CS

1812401160 01
Vishwas Acharya

Assignment-3

Date: Page: 1

Q.1) Discuss cybercrime investigation in detail?

Ans- Cybercrime investigation is the process of investigating, analyzing and recovering critical forensic digital from the network involved in the attack.

- Cybercrime Investigation, or computer oriented crime, is crime that involves a computer and a network.
- Cybercrime investigators must be experts in computer science, understanding not only software, file systems and operating systems, but also how ~~all~~ networks and hardware work.
- They must be knowledgable enough to determine how the interactions between these components.

- Unauthorized access Investigation

- We investigate and analyze unauthorized cyber access or hacking incidents such as when someone gain access to your cloud, server or physical device without your permission.

- Sophisticated attacks Investigation

- Sophisticated criminals are active daily to exploit vulnerabilities on computers and other devices.

- Some of the techniques they use include:

- unanthorised access or hacking
- malware
- denial of service attacks.

- Email - Fraud Investigation

- Digitpol's Cybes and Fraud Team are certified fraud and forensic examiners and can deploy to assist with all cases related to email fraud, email spear phishing attacks, email scams and on-line related fraud.

- ~~Phish~~ Phishing Attack Investigation

- Phishing attacks, email fraud, scams, online fraud happens in most cases when cybes criminals find ways to hack into the email sevices or accounts of small and medium companies, often targeting those with buisness in asia countries

- Who conducts cybescrime investigation?

- Criminal justice agencies
- National security agencies
- Private security agencies.

Q.2) Write the short note on key logges & spyware?

Ans * Keyloggess:

- It is also known as key stroke logging or key logging.
- Keyloggers are a type of monitoring software designed to record keystrokes made by a user.
- One of the oldest forms of cybes threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

:- How does a keylogger works ?

- keylogges collects information and send it back to a third party - whether that is a criminal, law enforcement or IT dept.
- It is a software programs that leverage algorithms that monitor keyboard strokes through pattern recognition and other techniques

:- Best practices for detecting and removing keyloggers:

1) Monitor resource allocation, processes and data
2) keep antivirus and anti-rootkit protection up to date.

3) Use anti-keylogger software
4) consider virtual onscreen keyboards.
5) Disable self-running files on external devices
6) Have a strong password policy.

* Spyware

- It is loosely defined as malicious software designed to enter your computer device, gathers data about you, and forward it to a third-party without your consent.
- Spyware can also refer to legitimate software that monitors your data for commercial purposes like advertising.
- It is mostly classified into four types
  - adware
  - system monitors
  - cookies
  - Trojans
- Examples of notorious types include digital rights management capabilities that "phone home", keyloggers, rootkits, and web beacons.

∴ Types of spyware

1) Trojan spyware enters devices via Trojan malware, which delivers the spyware program.

2. Adware may monitor you to sell data to

advertisers or serve deceptive malicous code.

3. Tracking cookie files can be implanted by a website to follow you across the internet.

4. System monitors track any activity on a computer, capturing sensitive data such as keystrokes, sites visited, emails, and more, Keyloggers typically fall into this group.

:- Problems Caused by Spyware

- Data Theft and Identify Fraud
- Computer Damages
- Disruptions to your Braosing Experience

:- How to protect your computer from spyware

1. Enable or download a pop-up blocker
- Many browsers offer built-in blockers now, but you may want to set the filter on high to prevent anything from slipping in.

2. Limit runnable applications to a pre-approved whitelist.
- You can control which applications run and what permissions they have. On your admin-level account, set of malware, links and attachments can carry all kinds of malicious payloads

Q.3) Write a short note on Trojan and backdoors?

Ans - Trojan is a type of malware that is often disguised as legitimate software.
- It can be employed by cyber-thieves and hackers trying to gain access to user's systems
- It can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.
- These actions can include:
  - Deleting data
  - Blocking data
  - Modifying data
  - Copying data
  - Disrupting the performance of computers networks

- Unlike computes virus and worms, Trojans are not able to self-replicate.

