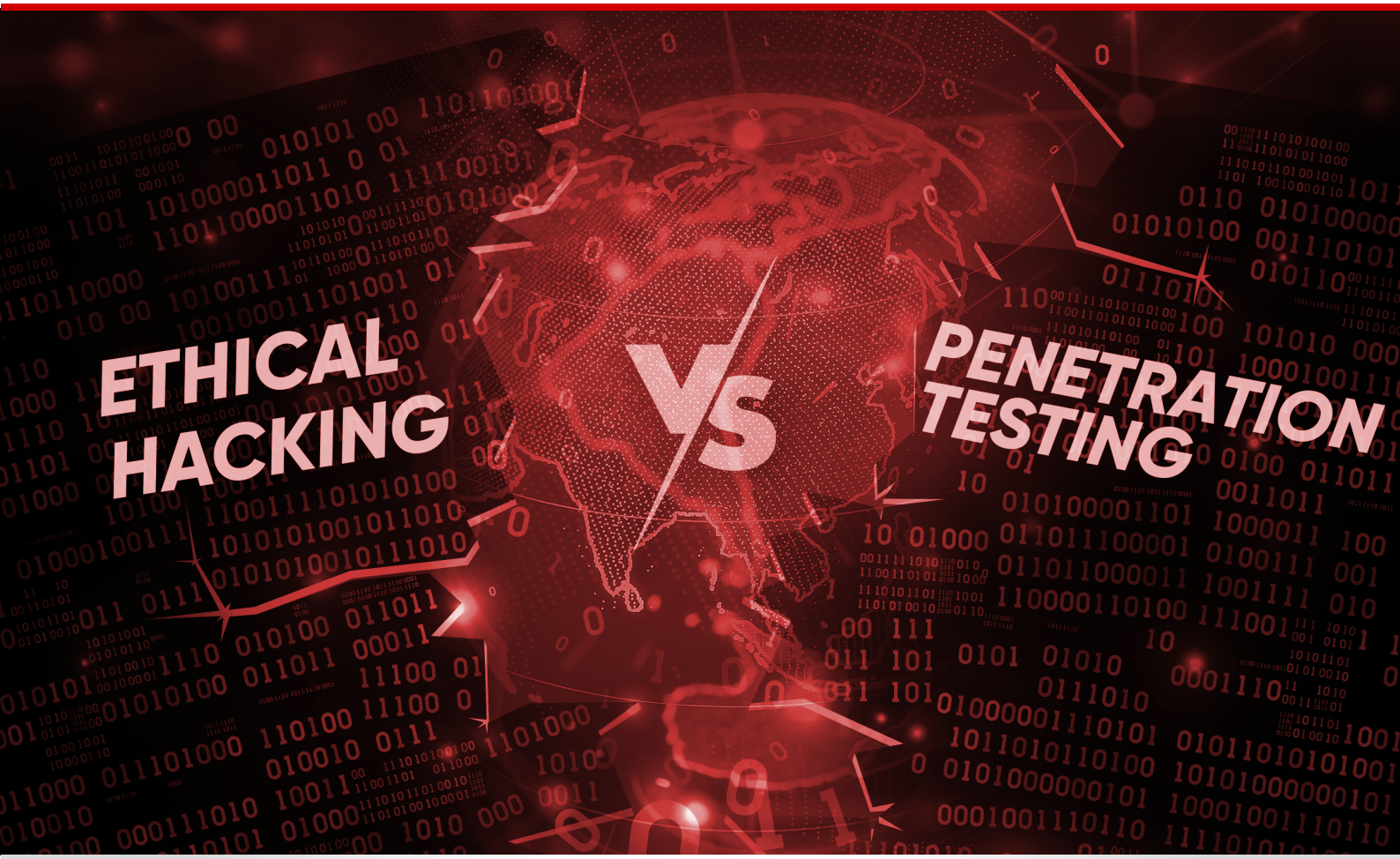
CISO MAG

beyond cybersecurity



WHITEPAPER

Ethical Hacking vs. Penetration Testing: Unraveling the Distinctions for Effective Cybersecurity Strategies

Authored by:
Jagdish Mohite,
OSCP, OSWP, CRTP, CISSP, CISA, CEH, CHFI, PMP

Abstract

This thought leadership white paper delves into the key differences between ethical hacking and penetration testing (penetration testing) in the realm of cybersecurity. It explores the distinct methodologies, objectives, and scopes of these two crucial security practices. By examining the unique purposes, techniques, and legal considerations associated with each approach, this white paper provides valuable insights to help organizations and professionals understand the nuances and make informed decisions regarding their cybersecurity strategies. Gain a comprehensive understanding of ethical hacking and penetration testing and leverage this knowledge to strengthen your organization's security posture.

