



Why Penetration Tests are important to Network Security?

Cyber 51 LTD.

DOCUMENT CLASSIFICATION:

PUBLIC

Copyrighted Material

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distance learning, in any form or by any means such as any information storage, transmission, or retrieval system, without prior written permission from the author.



Table of Contents

INTRODUCTION.....	3
WHY PENETRATION TESTS ARE IMPORTANT TO NETWORK SECURITY?	3
WHY PENETRATION TESTING IS IMPORTANT.....	3
HOW PENETRATION TESTING WORKS	4
PENETRATION TEST RESULTS.....	4
WHY WEB APPLICATION PENETRATION TESTS ARE IMPORTANT TO NETWORK SECURITY?	4
WHY WEB APPLICATION PENETRATION TESTING IS IMPORTANT.....	5
HOW WEB APPLICATION PENETRATION TESTING WORKS.....	5
WEB APPLICATION PENETRATION TEST RESULTS.....	5



Introduction

In today's world, the number and variety of threats to IT systems are multiplying daily, as is the number of security products and services to address them. Businesses that trade electronically are particularly vulnerable to risks such as fraud or breaches of confidentiality, causing loss of assets and damage to their reputation. For these companies, information and transactions need to be protected by means appropriate to their value and their potential for consequential loss.

Our Security Services address the numerous mission-critical information security challenges faced by our enterprise clients throughout the world. Our approach is to help you build-in security right from the start.

Working with you throughout the different stages of your IT business change cycle, we assist with the early identification of security threats through code reviews, functional security tests and vulnerability checks. For existing systems, we can provide independent technical design and implementation reviews, followed by a detailed testing cycle to ensure the system is secure when operational.

We are the ideal partners to ensure the systems you implement support the security needs of your business in a comprehensive and robust manner.

Why Penetration Tests are Important to Network Security?

Penetration testing is often referred to as a "pen test" and is a testing procedure that is performed to test the perimeters of a network for security breaches and vulnerabilities. Penetration testing is also known as ethical hacking.

If the vulnerabilities are discovered it helps the organization to defend itself against further attacks.

Why Penetration Testing is Important

Penetration takes network security to the next level by actually exploring the network for vulnerabilities. Simply deploying a firewall, vulnerability scanner, and an antivirus program are not enough to protect the system against an attack.

Regardless of how many security systems you use, there is still a good chance of weaknesses that exist within the network. Without a comprehensive test, sensitive data is prone to disclosure and some organizations can face legalities if they do not comply with network security guidelines for data protection.



How Penetration Testing Works

Penetration testing works on the premise that hackers have more knowledge of network vulnerabilities than the organizations that run the networks, and they are always stay one step ahead of network professionals. Therefore it is necessary for a team of network security experts to perform the tests using the same techniques that hackers would use to breach network security.

The penetration test involves two stages: the first stage involves locating the potential vulnerabilities in the network and then the second stage exploits the vulnerabilities.

Our security professionals have the knowledge of the same methods that hackers use to breach the security of a network. The difference is the professionals that we employ perform the test in a professional manner that does not jeopardize the data on the network or open up any other applications to risks.

Penetration Test Results

When the penetration test is complete, the security experts prepare a report for your organization that includes vulnerabilities in the network system.

Basically the report provides a way to evaluate the network systems from an outside criminal's point of view so that the necessary steps can be taken to repair the vulnerabilities and provide optimum network security.

Why Web Application Penetration Tests are Important to Network Security?

Web applications have become increasingly vulnerable to different forms of hacker attacks. According to a Gartner Report, 75% of attacks today occur at the application level. A Forrester survey states "people are now attacking through web applications, because it's easier than through the network layer."

Despite common use of defenses such as firewalls and intrusion detection or prevention systems, hackers can access valuable proprietary and customer data, shutdown websites and servers and defraud businesses, as well as introduce serious legal liability without being stopped or, in many cases, even detected.



Why Web Application Penetration Testing is Important

Customers would benefit from web application penetration testing on the application as it gives an in-depth analysis of your current security posture, recommendations for reducing exposure to currently identified vulnerabilities are highlighted and it allows the customer to make more informed decisions, enabling management of the company's exposure to threats.

How Web Application Penetration Testing Works

Web Application Penetration Testing is a comprehensive security risk assessment solution used to identify, analyze and report vulnerabilities in a given application.

As part of the web application penetration test, the security team will attempt to identify both inherent and potential security risks that might work as entry points for the hacker.

The vulnerabilities could be present in a web application due to inadvertent flaws left behind during development, security issues in the underlying environment and misconfigurations in one or more components like the database, the web servers etc.

When conducting a Web Application Penetration Testing assignment, we adopt a strong technology and process-based approach supported by a well-documented methodology to identify potential security flaws in the application and underlying environment. Adherence to industry standards such as OWASP, customized tests based on technology and business logic, skilled and certified security engineers, risk assessment on the vulnerabilities found, scoring system based on CVSS (Common Vulnerability Scoring System) make us different from the other vendors in this space.

Web Application Penetration Test Results

The security assessment report submitted on completion of the engagement provides a detailed and prioritized mitigation plan to help customers in addressing security issues in a phased manner.