International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue (6) NCRTCST-2013, ISSN 2249–071X

National Conference on Recent Trends in Computer Science and Technology (NCRTCST)-2013

A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing

Sugandh Shah
School of Computer and Information Sciences
University of Hyderabad Hyderabad (A.P), INDIA
Email: sugandhshah@idrbt.ac.in

B. M. Mehtre
Institute for Development & Research in Banking Technology
Established by Reserve Bank of India Hyderabad (A.P), INDIA
Email: bmmehtre@idrbt.ac.in

***Abstract* – Internet has opened unlimited avenues of opportunity by enabling organizations to conduct business and share information on a global basis. However, it has also brought new levels of security concerns and Cyber threats. It exposes valuable corporate information, mission critical business applications and consumer's private information to more risk than before. But security of IT infrastructure is something that Organizations cannot afford to compromise. Vulnerability Assessment and Penetration Testing (VAPT) helps to assess the effectiveness or ineffectiveness of the security infrastructure installed by the Organizations to remain protected from the emerging Cyber threats. Hence it enables the Organizations to install patches and adopt required security measures to safeguard themselves from possible cyber attacks. This paper describes in brief the methodologies and techniques involved in VAPT, Along with its benefits and precautions. The paper aims at creating high level of Cyber Security awareness and importance at all levels of an Organization, enabling them to adopt required up-to-date security measures and remain protected from various Cyber attacks.**

***Keywords* – Cyber Security, Vulnerability Assessment, Penetration Testing, Ethical Hacking, VAPT.**

I. Introduction

Cyber Security remains one of the major issues of Corporate Information Systems. The growing connectivity of computers through the Internet, the increasing extensibility of systems, and the unbridled growth of the size and complexity of the systems have made Cyber security a bigger problem now, than in the past. Furthermore it is a *Business Imperative* to adequately protect an Organization's Information assets by following a comprehensive, and structured approach to provide protection from the risks an organization might face.

In an attempt to resolve the Cyber threats, and comply with the mandated security regulations, *Vulnerability Assessment and Penetration Testing (VAPT)* proves to be an assured assessment tool to ensure the *Cyber Security* arrangements of an Organization. The Technique has become a widely used and integral part of Quality Assurance Techniques for the systems used by various financial organizations particularly *Banks. Vulnerability Assessment*, as the name suggests, aims at discovering the possible threats and subset of input space with which a malicious user can exploit logical errors in a system to gain profit or drive the system into an insecure state [6].

While *Penetration Testing*, aims at assessing the difficulty level for someone (basically an attacker/hacker) to penetrate an Organization's Cyber security controls against unauthorized access to its information and information systems. VAPT is done by simulating an unauthorized user (attacker) attacking the system using either *Automated Tools* or *Manual Excellence* or a combination of both. Hence the process of VAPT is sometimes also referred as *Ethical Hacking.*

VAPT helps in identifying Cyber Threats and vulnerabilities under controlled circumstances, so that they can be eliminated before actual hackers/attackers aim to exploit them.

II. An Overview of VAPT

The complete process of VAPT is conducted in two major parts. The *first* part deals with the *Analysis* and *Discovery* of existing Vulnerabilities, which may leads to various Cyber threat. The *second* part deals with the *Exploitation* of the detected set of Vulnerabilities, to judge their *Severity* and *Impact* over the Target system.

A. Vulnerability Assessment

A *Vulnerability* is a software or hardware bug, or misconfiguration that a malicious individual can *Exploit* [2]. The existence of a vulnerability in a system imposes a Threat.

These vulnerabilities are ranked on the basis of their Severity and Impact. Communities like *OWASP* and *SANS* provides the standard list of most common and serious security vulnerabilities.

The *OWASP Top 10* list emphasizes on *Web Application Security*, and represents a broad consensus about what the most critical web application security flaws are. Similarly the CWE/SANS Top 25 Vulnerability list, maintained by security experts from *SANS* and *MITRE*, aims at listing the top 25 vulnerabilities in all kind of applications. Both of these lists help in assessing the severity of the vulnerabilities found.