Contents

Introduction

Ethical hacking and penetration testing are cybersecurity practices to identify vulnerabilities and weaknesses in computer systems, networks, and applications. These practices are conducted with the permission of the system owners to ensure the security and integrity of their digital assets. Ethical hacking, also known as white hat hacking or penetration testing, involves simulating real-world cyber attacks on systems to uncover potential security flaws. Ethical hackers use similar techniques and tools as malicious hackers (Schulz), but their purpose is to identify vulnerabilities and provide recommendations for improving security. They seek to ensure systems and data confidentiality, integrity, and availability through a structured and legal approach. Penetration testing is a more structured and formalized approach to testing the security of computer systems. It involves evaluating the security posture of networks, applications, or specific components by identifying vulnerabilities that attackers could exploit. A team of skilled professionals with deep knowledge of attack vectors and techniques typically conducts penetration tests. Both ethical hacking and penetration testing play crucial roles in identifying and addressing security weaknesses before malicious actors exploit them. They help organizations improve their security measures, protect sensitive data, and maintain the trust of their customers and stakeholders.

Given the growing reliance on technology and the proliferation of cyber threats, cybersecurity has become paramount in this digital age. As our lives become more interconnected and dependent on digital systems, the potential risks and consequences of cyber attacks have amplified. Safeguarding sensitive information has become crucial with the digitization of personal, financial, and business data. Cybersecurity measures help prevent unauthorized access, data breaches, identity theft, and financial fraud. Cyber criminals exploit network, system, and application vulnerabilities to carry out various malicious activities such as hacking, phishing, ransomware attacks, and data theft. Effective cybersecurity measures help detect, prevent, and mitigate these cyber threats, reducing the impact of cyber crime. In the digital age, privacy is increasingly at risk. Cybersecurity plays a vital role in preserving privacy by ensuring the confidentiality and integrity of personal data. Protecting individuals' private information builds trust and confidence in digital systems and services.

Organizations heavily rely on digital infrastructure to conduct their operations. Cyber attacks can disrupt critical systems, leading to financial losses, reputational damage, and potential downtime. Robust cybersecurity measures help maintain business continuity by mitigating the impact of attacks and facilitating swift recovery (Baloch, 2017). Cyber threats extend beyond individual organizations and affect national security. Governments, military institutions, and critical infrastructure are prime targets for cyber attacks. Strong cybersecurity measures are essential to protect sensitive national assets, defend against cyber espionage, and ensure the integrity of basic services. Trust and confidence in digital systems are vital, given the spread of technology across all aspects of our lives. By implementing effective cybersecurity measures, individuals and organizations can demonstrate their commitment to protecting users' interests, fostering trust in online interactions, and promoting the adoption of innovative technologies (Plume, 2017).

Various industries and jurisdictions have established cybersecurity regulations and standards to protect individuals' privacy, prevent data breaches, and mitigate cyber risks. Adhering to these requirements helps organizations avoid legal penalties, reputational damage, and other consequences. Cybersecurity is not a one-time effort but an ongoing process. It involves identifying vulnerabilities, implementing protective measures, monitoring for threats, and responding to incidents. Organizations can effectively manage risks and minimize potential harm by adopting a proactive approach to cybersecurity. The digital age has brought tremendous benefits and opportunities but has also exposed us to increased cyber threats. Prioritizing cybersecurity is essential to protect sensitive information, defend against cyber crime, preserve privacy, ensure business continuity, safeguard national security, foster trust, comply with regulations, and manage risks effectively in our increasingly connected world (Plume, 2017).

