International Journal Of Scientific & Engineering Research, Volume 11, Issue 7, July-2020
ISSN 2229-5518

The Defense Strategies, Benefits and Challenges of Pen Test against Cyber Attacks – A Review

Sanal Kumar S, Dr Palanivel S

Abstract -Cyber Security is a major challenge faced by the current internet business scenario due to the infrastructural complexity of universally scattered systems and the interrelationship among computer, communication, and power infrastructures across the globe. .A security policy focuses on preventing and detecting an attack on a personal or enterprise systems, that policy may not include a process to expel a hacker. Studies regarding security testing for corporate environments, networks, and systems were developed and implemented in the last years. The primary goal of a pen test is to identify weak areas in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether and how the organization would be subject to security disasters. This paper is a scholarly article which provides an overview of penetration testing, its benefits, issues, strategies, application scenarios, models and tools.

Index Terms - Penetrating Testing, Pen Test, Ethical Hacker, White Hat, Black Box Testing, White Box Testing, IP address, Cyber Attacks.

1. INTRODUCTION

PEN Test or Penetration testing is a process undertaken to identify and exploit security issues. Penetration testing can be automated with software applications or performed manually. The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents. Organizations should perform pen testing regularly ideally, once a year to ensure more consistent network security and IT management. An organization with a smaller budget might only be able to conduct a penetration test once every two years while a company with a larger budget can do penetration testing once a year. A penetration test can also highlight weaknesses in a company's security policies. Pen testers use automated tools to uncover common application vulnerabilities.

- *Sanal Kumar S is currently working as Assistant Professor at the Dept of Instrumentation, NSS College , Nemmara,Palakkad ,Kerala,India. E-mail: sanalkumar_s@nssnemmara.ac.in*
- *Dr Palanivel S is currently working as Associate Professor at the Dept of Electronics & Instrumentation Engg , Annamalai University, Chidambaram , Tamilnadu, India.. E-mail: sp04266@annamalai.ac.in*

Penetration tools scan code in order to identity malicious code in applications that could result in a security breach. Pen testing tools examine data encryption techniques and can identify hard-coded values, such as usernames and passwords, to verify security vulnerabilities in the system. Pen Testing as a Service provides information technology (IT) professionals with the resources they need to conduct and act upon point-in-time and continuous penetration tests

2. PEN TEST?

Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

Penetration testing is essential because:

- ✓ It provides evidence to suggest, why it is important to increase investments in security aspect of technology.
- ✓ It evaluate the magnitude of the attack on potential business

International Journal Of Scientific & Engineering Research, Volume 11, Issue 7, July-2020
ISSN 2229-5518

- ✓ It identifies a simulation environment i.e., how an intruder may attack the system through white hat attack.
- ✓ It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
- ✓ It supports to avoid black hat attack and protects the original data.

Organizations should perform pen testing regularly to ensure more consistent network security and IT management. In addition to conducting regulatory-mandated analysis and assessments, penetration tests may also be run whenever an organization:

- ✓ Adds new network infrastructure or applications.
- ✓ Makes significant upgrades or changes to its applications or infrastructure.
- ✓ Establishes offices in new locations
- ✓ Applies security patches
- ✓ Modifies end-user policies

However, because penetration testing is not one-size-fits-all, when a company should engage in pen testing also depends on several other factors, including:

- ✓ The complexity of the company. Companies with a larger presence online have more attack vectors and so are more-attractive targets for hackers.
- ✓ Penetration tests can be costly, so a company with a smaller budget might not be able to conduct them annually. An organization with a smaller budget might only be able to conduct a penetration test once every two years while a company with a larger budget can do Pen testing once in a year.
- ✓ Regulations and compliance. Organizations in certain industries are required by law to perform certain security tasks, including pen testing.
- ✓ A company whose infrastructure is in the cloud might not be allowed to test the cloud provider's infrastructure and in such cases the provider may be conducting pen tests itself according to the current platform.

