ISSN:2320-0790

An International Journal of Advanced Computer Technology

Penetration Testing: A Review

Kumar Shravan[1], Bansal Neha[2], Bhadana Pawan[3]

[1]Research Scholar, PG, Dept. of CSE, B.S.A.I.T. M, Faridabad
[2]Asst. Professor, Dept. of CSE/IT, B.S.A.I.T.M, Faridabad
[3]Associate Professor, Dept. of CSE/IT, B.S.A.I.T.M, Faridabad

Abstract: Network Security is becoming more and more crucial as the volume of data being exchanged on the Internet increases. When people use Internet, they have certain expectations. They expect confidentiality, data integrity and authentication (CIA Standards). In 1980's most organizations had only a physical boundary that needed protection of the assets. Today, due to the changes in the way resources are made available Organizations are forced to verify that their assets are protected from both the external and internal threats that our working environment has enabled. Due to the increasing dependency of our society on networked information system the overall security of these systems should be measured and improved. The most accurate method to evaluate organization's information security stance is to observe how it stands up against an attack. Network administrators have often tried their best by improving their network security, however with rapid surface of new exploits; the best way of ensuring that the system is secure is to attempt penetration testing. This would be the most effective way to find exploits and to proof whether a system is vulnerable. Penetration testing often allows the security analyst to find new vulnerabilities.

Keywords: confidentiality, integrity, authentication, threats, vulnerability, penetration testing.

A. Introduction:

There are many methods of security assessment such as audit trails and template applications. Penetration Testing aims at finding and identifying Exploits and vulnerabilities that exist within an organization's IT infrastructure and helps to confirm whether the current security measures implemented is effective or not. Penetration Testing helps to identify what is the information that is exposed to the public or the Internet World. Existing security metrics have generally focused on measuring individual vulnerabilities without considering their combined effects. The effectiveness of security testing depends on the skill and experience of the testers. Security testing also requires a special kind of insight that cannot be systematized. The current practice on security only focuses [4] on specifics, such as firewall testing, web server testing etc. A generic model is not available for security aspirant to use a guideline when doing penetration testing, as compared to any other field, such as software engineering.

B. Penetration Testing:

"Penetration Testing is the process of validating that the securities of our assets in our entire environment meet the CIA standard [5] as specified by the company." It is a form of stress testing, which exposes weaknesses of flaws in a computer system. It is more art of finding an open door from where attack is possible.

Penetration testing is a testing technique for discovering understanding, and documenting all the security holes that can be found in a system. It is an authorized attempt to violate specific constraints stated in the form of a security or integrity policy. It is a test for evaluating the strengths of all possible security holes and provides suggestions for fixing them. This testing typically includes network penetration testing and application security testing as well as controls and processes around the networks and it should occur from both outside the network trying to come in (external testing) and from inside the network(internal testing).

Confidentiality: Confidentiality means that the sender and the receiver both expect privacy. The transmitted message should make sense to only the intended receiver. To all others, the message should be unintelligible. A good encryption/decryption technique guarantees to some extent that a potential intruder cannot understand the contents of the message.

Integrity: Data integrity means that the data must be arrive at the receiver exactly as it was sent. There must be no changes during the transmission, either

accidental or malicious. As more and more monetary exchanges occur over the Internet, integrity is crucial. For example: It would be disasters if a request for transferring $100 changes to a request for $1,000 or $10,000.
The integrity of the message should be preserved in a secure communication.

Authentication: Authentication means that the receiver is sure of the sender's identity and that an imposter has not sent the message.

Threats: A threat is any event that could create loss in damage that could affect the CIA standard of the asset.
It can be both intentional, such as malicious modification of sensitive data, and accidental, such as deletion of a file.

Vulnerabilities: It is best defined as a weakness that can be exploited by a threat to our assets, whether it is people, data, hardware, or software that allows intruders to infiltrate our security environment.

