



The role of Ethical hacking in cybersecurity

In this modern technological era, cyber threats have been become more frequent and sophisticated. This has created a strong and crucial need of cybersecurity and its core part is ethical hacking.

By **Hamna Shafiq** | University of Agriculture, Faisalabad | Published: June 2026
hamnshafiq83@gmail.com | Position: Student

Introduction

Nowadays, the widespread use of technology has made cybersecurity more important than ever. Due to huge rise in digital attacks, companies and organizations suffer heavily from serious risks like data breaches, privacy violation or financial loss. As cybercrimes continue to grow more advanced and breakthrough techniques, just depending on traditional security system is definitely not enough.

This is where Ethical hacking plays an important role in cybersecurity. Ethical Hackers use their skills and knowledge to identify the vulnerabilities of the system before the actual hacker attack them or hack the system. By examining and strengthening the security systems, they assist organizations prevent imminent risks and strengthen overall system. In this way, ethical hacking acts as preventive method to defending digital information and maintaining trust in today's technology driven era.

"Thinking like an attacker to defend better."

Technology Overview

Ethical hacking is engaged with a wide range of advanced technologies that are generally used in digital systems. These technologies may include computer network, databases and web applications. Ethical hackers need basic knowledge of how these technologies works to in order to recognize possible security threats.

For example, One essential part is networking, where hackers study how data is being transmitted and look for vulnerabilities like misconfigured devices or insecure connections. Operating systems like windows and linux are also critical, as they control the behavior of software and hardware interaction. Furthermore, web technologies like websites and online applications are the common targets to attack.

By understanding these technologies, ethical hackers mimic the real word attacks and help companies strengthens their security systems against actual cyber attacks.



Figure 1: Role of ethical hacker

Types of Hackers

In the area of cybersecurity, hackers are normally categorized in three types depending on their objectives and activities.

White Hat Hackers: White hat hackers are approved professional hackers hired by organizations to use their skills to identify vulnerabilities. They work legally to find the weakness of the system and fix them before real attack occurs. Their main goal is to protect organization data from unauthorized access.

Black Hat Hackers: They are the ones who use their knowledge and skills for illegal and harmful activities. They exploit system vulnerabilities to gain unauthorized access or to steal personal information. Their main goal is privacy breach or financial data.

Grey Hat Hackers: Grey hat hackers fall between white hat hackers and black hat hackers. They may gain unauthorized access to the system but not with ill intentions. Sometimes, they identify flaws and tell the organizations but their actions still considered illegal and unethical.

Key Findings & Impact

This discussion shows how ethical hacking plays a massive role in cybersecurity by finding the vulnerabilities of the system before anyone can actually exploit them. It highlights that the standard traditional security



systems are not enough for security in modern days as cyber attack are evolving rapidly. Ethical hacker acts the defensive layer by testing systems to check weakness and improving them.

The impact of ethical hacking is huge. As it helps companies prevent data breaches, protect sensitive data and reduce financial and reputational damages. It can also raise trust among users by safer digital environment. Overall ethical hacking has become an important component in maintaining strong and reliable cybersecurity systems.

What's Next?

As the technology continues to expand, the importance of cybersecurity and ethical hacking also increase. Companies are constantly facing new and more advanced cyber threats, Which increase the growing demand of ethical hacking.

For students and newcomers, Learning areas like network security, penetration testing and programming can help you become ethical hacker. So, you can use your skill to benefit the society. With continuous practice and learning, individuals can contribute to create safer digital systems. Hacking is not just the technical skill but also responsibility towards maintaining security in the digital world.

About the Author

Hamna Shafiq is a IT student at Agricultural university. She can be reached at hamnashafiq83@email.com.

Keywords: Artificial Intelligence; Cybersecurity; IoT;

References

- [1] Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson.
- [2] EC-Council. (n.d.). *What is Ethical Hacking?*