Journal of Information Technology & Software Engineering

OPEN ACCESS Freely available online

Commentary

Measuring Technical Breaches in Electronic Communication Platforms with Ethical Hacking Models

Thomas Richard*

Department of Artificial Intelligence, Istanbul Nisantasi University, Maslak, Turkey

DESCRIPTION

In an increasingly interconnected world, where the lines between our physical and digital lives are blurred, the importance of cyber-security cannot be overstated. With the rise of cybercrime, data breaches, and privacy violations, individuals and organizations alike are constantly under threat. Ethical hacking often referred to as "white hat hacking," is a practice where individuals, known as ethical hackers or penetration testers, use their technical skills to identify and address security vulnerabilities within computer systems, networks, and applications. The primary goal of ethical hacking is to strengthen the security of these systems, thereby preventing unauthorized access, data breaches, and other malicious activities. Ethical hackers leverage the same techniques and tools used by cybercriminals but with a critical difference: their intentions are purely altruistic. They seek vulnerabilities not to exploit them for personal gain but to help organizations and individuals protect their digital assets. By simulating real-world cyber-attacks, ethical hackers identify weak points in a system's defences. Ethical hackers play a crucial role in identifying and addressing vulnerabilities in applications, ensuring that our sensitive information remains confidential and safe from prying eyes.

Critical infrastructure, including power grids, water supply systems, and transportation networks, relies heavily on digital technology. Ethical hackers help protect these systems from potential cyber-attacks that could have catastrophic consequences, ensuring the safety and well-being of entire communities. Ethical hackers contribute to the security of nations by identifying and mitigating threats to government networks, defense systems, and sensitive information. In the digital world, innovation and progress depend on secure technologies. Ethical hacking promotes innovation by keeping systems secure and providing a safe environment for technology developers to create new solutions. Critics may argue that the act of hacking, even for ethical purposes, is morally ambiguous. However, it's crucial to differentiate between malicious hacking and ethical hacking in terms of intent, purpose, and adherence to a code of ethics. The key ethical distinction between malicious and ethical hacking lies in the intent and purpose. Malicious hackers seek personal gain, harm, or disruption, while ethical hackers aim to enhance security and protect the interests of individuals, organizations, and society as a whole. Ethical hackers must always operate within the boundaries of the law and with explicit permission from the system's owner. This is usually done through legal agreements such as "bug bounties," where organizations invite ethical hackers to test their systems in exchange for rewards. Without consent, ethical hacking could cross into illegal territory, violating privacy and causing harm. When an ethical hacker identifies vulnerability, they have a moral obligation to report it to the system's owner rather than exploiting it or making it public. This responsible approach allows organizations to fix vulnerabilities before they can be exploited for malicious purposes.

Ethical hackers must take measures to minimize harm during the testing process. While their goal is to expose vulnerabilities, they should avoid causing any significant damage to the systems they test. The primary objective is to enhance security, not disrupt operations. Ethical hacking is an essential component of the broader field of cyber-security. It contributes to safeguarding digital assets, protecting privacy, and preventing cybercrimes.

Traditional security measures are often reactive, responding to threats after they occur. Ethical hacking introduces a proactive approach by identifying vulnerabilities before they can be exploited, allowing organizations to take preventative actions. Ethical hackers perform comprehensive vulnerability assessments that help organizations prioritize and address the most critical security weaknesses. This targeted approach ensures that resources are allocated efficiently. Ethical hackers play a vital role in the continuous improvement of security measures, helping organizations stay one step ahead of cyber threats. Many industries and sectors are subject to cyber-security regulations and standards. Ethical hackers assist organizations in ensuring compliance with these regulations, reducing legal and financial risks. Public trust is essential for businesses and institutions that collect and store personal data. Ethical hacking practices demonstrate a commitment to data security, fostering trust among users and customers. The legal framework surrounding ethical hacking is often complex and varies from one jurisdiction

Correspondence to: Thomas Richard, Department of Artificial Intelligence, Istanbul Nisantasi University, Maslak, Turkey, E-mail: turkeyrechard@mav.tr

Received: 25-Aug-2023, Manuscript No. JITSE-23-27748; **Editor assigned:** 29-Aug-2023, PreQC No. JITSE-23-27748 (PQ); **Reviewed:** 12-Sep-2023, QC No. JITSE-23-27748; **Revised:** 19-Sep-2023, Manuscript No. JITSE-23-27748 (R); **Published:** 26-Sep-2023, DOI: 10.35248/2165-7866.23.13.355

Citation: Richard T (2023) Measuring Technical Breaches in Electronic Communication Platforms with Ethical Hacking Models. J Inform Tech Softw Eng. 13:355.

to another. They may encounter legal obstacles or uncertainty, which can hinder their work. Some ethical hackers may misuse their skills for personal gain or to settle personal vendettas. This misuse not only damages the reputation of ethical hacking but also undermines the trust placed in white hat hackers. Ethical hackers must always take responsibility for their actions and be accountable for any harm caused during their testing. A lack of accountability can lead to ethical dilemmas.