TOPIC: Ethical Hacking & Penetration Testing

CYSE 250

Cybersecurity

Madelene McFarlane

UIN: #01096496

Abstract

The world today is more reliant on technology more then ever before. From users' main source of entertainment to the ways that hospitals store personal information society has moved to technology. As technology grows and advances so do the threats against it. Black-hat hackers and other types of threats grow to the shaping technology in order to breach private data and use it for their own gain. In order for security to stay one step ahead of black-hat hackers they must think like hackers. Reason for the introduction of white-hat hackers and prevention testing in order to prevent and advance the systems that keep society turning.

Keywords: Threats, black-hat, white-hat, prevention testing

Introduction

The growth of technology has impacted society in many different ways. These ways expanding the ability of companies to grow and people to connect with one another. However, this growth has also affected crime and the level of security needed to keep these networks safe. As cybercrime increases so do the efforts in order to create preventative and combative ways of protections to networks and individual devices.

The starting point of any type of prevention system is to understand what exactly the prevention is aimed at. In the case of cybersecurity black-hat hackers are one of the main sources of motivation for prevention systems. Therefore, to truly understand black-hat hackers the prevention must stem from their point of view. In order to achieve this the birth of white-hat hackers raised up in the cybersecurity community.

White-hat hackers were introduced to the system in order to have a better understanding as to why and how black-hat hackers were able to perform their attacks. By performing what is known as 'ethical hacking' these white-hat hackers assume the role of the black-hat hackers in a network. The ethical hackers then hacking their way into the network by use of the threats that lay in the network. The process showing the vulnerabilities that are hiding within the network and the measures that then should be implemented to safeguard the network within the white hat hacking operation.

Ethical hacking provides benefits to a variety of networks. Big name organizations, small business, family homes, and individual devices all have found growth from the introduction of ethical hacking. Networks all can be upgraded to something more powerful and secure with the help of knowing how a black-hat hacker infiltrates a device or a network system. This knowledge has been the blueprint of software that is available to the everyday person in order to create a more secure network. Some software examples being *Norton* and *Malwarebytes* that are very common in every family home network.

While *Norton* and *Malwarebytes* are extremely helpful pieces of software to networks. They are not the only sources of advancements that ethical hacking has provided the cybersecurity field. Cybercrime is constantly evolving along with technology therefore the advancements are growing as well. White-hat hacking serves as the bridge between the systems being created and the evolving black-hat hackers' methods of attacking growing networks. This ethical hacking providing the needed groundwork to create the needed security measures for an ever-changing environment.

Types of 'Hats' Hackers

Within the topic of ethical hacking and prevention testing it is important to understand the different roles, hats, of hackers. The main two types of hackers being white-hat and black-hat hackers. Though there is actually a grand total amount of six different types of hackers. Aside from white and black-hat hackers there is also grey, blue, green, and red-hat hackers.

White-hat hackers are often times referred to as the 'good guys' of the hacker community. They provide their skills in order to analyze a system to be able to identify possible vulnerabilities that are open to attacks. As well as providing possible solutions that the system can implement to safeguard these vulnerabilities if not cover them completely. White-hat hackers go through with this process in an ethical and legal manner thus giving these professionals the name ethical hackers.

On the opposite end black-hat hackers are on the other end of the moral spectrum than the white-hat hackers. Black-hat hackers can be looked at as the attackers that will exploit the vulnerabilities in a system. With these attacks the black-hat hackers will then use the data in some way that benefits them directly. This form of hacking is of course always done illegally and or unethically.

White and black-hat hackers being looked at as the 'good' and the 'bad' hats of hacking. Where grey-hat hackers are the combination of the two. They do not usually steal or cause harm to a system or network. However, they do take unethical measure to reach the system and offer help to secure the system better for a fee. Grey-hat hackers along with white and black-hat hackers being the most common out of the six variations.

The remaining three types of hackers being red, blue, and green-hat hackers. Red-hat hackers being good, but in a bad way. Using illegal or unethical methods to take down bad hackers. Then blue-hat hackers have two forms. One being that of revenge seekers who are not caring much about materiel gain, but that of causing harm to deemed enemies. The second form of blue-hat hackers being outside security professionals. This form of hacker being hired to perform penetration testing on companies' new software. Finally, there is green-hat hackers. Green-hat hackers are new to the world of hacking and these hackers are often times unaware as to the laws of hacking and may cause damage that they did not mean to inflict. Nor understand the methods to fix the damage that they have caused.

