International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 2, ISSN No. 2455-2143, Pages 72-76
Published Online June 2019 in IJEAST (http://www.ijeast.com)

VULNERABILITY ASSESSMENT AND PENETRATION TESTING AS CYBER DEFENCE

Bohara Anand Chandrakant
Department of Computer Engineering
NBN Sinhgad Technical Institutes Campus,
Pune, Maharashtra, India

Jorvekar Priti Prakash
Department of Computer Engineering
NBN Sinhgad Technical Institutes Campus,
Pune, Maharashtra, India

Abstract— **In last ten years, use of internet applications,web hacking activities have exaggerated speedily. Organizations facing very significant challenges in securing their web applications from rising cyber threats, as compromise with the protection issues don't seem to be reasonable. Vulnerability Assessment and Penetration Testing (VAPT) techniques help them to go looking out security loopholes. These security loopholes could also be utilized by attackers to launch attacks on technical assets. Thus it is necessary ascertain these vulnerabilities and install security patches. VAPT helps organization to determine whether their security arrangements are working properly. This paper aims to explain overview and various techniques used in vulnerability assessment and penetration testing (VAPT) in detail. Also focuses on making cyber security awareness and its importance at various level of an organization for adoption of required up to date security measures by the organization to stay protected from various cyber- attacks**

Keywords— **VAPT, Vulnerability Assessment, Penetration Testing, Vulnerability, Penetration, Security, Cyber, Cyber attacks, attacks, VAPT Tools, Cyber defence, System Security, Cyber defence Technology**

I. INTRODUCTION

In information system, we frequently hear that security is a journey and not a destination. That’s true as things go when managing the security of network, we always have to take efforts and stay one step ahead of our competitor – the criminals, hackers, malcontents, miscreants and spies. They steal information and data without breaking any glass. Keeping data private is one core mission of network security. Opponents are always improving their method and techniques each day to exploit network security and access the private information. These exploits are attacks against: Secretiveness, availability and purity of network resources. Secretiveness (being preserved from unapproved connection) Secretiveness specifies to restricting data access and revelations to approved user and preventing access and restricting from unapproved ones. Availability (resources are regularly used by approved user) Availability specifies to the convenience of the data assets. It assures that data must be used to approved user only. Purity (accuracy and capacity of data) Purity specifies to the Purity of data assets. It convice that data has not been transfered wrongly either by purposely or unintentionally harmful activity.

II. VULNERABILITY ASSESSMENT

"Vulnerabilities are the gateways via which threats are expose”. Vulnerabilities are literally flaws in system. A system will be any of the following: network nodes, computer system, switches, routers, and computer or network application. It obtain glitch in web applications or even in network structure. It is a state of being exposed to the attacked or harmed. Vulnerabilities are open gateways to exploitation. This generates the risk for penetration inside the systems that may fallout in illegal approach and a compromise of secretiveness, availability and purity of network resources. Vulnerability testing is a series of actions to achive results to study system from well-known vulnerabilities. Vulnerability Assessment is the method of recognize, calculating and evaluate the vulnerabilities in the system. In this progress, such as network and operating systems are considered in order to find out the existence of well-known and unknown vulnerabilities. These vulnerabilities are arise due to irrelevent software design, unsure conformation or even much vulnerabilities come into sight as a result of misconfiguration.

A. Processof Vulnerability Assessment–

1. **Goals and Objectives:** Gives description of target and intention of Vulnerabilities examination.

2 **Scope:** While executing assessments, the range of the task demands to be accuratly characterized.The scope is rely on the resources to be tested. The following are the three available scopes that exist:

A. **Black Box Testing:** Testing from an outward network without any preceding knowledge of the inhouse structure and networks.

B. **White Box Testing:** Achieving the test from surrounded by the network with the preceding knowledge of the network architecture. This is also cited to as internal testing.

C. **Gray Box Testing**: Testing from an outward or in-house network, with preceding knowledge of the in-house structure and networks. This is almost always a fusion of black box testing and white box testing.

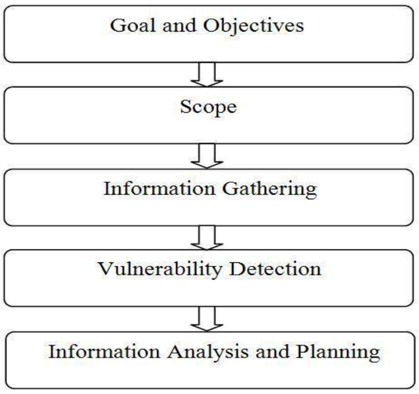

Fig.1 Process of Vulnerability Assessment

Fig. 1. Process of Vulnerability Assessment

3 **Information Gathering:** The series of action to achive result of information gathering is to get hands on as much inside data as possible about the IT surroundings such as IP addresses, networks, operating system version etc. This is fit to all the three types of scope as discussed earlier.

