***Cybercrime*** is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, ***cybercrime*** is committed by ***cybercriminals*** or hackers who want to make money. ***Cybercrime*** is carried out by individuals or organizations.

## Common forms of cybercrime include:

- phishing: using fake email messages to get personal information from internet users;
- misusing personal information (identity theft);
- hacking: shutting down or misusing websites or computer networks;
- spreading hate and inciting terrorism;
- distributing child pornography;
- Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy.

**KEY TERMINOLOGIES :**

Vulnerability

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks. The existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system. Exploit code is written to target vulnerability and cause a fault in the system in order to retrieve valuable data.

Exploit

A piece of software or technology that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system. Malicious hackers are looking for exploits in computer systems to open the door to an initial attack. Most exploits are small strings of computer code that, when executed on a system, expose vulnerability. Experienced hackers create their own exploits, but it is not necessary to have any programming skills to be an ethical hacker as many hacking software programs have ready-made exploits that can be launched against a computer system or network. Specific way to breach the security of an IT system through a vulnerability.

Exposure

Exposure is a problem or mistake in the system configuration that allows an attacker to conduct information gathering activities.

Threats

A threat is an action that takes advantage of security weaknesses in a system and has a negative impact on it.

### Attack

An attack occurs when a system is compromised based on a vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the systems, and to preventan attack.

**Target of Evaluation**: A target of evaluation is an IT system, product, or component that is identified subjected to a required security evaluation. This kind of evaluation helps the evaluator understand the functioning, technology, and vulnerabilities of a particular system or product.

Ethical hackers are usually concerned with high-value TOEs, systems that contain sensitive information such as account numbers, passwords, Social Security numbers, or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high-value TOEs to determine the vulnerabilities and patch them to protect against exploits and exposure of sensitive data.

# Ethical Hackers

Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes. Ethical hackers who are security professionals test their network and systems security for vulnerabilities using the same tools that a hacker might use to compromise the network.

Ethical hackers usually fall into the white-hat category, but sometimes they’re former gray hats who have become security professionals and who now use their skills in an ethical manner.

## Goals Attackers Try to Achieve

Whether perpetuated by an ethical hacker or malicious hacker, all attacks are an attempt to breach computer system security. Security consists of four basic elements: 1. Confidentiality 2. Authenticity 3. Integrity 4. Availability.

A hacker’s goal is to exploit vulnerabilities in a system or network to find a weakness in one or more of the four elements of security. For example, in performing a denial-of-service (DoS) attack, a hacker attacks **the availability** elements of systems and networks. Although DoS attack can take many forms, the main purpose is to use up system resources or bandwidth. A flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to legitimate users of the system. Although the media focuses on the target of DoS attacks, in reality such attacks have many victims—the final target and the systems the intruder controls.

Information theft, such as stealing passwords or other data as it travels in clear text across trusted networks, is a **confidentiality attack**, because it allows someone other than the intended recipient to gain access to the data. This theft isn’t limited to data on network servers. Laptops, disks, and backup tapes are all at risk. These company-owned devices are loaded with confidential information and can give hacker information about the security measures in place at an organization.

Bit-flipping attacks are considered **integrity attacks** because the data may have been tampered with in transit or at rest on computer systems; therefore, system administrators are unable to verify the data is as the sender intended it. A bit-flipping attack is an attack on a cryptographic cipher: the attacker changes the cipher text in such a way as to result in a predictable change of the plain text, although the attacker doesn’t learn the plain text itself. This type of attack isn’t directed against the cipher but against a message or series of messages. In the extreme, this can become a DoS attack against all messages on a particular channel using that cipher. The attack is especially dangerous when the attacker knows the format of the message. When a bit-flipping attack is applied to digital signatures, the attacker may be able to change a promissory note stating “I owe you $10.00” into one stating “I owe you $10,000.”

MAC address spoofing is an **authentication attack** because it allows an unauthorized device to connect to the network when Media Access Control (MAC) filtering is in place, such as on a wireless network. By spoofing the MAC address of a legitimate wireless station, an intruder can take on that station’s identity and use the network.

## What is Hacking?

**Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access**. Example of Hacking: Using password cracking algorithm to gain access to a system.

