International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 8 5297 - 5302

# Evaluation and Taxonomy of Penetration Testing

Arpita Tewai
Department of Computer Science and Engineering
Motilal Nehru National Institute of Technology, Allahabad
*tewari_arpita@yahoo.com*

Arun Kumar Misra
Department of Computer Science and Engineering
Motilal Nehru National Institute of Technology, Allahabad
*akm@mnnit.ac.in*

***Abstract-*** The dependence of organizations on networks/Internet for efficient operations and services to customers has made the network security issues a vital one. In the present paper penetration testing manners and technologies are first surveyed and then analyzed in the real world context. Penetration testing has been performed mid/large cooperate organization pointing to certain conflicts in the requirements of testing. The paper also discusses about the processes and methodologies of today's trends that also undergo continuous changes due to rapid technological developments. Some complications in penetration testing have also been highlighted and requirements for adopting the technique in modified way have been discussed. The paper further describes different phases of penetration testing techniques and we have also purposed a new methodology that is able to resolve the shortcoming of existing one. Penetration testing has been performed mid/large cooperate organization pointing to certain conflicts in the requirements of testing.

***Keywords:*** *Penetration, Network Security, Gray box, White box, Black box, Vulnerability Scanning.*

*****

## I. INTRODUCTION

Efforts put by companies and organizations in doing global business through Internet have made security issues a vital one. Companies accessing the Internet are seeking methods of protecting their network sites against external attacks and intrusions. Setting up a firewall, one of the best solutions, for private network sites in organizations and at home is no longer a fancy thing. Penetration impact may cause major concerns, such as: Is there a significant privacy in uncovering that may be a great cause of loss while incorporating a secure environment using a firewall for the Internet connection? Or "To what level of security should we expect without sacrificing the available network security?" This paper addresses the above queries and about the design of a secure network by performing pure security through penetration testing on firewall at different security levels. "Testing validates and ensures that controls specified in the Security Plan are functioning properly". [7, 24]

A penetration test is not just a mere hacking exercise. It is a very essential part of the complete Risk Assessment Strategy of the organization. If used effectively, penetration test is an effective tool by which any organization can measure the current security level of its network and systems. It is suggestive in literature [31], to have a penetration test done at regular intervals.

The organization of the paper is as follows: In II section Requirement satisfaction for penetration testing is defined. Types of pen test are discussed in III section. In IV section the contribution of penetration test in network security are discussed. Comparison of penetration with others is done in V section. Tools available for penetration testing are described in VI section. Related researches are given in VII section. The benefits and challenges of penetration testing have been described in section VIII. In IX section a modified architecture for penetration testing to improve the efficiency has been proposed. Proposed methodology and its description have been given in section X. Lastly the conclusion is given section XI.

## II. REQUIREMENTS FOR PENETRATION TEST

Requirements for Penetration testing should be realistic, because it deals with an attack performed by real opponent. Respect of employees during testing is a major issue. They should not be deceived. Penetration testing should also be reliable and reportable. Penetration testing should fulfill following five requirements, which are known as R* requirements [2].

***Restriction*** -Employees should not act or behave during testing as they would act and behave in everyday life.
***Respect*** -All the employees are treated with respect during testing. Employees should neither be stressed, pressured, and uncomfortable, nor feel risk and should maintain mutual trusts amongst themselves.
***Reliable*** -Penetration testing should not become a cause for the productivity loss of the employees.
Repeatable -Testing is repeated many times and incase the environment does not change then the result of the testing should be same.
***Reportable*** -All the actions during the testing should be logged and the output of the test should be in a form that allows a meaningful and actionable document of findings and recommendations [2, 3].

 ISSN: 2321-8169
5297 - 5302

## III. Types of Penetration Test

Following types of penetration testing are in practice [8, 14]:

*Black box*—Testers do not have the full information about the internal environment of the organization. They have the data which is publically available. This type of test is used to perform a real pen test since attacker starts with no knowledge about the system. It is also known as zero knowledge tests. Black box testing is best conducted from outside.