C. Objectives of Penetration Testing:

For a successful penetration test that meets the client's expectations, the clear definition of goals is absolutely essential. If goals cannot be attained or cannot be achieved efficiently, the tester should notify the client in the preparation phase and recommend alternative procedures such as an IT auditor IT security consulting services.
Client goals that can be attained by penetration testing can be divided into four categories:

1. Improving security of technical systems
2. Identifying vulnerabilities
3. Having IT security confirmed by an external third party.
4. Improving security of organizational and personnel infrastructure.

The result of an IT penetration test should therefore be more than just a list of existing vulnerabilities; ideally it should also suggest specific solutions for their elimination.
These four goals are discussed below, with examples.

Improving Security of Technical Systems

Most penetration tests are commissioned with the objective of improving the security of technical systems. The tests are confined to technical systems such as firewalls, routers, web servers, etc., with organizational and personnel infrastructure not being explicitly tested. One example is a penetration test to expressly check whether unauthorized third parties are able to access systems within the company's LAN from the internet. Possible test results of findings are unnecessary open firewall ports or vulnerable versions of internet applications and operating systems.

Identifying Vulnerabilities

In contrast to the other three goals, identification is the actual objective of the test. For example, before combining two LAN's in the wake of a company merger, the new LAN can be tested to see whether it is possible to penetrate it from outside. If this can do in the penetration test, action has to be taken to secure the interface the merger, or the two networks should not be combined at all.

Having IT Security Confirmed by an External Third Party:-

A penetration test can also be conducted to obtain confirmation from an independent external third party.
It is important to note that a penetration test only ever reflects the situation at a particular point in time and cannot therefore yield assertions about the level of security that are valid in the future.
Nevertheless, regular penetration testing may be suitable for demonstrating the increased security of customer data in a web shop or other internet application.

Improving Security of Organizational and Personnel Infrastructure:-

Apart from testing the technical infrastructure, a penetration test can also test the organizational and personnel infrastructure, to monitor escalation procedures, for instance, with the scope and/or aggressiveness of the tests being increased step by step. Social engineering techniques, such as requesting passwords over the telephone, can be employed to assess the level of general security awareness and effectiveness of security policies and user agreements.

D. Process of Penetration Testing [1]:

The process f penetration testing is shown in the given figure. It can be broadly divided into four phases:

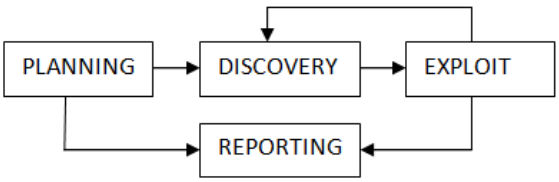

Figure: Penetration testing methodology diagram

1. Planning:-

Initially at the planning phase, the scope for the assignment is defined. Management approvals, documents and agreements like NDA (Non Disclosure Agreements) are signed under the guidance of responsible legal departments and lawyers. After the management consent, the penetration testing team gathers crucial input about the organization operational procedures and security policies, towards defining the scope for the test.

2. Discovery:-

Following the initial planning, the actual penetration test starts with the discovery phase, also known as information gathering phase. During the information gathering process the penetration testing team launches scanning and enumeration procedures to gain as much information as possible about the target network and the participating systems and services .The gathering phase can be further divided into non-intrusive (public repositories, documents, mailing lists, web profiles etc.) and intrusive(port scanning, firewall rules, matching OS fingerprints etc.)Inspection processes. Having adequate amount of information the testing team can profile the target network and enumerate possible or personal security knowledge bases.

3. Exploitation phase:

The third and most important phase of a penetration test is the exploitation phase. Using as input the discovered vulnerabilities arriving from the previous phase, the penetration testing team revises matching proof-of-concept exploits that may lead to a network or service security bridge. Depending on the agreement with the management and the exploitation implication level, the attacks can be launched either in an identical network vulnerabilities and mis-configurations, the testing team might discover additional information that can feedback the discovery phase, resulting in new attack scenarios and exploits. This interaction between the discovery and exploitation phases is continuous throughout the actual test.

4. Reporting Phase:-

The last phase that completes a penetration test process is the reporting phase. The report writing can begin in parallel to the other three stages, although must finish after exploitation phase has been completed. A successful report details all the findings and their impacts to the organization by taking into account both the technical and management to conduct a fully detailed and well documented report in order to inform the management about the security risks and provide technical details and high level recommendations to the ICT department.