Penetration Testing

As mentioned previously penetration testing goes hand in hand with that of ethical hacking. Penetration testing allow systems to strengthen themselves through the ability of seeking ways in and out of the network. Although penetration testing is often referred to in a solid term there is two types of penetration testing.

The two types of penetration testing being:

- External penetration testing- The main goal of external penetration testing is to seek out vulnerabilities in a system that potential attackers could exploit by the use of a public network. These public networks being networks that are used by applications or websites.
- Internal penetration testing- The main goal of internal penetration testing is to look over internal networks and find hidden vulnerabilities that could be potential exploited within the network by other malicious members of said network. These malicious members possibly containing employees or business partners that have access.

In combination these two methods of penetration testing prove to help systems security. When penetration testing is being preformed before areas of a network need to be looked over for signs of vulnerability. Then once the vulnerability is located solutions can they be provided in order to prevent malicious attacks. This testing keeping user's ability to stay ahead of those with malicious intent before they are able to launch an attack.

Penetration Testing Combined with Ethical Hacking

The development with penetration testing along with ethical hacking has implements many advancements for cybersecurity. Both of these methods help systems able to identify their weaknesses and gain solutions to improve. These two terms often being used interchangeably due to their close nature. However, there are some key differences that make the two different. These differences leading to a powerful combination between the two.

Where a tester may excel an ethical hacker might fall behind and vice versa. Some good examples of this are that testers are not required to write a very detailed report of the test. They are given the ability to be more relaxed within their report writing. Where an ethical hacker needs to be an expert of report writing. This difference is due to the skill level needed to be a tester versus an ethical hacker. Another key difference between the two is that penetration testing is far faster then compared to that of ethical hacking. Penetration testing is just as the name implies running a test in order to see where things go wrong, and vulnerabilities arise and then the work is over. The next part being that of finding a solution for the problems and weaknesses that are found during the test which sometimes may fall onto the tester but is not certain to also be included in the title. However, with ethical hacking there is a lot of time, effort, and skill need in comparison to that of a penetration tester. Within ethical hacking there is a much deeper understanding and search within a network or system to locate vulnerabilities and potential threats that may occur. Thus, this resulting in a lot more time and energy required in order to provide the proper service.

Despite the differences that penetration testing, and ethical hacking may have they combined force remains and excellent tool for cybersecurity advancement. Both methods being involved with proactive cybersecurity practices and requiring permission from the network in order to test. These methods allow a system to prevent an attack from occurring in the first place instead of dealing with an attack while or after the attack has occurred. Within the field of cybersecurity proactive practice is the best approach in avoiding attacks and damage to a systems network.

Benefits of Proactive Cybersecurity

While there are other measures of proactive cybersecurity the main two leading the way are ethical hackers and penetration testers. Proactive cybersecurity refers to protective measures that are being developed and implemented before any sort of attack or breach occurs. The reasoning for proactive cybersecurity is that it is much safer and somewhat easier to prevent something bad from happening then to repair the damages if possible after an attack. A more common comparison that can be used is that of a safety belt in a car. It is much safe to wear a safety belt while driving in case of a possible accident then to not wear one and suffer the consequences or possible violations of not wearing a safety belt.

A team that is constantly reacting to threats and attacks will become drained. This is because if a system is constantly under attack that means the team is jumping from one chaos to another. Leading to burn out of the team. Where preventing potential attacks would mean more planning and preparing then having to practically jump from attack to attack. Another team benefit to proactive cybersecurity is that it builds team compliance. Within the many layers of defense, understanding the risks, and engaging in risk analysis builds a compliance framework. This framework requires a set level of security measures which a team is more likely to meet with compliance guidelines.

Proactive cybersecurity also has many internal benefits as well. A baseline example of this is that due to the internal work that has to be done within the system the team is more likely to notice mistakes that are made. With reactive security the focus is placed on the problem at hand and there is little time to instead look at the system itself for possible other mistakes. Where with proactive measures these mistakes can be caught, and the focus can then be moved in the infrastructure.