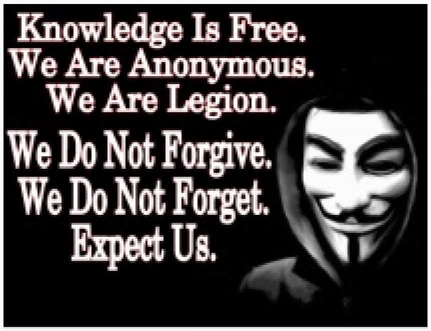
## Who is a Hacker? Types of Hackers

A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

| **Symbol** | **Description** |
|---|---|
| | **Ethical Hacker (White hat):** A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments. |
|  | **Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc. |

| | |
|---|---|
| | |
| | **Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner. |
| | **Script kiddies:** A non-skilled person who gains access to computer systems using already made tools. |

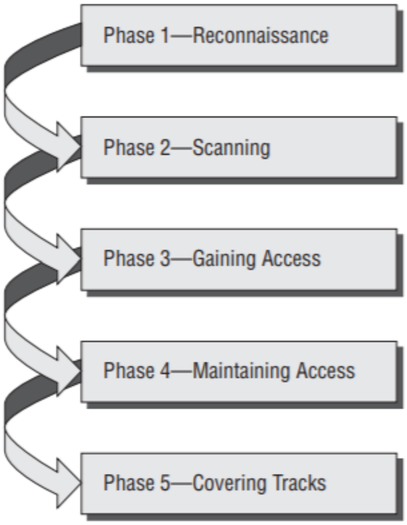
| | |
|---|---|
| | |
|  Knowledge Is Free.<br>We Are Anonymous.<br>We Are Legion.<br>We Do Not Forgive.<br>We Do Not Forget.<br>Expect Us. | **Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website. |
| | **Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers. |

## Phases of Hacking

The process of ethical hacking can be broken down into five distinct phases. Not necessarily a hacker has to follow these 5 steps in a sequential manner. It’s a stepwise process and when followed yields a better result.

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are. Figure 1.1 illustrates the five phases that hackers generally follow in hacking a computer system.

**FIGURE 1.1** Phases of hacking



# Phase 1: Reconnaissance

This phase is also called as Footprinting and information gathering Phase, and in this phase hacker gathers information about a target before launching an attack.  It is during this phase that the hacker finds valuable information such as old passwords, names of important employees.

What's footprinting? It's a method that used for collecting data from target system. These data include important areas such as:

Finding out specific IP addresses

TCP and UDP services

Identifies vulnerabilities

Having such information is enough to start a successful attack.

There are two types of Footprinting:

**Active**: Directly interacting with the target to gather information about the target.

**Passive**: Trying to collect the information about the target without directly accessing the target. To this purpose, hacker can use social media, public websites etc.

## Phase 2: Scanning

In this phase, hackers are probably seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts. In fact, hacker identifies a quick way to gain access to the network and look for information. This phase includes usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data.

Basically, at this stage, four types of scans are used:

Pre-attack: Hacker scans the network for specific information based on the information gathered during reconnaissance.

Port scanning/sniffing: This method includes the use of dialers, port scanners, and other data-gathering equipment.

Vulnerability Scanning: Scanning the target for weaknesses/vulnerabilities.

Information extraction: In this step, hacker collects information about ports, live machines and OS details, topology of network, routers, firewalls, and servers.

**Network Mapping:** Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

## Phase 3: Gaining Access

Where most of the damage is usually done, yet hackers can cause plenty of damage without gaining any access to the system  Access can be gained locally, offline, over a LAN, or over the Internet  A hacker's chances of gaining access into a target system are influenced by factors such as:  Architecture and configuration of the target system  Skill level of the perpetrator  Initial level of access obtained.

At this point, the hacker has the information he needs. So first he designs the network map and then he has to decide how to carry out the attack? There are many options, for example:

1. Phishing attack
2. Man in the middle attack
3. Brute Force Attack
4. Spoofing Attack
5. Dos attack
6. Buffer overflow attack
7. Session hijacking
8. BEC Attack

Anyway, hacker after entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

## Phase 4: Maintaining Access

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Also, the hacker secures access to the organization's Rootkits and Trojans and uses it to launch additional attacks on the network. An ethical hacker tries to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

Attackers, who choose to remain undetected  Remove evidence of their entry  Install a backdoor or a Trojan to gain repeat access  Install rootkits at the kernel level to gain full administrator access to the target compute.

