The Ethics of Hacking

Written by: Michelle R. Sellers

April 12, 2015

Abstract

This paper will explore the ethics of hacking. There are two main types of hacking, ethical hacking and unethical hacking. For the purposes of this paper I will attempt to explain the differences between the two and argue my viewpoints on the topic. I will support my arguments with valuable resources, and explain how the typical ethical theories pertain to this topic. I will follow with ways to prevent being a victim of the crime of hacking.

Table of Contents

Introduction 4

Literature Review 5

Discussion 6

Conclusion 11

References 12

The Ethics of Hacking

Hacking is defined as “any technical effort to manipulate the normal behavior of network connections and connected systems” (Mitchell). Hacking has been around for several years dating back into the 1800’s when the phone was first invented by Alexander Graham Bell. It wasn’t until the computer movement in the 80’s that hacking became popular. In 1986 Congress passed the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act which made hacking illegal.

Hacking in any form can be known as “the art of exploitation”. There are two very different types of hacking. There is ethical hacking, also known as “white hat hacking”, and unethical hacking, also known as “black hat hacking”. Below I will cover the definitions, the purposes, and a few differences that exist between these two types of hacking.

Ethical Hacking

By definition, ethical hacking is the legal act of systematically penetrating a computer system or network to find security vulnerabilities that could be exploited by an unethical hacker. The purpose of ethical hacking is usually for the good of the organization and is to find vulnerabilities before unethical hackers do. These vulnerabilities could be in software, firewalls, wireless networks, or just the network in general. The benefit of having an ethical hacker audit the security of a company’s network is to be able to fix vulnerabilities before they turn into a larger problem caused by an unethical hacker. The problem is that companies are now being held responsible for security breaches to customer data. A large scale breach could cause even

the largest of businesses to have to close their doors forever. Companies are better off being proactive rather than reactive.

Unethical Hacking

By definition unethical hacking is the illegal act of targeting a network or system to steal information, money, or to cause damage. Unethical hackers get enjoyment out of causing harm to systems and attempt to steal passwords and credit card information for personal gain. Some unethical hackers just want to see if they can get into a system and look around, while others try to unleash a virus with no financial gain only to cause significant damage to a company's network. Many unethical hackers like to do it only for status with other hackers, earning a name for themselves.

For the purposes of this paper, I will focus mainly on the topic of unethical hacking and explain my viewpoints on the subject. I will also attempt to associate the typical ethical theories and how they pertain to unethical hacking.

Literature Review

The Mentor (1986) wrote the Hackers Manifesto. This was a manifesto written from the mind of a hacker. It's become a very popular writing in the hacker world even nearly 30 years later. Reading this short writing by a former hacker can help someone to understand how a hacker thinks.

Discussion

For the purposes of this paper I will discuss the following theories and how they pertain to unethical hacking:

Consequentialism – Consequentialism is the theory that the consequence of the action makes the action or behavior good or bad. This theory has a small amount of truth to the unethical hacker. Some hackers actually like to be caught. They feel like it gives them some type of notoriety in the hacker realm. So, even though there is a consequence to their actions, they don't really fear the consequence, but more so look forward to it.

Utilitarianism – Utilitarianism is the theory that the right decision is the one that can cause the most happiness. Some hackers may lean towards this theory because they feel that in the long run everyone will be better off for their actions.

Deontological Ethical Theory – Deontological theory is the theory that focuses on rights, obligations, duties, and rules. This theory plays true for many hackers because they feel even though they know it is illegal that it is their obligation to hack a network. Some feel that they are doing a good thing by hacking a network because it will make a company harden their security.

Ethics of Caring – Ethics of Caring is the theory that involves caring for other individuals. This doesn't typically follow as a theory for the unethical hacker, more so the ethical hacker. I can see though, that sometimes hackers like to hack knowledge bases or government sites to make information available to the public. I could see how they might consider the fact that they care

about the people, so they make the information available to people because they feel they need to know or have a right to know everything.

Ethics of Justice – The ethics of justice are qualities of many theories which consist of impartiality and universality. I don't think hackers are concerned with this theory at all. There is no misconception that they should live up to the same standards that are held up for other people. If anything, they feel that they should do this type of work to hold other people accountable for their actions.

Contractarianism – Contractarianism is the theory that involves coming together for a mutual benefit. The person under this theory is able to act for their own self-interests while acting for the public good. The hacker may consider themselves working under this theory also. They think differently than the average person and just because it's illegal don't mean it's bad if it is going to help the general public open their eyes to whatever they feel they need to know.

Virtue Theory – Virtue theory is the theory that focuses on the greater good. I don't feel that this theory pertains to the hacker at all.

Cultural Relativism – Cultural Relativism is the theory that that there is no valid rational criterion for determining the right thing to do. I don't feel that this theory pertains to the hacker really. Hackers do have their own culture, but their culture is within a larger culture that is still expected to adhere to the norms of the public.

Divine Command Theory – The Divine Command Theory is the theory that an action is good because God commands it. This theory definitely doesn't play a part in the mind of a hacker. I have never heard of a hacker that compromises a network because God told him to do it.

Of all the theories I think the strongest theories that could hold true for the unethical hacker is the Consequentialism Theory and Deontological Theory. I feel that hackers enjoy the consequences of their actions and I think they feel it is their right or obligation to do what they do.

This raises the question of whether or not hacking should be illegal. There are currently many laws against the unauthorized access of computer systems, most vary by state. In my opinion, there can sometimes be a fine line between whether it should be illegal or not. I think for hackers that have the intent of acting maliciously it should definitely be illegal, but for hackers that just want to see if they can get in to a network, I don't feel it should be illegal as long as they don't cause any harm. I do feel though that if a hacker contacted my office to tell me they have breached our network I would have a different feeling about it. It seems that it's different when it happens in your territory. I would feel violated, but would also do everything I can to make sure the hole is sealed up to prevent it from happening again.

As a society we see hacking as bad. If we asked a normal person on the street they would tell us that it's bad. Hackers have been seen in a bad light. Most people don't realize there are good hackers and bad hackers; they just see hacking in general as bad.

Hacking Prevention

To avoid being a potential target of attack for a hacker there are several steps that should be followed.

1. Only enter personal data on sites that use the https extension. These sites are more secure and encrypt data that goes through the internet.
2. Keep your computers and servers updated with the latest updates. Updates provided by software companies and manufacturers can contain fixes to security problems that exist in the software or on your system. Applying these updates can improve your security and keep hackers out.
3. Put a piece of tape over your webcam. Hackers are now able to activate your webcam remotely and use information they are able to see against you.
4. Use anonymous browsing. Many web browsers now offer the option of anonymous browsing so no one can see where you have been. This can be helpful to prevent hackers from being able to log in as you on the sites you have been to.
5. Get rid of unnecessary software. It's difficult enough to apply upgrades and fixes to the necessary software on your system. Keep it to a minimum. If you don't need the software, get rid of it so you don't have to worry about keeping it secure.
6. Use a firewall to prevent unauthorized entry into your system.
7. Secure your router. Don't just take your router out of the box and assume it's secure. Make sure to change the default passwords and require authentication to be able to connect to it.

8. Use secure passwords. Don't use real words, don't use numbers of significance, and change your passwords regularly. The most secure passwords are at least 8 characters long, contain special characters, upper case and lower case letters, and numbers.
9. Use caution opening emails or downloading anything from the internet. Don't open any emails from anyone that you don't know, or download software from sites that you think may not be secure.
10. Use antivirus software to protect your system and make sure to keep it up to date with the latest spyware definitions.

Although these are all great steps to help secure your network and to avoid being the target of a hacker, none of these are foolproof. You still need to remain diligent at keeping your information secure and always think twice about what you do on the internet. It's always best to think that someone can see everything you're doing and that you're not safe.

Conclusion

Hacking isn't going to stop anytime soon, we can only attempt to prevent it from happening to us. A skilled hacker will always find a way to do what they do best and usually doesn't care about the consequences of their actions. To quote a passage from The Mentor (1986), "You may stop this individual, but you can't stop us all" (The Conscience of a Hacker, para. 11). This still stands true even though it was written back in 1986. No matter how much the government tries to step in, there is no way to stop them all.

References

Brinkman, B., & Sanders, A. F. (2013). Ethics in a Computing Culture. Boston, MA: Cengage Learning

Mitchell, B. (n.d.). *What is a Hacker?* Retrieved from http://compnetworking.about.com/od/networksecurityprivacy/f/what-is-hacking.htm

Devitt, M. (2001). A Brief History of Computer Hacking. *Dynamic Chiropractic. Vol.19, Issue 13.* Retrieved from www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078.

The Mentor. (Jan. 1986). The Conscience of a Hacker. *The Hackers Manifesto.* Retrieved from http://phrack.org/issues/7/3.html

Jin. (Apr., 2014). Difference between Ethical Hacking and Non Ethical Hacking. *Researchopedia.* http://researchpedia.info/difference-between-ethical-hacking-and-non-ethical-hacking/

Author Unknown. (n.d.). Unethical Hack. *Computer Hope.* Retrieved from http://www.computerhope.com/jargon/u/unethical-hack.htm

Rouse, M. (n.d.). Ethical Hacker. Retrieved from http://searchsecurity.techtarget.com/definition/ethical-hacker

Author Unknown. (Jun. 2014). Computer Crime Statuses. *National Conference of State Legislatures.* Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

O'Toole, J. (Jun. 2014). Simple Tips to Avoid Getting Hacked. *CNN Money.* Retrieved from http://money.cnn.com/2014/06/13/technology/security/dont-get-hacked/

Author Unknown. (n.d.). Hacking Attacks – Prevention. Retrieved from http://www.crucialp.com/resources/tutorials/website-web-page-site-optimization/hacking-attacks-prevention/

Author Unknown. (n.d.). Tips for Creating a Strong Password. *Microsoft.* Retrieved from http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password