Internal Assessment Test 1 – June 2024

Solution

Sub:	Introduction To Cyber Security(Open Elective Course)					Sub Code:	21CS653	Branch :	ECE,ME
Date:	05/06/2024	Duration:	90 mins	Max Marks:	50	Sem / Sec:	VI		

1	Define Cybercrime and Cyber security. List and explain types of Cyber criminals. Sheme: Definition of cybercrime and cyber security - 2MARKS 3 different types of cybercriminals and examples with explanation-8MARKS Solution Cybercrime :Definition: "A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime Cyber security: Is the protection of internet-connected systems, including hardware, software and data, from cyber attacks". Types of Cyber criminals. They can be categorised into three groups that reflect their motivation. We have three types of Cybercriminals Type I: Cybercriminals hungry for recognition Type II: Cybercriminals not interested in recognition Type III: Cybercriminals the insiders <u>Type I: Cybercriminals-Hungry for recognition</u> • Hobby hackers • IT professionals: ethical hacker • Politically motivated hackers • Terrorist organizations <u>Type II: Cybercriminals-not interested in recognition</u> • Psychological perverts • Financially motivated hackers (corporate espionage): make money from cyberattacks

	• State sponsored hacking (National espionage or sabotage): Extremely • professional groups working for governments. • Organized criminals <u>Type III: Cybercriminals the insiders</u> • Dissatisfied or former employees seeking revenge. • Competing companies using employees to gain economic. • advantage through the damage for theft.
2	Write a short note for below: a)Cyber defamation b)Salami attack c)Data diddling d)Software piracy e)Mail bombs **Scheme** :For each question give cybercrime classification and explanation – 2MARK <u>a)Cyber defamation:</u> This comes under classification **Cybercrime against Individual.** • It is a cognizable(evident) offense. • Cyber defamation occurs when defamation takes place with • the help of a computer and/or internet. • For example: someone publishing defamatory matter about someone on a website or send emails contain defamatory information to all friends of that person. • <u>b)Salami attack</u> This comes under classification **cybercrime against Organization.** • These attacks are used for committing financial crimes • The idea here is to make the alteration so insignificant that ina single case it would go completely unnoticed; • For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month. <u>c)Data diddling :</u> This comes under classification **Cybercrime against Organization** • A data diddling (data cheating) attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. • Example :employee manipulate financial records to divert funds to their own account once funds sent changes record to original form. <u>d)Software piracy:</u>This comes under classification **Cybercrime against Organization**

	• "software piracy" : is theft of software through the illegal copying of genuine programs or the counterfeiting anddistribution of products intended to pass for the original. Different menthod of s/w piracy • **end-user copying:**friends loaning disks to each other • **hard disk loading with illicit means**: hard disk vendors load pirated software; • **counterfeiting**: large-scale duplication and distribution of illegally copied software; • **Illegal downloads** from the Internet: e)Mail bombs This comes under classification **Cybercrime against Organization** • E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account(in the case of an individual) or to make victim's mail servers crash (in the case of a company or an E-Mail service provider). • Computer program can be written to instruct a computer to do such tasks on a repeated basis. In recent times, terrorism has hit the Internet in the form of mail bombings. • By instructing a computer to repeatedly send E-Mail to a specified person's E-Mail address, the cybercriminal can overwhelm the recipient's personal account and potentially shut down entire systems.
3	Discover the classification of Cybercrime for below scenarios and explain in brief each scenario: a)Sending spoofed E-mail. b)Using the Internet hours paid by another person. c)Forcefully taking control of website. d)Using Internet to stop normal functioning of computer. e)Illegal and unethical theft of business trade secret. Scheme ● For each question give cybercrime classification- 1 MARK ● And mention the name of cybercrime and briefly explain -1MARK a**) E-mail Spoofing.** • Classification:Cybercrime against Individual • A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source. • Example: email address of Roopa -→roopa@cmrit.ac.in someone else say x person spoof her email and sends vulgar messages to all her contacts. b)Using the Internet hours paid by another person: **Internet Time Theft** • Classification: Cybercrime against Property Such a theft occurs when an unauthorized person

