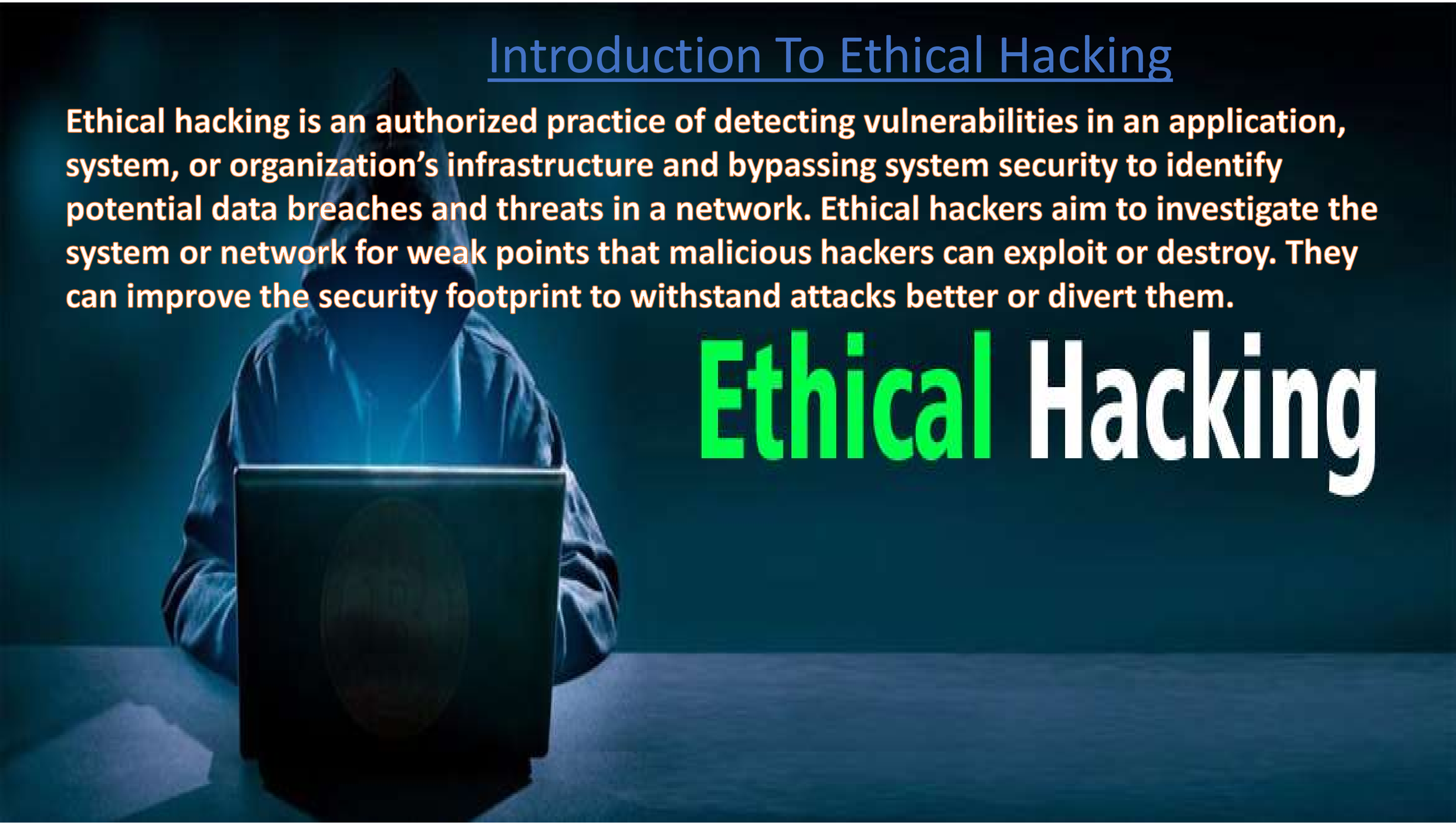
Introduction To Ethical Hacking

Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and bypassing system security to identify potential data breaches and threats in a network. Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They can improve the security footprint to withstand attacks better or divert them.



Why Ethical Hacking is Important?

- In the age of digitalization, every organization needs to be assertive while ensuring the security and privacy of the data and information they deal with.

- Ethical hacking is extensively used to test security systems. Ethical hacking is also used during executing, managing and designing stages of test security systems. It finds the security vulnerabilities and corrects them.

- Ethical hacking is also used to secure crucial data from adversaries. It prevents malicious users from exploiting the organizational or an individual. It reduces the risk of getting blackmailed by a person or organization with ill intentions.

