**Dr.Mahalingam College of Engineering and Technology**

**CCET- I Answer Key**

**Name of the Programmme:** Mech, Mechatronics, Auto, Civil, ECE

**Semester :** 7

**Course Code & Course Name:** 19ITOC1004 / CYBER LAW AND INFORMATION SECURITY

**Section -A**

1.**Specify the phases involved in planning cybercrime.**

* Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
* Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
* Launching an attack (gaining and maintaining the system access).

2.**Outline Cyber Crime with an example.**

* Cybercrime refers to criminal activities that are carried out using digital technology, typically over the internet.
* phishing email impersonates a bank, tricking the recipient into revealing their login credentials, leading to unauthorized access and potential financial loss.

**3. Define Phishing.**

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a genuine (legal) organization to ensnare individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

**4. Differentiate active and passive attack.**

Active attacks are usually used to alter the system, whereas passive attacks attempt to gain information about the target.

Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality.

**5. Specify the factors that contribute to outbreaks on mobile devices.**

* Enough target terminals
* Enough functionality
* **Enough connectivity**

**6. List the popular types of attacks against 3G mobile networks.**

* Malwares, viruses and worms
* Denial-of-service (DoS)
* Overbilling attack
* Spoofed policy development process
* Signaling-level attacks

7. **Compare viruses and worms.**

**viruses**

* Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
* A computer virus passes from computer to computer.

**Worms**

* A computer worm is a self-replicating malwarc computer program.
* It uses a computer network to send copies of itself to other nodes (computers to the network) and it may do so without any user intervention.

**8. Predict the use of warning labels and stamp in mobile phones.**

Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves.

These labels cannot be removed easily and are a low-cost solution to a laptop theft.

**9. Enumerate Proxy server in terms of response time.**

* Cache memory can serve all users.
* If one or more websites are requested frequently, may be by different users , it is likely to be in the proxy’s cache memory, which will improve user response time.
* There are special servers available known as cache servers.

10. **Outline the methods used to analyse the password cracking.**

* Phishing
* Social Engineering
* Key logging
* Man in the middle attack

**Section-B**

**11. a. i) Explain in detail about cybercrime and Indian ITA 2000.**

* Cybercrime is any criminal activity that involves a computer, networked device or a network.
* While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them.

Cyber crimes can be classified in to 4 major categories as the following:

1. Cyber crime against Individual
2. Cyber crime Against Property
3. Cyber crime Against Organization
4. Cyber crime Against Society

**Cyber crime against Individual**

* **Email spoofing :** A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.
* **Spamming :** Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
* **Cyber Defamation :** This occurs when defamation takes place with the help of computers and/or the Internet.

E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

* **Harassment & Cyber stalking :** Cyber Stalking Means following an individual's activity over internet.

It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

1. Credit Card Fraud :

As the name suggests, this is a fraud that happens by the use of a credit card.

This generally happens if someone gets to know the card number or the card gets stolen.

2. Intellectual Property crimes :

Software piracy: Illegal copying of programs, distribution of copies of software.

Copyright infringement: Using copyrighted material without proper permission.

Trademarks violations: Using trademarks and associated rights without permission of the actual holder.

Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

3. Internet time theft : This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

**Cyber crime Against Property**  
1. Credit Card Fraud :

* As the name suggests, this is a fraud that happens by the use of a credit card.
* This generally happens if someone gets to know the card number or the card gets stolen.

2. Intellectual Property crimes :

* Software piracy: Illegal copying of programs, distribution of copies of software.
* Copyright infringement: Using copyrighted material without proper permission.
* Trademarks violations: Using trademarks and associated rights without permission of the actual holder.
* Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

3. Internet time theft : This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

**Cyber crime Against Organization**

**(i) Unauthorized Accessing of Computer:** Accessing the computer/network without permission from the owner.

It can be of 2 forms:

a) Changing/deleting data: Unauthorized changing of data.

b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

**(ii) Denial Of Service :** When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

(iii) Computer contamination / Virus attack :

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it.

Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

(iv) Email Bombing : Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

(v) Salami Attack :

When negligible amounts are removed & accumulated in to something larger.

