Hacking Hats

Levi Seibert

Athens State University

IAM 409: Management of Information Assurance

Dr. Robert Grant

19 April 2020

Abstract

The practice of grey hat hacking is considered from the ethical, moral, and legal positions. Grey hat hacking is the unauthorized, yet unmalicious, act of hacking into a computer system or network. The practice is typically recreational with hackers “testing” random or specific targets to try to penetrate. If successful, the hacker often times will report the vulnerabilities they have found to the organization they target; however, not all will.

Keywords: hacker, grey hat, white hat, black hat, ethics, morals

Body

Introduction

A hacker is someone who breaks into a secure computer system or network. There are three types of hackers, each given a title of a different colored hat. The black hat hackers are the "bad guys." These are what most people think of when they hear the term "hacker". Black hat hackers break into networks for malicious purposes and often cause chaos for their victims. On the other side of the spectrum, white hat hackers are the "good guys." They are computer professionals who get hired by companies to try to penetrate their network without causing undue harm (an ethical action known as penetration testing). In between the two extremes are grey hat hackers: those who hack into systems without authorization but also without malicious intent. Some grey hat hackers report their findings to the organization they penetrated, while others keep it private. Regardless of what they do with the information they discover, grey hat hackers are differentiated from black hat hackers in that causing harm is not their intention, although it often is possible. They also differ from white hat hackers in that their actions are not authorized by the organization, even if the organization is later appreciative of the hacker's discovery of the vulnerabilities. The practice of grey hat hacking is deemed admirable by some, abhorrent to others, and neutral to still others. When the ethical, moral, and legal aspects of grey hat hacking are considered, it is apparent that it is wrong.

Ethicality of Grey Hat Hacking

Grey hat hacking is sometimes referred to as ethical hacking; however, this is quite far from the truth. According to Michael Whitman and Herbert Mattord in their textbook, *Management of Information Assurance*, ethics is the way humans ought to act (2018). This definition is very broad, yet it offers the basic premise that there is an inherent "ethical" standard that is applicable to the entirety of the human race. Writingexplained.org, a website geared to educating its readers about the proper use of grammar and writing style, further explains that ethics are "rules concerning upright behavior" (Writing Explained, n.d.). The term "upright" implies that the behavior is proper, honorable, honest, and above reproach ("upright", 2020). Unauthorized exploitation of a network, for any reason, does not fit into this definition. Only in the situation when a white hat hacker is hired by an organization to test its own network for vulnerabilities is breaking into a network ethically reasonable. Many times, a grey hat hacker's purposes and motives are honorable. For example, their goal is to unmaliciously search for vulnerabilities in an organization's network and then report their findings to the organization in order to increase the security thereof. Despite their good objectives, intentional unauthorized access does more harm than good.

According to The Association for Computing Machinery's (ACM) Committee on Professional Ethics, there are at least three main reasons grey hat hacking is unethical. First of all, they assert that it is not possible for an individual to know that no damage will be done by their "harmless" behavior. The Committee cites the example of the 1988 Morris Worm, caused by Robert Morris Jr. Morris had written a code that was supposed to count the number of machines on the Internet; however, the program had a bug in it and accidentally shut down numerous computers around the world and caused millions of dollars of damage. His intentions were not malicious; yet, his actions backfired drastically. Although this is a drastic case, the principle is still there: grey hat hacking is a risky business. The ACM Committee on Professional Ethics also states that intentional bypass of security mechanisms is wrong. This should be obvious. Security measures are put into place to keep people out, rather than invite them in. Finally, the Committee claims (rightfully so) that any intrusion is a breach of confidentiality. Since the goal of information assurance is to protect confidentiality, integrity, and availability, intruding on private data does cause harm, even if only theoretical (ACM Committee on Professional Ethics, n.d.). Data security is important and should be highly valued by all organizations. A beneficial tool for risk assessment is penetration testing; however, grey hat hackers should not hire themselves for the job without being asked. There is a large community of white hat hackers who are available for companies to enlist for the job. Penetration testing is a proper and ethical way of finding vulnerabilities and assessing risk to an organization's information assets. Grey hat hacking may have the same final effect, but it is not ethical. In fact, those who call the exploitation and intrusion of a private networks ethical actually lower the ethical standard for the rest of society.

Morality of Grey Hat Hacking

It is apparent that grey hat hacking does not meet the standards of upright ethics; however, one may wonder about its morality. According to the aforementioned Writingexplained.org website, "Morals refer to principles of right and wrong behavior...Morals are the way people exercise their ethics." (Writing Explained, n.d.). Obviously, ethics and morals and very closely aligned. Morals are the practical application of ethics. Therefore, if grey hat hacking is ethically wrong, it is then implied that it is morally wrong as well. Morals does have a bit of a broader scope; however. Dictionary.com states that morals "refer mainly to guiding principles" while ethics "refer to specific rules and actions, or behaviors" (Dictionary.com, n.d.). In morals, there is more a sense of black vs. white and good vs. wrong. There is little room for grey areas, a principle which Courtney Falk, Dr. of Philosophy, claims has a direct link to the field of hacking. After considering Mill's, Kant's, and Aristotle's theories of morality, he concludes that grey hat hacking "is a morally wrong action and … should be neither condoned…nor practiced" (Falk, 2004). If morals are supposed to be guiding principles of a proper lifestyle, then grey hat hacking would definitely fail. Does grey hat hacking set good precedence for other computer related activities? Obviously, it does not. As an example of its immorality, unauthorized access to a computer is actually a form of spying. Inevitably, a hacker will see information that was not meant for their eyes (it is supposed to be confidential). According to most, if not all, moral standards in the world, espionage is not endorsed. If spying is morally allowed for grey hat hackers, why should it not be for everyone else? Permitting unauthorized prying into confidential data is an affront to not only the organization's privacy but possibly also that of its customers/clients' data. Therefore, it is clear that the unmalicious, recreational practice of grey hat hacking is immoral as well as unethical.

