Security is Individual Responsibility

♠♣♦►Disclaimer◄♦♣♠

This course is to know about the cyber security issues in real time, tools, demonstrations will be used to make you understand better. Trying yourself for bad motive or threatening, or abusing others leads to punishable from Law and for all your bad motive you are only responsible for your act.

The course coordinator is not responsible.

Suggestion / Input / Guidance

Learn by DOING

Earn Certifications in Cyber Security

Practice only makes you cyber professional

Course Objectives and Course Outcomes (Cos)

Course objectives:

This course will enable students to

1. Understand the importance of cyber security practice in day-to-day life.
2. Learn the key terminologies used in the cyber security domain.
3. Understand the tools and technologies used by the cyber security domain.
4. Gain familiarity with the security concepts in the various levels of security.
5. Learn the forensic science life cycle and IPR.

Course outcomes:

The students will be able to:

CO1: Explore the Cyber Security and IPR Principles.

CO2: Apply the cyber security concepts to secure from cyber-attacks.

CO3: Formulate the possibilities of cyber-attacks in a given usecase, as a penetration tester.

CO4: Analyze cyber security tools to protect individual data.

CO5: Apply Digital Forensic tools to address cyber security issues.

Pre requisites for the course:

Understanding of the Operating Systems, like Windows and Linux, Basic Programming skills, Analytical skills and self-learning capability of latest tools. And also understanding of basics of Networks, clouds and databases.

Post requisites for the course:

Continuous up-gradation on latest cyber security technologies.

Instructions to students:

Learn scanning and finding vulnerabilities in systems and networks.

Open Ended Problems: ------

Fast Learners are encouraged to involve in proactive design technologies for cyber security issues.

Scheme of Evaluation

CIE:

- **50% of CIE is based on Internal Assessments – Average of 3 tests will be taken**
- **50% of CIE is based on Alternate Assessment Methods**

SEE:

- **SEE will be conducted for 100 marks.**

Module-1 Topics to be discussed:

Introduction to Cybercrime & Security:
Cybersecurity Foundation Concepts -
Cybercrime and Information Security, who are Cyber criminals.
Classifications & Categories of Cybercrimes, Social Engineering.
Cyber stalking, Cybercafé & How Criminals Plan Attacks, Botnets.
Attack Vector, Introduction to Defensive Cybersecurity & Offensive Cybersecurity.
Difference between Defensive Cybersecurity & Offensive Cybersecurity.
Principles of Defense and Offense.

Introduction, Cybercrime: Definition and Origins of the word

The following websites will give information about the cyber crimes, data threat and severity Of cybersecurity to be addressed by Engineers and Academicians.

1. https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
2. https://threatmap.checkpoint.com/

Q Which is the Weakest link in Cyber Security?

a. Technology
b. E-Devices
c. Human
d. None of the above

Exercise-1

Explore the few more sources of attack Map and List them and prepare documentary evidence for the same.

Introduction

- Internet in India growing rapidly
- Unrestricted number of free websites, the Internet has deniably opened a new exploitation known as cybercrime
- Activities involve the use of computer, Internet, Cyberspace and WWW
- 1st recorded cybercrime took place in the year 1820
- **26,100 Indian websites** were hacked during 2020 (source: https://www.business-standard.com/article/technology/over-26-100-indian-websites-were-hacked-during-2020-dhotre-121021101179_1.html)
- 2,000 Indian websites hacked in **June-July 2022**, highest threat from Far East (Source: https://www.business-standard.com/article/current-affairs/)

Cyberspace: (by William Gibson in 1984)

- Worldwide network of Computer networks that uses the TCP/IP for communication to facilitate transmission and exchange of data

Cybersquatting:

- Means registering, selling or using a domain name with intent of profiting from goodwill of someone else's trademark

Cyberpunk: (by Bruce Bethke, 1980)

- Mean something like "anarchy via machine" or "machine/ computer rebel movement"

Cyberwarfare:

- Means information warriors unleashing vicious attacks against an unsuspecting opponent's computer networks, wreaking havoc and paralyzing nations.

Cyberterrorism: (by Barry Collin, 1997)

- Use of disruptive activities, or the threat, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives

Cybercrime and information Security, Who are Criminals

"A crime conducted in which a computer was directly or significantly instrumental"

"Cybercrime is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them."

Computer related crime, Computer crime, Internet crime, E-crime, High-tech crime etc. are synonymous terms

Cybercrime: Definition and Origins of the Word

Few definition of Cyber Crime:

- A crime committed using a computer and the Internet to steal person's identity
- Crime completed either on or with a computer
- Any illegal activity done through the Internet or on the computer
- All criminal activities done using the medium of computers, the Internet, cyberspace and WWW

Electronic devices

www.facebook.com/onlineenglishteacher101

Source: https://i.pinimg.com/originals/8f/79/e8/8f79e84d7fd928e90ecb98845c35942e.jpg

Types of attack

- Techno-crime:

A premeditated act against a system or systems with the intent to copy, steal, corrupt or otherwise deface or damage part of or the complete computer system