B. Vulnerability Assessment Strategies

The *Vulnerability Assessment strategies* can be broadly classified into two types:

1) *Exploratory Testing:* The VAPT tester scans all the system component for existing vulnerabilities without any specific *Test Plan.* The security evaluation in this technique is based on tester's instinct and prior experiences [9].

2) *Systematic Testing:* In this technique the tester follows a predefined *Test Plan* rather than exploring. The VAPT tester makes a thorough study of all the system components, based on which he develops an efficient test plan. And further sticks to the plan in the entire process of finding vulnerabilities.

Static Analysis: Apart from above stated two assessment techniques the testers sometimes also opt for *Static Analysis* of Source Codes. The tester in this technique, evaluates a system and its components, based on its *Form, Structure, Contents* and *Documentations* which in any case does not require the Program's execution [3].

C. Penetration Testing

Penetration Testing can be defined as the *illegitimate acquisition* of *legitimate authority*. *Penetration Testing* is the art of finding an open door to penetrate into the target system in an *ethical* approach with an aim to audit and rectify the security infrastructure of the target system. The Penetration Testing also provides a *Proof of Issue* for security investments to senior management.

D. Penetration Testing Strategies

The VAPT testers follow Three Penetration Testing Strategies based on the *Scope* and *Type* of Auditing required:

1) *Black Box Testing:* in this approach the testers have no prior knowledge of the test target. They are supposed to figure out all the loopholes of the system based on there experience and individual expertise. The tester basically aims at auditing the *External* Security boundary of the test target hence the tester simulates the actions and procedures of a real attacker who may be present at some other place outside the boundary of the test target and has no information about the test target.
2) *White Box Testing:* This approach is contrary to Black Box. In this approach the testers are provided with all the necessary information and credentials regarding the test target, and the VAPT tester audits the *Internal* security arrangements of the test target hence the test simulates the actions and procedures of a real internal threat like a malicious employee who is present within the boundaries of the target.
3) *Grey Box Testing:* This approach can be simply understood as the combination of the above two approaches, in this approach the VAPT tester is provided with partial disclosure of information about the test target, hence the tester gathers further information by conducting the test.

III. Scope and Benefits of VAPT

VAPT is conducted in three major areas *Physical Structure* of the system, *Logical Structure* of the system and the Response/*Work flow* of the concerned system. These three areas are comparatively most prone to cyber attacks hence assessing these three areas gives a complete idea of the level of Cyber Security arrangements in the target system.

A. Scope of Vulnerability Assessment & Penetration Testing

The above stated three areas of concern, conclude and define the overall scope of vulnerability assessment and penetration testing process.

1) *Network Testing:* In this part, the VAPT tester aims at identifying the security flaws associated with the Design, Implementation and Operation of the target organization's network. The tester analyses and checks various components like Modems, Remote Access Devices and other connections for possible mis configurations, which may act as an entry point for an attacker to hack into the target's network.
2) *Application Testing:* The VAPT tester here, aims at testing the applications possessed by the test target primarily the web applications as they remain comparatively more vulnerable to attacks. The tester exposes the effectiveness of an application's security controls by highlighting the risks posed by actual exploitable vulnerabilities.
3) *Social Engineering:* In this part of VAPT the tester aims at auditing the Work flow of the target Organization, by targeting the human interactions to gather confidential information regarding the target or any of its component systems, which otherwise is supposed to be kept confidential.

B. Benefits of Vulnerability Assessment & Penetration Testing

VAPT is a valued assurance assessment tool that benefits both business and its operations. For an Organization to remain assured of its *Security Infrastructure,* it must conduct VAPT periodically, it not only assures the Security level of its component systems and resources, but also informs about new vulnerabilities and exploits possible, which may lead to financial and data losses.

