Cyber security (IT)

(R22 IT 7th IPE)

PART-A

1a) Who are cybercriminals?

Ans: Individuals or groups who use computers, networks or digital devices to commit illegal activities like hacking, fraud, datatheft, or Malware attacks.

b) What is meant by information security?

Ans: Protecting information from unauthorized access, Modification, destruction, and ensuring confidentiality, integrity and availability (CIA triad).

c) What is cyberstalking?

Ans. Repeated online harassment or monitoring of a person using emails, social media, messages, or tracking tools.

d) define attack vector?

Ans. The path or Method used by an attacker to gain unauthorized access to a system.
Eg: phishing, Malware, USB, weak Wi-fi.

e) What is credit card fraud in mobile computing?

Ans: Unauthorized Use of credit card information through Mobile devices, apps, fake websites, or insecure networks.

f) List any two registry settings that improve Mobile device security?

Ans: The two registry settings that improve mobile device security.

The two registry settings that improve Mobile device security.

1. Disable installation of untrusted apps.
2. Enable device password / PIN and encryption.

g) What is Trojan horse?

Ans: Malicious software disguised as a legitimate application, which secretly performs harmful activities once installed.

h) Define Steganography?

Ans The process of hiding secret information inside another file (image, audio, video, text) so the existence of the message is concealed.

(i) What are Web threats?

Ans Cyber attacks delivered through websites or web applications such as Phishing sites, Malware downloads, SQL injection, XSS, and DDOS.

j. What is the meaning of social media marketing.

Using social media platforms to Promote Products, build brand identity, engage, customers, and increase business visibility.

PART – B

2. Describe the relationship between cybercrime and information security with examples?

Ans Cybercrime refers to illegal activities carried out using computers, Networks, and digital devices. These crimes include hacking, phishing, identity theft, online fraud, ransomware attacks, website defacement, and data breaches. Cybercriminals take advantages of weak passwords, system Vlunerabilites, software flaws, unsecured networks, or human mistakes to steal information, cause financial loss, or disrupt services, cybercrime affects individuals, businesses, and governments because of the growing dependence on digital platforms.

Information security, on the other hand deals with protecting information from unauthorized access, misuse, modification or destruction. It ensures that data remains confidential, accurate, and available whenever needed. Information security uses tools such as authentication, encryption, firewalls, intrusion detection systems, secure coding, policies and user awareness to protect digital assets. While cybercrime represents the threat,

Information security represents the protection mechanism that reduces or prevents these threats.

The relationship between cybercrime and Information security is very close because both deal with the same environment. cybercrime exposes weakness in systems, and information security aims to close those weaknesses. When information security controls fail, cybercrime succeeds, when information security is strong, the Chances of cybercrime are minimized.

Essentially, cybercrime motivates the development of stronger security policies, and information security evolves continuosly to defend against new forms of cybercrime. Both are interconnected, and one cannot be understood without the other.

A simple example of cybercrime is a phishing email that steals a user's banking username and password. A corresponding example of information security is enabling two-factor authentication, which prevents attackers from logging in even if the password is stolen. These examples show how cybercrime and information security operate against each other in the digital world.

(3) Analyze how the IT Act 2000 addresses Cybercrimes in India and its limitations.

Ans The Information Technology Act 2000 is India's first cyber law created to give legal recognition to electronic records and digital signatures, and to define punishments for cybercrimes. It was later amended in 2008, 2009, 2011 and 2018 to address new cyber threats like identity theft, data protection issues, and cyber terrorism.

IT Act - year-wise - Amendments

2000 - IT Act introduced:

Original IT Act created to give legal recognition to electronic records and define Cybercrimes.

2008 - IT Amendment ACT:-

Added data protection rules, stronger penalities identity theft sections, and established CERT-In

2009 - IT Amendament ACT:-

Enhanced rules for electronic signatures and Provided more power to government agencies.

2011 - Intermediary Guidelines:

Addressed issues related to electronic signatures, digital authentication, and responsibilities of social media platforms

2018 - Updated Data & Privacy Rules:-

Focused on authentication procedures, protection of sensitive personal data, and increased Penalties for violations

Sections for each Amendment:-

Section 65: Tampering of source code of Computer.

Punishment: 3years / ₹ 2lakh

Matter: Deals with tampering or destroying Computer source code intentionally.

Section 66 : Hacking :-

Punishment : 3years / ₹ 5 lakh

Matter: Covers hacking and all computer-related offences done dishonestly or fraudulently.