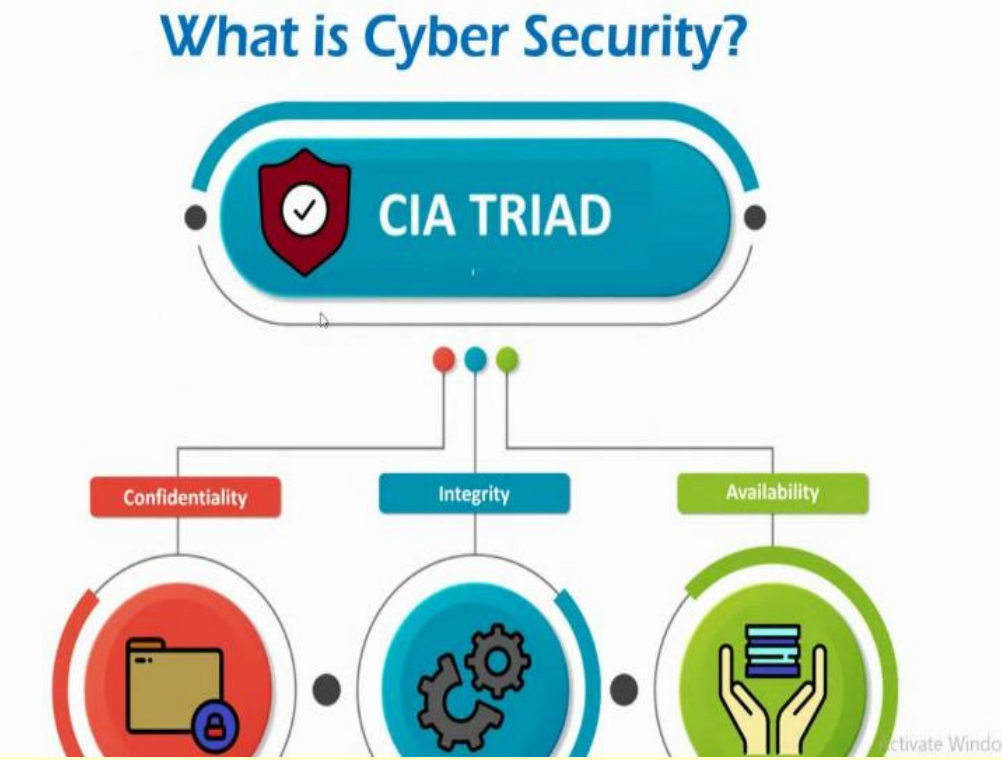
Possible when computer connected with the Internet 24 X 7

- Techno- vandalism :

These acts of “brainless” defacement of websites and/or other activities, such as copying files and publicizing their contents publicly

Cybercrime and Information Security

Cybersecurity means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.



Who are cybercriminals?

Categorized in 3 groups:

- Type I: Cybercriminals-
  - hungry for recognition
  - Hobby hackers
  - IT professionals
  - Politically motivated hackers
  - Terrorist organizations

- Type II: Cybercriminals-
  - ► not interested in recognition
  - ► Psychological perverts
  - ► Financially motivated hackers
  - ► State-sponsored hacking
  - ► Organized criminals

- Type III: Cybercriminals-
  - ► the insiders
  - ► Former employees seeking revenge
  - ► Competing companies using employees to gain economic advantage through damage and/or theft

Classification of Cybercrimes

1. Cybercrime against individual:

- E-Mail spoofing and other online fraud
- Phishing
- Spamming
- Cyber defamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses

2. Cybercrime against property:

- Credit card frauds
- Intellectual property crime
- Internet time theft

3. Cybercrime against organization:

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus
- E-Mail bombing
- Salami attack
- Logic bomb
- Trojan horse
- Data diddling
- Industrial spying
- Crimes emanating from Usenet newsgroup
- Computer network intrusions
- Software piracy

4. Cybercrime against society:

- Forgery
- Cyberterrorism
- Web jacking

5. Crimes emanating from Usenet newsgroup:

- Usenet group may carry very offensive, harmful, inaccurate or otherwise inappropriate material or postings that have been misplaced or are deceptive in another way

E-mail Spoofing:

A spoofed email is one in which e-mail header is forged so that 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.

- Difficult to control
- In context of “search engine spamming”, spamming is alternation or creation of a document with the intent to deceive an electronic catalog or filing system

Cyber Defamation:

- Cognizable offense
- 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.

Internet Time Theft

- The usage of the Internet hours by an unauthorized person which is actually paid by another person
- Comes under hacking

Salami Attack / Salami Technique

♣ When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

Data diddling:

♣ This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Forgery:

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

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.

Industrial spying / Industrial espionage:

♣ "Spies" can get information about product finances, research and development and marketing strategies, an activity known as Industrial spying.

Hacking:

♣ Every act committed toward breaking into computer and/or network is hacking

♣ The purpose of hacking Power, publicity, revenge, adventure, desire to access forbidden information, destructive mindset

Online Frauds:

♣ Spoofing website and E-Mail security alerts, lottery frauds, virus hoax E-Mail.

