Ethical Hacking

Jerome Z. Cunningham

Rutgers University

Ethical Challenges in Public Affairs

20:834:515:01

May 04, 2023

Ethical Hacking

1. Introduction

The cybersecurity industry would be significantly hampered without the technique of ethical hacking. It aids businesses in pinpointing security holes in their infrastructure so they may fortify themselves against cyberattacks. Concerns regarding the security of computer systems and networks have arisen in response to the advent of cyberterrorism and the increasing frequency of terrorist acts. Ethical hacking has become an option for warding off these kinds of assaults. Ethical hacking aims to improve the security of online systems and networks by locating and fixing any flaws discovered in the system. This paper will explain how ethical hacking can help stop terrorist attacks and cyberattacks.

2. Overview of the Certified Ethical Hacker Credential

The Certified Ethical Hacker (CEH) credential is recognized as the gold standard for ethical hackers, as conferred by the EC-Council or International Council of Electronic Commerce Consultants. According to Baloch (2017), individuals who earn the CEH credential have demonstrated a comprehensive understanding of the legal and ethical aspects and the methods, tools, and techniques of ethical hacking. Shimonski (2016) reports that ethical hackers can earn many credentials, including the Certified Information Systems Security Professional (CISSP) and the Offensive Security Certified Professional (OSCP) certificates, in addition to the ubiquitous CEH. These credentials vary in their prerequisites and areas of study, but they all share an emphasis on ethical hacking. Shimonski (2016) notes that while ethical hacking is a valuable technique, it must be carried out per all applicable laws and regulations. Ethical hackers must follow strict principles to ensure their hacking is legal and beneficial (Shimonski, 2016). They must also consider the lawfulness of their acts and avoid infringing any regulations.

Before attacking a system or network, an ethical hacker should always ask the administrator for permission. As noted by Wang and Yang (2017), the scope and parameters of the authorized hacking activity must be specified in writing. This way, the system or network is protected from potential harm, and the ethical hacker does not violate any laws. After gaining access, ethical hackers must use their expertise and abilities to mimic an attack on the system or network (Wang & Yang, 2017). Several methods for scanning the system for security flaws may be necessary. Wang and Yang (2017) note that a report detailing their findings must be provided to the network or system owner by ethical hackers. The information should focus on describing the vulnerabilities in-depth and offering solutions.

3. Adhering to Legal and Ethical Principals

In addition to engaging in ethical hacking practices, professionals in this field must also avoid breaking the law. Harper et al. (2022) assert that as part of this, hackers must refrain from violating the privacy of others, stealing or damaging data, or sharing any sensitive information found through hacking. Ethical hackers must follow all privacy and data protection laws and regulations. Various certifications and guidelines are available to ensure that ethical hackers adhere to the highest ethical and legal standards (Harper et al., 2022). The EC-Council, for instance, offers a Code of Ethics for ethical hackers that details the moral and legal guidelines they should adhere to. Professional accountability, confidentiality, and privacy are only a few of the ethical issues addressed in the CEH certification's ethics module.

Ethical hacking aims to find security flaws in a system or network without causing harm to it. According to Grimes (2017), the motivation behind a hacking endeavor is the defining characteristic of whether it is ethical or harmful. The goal of ethical hackers is to assist businesses in finding and fixing security flaws before criminals exploit them (Grimes, 2017).

Ethical hackers work to strengthen the defenses of computer systems and networks. It is now more important than ever to ensure that computers and networks are safe, considering the prevalence of cybercriminals. Grimes (2017) reports that professional "white hat" hackers can find security flaws in a system and advise businesses on how to solve them. Exposing security holes in networks and systems is another driving force behind ethical hacking. Manjikian (2022) notes that institutions like banks and government agencies that handle sensitive information may benefit significantly from this. Ethical hackers help businesses and government agencies improve their cyber security by pointing out weak spots in their defenses.

4. Methods of Ethical Hacking

Ethical hackers have several methods to locate security holes, such as social engineering, penetration testing, and vulnerability scanning. Manjikian (2022) asserts that social engineering aims to get victims to provide sensitive information, including login credentials, while penetration testing is trying to get into a system or network by finding and using its flaws. On the other hand, vulnerability scanning entails scanning the web with software to look for security flaws (Manjikian, 2022). In addition to these skills, ethical hackers must follow a rigid set of moral guidelines. The organization being tested must consent, and the testers must not hurt the company or its customers. They must also be trustworthy and discreet when reporting risks to the proper authorities. Ethical hacking is gaining prominence as businesses embrace digital solutions (Manjikian, 2022). With the increasing number of cyber threats, companies must proactively discover and fix security holes in their infrastructure.

