Penetration Testing:

Why it is Important and How Society Deals with Cyber Security

Ethen Brandenburg

Old Dominion University

IDS 200: Interdisciplinary Theory and Concepts

Professor Oliver

August 6, 2022

Abstract

Penetration testing is rapidly becoming more and more a major part of cyber security and has been growing exponentially within the past few years. Every device from cell phones and TVs, to now smart watches and even homes are becoming connected to the internet. The risk of intruders or hackers has risen dramatically, and along with it the need for cybersecurity professionals: most especially penetration testing or ethical hackers. Throughout this paper, the reader will see what exactly ethical hacking is and why it is important, as well as why it is now increasingly more important for simple cyber security skills to be taught in schools. The paper will also touch on how society interacts and deals with ethical and unethical hackers.

The interdisciplinary theory is a fancy term for a topic intertwining with a few different and various topics. For instance, baking can be a science of cooking, but it can also be interlaced with psychology and society. For the psychology discipline, an example could be that certain people only like vanilla cakes while others like chocolate. There is actually a science behind it all. Society discipline could be like people being influenced to eat at a certain bakery because one might support a political group that another bakery does not. Interdisciplinary theory can be applied to many different topics- pretty much any topic you can think of. In my case, I will apply this theory to the topic of penetration testing, or ethical hacking, and compare it to three different disciplines: education, technology, and society.

Penetration testing, or ethical hacking, is a very important cyber security role and can be made of many different tasks. For instance, some of the ethical hacking tasks would consist of scanning and analyzing computer systems and networks. Along with scanning the systems, they see how they can get into a system, and if there is a vulnerability, they help create a patch for that weakness. Ethical hacking has been around for many years, and it even existed before it was made a “real” role for professionals in the way we know it to be today. Hacking itself has been around for many years, and it originally existed in the form of viruses, or at least that's what was first recognized by frequent internet users. These malicious attacks slowly evolved into what we refer to today as hacking. Hacking usually consists of someone on the outside trying to steal sensitive information and would sell that information or do worse things with it. Some of these breaches result in identity theft, or in even worse cases they can use ransomware to encrypt one's data and force them to pay for access. Ethical hackers, on the other hand, are cyber security professionals who stress test computer systems and see where an unethical hacker can break in and steal information.

When it comes to education, the people of society are no strangers. But internet education is something that most people are not familiar with, or at least significantly less so. Most are certainly not informed enough on the dangers of the internet to the degree that they should be. Internet education- or education about safe practices on the internet- is not a new concept, but it really has not grown past very simple practices. Most of the concepts that are taught in school about the internet are to create “strong” passwords and not go on “bad” websites. Schools should really show kids how to identify malicious emails, websites, and downloads and how to steer clear of them, as well as why they should steer clear. With this knowledge, teens, or really people of any age, could be more vigilant when they browse the internet late at night, instead of being as vulnerable as they tend to be now. (Rahman N. A. A, et al., 2020) This, however, is where the skill and expertise required for penetration testing come into play. One of the main purposes, as well as the most important, of an ethical hacker, is to help prevent many of these dangers from infiltrating the private lives of people through technology. In doing so, they can make up for some of the lack of preparedness and information among the majority of internet users.

Cyber security education does not have to stop in school. It should be taught to people throughout their lives. Now, some people do not even realize that companies are slowly trying to teach people how to live safer lives, such as telling them how to create a good password in terms of length requirements and different alphanumerical requirements. (Muhlenberg College, 2022) These simple practices are slowly teaching the average person how to live a slightly safer life when perusing the internet, and in doing so it will make their lives outside the internet easier and safer as well. But that is only one part of the equation, as there is more going on in the background with how those policies work and why we use them. Penetration testers are the big player in creating those password requirements, along with other safe practice policies that are trying to make the world a safer place one rule at a time.

Ethical hackers are known by many different names, such as Pen Testers, White Hat Hackers, and Red Teaming just to name a few. (Engebretson & Kennedy, 2013) You may not know it, but ethical hackers keep your information safe from day to day. They work for many services that people use every day such as social media or the infotainment system services in your own home; all of those frequently used systems are being protected by ethical hackers. In society, ethical hackers should be considered the “good guys” but in reality, there is a big controversy concerning whether or not they are really ethical. The biggest problem that people have with ethical hackers is that there's no saying, so far as the general public knows, what happens during a test. (Jamil, D., Numan, M., & Khan, A, 2011) For example, there's no saying what the tester actually does because testers cover their tracks, as they should. A tester, for all they know, could be a malicious hacker that wants to get into a system, and the way he might see fit to do that would be to get a job as a pen tester.

Society views hacking in general as a bad thing to do, but in reality, it is just the unethical hackers who have “brainwashed” everyone into thinking that. In fact, for the longest time, I personally thought hackers were terrible and illegal. Until one day, I came across an article that talked about a penetration tester and what he did to keep the world safe. That article changed my view on hacking and enlightened me on how certain cybersecurity policies were invented and evolved over time. Anytime people hear of the word hacker or even google the word hacker, you see articles about people stealing your information and that is really only one side of the story. Social engineering is what hackers even apply to make people afraid of hackers and that's how they can steal your information. (Jaquet-Chiffelle & Loi, 1970) Black hat hackers, or unethical hackers, use this fear and anxiety to make people vulnerable and they eventually spit out their passwords mainly by using phishing emails or malicious websites. However, just like with many other things, the skills required to hack can just as well be used for good purposes as they can for bad. There are many different social views that one could take with ethical hacking and I have only just covered a few very briefly.

