GRADAMIC

B.Tech–2nd Year Session 2024–25 Odd Semester

Dr. A. P. J. Abdul Kalam Technical University
Lucknow, Uttar Pradesh

BCC 301/ BCC 401/ BCC 301H / BCC 401/H

CYBER SECURITY

app.gradamic.com

UNIT – 1st

UNIT -I

INTRODUCTION TO CYBER CRIME

INTRODUCTION TO CYBER CRIME: *Cybercrime- Definition and Origins of the word Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. Cyber offenses: How Criminals Plan the Attacks, Social Engineering, Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector.*

Medium Answer Type Questions –

Que 1. What is the definition of cybercrime? Discuss types of attacks prevalent in cybercrime.

Cybercrime specifically can be defined in several 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.

Types of attacks prevalent in cybercrime

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 2. Explain the origins of the word "cybercrime".

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 for unlawful activities or acts that violate laws and regulations. It encompasses a wide range of illegal behaviours 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.

Que 3. How do cybercrimes differ from traditional crimes?

S.NO	Aspect	Cybercrimes	Traditional Crime
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 4. Explain information security. How does information security relate to the prevention of cybercrimes?

Ans. 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 cybercrimes:

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 cybercrimes.
5. **Vulnerability management:** Information security practices include vulnerability assessments and patch management.
   Addressing vulnerabilities promptly reduces the risk of cybercriminals exploiting security flaws.

Que 5. Who are cybercriminals? What are their types?

Ans. 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:

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.

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.

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.

Que 6. What are the different categories or types of cybercrimes?

Ans. 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 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 cybercrime 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. **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 7. What is the impact of cybercrimes on individuals, property, and government?

Ans. 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 cybercrimes. 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 cyberbullying, online harassment, or cyberstalking 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. Against Organisation or 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.

Que 8. What are the 5P's? Or

Discuss the survival mantra for the netizens for online security.

- The 5P netizen mantra for online security provides a comprehensive approach to staying safe in the digital world.
- 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 sceptical 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.
2. 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.

Que 9. What do you understand by cyber offenses? Also explain the terms hackers, crackers, and phreakers.

Ans. **Cyber Offenses can be defined as:**

A. Cyber offenses

1. Cyber offenses, also known as cybercrimes, 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 telecommunication systems, often with a focus on gaining free access to phone services or exploring the inner workings of the telephone network.

Que 10. Explain how cybercriminals plan the attacks.

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. The following phases are involved in planning cybercrime:

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 analyse 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.

Que 11. Explain the term "social engineering" in context of cyber security.

Ans. Social engineering is defined as:

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 behaviour 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 12. Give a classification of social engineering.

Ans. Social engineering is classified as follows:

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 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.

Que 13. What do you understand by cyberstalking? Also, give its key characteristics.

Ans. Cyberstalking:

1. Cyberstalking 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. Cyberstalking 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 cyberstalks.
6. Victims of cyberstalking are encouraged to report incidents to law enforcement agencies and take steps to protect their online privacy and security.

Key characteristics of cyber stalking

1. **Repetitive behaviour:** Cyberstalks 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:** Cyberstalks 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:** Cyberstalks 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 14. What do you mean by cybercafe? How cybercafes are associated with cybercrimes in India?

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. Cyber cafes have played a significant role in India's digital revolution. providing access to the internet and online services for millions of people.

Here's a brief overview of the role of cybercafes:

1. **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.
2. **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.
3. **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 cybercrimes 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 the 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 cybercrime investigations.

Que 15. What is the Indian government's response to combat cybercrimes using cybercafes?

- The Government has taken steps to spread awareness about cybercrimes, issuing alerts/ advisories, capacity building of law enforcement personnel/prosecutors/judicial officers, improving cyber forensic facilities, etc.
- Cyber Surakshit Bharat is an initiative from the Ministry of Electronics and Information Technology (MeitY) that aims to create a robust cybersecurity ecosystem in India.
- The government has established cybercrime cells and cyber forensic laboratories to investigate and prosecute cybercrimes effectively.
- There is an ongoing effort to raise awareness about cybersecurity among cybercafe owners and the general public to mitigate cyber threats.

Que 16. What are the measures 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:** 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.

Que 17. What are Botnets? Why are they considered "The Fuel for Cybercrime"?

Ans. 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.

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. **Invisibility:** 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 exfiltration 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 18. What measures should an individual take to secure his system from botnets?

Ans. The 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 mailbox - "sent items" or "outgoing" for those messages you did not send.
7. Take immediate action if your system is infected.

Que 19. Define Malware and it's types.

Ans. Malware is defined as:

- Any software designed with the malicious intent either to harm or exploit any programmable device, service, or any network or gain access of user's computer system control without their permission is referred to as Malware.

- We can say that Malwares are developed by the cyber criminals to steal data or damage or destroy the user's computer system completely.

Types of Malwares are as:

1. **Viruses:** A computer virus is a type of malicious programme that multiplies and inserts its own code when it is run. This code infects the other files and programmes on your system after the replication is completed. There are numerous varieties of these viruses which can affect the system in different ways.
2. **Worms:** A type of malware that can automatically self-replicate without the human interaction, spreads over through the hardware affecting many other systems. One of the biggest dangerous abilities is to send out hundreds or thousands of copies of itself. Mostly uses the LAN (Local Area Network) to spread.
3. **Spyware:** Spyware = SPY (snoopy or spying) + WARE. Spywares are the malwares that secretly enters the user's computer system to steal data and send it to the host without being caught by user. It collects user's personal, professional, financial & identical information and uses it with harmful intent with user's permission.
4. **Ransomware:** The word 'Ransom' stands for the demanding the money. Ransomware is one of the widely used malware which holds the victim's sensitive or personal information like device hostage and then threating to keep it locked or worse or unless the victim pays demanding amount to the attacker.
5. **Trojan Horse:** Malicious actions seem to be nice or an approved activity such as playing online games or downloading from web but it attaches itself to non-executable items like image or audio files having dangerous intent to damage or steal information, also it differs from a virus.
6. **Adware:** Adware term is used for displaying unwanted ads and pop-ups on your device. By slow down your device, taking control over browser, installing hidden viruses, Adware has the ability to turn dangerous or damage it.
7. **Rootkit:** It is defined as the malware programme which enables the cybercriminals to gain the access to and infiltrate the data from computers anonymously. It covers software toolboxes intended to infect machines, grant remote control to the attacker and stay undetected for an extended period of time.

Que 20. What do you mean by "attack vector"? How are attack vectors launched?

Ans. Attack Vector is defined as:

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 the 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.