*White box*—Testers have full knowledge and information about the target system. Unlike black box in which experts are required to go through the code step by step and identify the faults due to which there may a possibility to attack. This is also called source code analysis because tester has full information about the application and source code.

*Gray box*— It is known as partial knowledge test and tester has partial knowledge about the organization.

## IV. The contribution of penetration in network security[4]

Earlier, penetrations were mainly attempted from the inside of a network but with the advent of Internet; networks are vulnerable to attacks from all over the world [23]. A firewall provides improved security [5] and has a way of controlling access to our systems and networks. Steps involved to a successful penetration testing for network security are as follows—

Detect the process mostly used by an attacker for attacking a system or organization.

Identify the weak points of the system or organization which need to be defended.

Determine how the attacker uses these weaknesses.

Identify the assets that can be used, manipulated or destructed by an attacker.

Check that an attack by an attacker was detected.

Check what the footprints of an attack look like?

Prepare some favorable comments.

## V. Comparison of Penetration testing with others [25, 28]

| Types of test | Strength | Weakness |
|---|---|---|
| 1.Penetration Testing (a)Traditional penetration testing | Its major focus is in verifying technical vulnerabilities by using various methodologies and tools. | It is very labour intensive and requires great proficiency. Having proper set of tools is very complex and expensive. |
| (b)Risk based penetration testing Vulnerability Scanning | It not only verifies the vulnerability but also explains how these vulnerabilities can gain enormous access. It requires both technical and professional knowledge but mainly concerns with professional risks. It works under critical situation of corporate and application. | Usually insider works because persons must have knowledge and skills of corporate process. It is essential to understand the rules and regulations of corresponding body. |
| 2.Network Scanning | It is faster than vulnerability and penetration testing and highly automated. It effectively scans the number of hosts in the network with minimum cost. | It is used in preceding part of penetration testing and not executed as final test. It involves expertise skills to execute result. |
| 3. | It is highly automated but speed depends on the number of hosts scanned. It not only identifies but also provides solution for mitigating known vulnerabilities and on regular basis. | Sometimes identify only exterior vulnerabilities and is often unable to detect recent vulnerability. Generally identified by IDS, firewall or even end users and as such is not able to maintain secrecy. |

## VI. PENETRATION TESTING TOOL

Many testing tools are used by testers in organization to test the network or system for security purpose. Some of these tools are described below:

*Nmap*: Nmap allows for a variety of different types of port scans to be used in order to determine whether a port is open or closed. [11,25]

*Nessus:* Premier UNIX vulnerability assessment tool. Nessus is a fast and modular vulnerability scanner released by Renaud Deraison. The freeware client/server tool audits a network remotely to enumerate and test the known vulnerabilities against a database that is updated daily by the Internet security community in the form of plug-ins. [11]

*Metasploit* Framework: It is an advanced open-source platform for developing, testing, and using exploit code. The extensible model through which payloads, encoders, no-op generators, and exploits can be integrated has made it possible to use the Metasploit Framework as an outlet for cutting-edge exploitation research. [11]

## VII. RELATED RESEARCH

DTI [18] recommends that, "Draw on the right expertise and international standards to understand the security threats and legal responsibilities. Integrate security into normal business practice, through a clear security policy and staff education. Use risk assessment to target investment in security controls at the areas of maximum business benefit.

Stephen Northcutt et.al[19] & [20] have emphasized that by performing penetration tests against environment, replicate the types of actions that a malicious attacker would take, giving a more accurate representation of security posture at any given time.

N. Y. Hamisi et.al[21] have observed that the objectives of using penetration test methods in an organization's LAN were to identify different form of network attacks and methods used to capture the hacking. The risks and attacks caused by hackers to the network were evaluated. The results obtained are seen as a good indicator of the security state of the network. The network administrator permitted network information like internet protocol (IP) address to be gathered and analyzed and to perform the penetration test that enabled hackers and attackers methods to be identified. It was realized that 90% of network users has no fear of the network security risk inspite of the finding that network security rating of the case study is at 50 percent.

