ETHICAL HACKING

Marissa Cleroux

Systems IV

Christine Donohue

March 12, 2020

1. Executive Summary

For as long as computers have existed there are have been individuals trying to distort the original designers and programmers' intentions. Ethical hacking is a necessary tool for catching these distortions or vulnerabilities before malicious actors can exploit them (James). Ethical hackers are in high demand, as is shown by job boards and the rise of bug bounty platforms, where organizations put out calls to be hacked (Sharpe). The definition of an ethical hacker for this report is a hacker who is hired by the system's owner to hack their system and disclose any bugs or vulnerabilities found (EC-Council), although this definition is not official by any means.

Hackers must follow many of the same steps as a regular hacker to conduct their business. They conduct a hack by gathering information, testing the boundaries, and then exploiting the system when they think they have found a way in (Engebretson, 19). Once the hacker exploits the system, they document their findings and disclose them to the system owner and they system owner only, which is know as responsible disclosure (Detectify).

Organizations benefits greatly from ethical hackers because they make the organization's system more robust and secure (EC-Council). However, ethical hackers also face a great deal of risk. They must practice their work diligently and with great care to not put their employer's system at risk (Johansen). Ethical hackers may also not be paid enough for their work, as they can put many hours of research into a job, and come up with nothing, therefor losing out on that time and money spent researching (Lu).

As ethical hacking is already being incorporated into the new program it shows the importance of the profession in the field. Students must also learn the risks and laws associated with ethical hacking and how to properly protect themselves from persecution.

Table of Contents

2. Introduction

Ethical hacking is not well-defined and depending on who is talking, it can be a very specific type of hacking or a variety of types of hacking that is done with “good intentions.” Some experts define ethical hacking as a strict profession: an ethical hacker is someone who hacks in a “professional manner” with the full knowledge and permission of a client (EC-Council). Others may include a broader group of individuals such as hacktivists, military hackers, and security activists (Maurushat). As such, it is difficult to pinpoint which view is right. For the purposes of this research paper, an ethical hacker is an individual who has been hired to test the security of a system by the owner of the system. This does not reflect the belief of the author but sets a clear scope for this research paper. The purpose of this report is to explore ethical hacking and how the Computer Science program at Heritage College can incorporate ethical hacking.

3. The Hacker Hats

3.1. Black Hat Hacker

Black hat hackers are those hackers that tend to hack with malicious intent. They are often motivated by profit (Maurushat, 20) or provoking chaos. They are usually responsible for writing malware, a popular avenue for gaining access to machine (Norton Life Lock). Black hat hackers can range from novice to expert.

3.2. Grey Hat Hacker

A grey hat hacker typically does not have malicious intent or profit in mind when they hack. They might be hacking legally or illegally (Maurushat, 20). They are usually not authorized to perform penetration testing on a system by the system owner, but seek out exploits for various reasons, from making the internet more secure to just proving they can do it. A grey hat hacker may or may not disclose their discoveries to the system owner via responsible disclosure, but usually does not exploit the system for gain (Norton Life Lock). Responsible disclosure is the process of notifying a system owner of a vulnerability found in their system and not telling any other organization about the vulnerability until after a solution has been implemented. If an organization does not have a responsible disclosure policy in place it can be risky for a grey hat hacker to notify them as they could be punished (Detectify).

Grey Hat hackers may or may not include those hackers who hack nation states on behalf of their own nation state. It is debatable whether a grey hat hacker who hacks with good intentions is an ethical hacker.

3.3 White Hat Hacker

A white hat hacker is someone who hacks with the full permission of the system owner. They have no “criminal intention” and only seek renumerations. They abide by strict rules put in place by their clients and hack systems to find vulnerabilities before outsiders can or to suggest how the system can be made more robust (Maurushat, 20). White hat hackers can also use social engineering or gaining physical access to building as a means of penetration testing. (NEED REF)

4. Code of Ethics

One of the reasons it’s so difficult to define who is and who is not an ethical hacker is that there is no industry standard. Most hacking is in fact illegal, and as such there is no board for regulating Ethical

Hacking in Canada, nor to define a code of ethics. The laws surrounding hacking are broad to allow for prosecution when necessary (Maurushat, 301). Many attempts of creating a code of ethics (Johansen) or framework (Maurushat, 301) do exist, but they are fragmented and often come from a singular perspective.

5. History of Hacking

Hacking has been a phenomenon for as long as computers have existed. One of the first common hacks was called "Phreaking." Phreaking was the act of employing vulnerabilities in the phone networks to access resources the "phreakers" didn't have available to them, such as long-distance calls. They would use whistles or other mechanisms to copy the tones used in the network that allowed callers to connect to different regions. This was a well-known hack and was exploited by many (James).