Pornographic offenses:

♣ Child pornography means visual depiction

Software Piracy:

♣ Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

♣ Illegal copying of programs, distribution of copies of software

Computer Sabotage

♣ The use of the Internet to hinder the normal functioning of a computer system through the introduction of worms, viruses or logical bombs is referred to as computer sabotage

E-mail Bombing / Mail Bombs:

♣ Sending a large no. of E-Mails to the victim to crash victim's E-Mail account or to make victim's server crash

Usenet Newsgroup as the Source of Cybercrimes

♣ Usenet is a popular means of sharing and distributing information on the web with respect to specific subjects or topic

♣ Following criminal use Usenet:

- Distribution/sale of pornographic material
- Distribution/sale of pirated software package
- Distribution of hacking software
- Sale of stolen credit card number
- Sale of stolen data/stolen property

Computer Network Intrusions

♣ Crackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert trojan horse or change username and passwords

Password Sniffing:

♣ Programs that monitor and record the name and password of network users as they login at a site

Exercise-2

♣ Credit Card Frauds

♣ Newsgroup Spam / Crimes Emanating from Usenet Newsgroup

How Criminals Plan the Attacks,

Phases involved in planning cybercrime:

i. Reconnaissance:

Information Gathering, first phase, passive attack

ii. Scanning and scrutinizing the gathered information

For validity of the information as well as to identify the existing vulnerabilities

iii. Launching an attack

Gaining and maintaining the system access

Types of Attacks

- Active Attack
  - Used to alter system
  - Affects the availability, integrity and authenticity of data
- Passive Attack
  - Attempts to gain information about the target
  - Leads to breaches of confidentiality
- Inside Attack
  - Attack originating and / or attempted within the security perimeter of an organization
  - Gains access to more resources than expected
- Outside Attack
  - Is attempted by a source outside the security perimeter
  - May be an insider or an outside, who is indirectly associated with the organization
  - Attempted through internet or remote access connection

Reconnaissance :

- A Reconnaissance attack occurs when an adversary tries to learn information about your network
- Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities
- Reconnaissance is also known as information gathering
- Reconnaissance is somewhat analogous to a thief investigating a neighborhood for vulnerable homes, such as unoccupied residence or a house with an easy-to-open door or windows. In many cases, intruders look for vulnerable services that they can exploit later when less likelihood that anyone is looking exists.
- Is the preparatory phase to understand the system, its networking ports and services and other aspects of security, that are needful for launching the attack
- An attacker attempts to gather information in two phases
  - Passive attacks
  - Active attacks

Passive Attacks:

- Involves gathering information about the target without his/ her knowledge.
- Google or yahoo search: to locate information about employees
- Surfing online community group: facebook; to gain information about an individual
- Organizations website: for personnel directory or information about key employees; used in social engineering attack to reach the target
- Blogs, newsgroups, press releases, etc
- Going through job postings
- Network sniffing: information on Internet Protocol address ranges, hidden servers or networks or services on the system.

Tools used during passive attacks

- Google earth
- Internet Archive: permanent access for researchers , historians and scholars to historical collections
- Professional community:
- linkedIn
- People Search
- Domain Name Confirmation
- WHOIS
- Nslookup
- Dnsstuff
- Traceroute
- VisualRoute
- TraceTrackerPro
- HTTrack and many more….

Active Attacks Rattling the doorknobs Active reconnaissance

- Involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
- Can provide confirmation to an attacker about security measures in place.

Tools used during active attacks

- **Arphound**
- **Arping**
- **Bing**
- **Bugtraq**
- **Dig**

Tools used during active attacks contd..

- DNStacer
- Dsniff
- Filesnarf
- FindSMB
- Hmap
- Hping
- Hunt
- Netcat
- Nmap
- TCPdump
- TCPreplay and many more …..

Scanning and Scrutinizing gathered information

- Is a key step to examine intelligently while gathering information about the target.
- The objectives are:
  - Port scanning
  - Network scanning
  - Vulnerability scanning

Exercise-3:

a) Explore about Jonathan James

b) Lizard Squad

What is Port Scanning?

- The act of systematically scanning a computer's ports.
- Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer.
- It is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked.
- There is no way to stop someone from port scanning your computer while you are on the Internet because accessing an Internet server opens a port, which opens a door to your computer.
- There are, however, software products that can stop a port scanner from doing any damage to your system.

What is Port Scanning? Continued…

- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two of the protocols that make up the TCP/IP protocol suite which is used universally to communicate on the Internet.
- Each of these has ports 0 through available so essentially there are more than 65,000 doors to lock.
- The first 1024 TCP ports are called the Well-Known Ports and are associated with standard services such as FTP, HTTP, SMTP or DNS.
- Some of the addresses over 1023 also have commonly associated services, but the majority of these ports are not associated with any service and are available for a program or application

Port scan

- A port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.
- The result of a scan on a port is usually generalised into one of the following categories:
  - Open or accepted
  - Closed or not listening
  - Filtered or blocked.

Types of port scans:

- vanilla: the scanner attempts to connect to all 65,535 ports
- strobe: a more focused scan looking only for known services to exploit
- fragmented packets: the scanner sends packet fragments that get through simple packet filters in a firewall
- UDP: the scanner looks for open UDP ports
- sweep: the scanner connects to the same port on more than one machine
- FTP bounce: the scanner goes through an FTP server in order to disguise the source of the scan
- stealth scan: the scanner blocks the scanned computer from recording the port scan activities.

Scrutinizing phase Called as "enumeration" in the hacking world

- The objective behind this step is to identify:
- The valid user accounts or groups
- Network resources and/or shared resources
- OS and different applications that are running on the OS.

