**UNIT-II**

**What is Hacking?**

**Hacking** is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

## Who is a Hacker?

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.

## Types of Hackers

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

|  |  |
| --- | --- |
| **Symbol** | **Description** |
| [White hat hacker](https://www.guru99.com/images/EthicalHacking/img1.png) | **Ethical Hacker (White hat):**A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration[Testing](https://www.guru99.com/software-testing.html)and vulnerability assessments. |
| [Black hat hacker](https://www.guru99.com/images/EthicalHacking/img2.jpg) | **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 hacker](https://www.guru99.com/images/EthicalHacking/img3.jpg) | **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](https://www.guru99.com/images/EthicalHacking/img4.jpg) | **Script kiddies:**A non-skilled person who gains access to computer systems using already made tools. |
| [Hacktivist](https://www.guru99.com/images/EthicalHacking/img5.jpg) | **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](https://www.guru99.com/images/EthicalHacking/img6.png) | **Phreaker:**A hacker who identifies and exploits weaknesses in telephones instead of computers. |

## Introduction of Cybercrime

**Cybercrime** is the activity of using computers and networks to perform illegal activities like spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrime hacks are committed through the internet, and some cybercrimes are performed using[Mobile](https://www.guru99.com/mobile-testing.html)phones via SMS and online chatting applications.

**Type of Cybercrime**

* The following list presents the common types of cybercrimes:
* **Computer Fraud:**Intentional deception for personal gain via the use of computer systems.
* **Privacy violation:**Exposing personal information such as email addresses, phone number, account details, etc. on social media, hacking a websites, etc.
* **Identity Theft:**Stealing personal information from somebody and impersonating that person.
* **Sharing copyrighted files/information:**This involves distributing copyright protected files such as eBooks and computer programs etc.
* **Electronic funds transfer:**This involves gaining an un-authorized access to bank [computer networks](https://www.guru99.com/types-of-computer-network.html)and making illegal fund transfers.
* **Electronic money laundering:**This involves the use of the computer to launder money.
* **ATM Fraud:**This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
* **Denial of Service Attacks:**This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
* **Spam:**Sending unauthorized emails. These emails usually contain advertisements.

**What is Ethical Hacking?**

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

* Get **written permission** from the owner of the computer system and/or computer network before hacking.
* **Protect the privacy of the organization** been hacked.
* **Transparently report** all the identified weaknesses in the computer system to the organization.
* **Inform** hardware and software vendors of the **identified weaknesses**.

**Why Ethical Hacking?**

* Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization’s image and save an organization a lot of money.
* Fake hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

**Legality of Ethical Hacking**

**Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking**. The [International Council of E-Commerce Consultants (EC-Council)](http://www.eccouncil.org/) provides a certification program that tests individual’s skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

**The Five Phases of Ethical Hacking**

While the phases discussed in the webinar are from the perspective of a hacker, King explains that these are the same phases used by a white hat hacker to test an organization’s network. To put it simply, an attacker uses this approach to breach the network, while the ethical hacker uses it to protect it.

### 1. Reconnaissance

Reconnaissance, also known as the preparatory phase, is where the hacker gathers information about a target before launching an attack and is completed in phases prior to exploiting system vulnerabilities. One of the first phases of Reconnaissance is dumpster diving. It is during this phase that the hacker finds valuable information such as old passwords, names of important employees (such as the head of the network department), and performs an active reconnaissance to know how the organization functions. As a next step, the hacker completes a process called footprinting to collect data on the security posture, reduces the focus area such as finding out specific IP addresses, identifies vulnerabilities within the target system, and finally draws a network map to know exactly how the network infrastructure works to break into it easily. Footprinting provides important information such as the domain name, TCP and UDP services, system names, and passwords. There are also other ways to do footprinting, including impersonating a website by mirroring it, using search engines to find information about the organization, and even using the information of current employees for impersonation.

### 2. Scanning

In this phase, the hacker identifies a quick way to gain access to the network and look for information. There are three methods of scanning: pre-attack, port scanning/sniffing, and information extraction. Each of these phases demonstrates a specific set of vulnerabilities that the hacker can utilize to exploit the system's weaknesses. The pre-attack phase is where the hacker scans the network for specific information based on the information gathered during reconnaissance. The port scanner or sniffing phase is where scanning includes the use of dialers, port scanners, vulnerability scanners, and other data-gathering equipment. The information extraction phase is where the attackers collect information about ports, live machines and OS details to launch an attack.

### 3. Gain Access

The hacker gains access to the system, applications, and network, and escalates their user privileges to control the systems connected to it.

### 4. Maintain Access

Here, the [hacker secures access](https://null-byte.wonderhowto.com/how-to/five-phases-hacking-0167990/) to the organization’s Rootkits and Trojans and uses it to launch additional attacks on the network.

### 5. Cover Tracks

Once the hacker gains access, they cover their tracks to escape the security personnel. They do this by clearing the cache and cookies, tampering the log files, and closing all the open ports. This step is important because it clears the system information making hacking a great deal harder to track.

**Active attacks:** An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

**Types of Active attacks:**

**Masquerade:** in this attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.  
**Session replay**: In this type of attack, a hacker steals an authorized user’s log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.  
**Message modification**: In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.  
In a **denial of service (DoS)** attack, users are deprived of access to a network or web  
resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.  
In a **distributed denial-of-service (DDoS)** exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

**Passive Attacks:** *Passive attacks* are relatively scarce from a classification perspective, but can be carried out with relative ease, particularly if the traffic is not encrypted.

**Types of Passive attacks:**

***Eavesdropping (tapping)***: the attacker simply listens to messages exchanged by two entities.  
For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.  
***Traffic analysis*:** the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.  
**Software Attacks:** Malicious code (sometimes called *malware*) is a type of software  
designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging. Common malware examples are listed in the following table: