Cody Cain

CSCI 235 Procedural Programming

Dr. Sean Hayes

2-11-19

The Ethics of Hacking

Cyber threats are one of the largest problems facing our world today. People, companies, and even governments are constantly under threat of attacks, and it is a continuously growing problem. Most people only hear the word “hacker” after being told their personal information has been stolen from a database held by their credit card company, bank, or government agency. For this reason that word, understandably, has a negative connotation. However, according to the “Internet Users Glossary”, a hacker is “A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular” (Malkin). This paper will attempt to show the ethics of hacking.

First of all, is hacking ethical? It depends. Mostly it depends on permission. If the hacker has been given permission by the owner of the network, than it is ok. Otherwise, it is unethical not to mention illegal. According to Robert Cain, a certified ethical hacker, when a hacker works for the owner doing penetration testing, which is the ethical side of hacking, they are given an ROE or Rules of Engagement. These rules clearly spell out how far they are allowed to go and what they are and are not allowed to do. If they exceed these rules, they could face termination or even have legal action taken against them (Cain). Hacking for any other reason, regardless of intention, is unethical as well as illegal.

Now what should a hacker that has not been authorized by the owner do if they find a vulnerability? How should the company respond? If an unauthorized hacker finds a vulnerability, then they should report it. If the owner is inclined to listen and realizes that it is a legitimate threat, then they should attempt to patch it. The hacker should expect no recognition or compensation. Doing so would be borderline ransom, asking for reward for a service that was not requested. However, this situation should not come up in the first place. If the hacker has been employed by the owner to do a penetration test then they are responsible to report their finding as part of their job, pay would be included as part of their contract or employment by the owner. However, if the hacker has not been given explicit permission by the owner to look for vulnerabilities then they never should have been looking in the first place. They would be acting unethically.

In reference to Yosi Dahan voluntarily hacking into United Airlines network, he was acting unethically because he did not have permission from United Airlines to look for vulneraries. United Airlines had no obligation to respond to his claims. Whether or not they investigate is their discretion (Kharpal). There is a way to go about ethical hacking, but this was not it. That way is to be employed or given permission by the owner.

The problem with people hacking without authorization is that no matter how ethical they think they are, there is no accountability. Many see hacking as a grey area, where the wrong things are ok if done for the right reasons. But the Bible teaches that the methods that are used are just as important as the intentions. Romans 13:1 tells us that we must obey the laws of the land. According to “Ethical Hacking and Countermeasures” a textbook by the International Council of Electronic Commerce Consultants (EC-Council), “It remains a fact that gaining unauthorized access is a crime, *no matter what the intention is*” (EC-Council, p.15).

Works Cited

Cain, Robert. Personal Interview. 10 Feb. 2019.

Ethical Hacking and Countermeasures v7.1. EC-Council, 2011.

"Internet Users Glossery." Edited by G. Malkin, *Ietf.org*, Aug. 1996, datatracker.ietf.org/doc/rfc1983/.

Kharpal, Arjun. "Are Companies Still Scared of 'Ethical' Hackers?" *CNBC*, CNBC, 19 June 2015, www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html.

The Holy Bible: New International Version. Zondervan, 1984.