Section 66 B : Data theft:

Punishment : 3years / ₹ 1 lakh.

Matter:- Receiving stolen Computer devices or data knowingly.

Section 66C: Identity theft

Punishment: 3 years / ₹ 1 lakh

Matter: Identity theft through misuse of passwords digital signatures, or online identities.

Section 67B: Child pornography:-

Punishment: 7 years.

Matter:- child pornography and exploitation of minors through online content.

Section 66F: cyber Terrorism:-

Punishment: life imprisonment

Matter: cyber terrorism aimed at threatening national security.

Section 43: unauthorised access to computers:

Punishment: Compensation (amount depends on loss).

Matter: Failure of a company to protect sensitive personal data of users.

4. Explain how social engineering can be used to execute cyber offenses.

Ans Social engineering is a technique where attackers manipulate people into revealing confidential information or performing actions that allow cybercrimes to occur. Instead of attacking software or hardware directly, the attacker targets the human mind. Humans trust easily, respond to fear or urgency, and rarely verify identity — these weaknesses make social engineering extremely successful in cyber attacks.

Human-based social engineering occurs through direct person-to-person interaction. The attacker pretends to be someone trustworthy, such as a bank employee, IT technician, government officer, or HR executive. They use friendly conversation, fear, urgency, or authority to convince the victim to share passwords, OTPS, or personal details. Common methods include impersonation, pretexting, tailgating and shoulder surfing. Human based attacks succeed because people naturally respond to requests when someone speaks confidently.

Computer-based social engineering uses digital communications like emails, sms, websites, pop-ups, or mobile apps. These attacks are faster and target thousands of people at once. The most common form is phishing, where the

attacker creates fake emails or websites that look identical to those of banks, social media platforms, or delivery companies. When victims enter their login details, the attacker captures them instantly. Smishing (SMS phishing) and Vishing (phone fraud) are also widely used. Fake software updates, malicious attachments, and deceptive advertisements are examples of computer based social engineering.

Both types of social engineering are used to launch cyber offenses such as identity theft, credit card fraud, unathorized access to systems, ransomware attacks, and financial scams. Even a single careless action by an employee – such as clicking a link or sharing a password – can compromise an entire organization. This is why social engineering is considered more dangerous than purely technical hacking, because it targets human vulnerability rather than system weakness.

(5) Evaluate the role of botnets in large-scale cyber attacks?

Ans A botnet is a network of thousands or millions of infected devices that are secretly controlled by a hacker known as the botmaster. These devices – laptops, mobiles, routers, CCTV cameras, IoT devices

become "bots" once infected with malware. Because users do not realize their device is compromised, botnets grow silently and can be used to perform large-scale cyber attacks without any physical presence of the attacker

Botnets are extremely powerful in cyber attacks because the botmaster can control every infected device from a central command-and-control (C_2) server. When the attacker sends a command, all bots act simultaneously. This makes botnets useful for launching massive, Distributed Denial of service (DDoS) attacks. In a DDoS attack thousands of bots send continuous traffic to a target website or server until it becomes overloaded and crashes. No single computer can generate this much traffic, which is why botnets are used for attacks that require scale and speed.

The complete setup of botnet follows a clear pattern. First, the attacker spreads malware through phishing emails, malicious downloads, or infected systems websites. When users unknowingly install this malware, their devices get connected to the C_2 server. The botmaster can then issue commands like "send traffic", "steal passwords" "spread malware", or scan for vulnerabilities.

Because botnets use many different Ip addresses, it becomes extremely dificult for security systems to block or trace the attack back to its orgenal source.

Botnets are used not only for DDos attacks but also for Sending spam emails, Carrying out click fraud, stealing banking information, mining Cryptocurrency Using Victims devices, and Spreading ransomeware acsoss networks. their ability to operate globally and silently makes them a major threat to cybersecurity.

-A real-time example is the mirai Botnet attack in 2016. mirai infected millions of IOT devices like Cameras and routers by exploiting weakpass-words. the botnet lanched a huge DDos attack on Dyn, a major DNS provider, which caused popular websites Like Twitter, NetFlix, Reddit, and GitHub to go offline for hours. This incident showed how easily everyday devices can be turned into a massive cyber weapon.

(6) Major security challenges in the mobile and wireless computing era

Ans Mobile and wireless computing has made devices highly convenient but also highly vulnerable Because phones and tablets stay connected all the time, attackers get more chances to exploit them.

Mobile Malware:- Malicious apps, fake updates, sms links, and infected downloads easily enter Mobile devices. Malware steals passwords, banking data, photos, and contacts.

