Cybersecurity Professional Career Paper: Ethical Hacking and the Social Sciences

Ava McLaughlin

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

April 16, 2026

Ava McLaughlin

Introduction

Ethical hacking, also known as white hat hacking or penetration testing, is a well-known cybersecurity career in which professional hackers are hired to find and report system vulnerabilities to organizations without causing harm. Cybersecurity careers like ethical hacking are extremely important in the modern world because technology is rapidly advancing, and attackers continue to develop new cybercrime methods faster than defenders can keep up with. Ethical hacking involves thinking like an attacker, allowing for vulnerabilities to be discovered before they are exploited. The purpose of this paper is to examine how professionals in the field of ethical hacking rely on social science research and principles, and it will cover social science principles, the application of key concepts, marginalization, and career connections to society.

Social Science Principles

Social science research is essential in understanding human behaviors related to cybersecurity by explaining cybercriminals' motivations, highlighting ethical concerns, and identifying behavioral patterns that attackers exploit. The seven social science principles are: determinism, relativism, objectivity, parsimony, empiricism, skepticism, and ethical neutrality (CYSE201S (Module 2)); these principles are integrated into cybersecurity practices by ensuring that cyber-user behavior analysis is evidence-based, ethical, unbiased, and interpreted in its full context. Ethical hackers often use social science insights to develop strategies for cybersecurity awareness and education; for example, they apply ethical neutrality by signing a Non-Disclosure Agreement (NDA) and using sensitive company information to improve security awareness rather than for malicious purposes (Yaacoub et al., 2021). Another example is the application of empiricism, as ethical hackers share their real-world experiences on podcasts like Darknet

Diaries to provide evidence of cybercriminal behavior and educate vulnerable technology users (Darknet Diaries – True Stories from the Dark Side of the Internet).

Application of Key Concepts

The ethical hacking profession demonstrates four key concepts seen in class: social engineering, the NICE framework, human factors, and cyber-professional skills/mindsets. Ethical hackers often attempt social engineering, "the art of 'Human Hacking' by manipulating people to give up confidential information or bypass security protocols," (CYSE201S (Module4)) when pen-testing for a company (often posing as an employee or cleaner) before applying more technical attacks, as employees often lack sufficient training (Yaacoub et al., 2021). Ethical hackers fall under the Protection and Defense work role category of the NICE framework, which describes cybersecurity work of all types, whether large or small (NICE Workforce Framework for Cybersecurity). In this role, ethical hackers use techniques such as non-technical attacks, network-infrastructure attacks, and operating-system attacks to identify risks to technology systems (Farsole et al., 2010).

Human factors, "the application of knowledge about human capabilities (physical, sensory, emotional, and intellectual) and limitations to the design and development of tools, devices, systems, environments, and organizations," (CYSE201S (Module 4), are also seen throughout the field of ethical hacking. Ethical hackers apply knowledge of human limitations, like weak passwords, to develop tools that display their weaknesses (that are then used to create solutions), like password crackers; the most common tools include password cracking tools like John the Ripper, a general port scanner like Super Scan, and a web-application assessment tool like Whisker (Farsole et al., 2010). Lastly, Module 5 claims that "a good cybersecurity professional must possess a rich and diverse skill set" (CYSE 201S (Module 5)). Ethical hackers

possess many soft and hard skills, such as communication, problem-solving, adaptability, networking/system administration, knowledge of operating systems/virtual machines, etc, that help them think like criminals (Yaacoub et al., 2021).

Marginalization

According to Module 3, only 18% of science and engineering professions consist of minority groups like African Americans, Hispanics, American Indians, Alaskan Natives, etc., which is largely due to marginalization (CYSE201S (Module 3)). Unfortunately, this trend can also be seen in the ethical hacking profession. After being interviewed, minority groups in the ethical hacking field reported that it is competitive and uncertain, some resources were unstructured and constrained, participants had difficulty being taken seriously, others were often reluctant to share information, environments were unwelcoming, participants often experienced discrimination (sexism, racism, sexual assault, transphobia, homophobia), participants faced a lack of opportunities and awareness, and mentors were often unhelpful (Fulton et al., 2023). Efforts to address these challenges include mentoring members of marginalized populations, helping mentees reach mentors, forming affinity groups with care, clarifying rules of engagement, and improving entry-level opportunities (Fulton et al., 2023).