Understanding the differences between ethical hacking and penetration testing is essential. While both terms are often used interchangeably, they have distinct meanings; ethical hacking refers to intentionally and legally attempting to penetrate computer systems or networks with the permission of the system owner. Ethical hackers use their skills and knowledge to identify vulnerabilities and weaknesses in security systems. Ethical hacking aims to assess an organization's security posture, identify potential threats, and provide recommendations for improving security. Penetration testing, often abbreviated as penetration testing, is a subset of ethical hacking. It involves conducting controlled and simulated computer system or network attacks to identify and exploit vulnerabilities. The objective of penetration testing is to assess the security of a system by attempting to bypass security controls and gain unauthorized access. Pen testers follow a predefined scope and methodology and use various tools and techniques to simulate real-world attacks. There are significant differences between ethical hacking and penetration testing regarding scope, process, authorization, and end goal (EC-Council).

Ethical hacking encompasses various activities, including vulnerability assessment, risk analysis, and security consulting. Penetration testing is a focused exercise that aims to exploit vulnerabilities within a defined scope. In terms of methodology, ethical hacking involves a systematic approach to identify vulnerabilities, assess risks, and provide recommendations. Penetration testing follows a specific method, often involving reconnaissance, scanning, exploitation, and post-exploitation phases. Ethical hacking is conducted with explicit permission from the system owner. Penetration testing is also performed with authorization, but it is a subset of ethical hacking that focuses on simulating attacks (Baloch, 2017). The end goal of ethical hacking is to identify weaknesses and vulnerabilities to improve overall security. Penetration testing aims to exploit vulnerabilities to assess the effectiveness of security measures and identify potential areas of improvement.

Ethical hacking is a broad concept covering numerous security assessments, while penetration tests specifically include simulations of attacks to assess the effectiveness of safety measures. Both play crucial roles in identifying and mitigating security risks in an organization.

Ethical Hacking

Ethical hacking refers to intentionally and legally attempting to penetrate computer systems or networks with the system owner's permission (University of Michigan Information and Technology Services). The objective of ethical hacking is to identify vulnerabilities, weaknesses, and security flaws to improve the overall security posture of an organization. Ethical hackers help organizations strengthen their defenses and protect sensitive information from malicious attacks by identifying potential threats and weaknesses.

Roles and Responsibilities of Ethical Hackers

The roles and responsibilities of ethical hackers may vary depending on the specific engagement or project, but generally include the following:

1. Conducting Vulnerability Assessments: Ethical hackers perform comprehensive assessments to identify vulnerabilities in computer systems, networks, applications, or infrastructure (Hickey & Arcuri, 2020).
2. Penetration Testing: They simulate real-world attacks to exploit vulnerabilities and assess the effectiveness of security controls and measures.
3. Security Auditing: Ethical hackers assess an organization's security policies, procedures, and practices to ensure compliance with industry standards and best practices.
4. Reporting and Recommendations: They document and report their findings, including vulnerabilities discovered, potential risks, and recommendations for improving security.
5. Continuous Learning: Ethical hackers must stay updated with the latest hacking techniques, security trends, and industry developments to identify and address emerging threats effectively.

Common Tools and Techniques Used by Ethical Hackers

Ethical hackers employ a variety of tools and techniques to perform their assessments. Some commonly used tools include:

1. Network Scanners: Tools like Nmap, Nessus, and OpenVAS help identify open ports, services, and vulnerabilities in network infrastructure.
2. Password Crackers: Tools like John the Ripper and Hashcat are used to crack passwords and test their strength.
3. Exploitation Frameworks: Frameworks like Metasploit provide a range of ready-to-use exploits and payloads for testing vulnerabilities.
4. Wireless Hacking Tools: Aircrack-ng and Kismet are used for wireless network security assessments and cracking WEP/WPA keys.
5. Web Application Scanners: Tools like Burp Suite, OWASP Zap, and Nikto assist in identifying vulnerabilities in web applications.

Benefits and Challenges of Ethical Hacking

Benefits

1. Enhanced Security: Ethical hacking helps organizations proactively identify and address vulnerabilities, strengthening their security posture.
2. Risk Mitigation: By uncovering potential threats, ethical hackers assist organizations in mitigating risks and preventing possible attacks.
3. Compliance and Standards: Ethical hacking aids in ensuring compliance with industry standards, regulations, and best practices.
4. Incident Response Preparation: Ethical hacking can help organizations prepare for potential security incidents by identifying weaknesses and improving incident response capabilities.

