Sardar Patel College OF Engineering ,Bakrol

# UNIT -5

Cyber Security

(3150714)

Prepared By

Prof.Keyur Patel

Department : Information Technology

## What is Cybercrime Investigation

Cybercrime investigation is the process of investigating, analyzing and recovering critical forensic digital data from the networks 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 networks and hardware work. They must be knowledgeable 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 gains access to your cloud, server or physical device without your permission. Hackers may gain access to your computer or device through security weaknesses, malware or phishing. Once they have compromised your email, banking or social media accounts, they can change passwords preventing you from accessing your account. Scammers often send out messages impersonating and directing people to fake websites, or asking them to send money. Modern attacks are very sophisticated the fake websites may seem to be genuine.

## Sophisticated attacks Investigation

Sophisticated criminals are active daily to exploit vulnerabilities on computers and other devices. Some of the techniques they use include:

- **unauthorised access or hacking** – when someone gains access to your computer or device without permission,
- **malware** – malicious software (such as viruses, trojans and spyware) which monitor your online activity and cause damage to the computer,
- **denial of service attacks** – an attack which floods a computer or website with data, causing it to overload and prevent it from functioning properly. This type of attack is more frequently targeted at businesses, rather than individuals.

## DDOS - Denial of service or distributed denial of service attacks Investigation

Cyber attacks are common and often a method seen is a denial of service attack which floods a computer or website with data, which can overload the system or computer and prevent it from functioning properly. Unlike hacking or malware, it generally doesn't involve access to the computer system. A distributed denial of service (DDoS) attack is a denial of service attack that comes from multiple systems, often a network of compromised computers.

## Email Fraud Investigation

Digitpol's Cyber 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. Digitpol can deploy forensic examiners to investigate hacking, determine how it took place and report the findings, Digitpol ensures that hackers are not active in your network and ensure your user accounts policies and rules are configured correctly to prevent further attacks.

## Phishing Attack Investigation

Phishing attacks, email fraud, scams, online fraud happens in most cases when cyber criminals find ways to hack into the email servers or accounts of small and medium companies, often targeting those with business in Asia countries. Cyber criminals gain access to email accounts and search through email accounts looking for sensitive information such as outstanding, unpaid invoices or data relating to financial transactions and business between supplier, vendor and clients. When cyber criminals identify a sale or a due invoice, the fraudsters then send various fictitious emails from the hacked email account or an email address replicated to the original purporting to be in charge of the sale or due invoice to be paid, the fraudster is then asking for transfers of funds into a nominated bank account, usually giving an excuse that there is a problem at the bank and an alternative account needs to be used. It is common that the nominated account is in the same name as the company name or with a very slight change such as an extra letter. It is common the bank account to be in the same city as the victim or client.

## Cyber Crime

bank Fraud
Email Fraud
Online Fraud
Social Media Fraud
Phone / SMS

## Who conducts cybercrime investigations?

**Criminal justice agencies**
**National security agencies**
**Private security agencies**

**Cybercrime investigation techniques**

While techniques may vary depending on the type of cybercrime being investigated, as well as who is running the investigation, most digital crimes are subject to some common techniques used during the investigation process.

- **Background check**: Creating and defining the background of the crime with known facts will help investigators set a starting point to establish what they are facing, and how much information they have when handling the initial cybercrime report.
- **Information gathering**: One of the most important things any cybersecurity researcher must do is grab as much information as possible about the incident.
- **Tracking and identifying the authors**: , both private and public security agencies often work with ISPs and networking companies to get valuable log information about their connections, as well as historical service, websites and protocols used during the time they were connected.
- **Digital forensics**: Once researchers have collected enough data about the cybercrime, it's time to examine the digital systems that were affected, or those supposed to be involved in the origin of the attack. This process involves analyzing network connection raw data, hard drives, file systems, caching devices, RAM memory and more. Once the forensic work starts, the involved researcher will follow up on all the involved trails looking for fingerprints in system files, network and service logs, emails, web-browsing history, etc.

# Keylogger

Keyloggers : Key loggers is also known as keystrock logging ot key logging.