Career Connection to Society

As the principle of relativism suggests, ethical hackers not only reside in the world of cybersecurity but are also interconnected to other social systems. Ethical hackers impact education, business, the workplace and its safety, technology, sensitive information, and individuals in supporting their safe and comfortable lives (Ul Haq et al., 2022). There are several positive impacts of ethical hackers, such as testing and approving convenient devices like Alexa

and Google Home; with the rise of the Internet of Things (IoT), ethical hackers ensure we are not being spied on in our everyday lives. However, there are also several questionable impacts of ethical hackers on society, like students taking ethical hacking courses for the wrong reasons (easy profit); According to Ul Haq et al., “In classes, 95% of students can take lessons well, while the remaining 5% can be malicious” (Ul Haq et al., 2022). Public policies like those provided in the NIST framework allow businesses from all types of social systems and sizes to protect their sensitive information and defend against the rising number of young, malicious hackers (Cybersecurity Framework).

Conclusion

In conclusion, ethical hacking is a complex cybersecurity career that is strongly related to social science principles like ethical neutrality and empiricism, key social science concepts like social engineering, the NICE Framework, human factors, and cyber-professional skills/mindsets, issues of marginalization like limited access to resources and hostile environments, and broad societal impacts such as securing IoT devices and encouraging interest in hacking among young people, whether positive or harmful.

References

Cybersecurity framework. NIST. (n.d.). https://www.nist.gov/cyberframework

Darknet Diaries – True Stories from the Dark Side of the Internet. (n.d.). https://darknetdiaries.com/

Farsole, A. A., Kashikar, A. G., & Zunzunwala, A. (2010). *Ethical Hacking*. International Journal of Computer Applications. https://d1wqtxts1xzle7.cloudfront.net/33615366/ethi-libre.pdf?1399090455=&response-content-disposition=inline%3B+filename%3DEthical_Hacking_Ethical_Hacking_Procedur.pdf&Expires=1776402822&Signature=V-fWARYBPq~nLflZV2E1~CXU2XP~r1Hdtrj6bVchNFD9x2W1uwTHZkWaNt9pJ8R6AUFcWYhLjOVP-HfgxTkx-LFwNA6MF0hpgJSstfyMkJpzajODbLH3cNbmGSot4yWqk43Mv3J0MsX6EOsgtyRw4Wc-hWEzEfZnNPGyXxPA-Bwfr9ORwWmjQWi7lJxOPB4iuFgElvkSCEtUCT1Zr5y6sHmM7Ueww7fRpKxXIPStcrG1HumUQvs0hszwl-uK9bFX0J~Q7VfOvSKYBd2b0HFMuTEZ4CAmrt-nCytQ2JuraAQWFpABulL7YG3PXzojJubafbqbPgy1wgBEFV9O3nxcNg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Fulton, K. R., Katcher, S., Song, K., Chetty, M., Mazurek, M. L., Messdaghi, C., & Votipka, D. (2023). *Vulnerability Discovery for All: Experiences of Marginalization in Vulnerability Discovery.* IEEE Symposium on Security and Privacy (SP). https://kfulton121.github.io/assets/pdf/v4a.pdf

NICE Workforce Framework for Cybersecurity. National Initiative for Cybersecurity Careers and Studies. (n.d.). https://niccs.cisa.gov/tools/nice-framework

Old Dominion University. (n.d.). *CYSE201S (Module 2) Principles of Social Sciences and Cybersecurity.* https://canvas.odu.edu/courses/201835/files/58917413/download?download_frd=1

Old Dominion University. (n.d.). CYSE201S (Module 3) *Strategies to Study Cybersecurity through an Interdisciplinary Social Sciences Lens.* https://canvas.odu.edu/courses/201835/files/57930187/download?download_frd=1

Old Dominion University. (n.d.). *CYSE201S (Module 4) Cybersecurity and Human Factors.* https://canvas.odu.edu/courses/201835/files/59116295/download?download_frd=1

Old Dominion University. (n.d.). CYSE201S (Module 5) *Applying Psychological Principles of Cyber Offending, Victimization, and Professionals.* https://canvas.odu.edu/courses/201835/files/59994035/download?download_frd=1

Ul Haq, H. B., Hassan, M. Z., Hussain, M. Z., Khan, R. A., Nawaz, S., Khokhar, H. R., & Arshad, M. (2022). The Impacts of Ethical Hacking and its Security Mechanisms. *Pakistan Journal of Engineering and Technology*, 5(4), 29–35. https://doi.org/10.51846/vol5iss4pp29-35

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021, March 30). *A Survey on Ethical Hacking: Issues and Challenges.* arXiv.org. https://arxiv.org/abs/2103.15072