Chapter 13
Penetration Testing:
A Way to Secure IT Industries

Aditya Sharma
Ajeenkya D.Y. Patil University, India

Amna Kausar
https://orcid.org/0009-0000-3940-8845
Ajeenkya D.Y. Patil University, India

Atharva Saraf
https://orcid.org/0009-0006-3842-5508
Ajeenkya D.Y. Patil University, India

Susanta Das
https://orcid.org/0000-0002-9314-3988
Ajeenkya D.Y. Patil University, India

ABSTRACT

To identify system vulnerabilities, pen testing is essential for cybersecurity. Phases of preparation, reconnaissance, scanning, exploitation, and reporting are all involved. Every phase makes use of tools such as Nmap, Nessus, and Metasploit. To guarantee system, network, and data security, businesses should conduct pen tests regularly using skilled testers. This chapter delves into this important domain of cybersecurity as well as information technology industries. The chapter also discusses ethical issues and various challenges associated with it.

DOI: 10.4018/979-8-3693-5728-6.ch013

INTRODUCTION

Testing a system to identify security flaws is known as penetration testing. The goal of the research is to present a thorough understanding of the strategies and tactics applied in this process, emphasizing areas that require improvement and best practices. This covers the stages of a penetration test that involve planning, reconnaissance, scanning, exploiting, and reporting. By offering insightful information about the testing procedure, the research will assist organizations in optimizing their information security posture. Through the examination of current literature on penetration testing techniques, the study will provide a useful tool for enhancing information security assessment procedures and safeguarding confidential data. Improving penetration testing's efficacy and efficiency as a tool for information security assessment is the ultimate objective (Ziro et al., 2023). Several factors can lead to vulnerability, including inadequate programming or an antiquated system (Hasan & Meva, 2018). Information assurance can be impacted by system vulnerabilities and security issues. While achieving a totally secure system may be challenging, lowering the amount of vulnerabilities can greatly improve system security. Nonetheless, penetration testing and vulnerability assessment are frequently undervalued. These actions frequently go unnoticed and are thought of as mere formalities. Organizations can lessen their vulnerability to attacks and have a more secure system by regularly and effectively performing vulnerability assessments (Abu-Dabaseh & Alshammari, 2018). The goal of penetration testing is to identify and fix system vulnerabilities before unauthorized users can take advantage of them. A vulnerability that is left unchecked could be exploited to obtain unauthorized access to business resources and compromise the system. Penetration testing aims to find and address these vulnerabilities to keep the system safe and stop similar compromises (Kesharwani et al., 2018). Access to a wide range of services, such as telehealth, digital transactions, e-commerce, online business, audio/video conferencing, e-commerce, dependable treatment, shipping and aviation services, and mobile payment systems, is becoming more and more dependent on the internet. As a result, a great deal of sensitive and private data is produced online. However, there's also a growing chance of cyberattacks, which can result in lost or corrupted data, compromised user credentials, and interrupted services. Because of this, the business community is starting to take this seriously (Sarker et al., 2023).

Cybercriminals launch attacks by taking advantage of different weaknesses in devices, apps, networks, and user behavior. These vulnerabilities may be the result of human error, complex computing systems, out-of-date hardware and software, poorly configured systems, and design flaws. Governmental bodies, for-profit businesses, and global trade hubs are concentrating on cyber defense in order to combat these threats. An essential component of cyber defense is penetration testing, which