## Keylogger definition

Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

## How do keyloggers work?

Keyloggers collect information and send it back to a third party – whether that is a criminal, law enforcement or IT department. “Keyloggers are software programs that leverage algorithms that monitor keyboard strokes through pattern recognition and other techniques,”

The amount of information collected by keylogger software can vary. The most basic forms may only collect the information typed into a single website or application. More sophisticated ones may record everything you type no matter the application, including information you copy and paste. Some variants of keyloggers – especially those targeting mobile devices – go further and record information such as calls (both call history and the audio),information from messaging applications, GPS location, screen grabs, and even microphone and camera capture.

## Best practices for detecting and removing keyloggers

**1.Monitor resource allocation, processes and data :** Observing resource allocation and background process on machines, as well as data being transmitted from the device outside the organization can help identify if a keylogger is present. Keyloggers usually need root access to the machine, which can also be a telltale sign of a keylogger infection.

**2.Keep antivirus and anti-rootkit protection up to date :** As keyloggers often come bundled with other forms of malware, discovering keylogger malware might be an
indicator of a wider attack or infection. Up-to-date antivirus protection and anti-rootkit protectors will remove known keylogger malware, according to Jeff Wichman, practice director for Optiv Security, but may warrant further investigation to determine whether the keylogger was just one component of a larger attack.

**3.Use anti-keylogger software:** Dedicated anti-logger software is designed to encrypt keystrokes as well as scan for and remove known loggers and flag unusual keylogging-like behavior on the machine. Blocking root access for unauthorized applications and blacklisting known spyware apps will also help

**4.Consider virtual onscreen keyboards:** Virtual onscreen keyboards reduce the chance of being keylogged as they input information in a different way to
physical keyboards. This might impact user productivity, isn't foolproof against all kinds of keystroke monitoring software, and doesn't eliminate the cause of the problem

**5.Disable self-running files on external devices:** Disabling self-running files on externally connected devices such as USBs and restricting copying of files to and from external to computers may also reduce the possibility of infection

**6.Have a strong password policy :** "While checking task managers for unknown or suspicious installations, and recognizing odd occurrences such as keys pausing or not displaying on screen when typing can help individuals detect keyloggers in certain cases,"
advises Bain, "the best way for organizations to stay safe is to ensure that their password policy is multi-faceted, and that two-factor authentication is implemented across company accounts and devices. It's important to never assume that the average antivirus technology is enough."

## Spyware

**Spyware** is loosely defined as malicious software designed to enter your computer device, gather 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.
examples of spyware
Spyware is mostly classified into four types: adware, system monitors, tracking cookies, and trojans; examples of other notorious types include digital rights management capabilities that "phone home", keyloggers, rootkits, and web beacons.

Malicious spyware is a type of malware specifically installed without your informed consent. Step-by-step,
spyware will take the following actions on your computer

1.Infiltrate — via an app install package, malicious website, or file attachment.
2. Monitor and capture data — via keystrokes, screen captures, and other tracking codes.
3. Send stolen data — to the spyware author, to be used directly or sold to other parties
Data compromised by spyware often includes collecting confidential info such as:

- Login credentials — passwords and usernames
- Account PINs
- Credit card numbers
- Monitored keyboard strokes
- Tracked browsing habits
- Harvested email addresses

## Types of Spyware

Spyware is generally classified into four main categories:

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 malicious ads.
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 Identity Fraud:** your computer, it can harvest more than enough information to imitate your identity. Information used for this purpose includes browsing history, email accounts, and saved b passwords for online banking, shopping, and social networks. Also, if you've visited online banking sites, spyware can siphon your bank account information or credit card account and sell it to third parties — or use them directly.

**Computer Damages:** More commonly, you will face the damage spyware can do to your computer. Spyware can be poorly designed, leading to system-draining performance. The lack of performance optimization can take up an enormous amount of your computer's memory, processing power, and internet bandwidth. As a result, infected devices may run slowly and lag in between applications or while online. Worse cases include frequent system crashing or overheating your computer, causing permanent damage. Some spyware can even disable your internet security programs.