3. TYPES ?

The different types of Pen test depends on the application, requirements and scope and the organization. The three main important types of Pen test are i) Grey box ii) Black box testing iii) White box testing.

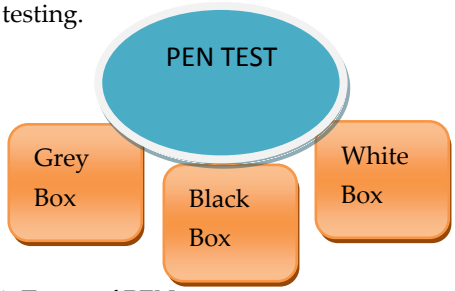

Fig 1: Types of PEN test

3.1 Grey Box Penetration Testing

In Grey Box test, a testing authority provides only a limited data about the source code details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents. As the tester does not require the access of source code, it is non-intrusive and unbiased. As there is clear difference between a developer and a tester, so there is least risk of personal conflict.

3.2 Black Box Penetration Testing

In Black box testing the tester need not be a technical or programming expert as he only collects data about destination network or system. The information regarding testing system or network will be completely hidden from the testing authority and no verification of source code is done. The main drawbacks of this testing are mainly in the difficulty in the design of the test and it does not cover everything

3.3 White Box Penetration Testing

In white box testing the testing authority verifies the source code and do data flow, path and loop testing and thus it makes a comprehensive testing among all other pen tests as the tester has been provided with full information of the network. It is also known as clear box testing and open box testing. White box testing finds the design errors happened due to unsynchronized logical flow of the program and the real time program execution.

International Journal Of Scientific & Engineering Research, Volume 11, Issue 7, July-2020
ISSN 2229-5518

4. PEN TESTER?

A Penetration Tester (Pen Tester or Ethical Hacker) exploits security vulnerabilities in web-based applications, computer networks and systems. A pen tester gets to use a series of penetration tools –to simulate real-life cyber attacks. His ultimate aim is to help an organization improve its security. During the penetration test, a pen tester will typically focus on exploiting vulnerabilities. The major responsibilities of a pen tester are

- ✓ Incorporate business considerations into security strategies.
- ✓ Employ social engineering to uncover security holes.
- ✓ Perform formal penetration tests on web-based applications, networks and computer systems.
- ✓ Conduct physical security assessments of servers, systems and network devices.
- ✓ Design and create new penetration tools and tests.
- ✓ Pinpoint methods that attackers could use to exploit weaknesses and logic flaws.
- ✓ Research, document and discuss security findings with management and IT teams
- ✓ Review and define requirements for information security solutions
- ✓ Work on improvements for security services, including the continuous enhancement of existing methodology material and supporting assets
- ✓ Provide feedback and verification as an organization fixes security issues

5. PENETRATION TESTING TOOLS

Pen testers often use automated tools to uncover standard application vulnerabilities. Penetration tools scan code in order to identity malicious code in applications that could result in a security breach. Pen testing tools examine data encryption techniques and can identify hard-coded values, such as usernames and passwords, to verify security vulnerabilities in the system.

Penetration testing tools should:

- ✓ Categorize vulnerabilities based on severity.
- ✓ It must be easy to deploy, configure and use.
- ✓ It can scan a system easily.
- ✓ It must be capable of automating the verification of vulnerabilities.
- ✓ It can generate detailed vulnerability reports and logs.

Many of the most popular penetration testing tools are free or open source software; this gives pen testers the ability to modify or otherwise adapt the code for their own needs. Some of the most widely used free or open source pen testing tools include:

- The Metasploit Project is an open source project owned by the security company Rapid7, which licenses full-featured versions of the Metasploit software. It collects popular penetration testing tools that can be used on servers, online-based applications and networks.
- Nmap, short for "network mapper," is a port scanner that scans systems and networks for vulnerabilities linked to open ports. Nmap is directed to the IP address or addresses on which the system or network to be scanned is located and then tests those systems for open ports.
- Wireshark is a tool for profiling network traffic and for analyzing network packets. Wireshark enables organizations to see the smaller details of the network activities taking place in their networks. This penetration tool is a network analyzer/network sniffer/network protocol analyzer that assesses vulnerabilities in network traffic in real time. Wireshark is often used to scrutinize the details of network traffic at various levels.

