Ethical hacking

Christian Carrion

4/4/24

Introduction

Ethical hacking or sometimes referred to as penetration testing is the use of hacking tools to seek security vulnerabilities in networks or computer systems with authorized permission, according to IBM. In essence, an ethical hacker has the same skills set as an malicious hacker, but doesn't conduct hacking activities for malicious proposes. The point in having ethical hackers is to have people find vulnerabilities in systems, before the "bad" hacker does, to create a more secure digital environment.

Social Science Principles

There consists of six main principles of science:

1. Relativism
2. Determinism
3. Objectivity
4. Ethical Neutrality
5. Skepticism
6. Parsimony

For this paper I will primarily focus on these two principles: Ethical Neutrality and Determinism. Ethical neutrality is defined as scientists adhering to an ethical standard when conducting research. Hacking any protected device or network is considered illegal and a federal crime. It is essential for an ethical hacker/penetration tester to adhere to an ethical standard. According to an article called "Ethical and Unethical Hacking", written by David-Olivier Jaqute Chiffelle (

Professor at the school of Criminal Justice) & Michele Loi (AI ethics researcher) there are a few code of conduct that ethical hacker should adhere to:

1. Gain permission prior to assessing clients It security.
2. Stay within the scope the client has given permission to.
3. Use sophisticated documentation and scientific processes.
4. Remove traces and not create backdoors in the system.
5. If vulnerabilities are found, inform the software and hardware vendors.

Determinism is a principle of science that a behavior is caused by preceding events. Due to the affordance and easy access to devices and the internet, this has caused many people to find ways to exploit both. Also, this has caused companies to search to search for people with the same skills as a malicious hacker, to uncover their own security vulnerabilities and fix them, before the malicious hackers do.

Key Concepts

There are two main concepts that will be covered in this paper. This includes:

1. Personality Theories
2. Reinforcement Sensitivity

Personality theories compare how people's personal traits contribute to their behavior. In terms of an individual who is an ethical hacker, their main personality traits are clevenes and curiosity. In turn, ethical hackers tend to be more agreeable and more communicative. This will prove to be useful, because most companies will limit a scope in how far penetration testers can break into a system and what tools they are and are not allowed to use.

Reinforcement sensitivity is a theory of motivation. Individuals have different responses to their environment depending on different sensitivities of basic brain systems that respond to punishing or rewarding stimuli. Individuals that display a goal-driven persistence is extremely useful in penetration testing. Since the field of technology is changing rapidly, an ethical hacker needs to constantly have a mind-set of continuous learning. Also like a malicious hacker having persistence will prove beneficial, because in most scenarios they won't find success the first time they attempt to break into a system.

Challenges

There are three ways hacking can be classified. There are white hat, black hat and gray hat hackers. The main purpose of an ethical hacker/white hacker is to test the security of companies or organizations, and find potential vulnerabilities and report them, with authorized permission. Unfortunately, there is a bad reputation about the hacking community, and this brings ethical dilemmas that ethical hackers encounter. Some of these challenges relate to consent, respecting a companies or organizations confidential data, and following complex legal laws and regulations.

Connection to society

Ethical hacking can help improve an organization's security and detect vulnerabilities and patch them before malicious hackers can use them to exploit a company's weakness. In order to further secure a system there needs to be a shift to a hacker mindset. Ethical hackers can bring that perspective and act as a teacher or consultant to educate employees or people how to protect themselves in the digital environment.

Conclusion

Overall, an ethical hacker plays a pivotal role in the cybersecurity world. Having similar skill sets to a malicious hacker and bringing insight on how to improve security. Also, it could potentially assist in predicting how hackers perform their cyber attacks, and prevent them from inflicting damage.

Citation

Ethical hacking issues: professional, legal, social & cultural. (2024, January 17). https://www.knowledgehut.com/blog/security/ethical-hacking-issues

Jaquet-Chiffelle, D.-O. and Loi, M. (1970) *Ethical and unethical hacking*, *SpringerLink*. Available at: https://link.springer.com/chapter/10.1007/978-3-030-29053-5_9 (Accessed: 07 April 2024).

What is ethical hacking?. IBM. (n.d.). https://www.ibm.com/topics/ethical-hacking

MIE-Modern International Education. (2022, April 17). *Society impacts of ethical Hacking.* https://www.linkedin.com/pulse/society-impacts-ethical-hacking-mie-modern-international-education/