Culture, Society, and Praxis

Volume 13
Number 2 *Looking Forward, Looking Back*

Article 4

December 2021

Ethical Hacking

Mollie Brogdon

Culture, Society, and Praxis

Ethical Hacking

Mollie Brogdon

INTRODUCTION

When most people hear the word *hacker*, they perceive an ominous person in a dark room, lit solely by computer screens as they attempt to steal someone's information or data online in an illegal manner. While this may be true of some hackers there is much more to hacking than criminal activity. Ethical hacking is conducted by an individual or company to help identify possible threats on a network, computer, or other system. Also known as "white hat" hackers or "penetration testers", they find holes or weaknesses in these platforms that criminal hackers could exploit. The information that the ethical hackers find allows their employers to secure their systems and protect private information against criminal "black hat" hacking.

Given the public's negative perception of hacking, how do ethical hackers demonstrate ethical conduct in order to perform in a professional setting? This paper proposes that the formal educational and professional community of ethical hackers helps to maintain their professional integrity. First, I argue that formal education develops integrity and socializes students into the established community of ethical hackers. Then, I examine an ethical hacking community to demonstrate how it creates and upholds professional norms.

EDUCATION

While most information available on teaching ethical hacking provides suggestions on pedagogy, there are no studies that demonstrate the effectiveness of different methodologies for educating ethical hackers. However, there is consensus on what professionals involved in the field of white hat hacking believe to be the best course of action.

Many scholars argue that computer science programs must teach ethics along with technical skills. Students are less likely to pursue criminal activities when correctly taught in a fashion that discourages the mistreatment of information (Pike, 2013). This is why starting the appropriate education on the intricacy of hacking, and the associated ethics, from the beginning of a white hat's career is crucial. Consequently, students must be educated on practices, law, and outcomes of their actions (Logan & Clarkson, 2004), which could be accomplished through courses on law and computer ethics (Pashel, 2007). Finally, computer ethics policies are a vital part of ethical hacking education. Providing the sufficient resources and knowledge surrounding these policies is overwhelmingly projected to reduce unethical behavior (Hartley, 2015).

Other scholars argue that universities must lead education efforts on ethical hacking through detailed instruction on campus information security policies, and strict enforcement of these policies. It is not beneficial for students when universities only state policies in a syllabus or have brief discussions on them; instead, universities must provide in-depth explanations of guide-

Mollie Brogdon is a Social and Behavioral Sciences major with a concentration in Anthropology and a minor in Environmental Studies. She can be reached at mbrogdon@csumb.edu.

lines and policies (Logan & Clarkson, 2004). Students must also understand—and fear—the consequences of illegal actions. Instilling this fear, at the university level, proves to be a powerful deterrent (Greene, 2004). Failure to inform students of the repercussions at such an influential point in their hacking career is a risk to future security professionals (Logan & Clarkson, 2004).

COMMUNITY

The community that information security specialists and ethical hackers have established further contributes to maintaining professional integrity. Participation in the community and adherence to community standards develops a hacker's own ethical standings. Members of the community have identified social interaction/support systems and competitions, as important contributors to their community. Involvement in these categories is important for students because it strengthens the foundational aspects of their careers, protecting them from future misconduct (Pike, 2013).

Affiliation with peer groups has an impact on white hat education as there is a strong desire for acceptance within the community. A person is more likely to make decisions based on what their peers deem acceptable, in addition to their own personal ethics (Wible, 2003). Therefore, the interaction between community members and understanding of their peers has a significant impact on their overall ethical standards.

Competition assists in upholding ethical ideals. While an extensive range of different types or styles of competitions exist, the most common consists of a group of hackers attempting to hack into other competitors' systems while simultaneously safeguarding their own. Competitions establish positive incentives and provide hackers with a clear understanding of what is ethical or acceptable behavior (Wible, 2003). These competitions have multiple indirect positive influences. Frequently, competition is the first real experience some students have in the ethical hacking field, which helps beginners get a better understanding of how the professional or working world in their field will operate (Pike, 2013). Maintenance of community expectations is an additional result of competitions. Clarification and observance of proper and acceptable action when faced with ethically dependent decisions results in an increase of law-abiding hacking (Wible, 2003). In other words, reflected in the way they compete, experienced members have better understanding of the ethical standards their community maintains. New hackers and other community members watch and learn, in real time, about the appropriate ethical decisions these veterans make. This natural acculturation by way of competitions is a significant contributor to their overall professional integrity.

A LOOK AT THE COMMUNITY

You can learn a lot about a person from the community with which they are involved. This is why I sought a platform where I could observe community and interaction between those who share the same professions and interest in the ethical hacking realm. One of the most popular sites that I was able to find was Ethicalhacker.net, The Ethical Hacker Network. Ethicalhacker.net is a free online magazine and community for security professionals. They post news articles and informative pieces and provide a space for discussion on a wide variety of topics related to cyber security. Here you can find students, beginners, educators, certified professionals, or those simply interested in the field of cybersecurity. The website advertises its ability to connect new and experienced white hats and provide professionals a space to expand their network, look into publishing, and help others. On Ethicalhacker.net, I observed commitment, reciprocity, and different rules of interaction.

