information from unsuspecting individuals.

Que 3.36. **How to prevent being a victim of ID theft ?**

Answer

By implementing the following security precautions, you can avoid falling victim to identity theft :

1. Vigilantly oversee your credit history.
2. Maintain comprehensive records of your financial activities and transactions.
3. Deploy security software for added protection.
4. Utilize an up-to-date web browser.
5. Exercise caution when dealing with email attachments and links in both email and instant messages.
6. Safely store sensitive information.
7. Shred documents containing personal data.
8. Safeguard your personally identifiable information.
9. Remain vigilant regarding the most recent scams and frauds.

☺☺☺

4 UNIT

Understanding Computer Forensics

CONTENTS

PART-1

Intruduction.

Que 4.1. What do you understand by cyber forensics/digital forensics/computer forensics ?

Answer

1. The terms cyber forensics/digital forensics/computer forensics are often used interchangably.
2. Cyber forensics is simply application of computer investigation and analysis techniques in the interest of determining potential legal evidence.
3. Cyber forensics is one of the emerging professions of 21st century.
4. It can be thought of as an investigation of computer based evidence of criminal activity, using scientifically developed methods that attempts to discover and reconstruct event sequences from such activity.
5. This science works on the fact that the computer operating system invariably leaves behind the computer evidences transparently without the knowledge of computer operator. The information may actually be hidden from view.
6. Any enterprise that uses computer networks should have concern for both security and forensic capabilities.
7. Forensic tools should be developed to scan continually computers and networks within an enterprise for illegal activities.
8. When misuse is detected these tools should record sequence of events and store relevant data for further investigation.
9. Special forensic software tools and techniques are required in order to recognize and retrieve such evidences.
10. Cyber forensics involves obtaining and analyzing such digital information for use in civil/criminal or administrative cases.
11. Digital evidence was not considered as tangible evidence in courts until recently but now they are gaining importance.

PART-2

Digital Forensics Science.

Que 4.2. What is digital forensics ? Explain the role of digital forensics.

Answer

Digital forensics :

1. Digital forensics entails employing analytical methods to ensure the dependable and impartial gathering, examination, comprehension, and exposition of digital proof.
2. The goal of "cyberforensics" is to find digital proof of something specific or general.
3. Defining "digital evidence" is tricky because it comes from things like phones, iPods, and other devices that aren't seen as computers in the usual sense.

Role of digital forensics : In general, the role of digital forensics is to :

1. **Uncover and document evidence and leads :** Digital forensics experts use specialized techniques to uncover and document digital evidence from various electronic devices. This evidence can include text messages, emails, documents, images, and more.
2. **Corroborate evidence discovered in other ways :** Digital forensics can act as a crucial validation tool. When evidence is discovered through other means, such as witness testimonies or physical evidence, digital forensics can corroborate or refute these claims.
3. **Assist in showing a pattern of events :** Digital forensics also helps in piecing together a timeline or pattern of events. By analyzing digital data, forensics experts can help investigators reconstruct the sequence of events, shedding light on motives and actions.
4. **Connect attack and victim computers :** In cases of cybercrimes or computer-based attacks, digital forensics plays a critical role in connecting the attacker to the victim. Forensics experts can trace the digital footprints left behind during an attack.
5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.
6. Extract data that may be hidden, deleted or otherwise not directly available.

Que 4.3. Give examples of some typical scenarios in which digital forensics are used.

Answer

Following are examples of some typical scenarios in which digital forensics are used :

1. **Employee internet abuse :** In the workplace, employees may misuse company resources, including internet access, for personal reasons.

Digital forensics can track an employee's online activities, revealing unauthorized downloads, excessive social media usage, or visits to prohibited websites.

2. **Data leak/data breach :** When sensitive data is leaked or breached, digital forensics experts investigate the incident to determine how the breach occurred and what data was compromised. They analyze system logs, network traffic, and compromised devices to identify the point of entry and the extent of the breach.

3. **Industrial espionage :** In cases of corporate espionage, competitors may attempt to steal valuable intellectual property or trade secrets. Digital forensics helps uncover evidence of unauthorized access, data exfiltration, or insider involvement.

4. **Criminal fraud and deception cases :** Digital forensics is frequently employed in cases of fraud, embezzlement, or financial deception. Investigators analyze financial records, emails, and digital communications to trace fraudulent activities and identify individuals responsible.

5. **Criminal cases :** Digital forensics is a fundamental tool in criminal investigations, including cases involving cybercrimes, cyberbullying, or cyberstalking. It helps law enforcement gather evidence from electronic devices such as computers, smartphones, and GPS systems.

6. **Copyright violation :** In cases of copyright infringement, digital forensics experts can analyze digital content to determine its origin and authenticity. They examine metadata, file signatures, and digital watermarks to establish whether copyrighted material has been used without permission.

PART-3

The Need for Computer Forensics.

Que 4.4. What is the need for computer forensics ?

Answer

1. The synergy between advancements in Information and Communications Technology and the widespread adoption of computers worldwide has yielded numerous benefits for humanity.
2. Simultaneously, the immense technical capabilities of computing devices create both opportunities for misuse and potential for criminal activities.
3. Consequently, this has led to fresh risks for computer users and an elevated potential for societal harm.

4. Users have to live with an ongoing threat posed by hackers, who employ various techniques and tools to infiltrate computer systems, manipulate information, and create chaos.
5. The need for computer forensics can be attributed to two key factors : law enforcement's growing reliance on digital evidence and the universal proliferation of computers resulting from the microcomputer revolution.

Que 4.5. What is "chain of custody" concept ? Explain its importance. Provide illustration to support your answer.

Answer

Chain of custody :

1. It refers to the chronological record or documentation process that signifies the acquisition, possession, control, transfer, examination, and final handling of evidence, whether it is in physical or electronic form.
2. The primary purpose of the chain of custody is to ensure the integrity and reliability of the evidence, as well as to demonstrate that it has not been tampered with or compromised at any point during its handling.

Importance of the chain of custody :

1. **Maintaining integrity :** The chain of custody ensures that evidence remains unaltered and untampered with throughout its journey.
2. **Admissibility in court :** Properly maintained chain of custody records are essential for evidence to be admitted in court.
3. **Preserving rights :** It safeguards the rights of the accused.
4. **Accountability :** The chain of custody holds individuals and organizations accountable for the evidence they handle.
5. **Enhancing trust :** It enhances public trust in the criminal justice system.

Illustration : Consider a criminal case involving a burglary. The police collect various pieces of evidence at the crime scene, including a fingerprint on a window, a broken glass shard, and a stolen laptop. Here's how the chain of custody works in this scenario :

1. **Collection :** An officer carefully collects the evidence, labels each item, and records the date, time, and location of collection.
2. **Transport :** The evidence is then securely transported to the forensic lab, where it is signed over to the evidence custodian.
3. **Storage :** The evidence custodian stores the items in a controlled environment, maintaining their integrity and security.
4. **Analysis :** If needed, forensic experts may analyze the evidence, such as comparing the fingerprint to known suspects.
5. **Court presentation :** If the case goes to trial, the chain of custody records are used to show that the evidence was handled correctly and that it has not been tampered with.

6. **Disposition :** After the trial, the evidence is either returned to its rightful owner or kept in long-term storage, depending on the case's outcome and legal requirements.

PART-4

Cyber Forensics and Digital Evidence.

Que 4.6. What do you understand by digital evidence ? Compare physical evidence and digital evidence.

Answer

Digital evidence :

1. Digital evidence refers to any information or data that is stored or transmitted in a digital form and can be used as evidence in legal proceedings.
2. It encompasses a wide range of digital sources, including: electronic documents, computer files, log files, metadata, internet activity and device information.
3. Digital evidence can be critical in a wide range of legal cases, including criminal investigations, civil litigation, intellectual property disputes, and cyber security incidents.
4. It is subject to the same legal standards and rules of admissibility as physical evidence.
5. Its proper handling, preservation, and presentation are essential to ensure its validity in court.

Comparison :

S. No.	Aspect	Physical Evidence	Digital Evidence
1.	Nature	Tangible, physical	Intangible, electronic
2.	Examples	Weapons, documents	Emails, computer files
3.	Storage	Physical form, lockers	Electronic devices, servers
4.	Preservation	Protect from damage	Safeguards against corruption
5.	Collection	Traditional methods	Specialized software
6.	Alteration Risk	Tampering and contamination	Digital alteration, data loss
7.	Presentation	Presented physically	Presented digitally

Que 4.7. Explain some of the best practices in handling digital evidence.

Answer

Following are some of the best practices in handling digital evidence :

1. **Document the chain of custody :** Maintain a detailed record of everyone who has had access to the digital evidence from the moment of collection to its presentation in court. Note any transfers, handling, or examinations, including dates, times, and reasons for access.
2. **Preserve the original evidence :** Make forensic copies (bit-for-bit copies) of the original digital evidence for analysis. Keep the original evidence intact and in a secure, controlled environment to prevent tampering or alteration.
3. **Use write-protect tools :** Employ hardware or software write-blocking tools to ensure that the original evidence remains unaltered during the copying process. Avoid any actions that could write data to the original media, such as booting from it.
4. **Maintain a clean and controlled environment :** Ensure that the forensic examination environment is clean, secure, and free from potential contaminants. Minimize electromagnetic interference, which can affect digital evidence.
5. **Authenticate the evidence :** Establish the authenticity of digital evidence by verifying its source, integrity, and reliability. Document the methods used to validate the evidence, including hash values and digital signatures.
6. **Adhere to legal procedures :** Comply with relevant laws, regulations, and court orders when collecting, preserving, and presenting digital evidence. Seek proper authorization or warrants as required by law.
7. **Properly label and document evidence :** Label all evidence items clearly and comprehensively, including details like case numbers, exhibit numbers, and descriptions. Document the context in which evidence was found, its location, and its relevance to the case.
8. **Secure the evidence log and case files :** Protect all logs, case files, and documentation associated with the digital evidence to maintain their integrity and confidentiality. Encrypt and restrict access to these materials.
9. **Maintain evidence integrity during analysis :** Take precautions to prevent altering or contaminating evidence during analysis. Use forensic copies for analysis, not the original evidence.
10. **Document analysis procedures :** Keep a record of the methods, tools, and procedures used during the analysis of digital evidence. Note any findings, observations, or changes made during the analysis.

Que 4.8. **Write a short note on: Rules of evidence.**

Answer

1. The Rules of Evidence under the Indian Evidence Act, 1872, provide a structured framework for the admission and exclusion of evidence in Indian courts.
2. These rules play a pivotal role in ensuring that trials are fair, evidence is reliable, and justice is served.
3. Here's a brief overview of the key aspects of the Rules of Evidence in the Indian Evidence Act :
   i. **Relevance of evidence :** One of the fundamental principles is that evidence must be relevant to the case. Evidence is considered relevant if it has a direct or indirect bearing on the facts in issue or is related to the credibility of a witness. Irrelevant evidence is not admissible.
   ii. **Admissibility of oral and documentary evidence :** The Act classifies evidence into two main categories: oral evidence (statements made by witnesses during trial) and documentary evidence (written or printed documents). It provides rules regarding the admissibility of both types of evidence.
   iii. **Primary and secondary evidence :** The Act distinguishes between primary evidence (original documents) and secondary evidence (copies or duplicates). Primary evidence is generally preferred, but secondary evidence may be admissible under certain circumstances.
4. The Indian Evidence Act, 1872, is a comprehensive legislation that governs the admissibility and weight of evidence in Indian courts.
5. It plays a critical role in ensuring that trials are conducted fairly, evidence is evaluated impartially, and justice is administered effectively.

PART-5

Forensics Analysis of E-Mail.

Que 4.9. **What do you understand by forensics analysis of e-mail ?**

Answer

1. Forensic analysis of e-mails is a process of systematically examining e-mail messages and associated data to gather evidence for legal or investigative purposes.
2. This type of analysis is commonly used in various fields, including law enforcement, corporate investigations, cyber security, and legal proceedings.

3. Various cybercrime offenses can be committed by criminals using fake emails.
4. There are tools available to assist in the creation of fraudulent e-mails.
5. The act of tracing an e-mail is a crucial component of forensic investigation when an e-mail is suspected to be linked to a cybercrime.
6. The forensic analysis of e-mails plays a vital role in cyber forensics as it aids in confirming the legitimacy of an e-mail under suspicion.
7. With e-mail being the most prevalent global communication method, it becomes a subject of forensic scrutiny when it potentially constitutes "digital evidence."
8. Due to increased regulatory agency pressure, organizations are compelled to electronically retain information to comply with requests for discovery and disclosure support.

Que 4.10. Explain message header of an e-mail.

Answer

Following is an example of message header :

1. Return-Path: <sender@example.com>
2. Received: from mailserver1.example.com (mailserver1.example.com [192.168.1.100])
   by mailserver2.example.com (mailserver2.example.com [203.0.113.42])
   with ESMTP id ABC123456789
   for <recipient@example.net>; Tue, 19 Sep 2023 15:30:00 -0400 (EDT)
3. From: John Doe <sender@example.com>
4. To: Jane Smith <recipient@example.net>
5. Cc: Additional Recipient <cc_recipient@example.org>
6. Bcc: Secret Recipient <bcc_recipient@example.com>
7. Subject: Example Email Header
8. Date: Tue, 19 Sep 2023 15:29:45 -0400
9. Message-ID: <XYZ987654321@mailserver1.example.com>
10. MIME-Version: 1.0
11. Content-Type: text/plain; charset="utf-8"
12. X-Originating-IP : [199.196.144.42]

The message header typically includes the following information :

1. **Return-Path :** This field specifies the e-mail address to which bounce-back messages (non-delivery reports or bounce messages) are sent if the e-mail cannot be delivered.