5. Benefits of Ethical Hacking

Ethical hacking is advantageous since it can help businesses save money and time in the long term. Sahu and Acharya (2020) note organizations can save money by preventing data

breaches and other security events by finding and fixing vulnerabilities before an attack happens. That may also aid in shielding the company from negative publicity and legal or regulatory action. Ethical hacking is also helpful since it may ensure businesses adhere to all applicable rules and laws (Sahu & Acharya, 2020). Regulations and contractual responsibilities place unique security requirements on companies across several sectors. According to Sahu and Acharya (2020), businesses can benefit from the expertise of ethical hackers to guarantee that their security procedures are adequate.

7. Challenges of Ethical Hacking

However, there are obstacles to overcome in the field of ethical hacking. Keeping up with the ever-changing nature of threats is a significant obstacle (Yaacoub et al., 2021). To stay ahead of the game, ethical hackers must constantly adapt and enhance their methods in response to the ever-evolving strategies used by cybercriminals to exploit vulnerabilities.

Another difficulty is that even ethical hackers can sometimes unintentionally compromise the systems they are trying to evaluate. Yaacoub et al. (2021) report that an ethical hacker may crash a system or otherwise interfere with its normal functioning, even if they have the best intentions. Ethical hackers must, therefore, be thoroughly familiar with the systems they are examining and take adequate measures to avoid unexpected outcomes (Yaacoub et al., 2021). Ethical hackers must also balance security and usability (Grimes, 2017). Users may become frustrated and less productive if security measures make accessing necessary resources harder. Therefore, ethical hackers must engage closely with stakeholders to guarantee that security measures are implemented to balance security and usability requirements.

There is also the possibility of internal pushback against ethical hackers. The results of an ethical hacker's investigation may be taken seriously by only some parties involved (Grimes,

2017). Effective communication about the significance of their job and the value of their testing is essential for ethical hackers. Furthermore, Manjikian (2022) suggests that technical expertise in computer systems and networks is necessary for ethical hacking. That calls for continuous learning and education to meet evolving industry standards. Strong problem-solving skills and the ability to think imaginatively are also essential for ethical hackers (Manjikian, 2022). Despite these obstacles, ethical hacking has the potential to be a highly lucrative career path. Ethical hackers may substantially impact enterprises' security posture when protecting sensitive data and critical infrastructure from cyber threats. Ethical hacking can also be lucrative due to the enormous demand for qualified professionals from businesses worldwide.

8. Ethical Hacking Blocks

The five blocks of ethical hacking, which are surveillance, maintaining access, scanning, enumeration, gaining access, and clearing tracks, provide a framework for ethical hacking.

I. The Reconnaissance Phase

In the reconnaissance stage of ethical hacking, hackers learn as much as possible about the system or network they are trying to break into. Gandhi et al. (2022) note that a comprehensive map of the target's infrastructure, OS, services, and ports may be constructed after gathering this data. This map will pinpoint potential entry points or flaws as the hacking progresses (Gandhi et al., 2022). Without actively engaging with the target system or network, a passive survey gathers information from publicly available sources. According to Gandhi et al. (2022), researching a firm involves looking at its online presence, including its website, social media pages, public records, and job listings. Adversaries can use this data to learn about a company's internal workings, technology, and security holes (Shimonski, 2016). Conversely, active reconnaissance methods require direct interaction with the target system or network to

obtain intelligence. That encompasses service discovery, network mapping, and port scanning (Sahu & Acharya, 2020). Port scanning searches for open ports and the services used on a remote machine or network.

Shimonski (2016) notes that the target system network architecture is mapped out in detail, including where and what kind of devices are connected, using a process known as "network mapping." For example, web servers, email servers, and database servers are services that might be identified on a target system. By the end of the reconnaissance phase, the attacker will know everything there is to know about the target system or network and can begin looking for weaknesses and devising an attack strategy (Sahu & Acharya, 2020). Before doing any surveillance or other hacking tactics, ethical hackers are required to seek authorization from the target organization. That is done to ensure the hacking stays within the bounds of the law and ethics. Ethical hacking is not a one-and-done activity but rather an ongoing process. Organizations must continually identify and address system and network vulnerabilities (Shimonski, 2016). One technique to ensure the efficacy of the organization's security measures is regular penetration testing, which involves simulating attacks to uncover weaknesses.

