Cyber Security

Subject Code:-102045607

Unit-2 Hackers And Cyber Crimes

Hackers and Types of Hackers

- Gaining access to a system that you are not supposed to have access is considered as hacking. For example: login into an email account that is not supposed to have access, gaining access to a remote computer that you are not supposed to have access, reading information that you are not supposed to able to read is considered as hacking. There are a large number of ways to hack a system.

- In 1960, the first known event of hacking had taken place at MIT and at the same time, the term Hacker was organized.

Hackers and Types of Hackers

Types of Hackers:-

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

Black Hat Hacker

- Black-hat Hackers are also known as an **Unethical Hacker or a Security Cracker**. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White Hat Hacker

- White hat Hackers are also known as **Ethical Hackers or a Penetration Tester**. White hat hackers are the good guys of the hacker world.
- These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray Hat Hacker

- Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.
- In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

Hackers and Crackers

- **Hackers:** Hackers are kind of good people who do hacking for a good purpose and to obtain more knowledge from it. They generally find loopholes in the system and help them to cover the loopholes. Hackers are generally programmers who obtain advanced knowledge about operating systems and programming languages. These people never damage or harm any kind of data.

- **Crackers:** Crackers are kind of bad people who break or violate the system or a computer remotely with bad intentions to harm the data and steal it. Crackers destroy data by gaining unauthorized access to the network. There works are always hidden as they are doing illegal stuff. Bypasses passwords of computers and social media websites, can steal your bank details and transfer money from the bank.

Hackers and Crackers

Difference between Hackers and Crackers:

Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled, some of crackers just knows a few tricks to steal data.
They work in an organisation to help protecting there data and giving them expertise on internet security.	These are the person from which hackers protect organisations .
Hackers share the knowledge and never damages the data.	If they found any loop hole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benifit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for there cause and harm the network.
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as there motive is to stay annonymous.
They are known as White hats or saviors.	They are known as Black hats or evildoers.

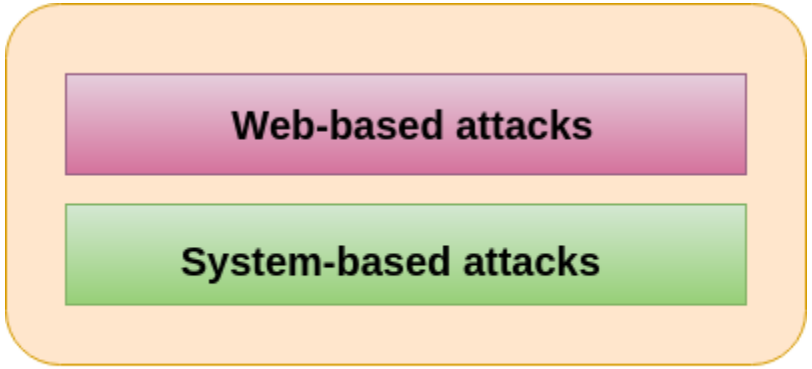
Cyber-Attacks

Types of Cyber Attacks

- A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

- We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

- Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Cyber-Attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

Cyber-Attacks

Web-based attacks

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is simulate as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server.

Cyber-Attacks

Web-based attacks

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

Cyber-Attacks

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

Cyber-Attacks

System-based attacks

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Vulnerabilities

- A vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for initiating cybercrimes and are open to exploitation through the points of vulnerability.

- These hackers are able to gain illegal access to the systems and cause severe damage to data privacy. Therefore, cybersecurity vulnerabilities are extremely important to monitor for the overall security posture as gaps in a network can result in a full-scale breach of systems in an organization.

- **Examples of Vulnerabilities-**

A weakness in a firewall that can lead to malicious hackers getting into a computer network, Lack of security cameras, Unlocked doors at businesses,etc.

Vulnerabilities

Types of Vulnerabilities

1. **System Misconfigurations**

- Network assets that have disparate security controls or vulnerable settings can result in system misconfigurations. Cybercriminals commonly probe networks for system misconfigurations and gaps that look exploitable. Due to the rapid digital transformation, network misconfigurations are on the rise. Therefore, it is important to work with experienced security experts during the implementation of new technologies.

2. **Out-of-date or Unpatched Software**

- Similar to system misconfigurations, hackers tend to probe networks for unpatched systems that are easy targets. These unpatched vulnerabilities can be exploited by attackers to steal sensitive information. To minimize these kinds of risks, it is essential to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.