	• uses the Internet hours paid for by another person.Basically, Internet time theft comes under hackingbecause the person who gets access to someone else's ISP user ID and password, either by hackingor by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge . c)Forcefully taking control of website : **Web jacking** Classification: Cybercrime against Society ● Occurs when someone forcefully takes control of a website (by cracking the password and later changing it). ● Thus, the first stage of this crime involves "password sniffing"(password finding). ● The actual owner of the website does not have any more control over what appears on that web. d)Using Internet to stop normal functioning of **computer Sabotage(crime against individual)** The use of the Internet to stop the normal functioning of a computer system through the introduction of worms, viruses or logic bombs, is referred to as computer sabotage. e)Illegal and unethical theft of business trade secret:**Industrial spying** Classification: **Cybercrime against organization**. ● Industrial spying is the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. ● It may include the theft of intellectual property, such as manufacturing processes, chemical formulas, recipes, techniques, or ideas.
4	Explain phases of how criminals plan the attack. Scheme: Three phases listed carries -1 marks Explain each phases - 3 *3 marks Phase 1:Reconnaissance Phase 2: Scanning and scrutinizing the gathered information Phase 3: Launching an attack and gaining and maintaining the system access. Phase 1:Reconnaissance ● It is an act of reconnoitering- explore, often with the goal of finding something or somebody (gain information about enemy potential enemy). ● In the world of "hacking," reconnaissance phase begins with foot printing this is the

	preparation toward preattack phase, and involves accumulating data about the target environment and computer architecture to find ways to intrude into that environment. ● 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. Two phases: passive and active attacks. Passive attack This Phase Involves gathering information about the target without his/her knowledge. Google or Yahoo search locate information about employees Surfing online community groups Facebook to gain information about an individual Organizations website may provide personal directory or information about the key employees used in social engineering attack to reach the target. Blogs news groups press releases etc., Going through job posting/job profile. Active Attacks: • It involves probing the network to discover individual host to confirm the information (IP address, operating system type and version, and services on the network) gathered in the passive attack phase. • Also called as"Rattling the Doorknobs" or "Active Reconnaissance" • Can provide confirmation to an attacker about security measures in place or not but also increases the chances of attacker being caught by system. Phase 2: Scanning and scrutinizing the gathered information: Is a key to examine intelligently while gathering information about the target The objectives are: 1.Port scanning:Identify open/close ports 2. Network scanning: Understand ip address related information 3. Vulnerability scanning: understanding weakness of system. Phase 3: Launching an attack and gaining and maintaining the system access. After scanning and scrutinizing (enumeration) the attack is launched using the following steps. 1. Crack the password 2. Exploit the privileges 3. Execute the malicious command or application 4. Hide the files 5. Cover the tracks- delete access logs, so that there is no 6. trial illicit activity
5	a)What is Social engineering? b)List and explain types of social engineering. Social engineering definition- 1 mark

Different types of social engineering explained – 9 mark

Social engineering Is a “Technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.

- Classification of social engineering
- Human based Social Engineering

Classification of social engineering:It refers to person to person interaction to get the required/desired information.

Impersonating an employee or valid user: Impersonation" (e.g.. posing oneself as an employee of the same organization) is perhaps the greatest techniques used by SE to deceive people.

Posing as an important user: The attacker pretends to be an important user for example a chief Executive Officer(CEO) or high-level manager who needs immediate assistance to gain access to a system.

Using a third person:An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorised personnel is on vacation .

Calling technical support:Help-desk and technical support personnel are trained to help users, which makes them good prey for Social Engineering attacks.

Shoulder surfing :It is a technique of gathering information such as usernames and passwords by watching over a person’s shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.

Dumpster diving : It involves looking in the trash for information written on pieces of paper or computer printouts.