These attacks are used for the commission of financial crimes.

**Cyber crime Against Society**

Forgery : Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism : Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.

(iii) Web Jacking : Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

**Indian ITA 2000**

* The Information Technology Act, 2000 also Known as an IT Act is an act proposed by the Indian Parliament reported on 17th October 2000.
* This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997.

**The offences and the punishments in IT Act 2000**

The offences and the punishments that falls under the IT Act, 2000 are as follows:

• Tampering with the computer source documents.

• Directions of Controller to a subscriber to extend facilities to decrypt information.

• Publishing of information which is obscene in electronic form.

• Penalty for breach of confidentiality and privacy & Hacking for malicious purposes.

• Penalty for publishing Digital Signature Certificate false in certain particulars.

• Penalty for misrepresentation & Confiscation.

• Protected System & Power to investigate offences.

• Penalties for confiscation not to interfere with other punishments.

• Act to apply for offence or contravention committed outside India.

• Publication for fraud purposes.

• Power of Controller to give directions.

**11. b. i) With suitable illustration explain how criminals plan the attack.**

**Criminals plan passive and active attacks**.

* Active attacks are usually used to alter the system, whereas passive attacks attempt to gain information about the target.
* Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality.

**Phases involved in planning cybercrime**

Reconnaissance (information gathering) is the first phase and is treated as passive attacks.

Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.

Launching an attack (gaining and maintaining the system access).

**Reconnaissance**

The literal meaning of "Reconnaissance" is an act of reconnoitering- explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy).

In the world of "hacking," reconnaissance phase begins with "Footprinting”.

Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities.

The objective of this preparatory phase is to understand the system, its networking ports and services and any other aspects of its security that are needful for launching the attack.

Thus, an attacker attempts to gather information in two phases: passive and active attacks.

**Scanning and scrutinizing gathered information**

* Scanning is a key step to examine intelligently while gathering information about the target.
* The objectives of scanning are as follows:

Port scanning: Identify open/close ports and services.

Network scanning: Understand IP Addresses and related information about the computer network systems.

Vulnerability scanning: Understand the existing weaknesses in the system.

* The scrutinizing phase is always called "enumeration" in the hacking world.

The objective behind this step is to identify:

1. The valid user accounts or groups
2. Network resources and/or shared resources
3. OS and different applications that are running on the OS.

**Gaining and Maintaining the System Access**

After the scanning and enumeration, the attack is launched using the following steps:

* Crack the password
* Exploit he password
* Execute the malicious command/applications;
* Hide the files (if required);
* Cover the tracks - delete the access logs, so that there is no trail illicit activity.

**12.A.i) Discuss about the Attacks on Mobile-Cell Phones with an example.**

**Attacks on Mobile-Cell Phones:**

The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million.

The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito.

This virus sent SMS text messages to the organization without the users' knowledge.

2. Enough functionality:

Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all.

The expanded functionality also increases the probability of malware.

3. Enough connectivity:

Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

**12.A.ii)Describe about Proxcy Server and anonymizes and analyse how it facilitating access to content on the world wide web.**

A proxy server is an intermediary server that acts as a gateway between a user's device and the internet. It serves as a buffer between the user and the websites they visit, allowing for various functions, including enhanced security, content filtering, and improved performance.

One of the key functions of a proxy server is to anonymize user activity. This is achieved by masking the user's IP address, which is a unique identifier associated with their internet connection. When a user connects to the internet through a proxy server, the server makes requests to websites on their behalf, effectively hiding the user's original IP address. Instead, websites only see the IP address of the proxy server, adding a layer of anonymity.

This anonymization process facilitates access to content on the World Wide Web in several ways:

Bypassing Geographic Restrictions: Proxy servers can be located in different regions or countries. By connecting through a proxy server in a specific location, users can bypass geo-restrictions imposed by websites or content providers. For example, a user in one country can access content that is typically restricted to another region.

Enhancing Privacy and Security: Anonymizing through a proxy server helps protect user privacy. It prevents websites and online services from tracking a user's online activities based on their IP address. Additionally, it adds a layer of security by acting as a buffer against direct connections to potentially malicious websites.