Challenges

1. Legality and Ethics: Ethical hacking must be performed within the boundaries of legal and ethical frameworks, ensuring proper permissions and adherence to guidelines (Engebretson, 2013).
2. False Positives and Negatives: Ethical hackers may encounter challenges in accurately identifying vulnerabilities or distinguishing false positives and negatives, requiring a thorough understanding of systems and technologies.
3. Limited Scope: Ethical hacking engagements are often scoped and may not cover all possible attack vectors or vulnerabilities, leaving some potential risks unidentified (Engebretson, 2013).
4. Confidentiality Concerns: Ethical hackers may come across sensitive information during assessments, requiring them to handle data with utmost confidentiality and integrity.

It's important to note that ethical hacking should always be conducted responsibly and lawfully, with proper authorization and consent from the system owner.

Penetration Testing

Penetration testing is a security assessment methodology that simulates real-world attacks on computer systems, networks, applications, or infrastructure to identify vulnerabilities and assess the effectiveness of security controls (Engebretson, 2013). The purpose of penetration testing is to proactively identify and exploit security weaknesses, evaluate the potential impact of an attack, and provide recommendations for improving an organization's security posture (HackerOne).

Roles and Responsibilities of Penetration Testers

Penetration testers have the following roles and responsibilities:

1. Scoping and Planning: Penetration testers define the scope of the engagement, including the systems, applications, or networks to be tested. They also plan the testing approach, methodologies, and tools.
2. Reconnaissance and Information Gathering: Testers research to gather information about the target environment, including system architecture, IP addresses, domain names, and other relevant details.
3. Vulnerability Identification and Exploitation: Testers use various tools, techniques, and methodologies to identify and exploit vulnerabilities in the target systems. They attempt to gain unauthorized access, escalate privileges, and compromise sensitive data.
4. Reporting and Recommendations: After conducting the tests, penetration testers document their findings, including identified vulnerabilities, exploited weaknesses, and potential impacts. They provide recommendations for remediation and improving security controls.

Types of Penetration Tests

There are different types of penetration tests, categorized based on the level of information provided to the testers:

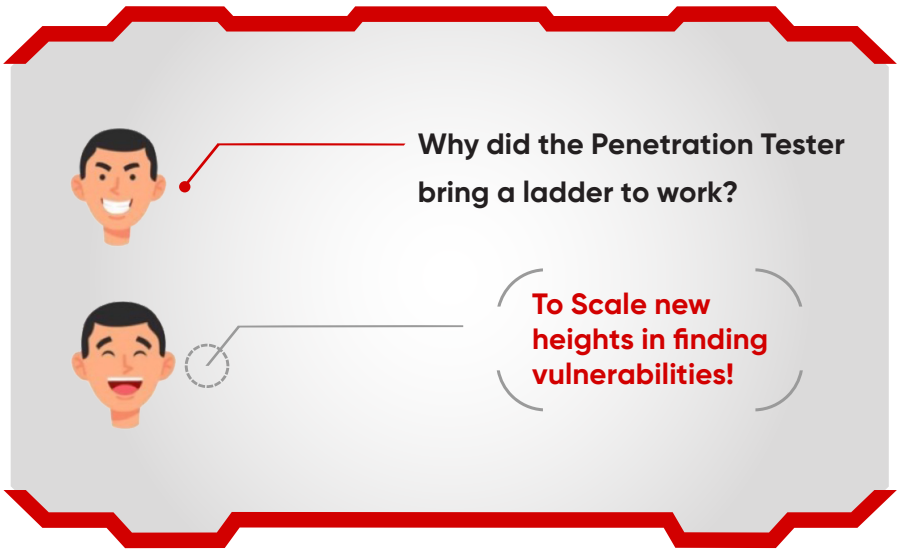
1. Black-Box Testing: Testers have not gained prior knowledge of the target system or network. They simulate an attack without any internal information, mimicking a real-world scenario where an attacker has limited knowledge.
2. White-Box Testing: Testers fully know the target system or network, including network diagrams, source code, and architecture. This type of testing allows for a more thorough assessment of the system's security (Engebretson, 2013).
3. Gray-Box Testing: Testers have partial knowledge of the target system. They are provided with information, such as network diagrams or limited access credentials, to simulate an insider threat or an attack scenario where partial information is available.