Device loss or theft:- Mobiles are often lost or stolen. if unlocked all emails, documents, cloud accounts, saved passwords, and business data become exposed to attackers.

Insecure Wi-fi networks:-

Public wifi allows hackers to intercept data using man-in-the-middle attacks. Even home wi-fi becomes risky if weak passwords or outdated encryption are used.

Malicious Mobile applications:-

Fake apps disguise themselves as games or utilities. poorly coded apps leak data, collect unnecessary permission or secretly unnecessary Permissions, or secretly monitor user activity.

BYOD (Bring your own Device) risks:

Employees bring personal mobiles into office networks. These devices may not have antivirus, updates, or encryption, making them an easy entry point for malware.

Mobile payment and financial fraud:-

Attackers use phishing SIM swapping, fake banking apps, and screen overlay attacks to steal OTPs and card details during mobile transactions.

Wireless protocal vulnerabilities:-

Weak Bluetooth settings, Open hotspots, and Outdated devices create more vectors for attackers.

Fragmented mobile ecosystem:-

Different brands, OS versions, and update cycles make it difficult to maintain uniform security across all devices.

These challenges together make mobile and wireless environments highly vulnerable unless strong security measures are enforced.

(7) How Organizational Policies reduce risks of mobile-based cyber threats

Ans Mobile threats increase when employees use their personal devices for office work. Strong orgnizational policies help control these risks by defining how devices should be used inside the company.

* BYOD Policy:-

This policy controls how personal devices access Office systems. It sets rules for app installation Secure network usage, password protection, and reporting of lost or stolen devices.

* Uses of mobile Device management (MDM)

Organizations enforce MDM tools to remotely lock, wipe, track, and manage smartphones. MDM ensures devices have updates, encryption, strong passwords, and only approved apps.

Access control rules:-

Policies enforce multi-factor authentication strong Passwords, and role-based access so employees only access necessary data. This prevents unathorized entry if a device is compromised.

Secure network usage guidelines:-

Employees are instructed not to use public wi-fi for office work. VPN is made mandatory for remote access, and office wi-fi uses strong WPA2/ WPA3 security

Data protection rules:-

Sensitive data stored on mobile devices must be encrypted. file sharing must happen through approved office apps, not through personal emails or messaging apps.

Employee training and awareness:-

Policies require higher regular training on Phishing, fake apps, smishing, vishing, and social engineering. most mobile attacks succeed due to human error, so awareness reduces risk.

Incident reporting procedure:-

Employees must report suspicious activity, malware alerts, or lost devices immediately. Quick response helps limit damage and protect the network.

By following these policies, organizations create a secure mobile environment and significantly reduce Mobile-based cyber threats.

(8) Explain the working principles of password cracking, spyware, and Keyloggers

Ans 1. password cracking:-

Definition:- Password cracking is the process of recovering or guessing passwords to gain unauthorized access to systems, accounts, or data.

How it works (Implementations):

-Attackers obtain password hashes from a system.

They run cracking tools that try thousands of combinations.

Methods include brute force, dictionary attack, hybrid attack, rainbow tables, and social engineering.

Offline cracking is faster because attackers Test passwords without systems restrictions.

Threats:

Unathorized access to accounts and systems.

Identity theft and financial fraud.

Complete takeover of email, banking, or social media.

Malware installation after access is Obtained.

How to Overcome:-

Use strong and long passwords.
Enable multi-factor authentication.
Avoid saving passwords on browsers.
Regularly update passwords.
Use accounts lockout policies.

Realtime examples:-

An attacker steals hashed passwords from a company database and uses a tool like John the Ripper to crack weak employee passwords within minutes.

2. Spyware:

Definition:- Spyware is malicious software that secretly monitor user activities and sends collected data to an attacker

How It works: Install silently through malicious downloads. fake apps, pop-ups. or Pirated software.

Records browsing history, keystrokes, screenshots, and app activity

sends stolen data to the attacker through the internet.

Threats:-

Threats of banking passwords, OTPs, PINs.

Identity theft:- Targeted ads and Privacy violations

Corporate espionage.

How to overcome:-

Install apps only from trusted sources.

use anti-spyware and antivirus

Avoid clicking unknown links or pop-ups.

Monitor app permissions

Keep OS and apps updated.

Real-Time example:-

The Pegasus spyware was used to secretly record calls, messages, and camera activity from targated mobile phones.

3. Key loggers:

Definition:- A keylogger is a program or device that records every keystroke typed by the user, including passwords and confidential data.