4 **Vulnerability Detection:** In this trail, job such as vulnerability scanners are used, and vulnerabilities are analyzed in the IT community by the way of scanning.

5 **Information Analysis and Planning:** This trail is used to inspect the identified vulnerabilities, associated with the information prosessed in the IT atmosphere, to build a plan for penetrating within the system and network.

B. Types of Vulnerabilities Assessment–

On the ground of vulnerabilities tool there are three prime categories of vulnerabilities assessment: Host Based, Database based and Network Based.

1. **Host Based:** Host Based Vulnerabilities Assessment diagnose an obstacles in selective systems or hosts. It is done via a host based scanner are adapted to cluster system-level vulnerabilities. The host based tools lead intermediary software onto the intended system that takes palce the events and reports it to the security analyst.
2. **Database Based:** Database Based Vulnerabilities Assessment estimate security exposal in database systems using tools and techniques to stay away from SQL- Injections exploit, that can read inside private data from the database and provides patch and update the database management system.
3. **Network Based:** Network Based Vulnerabilities Assessment broadcast open ports, diagnose unknown services carried out on these ports and uncover possible vulnerabilities inter-linked with these service. This is succeeded via network based scanners, rest on the network to reveal vulnerabilities.

C. Benefits of Vulnerabilities Assessment–

- Diagnose nearly all well-known vulnerabilities.
- Highly computerized for scanning.
- Easy to run on a daily basis.

D. Weaknesses of Vulnerabilities Assessment–

- Easily diagnosed by Intrusion Detection System firewall.
- Cause a denial of services by creating bulk of packets.
- Usually fail to concern most recent vulnerabilities.

III. PENETRATION TESTING

Penetration testing is more of an skill than a science. It is the proposition of trying to acquire unapproved entry to approved resources. Penetration testing is also admitted as an ethical hacking as “breaking into your individual structure to see how tough it is to do.” It is a leading branch of network security estimation, which point at a goal of supporting analysis to dig up the vulnerabilities and security liableness in networks. The task of penetration testing is to pick out the technique of bring in route to a system by using conventional tools and techniques established by hackers. After vulnerability assessments, which is are passed down to diagnose and accumulate specific vulnerability surrounded the organization's structure. Penetration testing gives best shot to take advantage of some of the vulnerabilities to accomplish unapproved entry in the system.

A. Methodology Penetration testing methodology consists of three types–[9]

A zero-knowledge Test: Penetration testing team has no realistic knowledge about the target environment.

A partial knowledge Test: Penetration testing team has constrained information about the target environment.

A full knowledge test: The client organisation provides full information to testing team.

B. Process of Penetration Testing–

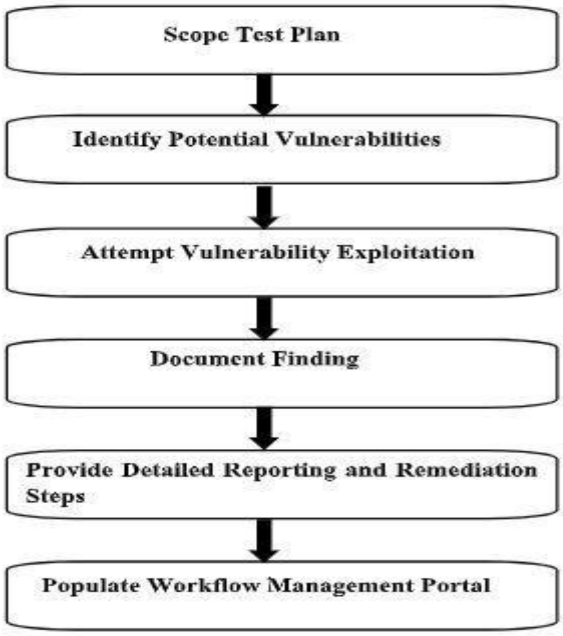
Scope Test Plan
Identify Potential Vulnerabilities
Attempt Vulnerability Exploitation
Document Finding
Provide Detailed Reporting and Remediation Steps
Populate Workflow Management Portal

Fig. 2. Process of Penetration Testing

1. **Scope test Plan:** In first step we restrict the area of our test to what is helpful to the client.
2. **Potential Vulnerabilities:** In this step accessible vulnerabilities are realized by using some tools. As vulnerabilities are caught then vulnerabilities are patched.
3. **Attempt Vulnerability Exploitation:** In this step, we catch the sight of the important achievable advantage that we can proceeds from vulnerabilities. The approved security analyst expands the a set of tools to exploit and access to the systems like significance servers, e-mail platforms and domain controllers etc.
4. **Document Finding:** While testing in-scope structures, the analyst, records all test preferences within the Frontline Services Platform (FSP), a secure multi-function portal that gives green light to clients to receive standardized reporting functionality.
5. **Provide Detailed and Remediation Steps:** At the end of previous step, the client is provided full adminstrative and technical reporting via the FSP client portal. Clients can voluntarily deal with approach to a workflow management tool that is also supported by Frontline. This tool permits you to operate and track remediation of the penetration test findings.
6. **Populate Workflow Management Portal:** Now clients can take this medium of the combined workflow management tool to do fast and efficiently deal with detected issues.

