CYBER CRIME AND LAW

Unit I

DEFINITION

- A crime committed using a computer and the internet.
- Crimes completed either on or with a computer.
- Any illegal activity done through the internet or on a computer.
- All criminal activities done using the medium of computers, internet, cyberspace and WWW

WHO ARE CYBERCRIMINALS ?

- Type I: Hungry for recognition
  - Hobby Hackers
  - IT professionals
  - Politically motivated hackers
  - Terrorist organizations

WHO ARE CYBERCRIMINALS ?

- Type II: Not Interested in Recognition
  - Psychological perverts
  - Financially motivated hackers
  - State-sponsored hacking
  - Organized criminals

WHO ARE CYBERCRIMINALS ?

- Type III: The Insiders
  - Disgruntled or former employees seeking revenge
  - Competing companies using employees to gain economic advantage through damage and / or theft

CLASSIFICATION OF CYBERCRIMES

- Cybercrime against individual
  - Email Spoofing
  - Phishing
  - Spamming
  - Cyber defamation
  - Cyber stalking and harassment
  - Computer sabotage
  - Password sniffing

CLASSIFICATION OF CYBERCRIMES

- Cybercrime against property
  - Credit card frauds
  - Intellectual property
  - Internet time theft

CLASSIFICATION OF CYBERCRIMES

- Cybercrime against organization
  - Unauthorized accessing of computer
  - Password sniffing
  - Denial of service attacks
  - Virus attack / dissemination
  - Email bombing
  - Salami attack
  - Logic bomb
  - Trojan Horse
  - Data diddling
  - Industrial spying / espionage
  - Computer network intrusion
  - Software piracy

CLASSIFICATION OF CYBERCRIMES

- Cybercrime against society
  - Forgery
  - Cyber terrorism
  - Web jacking

HOW CRIMINALS PLAN THE ATTACKS

The following phases are involved in planning cybercrime

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

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

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

HOW CRIMINALS PLAN THE ATTACKS

- Reconnaissance
- Begins with "*Footprinting*" – this is the preparation toward pre-attack phase involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.
- Footprinting gives an overview about system vulnerabilities and provides possible exploitation of those vulnerabilities.
- Attacker attempts to gather information in two phases:
  - Passive Attack
  - Active Attack

HOW CRIMINALS PLAN THE ATTACKS

- Reconnaissance
- Passive Attacks
  - Attack involves gathering information about a target without his/her (individual's or company's) knowledge.
  - It is usually done using Internet searches or by Googling an individual or company to gain information.
- Active Attacks
  - An active attack involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
  - It involves the risk of detection and is also called "Rattling the doorknobs"or "Active reconnaissance."
  - Active reconnaissance can provide confirmation to an attacker about security measures in place.

HOW CRIMINALS PLAN THE ATTACKS

- Scanning and Scrutinizing Gathered Information

The objectives of scanning are:

1. Port scanning: Identify open/close ports and services.
2. Network scanning: Understand IP Addresses and related information about the computer network systems.
3. Vulnerability scanning: Understand the existing weaknesses in the system.

HOW CRIMINALS PLAN THE ATTACKS

- Attack (Gaining and Maintaining the System Access)

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

1. Crack the password;
2. Exploit the privileges;
3. Execute the malicious commands/applications;
4. Hide the files (if required);
5. Cover the tracks – delete the access logs, so that there is no trail illicit activity.

SOCIAL ENGINEERING

- It is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- The sign of truly successful social engineers is that they receive information without any suspicion.

SOCIAL ENGINEERING

Classification of Social Engineering

- Human-Based Social Engineering refers to person-to-person interaction to get the required/desired information

1. Impersonating an employee or valid user
2. Posing as an important user
3. Using a third person
4. Calling technical support
5. Shoulder surfing
6. Dumpster diving

SOCIAL ENGINEERING

- Classification of Social Engineering

  - Computer-Based Social Engineering refers to an attempt made to get the required/desired information by using computer software/Internet

    1. Fake E-Mails
    2. E-Mail attachments
    3. Pop-up windows

PHISHING

- Attackers generally do phishing by impersonating the organizations or individuals you know well, and they would usually ask for details like password, credit card number, and other personal information.
- While using emails, you should be careful about such threats.
- Professional hackers prepare spam emails to extract information from other people.
- The phishing attackers would mainly target sectors like banking, technology, and healthcare because they are large scale business organizations where they would have many users with more data.
- By these phishing attacks, one could be incurring substantial financial losses as well as compromising one's confidential information.

THE STANDARD FORMS OF PHISHING ATTEMPTS

- Smishing
  - One of the forms of phishing is Smishing, where the sender would send an SMS to the recipient and try to lure the user into providing his details by offering some fake deals & offers or create a sense of urgency by sending messages such as "Your bank account is compromised. Share your password to get your access back."
- Vishing
  - The next one is Vishing in which the phishers would speak to you over the phone, pretending to be a relative of yours, and confidently ask for your details. Be careful of such phone calls.
- Search Engine Phishing
  - Another common type of phishing is called Search Engine Phishing. Here, phishers focus on some specific keywords and fabricate a webpage where you would be caught in while you search for the information you need. Hence, one needs to be cautious while looking for a webpage.