How it works:-

software keyloggers run in the background Capturing every thing typed.

Hardware keyloggers sit between keyboard and computer.

Logs are sent to the attacker through email or remote server.

Threats:

Complete password theft.

Online banking fraud.

Access to confidential company documents

Identity theft.

How to overcome:-

Use on-screen keyboards for sensitive inputs.

Enable antivirus and anti keylogger tools.

Keep system updated.

Avoid installing unknown applications.

Real-Time Example:-

Cyber cafe infected with keyloggers captured users banking passwords, resulting in multiple fraud cases.

(9) Analyze SQL injection and Buffer overflow can compromise system security

Ans 1. SQL injection:

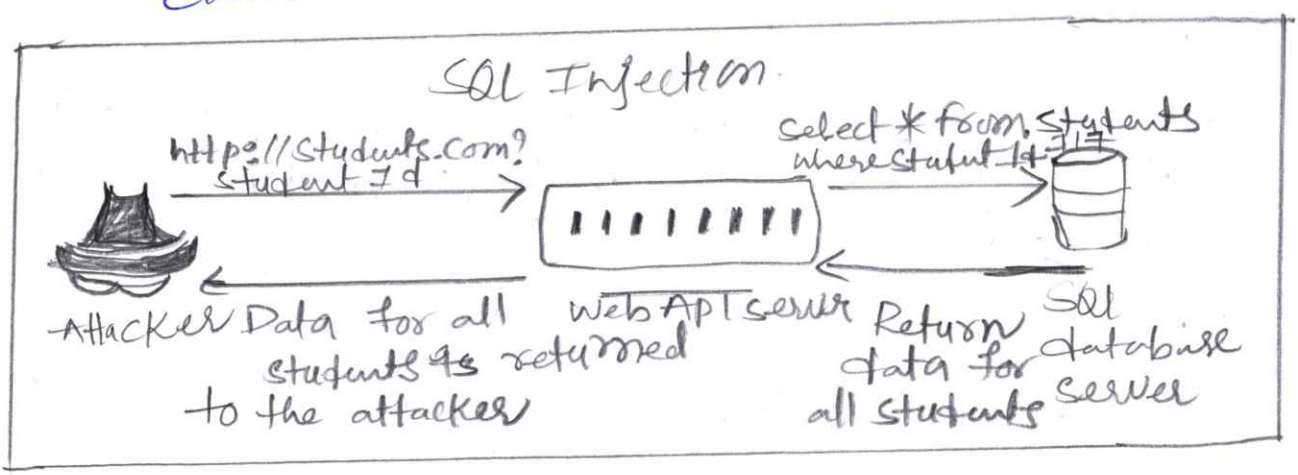
Defination: SQL injection is an attack where an attacker inserts malicious SQL code into input fields to manipulate the backend database

Impact on system security

Bypass login authentication
Steal sensitive customer data.
Modify or delete database records.
Execute administrative operations on database
Full database compromise.

Types:

Error-based SQL injection
Union based SQL injection
Blind SQL injection.
Classic SQL injection



Setup/working:

Attackers find a vulnerable input field.
sends SQL code like 'OR' 1' = 1' —
Database executes attackers code
Attackers gains unauthorized access.

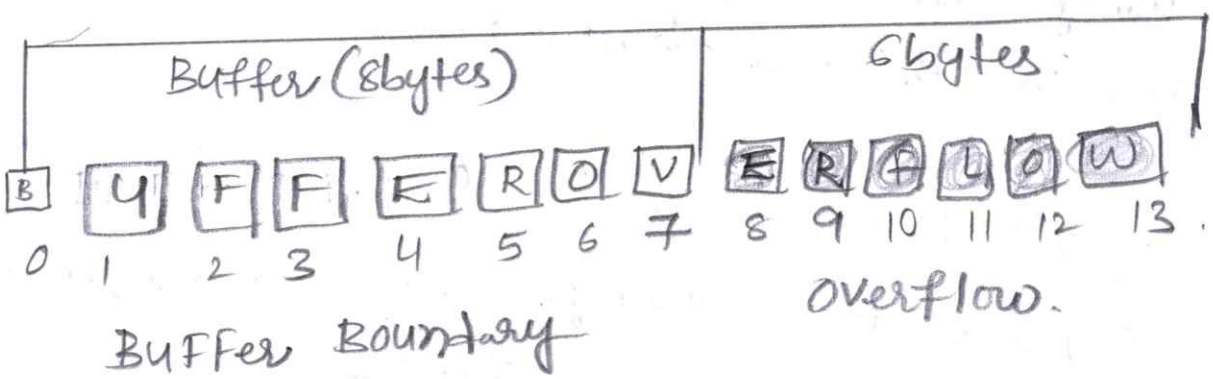
Real-time Example:- A shopping website login form was bypassed using SQL injection, leaking thousands of user credit card details.