Common Tools and Methodologies Used in Penetration Testing

Penetration testers employ a range of tools and methodologies during their assessments. Some commonly used tools include:

1. Metasploit Framework: A widely used framework that provides pre-built exploits, payloads, and post-exploitation modules.
2. Nessus: A popular vulnerability scanner that identifies known vulnerabilities in systems and networks.
3. Burp Suite: A suite of web application testing tools that help identify vulnerabilities, manipulate requests, and analyze responses.
4. Nmap: A network scanning tool for port scanning, host discovery, and service enumeration.
5. Wireshark: A network protocol analyzer for capturing and analyzing network traffic.

Methodologies used in penetration testing include the reconnaissance phase (information gathering), scanning and enumeration phase (identifying open ports, services, and potential vulnerabilities), exploitation phase (attempting to exploit identified vulnerabilities), and reporting phase (documenting findings and recommendations) (Jaquet-Chiffelle & Loi, 2020).



Benefits and Challenges of Penetration Testing

Benefits

1. Vulnerability Discovery: Realistic assessment gives an understanding and effectiveness of security controls and incident response capability; penetration testing simulates potential attacks (RedTeam Security).
2. Realistic Assessment: Penetration testing provides a realistic simulation of potential attacks, giving organizations insight into the effectiveness of their security controls and incident response capabilities.
3. Risk Mitigation: By identifying and addressing vulnerabilities, penetration testing assists organizations in mitigating risks and preventing potential security incidents.
4. Compliance and Standards: Penetration testing helps organizations meet compliance requirements and adhere to industry standards, such as those defined by regulatory bodies or frameworks like PCI DSS or ISO 27001.

Challenges

1. False Sense of Security: Organizations may develop a false sense of security after a successful penetration test, assuming all vulnerabilities have been addressed. However, new vulnerabilities can emerge over time due to software updates, configuration changes, or evolving attack techniques. Continuous testing is necessary to maintain a robust security posture (Protect4S, 2017).
2. Scope Limitations: Defining the scope of a penetration test can be challenging. Potential vulnerabilities may be overlooked if specific systems, applications, or attack vectors are not included in the scope. Proper scoping requires careful consideration of the organization's assets, critical systems, and potential risks.
3. Disruption of Services: Penetration testing involves actively bypassing security controls and gaining unauthorized access. In some cases, this can unintentionally disrupt services or cause system instability. Proper planning and communication are essential to minimize any potential disruption during testing.
4. Skill and Resource Requirements: Effective penetration testing requires skilled and experienced professionals with expertise in various areas, including network security, system administration, and attack methodologies. Acquiring or outsourcing these resources can be a challenge for organizations.
5. Reporting and Prioritization: Analyzing and interpreting the findings of a penetration test can be complex. The assessment report may contain many vulnerabilities, and prioritizing remediation efforts based on their severity and impact requires careful consideration. Clear and actionable reporting is crucial to facilitate remediation and risk management.

It's essential to address these challenges by working with qualified professionals, establishing clear objectives and scope, maintaining open communication, and regularly updating and improving security measures based on the findings of penetration tests.

Key Differences Between Ethical Hacking and Penetration Testing

Objective and Scope

Ethical hacking aims to identify vulnerabilities, weaknesses, and security flaws in computer systems or networks. It has a broader scope, including vulnerability assessment, risk analysis, and security consulting. Penetration testing aims to simulate real-world attacks to identify and exploit vulnerabilities. It focuses on a specific scope, often defined by the client, and involves actively attempting to bypass security controls and gain unauthorized access (EC-Council).

Skills

Ethical hackers require a broad range of skills and expertise, including knowledge of network protocols, operating systems, programming languages, web applications, and security frameworks. They need a deep understanding of various attack vectors, vulnerability analysis, and risk assessment methodologies (Baloch, 2017).

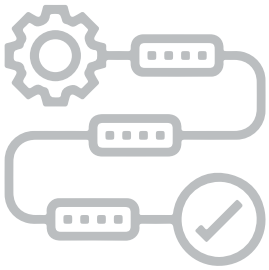
Penetration testers also need a strong understanding of network systems, operating systems, programming languages, and security concepts. However, their expertise focuses on attack methodologies, exploit development, and the ability to simulate real-world attacks while following a defined scope (Baloch, 2017).

