Department of Artificial Intelligence and Data Science

TE-AI&DS- CYBER SECURITY

Unit-6

[MAY-2024]

Q1) Identify and explore the different types of Cyber stalker attacks. [6]

[MAY-2024]

Ans –

In **Cyber Stalking**, a cyber criminal uses the internet to consistently threaten somebody. This crime is often perpetrated through email, social media, and the other online medium. Cyber Stalking can even occur in conjunction with the additional ancient type of stalking, wherever the bad person harasses the victim offline. There's no unified legal approach to cyber Stalking, however, several governments have moved toward creating these practices punishable by law. Social media, blogs, image sharing sites and lots of different ordinarily used online sharing activities offer cyber Stalkers with a wealth of data that helps them arrange their harassment. It includes actions like false accusations, fraud, information destruction, threats to life and manipulation through threats of exposure. It has stalkers take the assistance of e-mails and other forms of message applications, messages announce to an online website or a discussion cluster, typically even the social media to send unwanted messages, and harass a specific person with unwanted attention. Cyber Stalking is typically cited as internet stalking, e-stalking or online stalking.

Types of Cyber Stalking:

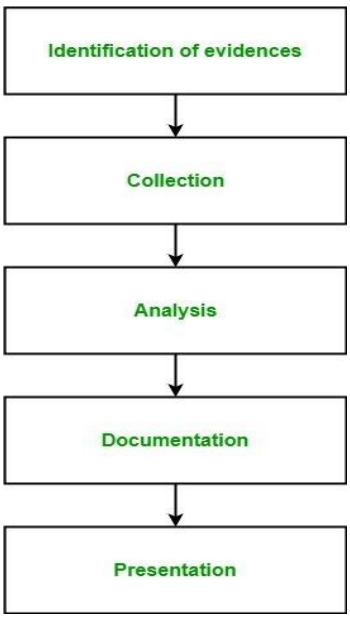
- **Webcam Hijacking:** Internet stalkers would attempt to trick you into downloading and putting in a malware-infected file that may grant them access to your webcam. the method is therefore sneaky that it's probably you wouldn't suspect anything strange.
- **Observing location check-ins on social media:** In case you're adding location check-ins to your Facebook posts, you're making it overly simple for an internet stalker to follow you by just looking through your social media profiles.

- **Catfishing:** Catfishing happens via social media sites, for example, Facebook, when internet stalkers make counterfeit user-profiles and approach their victims as a companion of a companion.
- **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.
- **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.

Q.2) Illustrate life cycle of cyber forensics?. [6] [MAY-2024]

Ans-

Digital Forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation. In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences. The first computer crimes were recognized in the 1978 Florida computers act and after this, the field of digital forensics grew pretty fast in the late 1980-90's. It includes the area of analysis like storage media, hardware, operating system, network and applications. It consists of 5 steps at high level:



1. **Identification of evidence:** It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.
2. **Collection:** It includes preserving the digital evidences identified in the first step so that they doesn't degrade to vanish with time. Preserving the digital evidences is very important and crucial.
3. **Analysis:** It includes analyzing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.
4. **Documentation:** It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.
5. **Presentation:** It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

Q.3) List VoIP hacking types and explore any 3? What are the counter measures for it. [5]

[MAY-2024]

Ans –

VoIP hacking is concerned with making use of unauthorized access to the phone system to steal data. The hackers try to listen to the calls and steal critical information. The hacking is also done to make calls and increase the bills of the international communicator. These types of attacks usually occur in a situation when an insider or a known person will serve important information. These types of attacks could result in the use of customer information which would include the use of credit card information and using this information to gain money.

Various types of VoIP hacking

1. Unauthorized use

It is a type of attack vendor user or the hacker make use of the information of the phone network to make calls to other person or organization pretending someone is from the organization. These types of hackers or malicious users make use of the autodial link and robot calling software to connect to the phone network system. When the receiver takes the call a prerecorded message please could ask the listener to enter their information such as credit card details or bank details.

2. Toll fraud

It is referred to as making international calls to other people and organizations that could result in increasing the bill amount and often resulting in major damage to the organization.