Exercise-3

a) Research on any 5 vulnerabilities and prepare a report of the vulnerability

b) Research on any 3 Cyber-attacks and prepare a report of how the attack was performed (i.e., details of the flaws), the loss occurred and what was compromised

Attack (Gaining and Maintaining the System Access)

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

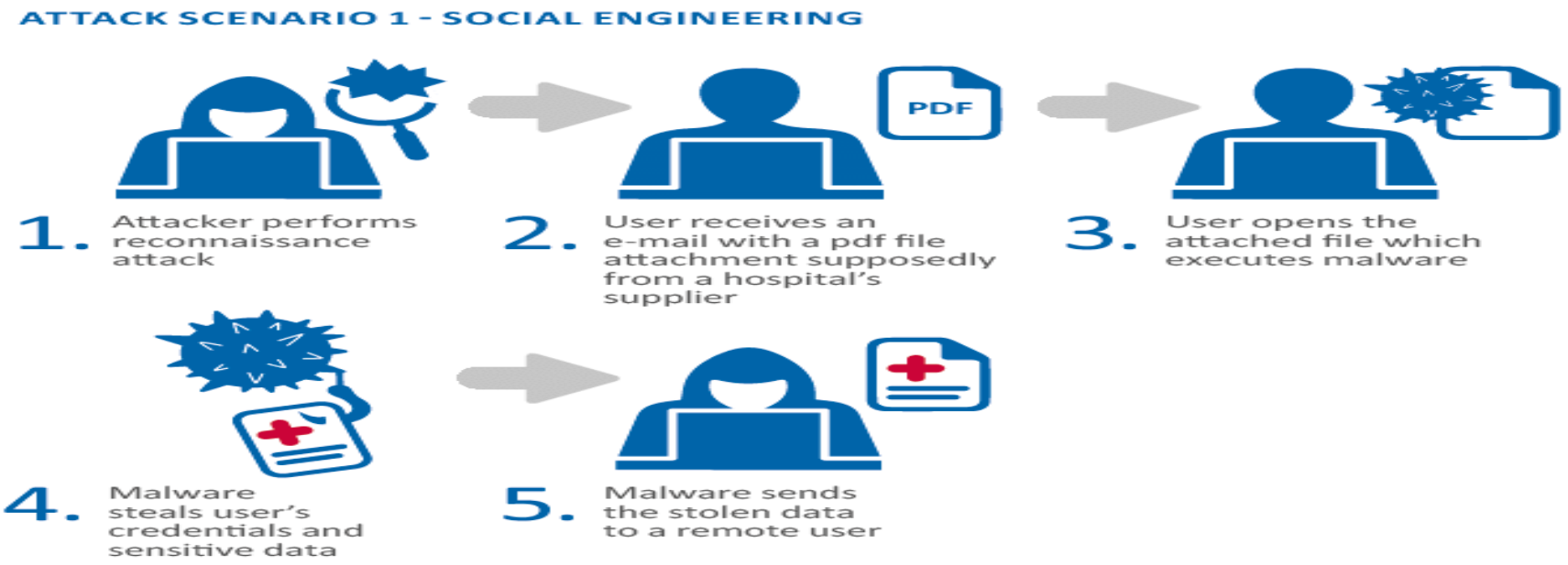
- Crack the password
- Exploit the privileges
- Execute the malicious command/ applications
- Hide the files
- Cover the track – delete access logs, so that there is no trail illicit activity.

Social Engineering

- Technique to influence and persuasion to deceive people to obtain the information or perform some action.
- A social engineer usually uses telecommunications or internet to get them to do something that is against the security practices and/ or policies of the organization.
- SE involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people.

Social Engineering continued..

- Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.
- A social engineer runs what used to be called a "con game."or example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security.
- Social engineers often rely on the natural helpfulness of people as well as on their weaknesses.
- They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.