Legal and Ethical Considerations

Ethical hacking must always be conducted within legal and ethical boundaries. It requires explicit permission and consent from the system owner or authorized personnel. Compliance with laws and regulations governing cybersecurity, privacy, and data protection is crucial (Whitaker & Newman, 2005).

Penetration testing follows the same legal and ethical considerations as a subset of ethical hacking. It requires authorization from the client or system owner before conducting any testing activities. Adherence to laws, regulations, and ethical guidelines is of utmost importance (Whitaker & Newman, 2005).

Reporting and Follow-up Actions



Ethical hackers provide comprehensive reports detailing vulnerabilities, weaknesses, and recommendations for improving security. They may also offer guidance on implementing security controls, best practices, and risk mitigation strategies. The focus is on providing insights and advice for overall security improvement.

Penetration testers provide detailed reports on vulnerabilities identified, exploited weaknesses, and potential impacts. The reports often include actionable recommendations for remediation and strengthening security controls. Penetration testing reports typically focus more on specific vulnerabilities within the defined scope.

In both cases, the reports are crucial for organizations to take appropriate actions to address vulnerabilities and improve their security posture.

It's important to note that "ethical hacking" and "penetration testing" are often used interchangeably, and the distinctions may vary depending on context and individual interpretations (Baloch, 2017). However, understanding these key differences can help clarify each term's objectives, scopes, skillsets, and ethical considerations.

Complementing Roles of Ethical Hacking and Penetration Testing

Ethical hacking can provide valuable support to penetration testing efforts in several ways:

1. Vulnerability Identification: Ethical hackers can perform thorough vulnerability assessments and identify vulnerabilities in systems, networks, or applications. Penetration testers can use this information as a starting point for testing and exploitation activities (Engebretson, 2013).

2. Exploit Development: Ethical hackers often develop or adapt exploits to target specific vulnerabilities. These exploits can be shared with penetration testers, enabling them to validate the effectiveness of security controls and assess the impact of potential attacks.

3. Realistic Attack Simulation: With their knowledge of various attack vectors and techniques, ethical hackers can assist penetration testers in simulating real-world attack scenarios. They can provide insights and guidance on attack methodologies, ensuring that the penetration testing efforts accurately replicate potential threats.

Penetration testing plays a crucial role in validating the effectiveness of ethical hacking initiatives:

1. Real-World Validation: Penetration testing involves simulated attacks that mimic real-world threats. By performing penetration tests after implementing the recommendations from ethical hacking assessments, organizations can validate the effectiveness of the security improvements and verify if the identified vulnerabilities have been adequately addressed (University of Michigan Information and Technology Services).

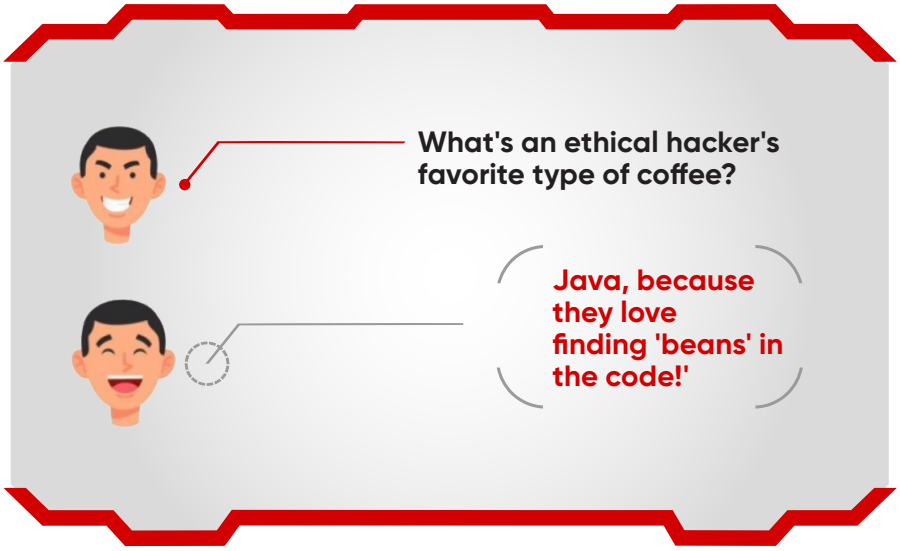
2. Testing Defensive Measures: Penetration testing focuses on actively bypassing security controls and gaining unauthorized access. It provides an opportunity to test the effectiveness of defensive measures implemented based on the findings of ethical hacking assessments; this helps evaluate if the implemented security controls are resilient to attacks and if they effectively mitigate identified vulnerabilities.

