UNIT II

Criminals Plan:

Technology can be good or bad.

- Some people, called "Crackers," use the internet and computers for bad things because many folks don't know much about cybercrimes.
- Bad computer activities include hacking, cyberterrorism, sneaking into networks, stealing passwords, and spreading computer viruses.
- Hackers are different from Crackers; hackers are usually good, but Crackers are the ones doing bad stuff.
- Brute force hacking is trying every password combination.
- Cracking is breaking into computers for bad reasons, and tools like Trojans, viruses, and worms make it easy on the internet.
- Phreaking is messing with phones without permission.
- Bad guys use weaknesses in networks, like not enough protection, weak access points, or computers with known problems.
- In the security world, "black hat" means bad hackers, "white hat" means good hackers protecting systems, "grey hat" shares hacking info publicly without caring how it's used, and "brown hat" hackers think before doing bad things.

Categories of Cybercrime:

Crimes Targeted at Individuals:

- Exploiting human weaknesses (greed, naivety)
- **Examples:** Financial frauds, sale of non-existent or stolen items, child pornography, copyright violation, harassment.
- IT and the Internet facilitate criminals, making it challenging to trace and apprehend.

Crimes Targeted at Property:

- Stealing mobile devices (phones, laptops, PDAs)
- Transmitting harmful programs to disrupt system functions and wipe out data.
- Malfunctioning attached devices (modem, CD drive, etc.).

Crimes Targeted at Organizations:

- Cyberterrorism against organizations/governments.
- Attackers use computer tools and the Internet to terrorize citizens, steal private information, damage programs/files, or gain control of networks/systems.

Temporal Classifications:

- Single Event of Cybercrime: For example, unknowingly opening an attachment containing a virus, leading to system infection (hacking or fraud).
- Series of Events: For example, attacker interacts with victims repetitively, establishing a relationship and exploiting it for crimes.

Reconnaissance:

Reconnaissance, which is like exploring, is a crucial part of hacking.

- It's about gathering info, especially about an enemy.
- In hacking, it starts with "Footprinting," where data about the target's computer setup is collected before an attack.
- This step seems harmless but is key in understanding system weak points.

- The goal is to figure out the system details, like its network ports and security features, needed for a successful attack.
- This prep work happens in two ways: passive (quietly observing) and active (directly probing for weaknesses).
- Both methods help hackers get a good understanding, setting the stage for a smart and potentially successful attack.
- So, reconnaissance is like a necessary first step that guides hackers through the tricky world of online security with a clear plan.

Passive Attacks:

A passive attack is when someone secretly gathers information about a person or a company without them knowing.

- It's like quietly watching a building to see when people come and go.
- On the internet, this is often done by searching on Google or Yahoo to find details about individuals or companies.
- People might also check online groups like Orkut or Facebook to learn more about someone.
- If a company has a website, it might have a list of employees with their contact details, which could be used for a social engineering attack.
- Information about a company or its employees can also be found in blogs, newsgroups, or press releases.
- Looking at job postings for technical positions can also reveal details about the kind of technology they use.

Active Attacks:

Active attacks are like knocking on the doors of a network to find out more about the individual computers there.

- This is done to confirm the information collected in the earlier phase where we quietly gathered details like IP addresses, the kind of operating system, and the services on the network.
- It's a riskier move because it might be noticed, and people call it "Rattling the doorknobs" or "Active reconnaissance."
- While this active checking can tell the attacker if security measures are good or not (like checking if the front door is locked), it also increases the chances of getting caught or making someone suspicious.

Scanning/Scrutinizing gathered Information:

Scanning and scrutinizing gathered information is like looking at things more closely to understand them better.

- First, we do something called "Port scanning," which is like checking if certain doors are open or closed on the target.
- Then, we do "Network scanning" to learn about the computer network, like finding out its IP addresses.
- Finally, there's "Vulnerability scanning," where we figure out if there are any weak points in the system.
- It's like trying to see where the system might need better protection.
- So, scanning helps us get a clearer picture of what we're dealing with.

Attack:

After scanning and figuring out details about the system, the next step is launching the attack.