II. Maintaining Access

The next stage for an attacker after gaining initial access is to stay logged into the system and create a permanent foothold in the network. The intruder wants to prevent any detection or lockout of their access to the system. According to Wallingford et al. (2019), backdoors, which are secret entryways that an attacker can use to circumvent security measures and acquire access to the system later, are one method of preserving access. Installing programs or altering configuration files are only two examples of how backdoors can be made (Wallingford et al., 2019). They can also be made to launch a remote shell, granting the attacker remote access to the

machine. One typical method attackers use to keep access is the establishment of hidden channels (Wallingford et al., 2019). A covert channel is a means of communication that cannot be detected by conventional means of surveillance. That is possible through encrypted communication or the concealment of contact within benign-looking traffic.

The intruder can also make it easier for themselves to acquire access in the future by creating new user accounts, changing permissions, and turning off security measures. As Harper et al. (2022) noted, an attacker can gain complete control of a system and access all its data by making new accounts with administrative capabilities. It can be more straightforward for an attacker to gain unauthorized access to a plan by modifying permissions and turning off security safeguards. Harper et al. (2022) suggest that keeping the hacker logged in is vital because it allows them to gather data, issue commands, and otherwise manipulate the system. Ethical hackers should follow ethical and legal rules to ensure hacking is done ethically and get permission from the target entity before attempting to maintain access to the system.

III. Scanning and Enumeration

When conducting penetration testing or ethical hacking, scanning and listing are crucial in discovering vulnerabilities and misconfigurations that hackers could exploit. According to Wang and Yang (2017), information on the targeted system or network is gathered through automated and human methods. Port scanning is one of the most popular methods of scanning and enumeration. Scanning for accessible ports, services, and protocols is what port scanning is all about (Wang & Yang, 2017). Using this data, we may estimate the target's attack surface and locate possible entry points. Network mapping is another method used in scanning and enumeration. Wang and Yang (2017) assert that to "map" a network is to record its topology and catalog all of the nodes that make up the network. Tools like Zenmap are helpful because they

reveal the network's IP addresses and ranges. Security analysts can benefit from thoroughly understanding the network topology by creating a system map.

Scanning for vulnerabilities is another vital part of the scanning and enumeration process. Baloch (2017) reports that automated vulnerability detection technologies like Nessus or OpenVAS are used in vulnerability scanning. In addition to software flaws, misconfigurations, and weak passwords, these programs can detect various other security issues. Additionally, scanning and enumeration employ "banner grabbing" to learn as much as possible about the target system (Baloch, 2017). Checking the system's banners and messages upon connection is the first step. The OS, web server, and other services installed on the target system can be determined using this data. As noted by Baloch (2017), sniffing is another method for scanning and enumeration. Credentials such as user names and passwords can be uncovered by intercepting and analyzing network data. Network traffic can be captured and analyzed with tools like Wireshark, which can then be used to locate security flaws in the underlying infrastructure.

IV. Gaining Access

One of the first things an attacker does is gain access to the system or network they intend to attack. Manjikian (2022) suggests that this can be done in several ways, such as by taking advantage of bugs in software or sloppiness on the user's part—for instance, password cracking, in which specialized tools are used to guess or brute-force the system. A user or administrator account is one of the most prevalent tactics attackers employ (Manjikian, 2022). Attackers also utilize buffer overflow attacks, which use a security hole to overwrite the program's allotted memory to gain entry (Yaacoub et al., 2021). An attacker can exploit this to access the system or network by injecting malicious code. Yaacoub et al. (2021) allude that attackers also employ SQL injection to breach databases by exploiting security holes in web

applications. An attacker can access private data or manipulate a database by inserting malicious SQL code into a web form.

Besides technical vulnerabilities, attackers frequently utilize social engineering to breach security. According to Yaacoub et al. (2021), that includes persuading users to disclose or install malicious software on their computers through social engineering or other psychological manipulation. Attackers can also utilize exploit frameworks like Metasploit to automate breaking into systems or networks (Sahu & Acharya, 2020). The weaknesses in systems and networks can be exploited due to the tools and use these frameworks provide. Sahu and Acharya (2020) report that an attacker might take complete control by elevating their privileges after infiltrating a system or network. They can then launch more sophisticated attacks, such as the theft of confidential information, the installation of malicious software, or the disruption of regular networks or system functioning.

Security logs and event monitoring are valuable tools for spotting intrusions. According to Sahu and Acharya (2020), these solutions facilitate the rapid identification of malicious network activities by alerting security personnel in real-time. Wallingford et al. (2019) suggest that organizations can benefit from regular security assessments and penetration testing in identifying and fixing vulnerabilities that attackers could use to compromise their systems and networks. In addition to taking technical precautions, businesses should train staff on proper data security procedures (Wallingford et al., 2019). That includes education on the significance of strong passwords, not disclosing confidential information to unauthorized parties, and instruction on spotting and reporting suspicious activity.

V. Clearing Tracks

For the hacker, clearing their digital footprint is crucial in protecting their anonymity and evading authorities. Gandhi et al. (2022) note that several steps ensure no evidence of the attempted hack remains in the system. That may involve obfuscating communication lines, encrypting data in transit, or erasing log files. Deleting log files is a typical practice for erasing digital footprints. The activities of a computer system, such as login attempts, system events, and network traffic, are recorded in log files (Wallingford et al., 2019). The intruder can hide their tracks by wiping these files from the machine. However, the absence of log files can raise red flags for system managers; therefore, this approach has risks. Changing the system files is another way to erase traces (Gandhi et al., 2022). To hide their footprints, attackers can tamper with system files by altering the file's date to make it look like it was not read during the attack.

Tracking can also be hidden via encryption. Manjikian (2022) reports that when an attacker uses encryption, they can hide their communication channels from system administrators. In addition, data transmissions can be encrypted, making them difficult to decipher and detect. Removing tracks is not an ironclad guarantee (Manjikian, 2022). There are still indicators of an assault that system administrators can look for, such as a change in file size or network traffic.

Furthermore, the attacker may leave insidious remnants—such as backdoors or rootkits—that grant them continued access to the compromised system (Grimes, 2017). Thus, it is preferable to concentrate on avoiding hacks rather than removing trails. According to Wang and Yang (2017), firewalls, intrusion detection systems, and data encryption are security measures businesses may use to safeguard their systems. They can also perform routine security audits to find and patch security holes before exploiting them (Grimes, 2017). Personal measures against

hackers include using robust and unique passwords, avoiding questionable emails and websites, and installing all available software updates.

9. Conclusion

In conclusion, I believe hacking can be a valuable tool in the fight against terrorist acts of all kinds, including cyber ones. However, ethical hackers must adhere to specific rules, certifications, and limits and conduct all ethical hacking per applicable ethical and legal norms. Furthermore, one can weigh the merits and downsides of ethical hacking regarding responsibility, openness, and efficiency by looking at real-world examples. Finally, the ethical hacking framework provided by the five pillars can be used to enhance the safety of computer systems and networks.

References

Baloch, R. (2017). *Ethical hacking and penetration testing guide*. CRC Press.

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.

Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. John Wiley & Sons.

Harper, A., Linn, R., Sims, S., Baucom, M., Fernandez, D., Tejeda, H., & Frost, M. (2022). *Gray hat hacking: the ethical hacker's handbook*. McGraw-Hill Education.

Manjikian, M. (2022). *Cybersecurity ethics: an introduction*. Taylor & Francis.

Sahu, P. K., & Acharya, B. (2020). A Review Paper on Ethical Hacking. *Technology*, *11*(12), 163-168.

Shimonski, R. (2016). *CEH v9: Certified Ethical Hacker Version 9 Study Guide*. John Wiley & Sons.

Wallingford, J., Peshwa, M., & Kelly, D. (2019). Towards understanding the value of ethical hacking. In *International Conference on Cyber Warfare and Security* (pp. 639-XIV). Academic Conferences International Limited.

Wang, Y., & Yang, J. (2017). Ethical hacking and network defense: choose your best network vulnerability scanning tool. In *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 110-113). IEEE.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A survey on ethical hacking: issues and challenges. *arXiv preprint arXiv:2103.15072*.