1) *Business Point of View:* For any financial Organization, its *Corporate Image remains* a big concern, VAPT helps an Organization to safeguard against any possible Failure by preventing Financial losses, proving due diligence and compliance to industry regulators, customers and shareholders, thereby preserving Corporate Image and rationalizing Information Security investments.

Organizations spend millions of dollars to recover from a security breach due to notification costs, remediation efforts, decreased productivity and lost revenue. The *Computer Society of India (CSI)* study estimates recovery efforts of around $167,713.00 per incident.

VAPT being a Proactive Service can successfully Identify and address security risks before actual security breaches occur, thus preventing any Unauthorized Access, Data Corruption and financial loss caused by security breaches. VAPT provides a Proof of Issue and a solid case for proposal of investment to senior management, thereby creating high awareness of Security's importance at all levels of an Organization.

2) *Operational Point of View:* Conducting VAPT helps an Organization in shaping *Information Security Strategies* through quick and accurate identification of vulnerabilities, Proactive elimination of identified risks, implementation of corrective measures and enhancement of IT knowledge. VAPT provides detailed information on actual, exploitable security threats if it is encompassed into an Organization's security Doctrine and Processes.

By providing the Information required to effectively and efficiently Isolate and Prioritize vulnerabilities, VAPT can assist the Organizations to Fine-tune the test configuration changes or Patches to pro actively eliminate identified risks.

IV. VAPT Methodology

The Complete process of VAPT is composed of many sub processes, the VAPT testers use many Open Source and Commercial tools in each of these sub-processes to analyze the Cyber Security arrangements of the entire system. VAPT testers use multiple tools for each sub-process so as to reduce the No. of *False Positives* at each step.

A. Phases of Vulnerability Assessment & Penetration Testing

As illustrated in Fig. 1 The complete process of VAPT is conducted in following three major phases:

1) *Test Preparation Phase:* As the name suggests, in this phase the Testers and the Organization meet to decide the *Scope, Objectives, Time* and *Duration* of the test. All the necessary Documents regarding the test are organized and finalized. Issues like *Information Leakage* and *Downtime* are resolved and put into legal agreement document. Some of the major Documents Required to conduct Vulnerability Assessment and Penetration Testing are mentioned as follows:

- Memorandum of Understanding.
- Non Disclosure Agreement.
- Confidentiality Agreement.
- Risk from Jail free Agreement.
- Return of Security Investment Agreement.
- Rules of Behavior.

2) *Test Phase:* In this phase the actual testing is done. The Operations in this phase are divided into two parts:

a) *Vulnerability Assessment:* In this part of the process, the VAPT tester aims at finding and analyzing the existing set of Vulnerabilities in the target system. This process is composed of many sub-processes:

- *Target Discovery:* The tester collects the crucial informations pertaining to the test target. These informations collected at this point of time help the VAPT tester to generate an image of the target's security infrastructure.
- *Scanning:* After successfully discovering the target the testers perform a scan of the complete system with an aim to identify the list of existing vulnerabilities, which intend to impose a threat to the security of the target system.
- *Result Analysis:* This phase inherits the output of the Scanning phase and analyses the set of vulnerabilities identified after scanning. The tester at this phase aims at prioritizing the identified vulnerabilities based on their severity and impact. The Vulnerabilities are later addressed and resolved in the same order.
- *Reporting:* After the successful accomplishment of initial phases, the tester in this phase aims at documenting the various operations performed and results obtained in the entire process. This documentation is done for the personal use of the VAPT tester.

b) *Penetration Testing:* As illustrated in Fig. 1, the second part of the *Test Phase* is *Penetration Testing.* This process aims at exploiting the identified set of vulnerabilities. By exploiting the vulnerabilities the VAPT tester checks the difficulty level of an attacker in exploiting the concerned vulnerabilities. The process also provides a *Proof-of-Concept* to support the test finding at later stages.