Bing Duan et. Al. [22] state that penetration testing is an important branch of network security evaluation, which aims at providing all-round investigation to find the vulnerabilities and security threats in systems and networks.

According to [35], hackers are unauthorized but that doesn't mean we can't perform an analysis of hacking. The goal of the hacker is to maximize some set of stated goals (Theft, Revenge etc.) while at the same time minimizing his risk. The defender, on the other hand, is looking to amplify the risk to the hacker while minimizing his exposure to potential abuse. From the methodology in [35], hackers begin by selecting and foot printing a target network. Once the target network is mapped, hackers proceed to map vulnerabilities and gain access by cracking passwords, using stack-smashing attacks, or spoofing the IP address of trusted machines. Hackers can then sniff internal network traffic or find other hosts that contain vital company secrets. Finally, a hacker can clean up system logs in order to conceal the fact that an attack occurred.

The Overall methodology for penetration testing [34] can be divided into three steps process:

Network enumeration: Discover as much as possible about the target.

Vulnerability analysis: Identify all potential avenues of attack.

Exploitation: Attempt to compromise the network by leveraging the results of the vulnerability analysis and finding as many avenues identified as time allows.

Above steps implies that discover as much as possible about the target, identify all potential avenues of attack, and attempt to compromise the network by leveraging the results of the vulnerability analysis.

## VIII. BENEFITS AND CHALLENGES OF PENETRATION TESTING

*Benefits*

Penetration testing has become a very important part of evaluating and ameliorating the security of an organization's or system's network. The focus of pen testing is to improve the security of a network seeking to compromise that system using a technique used by an attacker. There is confusion between vulnerability scanning and pen testing. A vulnerability scan determines the faults or problems which may already exist, whereas pen test evaluates against a real attack. Penetration test is active and is able to attack a system and evaluate its readiness. On the other hand vulnerability scan is passive and it does not identify the significance of an intrusion and only lists the possible potential vulnerabilities. The penetration testing is an authorized way to break the architecture of a system using attacker's technique.

***Challenges***

Though there are many challenges that can provide good opportunity to find out better solution to disable them and achieve better quality, major challenges of penetration testing in today's scenario are as follows:

*Limited time pressure*- In penetration testing it would take time to find out vulnerabilities in network and their patch up.

*Security*- "Is network hacker proof"? This is another major challenge for penetration test and it does not provide full proof either from hacker or from network flaws but can only mitigate them.

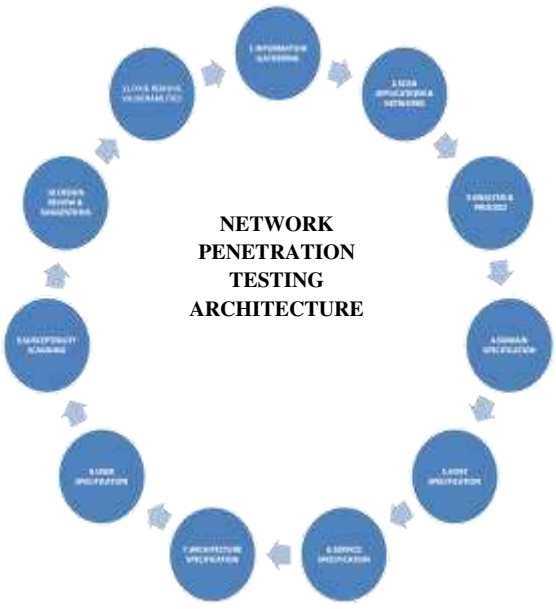
*Test automation*- Automation can be performed by using several tools that can reduce test execution time and perform regression testing after some modification or enhancements.