2. **Received :** This field records the path that the email took as it traveled from the sender's email server to the recipient's email server. It includes information about the servers involved, their IP addresses, and timestamps.
3. **From :** This field displays the sender's e-mail address and, often, their name. It indicates who sent the e-mail.
4. **To :** This field lists the recipient's e-mail address. In the case of multiple recipients, there may be multiple "To" fields.
5. **Cc (Carbon Copy) :** This field lists the e-mail addresses of additional recipients who receive a copy of the e-mail.
6. **Bcc (Blind Carbon Copy) :** Similar to "Cc," this field lists additional recipients. However, the difference is that the recipients listed in the "Bcc" field are not visible to other recipients.
7. **Subject :** This field contains the subject or topic of the e-mail message. It gives recipients an idea of the content of the e-mail.
8. **Date :** The date and time when the e-mail was sent are recorded in this field.
9. **Message-ID :** A unique identifier for the e-mail message generated by the sender's e-mail server. It is used for tracking and referencing specific messages, especially in e-mail threading.
10. **MIME-Version :** This field specifies the MIME (Multipurpose Internet Mail Extensions) version used in the e-mail. MIME is a standard for formatting and encoding multimedia content in e-mail messages.
11. **Content-Type :** This field indicates the type of content included in the e-mail (e.g., plain text, HTML, or attachments) and how it should be displayed or processed.
12. **X-Headers :** These are custom or non-standard fields that may be added by e-mail clients or servers for various purposes. They are typically prefixed with "X-."

Que 4.11. Explain how an e-mail can be traced for forensics purpose. Outline the various key steps involved.

Answer

Following are the key steps involved in tracing an e-mail for forensic purposes :

1. **Examine e-mail header :** The e-mail header contains crucial metadata about the e-mail's journey and source. To initiate the tracing process, examine the e-mail header.
2. **Review "received" sections :** Start by analyzing the "received" sections in the e-mail header, which provide a chronological record of the e-mail's path from sender to recipient. The "received" sections are listed from the bottom to the top, reflecting the order of e-mail server hops.

3. **Identify source server :** To determine the source of the e-mail, investigators should work their way up from the bottom of the "received" sections, identifying the originating e-mail server.
4. **Analyze timestamps :** Pay close attention to timestamps within the "received" sections. These timestamps provide valuable information about when the e-mail passed through each e-mail server.
5. **Examine e-mail content :** Analyze the e-mail's content for any details that could lead to the identification of the sender or their intent.
6. **Check server logs :** It is crucial to examine the logs of all e-mail servers in the received chain as soon as possible. Server logs may contain additional information, such as IP addresses, timestamps, and authentication records, which can aid in tracing the e-mail.
7. **Follow IP addresses :** Trace the IP addresses listed in the "received" sections to identify the geographic location and service provider associated with each hop in the e-mail's journey.
8. **Utilize timestamp analysis :** Timestamps are critical for e-mail tracing, especially since logs may get archived. Investigate HTTP and SMTP logs to match timestamps with e-mail server activity, helping to verify the e-mail's authenticity.
9. **Beware of fake headers :** Cybercriminals often use tools to create fake e-mail headers with false "from" e-mail addresses. Be cautious and exercise careful scrutiny when investigating all parts of the e-mail header to identify inconsistencies.
10. **Explore X-headers :** In addition to standard header sections, explore any X-Headers present. These headers may contain information useful for tracing and filtering e-mails.

PART-6

Digital Forensics Life Cycle.

Que 4.12. Write a short note on: digital forensics process.

Answer

1. The digital forensics process is a legal procedure that involves the preparation and presentation of evidence in a legal context.
2. Digital forensics evidence consists of digital exhibits presented by qualified witnesses to help establish facts and legal theories in a case.
3. Expert witnesses bridge the gap between technical issues related to digital evidence and legal theories.

4. In court proceedings, exhibits are introduced as evidence by either party, and testimony is presented to explain the processes involved in identifying, collecting, preserving, analyzing, and interpreting the evidence.
5. It must be established that the evidence is relevant, authentic, and not the result of hearsay.
6. The chain of custody is crucial, and individuals involved in handling the evidence testify about their roles and the processes used.
7. Digital forensics evidence is usually latent and requires specialized tools for examination.
8. Those using these tools must apply their scientific knowledge, skills, and training within defined standards.
9. Challenges to digital forensics evidence can be made by pointing out inaccuracies or omissions in content, context, process, relationships, timing, location, or consistency.
10. The trier of fact evaluates the evidence in conjunction with other evidence to make legal judgments.
11. Forensic experts formulate cost proposals, timelines, deliverables, and risk analyses for the investigation.
12. Flawless data acquisition (imaging) is essential for evidence admissibility, and strict protocols are followed to ensure authenticity and maintain a secure chain of custody.

Que 4.13. What are the various phases involved in the life cycle of a forensics investigation process ? Support your answer through various relevant examples.

Answer

Forensics life cycle involves the following phases :

1. **Preparation and identification of evidence :** In this stage, digital forensics experts prepare for the investigation by understanding the scope of the case and identifying potential sources of digital evidence.

   Example : If a company suspects an employee of data theft, they may prepare by identifying the employee's computer and relevant data sources.
2. **Collection and recording digital evidence :** Digital evidence is collected using forensically sound methods to ensure its integrity. This may involve seizing computers, mobile devices, or servers and making exact copies (forensic images) of their storage media.

   Example : Law enforcement seizes a suspect's computer and uses specialized tools to create a forensic image of the hard drive, preserving the original evidence.

3. **Storing and transporting digital evidence :** Collected evidence must be securely stored and transported to maintain its integrity. Chain of custody procedures are followed to document every transfer or handling of evidence.

   Example : Evidence is stored in tamper-evident bags and transported in sealed containers to a forensics lab.

4. **Examination/investigation digital evidence :** During this phase, experts conduct a detailed examination of the digital evidence. This includes searching for relevant files, examining system logs, and identifying potential areas of interest.

   Example : Investigators search a suspect's computer for files related to a cyber attack, looking for malware or intrusion indicators.

5. **Analysis, interpretation and attribution :** Experts analyze the collected data to draw conclusions. They interpret the evidence to understand what happened and attribute actions to specific individuals or entities.

   Example : Digital forensics experts analyze network traffic logs to attribute a cyber attack to a particular hacking group.

6. **Reporting :** A comprehensive report is prepared to document the findings of the investigation. This report includes details of evidence collection, analysis, interpretation, and attribution. It may also include expert opinions.

   Example : A corporate investigator provides a report to company management detailing the extent of an employee's unauthorized data access.

7. **Testifying :** In legal cases, digital forensics experts may be called upon to testify as expert witnesses in court. They present their findings, explain the methodologies used, and answer questions from attorneys and the court.

   Example : During a criminal trial, a digital forensics expert testifies about the evidence gathered from a suspect's computer and its relevance to the case.

Que 4.14. What are the various activities involved in the life cycle of a forensics investigation process ?

Answer

Forensics life cycle involves the following activities :

A. **Prepare :**

1. **Case briefings :** At the preparation stage, digital forensics experts gather information about the case, including the alleged misconduct, potential evidence sources, and key parties involved.

2. **Engagement terms :** Experts establish clear terms of engagement, outlining the scope of work, responsibilities, and expectations.
3. **Interrogatories :** Legal teams may prepare written questions (interrogatories) for opposing parties to gather information about the case.
4. **Spoliation prevention :** Developing a strategy to prevent data spoliation (intentional destruction of evidence).
5. **Discovery requests :** Legal teams request relevant evidence from opposing parties, including electronically stored information (ESI).

B. **Record :**

1. **Drive imaging :** Creating forensic images of digital storage media ensures a pristine copy of the original data is preserved.
2. **Indexing and profiling :** Creating an index of the acquired data and profiling it to identify key files and locations.
3. **Search plans :** Developing search strategies and criteria to locate relevant evidence efficiently.
4. **Cost estimates :** Providing estimates of the resources, time, and costs required for the investigation.
5. **Risk analysis :** Identifying potential technical and legal risks in handling digital evidence.

C. **Investigate :**

1. **Triage images :** Prioritizing which data to examine first based on relevance and importance to the case.
2. **Data recovery :** Attempting to recover deleted or damaged data to uncover hidden information.
3. **Keyword searches :** Employing specific keywords and search terms to identify relevant data.
4. **Hidden data review :** Examining steganography, encryption, or obfuscation techniques to uncover concealed information.
5. **Communication and iteration :** Collaborating with legal teams and clients, sharing findings, and refining investigative strategies.

D. **Report :**

1. **Oral vs. written :** Preparing reports that can be presented orally in court or submitted as written documents, depending on legal requirements.
2. **Relevant document production :** Compiling and producing relevant documents as evidence in legal proceedings.
3. **Search statistic reports :** Providing statistical reports on search efforts, including search terms used and the number of documents reviewed.

4. **Chain of custody :** Maintaining a detailed chain of custody to document the handling and storage of evidence.
5. **Case log reporting :** Documenting the steps taken during the investigation, including the identification of evidence, procedures followed, and outcomes.

E. **Testify :**

1. **Testimony preparation :** Preparing to testify in court, including reviewing findings, preparing visual aids, and anticipating questions.
2. **Presentation preparation :** Creating clear and compelling presentations to convey complex technical information to the court.
3. **Testimony :** Providing expert testimony in court, explaining findings, methodologies, and their relevance to the case.

Que 4.15. What are the different types of digital analysis that can be performed on the captured forensics evidence ?

Answer

Following are the different types of digital analysis that can be performed on the captured forensics evidence :

1. **Media analysis :** Media analysis involves examining storage media such as hard drives, USB devices, or memory cards. It aims to recover, identify, and analyze data stored on these devices.

   Purpose : To retrieve files, deleted data, and hidden information, which can be crucial in investigations involving data breaches, cybercrimes, or intellectual property theft.

2. **Media management analysis :** Media management analysis focuses on cataloging and organizing digital media, creating forensic images, and securely storing and preserving evidence.

   Purpose : To maintain the integrity and chain of custody of digital evidence, ensuring it is admissible in court.

3. **File system analysis :** File system analysis examines the structure, organization, and metadata of files and directories on storage media. It helps in reconstructing file access history and identifying user actions.

   Purpose : To uncover file manipulation, file deletion, and user interactions with data in cases like fraud investigations or data recovery.

4. **Application analysis :** Application analysis involves studying the behavior and artifacts left behind by specific software applications, including web browsers, email clients, and office suites.

   Purpose : To recover application-specific data such as browsing history, email communications, or document revisions, which can be vital in various investigations.

5. **Network analysis :** Network analysis examines network traffic logs, communication protocols, and network device configurations.

   Purpose : To trace the source of cyber attacks, identify vulnerabilities, and determine the extent of data breaches.

6. **Image analysis :** Image analysis focuses on digital images, including photographs and graphics. It aims to extract metadata, detect image manipulation, and analyze visual content.

   Purpose : To verify the authenticity of images, identify image tampering, and extract geolocation or timestamp information.

7. **Video analysis :** Video analysis involves the examination of digital video files.

   Purpose : To extract relevant information from video footage, identify persons of interest, and establish timelines in cases like surveillance footage analysis.

Que 4.16. What are the typical elements of a digital forensics investigation report ?

Answer

Following are the typical elements of a digital forensics investigation report :

1. **Identity of the reporting agency :** This section includes the agency's name, contact information, and jurisdiction that conducted the digital forensics investigation.
2. **Case identifier or submission number :** A unique alphanumeric code or number assigned to the case for tracking and reference purposes.
3. **Case investigator :** The name and contact information of the investigator responsible for conducting the investigation.
4. **Identity of the submitter :** Information about the entity or individual who submitted the digital evidence for examination.
5. **Date of receipt :** The date on which the submitted digital evidence was received by the forensic examiner or the reporting agency.
6. **Date of report :** The date when the investigation report is finalized and officially issued.
7. **Descriptive list of items submitted for examination :** A detailed inventory of the digital devices and storage media submitted for examination, including information such as serial numbers, makes, models, and a brief description of each item.
8. **Identity and signature of the examiner :** The name and signature of the forensic examiner who conducted the analysis.
9. **Brief description of steps taken during examination :** An overview of the forensic procedures, techniques, and methodologies employed during the examination such as string searches, graphics image searches and recovering erased files.

10. **Results/conclusions :** The main findings, results, and conclusions drawn from the digital forensic analysis.

Que 4.17. What precautions should be taken while collecting electronic evidence ?

Answer

1. Ensuring the evidence is accurately collected and maintaining a clear chain of custody from the crime scene to the investigator and ultimately to the court is one of the most crucial measures.
2. To uphold the integrity of digital evidence, it is necessary to adhere to specific rules.
3. Generally, the following principles apply :
   i. **Principle 1 :** Law enforcement agencies or their representatives must refrain from altering data on a computer or storage media, which may be used as evidence in court.
   ii. **Principle 2 :** In exceptional situations, if someone needs to access original data on a computer or storage media, that individual must be competent to do so and provide an explanation of the relevance and implications of their actions.
   iii. **Principle 3 :** An audit trail or another form of record for all processes applied to computer-based electronic evidence should be generated and preserved. An impartial third party should have the ability to review these processes and achieve the same results.
   iv. **Principle 4 :** The individual overseeing the investigation bears overall responsibility for ensuring compliance with the law and these principles.

