International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Protecting Organization's Data through Penetration Testing

Prerak Doshi

Gujarat Urban Development Company Ltd., (A Government of Gujarat Undertaking Company)

Abstract: ***Today's businesses and organizations are heavily dependent on computer network based applications. Many of such applications are using the Internet as a channel for exchanging information leading to a high risk of intrusion or fraud or misuse, such as phishing and other attacks. However, along with the suitability and easy access to information derives new risk. Major risks involved are loss of valuable information. In order to protect such resources, organization needs information security policy, measurement and periodical review of information security by using vulnerability assessment and penetration testing tools & technique. In this paper, various aspects of perpetration testing are discussed along with implementation aspects. Paper also describes various phases and types of penetration testing. By performing various penetration test, organization can secure their resources in better way***.

Keywords: Penetration Testing, Vulnerability Assessment, Computer Security, Attacks, Testing, Security Policy

1. Introduction

A penetration test is a technique of estimating the information security of a computer system or network by simulating an attack from a tools and utilities. Penetration testing called pen testing is the practice of testing a computer system, network or Web application to find security hole that an attacker could exploit. Wikipedia defines penetration test as "A test known as a pen test, is an authorised simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data"[1].

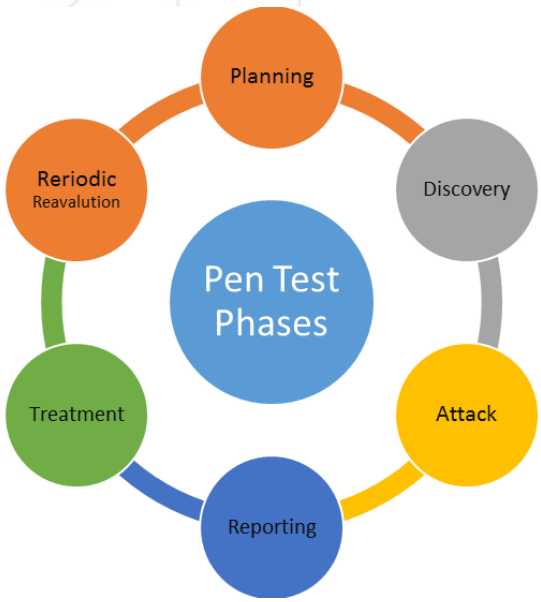
In this competitive century, only street business is not enough to maximize the business profit. Today's most familiar word the Internet is based on Information and Communication Technology, using which now it is possible for the businesses to perform their daily transaction and to provide services 24 X 7 and 365 days a year to their consumers. [2] Techniques for User Access Control can be used to enhance security of various networked based resources. [3] As you are aware, the Internet and associate computer systems is a Global System of interconnected computer networks that use the standard Internet protocol to serve billions of users worldwide. It is a network system of networks system that involves of millions of private and public networks system, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet transmits wide range of information resources and facilities.

A pen test can also be used to test an organization's information security policy compliance, its employees' information security awareness and the organization's capability to identify and counter to information security incidents.

What can be tested?
Your organization processes, captures, and stores information can be assessed; the systems that the information is stored in, the transmission channels that transport it, and the processes and personnel that manage it. Areas that are commonly tested are:

- Off-the-shelf products (operating systems, applications, databases, networking equipment etc.)
- Bespoke development (dynamic web sites, in-house applications etc.)
- Telephony (war-dialling, remote access etc.)
- Wireless (WIFI, Bluetooth, IR, GSM, RFID etc.)
- Personnel (screening process, social engineering etc.)
- Physical (access controls, dumpster diving etc.)

2. Penetration Testing Phase



3. Common type of Pen Test

3.1 Targeted Testing

Targeted testing is executed by the organization's Information Technology team and the pen testing group working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

3.2 External Testing

External test targets organization's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The goal is to find out if an external attacker can get in and in what way they can get in once they've gained access.

3.3 Internal Testing

Internal test mimics an inside attack behind the firewall by an official user with standard access privileges. This kind of test is useful for assessing how much damage a disgruntled employee could cause.

