Principle Ethical Hacking & Considerations

John Jackson

Ethical hacking is a phrase that is tossed around as a key descriptor to define a hacker that operates with good intention, or in other words, does the "right" thing. The issue with the phrase

"Ethical Hacker", is the representation of what ethical versus unethical really is. The philosophical field of ethics is complex and sometimes perception is not always the reality. In addition, someone's self-assigned ethics can be conflicting and biased. A lot of the issues within hacking culture are resultant of intention, and various restrictions on all ends of the hacking spectrum - especially as it pertains to the acquisition of knowledge.

When society thinks of the phrase ethical hacker, they imagine a hacker who does the right thing. In fact, non-technical individuals typically struggle to define what it means to be an ethical hacker. Over the years, there have been many internal fights, in an attempt to redefine what qualifies a hacker. Nonetheless, the matter isn't what qualifies a hacker, but what a hacker's intention looks like in relation to the vulnerabilities exploited. The primary issue with the phrase ethical hacker is that it's nearly impossible to come to an adequate conclusion on ethics within the confines of the law. In short - the justice system isn't concerned with moral and immoral, the enforcers of the law are concerned with whether an act is against the law or not.

The constraints placed by the law actually make it harder for a hacker to be considered ethical and even the ones that are considered as such sometimes are not, at least in the eyes of the prosecutors. Imagine the following instance: A security researcher is hacking different domains within the legal limits of a vulnerability disclosure or bug bounty program. During their research on the company, they discover a zero-day vulnerability that impacts multiple companies. When they report the vulnerability to the program, they are told strictly not to disclose the zero-day to the public until the vulnerability is patched or after 90-days passes. In some instances, holding onto the vulnerability for disclosure rather than immediately disclosing it can do more harm than good. Every situation varies, thus the intensity and progression of some form of escalation on the reporting and resolution process can quickly become hazy. In the perfect world, the program that the hacker reported to can manage and coordinate the zero-day efforts, in an instance where it's the enterprise's product - not disclosing for 90-days may be reasonable. People remain self interested, and a company may be more concerned with bad publicity than with the disclosure of a zero-day vulnerability.

For example, if the zero-day were to be on a third-party vendor's product, the company the vulnerability is reported to has no control of the vendor's clients. It would do more harm than good to refrain from disclosing the vulnerability as the researcher is only protecting the company that they reported it to while thousands of other companies remain vulnerable. Would it be more ethical to stay within the non-disclosure regulations from the company and help them, or to help thousands of other companies? Hacking has ironic utilitarian undertones, especially when the ethical space is analyzed. Unfortunately, again, the law/policy isn't concerned with morality therefore "unethical" if disobeyed, by definition. The hacker in a circumstance described as such would probably want to obtain a CVE ID and disclose - but one of the major issues with VDPs and Bug Bounty Program are restrictions that make sense for regular vulnerabilities, but work against the general public and "ethical" hackers in scenarios as described. If the company that the hacker reports the zero-day vulnerability to works with the vendor, the situation can be coordinated far cleaner - however that's not always the case and restrictions may work against the actual ethics of disclosing a vulnerability.

What about a hacktivist that operates as a Blackhat? Per hacking definitions, a Blackhat is considered "unethical" hardly ever doing the "right" thing. The true question is: in what sense? In both a legal and moral sense, the answer is, "sometimes not always". Complexities surrounding the ethics of hacking make security research and accountability exceedingly difficult, and the words are tossed around in a hurtful way that can actually destroy the goals that security research and hacktivism set out to create. As an example that coincides, imagine if a Blackhat without permission were to find a SQL

Injection vulnerability on an application hosted on a private-server containing evidence of human trafficking. If the Blackhat exposes this to the public, they are admitting to breaking the law by attacking the server, and could be punished for it. As far as the government is concerned, they are acting unethically and stepping outside of the bounds of what they have permission to hack. Situations like this are difficult to comprehend because any moral individual that evaluates the ethics of their actions would deem this is being ethical and a service to society. The law doesn't care about the ethics of actions, and this vigilante type of action could result in prosecution.

The two examples from the analysis of a "Whitehat" and a "Blackhat" have one thing in common: hackers are constantly battling with questions of what the most ethical or responsible approach is, for both society and involved parties. A Blackhat may consider it ethical and virtuous to dump a database full of PII belonging to known-child abusers, whereas a Whitehat will likely avoid testing the server of something that they don't have access to. For adequate comparison, a Greyhat might hack the server and submit the vulnerability to a federal agency anonymously or furnish this information to less "ethical" parties depending on the circumstance.

The problem with all of the different ethical determinations of hackers has an end result of restricted knowledge. As an example, the Information Security community doesn't like Blackhats. Tension creates unnecessary avoidance and problems because a lot of Whitehats also work in Information Security full time and many in the community may shun them for any sort of participation in research with hackers that are not deemed fully "ethical". On the inverse, a similar problem exists with Blackhats. A lot of blackhat culture revolves around psychological operations, personal rivalries tied to years of history, and no-restriction release of hacks/vulnerabilities. White or Greyhats that want to stay within the legal limits of the law, or even ensure that they may work in the Information Security field, will have to pick and choose what to avoid from both a hacking and historical-involvement based perspective. After all, an employer doesn't want to manage an employee who drops illegal hacks or gets involved with "malicious" groups, no matter how ethical of a cause society deems it to be. The bottom line: knowledge for hackers that want to learn a wide range of skill sets is restricted because the Information Security community will shun someone with "questionable" associates and the Blackhat community is allergic to hackers that they deem as being "afraid to hack", AKA "afraid to release vulnerabilities illegally". The knowledge gaps persist when another aspect is brought into question, which is the methodology that hackers use. In the ethical community, there's a lot of gatekeeping of hacking tools, technologies, and exploitation expertise. In the "unethical" communities, the opposite exists - they are willing to share tools and methodology for organized goals. Such a concept exists because the ethical space is riddled with hackers who are concerned with making money from bug bounty programs, and the less their competitors know, the better. In addition, Blackhats typically have more access to realistic knowledge because they are not binded by an operational program scope like Whitehats are. These various issues make it difficult for both communities to co-exist, and in turn, makes it harder for legitimate enterprises to receive better defense guidance.

Ethics in the hacking space and what defines an "Ethical Hacker" are controversial and will likely be argued until the end of time. Nonetheless, society as a whole, especially the Information Security community, needs to push for the abolishment of the CFAA [Computer Fraud Abuse Act] which is the law in place that prevents hackers from carrying out hacks on systems that they do not have access to or permission to test. Realistically, the establishment of the CFAA only works against security researchers that are hacking with good intention in mind. If a Whitehat or considerably ethical hacker were to stumble upon a major vulnerability, the CFAA strikes fear into the minds of many and the vulnerability may never be responsibly disclosed to the affected party. Punishment for crimes that relate to hacking should be redefined as laws that work off of the intention of a hacker. For example, hacking an enterprise and stealing money should obviously be considered crime, whereas hacking an enterprise and submitting the vulnerability to a company without leaking the vulnerability to the public should not be considered criminal behavior. If the CFAA were to be abolished, society could do away with the terms Blackhat, Whitehat & Greyhat and could focus on instances of hacking being considered criminal or not. Intention is everything in the hacking community and the only way we can fix the major legal ramifications and fear within the community is to unify all hats and focus on punishing actual criminal behavior such as theft, doxxing, fraud, or actions in which hackers become criminals for their own gain, psychologically and physically. ●