Classification of Social Engineering

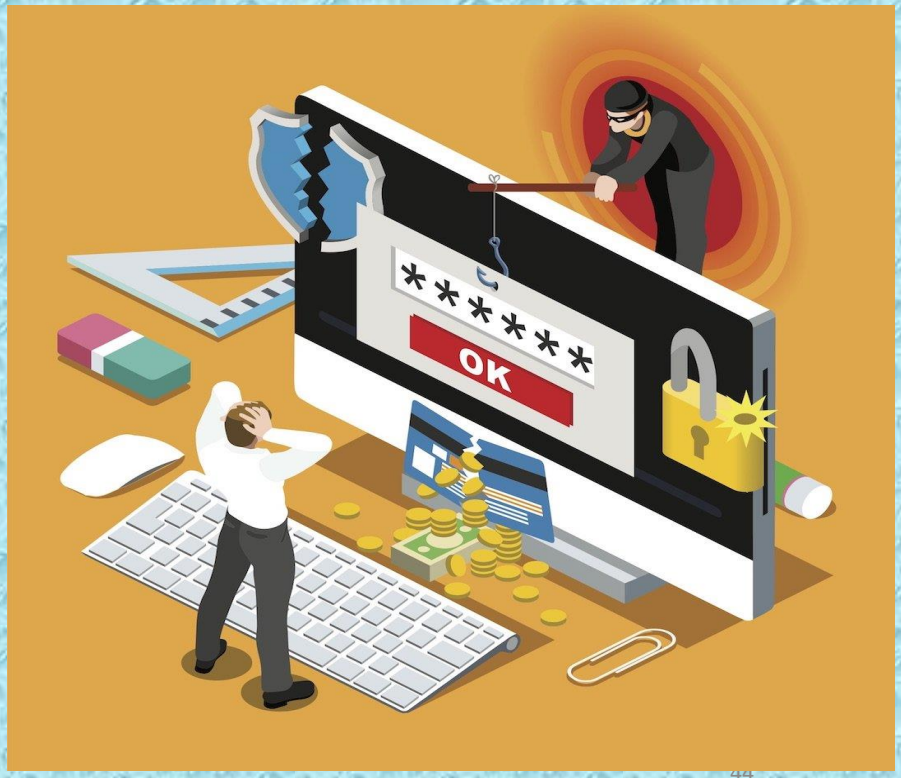
1. Human-Based Social Engineering

- needs interaction with humans; it means person-to-person contact and then retrieving the desired information. People use human based social engineering techniques in different ways; the top popular methods are:
- Impersonating an employee or valid user
- Posing as an important user
- Using a third person
- Calling technical support
- Shoulder surfing Dumpster diving

2. Computer –Based Social Engineering

Computer-based social engineering uses computer software that attempts to retrieve the desired information.

- Fake S
- Attachments
- Pop-up windows



1.1. Impersonation

- In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor.
- To attackers, sets of valid credentials are a coveted asset. An attacker who has obtained valid user credentials through social engineering techniques has the ability to roam the network with freedom searching for valuable data.
- In log data, the attacker's activities are easily hidden due to the inability to see the subtle differences in behaviors and access characteristics. Yet, this phase of the classic attack chain often represents the lengthiest portion of the attack.

1.2. Posing as an important user

- —In this type of attack, the hacker pretends to be a VIP or high-level manager who has the authority to use computer systems or files.
- Most of the time, low-level employees don't ask any questions of someone who appears in this position.

1.3. Being a third party

- —In this attack, the hacker pretends to have permission from an authorized person to use the computer system. It works when the authorized person is unavailable for some time.

1.4. Desktop support

- —Calling tech support for assistance is a classic social-engineering technique.
- Help desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

1.5. Shoulder surfing

- Shoulder surfing—Shoulder surfing is the technique of gathering passwords by watching over a person's shoulder while they log in to the system.
- A hacker can watch a valid user log in and then use that password to gain access to the system.

1.6. Dumpster diving

- —Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts.
- The hacker can often find passwords, filenames, or other pieces of confidential information like SSN, PAN, Credit card ID numbers etc
- Also called dumpstering, binning, trashing, garbaging or garbage gleaning.
- scavenging

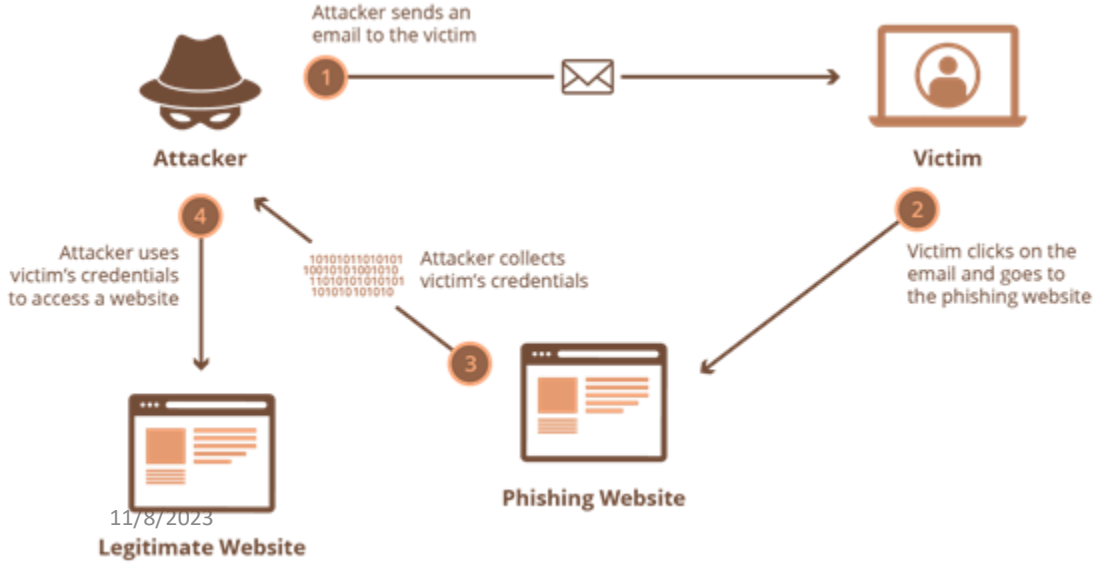
Exercise-4:

a) Prepare at least 4 scenarios of any Social Engineering attacks.

b) Try to find out, have you been hacked haveibeenpwned web site

2.1 Fake S

- —Phishing involves false s, chats, or websites designed to impersonate real systems with the goal of capturing sensitive data.
- A message might come from a bank or other well-known institution with the need to "verify" your login information.
- It will usually be a mocked-up login page with all the right logos to look legitimate.
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- They replaced "f" by "ph"



2.2 Baiting:

- —Baiting involves dangling something you want to entice you to take an action the criminal desires.
- It can be in the form of a music or movie download on a peer-to-peer site or it can be a USB flash drive with a company logo labeled "Executive Salary Summary Q1 2013" left out in the open for you to find.
- Then, once the device is used or downloaded, the person or company's computer is infected with malicious software allowing the criminal to advance into your system.