C. Penetration Testing Strategies–

There are two types of Penetration Testing Strategies:-

1. **Internal Testing:** It is performed from under roof of the same network. The prime duty is to obtain the internal network topology which gives the mapping to the fault-finding entry route.
2. **External Testing:** It accomodate via Internet. In internet, attack on the target network is done from outside of the network.

D. Benefits of Penetration Testing–

- Test structure or network by assigning the tools and techniques that attackers use.
- Demonstrate at which intensity vulnerabilities can be exploited.
- Authenticate vulnerabilities.
- Can provide the authenticity and proof needed to address security issue.

E. *Weaknesses of Penetration Testing–*

- It demands great proficiency and it is high-priced.
- Hazardous when handled by inproficient tester.
- Make source code public to third party.
- Some tools and methods may be banned by company regulation.

IV. VULNERABILITY ASSESSMENT VS PENETRATION TESTING

Parameters	Vulnerabilities Assessment	Penetration Testing
Focus on	Known Vulnerabilities that can be exploited	Finds unknown and exploitable vulnerabilities
Done by	Conducted by in-office staff using authorised asscess	Conducted by outside person with or without authorization
Frequency	It is done at least quarterly and especially after new functions are loaded or after network has some changes	It is done once or twice a year as well as anytime when equipements has be changed
Value	Determine when equipment could compromised	Recognize and reduces that vulnerabilities.
Reports	It contains what vulnerabilities exist and what is changed scince last report	It finds what data was compromised

V. VAPT TOOLS

Sr. No .	Name	Type	Operating System
1	Nessus	Vulnerability scanner	Cross-platform
2	OpenVAS	Vulnerability scanner	Cross-platform
3	QualysGuard	Vulnerability scanner	Cross-platform
4	GFI LanGuard	Vulnerability scanner	Windows
5	MBSA	Vulnerability scanner	Windows
6	Burp Suite	web vulnerability scanner	Cross-platform
7	w3af	web vulnerability scanner	Cross-platform
8	Paros proxy	web vulnerability scanner	Cross-platform
9	Acunetix WVS	web vulnerability scanner	Windows
10	AppScan	web vulnerability scanner	Windows
11	Metasploit	Vulnerability scanner and exploit	Cross-platform
12	Canvas	Vulnerability scanner and exploit	Cross-platform
13	Core Impact	Vulnerability scanner and exploit	Windows

14	Kali Linux	Collection of various tools	Linux
15	Nexpose	Entire vulnerability management lifecycle	Cross-platform

VI. CONCLUSION

In this article we concentrated on the vulnerability and penetration tests that provide security, an ethical way to recognize and figure out system flaws and then reduce the risks based on the output of such tests. Thus we have reached to a point that to avoid attacker from stealing our private data, Vulnerability Assessment & Penetration Testing is essential. Through VA we can recognize the vulnerabilities and then by PT we can patch the vulnerabilities.

VII. REFERENCE

[1] Prashant S. Shinde ,Shrikant B. Ardhapurkar ,"Cyber security analysis using vulnerability assessment and penetration testing" , 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)

[2] Krsul, I.. Computer vulnerability analysis: Thesis proposal 1997.

[3] Sectools.org: Top 125 network security tools. 2015. URL:http://sectools.org/.

[4] Owasp category: Vulnerability. 2015. URL: https://www.owasp.org/index.php/Vulnerability.

[5] Kals, S., Kirda, E., Kruegel, C., Jovanovic, N.. Secubat: a web vulnerability scanner. In: Proceedings of the 15th international conference on World Wide Web. ACM; 2006, p. 247–256

[6] Nist, usaid mission site vulnerability assessment and remediation. 2015. URL: http://www.nist.gov.

[7] Shah, S., Mehtre, B.M.. An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques 2014;:1–23.

[8] Cwe.mitre.org, "CWE -CWE List Version 2.9", 2016.

[9] Shah. Sugandh. and B.M. Mehtre. "A Modern Approch to CyberSecurity Analysis Using Vulnerability Assessment and Penetration Testing" NCRTCST - 2013, Nov. 2013, Hyderabad (A.P), India.

[10] Penetration Testing Limits http://www. praetorian.com/blog/penetration-testing/ limitations-of-penetrationtesting/

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

[12] Vulnerability Assessment and Penetration Testing http://www.aretecon.com/aretesoftwares/ vapt.html

[13] http://searchsoftwarequality.techtarget.com/definition/penetrationtesting

[14] http://www.netragard.com/penetration-testing- definition