3. Eavesdropping

It occurs when the attacker listens to certain business goals and communications without the user's information. This type of malicious activity occurs when the date of information is shared through an unencrypted or unsecured channel of communication.

4. Call tampering

It is one of the techniques used by the malicious user to create a disturbance in communication it could include injecting some noise packets to reduce the quality of communication.

5. DoS attack

It is a type of attack that includes making a particular service unavailable by injecting huge traffic from multiple ends to the system.

6. Buffer overflow attacks

It is a place for storing data temporarily. When more data is placed on a program or a system this results in the situation of data overflow. This could also result to the leaking of certain important data into other buffers that could also corrupt the owner's holding. In the situation of a buffer overflow attack, the extra information can reach malicious users and they can change the data and damage the files.

7. Viruses and malware

A virus is a court embedded that results to affecting the original information. The viruses are self-replicating and are being designed to hurt the program and the software. Malware is software that enters into the system without the owner's consent to steal private and confidential information.

Countermeasures

Countermeasures for dealing with VoIP are as follows −

- Access to the website or the content should be implemented in a careful and controlled manner so that unauthorized access to the information can be reduced.
- Choosing a trusted voice over Internet protocol is very important so that the information is safe.
- Detailed analysis and network tests should be done periodically so that the problems in the network can easily be identified.
- Regular checking of the call logs and the history is equally important as it will help in identifying any problem regarding the use of data.
- The Password set up for the website needs to be strong enough so that hackers cannot simply crack it.
- The company needs to concentrate on adding more security checks and train software handlers to look out for any unwanted behavior.

OR

Q 4) Who are cyber criminals? What are types of cyber crimes. [6] [MAY-2024]

Ans-

Cyber crime is taken very seriously by law enforcement. In the early long periods of the cyber security world, the standard cyber criminals were teenagers or hobbyists in operation from a home laptop, with attacks principally restricted to pranks and malicious mischief. Today, the planet of the cyber criminals has become a lot of dangerous. Attackers are individuals or teams who attempt to exploit vulnerabilities for personal or financial gain.

Types of Cyber Criminals:

1. Hackers: The term hacker may refer to anyone with technical skills, however, it typically refers to an individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes. The intent of the burglary determines the classification of those attackers as white, grey, or black hats. White hat attackers burgled networks or PC systems to get weaknesses so as to boost the protection of those systems. The owners of the system offer permission to perform the burglary, and they receive the results of the take a look at. On the opposite hand, black hat attackers make the most of any vulnerability for embezzled personal, monetary or political gain. Grey hat attackers are somewhere between white and black hat attackers. Grey hat attackers could notice a vulnerability and report it to the owners of the system if that action coincides with their agenda.

- **(a). White Hat Hackers –** These hackers utilize their programming aptitudes for a good and lawful reason. These hackers may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities. Security vulnerabilities are then reported to developers to fix them and these hackers can also work together as a blue team. They always use the limited amount of resources which are ethical and provided by the company, they basically perform pentesting only to check the security of the company from external sources.
- **(b). Gray Hat Hackers –** These hackers carry out violations and do seemingly deceptive things however not for individual addition or to cause harm. These hackers may disclose a vulnerability to the affected organization after having compromised their network and they may exploit it .
- **(c). Black Hat Hackers –** These hackers are unethical criminals who violate network security for personal gain. They misuse vulnerabilities to bargain PC frameworks. theses hackers always exploit the information or any data they got from the unethical pentesting of the network.

2. Organized Hackers: These criminals embody organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are typically teams of skilled criminals targeted on control, power, and wealth. These criminals are extremely subtle and organized, and

should even give crime as a service. These attackers are usually profoundly prepared and well-funded.

3. Internet stalkers: Internet stalkers are people who maliciously monitor the web activity of their victims to acquire personal data. This type of cyber crime is conducted through the use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.

4. Disgruntled Employees: Disgruntled employees become hackers with a particular motive and also commit cyber crimes. It is hard to believe that dissatisfied employees can become such malicious hackers. In the previous time, they had the only option of going on strike against employers. But with the advancement of technology there is increased in work on computers and the automation of processes, it is simple for disgruntled employees to do more damage to their employers and organization by committing cyber crimes.