**Disruptions to Your Browsing Experience:** Spyware can also manipulate search engine results and deliver unwanted websites in your browser, which can lead to potentially harmful websites or fraudulent ones. It can also cause your home page to change and can even alter some of your computer's settings. Pop-up advertisements are an equally frustrating issue that accompanies some types of spyware. Advertisements may appear even when offline, leading to inescapable annoyances.

## 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 for malware, links and attachments can carry all kinds of malicious payloads. Even filesfrom trusted senders can be malicious if their accounts have been hacked via phishing.

# Trojans

Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.

Trojans 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 or computer networks

Unlike computer viruses and worms, Trojans are not able to self-replicate.

## How Trojans can impact you

Trojans are classified according to the type of actions that they can perform on your computer:

- **Backdoor**
  A backdoor Trojan gives malicious users remote control over the infected computer. They enable the author to do anything they wish on the infected computer – including sending, receiving, launching and deleting files, displaying data and rebooting the computer. Backdoor Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.
- **Exploit**
  Exploits are programs that contain data or code that takes advantage of a vulnerability within application software that's running on your computer.
- **Rootkit**
  Rootkits are designed to conceal certain objects or activities in your system. Often their main purpose is to prevent malicious programs being detected
- **Trojan-Banker**
  Trojan-Banker programs are designed to steal your account data for online banking systems, e-payment systems and credit or debit cards.
- **Trojan-DDoS**
  These programs conduct DoS (Denial of Service) attacks against a targeted web address. By sending multiple requests – from your computer and several other infected computers – the attack can overwhelm the target address… leading to a denial of service.
- **Trojan-Downloader**
  Trojan-Downloaders can download and install new versions of malicious programs onto your computer – including Trojans and adware.
- **Trojan-Dropper**
  These programs are used by hackers in order to install Trojans and / or viruses – or to prevent the detection of malicious programs. Not all antivirus programs are capable of scanning all of the components inside this type of Trojan.

- **Trojan-FakeAV**
  Trojan-FakeAV programs simulate the activity of antivirus software. They are designed to extort money from you – in return for the detection and removal of threats… even though the threats that they report are actually non-existent.
- **Trojan-GameThief**
  This type of program steals user account information from online gamers.
- **Trojan-IM**
  Trojan-IM programs steal your logins and passwords for instant messaging programs – such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype and many more.
- **Trojan-Ransom**
  This type of Trojan can modify data on your computer – so that your computer doesn't run correctly or you can no longer use specific data. The criminal will only restore your computer's performance or unblock your data, after you have paid them the ransom money that they demand.
- **Trojan-SMS**
  These programs can cost you money – by sending text messages from your mobile device to premium rate phone numbers.
- **Trojan-Spy**
  Trojan-Spy programs can spy on how you're using your computer – for example, by tracking the data you enter via your keyboard, taking screen shots or getting a list of running applications.
- **Trojan-Mailfinder**
  These programs can harvest email addresses from your computer.

- **Other types of Trojans include:**
  Trojan-ArcBomb,Trojan-Clicker,Trojan-Notifier,Trojan-Proxy,Trojan-PSW

## 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**. A rigorous anti-malware solution – such as Kaspersky Anti-Virus – will detect and prevent Trojan attacks on your PC, while Kaspersky that defend the following devices against Trojans:

- Windows PCs
- Linux computers
- Apple Macs
- Smartphones
- Tablets

# 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.

backdoor attack can have two different meanings. The original term backdoor referred to troubleshooting and developer hooks into systems. During the development of a complicated operating system or application, programmers add backdoors or maintenance hooks. Backdoors allow them to examine operations inside the code while the code is running.

The second type of backdoor refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker. The program may allow a certain user ID to log on without a password or gain administrative privileges. The attacker is using a back door program to utilize resources or steal information
There are number of tools exist to create backdoor attacks on systems. One of the more popular is NetBus.

"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.