Computer based Social Engineering:It uses a computer software/Internet to get the required/ desired information.

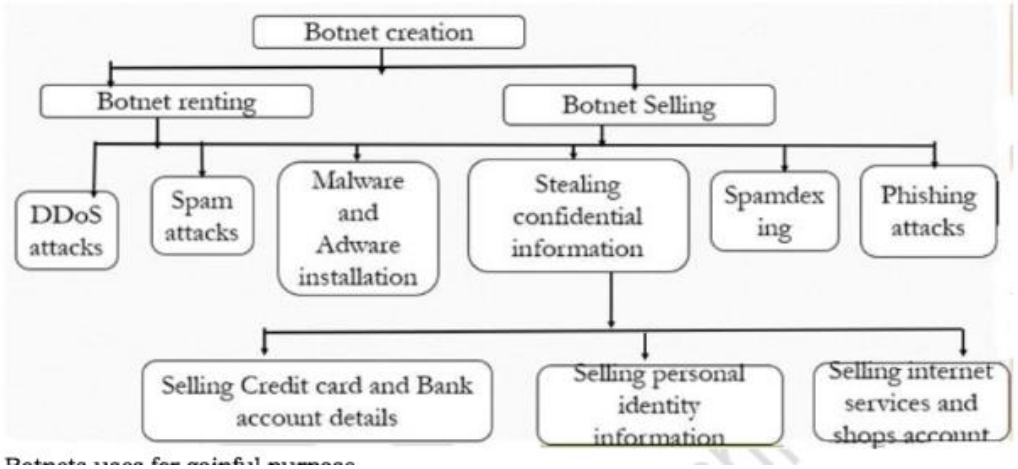
Fake E-Mails
An attacker sends emails to numerous users in such that the user finds it as legitimate mail. This activity is called as Phishing. Free websites are
available to send fake emails. One can observe here that "To" in the text box is a blank space.Phishing involves false emails, chats or websites
designed to impersonate real systems with the goal of capturing sensitive data.

E-Mail attachment
E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g. keylogger utility to capture passwords)
get executed.Viruses. Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

Pop-up windows
Pop-up windows are also used. in a similar manner to E Mail attachments Pop-up windows with special offer free stuff encourages to install malicious s/w.

6	a)Describe Zombie network and List different attack launched with attack vector. b)Define bot and botnet. With a diagram explain how botnet create business. Scheme Describe Zombie network - 2 MARKS and List different attack launched with attack vector- 3 MARKS ● A botnet (also known as a zombie network) is a number of network computer infected with malicious program, that allows cyber criminals to control the infected machines remotely without users knowledge. ● Botnet:Collection of bot that run autonomously and automatically. ● One can gain control of your system by infecting them with virus, malicious code.So your computer maybe part of botnet even though it appears to be normal. ● Botnet can conduct activities like spam/virus distribution, DOS attacks. Different ways to launch Attack By attack vector Attack Vector :An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcomes. 1) Attack by E-mail: 2)Attachments: 3)Attacks by deception: social engineering/hoaxes 4)Hackers 5)Heedless guests (attack by webpages):Heedless(careless) guest visiting fake website. 6)Attack of the worms 7)Malicious macros 8)Foistware (sneakware):Foistware is a term used to describe software downloaded to a computer without the owner's knowledge. 9)Viruses:malicious computer code. Scheme Definition of bot and botnet-1 MARK With a diagram explain how botnet create business-4MARK Bot: “ An automated program for doing some particular task, often over a network” ex:chatbot(used in business for customer service),spam bots Botnet:Collection of bot that run autonomously and automatically.

Explain with neat diagram how Botnets create business and used for gainful



- Zombie networks have become a source of income for entire groups of cybercriminals.
- If someone wants to start a business and has no programming skills, there are plenty of Bot for sale offers on forums.
- Obfuscation and encryption of these programs code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet. Figure shows how Botnet creates business.