Name: Tay Lamell
Date: November 24, 2024

Ethical Hacking

BLUF

Ethical hacking can play a crucial role in the protection of sensitive information both for organizations and the individuals they serve. It requires a strong ethical foundation, and the trust of all parties involved in order to be successful.

Introduction

Ethical hacking, sometimes also known as “white hat hacking,” refers to the practice of organizations hiring someone with the explicit purpose of infiltrating their cybersecurity systems. Utilizing methods similar to those of malicious hackers, the goal of white hat hackers is to find weaknesses in the organization’s defenses and advise them on how they can be corrected. Unlike malicious hackers, an ethical hacker’s only goal is to audit the system and protect the information of everyone involved. They do not set out to steal the information that they come across, nor do they seek to cause damage to the companies that are hiring them.

Ethical Neutrality

Another difference between ethical and malicious hackers, is that ethical hackers follow a strict ethical code. Their code is so strict, in fact, that organizations like the International Council of E-Commerce Consultants have even published said code in written format. Included in their moral code is the need for permission from the company before commencing the hack, adhering to legal methods during the hack, and maintaining the confidentiality of whatever they come

across. The last portion of the code is what specifically ties white hat hacking to the idea of ethical neutrality.

Where the term ethical neutrality refers to the idea that ethical standards must be adhered to when conducting research, as mentioned in their code, white hat hackers strive to do the same. The very nature of their work means that ethical hackers are faced with highly sensitive and classified information on a daily basis, and doing so requires the utmost trust between client and hacker that said information won't be used for anything nefarious. This trust is so crucial that IBM has maintained a refusal to hire ex-hackers to audit their systems for fear that they may be tempted to revert to old ways.

The CIA Triad

Similarly, the idea of a solid ethical foundation ties into another keystone in the world of cybersecurity: that of the CIA triad. Standing for confidentiality, integrity, and availability, ethical hackers are tasked with all three aspects of the triad each time they take a job. There needs to be an established belief that the hacker will maintain the confidentiality of their findings before they're even given the job. While the probing of the security system is testing the integrity of the defenses, when a white hat hacker shares their findings and how to improve upon weaknesses with their client, this is done with the intent to maintain the availability of said information going forward.

Social Engineering and the Cyber Criminal Subculture

Ultimately, the existence of ethical hacking entails the existence of malicious or “black hat hacking”, a subculture in the cybercriminal world. Because some white hat hackers are ex-malicious hackers, the knowledge and connection that they have with technology follows them from one side of the ethical fence to the other. Where social engineering is concerned, the main applicable are the concept of information gathering and the execution of the hack itself. However, as previously mentioned, where black hat hackers would infiltrate a system with the intent of using their findings for personal gain, white hat hackers conduct their hacks without the intent to cause harm in any way. That they’re auditing these systems is itself a testament to their work in preventing malicious social engineering from taking place.

Ethical Hacking in Society

Beyond merely auditing the cyber defense of an organization, ethical hacking can also be used to impact society in other ways. Through the use of open-source intelligence (OSINT), ethical hacking has been able to aid in the solving of missing persons cases and the protection of children’s rights online. Organizations such as the BADASS Army and Stop the Traffik even utilize OSINT to combat revenge porn and human trafficking. OSINT enables ethical hackers to do three main things: discover public-facing assets, discover information outside of the organization, and collect and combine said information into actionable intelligence. It has even allowed for early public health warnings to be delivered.

Conclusion

If the best offense is truly a good defense, then ethical hacking is one of the best offenses around. The job done by ethical hackers helps organizations keep up to speed on how to combat

potential threats to their system, which in turn helps buff up their protections of sensitive client information. Successful implementation of ethical hacking can help prevent crises like the recent data breach at Insomniac Games that saw the personal information of current and past employees, along with years worth of company planning, leaked onto the Internet for all to see.

References

Cybersecurity ethics: What cyber professionals need to know. (2023, August 21). Cybersecurity Ethics: What Cyber Professionals Need to Know. https://www.augusta.edu/online/blog/cybersecurity-ethics

Dincelli, E., Craig, V. S., & Yayla, A. (2023). Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools. *Communications of the Association for Information Systems, 53*, 1052-1071. https://doi.org/10.17705/1CAIS.05345

Gandhi, F., Pansaniya, D., & Naik, S. (2022). Ethical Hacking: Types of Hackers, Cyber Attacks and Security. *International Research Journal of Innovations in Engineering and Technology, 6*(1), 28-32. https://doi.org/10.47001/IRJIET/2022.601007

Gatlan, S. (2024, February 23). *Insomniac Games alerts employees hit by ransomware data breach*. BleepingComputer.

https://www.bleepingcomputer.com/news/security/insomniac-games-alerts-employees-hit-by-ransomware-data-breach/

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal, 40*(3), 769-780. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/ethical-hacking/docview/222417938/se-2

What is Ethical Hacking? (2024, August 29). *Ibm.com*. https://www.ibm.com/topics/ethical-hacking