Hacking

Name : Rupak Sarkar

Roll No.: 14271024036

Stream : MCA

Semester : Semester 2nd

Subject : Introduction to Cyber Security

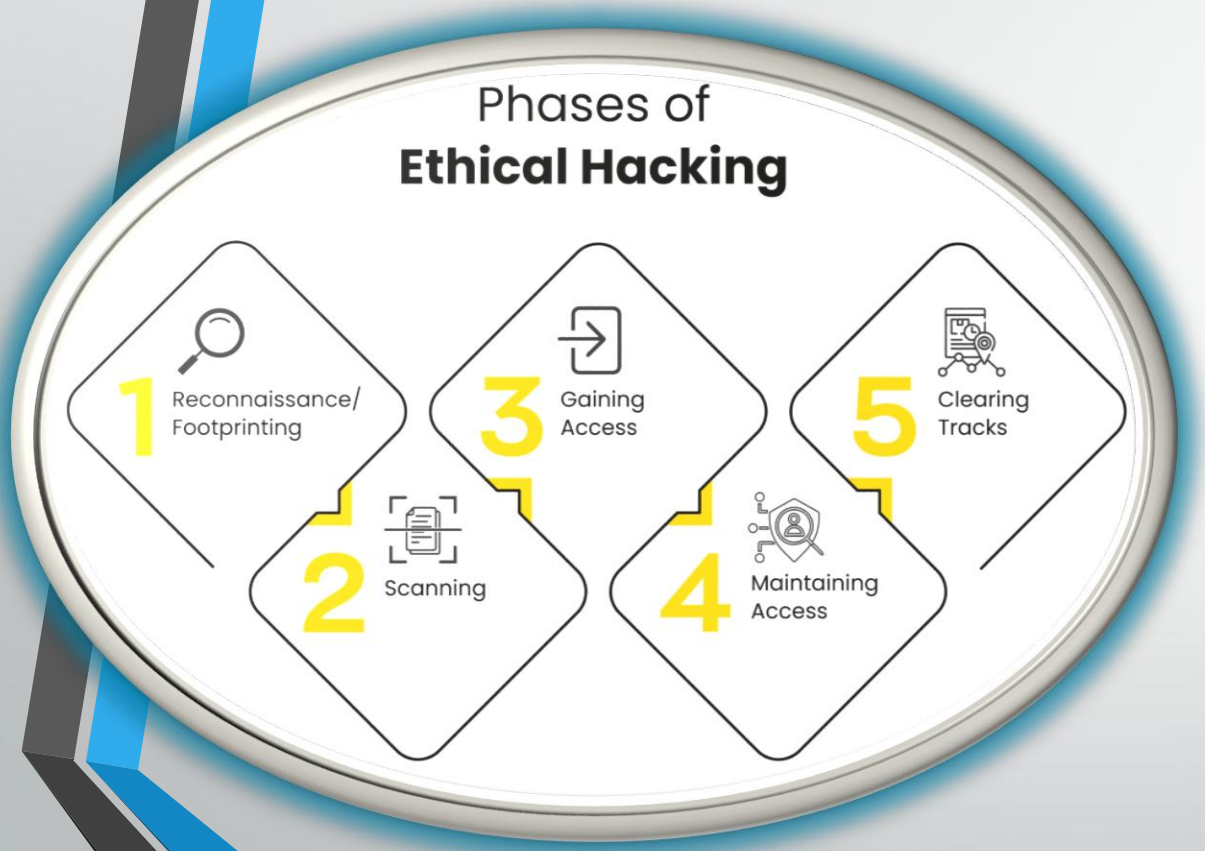
Subject Code : MCAN-E205D

Introduction to Hacking

An effort to attack a computer system or a private network inside a computer is known as hacking. Simply, it is unauthorized access to or control of computer network security systems with the intention of committing a crime. Hacking is the process of finding some security holes in a computer system or network in order to gain access to personal or corporate information.

One example of computer hacking is the use of a password cracking technique to gain access to a computer system. The process of gaining illegal access to a computer system, or a group of computer systems, is known as hacking. This is accomplished by cracking the passwords and codes that grant access to systems. Cracking is the term used to describe the process of obtaining a password or code. The hacker is the individual who performs the hacking.

Steps of Hacking



1. **Reconnaissance**: This is the first phase where the Hacker tries to collect information about the target.