E. Types of Penetration Test

Penetration testing normally depends upon what an organization wants to test, whether the scope is to simulate an attack by an insider or an external source. The three widely accepted approaches are Black-box, White-box and Grey-box. The main difference between these approaches is the amount of knowledge of the implementation details supplied to the tester about the system to be tested.

Black-box testing: The black-box testing is also referred as “external testing” or “remote penetration testing”. In this approach, testers simulates an attack as someone who have no prior knowledge of the infrastructure to be tested by deploying the number of real-world attack techniques (e.g. Social Engineering, Network Scanning, remote access, Trojans etc.) and following the organized test phases. For example, testers will be only provided with the organization’s website or network IP address rage. Therefore, the testers simulate all hacking techniques that may reveal some known and unknown set of vulnerabilities existed on the network. The main goal behind the black-box penetration test is to verify the integrity of an organization’s network and proactively reduce risks from an outside as well as inside attacks.

White Box Testing:-

The white box-testing is also referred as “internal testing”. In this approach, testers simulate an attack as someone who has knowledge of the infrastructure to be tested. Often including OS details IP addresses schema and network layouts, source code, and possibly even some passwords. For example: testers try to setup “backdoor accesses “that might be used to gain remote access once the internal security has been breached. The main goal behind the White box penetration test is to verify the integrity of organizations networks and proactively reduce risks from an internal individual like disgruntled employees.

The combination of both types of penetration testing provides a powerful insight for internal and external security view point. This combination is known as Gray-box testing. In this approach testers have or are provided with some knowledge and are put in a privileged position. It is a preferred method when cost is a factor as it saves time for the pen-testing team to uncover information that is publicly available. It is not the matter of which approach is superior to the other, but these approaches should be performed in a combination to bring more value to the organization. It will help to eliminate any internal or external security issues lying at the organizations infrastructure environment for an attacker to infiltrate.

For this, related information is provided to pen test teams to assess the security against specific attacks or specific targets. This method is chosen when the company needs to get a complete audit of its security.

Gray-box Testing:

In this testing, some knowledge is provided to the testers but this testing puts the tester in a privilege position. This would normally be a preferred method when cost is a factor as it saves time for the pen testing team to uncover information that is publicly available. Also, that approach would be suitable when the organization needs to obtain knowledge of the security assessment practices.

F. Phases of Penetration Testing [2]

There are three phases in a penetration test and the attacker could use these phases to conduct a real attack. These phases include the pre-attack phase, the attack phase, and the post-attack phase as show in the figure below:

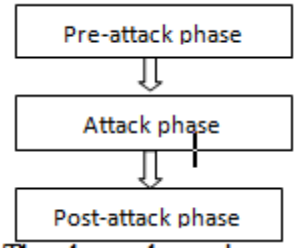

Figure: The three phases in a penetration test

The activities that take place in each phase depend on how the rules of engagement have specified the way penetration test be conducted.

The Pre-Attack Phases:- The pre-attack phase consists of penetration testing work or hacker's attempts to investigate or explore the potential target. This reconnaissance effort is normally categorized into two phases: active reconnaissance and passive reconnaissance.
Beginning with passive reconnaissance, which does not "touch" the network and is therefore undetectable by the target organization, the hacker or penetration tester will gather as much information as possible about the target company. Once all available sources for passive reconnaissance have been exhausted, attacker may get into active reconnaissance.

The Attack-Phase:-The attack phase involves the actual compromise of the target. Hackers may exploit a logical or physical vulnerability discovered during the pre-attack phase or use other methods such as a weak security to gain access to a system.

The Post-Attack Phase:-The post-attack phase is unique to the penetration test team. It focuses on returning any modified system(s) to the pretest state. With the exception of masking their tracks, real attackers care less about returning a compromised system to its original state. The longer the system remains compromised, the longer they can legitimately claim credit it includes reversal of each change made to the network to restore it to its pre-attack state. Some of the activities to accomplish are: removal of any files, tools, exploits or other test-created objects uploaded to the system during testing.

