IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

Overview, Issued and Implication of Ethical Hacking

Tanmay R. Sukhadeve
Dr. Ambedkar Institute of Management Studies and Research, Deekshabhoomi, Nagpur, India
tanmaysukhadeve2002@gmail.com

Abstract: *With the increasing use of technology, cybersecurity has become a critical issue for individuals, businesses, and governments. Ethical hacking, also known as white hat hacking, is a practice that seeks to identify vulnerabilities in computer systems and networks to help protect against malicious attacks. However, ethical hacking raises ethical issues, such as privacy concerns and the potential for unintended consequences. This paper provides an overview of ethical hacking, its benefits, and ethical considerations.*

Keywords: Hacking

I. INTRODUCTION

As technology continues to advance, cybersecurity has become an increasingly important issue for individuals, businesses, and governments. Cyber attacks, such as malware, phishing, and ransomware, have become more sophisticated and widespread, causing significant damage to individuals and organizations. Ethical hacking is a practice that seeks to identify and remediate vulnerabilities in computer systems and networks to help protect against these attacks. However, ethical hacking raises ethical issues, such as privacy concerns and the potential for unintended consequences.

Background:

Ethical hacking is the practice of using hacking techniques to identify vulnerabilities in computer systems and networks. Ethical hackers, also known as white hat hackers, are hired by organizations to identify and remediate vulnerabilities before they can be exploited by malicious actors. Ethical hacking can be conducted using a variety of techniques, including penetration testing, vulnerability scanning, and social engineering.

Certified Ethical Hacker (CEH):

Certified Ethical Hacker (CEH) is a qualification given by EC-Council and obtained by demonstrating knowledge of assessing the security of computer systems by looking for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system. This knowledge is assessed by answering multiple choice questions regarding various ethical hacking techniques and tools. The code for the CEH exam is 312-50. This certification has now been made a baseline with a progression to the CEH (Practical), launched in March 2018, a test of penetration testing skills in a lab environment where the candidate must demonstrate the ability to apply techniques and use penetration testing tools to compromise various simulated systems within a virtual environment.

Certified Ethical Hacker(CEH)
Issuing Organization EC-Council
Validity Duration 3 Years
Subject
Focus Ethical Hacking
Requirements
Two Years Of Experience
Type Multiple Choice
Duration 4 Hours

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

Relations
Certified Ethical Hacker (Practical)

Ethical hackers are employed by organizations to penetrate networks and computer systems with the purpose of finding and fixing security vulnerabilities. The EC-Council offers another certification, known as Certified Network Defense Architect (CNDA). This certification is designed for United States Government agencies and is available only to members of selected agencies including some private government contractors, primarily in compliance to DOD Directive 8570.01-M.[1] It is also ANSI accredited and is recognized as a GCHQ Certified Training (GCT).

Examination:

Certification is achieved by taking the CEH examination after having either attended training at an Accredited Training Center (ATC),[2] or completed through EC-Council's learning portal, iClass. If a candidate opts to self-study, an application must be filled out and proof submitted of two years of relevant information security work experience. Those without the required two years of information security related work experience can request consideration of educational background.[3] The current version of the CEH is V12, released in September 2022.[4] The exam, which uses the same EC-Council exam code (312-50) as the earlier versions, has 125 multiple-choice questions and a 4-hour time limit.[5][6]

The EC-Council and various ATCs administer the CEH examination.
Members holding the CEH/CNDA designation (as well as other EC-Council certifications) must seek re-certification under this program every three years, for a minimum of 120 credits

Benefits of Ethical Hacking:

- Ethical hacking provides several benefits for organizations, including:
- Identifying vulnerabilities before they can be exploited by malicious actors.
- Helping organizations meet compliance requirements.
- Improving the overall security posture of an organization.
- Reducing the risk of data breaches and other cybersecurity incidents.

Ethical Considerations:

Despite the benefits of ethical hacking, there are several ethical considerations that must be taken into account. Some of the key ethical issues associated with ethical hacking include:

- Privacy concerns: Ethical hackers may have access to sensitive data during their testing, which raises concerns about privacy and confidentiality.
- Consent: Organizations must obtain the consent of all parties involved in ethical hacking, including employees and customers.
- Unintended consequences: Ethical hacking can sometimes lead to unintended consequences, such as system downtime or data loss.
- Legal considerations: Ethical hacking must comply with all relevant laws and regulations, including those related to data privacy and intellectual property.

II. CONCLUSION

Ethical hacking is a critical practice for organizations looking to protect against cyber attacks. While ethical hacking provides several benefits, it also raises ethical concerns that must be addressed. Organizations must take a thoughtful and responsible approach to ethical hacking, ensuring that all ethical considerations are taken into account throughout the process. By doing so, organizations can improve their security posture while also upholding their ethical responsibilities.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, June 2023

REFERENCES

[1]. Certified Ethical Hacker - Wikipedia
[2]. What is Ethical Hacking? - Types, Meaning of Ethical Hacking (intellipaat.com)
[3]. Introduction to Ethical Hacking - GeeksforGeeks