- First, the attacker tries to "crack the password," like trying to unlock a door.
- If that works, they move on to "exploit the privileges," which means taking advantage of special access.
- Then, they "execute malicious commands or applications," kind of like making the system do things it shouldn't.
- If they need to, they might "hide the files" to cover their tracks.
- Finally, to make sure no one knows what they did, they "cover the tracks" by deleting the access logs, erasing any signs of their actions.
- So, it's like breaking in, doing sneaky stuff, and then making sure no one finds out about it.

Social Engineering:

Social engineering is like a trick where someone tries to influence or deceive people to get information or make them do something.

- Instead of hacking into computers, social engineers take advantage of the fact that people tend to trust others.
- It's widely agreed that people are the weak link in security, making social engineering possible.
- These tricksters often use phones or the internet to make people do things against security rules.
- The goal is to gain secret information or access by building fake trust relationships.
- Social engineers study how people behave, using their natural tendencies to be helpful, trusting, and scared of getting in trouble.
- Successful social engineers are so good at it that people give away information without even suspecting anything.
- For example, they might call someone, pretend to be from IT, and ask questions about what the person is working on, what passwords they use, and more. It's like a clever game of fooling people to get what they want.

  .

Classification of Social Engineering:

Social engineering comes in two types: one that involves talking to people (human-based) and another that uses computers (computer-based).

- Human-based social engineering means tricking people in person or over the phone to get information.
- For example, someone might pretend to be an employee, an important person, or even someone from tech support to gain access to a system.
- They might also watch over someone's shoulder to get usernames and passwords, a technique called "shoulder surfing."
- Another sneaky trick is "dumpster diving," where they go through the trash to find useful info.
- On the computer side (computer-based), social engineering happens through things like fake emails or messages, a tactic known as "Phishing."
- In phishing, attackers pretend to be trustworthy organizations to trick people into sharing personal info like usernames and passwords.
- They might also send harmful stuff through email attachments or pop-up windows, hoping people will click on them and unknowingly install bad software.

- It's like a digital game of pretending to be someone else to get what they want.

Cyberstalking:

Cyberstalking is like digital stalking using the internet.

- Stalking means following someone secretly or trying to approach them without being noticed.
- So, cyberstalking is when someone uses the internet to harass or bother another person or even an organization.
- This behaviour includes making false accusations, spying on someone, sending threats, stealing someone's identity, damaging their data or devices, and even trying to connect with minors for inappropriate reasons.
- In simple terms, cyberstalking involves repeatedly harassing or threatening someone online, just like someone might follow, visit, or call a person in real life.
- With the internet making communication easy, cyberstalkers take advantage of this to access personal information with just a few clicks.

Types of Stalkers:

There are two main types of stalkers: online and offline.

- Online stalkers use the internet to connect with their victims, usually through email or chat rooms, instead of traditional methods like calling.
- They want the victim to know they're being targeted and sometimes, they might even use someone else to harass the victim.
- On the other hand, offline stalkers start their attacks using old-school methods like following the victim or keeping an eye on their daily routines.
- They use the internet to gather information about the victim through message boards, personal websites, or people-finding services, and the victim might not even realize that the internet was involved in the attack.
- So, stalkers can be either digital or more traditional in how they go about their unwanted actions.

Working of Stalking:

Stalking works by the stalker gathering personal information about the victim, like their name, family background, phone numbers, addresses, and email.

- They then make contact through phone calls or emails, often with threatening or explicit tones.
- Some stalkers repeatedly email the victim asking for favours or making threats.
- In a more harmful twist, the stalker might post the victim's personal details on websites for sex services, pretending the victim posted it, and invite people to contact them for such services.
- The stalker might use offensive language to attract interested individuals.
- As a result, strangers might start calling the victim, asking for sexual services or relationships.
- In another harmful tactic, some stalkers sign up the victim's email for many porn sites, causing the victim to receive unsolicited explicit emails.
- So, stalking involves invading someone's privacy and using various methods to harm or harass them.

Real-Life Incident of Cyber stalking:

Here's a real-life incident about cyberstalking that happened in Delhi, India.

