International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 3, March-April 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Comparative Study between Vulnerability Assessment and Penetration Testing

Sharique Raza[1], Feon Jaison[2]

[1]Master of Computer Application, [2]Assistant Professor,
[1,2]Jain University, Bengaluru, Karnataka, India

ABSTRACT

The Internet has drastically changed in the past decade. Now internet has more business than before and therefore there is a increase in Advanced Persistent Threat groups and Adversaries. After all the advancement in technology and innovation Web application Security is still a challenge for most of the organization all over the world, Because every time APT's groups and Threat actors uses different Tactics Techniques and Procedure (TTPs) for exploiting any organization. There can be many techniques to mitigate such attacks such as defensive coding, hardening system firewall, implementing IDS and IPS using of SIEM tools etc. The solution contains monitoring different logs, events and regular assessment of organization's network which is known as Vulnerability Assessment which is a generalized or a sequenced review of a security system and the other one is penetration testing also known popularly as ethical hacking or red teaming assessment where the client's poses themselves as real Hackers and try to penetrate into the company's network to check if it's really secure or not.

In this paper we will be comparing these two methods and techniques and also decide at the end which of the above two method is more superior and why.

KEYWORDS: *Attack, VAPT, Security*

How to cite this paper: Sharique Raza | Feon Jaison "A Comparative Study between Vulnerability Assessment and Penetration Testing" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-3, April 2021, pp.1208-1211, URL: www.ijtsrd.com/papers/ijtsrd41145.pdf

IJTSRD41145

INTRODUCTION

After the Covid-19 Pandemic most of the organization opted work from home facilities permanently and Schools, Colleges started online classes too therefore the use of internet is increasing day by day, With time new complex software's and new web application technology are getting added as a result Threat actors are taking undue advantage and continuously trying to exploit and enter in the organization's network.

Threat actors exploit any network if they are able to find any possible loop holes or a possible vulnerability. A vulnerability is a fault in a network or in any Web Application that can allow an adversary to penetrate into the network and exploit it.

And Vulnerability Assessment is a process of scanning the whole network of any organization externally or internally for vulnerable assets or policies and fixing them to protect from any exploitation or attacks by following a series of vulnerability assessment lifecycle method.

Whereas penetration testing is a simulated cyber-attack on any organization's internal or external network to evaluate the safety or security of that organization.

Both the methods are widely used by the organization all over the world, This paper will give an idea to take effective actions which method or techniques to use for hardening any network system.

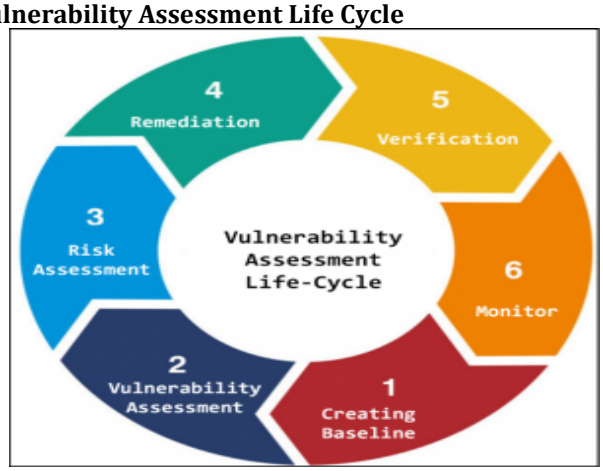
Current Security Trends in Web Applications

Technology is rapidly evolving and the business are changing their way they used to be operated a decade ago. It is estimated that almost 3 trillion dollars were lost in cyber threat attacks in 2020. There is a tremendous amount of shortage of skilled Cyber Security professionals all over the world, It is estimated that almost there is a rise of 272% data breach in 2020 as there was in 2019. Some of the current security trends which are pertaining in the market are -

1. Zero trust network access (ZTNA)
2. Cloud threats
3. Remote Works
4. Insider Threats
5. Owasp top 10
6. Zero Auth authentication

Still some of the organisations uses only firewall and do not implement (WAF) so there is only a perimeter level security and no level of security in layer 7 or layer 6 whereas firewall lives in layer 2 so most of the application level attacks happens in layer 7 so firewalls fails to stop those attacks as a result adversaries are able to exploit any network.

