**Difference between ethical hacking and malicious hacking**

The difference between **ethical hacking** and **malicious hacking** lies in **intent**, **legality**, and **authorization**. Here's a detailed comparison:

**🧑‍💻 Ethical Hacking vs. Malicious Hacking**

| **Feature** | **Ethical Hacking** | **Malicious Hacking** |
| --- | --- | --- |
| **Purpose** | To **identify and fix** security vulnerabilities | To **exploit** vulnerabilities for personal or financial gain |
| **Authorization** | Done with **permission** from the organization | Done **without permission**, illegally |
| **Legality** | **Legal** and often part of a security program | **Illegal** and punishable by law |
| **Intent** | To **protect** and improve systems | To **damage**, steal, or disrupt systems |
| **Tools Used** | Same tools as malicious hackers (e.g., Nmap, Metasploit) | Same tools, but used to break in and harm |
| **Common Alias** | White Hat hacker | Black Hat hacker |
| **Typical Employers** | Companies, governments, cybersecurity firms | Cybercriminal gangs, acting alone or with others |
| **Outcome** | Reports vulnerabilities, helps improve security | Steals data, installs malware, or causes service outages |

**📌 Example Scenario**

**Ethical Hacker:** A company hires a certified ethical hacker to conduct a **penetration test** on their web application. The hacker finds a SQL injection flaw and reports it, allowing the company to fix it before attackers exploit it.

**Malicious Hacker:** An attacker scans the same web app, finds the SQL injection flaw, and **steals user data** to sell on the dark web or blackmail the company.

**✅ Summary**

| **Ethical Hacking** | **✔ Security-focused✔ Legal✔ Authorized** |
| --- | --- |
| Malicious Hacking | ❌ Harmful intent❌ Illegal❌ Unauthorized |