PART-7

Chain of Custody Concept.

Que 4.18. Write a short note on: chain of custody concept.

Answer

1. The central concept in cyber forensics or digital forensics investigations is the "chain of custody." This process validates the collection, tracking, and protection of various types of evidence on its journey to a court of law.
2. It's crucial to consistently protect all pieces of evidence so that they remain admissible in court. Professionals in forensic investigations

understand that without a proper chain of custody, the value of the evidence diminishes, so they treat all evidence as if it may be used in litigation.

3. The purpose of the chain of custody is to require the presenter of evidence to prove its authenticity. This means demonstrating that the evidence is indeed what it claims to be and providing information about its origin and handling from acquisition onward.
4. The chain of custody is a chronological written record that identifies the individuals who had custody of the evidence from the moment it was collected until its final disposition.
5. The chain of custody begins when relevant evidence is collected and remains intact until the evidence is properly disposed of. It assumes continuous accountability, and this accountability is crucial because improper maintenance can render the evidence inadmissible in court.

PART-8

Network Forensics.

Que 4.19. Write a short note on: network forensics.

Answer

1. Network forensics is a branch of digital forensics that focuses on the monitoring, analysis, and investigation of network traffic and data to uncover security incidents, cyber attacks, and other network-related crimes.
2. It involves the collection, preservation, and analysis of network data to understand the nature of an event, identify malicious activities, and gather evidence for legal or investigative purposes.
3. Network forensics is a critical component of modern cyber security, helping organizations detect, respond to, and investigate security incidents.
4. It plays a vital role in maintaining the security and integrity of networked systems and is essential for both proactive threat detection and post-incident analysis.
5. Network forensics begins with the collection of network data; including packet captures (PCAPs), log files, and other network traffic records.
6. These data sources provide a detailed record of network activities.
7. Network data is then analyzed to identify anomalous or suspicious activities.

PART-9

Approaching a Computer Forensics Investigation.

Que 4.20. **What are the phases involved in computer forensics investigation ?**

Answer

Following are the phases involved in computer forensics investigation :

1. **Secure the subject system :** The first and most crucial step is to secure the subject system to prevent tampering or unauthorized changes during the investigation. This involves physically isolating the system or taking measures to ensure that no one can access or alter its data.
2. **Take a copy of hard drive/disk :** In many cases, it's essential to create a forensically sound copy of the hard drive/disk. This copy is a bit-for-bit duplicate of the original storage media. It ensures that the original data remains unchanged while investigators work with the copy.
3. **Identify and recover all files :** The investigation involves identifying all files on the storage media, including those that may have been deleted or hidden. Specialized forensic software and techniques are used to recover deleted or obscured files.
4. **Access/view/copy hidden, protected and temp files :** Investigators must access and analyze hidden, protected, and temporary files. These files may contain valuable evidence or information about the user's activities and intentions.
5. **Study "special" areas on the drive :** Special areas on the drive, such as slack space and residual data from previously deleted files, may yield valuable information. These areas are examined to find remnants of data that could be relevant to the investigation.
6. **Investigate application and program data :** The settings and data from applications and programs used on the system are scrutinized. This includes examining web browsers, email clients, and any other software that might contain relevant information.
7. **Consider the system as a whole :** Investigators must view the system from various perspectives, including its structure and overall contents. This includes examining the file system, registry entries, system logs, and any other components that may provide insights into the user's activities.
8. **Consider general factors relating to the user's activity :** Investigators also consider general factors related to the user's computer habits and behavior. This can include user profiles, browsing history, and any patterns of behavior that might be relevant to the investigation.

9. **Create detailed and considered report :** Finally, the investigator compiles all the data and information collected into a detailed and well-documented report. This report typically includes an assessment of the evidence, the methodology used, findings, and conclusions.

Que 4.21. What are the things to be avoided during a computer forensics investigation ? What are the things that cannot be avoided ?

Answer

A. Things to be avoided :

1. **Changing date/time stamps :** It is essential to avoid altering date and time stamps of files, as this can compromise the integrity of the evidence and potentially mislead investigators.
2. **Changing data :** Modifying or tampering with the data itself should be strictly avoided, as it can result in the loss of critical information and render the evidence inadmissible in legal proceedings.
3. **Overwriting unallocated space :** Overwriting unallocated space, which can occur during system reboots, should be prevented, as it may erase valuable remnants of data that could be relevant to the investigation.

B. Things that cannot be avoided :

1. **Engagement contract :** It is imperative to have an engagement contract in place before commencing an investigation. This contract outlines the terms and conditions of the service, defines the scope of work, and establishes the legal framework for the investigation.
2. **Non-Disclosure Agreement (NDA) :** A non-disclosure agreement is essential to protect sensitive information and maintain confidentiality. Both the computer forensics laboratory and the customer must agree to abide by the terms of the NDA to safeguard the integrity of the investigation.
3. **Customer agreement :** Customers of computer forensics laboratories must agree to adhere to the terms and conditions specified for the services provided. This agreement ensures that both parties understand their obligations and responsibilities throughout the investigation.
4. **Legal definitions :** Certain legal terms and definitions, such as "customer," "default," "the company," and "engagement," are crucial to defining the roles and responsibilities of each party involved in the investigation. These definitions help establish a clear understanding of the contractual relationship.

Que 4.22. Which important elements are addressed in a forensics investigation engagement contract ?

Answer

Following important elements are addressed while drawing up a forensics investigation engagement contract :

1. **Authorization :**
   i. Authorization defines the scope and purpose of the forensic investigation.
   ii. It clarifies what specific actions the investigator is authorized to undertake and the objectives of the investigation.
   iii. The contract should specify whether the authorization covers a full investigation, a specific incident, or a defined set of actions.
   iv. This ensures that the investigator knows the boundaries of their work.
2. **Confidentiality :**
   i. Confidentiality provisions are crucial to protect sensitive information and ensure that the investigation remains discreet and secure.
   ii. It safeguards the client's data and the integrity of the process.
   iii. The contract should outline the confidentiality obligations of both parties, including the investigator's responsibility to handle data with care and the client's expectation of privacy.
3. **Payment :**
   i. Payment terms are essential to establish the financial aspects of the engagement.
   ii. They clarify how and when the investigator will be compensated for their services.
   iii. The contract should detail the payment structure, including the fee structure, billing frequency, and any additional costs or expenses that the client may be responsible for.
   iv. It should also specify the payment method and deadlines.
4. **Consent and acknowledgment :**
   i. Consent and acknowledgment clauses ensure that both parties understand and agree to the terms and conditions of the engagement.
   ii. They provide a legal record of the client's consent.
   iii. The contract should include language indicating that the client consents to the forensic investigation and acknowledges that the investigator will follow legal and ethical standards.

5. **Limitation of liability :**
   i. Limitation of liability clauses define the extent of the investigator's responsibility and potential liability for damages or losses that may occur during the investigation.
   ii. The contract should specify the limits of the investigator's liability, such as the maximum amount they may be held accountable for in case of errors, omissions, or breaches of contract.

Que 4.23. Highlight the key steps to be performed in solving a computer forensics case.

Answer

Following are the key steps to be undertaken when solving a computer forensics case :

1. Prepare for the forensic examination.
2. Engage with relevant individuals to gather case details.
3. Verify the case's validity and begin data collection planning.
4. Retrieve data from the target media.
5. Extract data from the investigated computer.
6. Examine email records.
7. Analyze the gathered evidence.
8. Conduct comprehensive analysis.
9. Report your findings to the client.

PART-10

Forensics and Social Networking Sites : The Security / Privacy Threats.

Que 4.24. What is a "social networking" site ? What are the security threats that can emanate from social networking sites ?

Answer

Social networking site :

1. A "social networking" site is an online platform or website that enables individuals to create digital profiles, connect with other users, and engage in various forms of social interaction and communication.
2. These platforms are designed to facilitate the sharing of personal information, thoughts, updates, photos, videos, and other content with a network of friends, acquaintances, or even a broader audience.

3. Examples of well-known social networking sites include Facebook, X, Instagram, LinkedIn, Pinterest, and Snapchat, among many others.

Security threats : Security threats that can emanate from social networking sites are listed below :

1. **Corporate espionage :** Social networking sites can be a source of information leakage for organizations.
2. **Cross-site scripting (XSS) :** XSS attacks occur when attackers inject malicious scripts into web pages. On social networking sites, this can lead to the theft of user data or the spreading of malware.
3. **Viruses and worms :** Viruses and worms can be spread through links, attachments, or malicious apps on social networking sites, potentially infecting users' devices and compromising their security.
4. **Social networking site aggregators :** Aggregator sites can be used to aggregate and exploit user information without their consent, leading to privacy breaches.
5. **Social networking specific phishing :** Phishing attacks target users with deceptive messages. Social networking sites provide attackers with information to personalize these attacks, making them more convincing.
6. **Infiltration of networks :** Attackers can infiltrate social network connections and gain access to sensitive personal data, potentially leading to data breaches.
7. **ID theft :** Personal information shared on social networking sites can be exploited by cybercriminals for identity theft.
8. **Bullying :** Social networks can become platforms for cyberbullying.
9. **Content-based image retrieval (CBIR) :** CBIR techniques can be employed to search for and identify individuals based on their images, potentially invading their privacy and leading to misuse of their photos.
10. **Difficulty of complete account deletion :** Some social networks make it challenging for users to permanently delete their accounts.
11. **Spam :** Social networking sites can be targeted by spammers who flood users' feeds, messages, or notifications with unsolicited content.
12. **Stalking :** Social networking sites can be exploited by stalkers to gather information about their targets.

PART-11

Challenges in Computer Forensics.

Que 4.25. **What are the challenges in computer forensics ?**

Answer

Following are various challenges in computer forensics :

1. **Data volume challenge :** Investigating vast amounts of digital data, including large storage capacities, billions of messages, indexed webpages, and online documents.
2. **Data tampering risk :** Concerns about the potential alteration of digital data, making it difficult to ascertain the authenticity of evidence.
3. **Privacy concerns :** Protecting individuals' privacy amid data mining, intelligent information retrieval, and pattern analysis.
4. **Adaptation to technological advancements :** The need to swiftly adapt to new products and innovations with reliable examination and analysis techniques.
5. **Network forensics challenges :** Challenges related to multi-jurisdictional investigations, trusted timestamps, real-time data analysis, diverse protocols, and network bandwidth.
6. **Examination backlog :** The difficulty of examining all seized computers and addressing the backlog, necessitating data intake and reduction strategies.
7. **Technological obsolescence recognition :** Recognizing the rapid evolution of technology and its impact on investigations to prevent lost leads and ineffective prosecutions.
8. **Real-time data collection complexity :** Addressing legal issues, privileges, and avoiding inadvertent damage claims in real-time data collection efforts.
9. **Digital media alteration risks :** Concerns about data alterations when electronic devices are powered ON or OFF, and potential activation of malware during forensics efforts.

Que 4.26. What are the technical challenges associated with computer forensics ?

Answer

Following are the technical challenges associated with computer forensics :

A. **Complexity challenges :**

1. The "complexity problem" arises because acquired data is often in its rawest, most intricate form, making it challenging for non-technical individuals to interpret.
2. To address the complexity problem, specialized tools are employed.
3. These tools navigate data through one or more "layers of abstraction" until it becomes comprehensible.

4. For instance, to view directory contents from a file system image, tools process file system structures to display the relevant information.
5. These structures serve as layers of abstraction in the data.

B. Quantity challenges :

1. Digital forensics faces the "quantity challenge," characterized by the sheer volume of data to be examined.
2. Analyzing every individual piece of data is inefficient.
3. To address this issue, data reduction methods become necessary.
4. Data reduction entails the consolidation of data into larger events or the exclusion of known data.
5. Data reduction techniques serve as instances of abstraction layers in this context.

Que 4.27. What are the legal challenges associated with computer forensics ?

Answer

Following are the legal challenges associated with computer forensics :

1. **Legal jurisdiction and cross-border issues :** The global nature of the internet often leads to investigations involving multiple jurisdictions. Determining which legal framework applies and obtaining evidence across borders can be challenging.
2. **Data privacy and consent :** Striking a balance between investigating potential wrongdoing and respecting individuals' privacy rights is crucial. Gaining consent to access or analyze digital data, especially in private settings, can be a legal hurdle.
3. **Search and seizure laws :** Computer forensics often involves seizing and searching digital devices. Compliance with search and seizure laws, including obtaining proper warrants and ensuring the legality of evidence collection, is paramount.
4. **Chain of Custody :** Maintaining a clear and unbroken chain of custody for digital evidence is essential for its admissibility in court. Ensuring that evidence has not been tampered with or altered during the investigation is a legal requirement.
5. **Authentication and admissibility of digital evidence :** Proving the authenticity and integrity of digital evidence can be challenging. Legal standards for admitting digital evidence may vary, and forensic experts must adhere to these standards.

6. **Expert witness testimony :** Computer forensics experts may be required to testify in court. The admissibility of their testimony, their qualifications, and their ability to communicate complex technical information to non-expert judges and juries can be challenging.

7. **Volatility of digital evidence :** Digital evidence can be volatile and easily altered. Ensuring that evidence is collected and preserved in a manner that stands up to legal scrutiny is essential.