Penetration testing is undoubtedly a reliable way to solve security problems which network faces. If performed regularly and consistently as a part of security policy then organization's overall security definitely improves

## IX. PROPOSED ARCHITECTURE

Security Compass [23] provides an architectural recommendation layers that compete with an attacker to gain access to the internal network. This architecture iterates through the steps: Information gathering, domain enumeration, Host enumeration, Service enumeration, Architecture enumeration, User enumeration, Vulnerability scanning, Architecture review/recommendation and Vulnerability exploitation.

Though, scan and analysis of either application or network is essential for moving ahead in penetration testing cycle, the architecture proposed in [23] does not focuses on these. In the present paper, architecture for penetration testing has been proposed to overcome these limitations and also suggestions have been made to fix and remove vulnerabilities if detected. Three new states i.e. Scan application and network, Analysis and proceed and Fix and remove vulnerabilities are added. The proposed modified architecture is shown in figure below:




**Details of the proposed modified architecture:**

The proposed modified architecture is a modified one of the proposed architecture described in [28] and has three new states added as described earlier i.e. "Scan applications and networks", "Analysis & Proceed" and "Fix and remove vulnerabilities". Following are the details of the steps involved in the proposed modified architecture. The original steps have been retained as in [28].

***Information gathering*:** During this step data and background information are collected from internet which is related with company to create a business profile of the company.

***Scan applications and networks*:** This step covers the scanning process of applications as well as network by using various scanning tools suitable for application and network.

***Analysis and proceed:*** Outcomes of scan and other related information are analyzed here. This will improve the efficiency of penetration testing process.

***Domain specification*:** To successfully deal with flaws, a detailed network map is developed without having any previous knowledge about the network of an organization and its structure. Further a detailed description of design criteria for a domain is provided.

***Host specification*:** Various network scans are performed to identify the hosts in the network and also to make it confirm that company is the one who owns the network blocks.

***Service specification*:** Firstly hosts are identified and next the services provided by each hosts including the versions number of the services are described by using Internet data.

***Architecture specification*:** The details of information an active attacker can gather about the network from the internet and detailed access control are elaborated by the architectural diagram for clear understanding of the client.

***User specification*:** User specifications such as, user name, password etc. and brute-force i.e. try all possible values, authentication attacks on all the services provided by Internet and application and devices connected to Internet are identified.

***Susceptibility scanning*:** It is necessary to make sure that raw results are not provided after scanning. So tools are used for this purpose. Nessus and Nmap tools are used for susceptibility scanning. Firstly, identification of all the IP addresses that are connected to the Internet is done and then tools are used for susceptibility scanning.

***Design reviews and suggestions*:** Suggestions about the vulnerabilities which are removed in this cycle and also about the remaining vulnerabilities and how to resolve these vulnerabilities are made. Suggestions made in this phase, helps the tester to move in the right direction to remove the vulnerabilities remaining after this cycle.

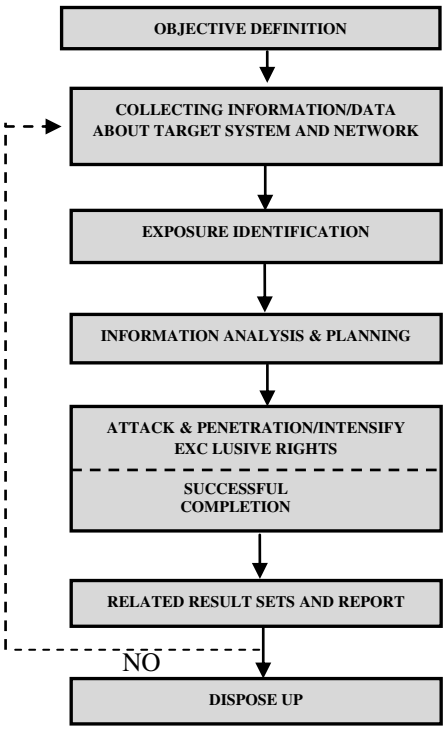
***Fix and remove vulnerabilities*:** It involves running exploits and determines the depth of access that an attacker can gain

from the internet. If possible then remove these vulnerabilities otherwise take them for further considerations.