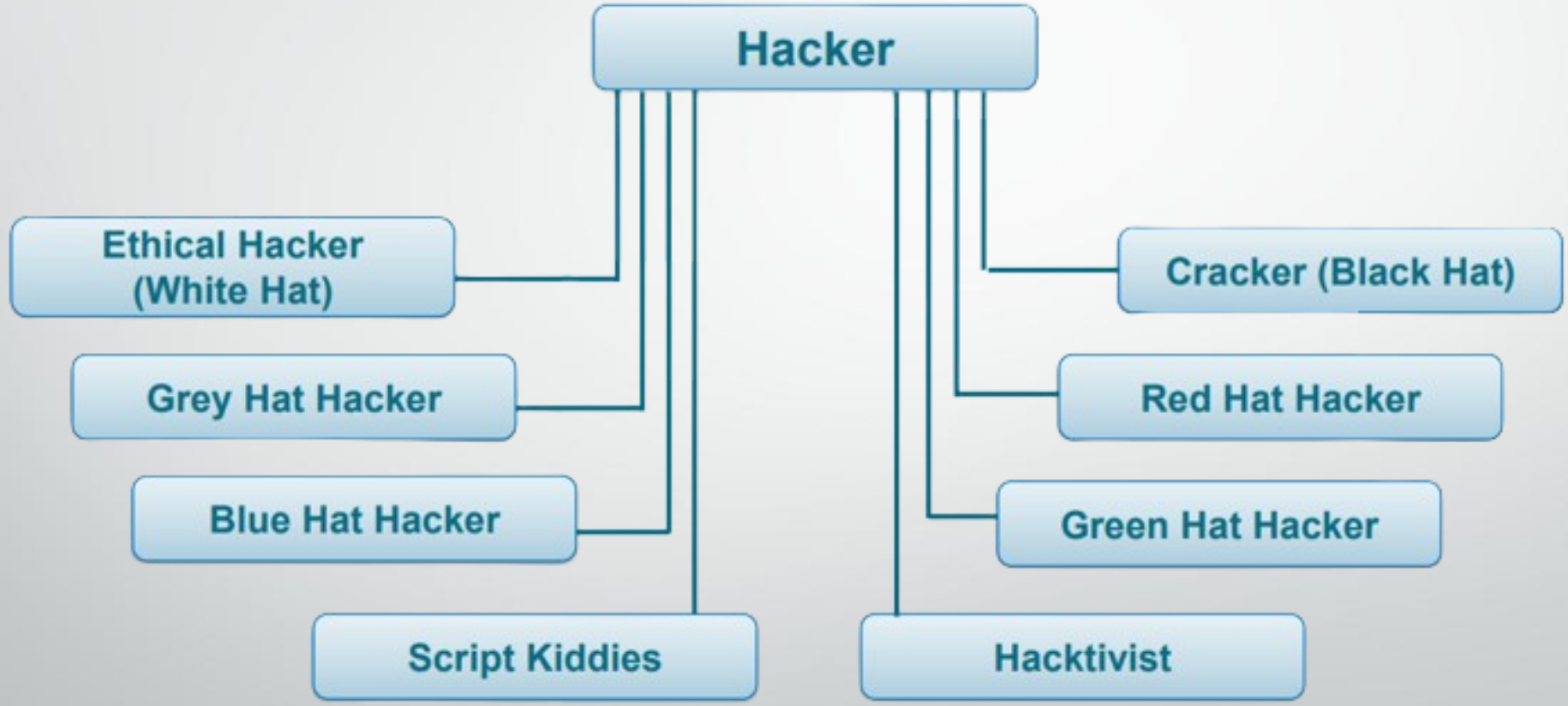
2. **Scanning**: This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data.

3. **Gaining Access**: In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2.

4. **Maintaining Access**: Once a hacker has gained access, they want to keep that access for future exploitation and attacks.

5. **Clearing Tracks**: Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity.

Different types of Hackers



Different types of Hackers

Ethical Hacker (White Hat)

- These hackers work legally to improve security.
- They find and fix vulnerabilities in systems to protect against cyberattacks.

Cracker (Black Hat)

- Malicious hackers who break into systems illegally.
- They steal data, spread viruses, or cause damage for personal gain or revenge.

Different types of Hackers

Grey Hat Hacker

- A mix of ethical and malicious hackers.
- They hack without permission but usually report vulnerabilities instead of exploiting them.

Green Hat Hacker

- Beginners in hacking who are eager to learn and improve their skills.
- They usually study ethical hacking or penetration testing.

Different types of Hackers

Red Hat Hacker

- Also known as vigilante hackers.
- They target black-hat hackers, using aggressive methods to stop them, sometimes even destroying their systems.

Blue Hat Hacker

- These hackers work outside security teams to test software and identify bugs before launch.
- Some also seek revenge through hacking.

Different types of Hackers

Script Kiddies

- Inexperienced hackers who use pre-made tools and scripts without understanding how they work.
- They often hack for fun or to show off.

Hacktivist

- Hackers who attack systems for political or social causes.
- They expose corruption, protest government actions, or spread awareness.

Thank You!