THE STANDARD FORMS OF PHISHING ATTEMPTS

- Spear Phishing
  - A major form of phishing attack is Spear Phishing. Spear phishing attacks are riskier as the phishers study and research as much as they can about a particular organization and then target one specific user or even the organization.
- Whaling
  - Similar to spear phishing, there is another form known as Whaling. In this, the attackers would be more attentive in searching for information about the people who are positioned high in an organization such as CFO, COO, and CEO. The reason for the attackers to target them is that the people who have a higher authority would have more sensitive information about the organization.

HOW DOES PHISHING WORK?

- Almost all types of phishing attacks can be broadly divided into two categories –

- Tricking Users
  - This involves directly tricking the user to pass on sensitive information via spoof sites. This method creates compelling communication messages that entice the user into visiting third-party, data harvesting sites.

- Installing Malware
  - With this the attacker, gets the user to install malware by when a call-to-action is clicked in a communication. In the method, the fraudster entices the user to click on a download link that in turn installs malware.

HOW TO SPOT A PHISHING EMAIL

- Poor grammar, punctuation and just plain tacky language
- Emails soliciting personal information
- Alarming content
- Urgent deadlines
- Unrealistic financial rewards
- Mismatched URLs
- Mis-matched domain name

HOW TO PREVENT PHISHING

- Avoid using open, public networks
- Avoid clicking on unknown shortened links
- Verify a site's security
- Never enter personal information in pop-ups
- Watch out for obviously suspicious emails
- Anti-phishing toolbars
- Anti-spam software
- Anti-virus software
- Firewalls

CYBER STALKING

- It is defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- Cyber stalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behaviour that an individual will conduct repeatedly.
- As the Internet has become an integral part of our personal and professional lives, cyber stalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

CYBER STALKING

- Types of Stalkers
  - Catfishing - In Catfishing, Stalkers create a fake profile on social media to approach victims. Sometimes they copy the existing user's profile with photos to look it like a real one.
  - Monitoring location check-ins on social media - Stalkers keep an eye on the activities of a victim from their check-ins on social media such as Facebook and Instagram. This is an easier job for a stalker to gauge a victim's behavioural pattern quite accurately.
  - Visiting virtually via Google Maps Street View - If a stalker discovers the victim's address, then it is not hard to find the area, neighbourhood, and surroundings by using Street View. Tech-savvy stalkers don't need that too. They can discover the victim's place from the posts or photos posted on social media.

CYBER STALKING

Types of Stalkers

- Hijacking webcam - Computer's webcam hijacking is one of the most disgusting methods of cyberstalking to invade the victim's privacy. Stalkers push malware-infected files into the victim's computer which gives them access to the webcam.
- Installing Stalkerware - One more method which is increasing its popularity is the use of Stalkerware. It is a kind of software or spyware which keeps track of the location, enable access to text and browsing history, make an audio recording, etc. And an important thing is that it runs in the background without any knowledge to the victim.
- Looking at geotags to track location - Mostly digital pictures contain geotags which is having information like the time and location of the picture when shot in the form of metadata. Geotags comes in the EXIF format embedded into an image and is readable with the help of special apps. In this way, the stalker keeps an eye on the victim and gets the information about their whereabouts.

PROTECT AGAINST CYBERSTALKING

- Review what online information exists about you and keep it to a minimum
- Regularly change your e-mail and passwords for key online accounts and keep them safe
- Review all your privacy and security settings
- Avoid public forums
- Ensure that your computer and mobile devices have updated antispyware software installed and turned on
- Ensure your wireless hub/router has security turned on.
- Unless you are using a secure web page, do not send or receive private information when using public WiFi
- Limit the personal and financial information you share on or offline
- Educate friends, family and work colleagues into the risks

BOTNETS: THE FUEL FOR CYBERCRIME

- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- Your computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.

BOTNETS: THE FUEL FOR CYBERCRIME

- One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer.
5. Downloading the freeware only from websites that are known and trustworthy
6. Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send.
7. Take an immediate action if your system is infected.

ATTACK VECTOR

- An "attack vector" is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception.
- The most common malicious payloads are viruses, 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.
  - ✓ Payload means the malicious activity that the attack performs.
  - ✓ It is the bits that get delivered to the end-user at the destination.

ATTACK VECTOR

- The attack vectors described here are how most of them are launched:

1. Attack by E-Mail
2. Attachments (and other files)
3. Attack by deception
4. Hackers
5. Heedless guests (attack by webpage)
6. Attack of the worms
7. Malicious macros
8. Foistware (sneakware)
9. Viruses

End of Unit 1