2.3 attachments

- — s sent by scammers may have attachments that include malicious code inside the attachment. Those attachments can include keyloggers to capture users' passwords, viruses, Trojans, or worms.

2.4 Pop-up windows

- Sometimes pop-up windows can also be used in social engineering attacks.
- Pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

Don't become a victim

- **Slow down. Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.**
- **Research the facts. Be suspicious of any unsolicited messages. If the looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.**
- **Delete any request for financial information or passwords. If you get asked to reply to a message with personal information, it's a scam.**
- **Reject requests for help or offers of help. Legitimate companies and organizations do not contact you to provide help.**
- **If you did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, answer your question, etc., a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations on your own to avoid falling for a scam.**

Don't become a victim continued…1

- Don't let a link in control of where you land. Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in will show the actual URL at the bottom, but a good fake can still steer you wrong.
- hijacking is rampant. Hackers, spammers, and social engineers taking over control of people's accounts (and other communication accounts) has become rampant.
- Once they control someone's account they prey on the trust of all the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an with a link or attachment check with your friend before opening links or downloading.
- Beware of any download. If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.
- Foreign offers are fake. If you receive from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

Don't become a victim continued…2

- **Set your spam filters to high. Every program has spam filters. To find yours, look under your settings options, and set these high–just remember to check your spam folder periodically to see if legitimate has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your provider plus the phrase 'spam filters'.**
- **Secure your computing devices. Install anti-virus software, firewalls, filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn't automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks.**

Cyberstalking

- Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization.
- It may include false accusations, defamation, slander and libel.
- It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.
- Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking.
- Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as or instant messaging (IM), or messages posted to a Web site or a discussion group.
- A cyberstalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.
- Cyberstalking messages differ from ordinary spam in that a cyberstalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

Types of Stalkers

- online Stalkers
- offline stalkers.

- Both are criminal offenses.
- Both are motivated by a desire to control, intimidate or influence a victim.
- A stalker may be an online stranger or a person whom the target knows.
- He may be anonymous and solicit involvement of other people online who do not even know the target.

How stalking works? Personal information gathering

- Establish a contact with the victim through telephone/ cell phone. – start threatening or harassing
- Establish a contact with the victim through .Keep sending repeated s asking for various kinds of favors or threaten the victim.
- Post victim's personal information on any website related to illicit services.
- Whosoever comes across the information, start calling the victim on the given contact details, asking for sexual services.
- Some stalkers may subscribe/ register account of the victim to innumerable pornographic and sex sites, bez of which victim start receiving such kind of unsolicited s

Cybercafé and Cybercrimes

- An Internet café or cybercafé is a place which provides Internet access to the public, usually for a fee / free.
- According to Nielsen Survey on the profile of cybercafes users in India:
- 37% of the total population use cybercafes
- 90% of this were males in age group years
- 52% graduates and post graduates> 50% were students

Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.

Role of Cybercafe

- used for either real or false terrorist communication.
- for stealing bank passwords, fraudulent withdrawal of money
- Keyloggers or spywares
- Shoulder surfing
- For sending obscene mails to harass people.
- They are not network service providers according to ITA2000
- They are responsible for “due deligence”

Illegal activities observed in Cybercafes

- Pirated softwares: OS, browser, Office
- Antivirus software not updated
- Cybercafes have installed “deep freeze” software
- This software clears details of all activities carried out, when one clicks “restart” button.
- Annual Maintenance Contract(AMC): not in place
- Is a risk bez a cybercriminal can install Malacious code for criminal activities without any interruption
- Pornographic websites and similar websites are not blocked
- Owners have less awareness about IT Security and IT Governance.
- IT Governance guide lines are not provided by cyber cell wing
- No periodic visits to cybercafes by Cyber cell wing(state police) or Cybercafe association

Safety and security measures while using the computer in Cyber Cafe

Always Logout:

- do not save login information through automatic login information
- Stay with the computer
- Clear History and temporary files

Be alert:

- don’t be a victim of Shoulder surfing
- Avoid Online Financial Transaction
- Change passwords
- Virtual Keyboards
- Security warnings

Botnets: The fuel for Cybercrime

- Bot: " an automated program for doing some particular task, often over a network"
- A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.
- Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator.
- Most computers compromised in this way are home-based.
- According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet

Botnet used for gainful purposes

- Botnet creation
- Botnet renting
- Botnet Selling
- DDoS attacks
- Spamdexing
- Phishing attacks
- Malware and Adware installation
- Spam attacks
- Stealing confidential information
- Selling Credit card and bank account details
- Selling internet services and shops account
- Selling personal identity information

Ways to secure the system

- Use antivirus and anti-spyware
- Install updates
- Use firewall
- Disconnect internet when not in use
- Don’t trust free downloads
- Check regularly inbox and sent items
- Take immediate action if system is infected

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 outcome.
- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception.
- All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.

To some extent, firewalls and anti-virus software can block attack vectors.