☺☺☺

5 UNIT

Introduction to Security Policies & Cyber Laws

CONTENTS

PART-1

Need for an Information Security Policy.

Que 5.1. What is an information security policy ? Why is an information security policy important ?

Answer

Information security policy :

1. An information security policy is a formal document that outlines an organization's approach to protecting its information assets.
2. It defines the rules and procedures that employees and other stakeholders must follow to ensure the confidentiality, integrity, and availability of information.

Important of information security policy : An information security policy is important because it helps organizations to :

1. Protect their information assets from unauthorized access, use, disclosure, disruption, modification, or destruction.
2. Comply with applicable laws and regulations.
3. Reduce the risk of financial losses, reputational damage, and other negative consequences of security incidents.
4. Create a culture of security awareness and accountability within the organization.

Que 5.2. What are the benefits of having an information security policy ?

Answer

The benefits of having an information security policy include :

1. Reduced risk of security incidents.
2. Improved compliance with laws and regulations.
3. Reduced financial losses.
4. Protected reputation.
5. Increased customer trust.
6. Improved employee awareness and accountability.

Que 5.3. What are the key components of an information security policy ? How to develop and implement an information security policy ?

Answer

Key components : The key components of an information security policy include :

1. A statement of purpose.
2. A definition of the scope of the policy.
3. A description of the organization's information assets and their classification.
4. A description of the security controls that will be used to protect information assets.
5. A description of the roles and responsibilities of employees and other stakeholders.
6. A description of the process for reporting and responding to security incidents.

Development and implementation : To develop and implement an information security policy, organizations should follow these steps :

1. **Assess your risks :** Identify the information assets that are most critical to your organization and identify the threats and vulnerabilities that could impact those assets.
2. **Develop your policy :** Based on your risk assessment, develop a policy that outlines the rules and procedures that will be used to protect your information assets.
3. **Communicate and train your employees :** Once your policy is developed, communicate it to all employees and provide training on the policy requirements.
4. **Monitor and enforce your policy :** Monitor employee compliance with the policy and take disciplinary action against employees who violate the policy.
5. **Review and update your policy regularly :** Review your policy regularly to ensure that it is up-to-date and effective.

Que 5.4. Why do India need cyber laws ?

Answer

1. Cyber law has been established as a framework to grant legal acknowledgment to all the risks associated with the use of computers and computer networks.
2. Within the scope of cyber law, various aspects are addressed, including intellectual property, data protection, privacy, freedom of expression, and offenses committed through computer usage.

3. India's initial cyber law, the ITA 2000, was enacted by the Indian Parliament with the aim of establishing the legal foundation for electronic commerce in the country.
4. The Indian government recognized the necessity of enacting pertinent cyber laws to regulate computer-related transactions conducted over the Internet within India.
5. It comprehensively manages all facets, issues, legal ramifications, and conflicts within the realm of cyberspace, the Internet, or the World Wide Web.
6. The rationale behind introducing cyber laws in India can be summarized as follows :
   i. Despite India's well-established legal system, covering various past and potential scenarios, there are gaps in addressing newly emerging internet technologies. To bridge this gap, it is imperative to establish suitable laws, given the increasing use of the internet and other computer technologies in India.
   ii. There is a need to legally recognize the significance of the internet, considering it is one of the predominant platforms for conducting business in today's global landscape.
   iii. Alongside the internet's growth, the concept of cyber terrorism emerged, encompassing disruptive activities with the intent to advance social, ideological, religious, political, or similar objectives, or to intimidate individuals for such purposes in the cyber realm. Essentially, it involves the commission of traditional offenses in innovative ways.
7. Taking all these factors into account, the Indian Parliament passed the Information Technology Bill on May 17, 2000, commonly referred to as the ITA 2000.
8. The ITA 2000 addresses cyber laws and establishes the legal framework for electronic records and other activities conducted through electronic means.

PART-2

Introduction to Indian Cyber Law.

Que 5.5. What is Indian cyber law, and what is its primary objective ?

Answer

Indian cyber law : Indian Cyber Law, formally known as the Information Technology Act, 2000 (ITA 2000) along with its amendments, is the primary legal framework governing cyberspace and electronic transactions in India.

Primary objective of Indian cyber law : Its primary objectives are as follows :

1. **Legal recognition :** The ITA 2000 provides legal recognition to electronic documents, digital signatures, and electronic transactions.
2. **Cyber crimes :** The act addresses various cybercrimes such as hacking, identity theft, data breaches, and the spread of malware.
3. **Data protection and privacy :** The ITA 2000 and its amendments include provisions for the protection of sensitive personal data and information. It outlines rules and regulations for the collection, storage, and processing of personal data to safeguard individual privacy.
4. **Digital signatures :** The act recognizes digital signatures as a means of authenticating electronic records and transactions.
5. **Electronic commerce :** The ITA 2000 facilitates electronic commerce by providing legal certainty for online contracts and transactions.
6. **Cyber security :** The act promotes the establishment of computer emergency response teams (CERTs) to handle cyber security incidents and threats. It encourages the development of cyber security practices and standards.
7. **Intermediary liability :** The ITA 2000 defines the liability of intermediaries, such as internet service providers and social media platforms, for content hosted on their platforms.
8. **Cyber terrorism :** The act addresses cyber terrorism by defining offenses related to using computers or communication devices for terrorist activities.
9. **Jurisdiction :** The act outlines the jurisdiction of Indian courts in matters related to cybercrimes and electronic transactions.
10. **Penalties :** The ITA 2000 prescribes penalties and punishments for various cybercrimes, including fines and imprisonment, to deter individuals and entities from engaging in illegal activities in cyberspace.

Que 5.6. How has Indian cyber law evolved over the years to address emerging cyber threats ?

Answer

Here is an overview of how Indian cyber law has evolved :

1. **Information Technology Act, 2000 (ITA 2000) :** This was the initial legislation that laid the foundation for Indian cyber law. It provided legal recognition for electronic transactions, digital signatures, and electronic records. However, as technology rapidly advanced, it became clear that the law needed to be updated to address new challenges.
2. **Amendments in 2008 :** In response to the growing importance of cyber security and the need for enhanced legal provisions, the ITA 2000 underwent significant amendments in 2008. These amendments were

aimed at addressing various aspects of cyber threats, including data protection, cybercrimes, and the role of intermediaries.

3. **Data protection and privacy :** The ITA 2000, as amended in 2008, introduced provisions related to data protection and privacy. It included rules and regulations governing the collection, storage, and processing of sensitive personal data and information.
4. **Cyber crimes :** The 2008 amendments expanded the definition of cybercrimes and introduced new offenses related to unauthorized access, identity theft, and the spread of malware. These changes reflected the evolving nature of cyber threats.
5. **Cyber security :** The amended law promoted the establishment of computer emergency response teams (CERTs) to handle cyber security incidents. It emphasized the importance of cyber security practices and standards.
6. **Intermediary liability :** The amendments clarified the liability of intermediaries, such as internet service providers and social media platforms, for content hosted on their platforms. It introduced provisions for the removal of unlawful content while protecting freedom of expression.
7. **Cyber terrorism :** The ITA 2000, as amended, included provisions to address cyber terrorism by defining offenses related to the use of computers or communication devices for terrorist activities.
8. **Subsequent amendments :** Over the years, the ITA 2000 has undergone further amendments and revisions to address emerging cyber threats and align with international best practices. These amendments have focused on issues such as digital payments, electronic signatures, and the protection of critical information infrastructure.
9. **Cyber security policies :** In addition to legislative changes, India has also developed cyber security policies and strategies to enhance its ability to respond to cyber threats effectively. These policies aim to strengthen the country's cyber security infrastructure and promote cyber security awareness and best practices.

Que 5.7. Explain the legal framework that governs cyber activities in India.

Answer

1. The legal framework that governs cyber activities in India is primarily based on the Information Technology Act, 2000 (IT Act).
2. The IT Act is a comprehensive law that covers a wide range of issues related to electronic commerce, digital signatures, and cyber security.
3. Some of the key provisions of the IT Act that are relevant to cyber activities include :

i. **Section 43 :** This section defines various cyber offences, such as hacking, data theft, and denial-of-service attacks.

ii. **Section 66F :** This section defines cyber terrorism and provides for punishment of up to life imprisonment for this offence.

iii. **Section 72A :** This section empowers the government to block websites and other online content that is found to be obscene, defamatory, or harmful to children.

iv. **Section 79 :** This section provides for compensation to victims of cyber crimes.

4. In addition to the IT Act, there are a number of other laws and regulations that govern cyber activities in India, such as :

i. **The Indian Penal Code, 1860 :** This code contains a number of provisions that are relevant to cyber crimes, such as those related to theft, fraud, and forgery.

ii. **The Evidence Act, 1872 :** This act contains provisions on the admissibility of electronic evidence in court.

iii. **The Copyright Act, 1957 :** This act protects copyright in original literary, dramatic, musical, and artistic works, including those in digital format.

iv. **The Trade Marks Act, 1999 :** This act protects trademarks registered in India, including those used in connection with online goods and services.

5. The Indian government has also established a number of institutions to deal with cyber crime and cyber security. These include :

i. **The Indian Computer Emergency Response Team (CERT-In) :** CERT-In is the nodal agency for cyber security in India. It is responsible for responding to cyber incidents, coordinating with law enforcement agencies, and issuing security advisories.

ii. **The Cyber Appellate Tribunal (CAT) :** The CAT is a tribunal that hears appeals against orders passed by CERT-In and other authorities under the IT Act.

iii. **The National Cyber Security Coordinator (NCSC) :** The NCSC is the apex body for cyber security in India. It is responsible for coordinating the efforts of various government agencies and stakeholders to protect India from cyber threats.

Que 5.8. What are the rights and obligations of individuals and organizations under Indian cyber law ?

Answer

A. **Rights of individuals :** Individuals have a number of rights under Indian cyber law, including the right to :

1. **Privacy :** Individuals have the right to protect their personal information from unauthorized access, use, or disclosure.
2. **Access to information :** Individuals have the right to access information that is held by the government or other organizations about them.
3. **Free speech :** Individuals have the right to express their views and opinions freely online, subject to certain restrictions.
4. **Compensation :** Individuals who are victims of cyber crimes have the right to compensation from the perpetrator of the crime.

B. **Obligations of individuals :** Individuals also have a number of obligations under Indian cyber law, including the obligation to :

1. **Not engage in cyber crimes :** Individuals must not engage in any cyber crimes, such as hacking, data theft, or cyber terrorism.
2. **Respect the privacy of others :** Individuals must not violate the privacy of others by accessing their personal information without their consent.
3. **Not post defamatory or obscene content online :** Individuals must not post any content online that is defamatory, obscene, or harmful to children.

C. **Rights of organizations :** Organizations have a number of rights under Indian cyber law, including the right to :

1. **Protect their intellectual property :** Organizations have the right to protect their intellectual property rights, such as copyright and trademark, from infringement online.
2. **Protect their business data :** Organizations have the right to protect their business data from unauthorized access, use, or disclosure.
3. **Take action against cyber criminals :** Organizations have the right to take legal action against cyber criminals who damage their business or reputation.

D. **Obligations of organizations :** Organizations also have a number of obligations under Indian cyber law, including the obligation to :

1. **Implement reasonable security measures :** Organizations must implement reasonable security measures to protect their information assets from cyber threats.
2. **Report cyber incidents to CERT-In :** Organizations must report certain cyber incidents to the Indian Computer Emergency Response Team (CERT-In) within a certain period of time.
3. **Comply with other applicable laws and regulations :** Organizations must comply with other applicable laws and regulations related to cyber security and privacy.

Que 5.9. What are the latest developments in Indian cyber law ?

Answer

The latest developments in Indian cyber law include :

1. **The Digital Personal Data Protection Act, 2023 :** This Act, which was passed in December 2022, is India's first comprehensive law on data protection. The Act establishes a number of rights and obligations for individuals and organizations in relation to the collection, use, and disclosure of personal data.
2. **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 :** These Rules, which were notified in February 2021, impose a number of new obligations on intermediaries, such as social media platforms and search engines. The Rules include requirements for intermediaries to take down illegal content, to provide information to law enforcement agencies, and to appoint grievance officers.
3. **The Indian Cyber Crime Coordination Centre (IC3) :** The IC3 was established in February 2021 to improve coordination between law enforcement agencies in the investigation and prosecution of cyber crimes. The IC3 also provides a platform for victims of cyber crimes to report their complaints.
4. **The National Cyber Security Strategy, 2020 :** This strategy, which was released in October 2020, outlines the government's approach to cyber security for the next five years. The strategy focuses on a number of areas, including capacity building, awareness and education, and international cooperation.

PART-3

Objective and Scope of the Digital Personal Data Protection Act, 2023.

Que 5.10. What is Digital Personal Data Protection (DPDP) Act, 2023 ? What are its main objectives ?

Answer

1. The Digital Personal Data Protection (DPDP) Act, 2023 is a law of the Parliament of India to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.
2. The Act applies to the processing of digital personal data by organizations within the territory of India, as well as to the processing of digital personal data outside of India if it involves providing goods or services to individuals within the territory of India.

3. The Act defines "digital personal data" as any data about an individual who can be identified, directly or indirectly, in that particular form or in combination with other information.
4. Examples of digital personal data include name, address, date of birth, email address, phone number, IP address, location data, and financial data.
5. The DPDP Act is a significant development in Indian law and is expected to have a major impact on the way that organizations collect, use, and disclose personal data.