Vulnerabilities

Types of Vulnerabilities

3. Missing or Weak Authorization Credentials

- A common tactic that attackers use is to gain access to systems and networks through brute force like guessing employee credentials. That is why it is crucial that employees be educated on the best practices of cybersecurity so that their login credentials are not easily exploited.

4. Malicious Insider Threats

- Whether it's with malicious intent or unintentionally, employees with access to critical systems sometimes end up sharing information that helps cyber criminals breach the network. Insider threats can be really difficult to trace as all actions will appear legitimate. To help fight against these types of threats, one should invest in network access control solutions, and segment the network according to employee seniority and expertise.

Vulnerabilities

Types of Vulnerabilities

5. Missing or Poor Data Encryption

- It's easier for attackers to intercept communication between systems and breach a network if it has poor or missing encryption. When there is poor or unencrypted information, cyber adversaries can extract critical information and inject false information onto a server. This can seriously undermine an organization's efforts toward cyber security compliance and lead to fines from regulatory bodies.

6. Zero-day Vulnerabilities

- Zero-day vulnerabilities are specific software vulnerabilities that the attackers have caught wind of but have not yet been discovered by an organization or user.
- In these cases, there are no available fixes or solutions since the vulnerability is not yet detected or notified by the system vendor. These are especially dangerous as there is no defence against such vulnerabilities until after the attack has happened. Hence, it is important to remain cautious and continuously monitor systems for vulnerabilities to minimize zero-day attacks.

Malware

Malware

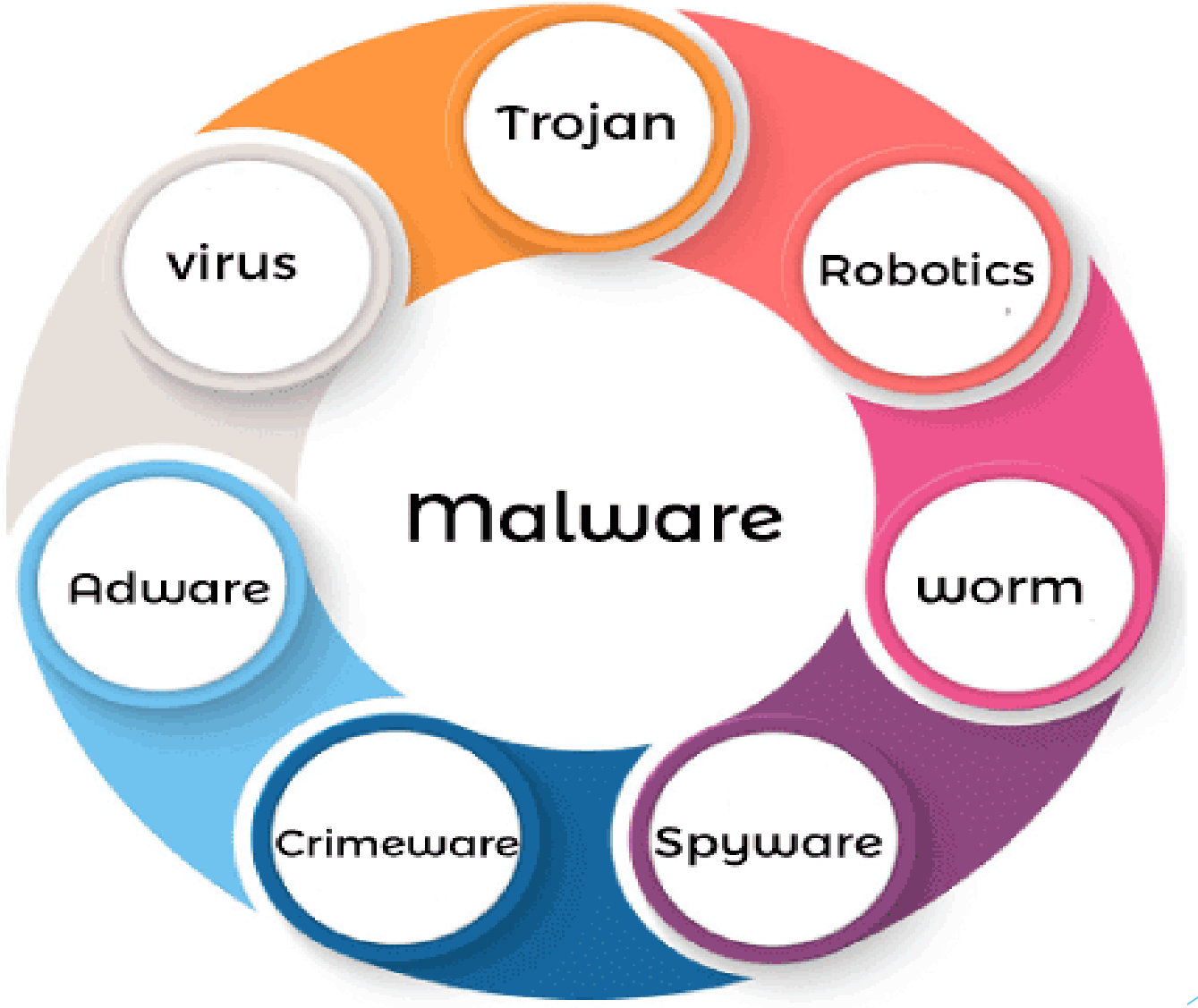
- Malware is **"Malicious software"**. It can be defined as a special kind of code or application specifically developed to harm electronic devices. It is an umbrella term that includes all types of malicious software like a virus, Trojan horses, worms, spyware, etc. Almost every kind of disruptive program is included in malware. It can cause many advertisements to appear on our computer screens, and those ads can be harmful if we accidentally click on them.