Content Filtering and Parental Controls: Proxy servers can be configured to filter out specific types of content, such as adult material or certain categories of websites. This is especially useful for organizations and parents who want to control the type of content accessed through their network.

Load Balancing and Performance Optimization: Proxy servers can distribute network traffic across multiple servers. This helps to balance the load and improve the overall performance of the network by reducing the burden on individual servers.

Caching Frequently Accessed Content: Proxy servers can store copies of frequently accessed content locally. When users request that content, the proxy can deliver it directly from its cache, reducing the need to fetch the content from the original server. This can significantly improve page load times.

**12.B.i)Describe about Security and Privacy implications from cloud computing.**

Security and privacy implications from cloud computing

Cloud computing is one of the top 10 Cyber Threats to organizations. There are data privacy risks through cloud computing.

Organizations should think about privacy scenarios in terms of “user spheres”.

1. User sphere:

Here data is stored on users’ desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc.

Organization’s responsibility is to provide access to users and monitor that access to ensure misuse does not happen.

2. Recipient sphere:

Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data.

Organizations responsibility is to minimize users privacy risk by ensuring unwanted exposure of personal data of users does not happen

3. Joint sphere:

Here data lies with web service provider’s servers and databases. This is the in between sphere where it is not clear to whom does the data belong.

Organization responsibility is to provide users some control over access to themselves and to minimize user’s futures privacy risk.

**12.B.ii)Predict tools used to spread viruses through the internet with neat diagram.**

Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus.

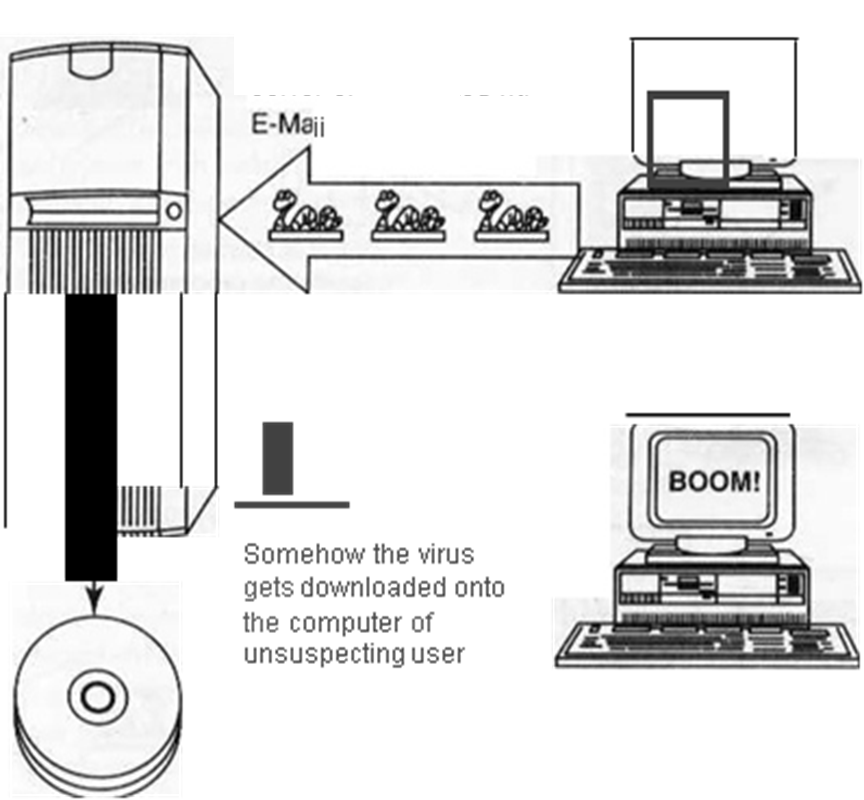
2. delete files inside the system into which viruses enter

3. scramble data on a hard disk

4. cause erratic screen behavior

5. halt the system (PC)

6. just replicate themselves to propagate further harm



The Internet server and hard disk are infected with the virus or the server facilitates distribution of the virus

Viruses are intentially uploaded to an Internet server or distributed via E-mail