ISSN 1945-5259

# Journal of Information Systems Technology and Planning

JISTP

Volume 5, Issue 12

INTELLECTBASE
INTERNATIONAL CONSORTIUM

Published and Sponsored by: Intellectbase International Consortium (IIC)

JISTP

# Journal of Information Systems Technology & Planning

Volume 5, Issue 12

***ISSN: 1945-5240*** *Print* ***ISSN: 1945-5267*** *Online* ***ISSN: 1945-5259*** *CD-ROM*

Full Article Available Online at: Intellectbase and EBSCOhost │ JISTP is indexed with Cabell's, JournalSeek, etc.

**JOURNAL OF INFORMATION SYSTEMS TECHNOLOGY & PLANNING**

Journal Homepage: www.intellectbase.org/journals.php │ ©2012 Published by Intellectbase International Consortium, USA

# ASPECTS OF INFORMATION SECURITY: PENETRATION TESTING IS CRUCIAL FOR MAINTAINING SYSTEM SECURITY VIABILITY

***Jack D. Shorter, James K. Smith and Richard A. Aukerman***
*Texas A&M University - Kingsville, USA*

## ABSTRACT

*P Penetration testing is the practice of testing computer systems, networks or web applications for their vulnerabilities and security weaknesses. These tests can either be conducted by automated software or manually [6.] Wikipedia has defined penetration testing as "a method of evaluating the security of a computer system or network by simulating an attack from a malicious source..." [11]. There are many different levels of penetration tests that can be performed on an organizations network and security infrastructure. These tests can range from simply attempting a brute force password attack on a particular system, all the way up to a simulated attack including, but not limited to social engineering.*

**Keywords:** *Penetration Testing, Black Box Penetration Testing, White Box Penetration Testing, Scanning and Enumeration, Target Testing, Internal Testing, Blind Testing, Double Blind Testing.*

## INTRODUCTION

Penetration testing is the practice of testing computer systems, networks or web applications for their vulnerabilities and security weaknesses. These tests can either be conducted by automated software or manually. The objectives of these tests are to provide valuable security information to the company being tested, and to serve as a blueprint for the areas that need improvement. Besides security issues, penetration testing is also performed to monitor an "organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents". Penetration tests are sometimes referred to as "White Hat attacks" due to the break-ins being conducted by information systems personnel who were ask to supply this service [6].

There are countless guides, books, and resources available for the modern network administrator or information technology executive to facilitate making the sensitive data on their networks and computer systems secure. He or she can have a highly secure network by having a robust Acceptable Use Policy (AUP), Security Policy (SP), along with well trained staff in both the information technology department and the organization as a whole. The data on the computers within the network can be protected by the most expensive up-to-date firewalls and encryption methods. The equipment can be physically protected by video monitoring, multiple security guards, and locked doors that lead to man-trap hallways. When all of this security is in place, how can a network administrator be confident that the