- How Trojans can impact you:

- Backdoor
- Exploit
- Rootkit
- Trojan-Banker
- Trojan-DDOS
- Trojan-Downloader
- Trojan-Dropper
- Trojan-FakeAV
- Trojan-GameThief
- Trojan-IM
- Trojan-Ransom
- Trojan-SMS
- Trojan-Spy
- Trojan-Mailfinder

- How to protect yourself against Trojans

- By installing effective anti-malware software, you can defend your devices - including PCs, laptops, Macs, tablets, and smartphones - against Trojans.

- 

* Backdoors

- Backdoor is a malicious computer program used to provide the attacker with unauthorized remote access to a compromised PC by exploiting security vulnerabilities.
- This backdoor virus works in the background and hides from the user.
- A backdoor, is a secret entry point into a program that allows someone that is aware of the backdoor to gain access without going through the usual security access procedures.

- "A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network, or software application."

-:- How can I protect against backdoors?

- Change your default passwords
- choose applications and plug-in carefully.
- Use a good cyber security solution
- Monitor network activity.

Q.4b Discuss DOS and DDOS attack?

Ans - A DDOS attack is launched from numerous compromised devices, often distributed globally referred ~~as~~ to as A botnet.

"A botnet is a number of Internet-connected devices, each of which is ~~run~~ running one or more bots. Botnets can be used to perform Distributed Denial-of-service (DDOS) attacks, steal data, send spam, and allows the attackers to access the device and its connection".

- Dos and DDOS attacks can be divided into three types:

- Volume Based Attacks: Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

- Protocol Attacks: Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDos and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (pps).

- Common DDoS attacks types:

- Some of the most commonly used DDoS attack types include:

  - UDP Flood
  - ICMP (Ping) Flood
  - SYN Flood
  - Ping of Death
  - Slowloris
  - NTP Amplification
  - HTTP Flood
  - zero-day DDos attacks

- Motivation behind DDos attack

- DDos attacks are quickly becoming the most prevalent type of cyber threat, growing rapidly in the past years in both number and volume according to recent market research.
- The trend is towards shorter attack duration, but bigger packet-per-second attack volume.

Q.5) Discuss on SQL Injection

Ans SQL injection (SQLi) is an application security weakness that allows attackers to control an application's database - letting them access or delete data, change an application's data-driven behaviours, and do other undesirable things - by tricking the application into sending unexpected SQL commands.

- How attackers Exploit SQLi Vulnerabilities.

- Attackers provide specially-crafted input to trick an application into modifying the SQL queries than the application asks the database to execute.
- This allows the attacker to :

- Control application behaviour that's based on data in the database,
- Alter data in the database without authorization,
- Access data without authorization,

- Anatomy of a SQL injection Attack

- A SQLi attack plays out in two stages
- Research : Attacker tries submitting various unexpected values for the argument, observes how the application responds, and determines an attack to attempt.

- Attack: It provides a carefully-crafted input value that, when used as an argument to a SQL query, will be interpreted as a part of a SQL command rather than merely data: the database then executes the SQL command as modified by the attacker.

Q.6] What is buffer overflow?

Ans A buffer overflow, or buffer overrun, occurs when more data is put into a fixed-length buffer than the buffer can handle.

- The extra information, which has to go somewhere, can overflow into adjacent memory space, corrupting or overwrite the data held in that space.
- The overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitary code or manipulate the coding errors to prompt malicious actions.

- Key concepts of Buffer Overflow

- This error occurs when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage.
- This vulnerability can cause a system crash, or, worse, create an entry point for a cyberattack.

- C and C++ are most susceptible to buffer overflow.

Q.7) Discuss about the attack on wireless network?

Ans Malicious activities putting at risk the security of the information and of the computing resources in wireless scenarios.

- A wireless attack is a malicious action against wireless system information or wireless network examples, can be denial of service attacks, penetration.

- Types of wireless Attack

1.) Rogue Wireless ~~Attacks~~ Devices:

- A rogue wireless device, is an unauthorized wifi devices added onto the network that isn't under the management of the network admins.
- They allow potential attackers or gateway into a network.

2) Peer-to-Peer Attacks:

- Devices that are connected to the same access point can be vulnerable to attacks from other devices connected to that access point.