- *Pre Attack Phase:* In this phase the tester conducts *Reconnaissance.* The strategy propagates in two parts: *Passive Reconnaissance* in which the tester passively gathers all the possible set of details without actually *Touching* the target network. Once the job is done, the attacker enters into *Active Reconnaissance*, in which various experiments are performed over the target to gather responses and detect vulnerabilities and loopholes in the target.
- *Attack Phase:* In this phase, the attacker tries to compromise the target system in real, by using various tools and techniques to exploit the logical and physical vulnerabilities exposed in the pre attack phase. Some of the techniques used in this phase are *Perimeter Penetration, Target acquisition* and *Privilege Escalation.*
- *Post Attack Phase:* In this phase the VAPT tester aims at returning the modified system to the pretest state. It includes reversal of each change made to the system to restore to its pre attack state. The activities performed during this phase includes removal of any files, tools, exploits, or other test created objects uploaded to the system during testing [10].

c) *Report Generation Phase:* This phase deals with the thorough investigation and validation of all the test results thereafter *Documentation* and *Reporting* of all the Test findings and a *Mitigation Plan.* This Confidential report generated at this phase is delivered only to the Concerned authorities of the test target along with the mitigation plan which holds suggestions for remediation of the identified vulnerabilities and exploits.

B. Risks involved in VAPT :

Security Testing causes risks to the target by its very nature. Like an *Attacker* the *VAPT Tester* deliberately leaves the relatively safe ground of intended use and expected activities. Security Testing is inherently invasive where it employs techniques similar to those used in an attack [7].

The *Specific Risks* of VAPT can be categorized as follows:

1) *Technical Risks:* These are the risks caused directly by the *Testing Activities* or by the *System being Tested.* Some of the major technical risks are *Failure* of the target or connected systems, *Disruption* of service, *Reduced* Performance, *Modification* or *Contamination* of data and *Disclosure* of data.
2) *Organizational Risks:* The VAPT testing also involves some Organizational side effects like Unnecessary *Triggering* of *incident handling* processes, *Disruption* of business processes, and Loss of *Reputation* if third parties are effected.
3) *Legal Risks:* These kind of risks are encountered due to legal obligations and possible side effects of third parties like *Violation* of *Legal Obligations* and *Inadvertently committing* punishable acts.

C. General Precautions for VAPT :

Based on the risk factors involved in VAPT, the testers need to focus on some precautions in order to prevent any unexpected harm to the target system. The testers generally adopt the following major strategies to do so:

1) *Indirect Testing:* The testers instead of testing the actual defects, aim to collect sufficient evidences to conclude that a vulnerability is likely to be present. The technique is useful when dealing with known vulnerabilities.
2) *Limited Exploitation:* The testers try to prefer *Test Cases* that demonstrate the vulnerability and its exploit, and try to reduce the actual amount of exploitation. The testers use certain Payloads that show measurable effects without causing any severe side effects.
3) *Delayed Effects:* Sometimes, if possible, testers design tests for delayed effects. The testers then evaluate the test results inside the system and cancel or inhibit any further processing before it would occur. The strategy is effective in cases where the tests have real-world effects.
4) *Interruptible Testing:* In Some testing Scenarios, testers have to ensure that they can interrupt their testing at any time, so that they can immediately react if any unintended consequences are observed.
5) *Throttled Tools:* When using Automated tools to execute large no. of individual tests, the VAPT testers must ensure that the target's won't be overloaded, as it may result into *Disruption* of services.
6) *Avoiding Lock-outs:* Sometimes repeated tests might trigger functions designed to *Lock-Out* attackers. For instance password protected systems often limit the no. Of failed login attempts. Testers must ensure they do not lead to such *Denial of Service* scenarios during the process.
7) *Testing Tests:* Exploratory testing approaches, where the testers develop new tests based on there vulnerability hypotheses, are inherently more risky than executing well planned tests. Hence testers must use a lab environment to develop and try tests before deploying them against real targets.
8) *Confining Tools:* VAPT involves continuous interaction of the tester and the target over a network. Hence to avoid any accidental execution of risky tests against attached systems other than the test target, the Scope of the test should be enforced at the network level itself. Some of the VAPT tools perform this job internally, while for others the *firewall* must be configured to do so.
9) *Partial Isolation and Replication:* Subsystems of the target system can sometimes be reconfigured for testing either dynamically or by setting up a *Replica* for the subsystem in a different configuration. Thereby reducing the side effects of testing.