② Buffer overflow :-

Definition: Buffer overflow occurs when a program writes more data into memory than allocated, causing overwrite of adjacent memory.

Impact on system security:

Security crash
Unauthorized code execution
Privilege escalation.
Complete system takeover.
Installation of malware or backdoors



Types: Stack buffer overflow.
Heap overflow.

setup/working

Program allocates fixed memory
Attacker sends oversized input.
Extra data overwrites return address.
Program executes attacker's shellcode.

Real time example:-

The Morris worm exploited a buffer overflow vulnerability in Unix, crashing thousands of systems world wide.

(10) Evaluate the cost of cybercrimes to organizations and suggest preventive startegies

Ans

Cost of cybercrime:

1. Direct financial loss:-

Money stolen through fraud, ransomeware payments and unauthorized transactions.

2. System Repair & Recovery cost:-

Expenses for restoring servers, removing malware, and repairing damaged software.

3. forensic Investigation cost:-

Companies hire experts to trace the attack source and access data loss.

4. Legal Penalties & compliance fines:—

Organizations Pay fines for failing to protect customer data.

5. Loss of Productivity:

Employees cannot work during downtime caused by attacks like DDOS or ransomware

6. Reputation Damage: Customers loose trust, affects long term revenue and brand value

~~Employees cannot work during downtime caused by attacks like DDOS or ransomware.~~

(7) Customer loss / Business loss:—

Data breaches make customers shift to competitors

(8) Increased security Investments:—

Costs rise due to buying new security tools, training staff, and hiring experts.

9. Ip (Intellectual property) Theft

Source code, research data, and designs get stolen, reducing competitive advantage.

(10). Higher Insurance premiums:—

Cyber insurance becomes more expensive after attacks.

Preventive strategies:—

1. Conduct regular security audits:

Identify vulnerabilities before attackers exploit them.

2. Implement strong authentication (MFA)
Stops unauthorized access even if passwords are stolen.

3. Encrypt sensitive data.
Keeps data safe even if breached.

4. Train employees on phishing & social engineering.
Human awareness blocks most cybercrimes.

5. Use firewalls, IDS, and antivirus solutions.
Prevents malware, hacking attempts, and intrusion.

6. Maintain regular databackups
Helps quick recovery during ransomware attacks.

7. Follow secure coding practies
Prevents SQL injection, buffer overflow, and Web attacks.

8. Create an incident response plan.
Quick action reduces Financial and Operational damage.

9. Apply strick BYOD Policies
Controls security risks from employee-owned mobile devices.

10. Purchase cyber insurance:

Minimizes financial impact from major attacks.

11. Discuss how social computing creates challenges for organizational privacy and security.

Ans Challenges to privacy & security

1. Data leakage:

Employees may accidentally share confidential files, project details, or customer data on social media.

2. Social Engineering Attacks:-

Hackers study employee profiles to craft targeted phishing, impersonation, or scam attacks.

3. Fake Profiles & Impersonation:-

Attackers create fake accounts pretending to be company officials to mislead customers or extract data.

4. Spread of malware:-

Malicious links, attachments, and pop-ups spread easily through social networks.

5. Reputation Damage:-

Negative posts, false news, or customer complaints can go viral and harm the brand.

6. Privacy violations:-

Social platforms collect personal and behavioral data, which may indirectly expose organizational information.

7. Employee Distraction & productivity loss:-

Constant access to social platforms reduces focus and work efficiently.

(8) Unauthorized sharing of company content:-

Employees may disclose internal updates without permission.

(9) Risk from Third party Apps:-

Quiz apps, Unknown extensions, and hackers may extract both personal and organizational data.

(10) Difficulty in monitoring & control:-

Large organizations cannot easily track all employee social media activity, increasing security blind spots.

How organizations Handle These Challenges.

1. Strong social media policy.
Clear rules about what employees can and Cannot share.

2. Training employees on safe online behaviour.
Helps avoid phishing, scams, and fake apps.

3. Multi-factor authentication for official accounts.
Prevents account hijacking

4. monitoring tools for brand protection Detects fake profiles and harmful posts.

5. Limiting social media access on office networks.
Reduces distractions and security risks.