- Most providers provide for an option such as "client Isolation" which ensures that clients connected to the access point cannot communicate with each other, preventing this issue

3) Eavesdropping

- These is where wireless communication are monitored.
- These are two types of eavesdropping.
- The first, casual ~~eves~~ eavesdropping, or sometimes called WLAN discovery, is where a wireless client actively scans for wireless access points
- The second type, malicious eavesdropping, is the illegal kind.
- This is where someone tries to listen in on the data transferred between clients and the access point.

4) Encryption Cracking:

- This is where the attacker attempts to crack the ~~not~~ encryption on the network.
- WEP networks are the most susceptible to this, being that they can be easily cracked in a little as 5 minutes.
- It is important to ensure that you use the most secure encryption you can, and avoid using WEP where possible.

5) Authentication Attack:

- This is where the attacker scrapes a frame exchange between a client authenticating with the network, and then they simply run an offline dictionary attack.
- With this sort of information, and depending on the strength of the password, it could be just a matter of time before they crack the password and gain access.

6) MAC Spoofing:

- MAC Spoofing is an extremely easy thing to do.
- Because of this, using MAC filtering to control which devices can connect to your network is secure at all.
- It can however be used in conjuction with other security measures to build up an overall more secure network architecture.

7) Management Interface Exploits:

- This sort of attack can become an issue when you make use of some devices such as wireless controllers that allow you to control your access point via things like web interfaces or console access.

8) Denial of services:

- This term covers a number of different things. DoS attack can occur on different layers.

Layer 1: attacks are known as RF jamming attacks, and can be both intentional and unintentional.

Layer 2: attacks can occur in a number of different ways.

Q.8b Write a short note is steganography?

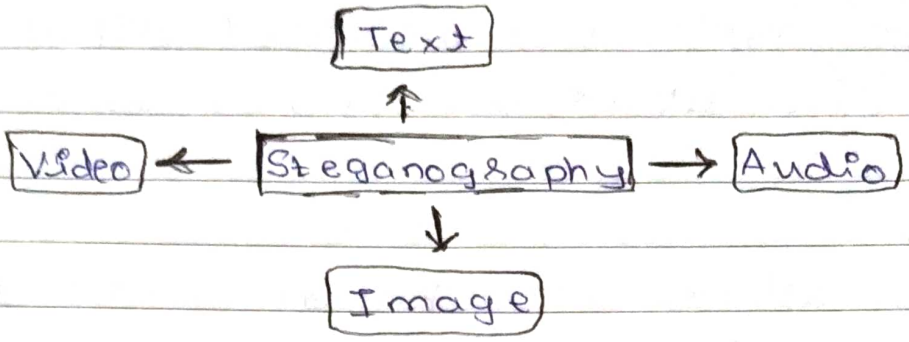
Ans - The art and science of hiding information by embalming it in some other data.

- Steganography primary goal is to hide data within some other data such that the hiddin data can not be detected.
- Most frequently steganography is applied to images but many other data or files are possible audio, video, text and executable programs

- Uses of steganography

- Steganography can also be used to implement watermarking.
- E-commerce allows for an interesting use of steganography
- The transportation of sensitive data is another key use of Steganography.

- Types of steganography




1) Image steganography
- JPEG compression is a commonly used method for reducing the size of an image, without reducing the aesthetic qualities enough to become noticeable by the naked eye.

2) Audio steganography
- It is the technology of embedding information in an audio channel. It is used for digital copyright protection

3) Video steganography
- Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too.

4) Text steganography
- One major category, perhaps the most difficult kind of steganography is text & linguistic steg becomes due to the lack of redundat info. in a text compared to Audio video

- Advantages

- Important files carrying confidential info. can be in the serves in and encrypted form No intruders can get any useful information from the original file during transmit.

- With the use of steganography ~~Corps~~ Corporation government and law enforcement agencies can communicate secretly.

- Limitation

- Hugh numbers of data, huge file size, so someone can suspect about it.

- If this techniques is gone in the wrong hands like hackers, terrorist, criminals then this can be very much dangerous