6. STRATEGIES?

One important aspect of any penetration testing program is defining the scope within which the pen testers must operate. Usually, the scope defines what systems, locations, techniques and tools can be used in a penetration test. Here are several of the main pen test strategies used by security professionals:

International Journal Of Scientific & Engineering Research, Volume 11, Issue 7, July-2020
ISSN 2229-5518

6.1 Targeted Testing is performed by the organization's IT team and the penetration testing team working together.

It's sometimes referred to as a "lights turned on" approach because everyone can see the test being carried out.

6.2 External Testing targets a company's externally visible servers or devices including domain name servers, email servers, web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

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

6.4 Blind Testing simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team performing the test beforehand. Typically, the pen testers may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

6.5 Double-blind Testing takes the blind test and carries it a step further. In this type of pen test, only one or two people 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.

6.6 Black Box Testing is basically the same as blind testing, but the tester receives no information before the test takes place. Rather, the pen testers must find their own way into the system.

6.7 White Box Testing provides the penetration testers information about the target network before they start their work. This information can include such details as IP addresses, network infrastructure schematics and the protocols used plus the source code.

6.8 Pen Testing as a Service , PTaaS provides information technology(IT) professionals with the resources they need to conduct and act upon point-in-time and continuous penetration tests. Using different pen testing strategies helps pen testing teams focus on the desired systems and gain insight into the types of attacks that are most threatening.

7. BENEFITS?

7.1 Enhancement of the Management System It provides detailed information about the security threats. In addition to this, it also categorizes the degree of vulnerabilities and suggests which one is more vulnerable and which one is less.

7.2 Avoid Fines Penetration testing keeps your organization's major activities updated and complies with the auditing system.

7.3 Protection from Financial Damage A simple breach of security system may cause millions of dollars of damage. Penetration testing can protect the organization from such damages.

7.4 Customer Protection Breach of even a single customer's data may cause big financial damage as well as reputation damage. It protects the organizations that deal with the customers and keep their data intact.

8. CHALLENGES?

8.1 To Determine the Test Coverage

In the traditional penetration testing, the test scenarios are decided by their test coverage and it is one of the major test measurement criteria. The testers look for the test cases that support to achieve a high level of test coverage. However, when it comes to today's complex environment, it becomes challenging to determine the length as well as the breadth of the test coverage since this testing exercises only on the external network interfaces. To achieve proper test coverage, the test team requires going beyond the traditional constitutes of the penetration testing.

8.2 To Determine What Kind of Pen Testing is Required.

International Journal Of Scientific & Engineering Research, Volume 11, Issue 7, July-2020
ISSN 2229-5518

This is the most common question that comes across when one decide to go for pen testing. Most people recommend starting with external network interface testing. However, the proper answer to this question depends on nature of the business environment. The organization must understand its environment and budget to decide what kind of pen testing that their business requires. It is important to make sure that to invest in the right testing type which suits the company needs.

8.3 To Understand Difference Between Penetration Testing and Vulnerability Scanning

The most common challenge in the IT security services has been the often confusion as well as interchanging of terms, which people think refer the same thing but refers different. The same thing happens when it comes to, penetration testing, many people confused with the terms penetration testing and vulnerability scanning. They often misused and even swapped out these two terms. The penetration testers must understand that the main objective of the vulnerability scanning is to determine as well as evaluate possible vulnerabilities in the technical perspective, whereas the penetration testing attempts to exploit the determined vulnerabilities, which may result in unauthorized malicious access, modification, interception of normal organization process and data.

8.4 To Determine the Risk Associated with Disclosure of Sensitive Data and Failure of System

The risk associated with t issues encompasses the chances of occurrence of the undefined events and their ability for loss within the organizations. Knowing the impacts allows to plan for the unexpected failure or data leakage and that will support to ensure the success of the application. It also defines how to handle the risks hence the penetration tester can determine, mitigate and avoid security problems. Hence, the penetration test scenarios should be established which should accurately test the application and its components to find whether there is risky or not.

