A study of penetration testing tools and approaches

Chiem, Trieu Phong

Abstract
As one of the most common techniques to assess information system security, penetration testing legally attempts to break into the target system by utilizing tools and techniques similar to those used by real hackers. The main objective of such technique is to effectively call to light potential vulnerabilities...

Keywords
Penetration testing; Information security; Vulnerability assessment

Date
2014

Item Type
Thesis

Supervisor(s)
Yan, WeiQi; Thorpe, Stephen

Degree Name
Master of Computer and Information Sciences

Publisher
Auckland University of Technology
No, penetration testing and vulnerability assessment are two different approaches, but with the same end-purpose of making software product/system safe and secure. People are often ambiguous between the differences or similarity between these two techniques and use them interchangeably. While, Vulnerability Assessment involves study and analysis of system with the help of testing tools to identify and detect security loopholes and flaws present in the system and making it vulnerable to multiple variants of security attack. Vulnerability Assessment methodology follows a pre-defined and established procedure, unlike penetration testing where the sole purpose is to break system, irrespective of adopted approaches. A variety of different techniques and tools are for penetration testing. Table 1 lists some of these tools. III. TESTING WORKFLOW In this work we studied various automated tools for penetration testing. By analyzing the behavior of different tools a common approach to automated penetration testing emerged. The procedure followed by these tools consists of three main phases: First scan host machines in the network under test to collect all possible information Secondly we need to identify vulnerabilities of these host by matching the results of the first phase i.e. scan with entries in a vulner $\S$ Penetration Testing Reporting Guidelines: Guidance for developing a comprehensive penetration test report that includes the necessary information to document the test as well as a checklist that can be used by the organization or the assessor to verify whether the necessary content is included. The information in this document is intended as supplemental guidance and does not supersede, replace, or extend PCI DSS requirements. While all references made in this document are to PCI DSS version 3.0, the general principles and practices offered here may be applied to any version of PCI DSS. 1.2