Logan Riley

Professor Hayes

Procedural Programming

2 February 2024

The Good Hacker?

The term “hacker” has been altered throughout the years since technology has been created. The correct definition of a hacker follows “A hacker is a person who breaks into a computer system. The reasons for hacking can be many: installing malware, stealing or destroying data, disrupting service, and more. Hacking can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed.” (Cisco,). Whether or not a hacker uses their skill to help a company secure their firewalls or they use their hacking skills for malice intent. Those who use their talents for ethical and company gain are called white hats, people who might not follow the ethical laws, but not have any malicious intent are called grey hats, and hackers with malicious intent are called black hats.

I believe system cracking is ethical, if it is for the good of the company and if the company allows hackers to test their security or any firewalls. If the company does not allow it, then the action of trying to hack a company would not be ethical. No matter if it is just for fun, no one wants their business or information being tampered with. If no theft, vandalism, or breach of confidentiality happens it still is not ethical for a hacker to still attempt. Once that attempt is started their name or title would be tarnished and people would be careful being around said person. Matthew 5:13 “You are the salt of the earth. But if the salt loses its saltiness, how can it be made salty again? It is no longer good for anything, except to be thrown out and trampled

underfoot.” Once you lose your white hat status, or your saltiness, you cannot gain it back or you will become a grey hat.

If a hacker discovers a vulnerability in a system, he or she should tell the user of the system about the vulnerability and how they discovered it. In the CNBC story Yosi Dahan did the right ethical thing by trying to contact the company. Even though the company did not reach out to him, this is why more companies need white hat hackers, the more technology advances, the further hacking tools and hackers will evolve as well. “Cyberattacks are one of the biggest threats facing businesses, and the cost of data breaches at companies is expected to hit $2.1 trillion globally by 2019, according to Juniper Research. While some firms are spending more on shoring up their defenses internally, independent researchers can often give another perspective on security flaws.” (CNBC, 2015). If I was Yosi Dahan and the company did not respond to the email and I had to go to the media for me to get their attention, I would have not even gone to the media. I would have kept abusing their system until they realized the importance of having a white hat hacker on their side.

Works Cited

"What Is a Hacker?" Cisco, www.cisco.com/c/en/us/products/security/what-is-a-hacker.html#~types-of-hackers.

"Ethics and Professional Responsibility in Computing | Online Ethics." Onlineethics.org, onlineethics.org/cases/ethics-and-professional-responsibility-computing.

Arjun Kharpal. "Ethical Hacking: Are Companies Ready?" CNBC, CNBC, 17 June 2015, www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html.