- Hackers or cybercriminals use malware to disrupt or damage a user's system. It is designed to destroy the data and resources of an organization or an individual. It can cause an error and can slow down the performance. It can be delivered by software installations, emails, internet surfing, etc.

- The most common way to keep your system protected from malware is by installing anti-malware or anti-virus software. Most of the malware can be scanned or removed by using an antivirus program.

Malware

Malware



Sniffing

- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

- There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

- In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

Sniffing

What can be sniffed?

One can sniff the following sensitive information from a network –

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

Sniffing

Types of Sniffing

Passive Sniffing

- In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

Active Sniffing

- In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques –

- MAC Flooding, DHCP Attacks
- DNS Poisoning, Spoofing Attacks
- ARP Poisoning

Gaining Access

- The Gaining Access in hacking is where an attacker uses all means to get unauthorized access to the target's systems, applications, or networks. An attacker can use various tools and methods to gain access and enter a system. This hacking phase attempts to get into the system and exploit the system by downloading malicious software or application, stealing sensitive information, getting unauthorized access, asking for ransom, etc. Metasploit is one of the most common tools used to gain access, and social engineering is a widely used attack to exploit a target.

- Ethical hackers and penetration testers can secure potential entry points, ensure all systems and applications are password-protected, and secure the network infrastructure using a firewall. They can send fake social engineering emails to the employees and identify which employee is likely to fall victim to cyberattacks.

Escalation of Privileges

An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privilege.

Escalation of Privileges:

There are two types of Privilege Escalation:

- **Horizontal Privilege Escalation** occurs when a malicious user attempts to access resources and functions that belong to peer users, who have similar access permissions.

- **Vertical Privilege Escalation** occurs when a malicious user attempts to access resources and functions that belong to a user with higher privileges, such as application or site administrators.

Executing Applications

- Intruder executes malicious applications after gaining administrative privileges so they can run malicious programs remotely, to capture all sensitive data, crack passwords, capture screenshots or to install a backdoor.

- Tool: RemoteExec, PDQ Deploy, DameWare NT Utilities

Keylogger

- keystroke loggers are programs or hardware devices that monitor each keystroke a user types on a keyboard, logs onto a file, or transmits them to a remote location.

- keyloggers are placed between the keyboard hardware and the OS

Escalation of Privileges

A key logger can

- Record each keystroke
- capture screenshots at regular intervals of time showing user activity such as when he or she types a character or click a mouse button
- Track the activities of users by logging window titles, names of launched applications and other information
- monitor online activity of users by recording addresses of the websites that they are have visited and with the keywords entered by them
- record all the login names, bank and credit card numbers and passwords including hidden passwords or data that are in asterisk or blank spaces
- record online chat conversion

Types of Keylogger

- Hardware Keylogger
- Software Keylogger

Hiding Files

Rootkits

Rootkits are programs that hackers use in order to evade detection while trying to gain unauthorized access to a computer. Rootkits when installing on a computer, are invisible to the user and also take steps to avoid being detected by security software.

A rootkit is a set of binaries, scripts and configuration files that allows someone to covertly maintain access to a computer so that he can issue commands and scavenge data without alerting the system's owner.

Depending on where they are installed there are various types of rootkits:

- Kernel Level Rootkits
- Hardware/Firmware Rootkits
- Hypervisor (Virtualized) Level Rootkits
- Boot loader Level (Bootkit) Rootkits

Covering Tracks

Once an attacker finishes his work, he wants to erase all tracks leading the investigators tracing back to him. This can be done using

- Disable auditing.
- Clearing logs.
- Modifying logs, registry files.
- Removing all files, folders created.