- Ethical hacking has a crucial role to play in the safety and security of any nation. Many national and state-funded organizations hire hackers to prevent cyber terrorism and terrorist attacks. Many government-employed personnel hire ethical hackers to protect their privacy

Ethical hacking scope

Ethical hacking has an infinite future. Many areas, including government, corporate enterprises, health care, entertainment, banking, and others, are quickly expanding in this arena.

Even though only 32% of people work in the ethical hacking industry. As a result, the demand for new staff is on the rise. Compared to last year, the number of ethical hackers is predicted to rise by 20% by the end of 2023. As a result, this number will continue to grow in the future.

limitations of ethical hacking

Limited scope : Ethical hackers cannot progress beyond a defined scope to make an attack successful. However, it's not unreasonable to discuss out of scope attack potential with the organization.

Resource constraints : Malicious hackers don't have time constraints that ethical hackers often face. Computing power and budget are additional constraints of ethical hackers.

Restricted methods : Some organizations ask experts to avoid test cases that lead the servers to crash (e.g., Denial of Service (DoS) attacks).

three main types of hackers

Black hat hackers

Black hat hackers are cybercriminals that illegally crack systems with malicious intent. Seeking to gain unauthorized access to computer systems is the definition of black hat hacking. Once a black hat hacker finds a security vulnerability, they try to exploit it, often by implanting a virus or other type of malware such as a trojan.

Ransomware attacks are another favored ploy that black hat hackers use to extort financial gains or breach data systems.

White hat hackers

White hat hackers are ethical security hackers who identify and fix vulnerabilities. Hacking into systems with the permission of the organizations they hack into, white hat hackers try to uncover system weaknesses in order to fix them and help strengthen a system's overall security.

Many cybersecurity leaders started out as white hat hackers, but the vital role played by ethical hacking is still widely misunderstood, as made clear by a recent ethical hacking case in Germany.

Gray hat hackers

Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don’t have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when gray hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them. But gray hat hackers may demand payment in exchange for providing full details of what they uncovered.

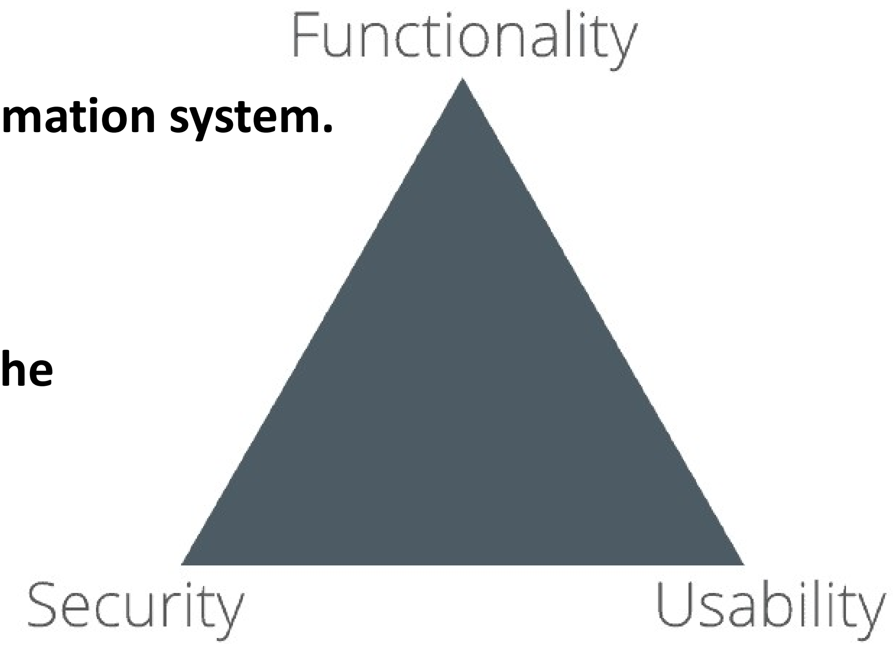
Reasons of hacking

Most often, cyber attacks happen because criminals want your:

- ✓ business' financial details
- ✓ customers' financial details (eg credit card data)
- ✓ sensitive personal data
- ✓ customers' or staff email addresses and login credentials
- ✓ customer databases
- ✓ clients lists
- ✓ IT infrastructure
- ✓ IT services (eg the ability to accept online payments)
- ✓ intellectual property (eg trade secrets or product designs)

Security Usability Triangle

The Security, Functionality and Usability Triangle is a foundational aspect of security. Like the CIA triad, this concept underpins any system, network, or device. The security triangle works in the following manner.



❑ **Functionality: The features provided by the information system.**

❑ **Usability: How easy the system is to use.**

❑ **Security: The restrictions imposed on accessing the various components of the system**