Inquiry: Ethics of Hacking in the Modern Age

Ramon Lopez Jr

Department of Cyber Security: University of Advancing Technology

NTS103: Identity Protection and Personal Security

Professor Aaron Rodriguez

May 28th, 2023

Inquiry: Ethics of Hacking in the Modern Age

Hacking is commonly defined as the act of finding and exploiting weaknesses in a system or network. While this often leads to unauthorized access or data breaches, it is important to recognize that not all hacking is inherently malicious (Kaspersky, 2022). Due to its frequent association with cybercrime, hacking tends to carry a negative connotation. However, there is a growing community of individuals—known as ethical hackers—who use hacking techniques with positive intentions. These include finding vulnerabilities, improving system integrity, and strengthening overall cybersecurity. Crucially, ethical hacking must always work within legal boundaries and with explicit consent from system owners.

White Hat vs. Black Hat: Defining Ethical and Malicious Hackers

Ethical hackers, often referred to as “white hats,” are individuals who conduct authorized security testing to improve digital infrastructure. This practice originated from curiosity and the drive to innovate, particularly through exploring programming languages and computer systems (Omoyiola et al., 2023). Today, white hats continue this mission by legally assessing vulnerabilities with the owner's permission.

In contrast, “black hat” hackers engage in criminal activities, exploiting weaknesses in systems for personal gain. One common method includes deploying ransomware to encrypt a victim's data, then demanding payment in exchange for access. These actions are illegal, harmful, and financially motivated. Their success encourages further attacks and often inspires others to join the underground economy of cybercrime (FBI, 2022).

While white hats work legally and for the public good, they must follow strict ethical standards. Failure to do so can result in legal consequences, including lawsuits or criminal charges.

The Grey Area: The Role of Grey Hat Hackers

Back in the day, there was only one type of hacker, and those were known as ethical hackers. In the present day, there are three major types of hackers that one could be classified into, each having their own intentions, approaches, and goals. These categories include ethical hackers (white hat), grey hat hackers, and malicious hackers (black hat). As told earlier, each has their own intentions, approaches, and goals. According to (Smith et al. 2022), ethical hackers engage in activities involving finding in a system or network to provide vulnerabilities recommendations on how to improve their security. Their intentions are meant to help improve network infrastructure and are authorized by the owner’s permission. Unlike an ethical hacker, malicious hackers will try to steal, damage, or disrupt a system or network. Their intentions are bad, and they may sell the data in an underground economy for financial profit. Then we have the grey hat hackers who occupy the middle ground of illegal activities and ethical ones. Unlike an ethical hacker, they do not seek authorization of the owner’s system and infiltrate it, they will then name any vulnerabilities. However, their intent is not malicious like a malicious hacker. They do not look to destroy, disrupt, or steal from their owner. But since their actions are not malicious, their activities are still considered illegal.

The Importance of Consent in Ethical Hacking

According to the EC-Council (2022), ethical hackers must always obtain explicit permission before conducting any form of penetration testing or vulnerability assessment.

Without legal authorization, even well-intentioned actions can be classified as cybercrimes. Proper consent protects not only the organization being tested but also the ethical hacker from liability. In today’s digital climate, where cyberattacks are on the rise, permission and legal frameworks are essential in distinguishing professional cybersecurity efforts from criminal behavior.

A Shift in Perception: From Innovation to Security

Historically, hacking was viewed as a form of digital tinkering—a creative pursuit aimed at developing innovative solutions and pushing the boundaries of technology. However, public feeling has shifted in recent decades due to high-profile cyberattacks and data breaches. Now, the term “hacking” more commonly evokes ideas of illegality and data theft. Despite this, ethical hacking continues to be an essential practice for defending against cyber threats. It stands for a proactive approach to naming security flaws before malicious actors can exploit them. Ethical hackers serve as guardians of digital systems, but they must be well-versed in legal guidelines and transparent in their operations.

Hacking, once seen as a purely innovative act, now straddles a complex spectrum—from malicious exploitation to vital security work. As the digital landscape evolves, so must our understanding of hacking’s ethical implications. Ethical hackers handle using within legal frameworks, obtaining clear authorization, and acting in the best interest of cybersecurity. Their work plays a crucial role in protecting personal, corporate, and national data in an increasingly interconnected world. ￼

References:

EC-Council. (2022, June 12). *Ethical Hacking: Understanding the Basics*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/ethical-hacking-understanding-basics/

FBI. (2022). *Ransomware*. Federal Bureau of Investigation. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

Kaspersky. (2022, July 1). *What is hacking? And how to prevent it*. Www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-hacking

Omoyiola, B., Bayo, O., Corresponding, O., & Olushola. (2018). The Legality of Ethical Hacking the Legality of Ethical Hacking. *IOSR Journal of Computer Engineering (IOSR-JCE) , 20*(1), 61–63. https://doi.org/10.9790/0661-2001016163

Smith, L., Chowdhury, M., & Latif, S. (2022). *Ethical Hacking: Skills to Fight Cybersecurity Threats*.