As computers became more popular, the number of exploits grew in quantity and severity, especially at the inception of the world wide web. In the early 1990s (and even today), hacking was seen as purely criminal (James). With high profile hackers like Kevin Mitnick (first hacker to appear on an FBI most wanted poster) (TutorialsPoint)and Vladmir Levin (stole $10,000,000 from Citibank in 1994) (IT Pro Team) making headlines and not much spotlight on ethical hacking, it's easy to see why hacking was seen so negatively.

Although it was not always in the spotlight, ethical hacking has existed for as long as black hat hacking. Businesses and governments have always hired ethical hackers to test and protect their systems from malicious actors (James).

6. The Importance of Ethical Hacking

6.1. Security

Due to the inherently vulnerable position of organizations having an internet presence or protected data, they must protect themselves with all available means. Ethical hacking enables businesses and governments to stay one step ahead by attempting to secure exploits before they are discovered by criminal hackers (EC-Council). With the help of ethical hackers' organizations can improve security and shore up their defences (Johansen).

6.2. The Cost of a Hack

Getting hacked is expensive. The minimum cost, regardless of business size according to one source states that it is $200,000. This cost is minimal to some businesses but can put many small businesses out for good (Steinberg). By employing ethical hackers, a business can decrease their risk of being hacked by black hat hackers, reducing the cost to a bug bounty or the wage of an ethical hacker.

6.3. Improves Products for Users

Ethical hackers discover bugs and holes that put customers at risk. They are a unique type of tester that will help organizations discover fatal bugs and vulnerabilities because they tend to not follow the paths laid out by the designers of the system to perform testing. Ethical hackers help to build a better and more robust products for users by taking different path then the set use cases (Forbes Technology Council). They also help organizations to develop better practices and security by using social engineering and actual physical access to locations as a means of ethical hacking. (NEED REF)

7. The Steps of Ethical Hacking

When an ethical hacker is hired or attempting to gain access to system, they generally follow the methodology of a black hat hacker. There are many ways to plan and perform a hack, but generally most follow the following steps: information gathering, scanning, exploitation, maintaining access and/or cleanup (Engebretson, 19). Unlike black hat hackers, ethical hackers have one important preliminary step, they must limit themselves by the rules of their employer or create the rules if the employer has never hired an ethical hacker before.

7.1. Defining the Boundaries

When an ethical hacker is hacking under bug bounties, the rules are usually quite clear on what is and isn't allowed as the organization. Bug bounty platforms will usually not encourage social engineering or exploiting the system by physically accessing the business. When an organization is hiring a specific person or business to ethically hack them, they may have a different idea of how they should be hacked, or they may wish to test other vulnerabilities in their organization, such as their employees knowledge in phishing or the security of their buildings. An ethical hacker must ensure they spell out what they are and are not allowed to do before they start hacking so that they do their due diligence by their employer and contract (EC-Council).

7.2 Information Gathering

An ethical hacker must first research their client. They must discover the systems and technologies in use by their client (Grimes, 11-13). With this knowledge they can plan what attacks might work or where the vulnerabilities lie. There are many ways a hacker can do this: online research, various tools, and social engineering (Engebretson, 21). This knowledge allows hackers to identify possible avenues for access (Grimes, 11-13). Some experts would argue that this is the most import step, as the more a hacker researches the more likely they are to succeed in discovering an exploit (Engebretson, 20). A black hat hacker can use any means necessary to complete their information gathering because they do not have to follow any strict code of conduct, whereas a white hat hacker may be limited in what they can do. It is important that a white hat hacker follow the guidelines laid out by their employers or bounties and only target their employers' assets when testing security (Engebretson, 22).

7.3 Scanning

Sometimes scanning is recognized as a subset of information gathering. It is also known as finger printing (Grimes, 11). The hacker will attempt connecting with their target's machines using various tools. This will allow the hacker to see if they can communicate with the target's infrastructure "from the outside." Port scanning also happens at this time. A hacker will compile notes on any open ports on any of theirs target system that can be accessed externally. The hacker will also try to identify all the services and software their target uses. The hacker usually cannot attempt to exploit the vulnerabilities of third-party software but they should report on any known vulnerabilities to their employer that is caused by the third-party software (Engebretson, 55).