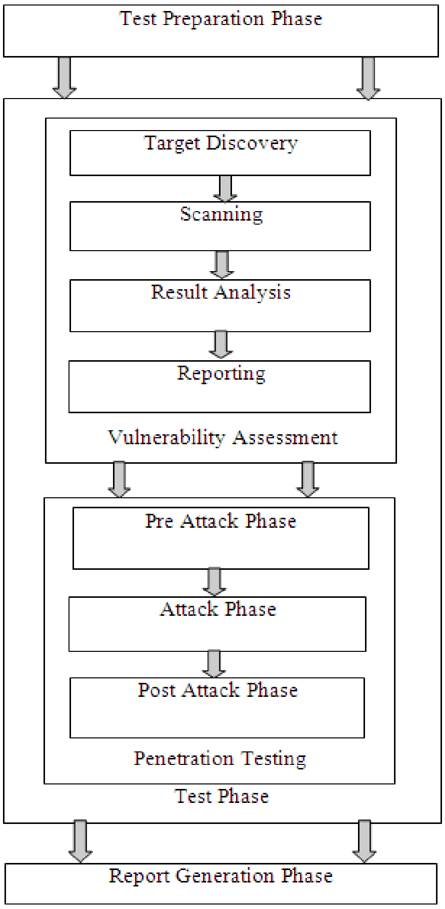

Fig.1. Phases of VAPT

10) *Rules of Engagement:* Last but not the least, Tester and the Client (organization) must establish clear and unequivocal rules of engagement, thereby clearly specifying the targets, test timings and the limits of testing. The third parties getting affected by the concerned tests must also be notified.

11) *Awareness and Education:* The VAPT testers need to be well aware of the risks and there specific *Rules of Engagements*, and the complete operation must be performed within the defined Boundaries with least or null intervention of third parties.

V. VAPT Standards

To ensure the accuracy and effectiveness of the process, the testers follow some standards to conduct VAPT. These standards ensure the correctness of the procedures being adopted therefore reducing the risk of failure.

There are four major *Vulnerability Assessment and Penetration Testing standards* widely adopted across the globe:

D. Open Source Security Testing Methodology Manual:

OSSTMM is a peer-reviewed manual of security testing and analysis which results in verified facts. These facts provide actionable information that can measurably improve your operational security.

The OSSTMM was released by *Pete Herzog*, and its standards are maintained by The *Institute for Security and Open Methodologies (ISECOM).*

E. Payment Card Industry Data Security Standards :

PCI-DSS is a proprietary Information security standard for organizations that handle *cardholders* informations for the major *Debit, Credit, Prepaid, E-Purse, ATM* and *POS cards*, it provides the requirements and Security assessment procedures for the testers when they conduct penetration test primarily in Banks and E-Commerce sites.

The PCI-DSS standards are maintained and distributed by *PCI Security standards Council.*

F. Open Web Application Security Projects :

The *OWASP Application Security Verification Standard (ASVS)* was first published in December 2008. The primary aim of this standard is to normalize the range of coverage and level of rigor available in the market when it comes to the issue of performing Application Level Security verifications using a Commercially Workable Open standard.

The OWASP ASVS is maintained by *OWASP Foundation*.

