Comparison of Vulnerability Assessment and Penetration Testing

Jignesh Doshi
LJ Institute of Management Studies,
Ahmedabad, Gujarat

Bhushan Trivedi
GLS Institute of Computer Technology,
Ahmedabad, Gujarat

ABSTRACT

Business using internet has grown drastically in past decade. Attacks on web application have increased. Web application security is a big challenge for any organizations as result of increasing attacks. There exist different approaches to mitigate various security risks are defensive coding, hardening (Firewall), Monitoring and auditing. These solutions found more towards prevention of attacks or of monitoring types of. Vulnerability assessment and Penetration testing are two approaches widely used by organizations to assess web application security. Both solutions are different and complimentary to each other. In this paper comparison of these two approaches are provided. The authors found that penetration testing is better compare to vulnerability assessment as it exploits the vulnerability, while vulnerability assessment is superior in terms of coverage over penetration testing.

General Terms

Vulnerability Measurement, Penetration Testing

Keywords

Attack, Vulnerability, Security Risk, VAPT

1. INTRODUCTION

Web application usage has increased as more and more services are available on the web. A business using Web applications is also increasing day by day. On the other side, a web application based attacks have increased. The web application has become the main target of attackers. The Major impact of attacks is a data loss or financial loss or reputation loss.

Various types of countermeasures exist to protect system against attacks like defensive coding, firewall, Intrusion detection system etc. [15]. The existing solutions are classified in two categories proactive and reactive. To secure web applications, thorough study of vulnerabilities is required. The study will help in taking effective actions. Vulnerability measurement and Penetration testing are widely used approaches by organizations for web application security assessment.

In this paper, the authors have compared vulnerability assessment and penetration testing.

The rest of the paper is organized as follows. Vulnerability assessment is discussed in section 2, Penetration testing is discussed in Section 3. Section 4 describes the comparison between vulnerability assessment and penetration testing. The conclusion is described in section 5.

2. CURRENT WEB APPLICATION SECURITY TRENDS

The number of internet users and websites are increasing rapidly in recent years [16]. Approximately 66% of web applications have problem as per Gartner. According to sophisticated vulnerability assessment tools, 60% vulnerabilities can be found in most of web applications [17].

Security measures most commonly applied for web application security are firewalls, Intrusion Detection System (IDS), Antivirus System and defensive coding [14] [15]. This solution either requires developer skills or efforts in common [15]. These solutions provide a way to assess the system, while organizations need a way to assess security countermeasure assessment. It is also necessary to assess web application periodically against security risks in order to take effective actions.

3. VULNERABILITY ASSESSMENT

Vulnerability is a weakness or flaw in a system. Reasons for vulnerability existence are weak password, coding, input validation, misconfiguration etc. The attacker attempts to identify vulnerabilities and then work it.

Vulnerability assessment is a proactive and systematic strategy to discover vulnerability. It is practiced to discover unknown problems in the system. It is also required by industry standard like DSS PCI from a compliance point of view.

Vulnerability assessment is achieved using scanners. It is a hybrid solution, which combines automated testing with expert analysis.

Vulnerability assessment is a one step process (Refer to figure 1). In Section 5, more details about vulnerability assessment is discussed.

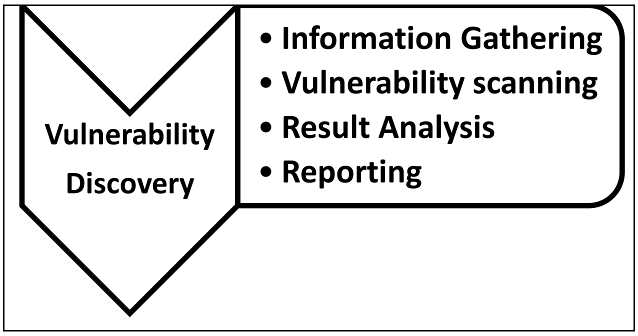

Figure 1: Vulnerability Assessment Process

4. PENETRATION TESTING

A penetration testing evaluates the security of a computer system or network by simulating an attack. It is a proactive and systematic approach for security assessment.

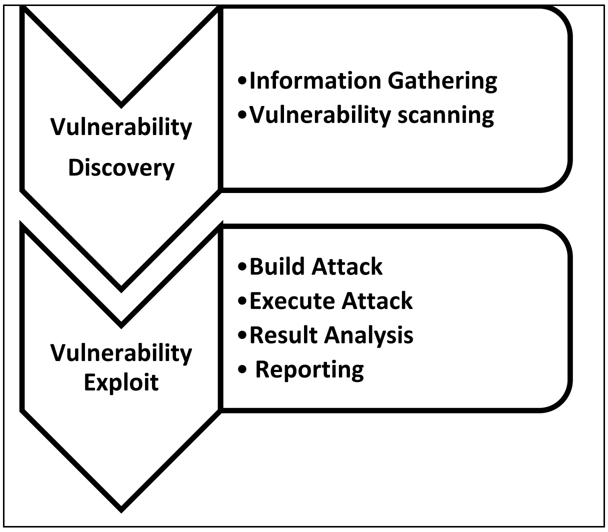

Figure 1: Penetration Testing Process

Penetration testing is a two step process (refer to figure 2). The next section describes in detail a penetration testing.