G. Methods

There are several ways of manipulating or damaging IT systems and of preparing an attack on IT systems.

Network-based attacks:-
"Network-based attacks" are attacks on network components, computer systems and/or applications using network protocol functionalities. This kind of attack exploits vulnerabilities or inadequacies in hardware and software in order to prepare or carry out attacks. Network-based attacks include port scanning, IP spoofing, session hijacking, DoS attacks, buffer overflow and format string attacks, swell as all other exploitation of vulnerabilities in operating systems and network protocols.

Social Engineering:-
Social Engineering attacks are attempts to manipulate people with privileged knowledge to make them reveal security-related information such as passwords to the attacker. For instance, an attacker could pretend to be an IT employee of an organization and trick an unsuspecting user into revealing his network password. The range of possible attack scenarios is particularly wide with this technique. In its broadcast sense, social engineering can also cover situations in which security related information is obtained by extortion.

Circumvention of physical security measures:-
There can be no IT security without the physical security of the technical infrastructure, if physical security can be defeated and physical access to IT systems gained, it is usually only a matter of time before an attack on or manipulation of stored applications and data can take place. An example is the unauthorized entry into the computer center of an organization and the removal of a hard disk on which confidential data are stored. This category also includes the searching of waste for documents with sensitive security-related information (dumpster driving).

H. Limitations of Penetration Test

Penetration tests are useful practices that can have tremendous value to tighten security of any system or product. However, penetration tests have limitations. First, penetration tests might not identify all the vulnerabilities due to time restriction or a project-focused test's limitation. Most organization cannot test everything, because of resource and time restriction but in real-world attackers may find flaws in areas that were not part of the penetration test project's scope. The attackers have ample amount of time to plot their attack, plan it out, whereas most

penetration tests processes just last for a short span of time. Furthermore, while a methodology can be followed, penetration testing is not an exact science. For example, one tester may examine multiple low risk vulnerabilities and when reviewed individually may conclude no serious risk exists. On the other hand, next tester, through experience, may see that when the individual low risk vulnerabilities are taken as a whole, they lead to a significant compromise of the environment. In addition to the limitations of project-focused tests and the time restriction, penetration testing is limited by the current known exploits4which are available publicly. Normally testers do not write their own exploits but instead rely on exploits written by others. Even for those testers who do write exploits, often there is not enough time to create a custom exploit for a newly discovered a flaw in a given target environment.

However, penetration test only provides no improvement in the security of a computer or network system, nor it guarantees that a successful attack will not occur, but it does significantly reduce the likelihood of a successful attack if the actions are taken to address vulnerabilities that were found as a result of conducting the penetration test. Although, penetration tests cannot replace the traditional IT security tests, nor is it a substitute for a general security policy but it supplements the established review procedures and tackles the new threats to effect of a penetration test is, however, relatively short-lived. The more protection the systems require, the more often penetration testing should be done in order to reduce the likelihood of a successful attack.

Testing usually requires a careful selection process under which one can determine the accountability, cost, and effectiveness of the assessment at optimum level. Thus, determining the right assessment strategy depends on several factors, including the technical details provided about the target environment, resource availability, Pen Tester' knowledge, business objectives, and regulatory concerns. A penetration testing methodology is like a "map" using which tester can reach to the final destination (i.e. end of a successful test).
Before a penetration test, certain key issues need to be placed in order to ensure useful and timely results. It includes the technical requirements such as time Constraints; cover the full range of the threats, the range of IP addresses over which the test is to be conducted and the systems that are to be attacked and also those that are not to be attacked as part of the test with minimal disruption to normal operation. Other requirements may also include legal and contractual issues specifying liability, information to individuals regarding the test taking place. Such requirements can vary depending on legal structures in the organization or even the host country of the organization. Beside above mentioned requirements, there are a number of ethical and technical competency issues that penetration testers face in conducting test, from testing systems or protocols not explicitly included or excluded from a test. Although Code of Conduct and Best Practice is laid out by numerous professional bodies, in actual practice the penetration tester is often required to take an informed decision given a particular situation. Therefore, the tester should possess the necessary procedures, ethical and technical training to ensure the penetration tests are conducted correctly and does not lead to a false or misleading sense of security.