3.4 Blind testing

Blind testing simulates the actions and process of a real attacker by severely limiting the information given to the team that's performing the test beforehand. Typically, they may only be given the name of the organization. Because this type of test can require a extensive amount of time for investigation.

3.5 Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only CIO within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

A penetration test involves gathering information about an organization's information systems and security infrastructure, and then using this information to attempt to identify and then exploit known or potential security vulnerabilities.

There are different free and commercial tools available for Pen test in the market. Popular penetration testing Operating System examples include [1]:

- Kali Linux based on Debian Linux
- BackBox based on Ubuntu
- Pentoo based on Gentoo Linux
- WHAX based on Slackware Linux

4. Advantages of Penetration Test

- A penetration test helps organizations to understand their present information security posture by identifying breaches in security. This assists organizations to develop an action plan to minimize the threat of attack.
- A virtuous documented penetration test result supports executives in creating a strong business case to justify a needed increase in the information security budget.
- Information Security is not a single point solution, but it is continuous process. Security measures need to be examined on a regular basis to discover new threats. A penetration test enable organizations to emphasis internal security resources where they are needed most.
- Penetration testing help organizations to meet regulatory compliances and legislative requirement.
- Corporate organization are involved close working with strategic partners, suppliers, customers and others upon whom the e-Business depends. Corporates allow partners, suppliers, and other trusted connections into their networks. Penetration test help organizations find the weakest links in this complex structure and guarantee that all connected entities have a standard baseline for information security.
- Penetration test provides critical validation response between corporate initiatives and information security framework that permits for successful implementation at minimal risk.
- Protecting your trademark by avoiding loss of consumer confidence and professional reputation.

Many organization focus on Vulnerability analysis for Computer, Network, Applications and database etc. There are different free and commercial tools available for vulnerability assessment in the market. But some major difference between Vulnerability assessment and Penetration testing are:

Difference between the two types of testing

- Vulnerability Analysis is the process of finding vulnerabilities on a computer, network, application, and database etc. whereas a Penetration Testing is focused on actually gaining unauthorized access to the systems and using that access to the network or data, as directed by the client.
- A Vulnerability Analysis provides an summary of the flaws that exist on the system while a Penetration Testing goes on to provide an impact analysis of the flaws finds the possible impact of the flaw on the underlying network, operating system, database etc.
- Vulnerability Analysis is passive process. In Vulnerability Analysis you use software tools that analyze both network traffic and systems to identify any exposures that increase vulnerability to attacks. Penetration Testing is an active exercise wherein ethical hackers are working to mimic an attack and test the network and systems' resistance.
- Vulnerability Analysis deals with possible risks, whereas Penetration Testing is actual proof of concept. Vulnerability Analysis is just a process of finding and measuring the security Vulnerabilities in a system. Vulnerability Analysis doesn't provide validation of information Security Vulnerabilities. Validation can be only done by Penetration testing.
- Vulnerability Analysis exercise might find absence of anti-virus software on the system or open ports as a vulnerability. The Penetration Testing will determine the level to which existing vulnerabilities can be exploited and the damage that can be inflicted due to this.

5. Conclusion

In this paper, various concepts of perpetration testing (pen test) are discussed along with its implementation aspects. Paper also describes various phases and types of penetration testing. By performing various penetration tests, organization

and individuals can provide better security to their resources, protect your product by avoiding damage of consumer confidence and organization reputation. This paper is one of the efforts from my side to give some direction of improving organization security by using pen test.

References

[1] https://en.wikipedia.org/wiki/Penetration_test, visited on 25th March 2017.
[2] Patel, Kuntalkumar P. "Decision Support System Based E-Commerce Model and It's Functioning." Management of Innovation and Technology, 2006 IEEE International Conference on. Vol. 1. IEEE, 2006.
[3] Bansi, Khimani, and Patel Kuntal. "A Novel Model for Security and Data Access for Jointly Accessing the Cloud Service." BIJIT - BVICAM's International Journal of Information Technology 7.1 (2015): 841-844.

Author Profile

Prerak Doshi hold 15+ years of experience in the field of Information Technology including information security management, IT infrastructure management, and e-Governance sector. He is currently looking after e-Governance practice for the State of Gujarat, India.