3. Incident Response Evaluation: Penetration testing can also evaluate an organization's incident response capabilities. By attempting to breach the systems, penetration testers can assess the effectiveness and timeliness of incident detection, response procedures, and mitigation efforts. This validation helps ensure that the organization is well-prepared to handle potential security incidents (Baloch, 2017).

Collaboration between ethical hackers and penetration testers is essential to maximize the effectiveness of security assessments:

1. Knowledge Sharing: Ethical hackers and penetration testers should collaborate to exchange knowledge, insights, and experiences. Ethical hackers can share information about emerging threats, new attack vectors, and vulnerabilities, while penetration testers can provide feedback on the practicality and feasibility of exploiting identified vulnerabilities.
2. Scope Definition: Ethical hackers and penetration testers should work together to define the scope of assessments. Ethical hackers can provide valuable input on potential areas of focus, high-risk targets, or specific vulnerabilities that will get tested. This collaboration ensures that the scope aligns with the organization's security needs (Engebretson, 2013).
3. Continuous Improvement: Collaboration between ethical hackers and penetration testers fosters a cycle of continuous improvement. Ethical hackers can provide feedback on the effectiveness of recommendations and remediation efforts, which will be used to refine future ethical hacking initiatives. Similarly, penetration testers can provide insights into the practicality and impact of identified vulnerabilities, helping ethical hackers refine their assessments (Baloch, 2017).

Collaboration between ethical hackers and penetration testers enhances the security assessment process promotes knowledge sharing, and helps organizations identify and address vulnerabilities effectively.



Case Study: Ethical Hacking and Penetration Testing in Practice

This case study will explore a real-world scenario involving ethical hacking and penetration testing. Ethical hacking involves identifying vulnerabilities and weaknesses in computer systems, networks, or applications with the owner's consent. This case study highlights the importance of ethical hacking and penetration testing in identifying and mitigating security risks.

Background

ABC Corporation, a multinational organization, recently experienced a security breach in a recent zero-day MOVEit SQLi vulnerability [CVE-2023-35708] where sensitive customer data was compromised. The incident highlighted the need for a comprehensive security assessment of their systems. The company decided to engage the services of a professional, ethical hacking and penetration testing firm, MeSecureTech Solutions, to identify vulnerabilities and recommend measures for improving its security posture.

Objectives

1. Identify vulnerabilities in the organization's network infrastructure, including servers, firewalls, and other network devices.
2. Evaluate the security of the organization's web applications and databases.
3. Assess the effectiveness of the existing security controls and incident response procedures.
4. Provide recommendations for mitigating identified vulnerabilities and improving overall security.

Methodology

MeSecureTech Solutions adopted a systematic approach to conduct ethical hacking and penetration testing engagement and followed these steps:

1. Reconnaissance: They gathered publicly available information about ABC Corporation, including its website, IP addresses, network structure, and employee details. This information helped to understand the organization's online footprint and potential attack vectors.
2. Scanning: Using network scanning tools, they identified active hosts, open ports, and services running on the network; this step helped create an inventory of systems to be further assessed.
3. Vulnerability Assessment: An in-depth vulnerability assessment of the identified systems and applications were conducted using automated vulnerability scanning tools and manual analysis to identify known vulnerabilities and misconfigurations.
4. Exploitation: Once vulnerabilities were identified, the penetration testing firm attempted to exploit them to gain unauthorized access to the organization's systems. This step helped evaluate the vulnerabilities' impact and severity and assess the effectiveness of existing security controls.
5. Post-Exploitation: After successful exploitation, they documented the steps taken, compromised data accessed, and the potential impact of the breach. This information was crucial in demonstrating the possible consequences of a real attack.
6. Reporting: Then, they prepared a detailed report outlining the findings, including a prioritized list of vulnerabilities and recommendations for remediation. The report provided actionable insights for ABC Corporation to improve its security posture.