## X. PROPOSED METHODOLOGY AND ITS DESCRIPTION

CORE IMPACT [23] has a seven step methodology for penetration testing, consisting of scope definition, information gathering, vulnerability detection, information analysis & planning, attack & penetration/privilege escalation, result analysis & reporting and clean up. These seven steps form a complete testing process. All the steps are essential to perform a successful penetration testing. If any step is skipped, some vulnerability may be remaining in the targeted system or network. The shortcomings of this model are as follows:

IP addresses are not verified in this model. This model does not clarify that which type of information is gathered during information gathering step.Special circumstances are not reviewed in this model.Vulnerability issues are not classified. To overcome these shortcomings the following seven step methodology is proposed.




The steps involved in the proposed methodology for penetration testing are as follows:

*Step 01—Aim/Objective definition*

The primary goal of penetration testing is to gain access to software systems that require authorized access and documenting all the security holes that can be found in a system or network.

*Step 02—Collecting information /Data*

This phase of penetration test is to collect information that concentrates on technical features of the target system or network as well as publicly available information related with owner, user and tester.

*Step 03—Exposure Identification*

In the selected system or network, identification of exposure can be performed manually or with the help of software like scanners that automatically scans the software vulnerabilities.

*Step 04—Information analysis and planning*

In this step comparison of technical public information that are collected from previous phases. Further, tester can collect the information in proper sequence and begin high level attack planning. From overall penetration approach it is tricky to identify which information is needed for further research.

*Step 05—Attack and penetration /Intensify exclusive rights*

In this phase, successful completions of previous phase are essential and fragmented down in convenient small parts such as available: Employ selection in which tester take out publicly available information and software programs to manipulate the faults identified. Employ reformation, here tester must modify the mistreat information or software program to execute according to object against their desired target. Employ expansion in it tester writes its own program for the specific target host, in case where no vulnerable program exist. Employ testing in formal penetration test each activity must be examined to avoid any harm which gets improperly executed if susceptibility identified.

*Step 06— Related result sets and Report*

In this phase the tester must maintain the sequence of information previously available and over all the related result set to the client or user. It consolidates the activities of information gathered, analysis, takeout conclusions and suggestions and then generates final appearance report.

*Step 07—Dispose up*

This is the final phase of penetration testing and involves disposing up all that has any susceptibility for injury or attack during the testing process. As any exposure is identified then corresponding changes are made to examine the system.

## XI. CONCLUSION

This paper has been aimed at evaluating the pros and cons of penetration testing in an organization. Paper gives the idea of basic requirements, which must be fulfilled for successful penetration testing. this paper has proposed test convergence functionality, called “Penetration Testing Architecture”. Presented approach is able to solve the problems like IP addresses verification, Vulnerability issues classification, Special circumstances etc. this approach can develop and

enhance the quality. In this paper only the Architecture at a time has been focused. However, penetration testing and its relationship with others such as traditional, Risk-based, Network Scanning, Vulnerability Scanning can be considered, which are planned to take up in next work.

## REFERENCES

[1] C. Edward Chow., "Penetrate Testing", https://www.cs.uccs.edu/~cs591/penetrateTest/penetrateTest.ppt.

[2] Trajce Dimkov, Wolter Pieters, Pieter Hartel "Two methodologies for physical penetration testing using social engineering", 2009.

[3] Chan Tuck Wai "Conducting a Penetration Test on an Organization", SANS Institute InfoSec Reading Room , SANS Institute Reading Room site,2002.

[4] John Wack, Miles Tracy, Murugiah Souppaya "Network Security Testing", Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930,NIST Special Publication 800- 42,October 2003.

[5] Reto E. Haeni "Firewall Penetration Testing", The George Washington University Cyberspace Policy Institute 2033 K Str. Suite 340 N Washington DC 20006 Washington DC, January 1997.