- But no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long, because hackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers.
- If vulnerabilities are the entry points, then attack vectors are the ways attackers can launch their assaults or try to infiltrate the building.
- In the broadest sense, the purpose of the attack vectors is to implant a piece of code that makes use of a vulnerability. This code is called the payload, and attack vectors vary in how a payload is implanted.
- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan horses, worms, and spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

To some extent, firewalls and anti-virus software can block attack vectors continued.....

- **The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan horses, worms, and spyware.**
- **If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.**

Different ways to launch Attack Vectors:

- Attack by Attachments
- Attack by deception: social engineering/ hoaxes
- Hackers
- Heedless guests (attack by webpage)
- Attack of the worms
- Malicious macros
- Foistware / sneakware
- viruses

A zero-day attack

- A zero-day (or zero-hour or day zero) attack or threat is an attack that exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch.
- Software vulnerabilities may be discovered by hackers, by security companies or researchers, by the software vendors themselves, or by users.
- If discovered by hackers, an exploit will be kept secret for as long as possible and will circulate only through the ranks of hackers, until software or security companies become aware of it or of the attacks targeting it.

Principles of Defense and Offense.

Cybersecurity is defined by five principles:

Confidentiality

Integrity

Availability

Nonrepudiation

Authentication

Confidentiality –

- Information has confidentiality if it can be accessed and read only by authorized users.
- Authorized users typically include the person generating the information and the intended recipients of the information.
- Violating confidentiality is often the goal of many cyber attacks.
- To violate confidentiality attackers may intercept the information while in transit (such as over an insecure WiFi connection or the internet). Or they may bypass security controls on a system to steal the information while at rest.
- Information commonly targeted by attackers includes personal communications (e-mail, text messages), pictures, trade secrets, payment information (credit/debit card numbers), personal identifiers (social security numbers), and sensitive government and military information.

Encryption and access control are typical mechanisms used to protect confidentiality.

Integrity

Information has integrity if it can be modified only by authorized users. Integrity should be verifiable, meaning it should be easy to determine if information has been modified by an unauthorized third party.

Integrity can be violated while information is in transit or at rest, and that violation can be accidental or intentional.

Accidental incidents include incorrect data entry, hardware failure, and effects from solar radiation. Intentional incidents include unauthorized modification of a file, database, or network packet.

Cryptographic hashing is often used to verify integrity of information.

• Availability

- Information is considered *available* if it can be accessed when and where it is needed. Access to information should also be timely and convenient for the user.
- Attacks against availability are becoming increasingly popular among nation-states and hacktivists, as they have an immediate and visible effect.
- Accidental incidents include loss of power, hardware failure, or software failure.
- Intentional acts include distributed denial-of-service (DDoS) attacks and ransomware attacks.
- Redundancy, data and power backups, and failover sites are typically used to maintain high availability rates.

Nonrepudiation

Nonrepudiation links an entity (user, program, etc.) to actions taken by that entity. For example, a person's signature on a legal contract can be used to prove that the person agreed to the terms of the contract.

It is difficult for the person who signed the contract to later deny or repudiate doing so because the evidence of the signature exists.

Common methods to ensure nonrepudiation include user authentication, digital signatures, and system logging.

• Authentication

- *Authentication* deals with positively identifying and verifying the identity of a user. This is a critical component to ensuring that only authorized users can access or modify information.
- Authentication mechanisms are one of the most targeted aspects of information systems, as the success of the other four principles is often dependent upon it.
- Common mechanisms used for authentication include usernames and passwords, electronic key cards, and biometrics.

Introduction to Defensive Cybersecurity & Offensive Cybersecurity.

What Is a Cybersecurity Specialist?

- Cybersecurity specialists execute various security measures meant to protect a business's computer systems and networks. They monitor, analyze, and fix potential system breaches that may be exploited by cyber criminals.
- Cybersecurity specialists also research trends in tech-based security to stay one step ahead of would-be attackers and their tactics.

- While a cybersecurity specialist helps a company keep its data secure, the protective nature of the role has a greater reach.
- By keeping an organization's information safe, cybersecurity specialists prevent sensitive customer data, such as addresses, social security numbers, and credit card information from falling into the wrong hands.[

These are the cybersecurity Approaches:

- General cybersecurity,
- Offensive cybersecurity, and
- Defensive cybersecurity.

Offensive Cyber Security - Deploys a proactive approach to security through the use of ethical hacking

Defensive Cyber Security – Uses a reactive approach to security that focuses on prevention, detection, and response to attacks

General Cyber Security - Utilizes a mix of offensive and defensive tactics to provide cybersecurity

Offensive Cyber Security - Deploys a proactive approach to security through the use of ethical hacking

Rather than relying on pure analysis and reacting to findings with preventive measures, offensive cybersecurity uses ethical hacking techniques to mimic cyber attacks.

This method exploits security vulnerabilities and can eliminate the guesswork of what may happen during an attack.

Offensive Cyber Security includes

- **Ethical Hacking –**
- **Penetration testing**-used to discover risks within an organization's network. Penetration testers use a variety of tools and methods to identify potential gaps in security before bad actors have a chance to find them.

- **Vulnerability Scanning** - uses a variety of tools and tactics to search for known security risks and vulnerabilities within a network.
Vulnerability scanning helps you identify and assess the risk associated with the vulnerabilities in your network.
Vulnerability scanning helps you prioritize what security vulnerabilities to remediate.