Q. 5) What is Botnet? How to protect from botnet? [6] [MAY-2024]

Ans-

A bot is an automated software program that is designed to perform a specific task over the internet. A content scraping bot, for example, is designed just to save content on many different web pages. A botnet is a network or cluster of such bots, typically using a group of computers (or other devices) that have been infected by malware and are now under the control of the malware owner. These botnets are being used to attack (and often infect) other computers and devices. Typically, hackers will do all they can to ensure that the victims aren't aware of the infection, which will allow them to exploit the botnet for as long as possible.

How to stop and prevent botnet attacks

1. Keep your software up to date

New viruses and malware are created every single day, so it's very important to ensure your whole system is also up-to-date to prevent botnet attacks. A lot of botnet attacks are designed to exploit vulnerabilities in apps or software, a lot of them have potentially been fixed in the form of security updates or patches. So, make a habit of updating your software and OS regularly. You wouldn't want to get infected by malware or any other types of cybersecurity threats just because you neglected to update software.

2. Closely monitor your network

Closely monitor your network for unusual activities. This will be much more effective if you have a better understanding of your typical traffic and how everything typically behaves ordinarily.

24-hour monitoring of the network should be the policy if possible, by using analytics and data-collection solutions that can automatically detect anomalous behavior, such as botnet attacks.

3. Monitor failed login attempts

One of the biggest threats to online companies is account takeover, or ATO. Botnets are often used to test large volumes of stolen username and password combinations in order to gain unauthorized access to user accounts.

Monitoring your usual rate of failed login attempts will help you establish a baseline, so that you can set up alerts to inform you of any spikes in failed logins, which may be a sign of a botnet attack. Do note that "low and slow" attacks coming from vast numbers of different IP addresses may not trigger these botnet attack alerts.

4. Implement an advanced botnet detection solution

The best approach to protecting your website and web server from botnet attacks is to invest in an advanced botnet detection software like DataDome, that can perform real-time botnet detection and employ top-level bot mitigation methods.

While botnet operators are now very sophisticated in masking the botnet's identity, DataDome's AI-powered solution can perform real-time behavioral analysis to detect botnet traffic and block all botnet activities before they even reach your web server. Implementing bot management and protection can even improve your initial server response time.

DataDome pools data from thousands of sites, analyzes billions of requests every day, and uses advanced machine learning to continuously update the algorithm. In this way, the botnet prevention solution can detect both familiar botnets and new threats in real time.

Best of all, DataDome requires no active botnet mitigation or other daily intervention on your part. Just set up your allow list of trusted partner bots, then DataDome will take care of all your unwanted traffic while you focus on more valuable projects.

Q. 6) Explain the terms:

i)Virus
ii)Phishing
iii) Spoofing
iv)Phone phishing
v)Internet pharming
vi)Cyber Forensic. **[6]**

[MAY-2024]

Ans-

i) Virus

Viruses are **microscopic organisms that can infect hosts, like humans, plants or animals**. They're a small piece of genetic information (DNA or RNA) inside of a protective shell (capsid). Some viruses also have an envelope. Viruses can't reproduce without a host.

ii) Phishing

Phishing is **a type of social engineering attack often used to steal user data, including login credentials and credit card numbers**. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

iii) Spoofing

Spoofing is a broad term for the type of behavior that involves a cybercriminal masquerading as a trusted entity or device to get you to do something beneficial to the hacker — and detrimental to you. Any time an online scammer disguises their identity as something else, it's spoofin

iv) Phone phishing

A fake bank security text, free data offer using the target's name, and a social engineering attack in Facebook Messenger. As email security solutions became better at detecting phishing campaigns, bad actors needed to innovate to keep their campaigns successful.

v) Internet pharming

Pharming is **online fraud that involves the use of malicious code to direct victims to spoofed websites in an attempt to steal their credentials and data**. Pharming is a two-step process that begins with an attacker installing malicious code on a victim's computer or server

vi) Cyber Forensic.

What is computer forensics (cyber forensics)? Computer forensics is **the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law**.