5. COMPARISON

5.1 Generic Feature Comparison

	Vulnerability Assessment	Penetration Testing
Working	Discover vulnerabilities	Identify and exploit vulnerabilities
	Alerts pre-existing flaws found in the code	Shows how damaging flaws pose a threat to application
	Do not differentiate between flaws that can cause harm or not	Gives a detail picture of flaws found in application with risk associated with it
Mechanism	Discovery & Scanning	Simulation
Process	One step: Find vulnerability	Two step process: Find and exploit vulnerabilities
Focus	Breadth over depth	Depth over breadth
Type	A Hybrid solution	One solution for multiple vulnerability testing
Coverage of completeness	High	Low
Defend ability	Medium	High
Control	Detective control, applied to detect when equipment is compromised.	Preventative control used to reduce exposures
Cost	Low to moderate cost	High
Performed by	In house staff can do this	Attacker, Pen tester

The above table shows a comparison of Vulnerability assessment with penetration testing with reference to general features.

5.2 Resource Requirements

	Vulnerability Measurement	Penetration Testing
Internal Resource Requirement	Medium	Low
External Resource Requirement	High	High
Tester Knowledge	High	Low

Above comparison shows that penetration testing requires low tester's knowledge and internal resources compared to vulnerability measurement.

5.3 Testing

	Vulnerability Measurement	Penetration Testing
Testing of other security Investments	Not possible here	Determine whether other security investments are working the right way or not
Security Risk Assessment	Not possible here	Provide security risk assessment as mimics attacks just like an attacker
Testing	Does not simulate attacks	Simulates real world attacks
How often to run	Continuously, especially after new equipment is loaded	Periodically

The key benefit of penetration testing is that we can run periodically and with it we can assess security investment and exploit risk.

5.4 Results

	Vulnerability Assessment	Penetration Testing
Reports	Comprehensive baseline of what vulnerabilities exist and changes from the last report	Short and to the point, identifies what data was actually compromised
Metrics	Lists known software vulnerabilities that may be exploited	Discovers unknown and exploitable exposures to normal business operations
Results	Provides partial evaluation of vulnerabilities	Provides complete evaluation of vulnerabilities

5.5 Limitations

Major limitations of Vulnerability Assessments are:

- Cannot identify potential access path
- Provides false positive
- Requires high technical skills for tester
- Hybrid solution
- Cannot exploit flaws

Major limitations of Penetration testing are:

- Identifies potential access paths
- Identifies only those which poses threats
- May not identify obvious vulnerability
- Cannot provide information about new vulnerabilities
- Cannot identify server side vulnerabilities

6. CONCLUSION

With the exception of coverage, penetration testing is superior to vulnerability management.

Key benefits of penetration testing over vulnerability assessment are:

- Technical capability required in penetration testing is low compared to vulnerability assessment
- Can be used at runtime
- With penetration testing, one can detect, confirm and exploit vulnerabilities.
- With penetration testing can limit the resulting impact on the system.

For effective protection, it is important to understand vulnerability in details.

Both are complimentary strategies to each other and proactive. The authors suggest to use penetration testing regularly.

7. REFERENCES

[1] Vulnerability Assessment and Penetration Testing: http://www.veracode.com/ security/vulnerability-assessment-and-penetration-testing

[2] John Barchie, Triware Net world Systems, Penetration Testing vs. Vulnerability Scanning: http://www.tns.com/PenTestvsVScan.asp

[3] Penetration Testing Limits http:// www.praetorian.com/blog/penetration-testing-limits

[4] Vulnerability Analysis, http://www.pentest-standard.org/index.php/ Vulnerability Analysis

[5] Open Web Application Security Project, https://www.owasp.org/index.php/Category: Vulnerability

[6] Penetration Testing: http://searchsoftwarequality .techtarget.com/definition/penetration-testing

[7] Vulnerability Assessment and Penetration Testing: http://www.aretecon.com/aretesoftwares

[8] Ankita Gupta, Kavita, Kirandeep Kaur: Vulnerability Assessment and Penetration Testing,

[9] International Journal of Engineering Trends and Technology- Volume4 Issue3- 2013, ISSN: 2231-5381 Page 328-330

[10] Konstantinos Xynos, Iain Sutherland, Huw Read, Emlyn Everitt and Andrew J.C. Blyth: PENETRATION TESTING AND VULNERABILITY ASSESSMENTS: A PROFESSIONAL APPROACH, Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010 available at : http://ro.ecu.edu.au/icr/16

[11] You Yu, Yuanyuan Yang, Jian Gu, and Liang Shen, Analysis and Suggestions for the Security of Web Applications,, International Conference on Computer Science and Network Technology, 2011, 978-1-4577-1587-7/111, IEEE

[12] Andrey Petukhov, Dmitry Kozlov, Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing, https://www.owasp.org/images/3/3e/OWASP-AppSecEU08-Petukhov.pdf accessed on 31st January 2015

[13] Parvin Ami, Ashikali Hasan: Seven Phrase Penetration Testing Model,International Journal of Computer Applications (0975 – 8887),Volume 59– No.5, December 2012

[14] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones,an overview of penetration testing, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011 DOI :10.5121/ijnsa.2011.3602

[15] Jignesh Doshi, Bhushan Trivedi, Assessment of SQL Injection Solution Approaches, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014 ISSN: 2277 128X

[16] Netcraft, Total Sites Across All Domains August 1995 - April 2010, http://news.netcraft.com.

[17] Gartner, Press releases, http://www.gartner.com