# Viruses

Any operating system that allows third-party programs to run can support viruses.
A computer virus is a program that performs unauthorized actions, without the knowledge of the user. The anti-virus company Symantec has defined two criteria a program must meet to be classified as a computer virus. These are:

- It must execute itself. It will often place its own code in the path of execution of another program
- It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike

To meet the first criterion the virus must be attached to executable code in files or memory. This will result in the execution of virus code every time the infected code is used. There are different ways to make the execution process of the virus *invisible* to the user. An often used approach in viruses is to turn over the control to the original portion of the infected program, when the execution reaches its end. The original program will start and the user will probably not notice the small, but a bit longer start-up time.

The second criterion is met when the virus attaches itself to other files or memory areas.

# Worms

A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.

## How do computer worms work?

Worms can be transmitted via software vulnerabilities. Or computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it's installed, the worm silently goes to work and infects the machine without the user's knowledge.

Worms can modify and delete files, and they can even inject additional malicious software onto a computer. Sometimes a computer worm's purpose is only to make copies of itself over and over — depleting system resources, such as hard drive space or bandwidth, by overloading a shared network. In addition to wreaking havoc on a computer's resources, worms can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings.

## How to tell if your computer has a worm

If you suspect your devices are infected with a computer worm, run a virus scan immediately. Even if the scan comes up negative, continue to be proactive by following these steps.

1. **Keep an eye on your hard drive space.** When worms repeatedly replicate themselves, they start to use up the free space on your computer.
2. **Monitor speed and performance.** Has your computer seemed a little sluggish lately? Are some of your programs crashing or not running properly? That could be a red flag that a worm is eating up your processing power.
3. **Be on the lookout for missing or new files.** One function of a computer worm is to delete and replace files on a computer.

## How to help protect against computer worms

Computer worms are just one example of malicious software. To help protect your computer from worms and other online threats, take these steps.

1. Since software vulnerabilities are major infection vectors for computer worms, be sure your computer's operating system and applications are up to date with the latest versions. Install these updates as soon as they're available because updates often include patches for security flaws.
2. Phishing is another popular way for hackers to spread worms (and other types of malware). Always be extra cautious when opening unsolicited emails, especially those from unknown senders that contain attachments or dubious links.
3. Be sure to invest in a strong internet security software solution that can help block these threats. A good product should have anti-phishing technology as well as defenses against viruses, spyware, ransom ware, and other online threats.

## DOS and DDOS attack

A DDoS attack is launched from numerous compromised devices, often distributed globally referred to as A botnet.

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

Broadly speaking, 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). more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second (Rps).

**Common DDoS attacks types**

Some of the most commonly used DDoS attack types include:

**UDP Flood**

A UDP flood, by definition, is any DDoS attack that floods a target with User Datagram Protocol (UDP) packets. The goal of the attack is to flood random ports on a remote host. This causes the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP 'Destination Unreachable' packet. This process saps host resources, which can ultimately lead to inaccessibility.

**ICMP (Ping) Flood**

Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.

**SYN Flood**

A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the "three-way handshake"), wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

**Ping of Death**

A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size – for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

**Slowloris**

Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by

creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

### NTP Amplification

In NTP amplification attacks, the perpetrator exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm a targeted server with UDP traffic. The attack is defined as an amplification assault because the query-to- response ratio in such scenarios is anywhere between 1:20 and 1:200 or more. This means that any attacker that obtains a list of open NTP servers (e.g., by a using tool like Metasploit or data from the Open NTP Project) can easily generate a devastating high-bandwidth, high-volume DDoS attack.

### HTTP Flood

An HTTP flood attack utilizes what appear to be legitimate HTTP GET or POST requests to attack a web server or application. These flooding attacks often rely on a botnet, which is a group of Internet-connected computers that have been maliciously appropriated through the use of malware such as a Trojan Horse.

### Zero-day DDoS Attacks

The "Zero-day" definition encompasses all unknown or new attacks, exploiting vulnerabilities for which no patch has yet been released. The term is well-known amongst the members of the hacker community, where the practice of trading zero-day vulnerabilities has become a popular activity.