8.5 To Approve the Target and Regularity of Pen Test

The penetration test begins with the corresponding tester enumerating the target to detect vulnerable systems. The penetration testers should start their asset attacking attempt by learning their pen test targets. They must aware of the OS platforms, IP addresses; version numbers advertised network ports that can cause the chance to exploit.

9. CONCLUSION

Ethical hacking done with appropriate direction help us to discover the security vulnerabilities. Pen testing is more valuable to identify the security weakness in a system. It offers benefits such as prevention of financial loss, compliance to industry regulators, customers and shareholders, preserving corporate image, proactive elimination of identified risks. It is useful to prevent loss of data, financial loss and proactive elimination of identified risks. Implementing penetration testing through regular auditing, intrusion detection and good system administration once can secure the sensitive data and protect valuable information from hackers. In conclusion ethical hackers use their knowledge and network skills to discover the security vulnerabilities and enlighten the customer, business and secure the system.

REFERENCES

[1] Agarwal, Ankit Kumar, Hacking : Research paper, online http://ankitkumaragarwal.com /hacking-a-research-paper.

[2] Wilhelm, Douglas. "2". Professional Penetration Testing.Syngress Press. p. 503.ISBN 978-1-59749-425-0

[3] Moore, Robert (2006). Cybercrime: Investigating High-Technology Computer Crime (1st ed.). Cincinnati, Ohio: Anderson Publishing. ISBN 978-1-59345-303-9

[4]EC-Council (n.d.). Ethical Hacking and Countermeasures,onlinehttp://www.eccouncil.org/ipdf/EthicalHacker.pdf .

[5] Ethical Hacking Basics Class part , online http://www.go4expert.com/forums/showthread.php

[6] Palmer, C.C.(2001,April 13). Ethical Hacking. IBM Systems Journal Vol. 40 No.3 2001 About Effective Penetration Testing Methodology byByeong-Ho KANG.

[7]"ApplicationPenetrationTesting,"https://www.trustwave.com/apppentest.php, accessed on Nov. 23, 2011.

International Journal Of Scientific & Engineering Research, Volume 11, Issue 7, July-2020
ISSN 2229-5518

[8] Mullins, M. (2005) "Choose the Best Penetration Testing Method for your Company,"http://www.techrepublic.com/article/choose-the-best-penetration-testing-method-for-yourcompany/5755555, accessed on Nov. 23, 2011.

[9] Saindane, M. "Penetration Testing – A Systematic Approach," http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf, accessed on Nov. 23, 2011.

[10] "Nmap – Free Security Scanner for Network Explorer, http://nmap.org/, accessed on Nov. 23, 2011.

[11]Sanfilippo, S. "Hping – Active Network Security Tool," http://www.hping.org/, accessed on Nov. 23, 2011.

[12]Superscan,http://www.mcafee.com/us/downloads/free-tools / superscan.aspx, accessed on Nov. 23, 2011.

[13]"White Paper on Penetration Testing," http://www.docstoc.com/docs/70280500/White-Paper-onPenetration-Testing, accessed on Nov. 23, 2011.

[14]Neumann, P. (1977) "Computer System Security Evaluation," Proceedings of AFIPS 1977 Natl. Computer Conf., Vol. 46, pp. 1087-1095.

[15]Pfleeger, C. P., Pfleeger, S. L., and Theofanos, M. F. (1989) "A Methodology for Penetration Testing," Computers &Security, 8(1989) pp. 613-620.

[16]Bishop, M. (2007) "About Penetration Testing," IEEE Security & Privacy, November/December 2007, pp. 84-87.

[17]Arkin, B., Stender, S., and McGraw, G. "Software Penetration Testing," IEEE Security & Privacy, January/Feburary 2005, pp. 32-35.

[18]"Penetraion Testing Guide", http://www.penetration-testing.com/.

.