The main difference between ethical hackers and unethical hackers is that ethical hackers work for an accredited company, and they always write a contract of services. For instance, before an ethical hacker even starts to think about accessing a company's network, they work out a bill of services and write out a written contract. Ethical hackers also have an ethics code book, just like doctors who take oaths for saving lives and not take them. Ethical hackers “take an oath”, and they do not touch a company's system before permission is given. Unethical hackers do not ask permission and do not ever have a written contract with the company or person they are hacking. (Jaquet-Chiffelle & Loi, 1970) They disregard all ethical decisions and just take what they want and do what they want with one’s own computers. Ethical hackers protect and attack for the purpose of protection, while unethical hackers attack with ill intent. An ethical hacker uses the hackers' own skills against them. In short, an “ethical hacker” is a professional and legitimate occupation today, for which some people even go to school. While that might be difficult for some individuals to grasp, it remains to be true, as well as necessary.

Technology is where an ethical hacker or really any type of hacker shines. In this day of technology, there are so many different tools and technologies available for hacking, both ethically and unethically. A very well-known tool, and even here at Old Dominion University, teaches students how to use it is called Metasploit Framework. Metasploit is a tool library that is designed by ethical hackers and houses the most well-known vulnerabilities, allowing you to test systems with them. Metasploit has the ability to scan a single computer or a whole network for large-scale systems and report data back in a very simple, easily understandable format. Along with scanning, it also can open backdoors into computers using vulnerabilities that have been exploited in past systems. With that knowledge, ethical hackers can fix the vulnerability and “seal” that backdoor.

Along with a big framework, ethical hackers can use the CVE database, which is where all the known exploits are logged. This database can show ethical hackers what breaches are possible with certain ports and services being open and running on a computer or network. (*CVE* 2022) Just like Metasploit, ethical hackers can use a tool called John the Ripper, which is an open-source computer program that is used for breaking passwords. This is one of the tools that help create the password requirements for companies as they know what type of passwords take the longest to crack open. Another great technology that is available for ethical hackers is WireShark. WireShark is a network analyzing tool that captures anything and everything that passes through a network, from website domains to packet protocols. Anyone on the network can see what anyone is doing and what traffic is coming in and going out. This tool is great for finding malicious software that is logging your information out to another computer somewhere in the world. Ethical hackers touch on so many parts of computer systems and most people are not even aware. For instance, they are often testing common applications like Facebook and Google for vulnerabilities in order to protect their users. Both are sites that are used by millions every single day, and there's a great deal that can occur without proper supervision, guidelines, and people who know to keep criminal-minded hackers from doing what they intend.

Ethical hacking or just any hacking has been frowned upon by most people because they have no idea what it really entails. Just like some news stories where you only get one side of the story at first and then when you hear the other side it completely changes the whole story, ethical hacking is just like that. Ethical hacking has been thrown in the same pot as hacking and it really is not hacking in the way we think of it. Most people think hacking is just a person wanting to steal their information and sell it online but that's just one side of it. Hacking can be used for good and it can be used for bad, just like anything in this world. I like to think of ethical hacking as a helping hand for companies who had previous cyberthreat trouble. Kind of like when a child falls and scrapes their knees they always run to an adult for help, ethical hackers are just like the helping adult.

Cybersecurity, and especially ethical hacking, is an essential backbone of this present-day society and touches on the disciplines of technology and education as well. Humans had to learn to navigate oceans, roads, and outer space. Technology and the internet have both joined that list, and ethical hacking plays and will continue to play a central role. As the world becomes increasingly more dependent upon the internet, it will continue to evolve for the better, but the areas of danger will evolve as well. That said, internet education will need to evolve among the general public as well as those interested in digitally-based careers. With technology constantly evolving and changing, so will ethical hacking-especially with the recent addition of AI technology. With hope, ethical hackers will evolve to become more powerful than their competition. Ethical hacking is just one of the many impactful cyber security jobs that can touch numerous different disciplines, stretching beyond disciplines such as political science and psychology. Though all of what I have mentioned has already grown and evolved rapidly, one could say this is only the beginning.

Works Cited:

Engebretson, P., & Kennedy, D. (2013). *The basics of hacking and penetration testing: Ethical hacking and Penetration Testing Made Easy*. Syngress/Elsevier.

Jamil, D., Numan, M., & Khan, A. (2011). *IS ETHICAL HACKING ETHICAL?* http://digitalmediafys.pbworks.com/w/file/fetch/60359759/JamilD2011EthicalHacking.pdf

(2020). *The Importance of Cybersecurity Education in School* [Review of *The Importance of Cybersecurity Education in School*]. Semanticscholar.org. https://pdfs.semanticscholar.org/f24d/d9d57c7c3c4a14cedfd4eb38073b78124d96.pdf

Guidelines for strong passwords. Muhlenberg College. (n.d.). Retrieved August 3, 2022, from https://www.muhlenberg.edu/offices/oit/about/policies_procedures/strong-passwords.html

Jaquet-Chiffelle, D.-O., & Loi, M. (1970, January 1). *Ethical and unethical hacking*. SpringerLink. Retrieved August 3, 2022, from https://link.springer.com/chapter/10.1007/978-3-030-29053-5_9

CVE. (n.d.). Retrieved August 3, 2022, from https://cve.mitre.org/