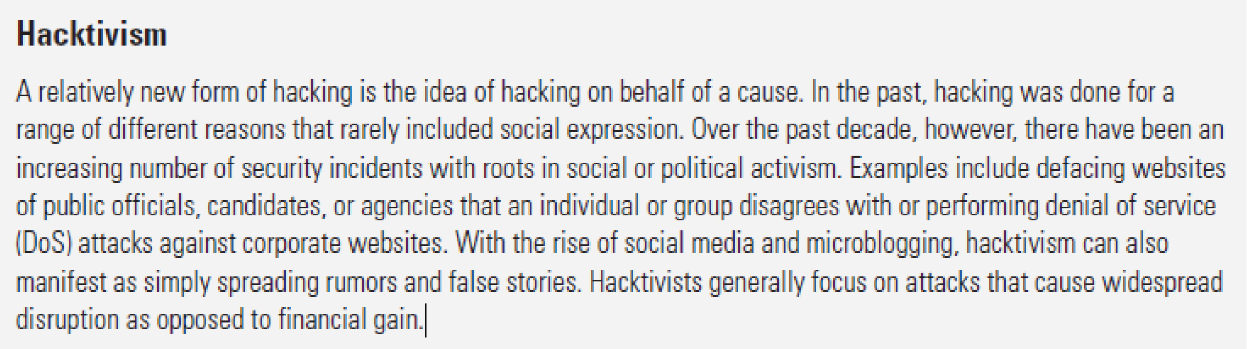
Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

(In this phase hacker has multiple e-mail accounts, he/she begins to test the accounts on the domain. The hacker from this point creates a new administrator account for themselves based on the naming structure and try and blend in. Hacker begins to look for and identify accounts that have not been used for a long time. The hacker assumes that these accounts are likely either forgotten or not used so they change the password and elevate privileges to an administrator as a secondary account in order to maintain access to the network. The hacker may also send out emails to other users with an exploited file such as a PDF with a reverse shell in order to extend their possible access. No overt exploitation or attacks will occur at this time. If there is no evidence of detection, a waiting game is played letting the victim think that nothing was disturbed. With access to an IT account the hacker begins to make copies of all emails, appointments, contacts, instant messages, and files to be sorted through and used later.)

## Phase 5: Clearing Tracks/Covering tracks

An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him/her.Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log. He/she does this by:

1. Clearing the cache and cookies
2. Modifying registry values
3. Modifying/corrupting/deleting the values of Logs
4. Clearing out Sent emails
5. Closing all the open ports
6. Uninstalling all applications that he/she be used



**Hacktivism**

A relatively new form of hacking is the idea of hacking on behalf of a cause. In the past, hacking was done for a range of different reasons that rarely included social expression. Over the past decade, however, there have been an increasing number of security incidents with roots in social or political activism. Examples include defacing websites of public officials, candidates, or agencies that an individual or group disagrees with or performing denial of service (DoS) attacks against corporate websites. With the rise of social media and microblogging, hacktivism can also manifest as simply spreading rumors and false stories. Hacktivists generally focus on attacks that cause widespread disruption as opposed to financial gain.

# Malware Attacks

Malware is a code that is made to stealthily affect a compromised computer system without the consent of the user. This broad definition includes many particular types of malevolent software (malware) such as spyware, ransomware, command, and control.

Malware differs from other software in that it can spread across a network, cause changes and damage, remain undetectable, and be persistent in the infected system. It can destroy a network and bring a machine's performance to its knees.

## Ransomware

Ransomware blocks access to a victim's data, typically threating delete it if a ransom is paid. There is no guarantee that paying a ransom will regain access to the data. Ransomware is often carried out via a Trojan delivering a payload disguised as a legitimate file.

## Trojan Horses

A Trojan is a malicious software program that misrepresents itself to appear useful. They spread by looking like routine software and persuading a victim to install. Trojans are considered among the most dangerous type of all malware, as they are often designed to steal financial information.

## SQL Injection

SQL injection, also known as SQLI, is a kind of attack that employs malicious code to manipulate backend databases to access information that was not intended for display. This may include numerous items including private customer details, user lists, or sensitive company data.

SQLI can have devastating effects on a business. A successful SQLI attack can cause deletion of entire tables, unauthorized viewing of user lists, and in some cases, the attacker can gain administrative access to a database. These can be highly detrimental to a business.

## Cross Site Scripting

Cross-site scripting (XSS) is a kind of injection breach where the attacker sends malicious scripts into content from otherwise reputable websites. It happens when a dubious source is allowed to attach its own code into web applications, and the malicious code is bundled together with dynamic content that is then sent to the victim's browser.

Malicious code is usually sent in the form of pieces of Javascript code executed by the target's browser. The exploits can include malicious executable scripts in many languages including Flash, HTML, Java, and Ajax. XSS attacks can be very devastating, however, alleviating the vulnerabilities that enable these attacks is relatively simple.

## **What is a Cyber Attack?**

A cyber attack is an intentional exploitation of computer systems, networks, and technology-dependent enterprises. These attacks use malicious code to modify computer code, data, or logic. Culminating into destructive consequences that can compromise your data and promulgate cybercrimes such as information and identity theft. A cyber attack is also known as a computer network attack (CNA).