Timothy Klein

04/08/2023

Professor Duvall

CYSE 201S

Cybersecurity Career Professional Paper: Penetration Tester

A penetration tester is an ethical hacker who seeks to find exploits within their employer's network to find weak points before a hostile third party finds then exploits the network vulnerabilities. There are many ways to infiltrate and bypass network security measures. Rather than being strictly technical in terms of programming, oftentimes these vulnerable points are those designed with human factors in mind. Understanding the human interactive component with network security means in order to be an ethical hacker worth their salt, they must have a working knowledge of the principles of cybersecurity applied social sciences.

Technology at its heart is a tool which we use to accomplish increasingly complex tasks which gives significance to understanding the reasons and motivations behind its use. Here lies the intersection of technology and psychology, Cyberpsychology, or how technology influences our thoughts, perceptions, and behaviors. In the context of ethical hacking the hacker could utilize social engineering tactics to find weak points in the authorized individuals cyberpsychology to gain access to the network such as gaining passwords or other system identifying information. More specifically a penetration tester may use a tactic called phishing which tricks an authorized user into sharing access to the network through links in emails or other electronic messages. Who to target and how to achieve the breach all require understanding how to use the psychology of the end user against them. If the ethical hacker is successful in

these social engineering attempts then the information gained may be used to ensure those same methods do not work in the future if used against them.

Black box testing is another critical aspect of an ethical hacker's job which involves seeking software specific vulnerabilities in a system from the outside. The penetration tester is given no knowledge of the methods of programming but studies the pattern of work that the system creator has left to find exploits. In this instance it is not an active manipulation of the individual's psychology but an analysis of it to search for vulnerabilities.

The information gained through ethical hackers benefits not just the company or organization which hires them but also gives educational insight to society at large on what common vulnerabilities are shared in certain demographics. Many times cyber victimization victims will not self report instances of successful attacks against them but ethical hackers are able to gain knowledge of how these bad actors operate and what works for them to help the public at large better understand how to better protect themselves. There is no better method of finding how to stop cyberattacks than to act them out but for the good of all rather than detriment. Education is a critical aspect of a penetration tester's job as their method is two-fold: find the vulnerability then teach others how to solve it.

While technical skills are required to become a penetration tester the reality is a majority of the profession both relies and adds to the collective knowledge of the social sciences. Technology is an extension of humanity's intention and motivations which many times are more fickle to manipulation than a systematic code. The human factor lies in influence within every system created and the individuals who operate it. Ethical hacking takes this critical information and uses it for greater education to secure the systems which grow in significance daily. This

knowledge which would otherwise just be in the hands of black hat hackers is able to be utilized to prevent cyberattacks systematically.

Sources

- Bhattacherjee, Anol, "Social Science Research: Principles, Methods, and Practices" (2012). Textbooks Collection. 3.
- *Ethical hacking: Social engineering basics*. (n.d.). Infosec Resources. https://resources.infosecinstitute.com/topic/ethical-hacking-social-engineering-basics/
- Poston, H. (2020, August 11). *What are Black Box, Grey Box, and White Box Penetration Testing? [Updated 2020]*. Infosec Resources. https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/
- Power, A. (2018). *Cyberpsychology and Society Current Perspectives*.