7.4 Exploitation

At this stage, an ethical hacker tries to execute their discovered vulnerabilities and exploit the system (Grimes, 13). This is the step that most people think of when they think of hackers. Few realize the work hackers must do before they are able to exploit a system. The hacker documents every vulnerability they were able to exploit, or what systems need work. Some exploits may lead to system take over and other less catastrophic exploits, lead to divulging protected information. In this step hackers can take several steps or perform any number of actions to gain control or access to their target's system (Engebretson, 79 - 80). Hackers will generally exploit a weakness in a system through its infrastructure, services, or applications. If they are allowed, they can also try to exploit the systems other weakness, the people behind the infrastructure via social engineering. These exploits will be discussed in the next section. It is not only important that an ethical hacker discover vulnerabilities, they should also disclose known solutions to their employer.

Common Vectors of Attack

Known Exploits

A lot of software and services used by organizations and businesses have well-known, documented exploits. These exploits are usually patched soon after they are discovered by the vendors, but many users do not keep up with the security updates. A hacker can determine if a system is using an unpatched software version and exploit the system via that avenue (Grimes, 14). These vulnerabilities can be devasting but are easy to fix when patches have been released.

Zero-days

Zero-days are bugs in a system that have yet to be discovered by owners of the system and is not known to the public. They are the most critical and severe as they can be exploited with the knowledge of the system owner. These exploits are particularly difficult to find (Grimes, 13). A system can never be deemed 100% secure, because a particularly clever hacker can one day discover a zero day (Engebretson, 193).

Physical access

Social Engineering

- Phishing
- Over the phone
- Exploiting humans (TutorialsPoint)

7. Career Paths in Ethical Hacking

7.1. Training

There are different directions one can take to become an ethical hacker. Courses and certifications are offered online and in school that allow individuals to obtain competencies – one that's hard to miss is the "Certified Ethical Hacker" certification offered by EC-Council. Another popular avenue is the self-taught path. There are many resources online and in books that allow any motivated individual to become adept in the trade.

7.2. Bug Bounties

Bug bounties are invitations by companies to either hack their system or test for vulnerabilities. It is important to note that bug bounties often have rules or guidelines on what some seeking to obtain a bounty can and cannot do. An ethical hacker must follow these rules. Not all companies offer bug bounties so it’s important to find out if they de before attempting to discover vulnerabilities. Compensation varies from company to company, usually depending on the severity of the vulnerability (Detectify). There are also platforms, such as HackerOne, which enable ethical hackers to easily find bug bounties.

7.3. Full Time Employee

Many businesses hire full time pen-testers, one example is IBM, who has regular postings on job boards. As well, there are many businesses who specialize in ethical hacking where they are hired by other businesses and organizations to perform ethical hacking on their systems, such as “Coalfire”.

6. The Problems Surrounding Ethical Hacking

6.1. Legality & Liability

As with any work in production environments, being an ethical hacker comes with great responsibility. Ethical hackers must ensure they perform their job with due diligence so that they don’t become liable for any issues they may cause when testing a system. This include ensuring they do not compromise the client’s system, or the data associated with the system. An ethical hacker who does endanger a client’s system by any means may be liable and can be sued by their client. Practicing due diligence and following the rules laid down by their client enables the ethical hacker to protect themselves in such legal cases (Johansen).

Ethical hackers are also at risk of being arrested and charged for doing their job. Before an ethical hacker performs any hacks on their employers’ systems, they must get a comprehensive list stating what they are and are not allowed to do on the system. They should also ensure that they have contacts that are aware when and where they are conducting their tests and that those contacts will be available if the ethical hacker needs a “get out of jail free card.” The importance of this can be shown by a case in the states where two ethical hackers were arrested and charged with burglary while testing the state of Iowa’s security. The charge was later downgraded to misdemeanour trespassing, but it remains on their records (Goodin).

6.2. Renumeration, or Lack Thereof

Considering qualified ethical hackers are extremely knowledgeable and skilled they can be relegated to bug bounties and that don’t pay enough for the work they do. Responding to bug bounties or performing ethical hacking is know quick job, as described in the steps to ethical hacking portion of this paper. Many bugs can take ethical hackers’ hours to research, resulting in bug that fetches them 50 to 100 dollars (Lu). If an ethical hacker goes the freelancer route it may be difficult for them to earn a living wage, especially in western countries (Winick)

8. Ethical Hacking and Heritage College

Systems are never perfect, but developers must strive to make their systems as secure as possible. As such, the Computer Science program at Heritage College has already integrated security into their program and the new program adds even more emphasis to security. The need for discovering bugs and vulnerabilities is great, and ethical hacking is one of the avenues for those discoveries. With the new program, ethical hacking is being taught in the 3rd year in the IT Security course. The Computer

Science program already sees the value added by educating their students in ethical hacking practices and as such it will not be impacted by the trend much.

