IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125230

PENETRATION TESTING USING ETHICAL HACKING

Girish Shivkumar Puranik(72170276H)[1], Simran Vishnu Makhija(72170281D)[2], Siddharth Rajeshkumar Bedmutha(72170251B)[3], Shruti Kundan Meshram(72170266L)[4]

G H Raisoni College of Engineering & Management, Ahmednagar ·Gate No.: 1030, Village Chass, Nagar Pune Road, Ahmednagar, Maharashtra 414008[1-4]

Abstract: The PEN testing allows a PEN tester to check the functional aspects of a system that how much a system is vulnerable to the Network security & intrusion attacks & to see its defense mechanisms to counterpart these attacks. In this research paper we have conducted a literature review on the work done by the various researchers in the area of Penetration (PEN) testing. We have tried to review the various aspects related to the PEN testing.

We have also studied the various tools used for PEN testing in terms of their utility, technical specifications, date of their release, Platform compatibility etc. various aspects related to the PEN testing. We have also studied the various tools used for PEN testing in terms of their utility, technical specifications, date of their release, Platform compatibility etc.

Keywords: Network security, defense mechanism, various tools, security of data.

I. INTRODUCTION

Penetration testing, also known as ethical hacking, is a systematic process of assessing the security of computer systems, networks, and applications. It involves simulating real-world cyber attacks to identify vulnerabilities that malicious attackers could exploit. Ethical hackers, or penetration testers, use various techniques and tools to uncover weaknesses in the target systems. They follow a structured approach that includes reconnaissance, vulnerability scanning, exploitation, and reporting.

The goal of penetration testing is to help organizations identify and mitigate security risks, strengthen their defenses, and protect sensitive data from unauthorized access. It provides valuable insights into potential vulnerabilities and helps organizations understand their security posture.

Ethical hacking requires a deep understanding of various technologies, networking concepts, programming languages, and security principles. Professionals in this field must adhere to strict ethical guidelines and obtain appropriate permissions before conducting any testing. In this guide, we will explore the fundamental concepts of penetration testing and ethical hacking.

We will delve into different methodologies, tools, and techniques used by ethical hackers to identify vulnerabilities. Additionally, we will discuss the importance of proper reporting and communication to ensure effective remediation. Web application penetration testing reveals real-world opportunities attackers could use to compromise applications in order to gain access to sensitive data or even take- over systems for malicious and non-business purposes.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125230

LITERATURE REVIEW

Sr. No.	Author	Year	Title	Remark
1	R. Shanmugapriya	2013	A study of network security using penetrationTesting.	This paper reviews stop the hacking for illegally and protect the website and web applications . Everyone should know the ethics of hacking and follow them to be safer.
2	Joel Dawson,J. Told McDonald.	2016	Improving the penetration Testing methodologies for security- based risk management.	In the research process would involvean effort to convert the abuse cases into definable vulnerabilities,if not genuine exploits. Further down the line, we would investigatethe application
3	Prashant Vats, Manju Mandot,AnjanaGosain	2020	A Comprehensive Literature Review of PenetrationTesting & Its Applications	In this paper, we have carried out a review of the work performed in the area of PEN testing. We have also reviewed that how the PEN testing can be helpful in detecting the vulnerabilitiesthat are present in our Network.
4	Arvind Goutam, Vijay tiwari.	2019	Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application	web applicationand on the financialweb applicationsmanytypes of research have been done. Basically,many researchers focused on the cross-site scripting,SQL injection,cross-site request forgery attack and focused on many other attacks on the financialweb application

14

II. CONCLUSION

Web penetration testing using ethical hacking is an essential and effective approach to securing web applications and systems. Ethical hackers, also known as penetration testers or white hat hackers, use their skills and knowledge to identify vulnerabilities and weaknesses in web-based platforms, with the goal of improving their security posture.

Through a systematic and controlled process, ethical hackers simulate real-world attack scenarios to identify and exploit vulnerabilities that malicious hackers could potentially exploit. By taking this proactive approach, organizations can identify and patch security flaws before they are exploited by cybercriminals, thereby reducing the risk of data breaches, financial losses, and reputational damage.

Web penetration testing involves various methodologies and techniques, including reconnaissance, vulnerability scanning, manual testing, and the use of automated tools. It requires a deep understanding of web technologies, protocols, and common attack vectors, as well as adherence to ethical guidelines and legal boundaries.

The benefits of web penetration testing using ethical hacking are numerous. It provides organizations with valuable insights into their security posture, highlighting vulnerabilities and weaknesses that may otherwise go undetected. By addressing these vulnerabilities, organizations can enhance their overall security, protect sensitive data, and ensure compliance with industry regulations and standards.

Furthermore, web penetration testing helps organizations build trust with their customers, partners, and stakeholders. It demonstrates a commitment to security and shows that proactive measures are being taken to protect valuable assets and maintain a secure online environment.

However, it's important to note that web penetration testing is not a one-time activity. As web technologies evolve, new vulnerabilities emerge, making regular testing and continuous monitoring crucial to maintaining an effective security posture. Additionally, organizations should consider the ethical, legal, and privacy implications of conducting web penetration tests and ensure that appropriate permissions and safeguards are in place.

In summary, web penetration testing using ethical hacking is a vital practice for organizations looking to secure their web applications and systems. By leveraging the skills of ethical hackers, organizations can identify vulnerabilities, remediate them, and ultimately strengthen their overall security posture, leading to increased trust, reduced risk, and improved resilience against cyber threats.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125230

REFERENCES

- **https://www.google.co.in/**
- **https://scholar.google.com/**
- **https://ieeexplore.ieee.org/Xplore/home.jsp.**
- **https://sci-hub.se/**

1. OWASP (Open Web Application Security Project): OWASP provides a comprehensive set of resources, including the OWASP Testing Guide, which covers various aspects of penetration testing methodologies and techniques. Their website is a valuable reference for understanding web application security.
2. NIST Special Publication 800-115: This publication by the National Institute of Standards and Technology (NIST) provides guidance on information security testing and assessment methods, including penetration testing.
3. Penetration Testing Execution Standard (PTES): PTES is a framework that provides guidelines and a methodology for performing penetration tests. It covers different phases of the testing process, including pre-engagement, intelligence gathering, vulnerability analysis, exploitation, and reporting.
4. SANS Institute: SANS offers numerous resources, including training courses and whitepapers, on penetration testing and ethical hacking. Their website is a valuable source of information for both beginners and experienced professionals.
5. Offensive Security Certified Professional (OSCP) Certification: The OSCP certification offered by Offensive Security is highly regarded in the penetration testing community. The associated training materials and lab exercises provide hands-on experience and practical knowledge in conducting penetration tests.
6. Metasploit Unleashed: Metasploit Unleashed is a comprehensive online resource provided by Rapid7, the creators of the Metasploit Framework. It offers detailed documentation, tutorials, and examples for using the Metasploit Framework in penetration testing.
7. Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman: This book provides a practical introduction to penetration testing and covers various techniques, tools, and methodologies. It includes step-by-step examples and exercises to reinforce learning.

It's important to note that the field of penetration testing is constantly evolving, and new resources and references emerge over time. Staying updated with the latest industry practices and attending relevant conferences and training programs can further enhance your knowledge in this field. Regenerate response

.