A measure of commitment on the site is seen through the length of time members are active on the site. A great example of this originates with a post made in 2008 by a 19-year-old college student. He was looking for advice on what other certifications in cyber security he would need before he graduates to have a leg up on his competition. After the initial surge of responses in 2008, the post lay dormant for 12 years. However, in January 2020 the former college student added another post to the forum. He updated everyone to let them know what he has accomplished with his career in ethical hacking and also mentioned that he is now married and has kids. A few of the members who responded to his original post also replied to this one. They congratulated him and wished him well. This long-standing interaction demonstrated a high level of commitment within the community.

I observed reciprocity in a forum on ethical hacking equipment opinions and how it impacts 'newbies' in the cybersecurity field. The original post discusses common questions that arise among those at the beginning of their careers. The most popular questions included, "What type of equipment is required?" and "How should the equipment be set up?". This particular post received much attention, as there was a surplus of people who wanted to share the type of equipment they have or their suggestions on what would be best for beginners. The first few responses shared information about different resources for those interested in what they call "hacking labs", where companies offer hackers to use their equipment for a paid amount. One individual commented that he was planning to re-do his own lab and wanted to know if anyone was interested in the idea creating a new thread that would discuss the details of his plans and outcomes. Many people responded to this with enthusiasm. The collective response was that his proposal would be beneficial for both new and seasoned folk. From this forum, I gathered that this online community has a great deal of reciprocity. Bettering the experiences of others within their field, along with their own, proved a strong interest for members.

Although the blogging site does not state any 'rules', a few guidelines are evident. While exploring posts, it quickly became clear that commentary on criminal hacking is shunned and unwelcome. A teenager made one post where he was looking for help on how to avoid the block that his parents put on his internet router that forced his internet shut off at a certain time of night. The advice he expected was not the responses he received. Those who responded to his original post made sure to let him know that this was not the website where he should be asking this type of question. It is important to note that almost all the respondents made it clear that they do not desire to help anyone hack under unethical terms. They refused to help this teenager, standing by their moral code as ethical people to not participate in unethical tasks, no matter how mundane it is. This is reflective of the standards of the ethical hacking community on and off ethical-hacking.net.

People who participate in ethical hacking have a deep respect for their profession. The utilization of sites like ethicalhacker.net where there is free and open discussion on facets of ethical hacking establishes that these are not people looking to use their knowledge for malicious purposes. Instead, they are actively engaged in professionalization through interaction in this community. The community demonstrates commitment to helping one another, reciprocity, and extremely low tolerance for criminal activity. It is a community of professionals wishing to communicate with others in their field to discuss a common interest and maintain their principles, including socializing newcomers into the ethics of the profession.

CONCLUSION

Both education and community prove to maintain the professional integrity of ethical hackers. Universities and educators play a significant role in establishing ethical groundwork, and the community of ethical hackers develops and maintains professionalism within the field. Competitions, peer groups, or online forums establish that the community values their own professional integrity and strives to maintain it. The main concern for the future is the remaining stigma or stereotype around the term 'hacking'. However, I remain optimistic that dismantling of this stereotype will take place as I project the demand for ethical hackers to increase in the following years as new technological advances continue to develop and evolve. I suggest this will be attainable if proper and intentional education for prospective ethical hackers takes place, along with educating businesses, companies, and the public on what the profession of ethical hacking is, the true community and people involved, and the many benefits that can arise from it.

BIBLIOGRAPHY

Greene, T. (2004 July, 22). Training ethical hackers: Training the enemy? *eBCVG*. https://defcon.org/html/links/dc_press/archives/12/ebcvg_training_ethical_hackers.htm.

Hartley, R. D. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management*, *24*(4). https://scholarworks.lib.csusb.edu/jitim/vol24/iss4/6/

Logan, P. and Clarkson, A. (2004). Is it safe? Information security education: Are we teaching a dangerous subject?. *Proceedings of the 8th Colloquium for Information Systems Security Education*. West Point, NY. http://cs.potsdam.edu/faculty/laddbc/Teaching/Ethics/StudentPapers/2006Pashel-TeachingStudentsToHack.pdf.

Pashel, B.A. (2007). Teaching students to hack: Ethical implications in teaching students to hack at the university level". *Proceedings of the 2006 Information Security Curriculum Development Conference. Association for Computing Machinery*. https://doi.org/10.1145/1231047.1231088.

Pike, R. (2013). The "ethics" of teaching ethical hacking. *Journal of International Technology and Information Management, 22*(4). https://scholarworks.lib.csusb.edu/jitim/vol22/iss4/4/

What is ethical hacking: Types of ethical hacking: *EC-Council*. https://www.eccouncil.org/ethical-hacking/.

Wible, B. (2003). A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime. *The Yale Law Journal*, *112*(6), 1577-1623. https://doi.org/10.2307/3657453.