Computer Application
17 COMPUTER ETHICS AND CYBER SECURITY
www.nammakalvi.org

Part II
Answer to the following questions (2 Marks):

1. What is harvesting?

A person or program collects login and password information from a legitimate user to illegally gain access to others' account(s).

2. What are Warez?

Commercial programs that are made available to the public illegally are often called warez.

3. Write a short note on cracking.

Cracking is where someone edits a program source so that the code can be exploited or modified. A cracker (also called a black hat or dark side hacker) is a malicious or criminal hacker.

4. Write two types of cyber attacks.

Malware is a type of software designed through which the criminals gain illegal access to software and cause damage.

Types: 1. Virus, 2.Worms, 3.Spyware, 4. Ransomware

5. What is a Cookie?

A cookie is a small piece of data sent from a website and stored on the user's computer memory (Hard drive) by the user's web browser while the user is browsing internet.

Type of cookies: HTTP cookie, web cookie, Internet cookie, browser cookie, or simply cookie

Part III
Answer to the following questions (3 Marks):

1. What is the role of firewalls?(layered security)

Firewalls also vary in type depending on where communication originates, where it is intercepted, and the state of communication being traced.

2. Write about encryption and decryption.

Encryption and decryption are processes that ensure confidentiality that only authorized persons can access the information.

Encryption is the process of translating the plain text data (plaintext) into random and mangled data (called cipher-text).

Decryption reverse process of converting the cipher-text back to plaintext.

Encryption and decryption are done by cryptography

3. Explain symmetric key encryption.

Symmetric encryption is a technique to use the same key for both encryption and decryption.

(Secret key)To exchange the key used to encrypt the data before they can decrypt it

4. What are the guidelines to be followed by any computer user?

- **Honesty**: Users should be truthful while using the internet.
- **Confidentiality**: Users should not share any important information with unauthorized people.
- **Respect**: Each user should respect the privacy of other users.
- **Professionalism:** Each user should maintain professional conduct.
- **Obey The Law:** Users should strictly obey the cyber law in computer usage.
- **Responsibility:** Each user should take ownership and responsibility for their actions

5. What are ethical issues? Name some.

An Ethical issue is a problem or issue that requires a person or organization to choose between alternatives that must be evaluated as right (ethical) or wrong (unethical).

These issues must be addressed and resolved to have a positive influence in society.

Some of the common ethical issues are listed below:

Cyber crime	Use of computers to commit fraud
Software Piracy	Sabotage in the form of viruses
Unauthorized Access	Making false claims using computers
Hacking	

Part IV
Answer to the following questions (5 Marks):

1. What are the various crimes happening using computer?

Crime	Function
Crime Function	Hacking, threats, and blackmailing towards a business or a person.
Cyber stalking	Harassing through online.
Malware	Malicious programs that can perform a variety of functions including stealing, encrypting or deleting sensitive data, monitoring user's computer activity without their permission.
Denial of service attack	Overloading a system with fake requests so that it cannot serve normal legitimate requests.

Fraud	Manipulating data, for example changing the banking records to transfer money to an unauthorized account.	
Harvesting	A person or program collects login and password information from a legitimate user to illegally gain access to others' account(s).	
Identity theft	It is a crime where the criminals impersonate individuals, usually for financial gain.	
Intellectual property theft	Stealing practical or conceptual information developed by another person or company.	
Salami slicing	Stealing tiny amounts of money from each transaction.	
Scam	Tricking people into believing something that is not true.	
Spam	Distribute unwanted e-mail to a large number of internet users.	
Spoofing	It is a malicious practice in which communication is send from unknown source disguised as a source known to the receiver.	

2. What is piracy? Mention the types of piracy?
How can it be prevented

Software Piracy is about the copyright violation of software created originally by an individual or an institution.

Software Piracy is "unauthorized copying of software"

S No	Type of Piracy	Function
1	Unauthorized access	Unauthorized access is when someone gains access to a website, program, server, service, or other system by breaking into a legitimate user account.
2	Hacking	Hacking is gaining unauthorized access to s computer system without the owner's permission.
3	Cracking	Cracking is gaining unauthorized access to computer systems to commit a crime, such as stealing the code to make a copy-protected program run thus denying service to legitimate users.

Prevented Action:

To pretend being your friend and talk to you on Internet Relay Chat(**IRC**) or by Instant messenger. e-mail can also be a source for them.

They may send official e-mail requesting some sensitive information.

It may look like a legitimate e-mail from bank or other official institution.