I. Requirements:-

1. Obtaining written approval from management should be the first step before penetration validation can commence. This is critical and often a minimum requirement from a penetration tester's perspective, with respect to legality issues.
2. A term of agreement should be established in the interest of the organization and the pen testing team's liability. The terms provide guidelines for the testers and means of interaction between the organization and the pen testing team.
3. Yet another basic requirement is the project scope of the pen test validation. Scope can be specific target systems or a comprehensive validation covering as much vulnerability throughout the entire organizational structure, on what is expected and what are the required deliverables in the form of documentation, and recommended corrective measures to safeguard the assets. A well define scope makes the penetration validation a feasible goal to obtain.
4. Liability insurance is another basic requirement that the pen testing team needs to provide the organization. This is necessary to cover expenses for faults caused by the pen testing team, making them liable for their actions.
5. Service level agreements (SLAs) [5] should be provided by the pen testing agency. They define the terms of services that are provided. Normally such SLAs cover both solutions and penalties. In general, SLAs dictate the minimum

levels of availability and the consequences of disruption of services.

J. Problem Statements:-

A methodology describes a set of rules, practices, procedures, and methods that are followed and implemented during the course of any information security audit program. A penetration testing methodology is a series of

All the problem statements are related to

The problem statements are:-

1. Investigate Penetration Testing tools and techniques.
2. Design and Setup an Isolated Network Laboratory to perform Penetration Test.
3. Investigate and identify a suitable Penetration Testing Methodology.
4. How a Network and System Administrator can utilize Penetration Testing to understand, analyze and address security issues?

K. **Conclusions**:

Apart from testing the technical infrastructure, a penetration test can also test the organizational and personnel infrastructure, to monitor escalation procedures; with the scope and/or aggressiveness of the tests being increased step by step. Social engineering techniques, such as requesting passwords over the telephone, can be employed to assess the level of general security awareness and the effectiveness of security policies and user agreements. The scope of such tests needs to be defined precisely in advance. The success of any penetration test depends on the underlying methodology. Although all the mechanisms are common security solutions deployed to ensure a data protection, and assist the Network and System Administrators in collecting, tracking and reporting the status of known security issue, but everyday new vulnerabilities, threats are discovered. News of security breaches and data theft are heard, which leads to arising questions. Are the security mechanisms sufficient for today's evolving network to combat against Cyber criminals? Should security mechanisms needs to be tested? These security mechanisms solutions address only a portion of a security concerns and are likely to face many only a portion of a security concerns and are likely to

rules or guidelines used to perform penetration testing on a computer system or network. Thus, penetration testing methodology works as a roadmap with practical ideas and proven practices which should be handled with great care in order to assess the system's security correctly.

It should also take account of the limited time available and must include an assessment of the potential risk or a cost analysis.

penetration testing, tools and penetration testing methodology.

face false positives. These false positive reports are misleading and can severely complicate the Network and System Administrator's ability to distinguish the different severity tasks.

Hacking [3] is now an issue that does not have any conclusion. The only way we can stop a hacker is by learning hacking. By learning we can read the minds of a hacker which enables us to know the reality. Hacking is not a crime but it is made a crime by misusing the knowledge of programming. Every hacker is a perfect programmer even more than a normal programmer. Everyone should know the ethics of hacking and follow them to be safer.

References:-

[1] Aiming at Higher Network Security through extensive penetration tests. IEEE Latin America Transaction, Vol. 10, No.3, April 2012

[2] A Research of Behavior-Based Penetration Testing Model of the Network 978-0-7695-4792-3/12 $26.00© 2012 IEEE

[3] A Study of Network Security using Penetration Testing

[4] Development of Penetration Testing Model for increasing Network Security 0-7803-84822/04/$20.00 (c) 2004 IEEE

[5] Penetration Testing (Allen Melmeg).