JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ETHICAL HACKING, TECHNIQUES, AND ITS SOCIAL ASPECTS

Prof. K. P. Raghuwanshi
Jay Karmale, Sanskruti Benodkar, Sejal Devikar, Rutika Jirapure
Department of MCA
Vidya Bharati Mahavidyalaya Amravati

Abstract: Ethical hacking, also known as white-hat hacking, is a proactive cybersecurity practice that identifies and mitigates weaknesses in networks, systems, and applications. It involves gathering information, conducting security testing, controlled exploitation, and social engineering using specialized tools. By integrating these methods, organizations can enhance their defenses and reduce cyber risks.

Index Terms: Ethical Hacking, Hackers, Security Testing, Security Tools, Cybersecurity.

I. Introduction

Ethical hacking evaluates systems for security vulnerabilities by exploiting known weaknesses and utilizing social engineering techniques. Network penetration testing may also assess physical security, such as access controls. This process emphasizes detecting and resolving vulnerabilities rather than predicting the intent of attackers. Promptly addressing weaknesses ensures systems remain secure and resilient.

II. Background

Cyberattacks are often driven by financial gain, a desire for competitive advantage, personal revenge, or political motives. The leaked Eternal Blue exploit, developed by the NSA, demonstrates the dangers of mishandled vulnerabilities. This case underscores the importance of responsible vulnerability management and careful use of offensive security tools.

1. Threats of Ethical Hacking:

Despite its advantages, ethical hacking carries risks such as misuse of skills by unethical individuals, exposure of sensitive information, high costs, and legal issues if performed without proper authorization. Over-dependence on ethical hackers can also reduce regular security practices.

2. Benefits of Ethical Hacking:

Ethical hacking improves security by preventing cyberattacks, data breaches, and financial losses. It ensures compliance with legal standards, builds customer trust, and promotes awareness about safe digital practices while also creating opportunities in the cybersecurity field.

3. Purposes of Ethical Hacking:

The main purpose of ethical hacking is to identify and fix security weaknesses in computer systems, networks, and applications before malicious hackers can exploit them. It helps organizations protect sensitive data, maintain trust, and ensure the smooth functioning of digital services.

III. Types of Ethical Hacking:

1. **White Hat Hackers (Ethical Hackers):** Authorized professionals hired by companies to test and secure systems. They break into their own networks to identify vulnerabilities and protect against cyber threats.
2. **Black Hat Hackers (Crackers or Malicious Hackers):** These hackers have malicious intentions, breaking into systems to cause harm, steal data, or disrupt operations for personal gain. They engage in illegal activities, such as defacing websites or cracking passwords.

3. Grey Hat Hackers: These hackers fall between White and Black Hats. While they may exploit system vulnerabilities without permission, they typically do not have malicious intent. Grey Hat Hackers might identify security flaws and report them to the organization, sometimes in exchange for a reward. However, their actions are still technically illegal since they break into systems without authorization.

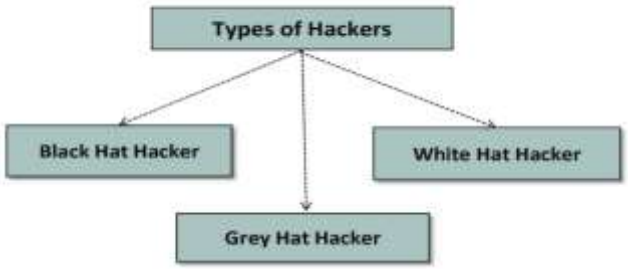

Fig. 1 types of hackers

IV. Ethical Hacking in Various Domains:

Ethical hackers assess various systems to identify vulnerabilities before attackers exploit them:

1. **Web Applications:** Detect issues like SQL injection and XSS to secure websites and online services.
2. **Network Security:** Test routers, firewalls, and other infrastructure for misconfigurations and exposed services.
3. **Wireless Networks:** Identify weak encryption, rogue access points, and insecure authentication.
4. **Social Engineering:** Simulate phishing and other attacks to measure staff susceptibility.
5. **Mobile Applications:** Find flaws in data storage, session handling, and API security.
6. **Cloud Services:** Check configurations and access controls for exposure risks.
7. **IoT Devices:** Inspect connected devices for weak firmware, default credentials, and privacy leaks.

By covering these areas, ethical hackers help organizations minimize attack surfaces and protect systems, networks, and applications.

V. Ethical Hacking Techniques and Technology:

Techniques:

Network Scanning: Maps hosts, open ports, and services to find entry points.

1. **Enumeration:** Gathers detailed system information like usernames and shared resources.
2. **Packet Sniffing:** Captures network traffic to detect sensitive data or misconfigurations.
3. **Social Engineering:** Exploits human behaviours to gain unauthorized access.
4. **Vulnerability Scanning:** Uses automated tools to identify flaws and insecure setups.
5. **OSINT(Open Source Intelligence):** Gathering and analysing information from publicly available sources.
6. **Log Analysis**: identify security threats, track unauthorized activity, and piece together the timeline of a security incident.

These approaches, combined with thorough testing practices, enable organizations to identify realistic threats and provide practical recommendations to enhance security.