Worms

A worm virus refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm virus exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.

Worms consume large volumes of memory, as well as bandwidth. This results in servers, individual systems, and networks getting overloaded and malfunctioning. A worm is different from a virus, however, because a worm can operate on its own while a virus needs a host computer.

Worms

Classifications and Names of Worms

- **Email-Worm**

An email-worm refers to a worm that is able to copy itself and spread through files attached to email messages.

- **IM-Worm**

An Instant Messenger (IM) worm is a kind of worm that can spread through IM networks. When an IM-worm is operating, it typically finds the address book belonging to the user and tries to transmit a copy of itself to all of the person's contacts.

- **IRC-Worm**

An IRC-worm makes use of Internet Relay Chat (IRC) networks to send itself over to other host machines. An IRC-worm drops a script into the IRC's client directory within the machine it infects.

- **Net-Worm**

A net-worm refers to a kind of worm that can find new hosts by using shares made over a network. This is done using a server or hard drive that multiple computers access via a local-area network (LAN).

- **P2P-Worm**

A P2P-worm is spread through peer-to-peer (P2P) networks. It uses the P2P connections to send copies of itself to users.

Trojans

Remember ??

Trojans

- A Trojan Horse Virus is a type of malware that downloads onto a computer hidden as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

- A simple way to answer the question "what is Trojan" is it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.

Trojans

Purpose of Trojans

- Steal information such as passwords, security codes, credit card information using keyloggers
- Use victim´s PC as a botnet to perform DDoS attacks
- Delete or replace OS critical files
- Generate fake traffic to create DoS
- Download spyware, adware and malware
- Record screenshots, audio and video of victim´s PC
- Infect victim´s PC as a proxy server for relaying attacks
- Use victim´s PC as a botnet to perform DoS, spamming and blasting email messages

Trojans

There are various types of Trojans like

- HTTP/HTTPS Trojan
- Remote access Trojan
- FTP Trojans
- VNC Trojans
- Banking Trojans
- DOM based Trojan
- Destructive Trojan
- Botnet Trojan
- Proxy Trojan
- Data hiding Trojan

Countermeasures

- Avoid opening emails from unknown users
- Do not download free software's from untrusted sites
- Always upgrade and keep firewalls, IDS and anti-virus updated with latest patches and signatures
- Block all unnecessary ports
- Periodically check startup programs and processes running to find any malicious files running.

Virus

A virus is a self-replicating computer program that produces its own copy by attaching itself to another program, computer boot sector or document.

- It infects other programs,
- Alters Data
- Transforms itself
- Encrypts Itself
- Corrupt files and Programs
- Self Propagates

Virus

Different types of Viruses:

- **Boot sector virus:** Replaces itself with boot sector moving boot sector into another location on the hard disk
- **File overwriting or cavity Virus:** Replaces the content of files with some other content leaving the file unusable
- **Crypter:** Encrypts the contents of the file which causes the file unusable for the user
- **Polymorphic virus:** The virus code mutates itself by keeping the algorithm intact.
- **Tunnelling Virus:** These viruses trace the steps of interceptor programs that monitor operating system request so that they get into the BIOS and DOS to install themselves. To perform this activity they even tunnel under anti-virus software programs
- **Macro Virus:** Infects Microsoft products like WORD and EXCEL. They are usually written in the macro language visual basic language or VBA

Virus

Different types of Viruses:

- **Cluster Virus:** Modifies the directory entries so it always directs the user to the virus code instead of the actual program
- **Extension Virus:** Hides the extension of the virus files, deceiving the unsuspecting user to download the files.
- **Metamorphic Virus:** As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behaviour as well as their appearance.
- **Add-on Virus:** Add-on viruses append their code to the host code without making any changes to the latter or relocate the host code to insert their own code at the beginning.

Backdoors

- **“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 (aka root access) on a computer system, network, or software application.”**

- Backdoors allow the attackers to quietly get into the system by deceiving the security protocols and gain administrative access. It is similar to the real-life robbery in which robbers take advantage of the loopholes in a house and get a 'backdoor' entry for conducting the theft.
- After gaining high-level administrative privilege, the cyber attackers could perform various horrendous tasks like injecting spyware, gaining remote access, hack the device, steal sensitive information, encrypt the system through ransomware, and many more.
- Backdoors are originally meant for helping software developers and testers, so they are not always bad.

Thank you!