# Assignment Final

**Shaban Zaman**

**BSCS-F19-M-65-B**

22/06/2021

—

Compiler Construction

—

Ma’am Aminah Ali

# Types of Hackers:

## 1) White Hat Hackers:

White hat hackers are types of hackers who are professionals with expertise in cybersecurity. They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system. They hack the system from the loopholes in the cybersecurity of the organization. This hacking is done to test the level of cybersecurity in their organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. White hat hackers work as per the rules and regulations set by the government. White hat hackers are also known as ethical hackers.

## 2) Black Hat Hackers:

Black hat hackers are also knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry. On gaining entry they might steal the data or destroy the system. The hacking practices used by these types of hackers depend on the individual's hacking capacity and knowledge. As the intentions of the hacker make the hacker a criminal. The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking.

## 3) Grey Hat Hackers:

The intention behind the hacking is considered while categorizing the hacker. The Gray hat hacker falls in between the black hat hackers and white hat hackers. They are not certified, hackers. These types of hackers work with either good or bad intentions. The hacking might be for their gain. The intention behind hacking decides the type of hacker. If the intention is for personal gain, then the hacker is considered to be a gray hat hacker.

## 4) Script Kiddies:

It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateur types of hackers in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites. The intention behind the hacking is just to get attention from their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.

## 5) Hacktivists:

These types of hackers intend to hack government websites. They pose themselves as activists, so known as a hacktivist. Hacktivist can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks. The data gained from government files accessed are used for personal political or social gain.

## 6) Red Hat Hackers:

Red Hat Hackers are synonymous with Eagle-Eyed Hackers. They are the types of hackers who are like white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is in the process of hacking through intention remains the same. Red hat hackers are quite ruthless while dealing with black hat hackers or counteracting with malware. The red hat hackers continue to attack and may end up having to replace the entire system set up.

# Types of Hacking:

## Website Hacking:
Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

## Network Hacking:
Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

## Email Hacking:
It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

## Password Hacking:
This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

## Computer Hacking:
This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.4

## Online Banking Hacking:
Online banking hacking is unauthorized accessing bank accounts without knowing the password or without permission of account holder.

## Phishing:
Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

## Cookie Theft:
Cookie theft occurs when a third-party copy unencrypted session data and uses it to impersonate the real user. Cookie theft most often occurs when a user accesses trusted sites over an unprotected or public Wi-Fi network.

## DNS Spoofing:
DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g., an IP address.

## Terminologies:

**Adware** − Adware is software designed to force pre-chosen ads to display on your system.

**Attack** − An attack is an action that is done on a system to get its access and extract sensitive data.

**Back door** − A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.

**Bot** − A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.

**Botnet** − A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.

**Brute force attack** − A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, repeatedly, until it gets in.

**Buffer Overflow** − Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.

**Clone phishing** − Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

**Cracker** − A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.

**Denial of service attack (DoS)** − A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

**DDoS** − Distributed denial of service attack.

**Exploit Kit** − An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the clie0nt.

**Exploit** − Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.

**Firewall** − A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.

**Keystroke logging** − Keystroke logging is the process of tracking the keys which are pressed on a computer.