Fig. 2 ethical hacking technique

VI. Technology :

1. **Firewalls:** Filter network traffic to block unauthorized access.
2. **IDS/IPS:** Detect anomalies and prevent attacks in real time.
3. **Encryption:** Secures data by converting it into an unreadable form.
4. **VAPT:** Identifies and tests system weaknesses to strengthen security.
5. **SIEM:** Collects and analyzes security events to detect threats and respond promptly.

6. **Methodologies of Ethical Hacking:**
7. **Reconnaissance:** Gather information about the target passively or actively.
8. **Scanning:** Identify vulnerabilities using tools such as Nmap or Nessus.
9. **Gaining Access:** Exploit weaknesses via SQL injection, password attacks, or other methods.
10. **Maintaining Access:** Remain undetected using backdoors or rootkits.
11. **Analysis & Reporting:** Document findings, exploit vulnerabilities, and recommend remedies

Fig. 3 ethical hacking methodology

12. **Social Impact of Ethical Hacking:** Ethical hacking significantly influences society. While it strengthens security, it also introduces ethical and operational concerns.
13. **Impact on Education:**

Teaching hacking carries the risk of misuse. Institutions should implement strict screening, emphasize ethics, and require certifications to promote responsible use.

14. **Impact on Business:**

As organizations rely on digital systems, ethical hackers protect sensitive data. However, their privileged access demands strong ethical standards and trust.

15. Impact on Workplace and Security:

Ethical hackers often access employee records and internal systems. Effective monitoring is essential to prevent misuse.

16. Impact on Technology:

Tools used for security testing are also available to malicious actors. Organizations and individuals—not tool creators—must ensure their responsible use.

17. Impact on Confidential Information:

Ethical hackers handle sensitive data in critical sectors. This access, though necessary, raises trust and misuse concerns.

VII. Conclusions and Future Work:

Ethical hacking is essential for fighting cyber threats. Increased collaboration between research and industry can boost the real-world use of academic security tools. Future efforts should focus on improving existing tools, integrating them into security operations, and using large language models to improve penetration testing. These actions will build trust, promote ethics, and strengthen cybersecurity resilience.

VIII. Reference:

1. Gurpreet K. Juneja, "Ethical hacking: A technique to enhance information security" *International Journal of Computer Applications* (3297:2007), vol. 2, Issue 12, December.
2. Ajinkya A. Farsole, Amurta G. Kashikar, and Apurva Zunzunwala, "Ethical Hacking", *International Journal of Computer Applications (0975-8887)*, Vol. 1 No. 10, pp. 14–20, 2010.
3. *What is Ethical Hacking*: [Online]. Available: https://www.eccouncil.org/ethical-hacking, Accessed 16 June 2021.
4. Bhawana Sahare, Ankit Naik, Shashikala Khandey, "Study of Ethical Hacking", *International Journal of Computer Science Trends and Technology (IJCST)* - Volume 2 Issue 4, Nov-Dec 2014.
5. Important Benefits of Ethical Hacking, *Cybersecurity Certification Course*, edureka, Nov 17, 2020.
6. *Ethical Hacking - Hacker Types*, https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_hacker_types.htm
7. C. M. Rakshitha, "Scope and Limitations of Ethical Hacking and Information Security", *Electronics and Sustainable Communication Systems 2020 International Conference on*, page number 613–618, 2020.
8. Modesti, P., Golightly, L., Holmes, L., Opara, C., & Moscini, M. (2024). *Bridging the Gap: A Survey and Classification of Research-Informed Ethical Hacking Tools*.
9. Asif, F., Sohail, F., Butt, Z. H., Nasir, F., & Asgar, N. (2024). *Ethical Hacking and Its Role in Cybersecurity: A Comprehensive Review*.
10. Georg, T., Burmeister, O., & Low, G. (2018). *Issues of Implied Trust in Ethical Hacking*. *ORBIT Journal*, 2(1), Article 77.
11. Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2023). *Ethical Hacking for IoT: Security Issues, Challenges, Solutions, and Recommendations*. *Internet of Things and Cyber-Physical Systems*, 1(4), 100024.
12. Asif, F., Sohail, F., Butt, Z. H., Nasir, F., & Asgar, N. (2024). *Ethical Hacking and Its Role in Cybersecurity: A Comprehensive Review*. arXiv preprint arXiv:2408.16033.
13. Modesti, P., Golightly, L., Holmes, L., Opara, C., & Moscini, M. (2024). *Bridging the Gap: A Survey and Classification of Research-Informed Ethical Hacking Tools*. *Journal of Cybersecurity and Privacy*, 4(3), 410–448.
14. 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.

15. Ahila, S., Raj, A., Prabhu, G., & Kumar, V. V. N. (2019). *Ethical Hacking Techniques with Penetration Testing*. *International Journal of Engineering Research & Technology (IJERT)*, 7(11), 1–5.

16. Azhar Ushmani. " Ethical Hacking" Research Gate IJIT - Volume issue 6, Nov-Dec 2018

17. Dr. Suneel Pappala, Dr. Kanigiri Suresh ITFMR" - Volume 7 Issue 2, March-April 2025.

18. K.S. Bala Chowdappa, S. Subba Lakshmi, Prov. S. Pavan Kumar "ITCSIT" Vol 5(3) Research Paper,2014