Main objectives : The main objectives of the DPDP Act are to :

1. Protect the right of individuals to privacy and to protect their personal data from unauthorized access, use, disclosure, modification, or destruction.
2. Promote responsible data processing practices by organizations.
3. Establish a framework for the governance of digital personal data in India.

Que 5.11. What are the rights given to individuals by DPDP Act ? Also mention the obligations imposed on organizations by DPDP Act.

OR

What are the implications of the Digital Personal Data Protection Act 2023 for businesses and individuals ?

Answer

A. Rights given to individuals : The DPDP Act establishes a number of rights for individuals, including the right to :

1. Access their personal data.
2. Correct their personal data.
3. Erase their personal data.
4. Object to the processing of their personal data.
5. Port their personal data.

B. Obligations imposed on organizations : The DPDP Act also imposes a number of obligations on organizations, including the obligation to :

1. Obtain consent from individuals before processing their personal data.
2. Implement reasonable security measures to protect personal data.
3. Notify individuals of data breaches.
4. Respond to individual requests regarding their personal data.

Que 5.12. What is the scope of the Digital Personal Data Protection Act, 2023 ?

Answer

1. The scope of the Digital Personal Data Protection Act, 2023 is broad, encompassing the processing of digital personal data within India or related to Indian goods and services.
2. The DPDP Act defines "digital personal data" as any data about an individual who can be identified, directly or indirectly, in that particular form or in combination with other information.
3. The DPDP Act applies to the processing of digital personal data by organizations within the territory of India, as well as to the processing of digital personal data outside of India if it involves providing goods or services to individuals within the territory of India.
4. The DPDP Act covers a wide range of data processing activities, including collection, storage, use, disclosure, transfer, and disposal of digital personal data.
5. The DPDP Act also applies to the processing of digital personal data by government agencies, but it provides certain exemptions for government processing in the interest of national security, public order, and prevention of offences.
6. Overall, the DPDP Act has a broad scope and covers a wide range of data processing activities, both in the public and private sectors.

PART-4

Intellectual Property Issues.

Que 5.13. What is intellectual property (IP) ? What are the different types of intellectual property ?

Answer

Intellectual property : Intellectual property is a category of property that includes intangible creations of the human intellect.

Types of intellectual property : There are many types of intellectual property, and some countries recognize more than others. The best-known types are :

1. **Patents :** Patents protect inventions for a limited period of time, typically 20 years from the date of filing. Inventions can include new products, processes, or machines.
2. **Copyrights :** Copyrights protect original works of authorship, such as books, movies, music, and software. Copyright protection lasts for the life of the author plus 70 years.

3. **Trademarks :** Trademarks protect words, symbols, and designs that are used to identify the source of goods or services. Trademarks can be registered for renewable periods of 10 years.
4. **Trade secrets :** Trade secrets are confidential information that gives a business an advantage over its competitors. Trade secrets can include formulas, recipes, and manufacturing processes.

Que 5.14. What are intellectual property (IP) issues, and why are they important in the digital era ?

Answer

Intellectual property (IP) issues :

1. Intellectual property (IP) issues refer to legal and ethical challenges related to the protection and management of intellectual property rights.
2. Intellectual property encompasses intangible creations of the human mind, such as inventions, artistic works, literary works, designs, symbols, names, and trade secrets.
3. These creations can be protected by various forms of IP rights, including patents, copyrights, trademarks, and trade secrets.

Importance of IP in the digital era : IP issues are important in the digital era because the digital environment has made it easier than ever to create, copy, and distribute IP. This has led to an increase in IP infringement and other IP disputes. Here are some specific examples of IP issues in the digital era :

1. **Copyright infringement :** Copyright infringement is the unauthorized copying or distribution of copyrighted material. Copyright infringement can occur online when people download pirated music, movies, or software, or when they share copyrighted material without permission.
2. **Trademark infringement :** Trademark infringement is the unauthorized use of a trademark in a way that is likely to cause confusion among consumers. Trademark infringement can occur online when people use trademarks in their domain names, website content, or online advertising without permission.
3. **Trade secret theft :** Trade secret theft is the unauthorized acquisition or use of a trade secret. Trade secret theft can occur online when people hack into computer systems to steal confidential information, or when they download trade secrets from the internet.

Que 5.15. Provide examples of common IP issues that individuals or organizations may face.

Answer

Following are some examples of common IP issues that individuals or organizations may face :

1. **Copyright infringement :** This can include unauthorized copying or distribution of copyrighted material, such as books, movies, music, and software.
2. **Trademark infringement :** This can include unauthorized use of a trademark in a way that is likely to cause confusion among consumers. For example, using a competitor's trademark in your own advertising or product packaging.
3. **Trade secret theft :** This can include unauthorized acquisition or use of a trade secret, such as a formula, recipe, or manufacturing process.
4. **Patent infringement :** This can include making, using, or selling a product or process that is protected by a patent.
5. **Counterfeiting :** This can include manufacturing or selling goods that are designed to look like or be passed off as the genuine product of another company.
6. **Plagiarism :** This can include copying someone else's work and passing it off as your own.

Que 5.16. How can businesses and individuals protect their intellectual property rights in the digital domain ?

Answer

A. For businesses :

1. **Registering their IP rights :** Registering IP rights, such as trademarks and copyrights, can help to deter infringement and make it easier to enforce IP rights in the event of an infringement.
2. **Develop a comprehensive IP policy :** This policy should outline how the business will create, protect, and use its IP assets.
3. **Using technical measures :** Businesses can use technical measures, such as encryption and digital watermarking, to protect their IP from unauthorized access and use.
4. **Educating employees and customers :** Businesses can educate their employees and customers about IP rights and the importance of respecting those rights.
5. **Monitoring online activity :** Businesses can monitor online activity for signs of IP infringement.
6. **Taking legal action :** If IP infringement is discovered, businesses can take legal action to enforce their IP rights.

B. For individuals :

1. **Understand IP laws :** Educate yourself about IP laws and how they apply to your digital activities, especially if you create content, software, or inventions.

2. **Respect copyright and licensing :** Always respect copyright laws when using digital content. Obtain proper permissions or licenses for copyrighted material.
3. **Protect personal data :** Be mindful of the personal data you share online. Understand privacy policies and control who has access to your data.
4. **Use strong passwords :** Protect your online accounts and digital assets with strong, unique passwords.
5. **Report infringements :** If you encounter IP infringements online, such as piracy or plagiarism, report them to the relevant authorities or copyright holders.
6. **Consult legal advice :** If you have questions about IP rights or believe your rights have been violated, seek legal advice from an attorney experienced in IP law.

PART-5

Overview of Intellectual Property Related Legislation in India.

Que 5.17. What are the key intellectual property-related legislations in India ?

Answer

The key intellectual property-related legislations in India are :

1. **The Patents Act, 1970 :** This law governs patents in India, defining the rights and procedures for inventors to protect their inventions for a specific duration.
2. **The Copyright Act, 1957 :** It deals with copyright protection for literary, artistic, musical, and other creative works. The Act also addresses issues related to performers rights and the protection of cinematographic films.
3. **The Trademarks Act, 1999 :** This Act governs the registration and protection of trademarks in India. It defines what can be registered as a trademark and outlines the rights of trademark owners.
4. **The Designs Act, 2000 :** This law governs the registration and protection of industrial designs in India, ensuring the exclusive right to use the design for a specified period.
5. **The Geographical Indications of Goods (Registration and Protection) Act, 1999 :** It provides protection to geographical indications, ensuring that products associated with specific regions maintain their unique identity and quality.
6. **The Semiconductor Integrated Circuits Layout-Design Act, 2000 :** This Act protects the layout designs of integrated circuits and provides exclusive rights to creators of such designs.

7. **The Plant Varieties Protection and Farmers' Rights Act, 2001 :** This legislation governs the protection of plant varieties and the rights of plant breeders and farmers.
8. **The Information Technology Act, 2000 :** While primarily focused on electronic transactions and cybercrimes, this Act also addresses issues related to electronic records and digital signatures, which are crucial in the digital domain.

PART-6

Patent, Copyright, Trademarks.

Que 5.18. What is a patent ? What are the requirements for obtaining a patent ?

Answer

Patent :

1. A patent is a legal document that grants the inventor exclusive rights to make, use, and sell an invention for a certain period.
2. It is a form of intellectual property protection designed to encourage innovation.
3. It provides inventors a limited monopoly on their inventions in exchange for disclosing the details of their inventions to the public.
4. The invention may be a product or a process that is new, useful, and non-obvious.

Requirements for obtaining a patent : To obtain a patent, an invention must meet certain requirements, which can vary slightly from one country to another but generally include the following key criteria :

1. **Novelty :** The invention must be new and not previously disclosed or known to the public before the patent application's filing date.
2. **Non-obviousness :** The invention must not be obvious to someone skilled in the relevant field of technology.
3. **Usefulness or utility :** The invention must have a practical, useful application. It should serve a functional purpose or provide some tangible benefit.
4. **Subject matter eligibility :** The invention must be of a type that is eligible for patent protection. In general, patents can cover processes, machines, manufactures, compositions of matter, or new and useful improvements to any of these categories.
5. **Adequate disclosure :** The patent application must provide a clear and complete description of the invention, enabling someone skilled in the field to understand and replicate it.

6. **Claim specificity :** The patent application should include one or more claims that define the precise scope of the invention.

Que 5.19. What are the rights of a patent holder ?

Answer

Following are the various rights of a patent holder :

1. **Exclusive use :** The primary right of a patent holder is the exclusive right to make, use, and sell the patented invention.
2. **Monopoly :** A patent provides the patent holder with a temporary monopoly over the patented invention, allowing them to control its commercialization and derive financial benefits from it.
3. **Legal enforcement :** The patent holder has the legal right to enforce their patent rights by taking legal action against individuals or entities that infringe on their patent.
4. **Licensing :** A patent holder can grant licenses to others, giving them permission to use the patented invention in exchange for royalties.
5. **Transferability :** Patent holders can sell their patents to others or use them as collateral for loans or investments.
6. **Exclusivity in specific territory :** A patent holder's exclusive rights apply within the jurisdiction of the patent-granting country or region.
7. **Right to prevent others :** Patent holders have the right to prevent others from making, using, selling, or importing the patented invention, even if the infringing party is unaware of the patent.
8. **Right to sue for damages :** In cases of patent infringement, the patent holder can seek damages, which may include compensation for financial losses incurred due to the infringement.

Que 5.20. How can individuals or businesses apply for and protect their patents ?

Answer

Here's a general overview of the process :

1. **Determine patent eligibility :** Determine whether your invention is eligible for a patent under Indian law. Ensure that it meets the criteria of novelty, non-obviousness, utility, and industrial applicability.
2. **Conduct a patent search :** Conduct a thorough search to check if your invention has been patented before. This step helps in assessing the novelty of your invention and can save time and resources.
3. **Prepare a detailed description :** Prepare a comprehensive description of your invention, including drawings or diagrams if applicable.

4. **Draft patent claims :** Draft claims that define the scope of protection you are seeking. Claims should be precise and specific in describing the essential elements of your invention.
5. **Choose the right type of patent :** Decide whether to apply for a provisional patent or a complete patent.
6. **File a patent application :** File a patent application with the Indian Patent Office. You can do this online through the official website or by submitting a physical application.
7. **Pay application fees :** Pay the required application fees, which can vary based on factors such as the type of applicant (individual, small entity, or large entity) and the number of claims.
8. **Examination and publication :** After filing, the patent application undergoes examination by the Indian Patent Office. The application is published after 18 months from the filing date or the priority date, whichever is earlier.
9. **Respond to office actions :** Address any objections or requests for clarification issued by the patent examiner during the examination process.
10. **Grant of Patent :** If the patent application meets all requirements and the examiner is satisfied, a patent is granted, and the patentee is issued a patent certificate.

Que 5.21. What is copyright ? What are the requirements for obtaining copyright ?

Answer

Copyright :

1. Copyright is a legal protection granted to the creators of original literary, artistic, musical, and other creative works.
2. It gives creators the exclusive right to reproduce, distribute, perform, and display their works for a specified duration.
3. Copyright is designed to encourage creativity and enable creators to control the use and distribution of their works.

Requirements for obtaining copyright : To obtain copyright protection following requirements must be met :

1. **Original work :** It means that work should be the result of the author's creative effort and not a direct copy of someone else's work.
2. **Work must be fixed :** The work must be fixed in a tangible medium, meaning it must be in a form that can be perceived, reproduced, or communicated.
3. **Authorship :** The author is the person who creates the work, and copyright is automatically granted upon the creation of the work.

4. **Duration :** Copyright protection lasts for the lifetime of the author plus an additional 60 years.

Que 5.22. What are the rights of a copyright holder ?

Answer

The specific rights of a copyright holder include :

1. **Reproduction right :** The right to make copies of the work, whether in print, digital, or any other format. This includes the right to create duplicates, print editions, or digital copies.
2. **Distribution right :** The right to distribute copies of the work to the public through various means, such as sale, rental, lease, or lending.
3. **Public performance right :** The right to publicly perform the work, which applies to live performances, plays, concerts, and other public presentations of the work.
4. **Public display right :** The right to publicly display the work, including exhibiting artwork, showcasing sculptures, or presenting visual materials in a public setting.
5. **Derivative work right :** The right to create derivative works based on the original, such as adaptations, translations, remixes, or modifications.
6. **Digital and online rights :** The right to control the distribution of digital copies, online streaming, or digital downloads of the work.
7. **Exclusivity :** Copyright holders have the exclusive right to exercise these rights, preventing others from using, reproducing, or distributing the work without permission.
8. **Duration :** In many countries, copyright protection lasts for the lifetime of the author plus an additional 50 to 70 years.
9. **Transferability and licensing :** Copyright holders have the option to transfer or license their rights to others.
10. **Enforcement :** Copyright holders have the legal right to enforce their exclusive rights through legal action.

Que 5.23. How can individuals or businesses apply for and protect their copyright ?

Answer

Individuals and businesses in India can apply for and protect their copyright by following these general steps :

1. **Creation of the original work :** Create an original literary, artistic, or creative work. copyright protection is automatically granted upon the creation of the work.

2. **Documentation and fixation :** Document and fix the work in a tangible medium, i.e., the work should be recorded, written down, or saved in a form that can be perceived, reproduced, or communicated.
3. **Copyright notice :** It is advisable to include a copyright notice on the work. A typical copyright notice includes the copyright symbol (©), the year of first publication, and the name of the copyright owner.
4. **Registration (optional) :** While copyright protection is automatic upon creation, individuals or businesses can choose to register their copyright with the Copyright Office in India.
5. **Record keeping :** Maintain detailed records of the work, including drafts, revisions, and any correspondence related to its creation.
6. **Licensing and permissions :** If you wish to grant others the right to use your copyrighted work, consider drafting licensing agreements that specify the terms and conditions of use.
7. **Enforcement :** If someone infringes on your copyright by using your work without permission, you have the legal right to enforce your copyright.

Que 5.24. What is a trademark ? What are the requirements for registering a trademark ?

Answer

Trademark :

1. A trademark is a distinctive sign or symbol, such as a word, phrase, logo, symbol, design, or combination thereof, that is used to identify and distinguish goods or services offered by one party from those of others.
2. Trademarks are valuable assets for businesses and play a crucial role in branding, consumer recognition, and protection against unfair competition.

Requirements for registering a trademark : The requirements for registering a trademark include :

1. **Distinctiveness :** To be eligible for trademark registration, the proposed trademark must be distinctive and capable of distinguishing the goods or services of one entity from those of others.
2. **Non-descriptiveness :** The trademark must not be directly descriptive of the goods or services it represents.
3. **Non-deceptiveness :** The trademark must not be deceptive or likely to deceive the public regarding the nature, quality, or geographical origin of the goods or services.
4. **Not similar or confusing :** The proposed trademark should not be similar or confusingly similar to existing trademarks in the same or related class of goods or services.

5. **Not offensive :** Trademarks that are offensive, scandalous, or immoral may be refused registration.
6. **Not prohibited by law :** The trademark should not be prohibited by any law in India, including being contrary to public policy or morality.
7. **Proper representation :** The trademark must be represented graphically in a clear and specific manner.

Que 5.25. What are the rights of a trademark holder ?

Answer

The specific rights of a trademark holder include :

1. **Exclusive use :** The primary right of a trademark holder is the exclusive right to use the registered trademark in connection with the specified goods or services for which it is registered.
2. **Prevent others from using similar marks :** Trademark owners have the right to prevent others from using trademarks that are identical or similar enough to their own trademark.
3. **Protection against infringement :** Trademark holders can take legal action against individuals or entities that infringe on their trademark rights.
4. **Exclusive right to license :** Trademark owners have the authority to grant licenses to others, allowing them to use the trademark for specific purposes and under certain conditions.
5. **Protection against dilution :** Trademark holders can protect their trademark against dilution, which occurs when the distinctiveness and uniqueness of the trademark are impaired by the unauthorized use of a similar mark, even if there is no likelihood of confusion.
6. **Enforcement :** Trademark holders have the legal right to enforce their trademark rights through legal means.
7. **Use as collateral :** Trademarks can be used as collateral for loans or financial transactions.

Que 5.26. How can individuals or businesses apply for and protect their trademark ?

Answer

Individuals or businesses can apply for and protect their trademark in India by following these general steps :

1. **Trademark search :** Conduct a comprehensive trademark search to ensure that the proposed trademark is unique and does not conflict with existing trademarks.
2. **Identify the appropriate class(es) :** Determine the class or classes of goods or services for which you intend to use the trademark.

3. **Create the trademark :** Design and create your trademark.
4. **Draft the trademark application :** Prepare the trademark application.
5. **Specify goods or services :** Clearly specify the goods or services associated with your trademark.
6. **Pay the application fee :** Pay the prescribed filing fee, which varies based on factors such as the type of applicant and the number of classes of goods or services.
7. **Trademark examination :** The trademark application undergoes examination by the Trade Marks Registry.
8. **Publication and opposition :** If the trademark application passes examination, it is published in the Trade Marks Journal. This publication opens a window for third parties to oppose the registration if they believe it conflicts with their rights.
9. **Registration :** If no opposition is successful or if any opposition issues are resolved in your favor, the trademark is registered.

Que 5.27. Explain the fundamental differences between patents, copyrights, and trademarks.

Answer

S. No.	Aspect	Patents	Copyrights	Trademarks
1.	Purpose	Protects inventions and innovations.	Protects original creative works.	Protects brand names, logos, symbols.
2.	Type of protection	Inventions, processes, products.	Literary, artistic, musical.	Symbols, names, logos, slogans.
3.	Subject matter	Novel and useful ideas.	Original creative expressions.	Distinctive signs for goods/ services.
4.	Duration	Typically 20 years from filing.	Generally life of the author + 60.	Indefinitely renewable.
5.	Registration required	Yes	No	Yes

☺☺☺

1 UNIT

Introduction to Cyber Crime (2 Marks Questions)

1.1. What is cyber crime ?

Ans. Cyber crime is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.

1.2. Discuss types of attacks prevalent in cyber crime.

Ans. Types of attacks prevalent in cyber crime :

1. Techno-crime
2. Techno-vandalism

1.3. What do you mean by information security ?

Ans. Information security is the practice of protecting information by mitigating information risks. Information security aims to safeguard information from unauthorized access, disclosure, alteration, and destruction.

1.4. Who are cybercriminals ?

Ans. Cybercriminals are individuals or groups who engage in illegal activities in the digital realm, using technology and the internet to commit various forms of cybercrime.

1.5. What are the types of cybercriminals ?

Ans. Following are different types of cybercriminals :

1. **Type I :** Cybercriminals – Hungry for Recognition.
2. **Type II :** Cybercriminals – Not Interested in Recognition.
3. **Type III :** Cybercriminals – The Insiders.

1.6. What are the different categories or types of cyber crimes ?

Ans. Following are the different categories or types of cyber crimes :

1. Cybercrime against individuals (persons).
2. Cybercrime against assets (property).
3. Cybercrime against organizations (government, business and social).
4. Cybercrime against society.

1.7. What are various cybercrime conducted against individuals (persons) ?

Ans. Following are various cybercrime conducted against individuals (persons) :

1. E-Mail spoofing
2. Online frauds
3. Phishing
4. Spamming
5. Cyberstalking and harassment

1.8. What are various cybercrime conducted against assets (property) ?

Ans. Following are various cybercrime conducted against assets (property) :

1. Credit card frauds
2. Intellectual Property crimes
3. Internet time theft

1.9. What are various cybercrime conducted against organizations (government, business and social) ?

Ans. Following are various cybercrime conducted against organizations (government, business and social) :

1. Unauthorized accessing of computers
2. Password sniffing
3. Denial-of-Service (DoS) attacks
4. Virus attacks

1.10. What are various cybercrime conducted against society ?

Ans. Following are various cybercrime conducted against society :

1. Forgery
2. Cyberterrorism
3. Web jacking

1.11. What is the impact of cyber crimes on individuals ?

Ans. Following is the impact of cybercrimes on individuals :

1. Financial losses
2. Privacy invasion
3. Identity theft
4. Emotional distress

1.12. What is the impact of cyber crimes on property ?

Ans. Following is the impact of cybercrimes on property :

1. Data breaches
2. Ransomware
3. Disruption of services

1.13. What is the impact of cyber crimes on government ?

Ans. Following is the impact of cybercrimes on government :

1. National security threats
2. Economic impact
3. Data breaches
4. Intellectual property theft

1.14. Discuss the survival mantra for the netizens for online security.

Ans. The 5P netizen mantra is the survival mantra for online security :

A. **Precaution :** It involves being cautious and aware of potential risks and threats when using the internet.

B. **Prevention :** It entails taking proactive measures to reduce the likelihood of falling victim to online threats.

C. **Protection :** Protection involves implementing security measures to safeguard personal data and online accounts.

D. **Preservation :** Preservation emphasizes the importance of preserving digital assets and records securely.

E. **Perseverance :** Perseverance represents the ongoing commitment to maintaining online security.

1.15. What do you understand by cyber offenses ?

Ans. Cyber offenses, also known as cyber crimes, are criminal activities committed in the digital realm using computer networks, the internet, or other forms of technology.

1.16. Explain the terms hackers, crackers and phreakers.

Ans.

1. **Hackers :** Hackers are individuals with advanced computer skills and knowledge who use their expertise to explore and manipulate computer systems, software, and networks.
2. **Crackers :** Crackers are individuals who engage in malicious or illegal activities, primarily focused on circumventing software protections (e.g., cracking software licenses or encryption) to gain unauthorized access or manipulate software for personal gain.
3. **Phreakers :** Phreakers, short for "phone phreaks," are individuals who manipulate or explore the telecommunication systems, often with a focus on gaining free access to phone services or exploring the inner workings of the telephone network.

1.17. Explain how cybercriminals plan the attacks ?

Ans. The following phases are involved in planning cyber crime :

1. Reconnaissance (Information Gathering).
2. Scanning and scrutinizing.
3. Launching an attack (Gaining and maintaining system access).

1.18. Explain the term "Social Engineering".

Ans. "Social engineering" refers to a set of manipulative techniques that cybercriminals use to exploit human psychology and deceive individuals into divulging confidential information.

1.19. Give classification of social engineering.

Ans. Social engineering is classified as follow :

1. Human-based social engineering.
2. Computer-based social engineering.

1.20. What are the ways of getting desired information using human-based social engineering ?

Ans. Following are some of the ways of getting desired information :

1. Impersonating an employee or valid user.
2. Posing as an important user.
3. Using a third person.
4. Shoulder surfing.
5. Dumpster diving.

1.21. What are the ways of getting desired information using computer-based social engineering ?

Ans. Following are some of the ways of getting desired information :

1. Sending fake e-mails.
2. Enclosing malicious e-mail attachments.
3. Generating fake pop-up windows.

1.22. What do you understand by cyber stalking ?

Ans. Cyber stalking refers to the act of using digital communication tools and online platforms to harass, intimidate, or threaten an individual or group of individuals repeatedly and persistently.

1.23. Give key characteristics of cyber stalking.

Ans. Key characteristics of cyber stalking include :

1. Repetitive behavior.
2. Unwanted contact.
3. Anonymity.
4. Monitoring.
5. Threats and harassment.
6. Manipulation.

1.24. Mention the types of cyber stalkers.

Ans. There are primarily two types of cyber stalkers :

1. **Online stalkers :** Online stalkers are individuals who engage in cyberstalking primarily through digital means and within the virtual realm. They use the internet and various online platforms to harass, intimidate, or threaten their victims.
2. **Offline stalkers :** Offline stalkers, on the other hand, are individuals who initially establish their obsession or harassment in

the physical world but may use online tools or information to further their stalking activities.

1.25. What do you mean by cybercafe ?

Ans. A cybercafe is a physical establishment or business where customers can access computers, the internet, and various online services for a fee. These cafes typically provide public access to computers and the internet to individuals for a specified period.

1.26. What are the measure an individual should take while using the computer in a cybercafe ?

Ans. Following are a few tips for safety and security while using the computer in a cybercafe :

1. Always logout.
2. Stay with the computer, avoid leaving it unattended.
3. Clear history and temporary files.
4. Be aware of your surroundings and the people near you.
5. Avoid online financial transactions.
6. Pay attention to security warnings.

1.27. What are Botnets ?

Ans. Botnets are networks of compromised computers (bots) that are remotely controlled by a cybercriminal or a group of cybercriminals known as "bot herders" or "botmasters." These compromised computers are typically infected with malicious software or malware, allowing the attacker to gain control over them.

1.28. What do you mean by "attack vector" ?

Ans. An attack vector is a path or a means by which a cyber attack can be carried out against a computer system, network, or organization. It represents the specific method or avenue that a malicious actor or hacker can use to exploit vulnerabilities and compromise the security of a target.

☺☺☺

2 UNIT

Cyber Crime (2 Marks Questions)

2.1. What are different types of mobile computers have been introduced in the market ?

Ans. Many types of mobile computers have been introduced since 1990s. They are as follows :

1. Portable Computer
2. Tablet PC
3. Internet Tablet
4. Personal Digital Assistant (PDA)
5. Ultramobile PC (UMPC)
6. Smartphone

2.2. What are different mobility types ?

Ans. Following are different mobility types :

1. **User mobility :** User mobility refers to the ability of individuals to move physically while maintaining network connectivity and access to services.
2. **Device mobility :** Device mobility refers to the ability of devices to move between different access points or networks while maintaining uninterrupted connectivity.
3. **Session mobility :** Session mobility refers to the capability to transfer an ongoing network session from one device or network to another without interruption.
4. **Service mobility :** Service mobility involves the ability to access the same services or applications from different devices or locations.