G. International Organization for Standardization 27001 :

ISO/IEC 27001:2013 is an Information Security Standard published on 25 September 2013, thereby replacing its previous version ISO/IEC 27001:2005. It is basically the specification for *Information Security Management System (ISMS).*

The Standard is Regulated and Maintained by *International Organization for Standardization (ISO)* and *International Electro-technical Commission (IEC).*

VI. Conclusion

In today's Electronic Era, where anything and everything remains connected and partially exposed. Cyber attacks and Cyber crimes are rapidly evolving and creating massive threat to Industry and Government across the globe. These attacks have caused losses worldwide amounting to billions of dollars. Though protection systems are developed, cyber criminals are finding new techniques to bypass them. Also these emerging threats are complex and stealthy. So, there is a need to carry out continuous research efforts & development solutions to protect from evolving cyber threats. VAPT proves to be an efficient, cost effective and assured assessment tool to periodically analyze the status of current security arrangements and help Organizations to install the required security patches in order to remain protected of the Outsider and Insider threats forever. VAPT being Proactive in nature, enables an organization to know about the possible set of threats and attacks even before their actual occurrence. Hence the organizations can take required actions to safeguard their Data resources and component systems much before the attacker actually plans to deploy an attack.

References

[1] James. S. Tiller, "CISO's guide to penetration testing", Taylor and Francis Group, CRC Press Publication, 2012

[2] P. Xiong and L. Peyton, "A Model driven Penetration test framework for Web Applications", IEEE 8th Annual International Conference on Privacy, Security & Trust, Aug 17-19, 2010, Ottawa, ON, Canada.

[3] B. Liu, L. Shi and Z. Cai, "Software Vulnerability Discovery Techniques: A Survey", IEEE 4th International Conference on Multimedia Information Networking and Security, Nov 2-4, 2012 Nanjing, China.

[4] B. Duan, Y. Zhang and D. Gu, "An easy to deploy Penetration testing platform", IEEE 9th International Conference for young Computer Scientists, Nov 18-21, 2008, Hunan, China.

[5] Dr. D. Geer and J. Harthorne, "Penetration testing: A Duet", IEEE Proceedings of 18th Annual Computer Security Application Conference, ACSAC'02, 2002, Washington, DC, USA

[6] S. Sparks, S. Embleton, R. Cunningham and C. Zou, "Automated vulnerability analysis: Leveraging control flow for evolutionary", IEEE 23rd Annual Computer Security Applications Conference, Dec 10-14, 2007, Miami, Florida.

[7] S. Turpe, J. Eichler, "Testing production systems safely: common precautions in Penetration testing", IEEE Academics and Industrial Conference, Sep 4-6, 2009, Windsor.

[8] W. Halfold, S. Choudhary and A. Orso, "Penetration testing with improved input vector identification", IEEE International Conference on Software Testing Verification and Validation, Apr 1-4, 2009, Denver, CO.

[9] A. Austin and L. Williams, "One technique is not enough: A comparison of vulnerability discovery techniques", IEEE International Symposium on Empirical Software Engineering and Measurement, Sep 22-23, 2011, Guenther, Ruhe.

[10] W. LanFang and K. HaiZhou, “A research of behavior based penetration testing model of the network”, IEEE International Conference on Industrial Control and Electronics Engineering, Aug 23-25, 2012, Xi'an, China

[11] N. Antunes and M. Vieira, “Benchmarking vulnerability detection tools for web services”, IEEE International Conference on Web Services, July 5-10, 2010, Miami, Florida

[12] A. Papanikolaou, V. Karakoidas, V. Vlachos and G. Zouganelis, “A Hackers perspective on educating future security experts.”, IEEE Panhellenic Conference on Informatics, Sep 30 - Oct 2, 2011, Kastoria, Greece.

[13] A. Kurilo, N. Miloslavskaya and S. Tolstaya, “Ensuring Information Security controls for the russian banking Organizations.”, ACM Conference SIN’09, October 6-10, 2009, Gazimagusa, North Cyprus.