9. Conclusion

Ethical hacking is a type of hacking that is performed by a hacker who has been hired by a system owner to hacker their system. Ethical hackers must follow the rules laid out by their employer, unlike black hat or grey hat hackers which can choose to exploit a system in any way they wish to. With those rules, there are still many means available to an ethical hacker to discover vulnerabilities. Ethical hacking has been a profession for as long as computers have existed. Ethical hacking enables the businesses to avoid being hacked by malicious actors which can be harmful to their customers, as well as costly to their reputation and finances. There are issues with becoming an ethical hacker surrounding legality, liability, and renumerations.

Students at Heritage College already learn about common exploits in multiple courses in the program, but they have little chance to see these exploits in action (this will change more in the new program). As developers we should all ensure we create and maintain secure systems that can withstand common exploits. Teachers could encourage or incentivise students in the Computer Science program to develop secure systems by allotting a certain amount of marks to security. If the teacher can penetrate their application using a common exploit, for example, cross-site scripting and SQL injection, the student will lose a portion of their marks for the security section.

Students should also be educated with the risks and liability that they take on when they perform ethical hacking. If the student is not diligent or their contract does not supply them with the necessary contacts to avoid arrest, they can be jeopardizing their future.

References

Detectify. *Guide to Responsible Disclosure and Bug Bounty*. 27 02 2017. 13 02 2020. <https://blog.detectify.com/2018/02/27/guide-responsible-disclosure/>.

EC-Council. 2020. 25 02 2020. <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>.

—. *Ethical Hackers: Get paid to break into computers*. 14 01 2020. 11 03 2020. <https://blog.eccouncil.org/ethical-hackers-get-paid-to-break-into-computers/>.

—. *What is Ethical Hacking?* 2020. 07 02 2020. <https://www.eccouncil.org/ethical-hacking/>.

Engebretson, Patrick. *Basics of Hacking and Penetration Testing : Ethical Hacking and Penetration Testing Made Easy*. Elsevier Science & Technology Books, 2013.

Forbes Technology Council. *Ethics And Hacking: What You Need To Know*. 06 03 2017. 09 02 2020. <https://www.forbes.com/sites/forbestechcouncil/2017/03/06/ethics-and-hacking-what-you-need-to-know/#10a4008d66d5>.

Goodin, Dan. *How a turf war and a botched contract landed 2 pentesters in Iowa jail*. 13 11 2019. 10 03 2020. <https://arstechnica.com/information-technology/2019/11/how-a-turf-war-and-a-botched-contract-landed-2-pentesters-in-iowa-jail/>.

Grimes, Roger A. *Hacking the Hacker - Learn From The Experts Who Take Down Hackers*. Wiley, 2017.

IT Pro Team. *The history of hacking*. 22 12 2017. 13 02 2020. <https://www.itpro.co.uk/security/innovation-at-work/30179/the-history-of-hacking>.

James, Mike. *A history of ethical hacking*. 29 08 2016. 09 02 2020. <https://staysafeonline.org/blog/history-ethical-hacking/>.

Johansen, Rowena. *Ethical Hacking Code of Ethics: Security, Risk & Issues*. 24 03 2017. 09 02 2020. <http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues>.

Knowles, Aidan. *How Black Hats and White Hats Collaborate to Be Successful*. 04 05 2016. 11 02 2020. <https://securityintelligence.com/how-black-hats-and-white-hats-collaborate-to-be-successful/>.

Lu, Donna. *When Ethical Hacking Can't Compete*. 08 12 2015. 11 02 2020. <https://www.theatlantic.com/technology/archive/2015/12/white-hat-ethical-hacking-cybersecurity/419355/>.

Maurushat, Alana. *Ethical Hacking*. University of Ottawa Press, 2019. <https://ruor.uottawa.ca/bitstream/10393/39080/1/9780776627922_WEB.pdf>.

Norton Life Lock. *What is the Difference Between Black, White and Grey Hat Hackers?* 2020. 09 02 2020. <https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html>.

Sharpe, Larry. *Ethical Hackers Are In Demand, And Here's How You Can Become One*. 29 02 2016. 11 03 2020. <https://www.huffingtonpost.in/larry-sharpe/ethical-hackers-a-growing_b_9304040.html>.

Steinberg, Scott. *Cyberattacks now cost companies $200,000 on average, putting many out of business*. 13 10 2019. 20 02 2020. <https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>.

TutorialsPoint. *Ethical Hacking Tutorial*. 2020. 13 02 2020. <https://www.tutorialspoint.com/ethical_hacking/index.htm>.

Winick, Erin. *Life as a bug bounty hunter: a struggle every day, just to get paid*. 23 08 2018. 25 02 2020. <https://www.technologyreview.com/s/611896/life-as-a-bug-bounty-hunter/>.