2.3. What are the popular types of attacks against 3G mobile networks :

Ans. Popular types of attacks against 3G mobile networks are as follows :

1. Malwares, viruses and worms
2. Denial-of-Service (DoS)
3. Overbilling attack
4. Spoofed Policy Development Process (PDP)
5. Signaling-level attacks

2.4. What do you mean by credit card frauds in context of mobile and wireless computing ?

Ans. In the context of mobile and wireless computing, credit card fraud refers to fraudulent activities that involve the unauthorized use of credit card information in mobile or wireless transactions.

2.5. What are different types and techniques of credit card frauds ?

Ans. Following are different types and techniques of credit card frauds :

1. **Traditional techniques :**
   i. ID theft
   ii. Financial fraud
2. **Modern techniques :**
   i. Triangulation
   ii. Credit card generators

2.6. What are the security challenges posed by mobile devices to cybersecurity ?

Ans. Mobility brings two main challenges to cybersecurity :

1. On the hand-held devices, information is being taken outside the physically controlled environment.
2. Remote access back to the protected environment is being granted.

2.7. What are the technical challenges associated with mobile security ?

Ans. Some well-known technical challenges in mobile security are :

1. Managing the registry settings and configurations.
2. Managing the authentication service security.
3. Cryptography security.
4. Lightweight Directory Access Protocol (LDAP) security.
5. Remote Access Server (RAS) security.
6. Media player control security.
7. Networking application program interface (API) security.

2.8. What do you understand by authentication services security ?

Ans. Authentication services security refers to the measures and practices put in place to ensure that users and devices attempting to access a network, application, or service are legitimate and authorized.

2.9. Discuss the types of attacks to which mobile devices are subjected to.

Ans. Mobile devices are subject to following types of attacks :

1. Push attacks
2. Pull attacks
3. Crash attacks

2.10. Describe the various types of attacks against mobile/cell phones.

Ans. Following the various types of attacks against mobile/cell phones :

1. Mobile phone theft
2. Mobile viruses
3. Mishing (Mobile Phishing)
4. Vishing (Voice Phishing)
5. Smishing (SMS Phishing)
6. Hacking Bluetooth

2.11. What are the various security implications for organizations related to mobile devices ?

Ans. Following are various security implications for organizations related to mobile devices :

1. Managing diversity and proliferation of hand-held devices.
2. Unconventional/Stealth storage devices.
3. Threats through lost and stolen devices.

2.12. Discuss what organizations can do toward safegaurding their information systems in the mobile computing paradigm.

Ans. Organizations can do following to safegaurd their information systems :

1. Encrypting organizational databases.
2. Including mobile devices in security strategy.

2.13. Which algorithms are employed to implement strong encryption of database files ?

Ans. Following two algorithms are employed to implement strong encryption of database files :

1. The Rijndael algorithm
2. The Multi-Dimensional Space Rotation (MDSR) algorithm

2.14. What are different ways to create policy for mobile devices ?

Ans. Following are different ways to create policy for mobile devices :

1. Creating a distinct mobile computing policy.
2. Including mobile devices under existing policy.
3. Hybrid approach (mobile devices fall under both existing general policies and a new one).

☺☺☺

UNIT 3

Tools and Methods Used in Cybercrime (2 Marks Questions)

3.1. Describe the basic stages of attack through which attacker can compromise a network.

Ans. Following are the basic stages of attack through which attacker can compromise a network :

1. Initial uncovering
2. Network probe (investigation)
3. Progressing toward electronic crime (E-crime)
4. Capturing the network
5. Grab the data
6. Covering tracks

3.2. Briefly explain proxy servers.

Ans. A proxy server, situated within a network, serves as an intermediary for connecting with other computers on that same network.

3.3. Briefly explain anonymizer.

Ans. An anonymizer, also known as an anonymous proxy, is a tool designed to enhance online privacy by rendering internet activity untraceable.

3.4. What is phishing ?

Ans. "Phishing" is a term denoting a cyberattack tactic that involves the use of email programs to trick internet users into divulging confidential information.

3.5. How phishing works ?

Ans. Phishers work in the following ways :

1. **Planning :** Phishing attacks begin with meticulous planning.
2. **Setup :** In this stage, phishers establish the infrastructure required for their phishing campaign.
3. **Attack :** Once the setup is complete, phishers initiate the attack.
4. **Collection :** As recipients fall for the deception and respond to the phishing messages, phishers collect sensitive information.
5. **Identity theft and fraud :** With the collected information, phishers proceed to carry out identity theft and fraudulent activities.

3.6. What do you mean by password cracking ?

Ans. Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

3.7. What is the purpose of password cracking ?

Ans. The purpose of password cracking is as follows :

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

3.8. Discuss the categories of password cracking attacks.

Ans. Password cracking attacks can be classified under three categories as follows :

1. Online attacks.
2. Offline attacks.
3. Non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving).

3.9. What do you mean by keylogging (keystroke logging) ?

Ans. Keylogging involves the practice of recording keystrokes on a keyboard, typically done discreetly so that the keyboard user remains unaware of the monitoring.

3.10. Discuss keylogger and give its classification.

Ans. A keylogger provides a faster and more straightforward method for capturing passwords and observing the digital behavior of victims.

Classification : It can be classified as :

1. **Software keylogger :** Software keyloggers are software programs installed on computer systems, often positioned between the operating system and the keyboard hardware, recording every keystroke.
2. **Hardware keylogger :** Hardware keyloggers are compact physical devices. They are connected to the PC and/or the keyboard, recording each keystroke either in a file or in the device's memory.

3.11. What do you understand by antikeylogger ?

Ans. An antikeylogger is a tool designed to identify and remove keyloggers that have been installed on a computer system.

3.12. Give the advantages of antikeylogger.

Ans. Advantages of antikeylogger are as follows :

1. Detection and removal of keyloggers.
2. Protection from unauthorized surveillance.
3. Preventing identity theft.

4. Preservation of online security.
5. Protecting business and financial data.

3.13. What do you mean by spyware ?

Ans. Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.

3.14. What is a computer virus ?

Ans. A computer virus is a program that can "infect" legitimate software by altering it to incorporate a potentially "mutated" version of itself.

3.15. List various types of viruses.

Ans. Following are various types of viruses :

1. Boot sector viruses
2. Program viruses
3. Multipartite viruses
4. Stealth viruses
5. Polymorphic viruses
6. Macro viruses

3.16. What is a computer worm ?

Ans. A computer worm is a type of malware computer program that possesses the ability to replicate itself. It leverages a computer network to distribute copies of itself to other nodes, or computers, within the network, often accomplishing this without requiring any user involvement.

3.17. What do you mean by Trojan Horse ?

Ans. A Trojan Horse is a program that conceals malicious or harmful code within seemingly harmless software or data, allowing it to take control and inflict damage.

3.18. What do you understand by Backdoor ?

Ans. A backdoor provides a means of accessing a computer program while bypassing its security mechanisms. A backdoor grants malicious individuals the capability to execute any conceivable action on a compromised system.

3.19. How to protect your systems from Trojan Horses and backdoors ?

Ans. Follow the given steps to protect your systems from Trojan Horses and backdoors :

1. Stay away from suspect websites/weblinks.
2. Surf on the Web cautiously.
3. Install antivirus/Trojan remover software.

3.20. What do you understand by steganography ?

Ans. Steganography involves the act of hiding a file, message, image, or video within another file, message, image, or video. The term "steganography" is derived from two Greek words: "steganos," which means "covered, concealed, or protected," and "graphein," which means "writing."

3.21. What do you understand by steganalysis ?

Ans. Steganalysis is the practice of identifying concealed messages within images, audio, or video files that have been encoded using steganography.

3.22. What is denial-of-service (DoS) attack ?

Ans. A DoS attack is an attempt to make a computer resource unavailable to its intended users. In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his e-mail box with Spam mail, making it hard for them to use their services.

3.23. Give classification of DoS attack.

Ans. Classification of DoS attack :

1. Bandwidth attacks
2. Logic attacks
3. Protocol attacks
4. Unintentional DoS attack

3.24. What is distributed denial-of-service (DDoS) attack ?

Ans. DDoS attack is a malicious attempt to disrupts networks or websites by flooding them with massive traffic from multiple sources. DDoS differs from traditional DoS as it uses multiple compromised devices, forming botnets, for a coordinated attack.

3.25. What is SQL injection ?

Ans. SQL injection is a method of injecting code that takes advantage of a security weakness occurring in the database layer of an application. SQL servers, which are commonly used by many organizations to store sensitive data, are the primary targets of these attackers.

3.26. What is Blind SQL Injection attack ?

Ans. Blind SQL injection is employed when a web application has a vulnerability to SQL injection, but the attacker cannot directly see the outcomes of the injection.

3.27. What is buffer overflow ?

Ans. A buffer overflow, also known as a buffer overrun, occurs when a process stores data in a buffer beyond the memory allocated for it by the programmer. This can lead to unreliable program behavior, such as memory access errors, incorrect results, program crashes, or even a compromise of system security.

3.28. What are different buffer overflow attacks ?

Ans. Following are different buffer overflow attacks :

1. Stack-based buffer overflow
2. NOPs (no-operation instructions)
3. Heap buffer overflow

3.29. How to minimize buffer overflow attacks ?

Ans. Following methods help to minimize buffer overflow attacks :

1. Assessment of secure code manually.
2. Disable stack execution.
3. Dynamic run-time checks.

3.30. What are different components of wireless network ?

Ans. Following are different components of wireless network :

1. 802.11 networking standards
2. Access points
3. Wi-Fi hotspots
4. Service Set Identifier (SSID)
5. Wired equivalence privacy (WEP)
6. Wi-Fi protected access (WPA and WPA2)
7. Media access control (MAC)

3.31. Discuss some of the traditional techniques of attacks on wireless networks.

Ans. Following are some of the traditional techniques of attacks on wireless networks :

1. Sniffing
2. Spoofing
3. Denial of service (DoS)
4. Man-in-the-middle attack (MITM)
5. Encryption cracking

3.32. What is phishing ?

Ans. Phishing is a cyber attack technique in which attackers impersonate legitimate individuals, organizations, or entities to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal data.

3.33. What is spam e-mails ?

Ans. Spam emails are types of unsolicited or deceptive emails. Spam emails are typically commercial or promotional in nature, seeking profit or engagement with recipients.

3.34. What is hoax e-mails ?

Ans. Hoax emails are types of unsolicited or deceptive emails. Hoax emails aim to deceive or misinform recipients with fabricated stories, warnings, or false information.

3.35. What are different methods of phishing attacks ?

Ans. Following are different methods of phishing attacks :

1. **Dragnet :** Dragnet phishing is a mass email phishing technique where cybercriminals send a large number of generic phishing emails to a wide audience.
2. **Rod-and-reel :** Rod-and-reel phishing is a more targeted approach in which attackers select specific individuals or organizations as their victims.
3. **Lobsterpot :** In lobsterpot phishing attackers focus on high-value individuals or entities.
4. **Gillnet :** Gillnet phishing is a method that combines elements of both dragnet and rod-and-reel phishing.

3.36. What is identity theft (ID theft) ?

Ans. Identity theft (ID theft) is a type of cybercrime where an individual's personal, financial, or confidential information is stolen by malicious actors with the intent of impersonating the victim for various fraudulent purposes.

3.37. Explain types of identity theft.

Ans. Types of identity theft :

1. Financial identity theft
2. Criminal identity theft
3. Identity cloning
4. Business identity theft
5. Medical identity theft
6. Synthetic identity theft
7. Child identity theft

☺☺☺

4 UNIT

Understanding Computer Forensics (2 Marks Questions)

4.1. What do you understand by cyber forensics ?

Ans. Cyber forensics is simply application of computer investigation and analysis techniques in the interest of determining potential legal evidence.

4.2. What is digital forensics ?

Ans. Digital forensics entails employing analytical methods to ensure the dependable and impartial gathering, examination, comprehension, and exposition of digital proof. The goal of "cyberforensics" is to find digital proof of something specific or general.

4.3. Explain the role of digital forensics.

Ans. The role of digital forensics is to :

1. Uncover and document evidence and leads.
2. Corroborate evidence discovered in other ways.
3. Assist in showing a pattern of events.
4. Connect attack and victim computers.

4.4. Give examples of some typical scenarios in which digital forensics is used.

Ans. Following are examples of some typical scenarios in which digital forensics is used :

1. Employee internet abuse.
2. Data leak/data breach.
3. Industrial espionage.
4. Criminal fraud and deception cases.
5. Criminal cases.
6. Copyright violation.

4.5. What is the need for computer forensics ?

Ans. The need for computer forensics can be attributed to two key factors: law enforcement's growing reliance on digital evidence and the universal proliferation of computers resulting from the microcomputer revolution.

4.6. What is "chain of custody" concept ?

Ans. It refers to the chronological record or documentation process that signifies the acquisition, possession, control, transfer, examination, and final handling of evidence, whether it is in physical or electronic form.

4.7. What do you understand by digital evidence ?

Ans. Digital evidence refers to any information or data that is stored or transmitted in a digital form and can be used as evidence in legal proceedings. It encompasses a wide range of digital sources, including: electronic documents, computer files, log files, metadata, internet activity and device information.