## Motivation behind DDoS attacks

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

**Attackers are primarily motivated by:**

- Ideology – So called "hacktivists" use DDoS attacks as a means of targeting websites they disagree with ideologically.
- Business feuds – Businesses can use DDoS attacks to strategically take down competitor websites, e.g., to keep them from participating in a significant event, such as Cyber Monday.
- Boredom – Cyber vandals, a.k.a., "script-kiddies" use prewritten scripts to launch DDoS attacks. The perpetrators of these attacks are typically bored, would-be hackers looking for an adrenaline rush.
- Extortion – Perpetrators use DDoS attacks, or the threat of DDoS attacks as a means of extorting money from their targets.

- Cyber warfare – Government authorized DDoS attacks can be used to both cripple opposition websites and an enemy country's infrastructure.

## Imperva solutions mitigate DDoS damage

Imperva seamlessly and comprehensively protects websites against all three types of DDoS attacks, addressing each with a unique toolset and defense strategy:

1. **Volume Based Attacks**

   Imperva counters these attacks by absorbing them with a global network of scrubbing centers that scale, on demand, to counter multi-gigabyte DDoS attacks.
2. **Protocol Attacks**

   Imperva mitigates this type of attack by blocking "bad" traffic before it even reaches the site, leveraging visitor identification technology that differentiates between legitimate website visitors (humans, search engines etc.) and automated or malicious clients.
3. **Application Layer Attacks**

   Imperva mitigates Application Layer attacks by monitoring visitor behavior, blocking known bad bots, and challenging suspicious or unrecognized entities with JS test, Cookie challenge,

In all these scenarios, Imperva applies its D DoS protection solutions outside of your network, meaning that only filtered traffic reaches your hosts. Moreover, Imperva maintains an extensive DDoS threat knowledge base, which includes new and emerging attack methods. This constantly-updated information is aggregated across our entire network – identifying new threats as they emerge, detecting known malicious users, and applying remedies in real-time across all Imperva-protected websites.

# Buffer Overflow

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 overwriting the data held in that space. This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary 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 more susceptible to buffer overflow.

# What is SQL Injection?

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 behavior, and do other undesirable things – by tricking the application into sending unexpected SQL commands. SQL injections are among the most frequent threats to data security.

SQL injection weaknesses occur when an application uses untrusted data, such as data entered into web form fields, as part of a database query. When an application fails to properly sanitize this untrusted data before adding it to a SQL query, an attacker can include their own SQL commands which the database will execute. Such SQLi vulnerabilities are easy to prevent, yet SQLi remains a leading web application risk, and many organizations remain vulnerable to potentially damaging data breaches resulting from SQL injection.

## How Attackers Exploit SQLi Vulnerabilities

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

- Control application behavior that's based on data in the database, for example by tricking an application into allowing a login without a valid password
- Alter data in the database without authorization, for example by creating fraudulent records, adding users or "promoting" users to higher access levels, or deleting data
- Access data without authorization, for example by tricking the database into providing too many results for a query

## Anatomy of a SQL Injection Attack

A developer defines a SQL query to perform some database action necessary for their application to function. This query has an argument so that only desired records are returned, and the value for that argument can be provided by a user (for example, through a form field, URL parameter, web cookie, etc.).

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

The research and attack stages can be easily automated by readily-available tools.

## Defending Against SQLi Attacks

There are easy ways to avoid introducing SQLi vulnerabilities in an application, and to limit the damage they can cause.

- Discover SQLi vulnerabilities by routinely testing your applications both using static testing and dynamic testing.
- Avoid and repair SQLi vulnerabilities by using parameterized queries. These types of queries specify placeholders for parameters so that the database will always treat them as data rather than part of a SQL command. Prepared statements and object relational mappers (ORMs) make this easy for developers.
- Remediate SQLi vulnerabilities in legacy systems by escaping inputs before adding them to the query. Use this technique only where prepared statements or similar facilities are unavailable.
- Mitigate the impact of SQLi vulnerabilities by enforcing least privilege on the database. Ensure that each application has its own database credentials, and that these credentials have the minimum rights the application needs.