Another internal benefit is that proactive practices can catch malicious inside jobs within an organization. Reactive measures are focused more so on external sources. Where proactive practices could catch an attack that stems from the inside of the network. By means of considering the possibilities of inside attack and monitoring for suspicious activity before the activity turns in to an attack.

Proactive security is sometimes even more important than reactive security. While both are need in any cybersecurity network proactive measures are needed for a variety of benefits for a system. These benefits also branching out to the team members and their workload due to the number of attacks that can be stopped before they even have the chance to start. Proactive security can stem from many different practices from just training and education of employees. To hiring ethical hacker and running penetration testing to find vulnerabilities in a system before users with malicious intent do.

Conclusion

Society is now more dependent on technology more then ever. The growth of the internet and networks has been a great success and has helped many people in many different ways. Though comes progress comes complications and this example being no exemption. As technology continues to grow so does the community that uses technology in illicit manners for their own gain. These malicious users finding new ways to exploit vulnerabilities and attack networks as fast as technology continues to grow.

These malicious users being the inspiration for proactive cybersecurity practices such as penetration testing and ethical hacking. Penetration testing containing two different types of tests, external and internal testing. These tests are put into place to run and find vulnerabilities in a system or network to be able to point out what might be exploited in an attack. Similarly ethical hackers are after the same goal. Though instead of just finding the vulnerabilities they are also doing a more in-depth search of the network as well as the physical system set in place. Then once vulnerabilities are found the white-hat hackers then come up with solutions in order to build a more solid infrastructure.

Many benefits come out of proactive cybersecurity measures. Proactive practices are needed just as much if not more then reactive measures in a system. These practices allow for organizations to catch up with cyber criminals and try to stay one step ahead of them in order to protect their system. Along with limiting the workload of their employees to avoid burnout and possibly stopping an inside job that may be developing within their own network.

Society is ever growing just like technology. New additions to the way of life are being implemented every day and with that comes possible new methods of danger and crime. As technology continues to grow so does cybersecurity. With proactive security measures can be taken so that way attacks are less likely to occur. Teams can continue to look forward instead of backtracking and looking behind them.

Reference

1) Hartley, R., Medlin, D., & Houlik, Z. (2017). *Ethical hacking: Educating future cybersecurity ... - ISCAP*. Ethical Hacking: Educating Future Cybersecurity Professionals. Retrieved January 25, 2022, from http://proc.iscap.info/2017/pdf/4341.pdf

2) Jagnarine, A. A. (2005, August 24). The Role of White Hat Hackers in Information Security. Retrieved January 25, 2022, from https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1012&context=honorscollege_theses

3) Juneja, G. (2013, December). *Ethical hacking: A technique to enhance information security*. ETHICAL HACKING: A TECHNIQUE TO ENHANCE INFORMATION SECURITY. Retrieved January 25, 2022, from http://www.ijirset.com/upload/2013/december/62_ETHICAL.pdf

4) Kumar, P., & K., P. (2021, April). *A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime*. A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime . Retrieved January 25, 2022, from http://www.jctjournal.com/gallery/16-april2021.pdf

5) M. Ashraf, A. Zahra, M. Asif, M. B. Ahmad and S. Zafar, "Ethical Hacking Methodologies: A Comparative Analysis," 2021 Mohammad Ali Jinnah University International Conference on Computing (MAJICC), 2021, pp. 1-5, doi: 10.1109/MAJICC53071.2021.9526243.

6) S., A., & K., T. (2018). *A brief information of ethical hacking - AIJR*. A brief information of ethical hacking. Retrieved January 25, 2022, from https://books.aijr.org/index.php/press/catalog/download/8/3/92-1?inline=1

7) Sigwadi, W. (2016, October 28). *The adoption and use of ethical hacking to secure information in small companies*. Academia.edu. Retrieved January 25, 2022, from https://www.academia.edu/29496652/THE_ADOPTION_AND_USE_OF_ETHICAL_HACKING_TO_SECURE_INFORMATION_IN_SMALL_COMPANIES

8) Sinha, Shivanshi and Arora, Dr. Yojna, Ethical Hacking:The Story of a White Hat Hacker (2020). International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN: 2347-5552, Volume-8, Issue-3, May 2020 , Available at SSRN: https://ssrn.com/abstract=3670801 or http://dx.doi.org/10.2139/ssrn.3670801