



Types of Hackers and Their Roles

Student Name: Ammar Yasser Mohamed

Course: ITI-Cybersecurity-Summer-2025

Date: August 2, 2025

Types of Hackers

1. White Hat Hackers

- Ethical hackers who help organizations find and fix security weaknesses.
- Work with permission, often in cybersecurity roles.

2. Black Hat Hackers

- Malicious hackers who exploit systems illegally for profit, revenge, or disruption.
- Engage in activities like data theft, malware distribution, and system damage.

3. Grey Hat Hackers

- Hackers who operate without permission but don't have malicious intent.
- May expose flaws publicly or report them without asking first.

4. Script Kiddies

- Inexperienced individuals who use existing hacking tools or scripts without fully understanding them.
- Often hack for fun or attention rather than skill or strategy.

5. Green Hat Hackers

- Newcomers or learners in the hacking world.

- Eager to gain knowledge and improve their skills, often found in forums or communities.

6. Blue Hat Hackers

- Hackers who seek revenge or personal vendettas.
- Sometimes used to describe external security professionals invited to test a system for vulnerabilities before launch.

7. Red Hat Hackers

- Vigilante-style hackers who target black hat hackers.
- Instead of reporting them, they may launch attacks to take them down or destroy their resources.

8. Hacktivists

- Use hacking to promote political or social agendas.
- May deface websites, leak sensitive information, or disrupt services to make a statement.

9. State-Sponsored Hackers

- Operate on behalf of a government to perform cyber espionage, surveillance, or cyber-warfare.
- Highly skilled and often well-funded.