[6] M. Zulkernine1, M.F. Raihan1, and M.G. Uddin2 "Towards Model-Based Automatic Testing of Attack" Lecture Notes in Computer Science, 2009, Volume 5775/2009, 229-242, DOI: 10.1007/978-3-642-04468-7_19 Computer Safety, Reliability, and Security In Springer-Verlag Berlin Heidelberg 2009.

[7] Achim D. Brucker_, Lukas Brüggery, Paul Kearneyz, and Burkhart Wolff "Verified Firewall Policy Transformations for Test Case Generation" Proceedings of the Third International Conference on Software Testing, Verification, and Validation (ICST), pp. 345–354, 2010, doi: 10.1109/ICST.2010.50, IEEE Computer Society, 2010.

[8] Debasis Mohanty: "Demystifying PenetartionTesting: HackingSpirits" www.hackingspirits.com;www.infosecwriters.com/text_resources/pdf/pen_test2.pdf.

[9] Philip R. Moyer,E. Eugene Schultz,"A SYSTEMATIC METHODOLOGY FOR FIREWALL PENETRATION TESTING" projects.cerias.purdue.edu/firewall/references/.

[10] Jim Hurst, "Penetration Testing" Domain 8: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) March 30th, 2007, http://www.giac.org/resources/whitepaper/planning

[11] http://sectools.org/

[12] War dialing : *en.wikipedia.org/wiki/War_dialing,searchsecurity.techtarget.com/.../0,,sid14_gci546705,00.html*

[13] IT Showcase: Microsoft IT Attack and Penetration TestingTeam, microsoft.com/.../MicrosoftITAttackAndPenetrationTestingTeamPPT.ppt-2004.

[14] Ron Gula, "BROADENING THE SCOPE OF PENETRATION-TESTING TECHNIQUES" Intrusion Detection Products Enterasys Networks , 1999.

[15] Manish S. Saindane, "PENETRATION TESTING – A SYSTEMATIC APPROACH" www.infosecwriters.com/text_resources/.../

[16] Gunnar Peterson: "Security Architecture Blueprint" 2006,2007 Arctec Group, LLC Peterson,http://www.arctecgroup.net/.

[17] Tomas Walke: "An Overview Of Penetration Testing" www.megapremium.info/.../an-overview-of-penetration-testing/ 2010 .

[18] 'dti' information security breaches survey 2006, technical report www.dti.gov.uk/industries/information_security.

[19] SANS ANALYST PROGRAM, penetration testing; accessing your overall security before attackers do. By-Stephen Northcutt, Jerry Shenk, Dave Shackleford, Tim Rosenverg, Raul Siles and Steve Mancini. june 2006.

[20] Information security breaches survey 2010, technical report, www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.

[21] N. Y. Hamisi, N. H. Mvungi, D. A. Mfinanga, B. M. M. Mwinyiwiwa, Member, MIEEE: "Intrussion detection by penetration test in an organization network", University of Dar es Salaam,P. O. Box 35131, Dar es Salaam,Tanzania.2nd International Conference on Adaptive Science & Technology,IEEE 2009 .

[22] Bing Duan, Yinqian Zhang, Dawu Gu :"An Easy-to-deploy Penetration Testing Platform", The 9th International lConference for Young Computer Scientists, IEEE 2009.

[23] "An Argument for an automated Penetration testing framework" With a Technical Introduction to CORE IMPACT-www.coresecurity.com/files/attachments/CORE_IMPACT-WhitePaper

[24] Tugkan Tuglular :"Test Case Generation for Firewall Testing" ,www.acsac.org/.../ACSAC-WiP06-04-Tuglular.

[25] K. K. Mookhey: "Risk-based Penetration Testing" Securitybyte & OWASP Confidential, www.securitybyte.org/.../ .

[26] Computer Network Defence , Ltd,2010; www.cndltd.com/

[27] Gray McGraw: "Software Penetration Testing", IEEE SECURITY & PRIVACY 1540-7993/05/ © 2005,IEEE.

[28] Article: "Network assessment", Security Compass2009 ,www.securitycompass.com/security.../.