Being an Ethical Hacker/Penetration Tester

Jaden Martin

CYSE 201S

Professor Armistead

December 3rd, 2023

Ethical hacking/penetration testing are career fields that solely relies on nonbiased views and a strict understanding of the mission at hand. This type of career is one that is along the more difficult and more decisive occupations within the cybersecurity world, and it takes a lot of knowledge, trust in self, and enigmatic decision making to work in. However, this career also pertains to a lot of the ideals and principles within the social sciences. Being a penetration relies on a deep understanding of social dynamics and policies and applying it to certain situations to best control or halt them. It also is beneficial to be able to completely comprehend and utilize each social science principle into everyday life to implement it into the workplace.

One of the main principles that penetration testers must adhere to when handling situations is the principle of objectivity. This principle refers to the idea that scientist don't use past opinion or bias to shape the way they handle/ research topics and situations (Armistead 2023). In this case, penetration testers must make sure that when they are breaching an organization, they aren't making common mistake in the workplace due to a potential worker conflict or a belief about the business that they don't like. Scientist often asks themselves questions regarding the value of the operation at hand. Relating this to penetration testers, they may have the option to ask themselves questions that pertain to the ethical value of them exploiting a system or organization (Hartley 2015). Also, being able to prepare for engagement and invasion is a key factor with how objectivity pertains itself to the job (Harthorne 2002). Being able to gather information while keeping a stable ground, a balanced mind, and control over impulses is key to being successful in the world of ethical hacking.

The second principle that pertains to cybersecurity fields, especially ethical hacking, is the principle of ethical neutrality. This principle in social sciences is quite literally the main point being ethical hacking, which is that scientist adhere to ethical standards when they do their

research (Armistead 2023). This can be defined to a penetration tester as the ability to make rational and ethical decisions while also thinking like a hacker and being very irrationally and unethically in the situation. Making sure that a companies' defense is top-notch while also validating the level of security this company has defines the principle of ethical neutrality. Understanding the tools that cybercriminals use to breach organizations and using it in a benign way as their job to further improve an organizations defense also tests the confines of ethical neutrality (Harthorne 2002). A professional in this career field is always at odds with this predicament, choosing how to use unethical tools and actions to make ethical and cordial improvements among organizations. A professional penetration tester can also relate this to how individuals within society make these types of ethical decisions in everyday life (Hartley 2015). Individuals choosing to do right by others or wronging others with small and big effects, while also feeling conflicted with their own ideals defines what ethical neutrality really is.

Ethical hacking splits the line between social ethics and individual ethics. Society deems these types of ethics separately all the time, even though they cross more times than not. Having personal doubts on actions taken upon others, to a select group making a collective decision that impacts the majority is a good example of that line between ethics (Hatfield 2019). This can be said for the decision that penetration testers must face when in the environment of security testing. Human factors are considered when testers realize the amount of unknown and random factors in each situation (Armistead 2023). An individual could easily distract the tester as they are trying to break into a system to hack it, or a security guard could catch on if the tester is physically in the organizations building trying to exploit them. Psychology is shown through these types of tribulations, where a tester must persuade another person to stray their attention

from the real issue at hand (Hatfield 2019). These changes can be sudden, and a tester must be able to make quick witted decisions in this accord.

Finally, penetration testers must be able to live within the mind of their counterpart hackers, having to understand the stakes and motivations of the hacker themselves. This can be described with the addition of psychological theories used within social sciences. Cognitive theories explain the way hackers may think and process information as they commit their crimes (Hartley 2015). Penetration testers must realize the paths these individuals will take to make these exploits work.

References

Dr. Armistead, L. (2023) CYSE 201S. Module Notes.

Harthorne, J. (2002). *Penetration testing: A duet | IEEE conference publication - IEEE xplore*. IEEE Xplore . https://ieeexplore.ieee.org/abstract/document/1176290/

Hartley, R. D. (2015). *Ethical hacking pedagogy: An analysis and overview of teaching students ...* Scholar Works. https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1055&context=jitim

Hatfield, J. M. (2019). *Virtuous human hacking: The ethics of Social Engineering in penetration-testing*. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S016740481831174X?casa_token=ugwnHH0x61wAAAAA%3A3heCr0qF-cPsK7-dPlcOc__abCOaVSsZHObh1UcJdesBF3vkerpsm9_DQcqbaSVyC_JFl-qH4Q