4.8. What do you understand by "Rules of evidence" ?

Ans. The Rules of Evidence under the Indian Evidence Act, 1872, provide a structured framework for the admission and exclusion of evidence in Indian courts. These rules play a pivotal role in ensuring that trials are fair, evidence is reliable, and justice is served.

4.9. What do you understand by forensics analysis of e-mail ?

Ans. Forensic analysis of e-mails is a process of systematically examining e-mail messages and associated data to gather evidence for legal or investigative purposes. This type of analysis is commonly used in various fields, including law enforcement, corporate investigations, cybersecurity, and legal proceedings.

4.10. Outline the various key steps involved in tracing an email for forensic purposes.

Ans. Following are the key steps involved in tracing an email for forensic purposes :

1. Examine e-mail header
2. Review "received" sections
3. Identify source server
4. Analyze timestamps
5. Examine e-mail content
6. Check server logs
7. Follow IP addresses
8. Utilize timestamp analysis
9. Beware of fake headers
10. Explore X-headers

4.11. What do you understand by digital forensics process ?

Ans. The digital forensics process is a legal procedure that involves the preparation and presentation of evidence in a legal context. Digital forensics evidence consists of digital exhibits presented by qualified witnesses to help establish facts and legal theories in a case.

4.12. What are the various phases involved in the life cycle of a forensics investigation process ?

Ans. Forensics life cycle involves the following phases :

1. Preparation and identification of evidence.
2. Collection and recording digital evidence.
3. Storing and transporting digital evidence.
4. Examination/investigation digital evidence.
5. Analysis, interpretation and attribution.
6. Reporting.
7. Testifying.

4.13. What are the various activities involved in the "preparation stage" of a forensics investigation process ?

Ans. Preparation stage involves the following activities :

1. **Case briefings :** At the preparation stage, digital forensics experts gather information about the case, including the alleged misconduct, potential evidence sources, and key parties involved.
2. **Engagement terms :** Experts establish clear terms of engagement, outlining the scope of work, responsibilities, and expectations.
3. **Interrogatories :** Legal teams may prepare written questions for opposing parties to gather information about the case.
4. **Spoliation prevention :** Developing a strategy to prevent data spoliation.
5. **Discovery requests :** Legal teams request relevant evidence from opposing parties, including electronically stored information.

4.14. What are the different types of digital analysis that can be performed on the captured forensics evidence ?

Ans. Following are the different types of digital analysis that can be performed on the captured forensics evidence :

1. Media analysis
2. Media management analysis
3. File system analysis
4. Application analysis
5. Network analysis
6. Image analysis
7. Video analysis

4.15. What are the typical elements of a digital forensics investigation report ?

Ans. Following are the typical elements of a digital forensics investigation report :

1. Identity of the reporting agency.
2. Case identifier or submission number.
3. Case investigator.
4. Identity of the submitter.
5. Date of receipt.

6. Date of report.
7. Descriptive list of items submitted for examination.
8. Identity and signature of the examiner.
9. Brief description of steps taken during examination.
10. Results/conclusions.

4.16. What is network forensics ?

Ans. Network forensics is a branch of digital forensics that focuses on the monitoring, analysis, and investigation of network traffic and data to uncover security incidents, cyber attacks, and other network-related crimes.

4.17. What are the phases involved in computer forensics investigation ?

Ans. Following are the phases involved in computer forensics investigation :

1. Secure the subject system.
2. Take a copy of hard drive/disk.
3. Identify and recover all files.
4. Access/view/copy hidden, protected and temp files.
5. Study "special" areas on the drive.
6. Investigate application and program data.
7. Consider the system as a whole.
8. Consider general factors relating to the user's activity.
9. Create detailed and considered report.

4.18. What are the things to be avoided during a computer forensics investigation ?

Ans. Things to be avoided :

1. Changing date/time stamps
2. Changing data
3. Overwriting unallocated space

4.19. What are the things that cannot be avoided during a computer forensics investigation ?

Ans. Things that cannot be avoided :

1. Engagement contract
2. Non-Disclosure Agreement (NDA)
3. Customer agreement
4. Legal definitions

4.20. Which important elements are addressed in a forensics investigation engagement contract ?

Ans. Following important elements are addressed before while drawing up a forensics investigation engagement contract :

1. Authorization
2. Confidentiality

3. Payment
4. Consent and acknowledgment
5. Limitation of liability

4.21. What is a "social networking" site ?

Ans. A "social networking" site is an online platform or website that enables individuals to create digital profiles, connect with other users, and engage in various forms of social interaction and communication.

4.22. What are the security threats that can emanate from social networking sites ?

Ans. Security threats that can emanate from social networking sites are listed below :

1. **Corporate espionage :** Social networking sites can be a source of information leakage for organizations.
2. **ID theft :** Personal information shared on social networking sites can be exploited by cybercriminals for identity theft.
3. **Bullying :** Social networks can become platforms for cyberbullying.
4. **Infiltration of networks :** Attackers can infiltrate social network connections and gain access to sensitive personal data, potentially leading to data breaches.
5. **Stalking :** Social networking sites can be exploited by stalkers to gather information about their targets.

4.23. What are the challenges in computer forensics ?

Ans. Following are the challenges in computer forensics :

1. Data volume challenge
2. Data tampering risk
3. Privacy concerns
4. Adaptation to technological advancements
5. Network forensics challenges
6. Examination backlog

☺☺☺

5 UNIT

Introduction to Security Policies & Cyber Laws (2 Marks Questions)

5.1. What is an information security policy ?

Ans. An information security policy is a formal document that outlines an organization's approach to protecting its information assets. It defines the rules and procedures that employees and other stakeholders must follow to ensure the confidentiality, integrity, and availability of information.

5.2. What are the benefits of having an information security policy ?

Ans. The benefits of having an information security policy include :

1. Reduced risk of security incidents.
2. Improved compliance with laws and regulations.
3. Reduced financial losses.
4. Protected reputation.

5.3. What are the key components of an information security policy ?

Ans. The key components of an information security policy include :

1. A statement of purpose.
2. A definition of the scope of the policy.
3. A description of the organization's information assets and their classification.
4. A description of the security controls that will be used to protect information assets.
5. A description of the roles and responsibilities of employees and other stakeholders.
6. A description of the process for reporting and responding to security incidents.

5.4. What is Indian cyber law ?

Ans. Indian Cyber Law, formally known as the Information Technology Act, 2000 (ITA 2000) along with its amendments, is the primary legal framework governing cyberspace and electronic transactions in India.

5.5. Briefly explain Information Technology Act, 2000 (ITA 2000).

Ans. The Information Technology Act, 2000 (ITA 2000) is an Indian legislation that governs electronic commerce and digital communication. It provides legal recognition to electronic transactions, digital signatures, and electronic records. The act also addresses cyber crimes and penalties for unauthorized access, data theft, and computer-related offenses.

5.6. What is Indian Computer Emergency Response Team (CERT-In) ?

Ans. CERT-In is the nodal agency for cyber security in India. It is responsible for responding to cyber incidents, coordinating with law enforcement agencies, and issuing security advisories.

5.7. What is National Cyber Security Coordinator (NCSC) ?

Ans. The NCSC is the apex body for cyber security in India. It is responsible for coordinating the efforts of various government agencies and stakeholders to protect India from cyber threats.

5.8. What are the rights of individuals under Indian cyber law ?

Ans. Individuals have a number of rights under Indian cyber law, including the right to :

1. Privacy
2. Access to information
3. Free speech
4. Compensation

5.9. What are the rights of organizations under Indian cyber law ?

Ans. Organizations have a number of rights under Indian cyber law, including the right to :

1. Protect their intellectual property
2. Protect their business data
3. Take action against cyber criminals

5.10. What are the latest developments in Indian cyber law ?

Ans. The latest developments in Indian cyber law include :

1. The Digital Personal Data Protection Act, 2023.
2. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
3. The Indian Cyber Crime Coordination Centre (IC3).
4. The National Cyber Security Strategy, 2020.

5.11. What is Digital Personal Data Protection (DPDP) Act, 2023 ?

Ans. The Digital Personal Data Protection (DPDP) Act, 2023 is a law of the Parliament of India to provide for the processing of digital

personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.

5.12. What are main objectives of the DPDP Act ?

Ans. The main objectives of the DPDP Act are to :

1. Protect the right of individuals to privacy and to protect their personal data from unauthorized access, use, disclosure, modification, or destruction.
2. Promote responsible data processing practices by organizations.
3. Establish a framework for the governance of digital personal data in India.

5.13. What are the rights given to individuals by DPDP Act ?

Ans. The DPDP Act establishes a number of rights for individuals, including the right to :

1. Access their personal data.
2. Correct their personal data.
3. Erase their personal data.
4. Object to the processing of their personal data.
5. Port their personal data.

5.14. What is intellectual property (IP) ?

Ans. Intellectual property (IP) is a category of property that includes intangible creations of the human intellect.

5.15. What are the different types of intellectual property ?

Ans. Following are the different types of intellectual property :

1. Patents
2. Copyrights
3. Trademarks
4. Trade secrets

5.16. What are intellectual property (IP) issues ?

Ans. Intellectual property (IP) issues refer to legal and ethical challenges related to the protection and management of intellectual property rights.

5.17. Provide examples of common IP issues that individuals or organizations may face.

Ans. Following are some examples of common IP issues that individuals or organizations may face :

1. Copyright infringement
2. Trademark infringement
3. Trade secret theft
4. Patent infringement

5. Counterfeiting
6. Plagiarism

5.18. How can businesses protect their intellectual property rights in the digital domain ?

Ans. Businesses can protect their intellectual property rights by :

1. Registering their IP rights.
2. Develop a comprehensive IP policy.
3. Using technical measures.
4. Educating employees and customers.
5. Monitoring online activity.
6. Taking legal action.

5.19. How can individuals protect their intellectual property rights in the digital domain ?

Ans. Individuals can protect their intellectual property rights by :

1. Understand IP laws.
2. Respect copyright and licensing.
3. Protect personal data.
4. Use strong passwords.
5. Report infringements.
6. Taking legal advice.

5.20. What is a patent ?

Ans. A patent is a legal document that grants the inventor exclusive rights to make, use, and sell an invention for a certain period. It is a form of intellectual property protection designed to encourage innovation.

5.21. What are the requirements for obtaining a patent ?

Ans. Following are the requirements for obtaining a patent :

1. Novelty
2. Non-obviousness
3. Usefulness or utility
4. Subject matter eligibility
5. Adequate disclosure
6. Claim specificity

5.22. What is copyright ?

Ans. Copyright is a legal protection granted to the creators of original literary, artistic, musical, and other creative works. It gives creators the exclusive right to reproduce, distribute, perform, and display their works for a specified duration.

5.23. What are the requirements for obtaining copyright ?

Ans. To obtain copyright protection following requirements must be met :

1. **Original work :** It which means that work should be the result of the author's creative effort and not a direct copy of someone else's work.
2. **Work must be fixed :** The work must be fixed in a tangible medium, meaning it must be in a form that can be perceived, reproduced, or communicated.

5.24. What is a trademark ?

Ans. A trademark is a distinctive sign or symbol, such as a word, phrase, logo, symbol, design, or combination thereof, that is used to identify and distinguish goods or services offered by one party from those of others.

5.25. What are the requirements for registering a trademark ?

Ans. The requirements for registering a trademark include :

1. Distinctiveness
2. Non-descriptiveness
3. Non-deceptiveness
4. Not similar or confusing
5. Not offensive
6. Not prohibited by law
7. Proper representation

☺☺☺

Quantum Series®
ENGINEERING

QUANTUM Series

Related titles in Quantum Series

For Semester - 3 & 4 (Common to All)

Common Courses

- Cyber Security
- Python Programming
- Technical Communication
- Mathematics –IV
- Universal Human Values and Professional Ethics

Open Elective Courses

- Material Science
- Energy Science & Engineering
- Sensor & Instrumentation
- Basics Data Structure & Algorithms
- Analog Electronics Circuits
- Electronics Engineering
- Digital Electronics
- Laser System and Applications

A comprehensive book to get the big picture without spending hours over lengthy text books.

Quantum Series is the complete one-stop solution for engineering student looking for a simple yet effective guidance system for core engineering subject. Based on the needs of students and catering to the requirements of the syllabi, this series uniquely addresses the way in which concepts are tested through university examinations. The easy to comprehend question answer form adhered to by the books in this series is suitable and recommended for student. The students are able to effortlessly grasp the concepts and ideas discussed in their course books with the help of this series. The solved question papers of previous years act as a additional advantage for students to comprehend the paper pattern, and thus anticipate and prepare for examinations accordingly.

The coherent manner in which the books in this series present new ideas and concepts to students makes this series play an essential role in the preparation for university examinations. The detailed and comprehensive discussions, easy to understand examples, objective questions and ample exercises, all aid the students to understand everything in an all-inclusive manner.

- **Topic-wise coverage in Question-Answer form.**
- **Clears course fundamentals.**
- **Includes solved University Questions.**
- **The perfect assistance for scoring good marks.**
- **Good for brush up before exams.**
- **Ideal for self-study.**

Quantum Publications®
(A Unit of Quantum Page Pvt. Ltd.)
Plot No. 59/2/7, Site-4, Industrial Area, Sahibabad,
Ghaziabad, 201010, (U.P.) Phone: 0120-4160479
E-mail: pagequantum@gmail.com Web: www.quantumpage.co.in
Find us on: facebook.com/quantumseriesofficial

Quantum Page™