- We've changed the names to keep things private.
- Mrs. Joshi started getting around 40 calls in just three days, and they were coming from places like Kuwait, Cochin, Bombay, and Ahmadabad.
- These calls messed up her life, and she decided to report it to the Delhi Police.
- Turns out, someone was using her identity to chat on a website called www.mirc.com.
- This person used her name, shared her address, and talked in an inappropriate way.
- What's worse, they deliberately gave out her phone number to others, encouraging them to call her at weird times.
- This incident marked the first time the police registered a case of cyberstalking.
- Cyberstalking is when someone uses the internet to threaten or bother another person, and this incident messed with Mrs. Joshi's peace of mind.

Cybercafe and Cybercrimes:

Using cybercafes comes with its risks, and it's crucial to be aware of them.

- A survey in India found that most cybercafe users were young males between 15 and 35 years old.
- Cybercafes have been misused for various crimes, including terrorist communication, stealing bank passwords, and sending harassing emails.
- Public computers in cybercafes pose two risks: unknown installed programs that may be malicious, and the possibility of others seeing your passwords.
- Indian law sees cybercafes as network service providers, holding them responsible for due diligence to prevent offenses on their network.
- Cybercriminals often choose cybercafes for their activities, identifying specific computers for their use.
- Challenges arise when investigating cybercrimes in cybercafes due to factors like pirated software, outdated antivirus programs, and lack of awareness about IT security.
- Users are advised to take precautions like logging out, staying with the computer, clearing history, and avoiding online financial transactions when using cybercafes.
- It's essential to be cautious and follow security measures to stay safe while using public computers.

Botnet:

A "bot" is like a computer program that does tasks automatically, often over the internet.

- When many of these bots work together, it forms a "botnet."
- While the term is often linked to harmful software, it can also refer to a group of computers using shared computing software.
- Essentially, a bot can take control of a computer by infecting it with a virus or other malicious code, even if the computer seems normal.
- Botnets are frequently used for various activities, such as spreading spam, viruses, and carrying out attacks.
- They allow cybercriminals to control infected computers remotely without the users knowing.
- Botnets, also known as zombie networks, are sometimes sold on forums, and their low maintenance cost and ease of management contribute to their popularity.
- To avoid being part of a botnet, it's important to limit access to your system, use antivirus and anti-spyware software, keep your system updated, use a firewall,

disconnect from the internet when not in use, download from trusted websites, check your email regularly, and take immediate action if your system is infected.

Attack Vector:

An "attack vector" is like a path that allows an attacker to access a computer or network to cause harm.

- Attack vectors can exploit vulnerabilities in systems, including human errors.
- They come in various forms, such as viruses, email attachments, webpages, pop-up windows, instant messages, and deception.
- Firewalls and antivirus software can provide some protection, but no method is entirely foolproof.
- Attackers are always updating their methods, making it challenging to stay completely secure.
- Malicious payloads, like viruses and Trojan Horses, are the harmful outcomes carried by these attack vectors.
- Each attack vector has its way of delivering these payloads, such as through email, attachments, deception, hackers, worms, malicious macros, foistware, and viruses.
- It's essential to be cautious and use security measures to protect against these potential threats.

Attacks on Mobile/Cell Phones:

Mobile phones have become essential in everyone's life, but along with their widespread use comes the risk of various attacks.

- One common issue is mobile phone theft, which has increased significantly.
- The factors contributing to outbreaks on mobile devices include the availability of many target terminals, the functionality of mobile devices, and their extensive connectivity options.
- Mobile viruses, like computer viruses, have become more common and can spread through communication protocols like Bluetooth and MMS.
- To protect against mobile malware attacks, it's important to download programs only from trusted sources and use antivirus software.
- Mishing, a combination of mobile phone and phishing, involves scams through calls or messages, while vishing uses social engineering over the phone to gain personal and financial information.
- Smishing, another criminal offense, is like phishing but uses text messages.
- Protecting against these attacks involves being cautious, not clicking on suspicious links, and reporting incidents.
- Bluetooth hacking is also a concern, with various tools allowing unauthorized access and potential exploitation of Bluetooth-enabled devices.
- It's essential to be aware of these threats and take steps to protect personal information on mobile phones.