- **Wireless Security Testing** - provides organizations with detailed information on vulnerabilities related to their wireless networks.
This technique addresses what networks exist, how strong their security is, as well as what devices are connected to these networks.

- **Social Engineering** - Social engineering is a manipulation technique that exploits human interaction in order to access and steal private information, assets, and other valuables.

In offensive cybersecurity, this technique is used by ethical hackers as a means to **detect and deter malicious actions**.

Defensive Cyber Security – Uses a reactive approach to security that focuses on prevention, detection, and response to attacks

- Uses more traditional methods to keep networks safe from cyber crime.
- The tactics rely on a thorough understanding of a system environment and how to analyze it to detect potential network flaws.
- This analysis influences the development and deployment of preventive and protective measures that discourage or outright stop cyber attacks.

Defensive Cyber Security includes

- **Security Information & Event Management,**
- **Digital Forensics**
- **Incident Response & Malware Analysis**
- **Virtualization & Cloud Security.**

Some of the **top defensive cybersecurity services** include:

IT Security Management

Practice of protecting an organization's information systems, network, and assets from internal and external cyber threats.

Security Operations Center (SOC) Services

The (SOC) serves as the team within an organization that is responsible for detecting, mitigating, and responding to cyber threats against the organization.

Managed Detection & Response

Managed Detection and Response (MDR) refers to the team of security professionals, usually located outside of an organization, that is responsible for threat detection and incident response to help prevent cyber attacks.

Cloud Security

cloud security refers to the collection of policies, technologies, applications, tactics, and controls used to protect cloud-based data, applications, services, and the accompanying cloud computing infrastructure of an organization.

Remediation Support

Remediation support is used by an organization to address a breach that has already occurred and limit the amount of damage that results from the breach.

Firewalls

Perhaps the most tried-and-true defensive cybersecurity tactic is the integration of a firewall before your organization's internal network. **Firewalls serve as the first line of defense** for your network by providing protection against external entities, making them one of the most effective ways to defend your organization from cyber attacks.

Access Controls

Access controls can include anything from usernames to passwords and biometric scans, and are an integral component of controlling who has access to your organization's systems and devices.

Employee Training

Employee security awareness is vital to ensure the security of your organization. By training your employees on defense measures and keeping them aware on the latest phishing attacks , you are effectively shielding your organization from all types of data breaches.

- **Security Information & Event Management,**

Combining security information management (SIM) and security event management (SEM), security information and event management (SIEM) offers **real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes**.

- **Digital Forensics**
- Digital forensics is a branch of forensic science that focuses on **identifying, acquiring, processing, analysing, and reporting on data stored electronically**. Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.

- **Incident Response & Malware Analysis**
- Incident Response and Malware Analysis will assist you gauge the influence of cyber breaches. An investigation is necessary, and a containment and recovery technique needs to be carried out by experts.

  Any corporation that is uncovered to an incident, faces a dent to their brand popularity and additionally any felony liability.

- **Malware Analysis**

Two types of analysis STATIC and DYNAMIC

STATIC Analysis – Basic static analysis does not require that the code is actually run. Instead, **static analysis examines the file for signs of malicious intent.** It can be useful to identify malicious infrastructure, libraries or packed files.

Technical indicators are identified such as **file names**, **hashes, strings such as IP addresses, domains,** and **file header data** can be used to determine whether that **file is malicious**. In addition, tools like **disassemblers and network analyzers** can be used to observe the malware without actually running it in order to collect information on how the malware works.

DYNAMIC Analysis-

Dynamic malware analysis executes suspected malicious code in a safe environment called a sandbox.

This closed system enables security professionals to watch the malware in action without the risk of letting it infect their system or escape into the enterprise network.

Dynamic analysis provides threat hunters and incident responders with deeper visibility, allowing them to uncover the true nature of a threat.

As a secondary benefit, automated sandboxing eliminates the time it would take to reverse engineer a file to discover the malicious code. The challenge with dynamic analysis is that adversaries are smart, and they know sandboxes are out there, so they have become very good at detecting them.

To deceive a sandbox, adversaries hide code inside them that may remain dormant until certain conditions are met. Only then does the code run.

- **Virtualization & Cloud Security.**

Virtualized security, or security virtualization, refers to security solutions that are software-based and designed to work within a virtualized IT environment. This differs from traditional, hardware-based network security, which is static and runs on devices such as traditional firewalls, routers, and switches.

Cloud security considerations (such as isolating multitenant environments in public cloud environments) are also important to virtualized security. The flexibility of virtualized security is helpful for securing hybrid and multi-cloud environments, where data and workloads migrate around a complicated ecosystem involving multiple vendors.

References:
[1] Cyber Security practices, nina godbole
[2] https://online.maryville.edu/online-bachelors-degrees/cyber-security/resources/understanding-cyber-security-tracks/
[3] https://www.evolvesecurity.com/blog-posts/defensive-vs-offensive-cybersecurity
[4] https://www.ibm.com/in-en/topics/siem
[5]https://www.vmware.com/topics/glossary/content/virtualized-security.html
[6] https://www.oreilly.com/library/view/cybersecurity-ops-with/9781492041306/ch04.html
[7] https://cybersrcc.com/incident-response-and-malware-analysis/