Legality of Grey Hat Hacking

Although the ethical and moral aspects of grey hat hacking are pretty clear-cut, one may still wonder if it is legal. The current evidence, however, does seem unfavorable for those who partake in the dishonorable hobby. The Computer Fraud and Abuse (CFA) Act, part of the U.S. Code states, states, "Whoever...access[es] a computer without authorization…and by means of such conduct ha[s] obtained…restricted data...shall be punished…" (Legal Information Institute, n.d.). This appears to mean that unauthorized hacking, of both the black and grey hatted nature, is illegal; however, due to the CFA's verbose legal nature, it is difficult to be sure of the correct interpretation. When the judicial precedence is considered, it does seem apparent that this is the proper understanding. Not long after the CFA was passed, it was used to convict the aforementioned Robert Morris Jr., who "accidentally" shut down the Internet (Zetter, 2014). Although Robert Morris Jr. wasn't really a hacker, he did access others' computers without authorization. His actions had obvious negative impacts, but many hackers' do not. This no more excuses grey hat hackers than it excuses speeders for never being in a wreck. The law is the law and disobeying it is, by definition, illegal. Despite this fact, many organizations will not prosecute hackers as long as the vulnerabilities are clearly brought to their attention in a non-malicious manner (Electronic Frontier Foundation, n.d.). This does not excuse the practice of breaking into a network. Companies may be appreciative for the information provided to them by the hacker, but if they want to test their security, they should hire a white hat hacker. Not only are they more ethical, moral, and legal, white hat hackers probably will provide much more robust information to the organization and they are accountable for their actions.

Conclusion

It is evident that grey hat hacking is unethical, immoral, and illegal. Ethically speaking, grey hat hacking is wrong in that it is a form of trespassing that comprises confidentiality and takes unnecessary risks. On a moral scale, it fails at being a benchmark for honesty. Legally, it breaks the Computer Fraud and Abuse Act and deserves to be prosecuted. Therefore, grey hat hacking is ultimately wrong. This is not to say, however, that all forms of "hacking" are unethical, immoral, or illegal. White hat hackers (also known as penetration testers or ethical hackers) offer their services to companies who want to test the strength of their information security. These individuals are given permission to break into otherwise secure networks; however, they are not supposed to compromise the confidentiality, integrity, or availability of the information inside. They find vulnerabilities, exploit them (unmaliciously), and then report their findings to the hiring company with the goal of securing the network from black hat (and grey hat) hackers. White hat hacking, therefore, is a practice that is above reproach. This makes sense, given the analogy of different colored hats. Black is the color of evil and wickedness; white of purity and virtue; and grey is a mix of the two. However, nothing can truly be both evil and good. As has been proven, grey hat hacking is improper and unacceptable. In fact, one could reasonably argue that it is purposeless, or colorless. Since black is the absence of light and color, it then could be implied that grey hat hacking is actually a form of black hat hacking that looks slightly positive from the outside. Unfortunately, looks can be deceiving. The miniscule amount of white in the grey (the goal of helping an organization) is overshadowed by its bleakness (unethical, immoral, and illegal unauthorized access into a secure system/network). Therefore, only two colors of hackers remain. In a derivate of the traditional battle of good versus evil, there is a combat between the hacking hats: white versus black.

References

ACM Committee on Professional Ethics. (n.d.). *Question: Is it ethical (or even legal) for a company to prosecute an individual for discovering a vulnerability when they purposely broke in, grey-hat style, but they caused no harm?* ACM Ethics. Retrieved February 2020, from https://ethics.acm.org/integrity-project/ask-an-ethicist/ask-an-ethicist-grey-hat-hacking/

Dictionary.com (n.d.) *What's The Difference Between "Morals" vs. "Ethics"?* Retrieved March 2020, from https://www.dictionary.com/e/moral-vs-ethical/

Electronic Frontier Foundation. (n.d.). *A "Grey Hat" Guide.* Retrieved February 2020, from https://www.eff.org/pages/grey-hat-guide

Falk, C. (2004). *GRAY HAT HACKING: MORALLY BLACK AND WHITE*. Retrieved February 2020, from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2004-20.pdf

Legal Information Institute. (n.d.) *18 U.S. Code § 1030.Fraud and related activity in connection with computers*. Cornell Law School. Retrieved February 2020, from https://www.law.cornell.edu/uscode/text/18/1030

Upright. (2020, February 23). In *Merriam-Webster.com dictionary*. Retrieved March 2020, from https://www.merriam-webster.com/dictionary/upright

Zetter, K. (2014, November 28). *Hacker Lexicon: What is the Computer Abuse and Fraud Act?* Wired. Retrieved February 2020, from https://www.wired.com/2014/11/hacker-lexicon-computer-fraud-abuse-act/

Whitman, M. & Mattord H. (2018). *Management of Information Security*. (6th edition). Cengage Learning. Retrieved from https://ng.cengage.com/static/nb/ui/evo/index.html?snapshotId=1537576&id=682385846&eISBN=9781337405737

Writing Explained. (n.d). *Ethics vs. Morals – What's the Difference?* Retrieved February 2020, from https://writingexplained.org/ethics-vs-morals-difference