## Wireless Network Attack

Malicious activities putting at risk the security of the information and of the computing resources in wireless scenarios. Learn more in: IDS and IPS Systems in Wireless Communication Scenarios

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

**Types of Wireless Attacks**

1. Rogue Wireless Devices
2. Peer-to-peer Attacks
3. Eavesdropping
4. Encryption Cracking
5. Authentication Attacks
6. MAC Spoofing
7. Management Interface Exploits
8. Denial Of Service

**1. Rogue Wireless Devices:**

A rogue wireless device, is an unauthorised WiFi device added onto the network that isn't under the management of the network admins. They allow potential attackers a gateway into the network.

This sort of device can be maliciously installed if the attacker has direct access to the wired network, but more often than not they are added by staff that are not aware of the implications.

2. **Peer-to-peer Attacks:**

   Devices that are connected to the same access points 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 eachother, preventing this issue.

3. **Eavesdropping:**

   This is where wireless communications are monitored. There are two types of of eavesdropping.

   The first, casual 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. Because of this, it is essential to encrypt your networks, as anything unencrypted can be listened in on.

4. **Encryption Cracking:**

   This is where the attacker attempts to crack the encryption on the network. WEP networks are the most susceptible to this, being that they can be easily cracked in as little as 5minutes.

   It is important to ensure that you use the most secure encryption you can, and avoid using WEP where possible.

5. **Authentication Attacks:**

   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. Because of this it’s important to keep your login credentials as secure as possible.

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 not secure at all.

It can however be used in conjunction 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 points via things like web interfaces or console access.

8. **Denial of Service:**

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

   **Layer 1** attacks are known as RF jamming attacks, and can be both intentional (attacker generating a Signal to deliberately cause interference) and unintentional (devices such as microwaves or wireless phones causing interference

   **Layer 2** attacks can occur in a number of different ways. For example, an attacker can flood an AP spoofed association and disassociation requests.

## Steganography

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 deleted.

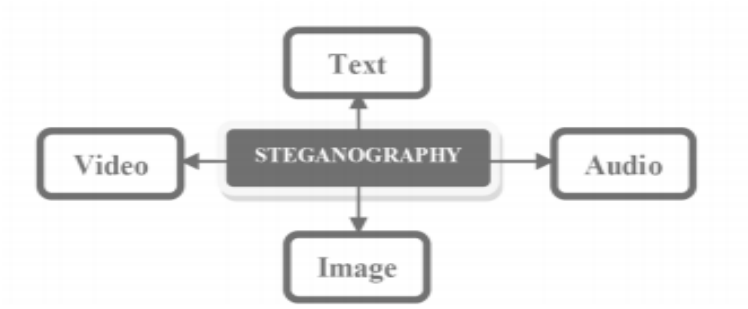
Most frequently Steganography is applied to images but many other data or files are possible audio ,video, text and executable programs.

## Uses Of Steganography

- Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
- It is also possible to simply use steganography to store information on a location.
- Steganography can also be used to implement watermarking.
- E-commerce allows for an interesting use of steganography.
- Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

- 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. Broadly speaking, it extracts all the information from an image that the human eye is not perceptible to and would therefore not miss should it not be there.

2. **Audio Steganography**

   Audio Steganography is the technology of embedding information in an audio channel. It is used for digital copyright protection. Watermarking is the technique which hides one piece of information [message] in another piece of information [carrier]. It is widely used for applications such as audio clip etc.

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. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images & sounds. Therefore, any small out otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

4. **Text Steganography**

   One major category, perhaps the most difficult kind of Steganography is text Steganography or linguistic Steganography because due to the lack of redundant information in a text compared to an image or audio. The text Steganography is a method of using written natural language to conceal a secret message. The advantage to prefer text Steganography over other media is its smaller memory occupation and simpler communication.

## ADVANTAGES

- The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.
- This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.
- Important files carrying confidential information can be in the server in and encrypted form No intruder can get any useful information from the original file during transmit.
- With the use of Steganography Corporation government and law enforcement agencies can communicate secretly.

## Limitation

- Huge number 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.