3. Write the different types of cyber attacks

S. No	Cyber Attack	Function
1.	Virus	A virus is a small piece of computer code that can repeat itself and spreads from one computer to another by attaching itself to another computer file. **Trojan:** A Trojan virus is a program that appears to perform one function (for example, virus removal) but actually performs malicious activity when executed.
2.	Worms	Worms are **self- repeating** and do not require a computer program to attach themselves. Worms continually look for vulnerabilities and report back to the author of the worm when weaknesses are discovered.
3.	Spyware	Spyware can be installed on the computer automatically when the attachments are open, by clicking on links or by downloading infected software.
4.	Ransom ware	Ransomware is a type of malicious program that demands payment after launching a cyber-attack on a computer system. This type of malware has become increasingly popular among criminals and costs the organizations millions each year.

Book Inside Question
What is Cryptography?
Cryptography a key is a piece of information (parameter) that determines the functional output of a cryptographic algorithm. Encryption and decryption are done by cryptography
Write TYPES OF ENCRYPTION
There are two types of encryption schemes as listed below:
    1. Symmetric Key encryption   2. Public Key encryption
PUBLIC KEY ENCRYPTION Or ASYMMETRIC ENCRYPTION
Public key encryption is also called Asymmetric encryption. It uses the concept of a key value pair, a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key.

Define Asymmetric Encryption in Digital Certificates:

- A digital certificate in a client-server model of communication is one of the example of Asymmetric Encryption.
- A certificate is a package of information that identifies a user and a server.
- It contains information such as an organization's name, the organization that issued the certificate, the users' email address and country, and user's public key.

What is Digital Signature

Digital signatures are based on asymmetric cryptography and can provide assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed by the signer

Define Ethics

Ethics is a set of moral principles that govern the behavior of an individual in a society, and Computer ethics is set of moral principles that regulate the use of computers by users.

Define CYBER CRIME

Cybercrime is an intellectual, white-collar crime. Those who commit such crimes generally manipulate the computer system in an intelligent manner.

Explain some Computer crimes and their functions

Cyber crime	Function
Hacking	Hacking is gaining unauthorized access to s computer system without the owner's permission.
Cracking	Cracking is gaining unauthorized access to computer systems to commit a crime, such as stealing the code to make a copy-protected program run thus denying service to legitimate users.
Malicious	Intentionally doing harm.
Freeware	Freeware is a software available free of charge.
Shareware	Shareware is a software that is distributed free of charge on a trial basis for a limited time.
Phishing	Phishing is a term used to describe a malicious individual or group of individuals who scam users by sending e-mails or creating web pages that are designed to collect an individual's online bank, credit card, or other login information.

What is SOFTWARE PIRACY

Software Piracy is about the copyright violation of software created originally by an individual or an institution.

Software Piracy is the copyright violation of software created originally by one person and illegally used by someone else.

Software Piracy is "unauthorized copying of software"

Explain MITM(Man In The Middle)

Man-in-the-middle attack (MITM; also Janus attack) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Explain Firewall?

- A firewall is a computer network security based system that monitors and controls incoming and outgoing network traffic based on predefined security rules.
- A firewall commonly establishes a block between a trusted internal computer network and entrusted computer outside the network.
- They are generally categorized as network-based or host-based.
- **Network based firewalls** are positioned on the gateway computers of LANs [**local area Network**], WANs [**Wide Area Network**] and intranets. Host-based firewalls are positioned on the network node itself.
- **The host-based firewall** may be a service as a part of the operating system or an agent application such as endpoint **security** or **protection**.
- Each has a role in **layered security**. Firewalls also vary in type depending on where communication originates, where it is intercepted, and the state of communication being traced.

Define proxy server

A proxy server is a gateway between a local network and a larger-scale network such as the Internet. Proxy servers provide increased performance and security.

What is use cookies?

•To collect demographic information about who has visited the Web site.

• Sites often use this information to track how often visitors come to the site and how long they remain on the site.

• It helps to personalize the user's experience on the Web site.

• Cookies can help store personal information about users so that when a user subsequently returns to the site, a more personalized experience is provided.

How to PREVENTION

25% of cyber crime remains unsolved. To protect the information the following points to be noted:

- Complex password setting can make your surfing secured.
- When the internet is not in use, disconnect it.
- Do NOT open spam mail or emails that have an unfamiliar sender.
- When using anti-virus software, keep it up-to-date.

India Cyber law and IT Act 2000

- IT Act 2000 is an act to provide legal recognition for transactions carried out by means of ElectronicData Interchange(EDI) and other means of electronic communication.
- It is the primary law in India dealing with cybercrime and electronic commerce(e-Commerce). e-Commerce is electronic data exchange or electronic filing of information.
- "Cyber law or Internet law" is a term that encapsulates the legal issues related to use of the Internet.
-

What are called Fraudulent

Dishonest, cheating, swindling, corrupt, criminal, illegal, unlawful.

G.Ganesh.,M.Sc.,B.Ed.,(C.S)
PGT-COMPUTER TEACHER,
SRGDS MHSS, Thiruvannamalai.
+918508689938.
Tvmganesh1991@gmail.com