Results and Recommendations

The penetration testing firm identified several critical vulnerabilities and provided the following recommendations to ABC Corporation:

1. Patch Management: Implement a robust patch management process to ensure that all systems and software are up to date with the latest security patches. Regularly review and apply vendor-released patches promptly.
2. Network Segmentation: Implement network segmentation to isolate critical systems and restrict access to sensitive data. This will limit the lateral movement of attackers within the network.
3. Web Application Security: Conduct regular security assessments of web applications, including penetration testing, to identify and fix vulnerabilities. Implement secure coding practices and web application firewalls to protect against common attacks.
4. Access Controls: Strengthen user access controls by enforcing the principle of least privilege. Regularly review and update user permissions to ensure that employees have access only to the resources necessary for their roles.
5. Incident Response: Develop and test an incident response plan to effectively respond to security incidents. Define roles and responsibilities, establish communication channels, and conduct regular tabletop exercises to validate the plan's effectiveness.

This case study illustrates the practical application of ethical hacking and penetration testing in identifying vulnerabilities and enhancing an organization's security.

Conclusion

Ethical hacking and penetration testing are crucial components of a comprehensive cybersecurity strategy. They involve assessing the security of computer systems and networks to identify vulnerabilities and protect against potential threats. Both roles aim to identify vulnerabilities and weaknesses in an organization's systems and networks but have different approaches and goals.
Considering the growing work and benefits we have witnessed in the Artificial intelligence domain, it will play a significant role in ethical hacking and penetration testing. It can automate specific tasks, enhance vulnerability detection accuracy, and help develop more sophisticated attack and defense mechanisms. As IoT devices continue to increase, ethical hackers and penetration testers will face new challenges in securing these interconnected devices and networks. Specialized knowledge and tools will be required to assess the security of IoT ecosystems. With the increasing adoption of cloud computing, securing cloud environments will become a critical focus for ethical hacking and penetration testing. Professionals must understand the risks and vulnerabilities associated with cloud platforms and services. Understanding the differences between ethical hacking and penetration testing is vital for developing a comprehensive cybersecurity strategy. It enables organizations to align their objectives, allocate resources effectively, ensure compliance, achieve comprehensive coverage, mitigate risks, and establish a continuous improvement cycle for maintaining robust security defenses.

References

Baloch, R. (2017). Ethical Hacking and Penetration Testing Guide. CRC Press. https://www.tsoungui.fr/ebooks/Ethickal-haking-postexploitation.pdf

EC-Council. (2023, January 4). Components of an Enterprise Penetration Testing Report. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-report/

EC-Council. (2023). What's the Difference Between Ethical Hacking and Penetration Testing? https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/ethical-hacking-vs-penetration-testing/

Engebretson, P. (2013, June). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Elsevier. https://www.sciencedirect.com/book/9780124116443/the-basics-of-hacking-and-penetration-testing

HackerOne. (2023). What Is Pentesting? How Does It Work Step-by-Step? https://www.hackerone.com/knowledge-center/what-penetration-testing-how-does-it-work-step-step

Hickey, M. & Arcuri, J. (September 2020). Hands on Hacking. https://www.oreilly.com/library/view/hands-on-hacking/9781119561453/

Jaquet-Chiffelle D-O, & Loi, M. (2020, February 11). Ethical and Unethical Hacking. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-030-29053-5_9

Protect4S. (2017, June 2). Why penetration tests provide a false sense of security. https://protect4s.com/2017/06/02/why-penetration-tests-provide-a-false-sense-of-security/

RedTeam Security. (2023). Advanced Adversary Simulation Methodology. https://www.redteamsecure.com/approach/cyber-red-teaming-methodology

Schulz, S. (2023). Parrot OS vs Kali Linux – Which is Better for Hacking. GOGET SECURE. https://gogetsecure.com/parrot-os-vs-kali/

Plume, S. (2017). Cyber/Information Security in the Digital Age. Center for Digital Strategies at the Tuck School of Business.
https://digitalstrategies.tuck.dartmouth.edu/publication/cyberinformation-security-digital-age/

University of Michigan Information and Technology Services. Penetration Testing (Ethical Hacking). https://safecomputing.umich.edu/protect-the-u/protect-your-unit/vulnerability-management/ethical-hacking

Whitaker, A. & Newman, D. P. Penetration Testing and Network Defense. Cisco Press. https://www.ciscopress.com/store/penetration-testing-and-network-defense-9780133433210