Vulnerability Assessment Life Cycle



Vulnerability assessment life cycle is a process of identifying security loop holes or vulnerabilities in a system or network. It identifies and prioritizes various assets and threats and score them based on the (CVSS) Common Vulnerability Scoring System.

1. Creating Baseline.

It is a pre-assessment phase or the first phase of any vulnerability assessment lifecycle. It checks the assets and the policies of the network externally or internally (based on the client requirements).

After that a Vulnerability analyst also have to check the application services of a particular network.

After gathering all the relevant information we create a inventory of all the resources such as assets, policies, application services and prioritizes the inventory about which scan should we go first.

In this stage a Analyst also maps the infrastructure and learn about security controls.

2. Vulnerability Assessment

A web application or any asset is scanned and it is a focused approach that focus on only target. It checks for server glitches, security glitches and other source code vulnerability in a web applications using some vulnerability assessment tool such as Qualys, Nessus, Nikto etc.

3. Risk Assessment

After the vulnerabilities have been found ,A vulnerability analyst job is to explain the organization about that particular identified vulnerabilities and the risk associated with it . For example - what will be the impact of to the organization if this vulnerability has been found by any external hacker. Based on the (CVSS) common vulnerability scoring system and (CVE) common vulnerability exposure vulnerabilities are marked as

A. Critical

B. High

C. Medium

D. Low

4. Remediation

Remediation phase includes the remedial actions for the detected vulnerabilities in the above step, in this step all the mitigation techniques takes place such as if there is a vulnerability of SQL injection then, the query is being examined and changed to parameterized query. Or implementing any security headers.

5. Verification

In this phase A Vulnerability Analyst ensures that all the vulnerabilities in the organization environment are properly eliminated or not by running a quick scan again, also following up with the stakeholders to check if the vulnerabilities have been fixed or not

6. Monitor

Always monitoring the system for any unsuspected attack

Penetration Testing

Penetration testing or Ethical Hacking is a set of attacks which is done on a computer system or a network to check the hardness or the security of the computer networks. It can be automated with the set of tools or It can be done manually.

The main goal of Penetration Testing is to find some internal loopholes/vulnerabilities or server miscon figurations which is missed in vulnerability assessment phase. Generally Pen-testers think like a real world hacker and try to penetrate into the network.

It is also known as Red Team assessment.

Some organization perform penetration testing coupled with vulnerability assessment which is together known as Vulnerability Assessment and Penetration Testing (VAPT).

Penetration Testing Life cycle

There are 7 phases of penetration testing life cycle.

1. Pre-Engagement - This is the most important phase in which most of the new comers or beginners overlook. This phase do not involve any tools it just requires to get hold of some information like employees email ID, employee information ,address about any particular organization in some job posting websites like linked-in, naukri.com etc.

2. Reconnaissance - The main goal of this phase is to gather as much information as you can either by banner grabbing or by using shodan.io or any other relevant sources, some of the tools which are used in this phase are nmap, nessus etc. This phase basically gives out the information about any open ports which are open as we all know that there are 65,535 ports in a computer and every port have some other purpose, it is just like the window of any house. We could also use social engineering or tailgating to get physical access of target's sensitive information.

3. Threat Modeling and Vulnerability Analysis phase -

- Also called Weaponization phase in which a pen-tester decide which payload to choose to exploit the target from (CVEs) -Common vulnerability exposures, there are some common techniques of attacks/payloads are present publicly which any one can use it to get into the system after finding the probable vulnerability in the network/system.

Generic Comparison

	Vulnerability Assessment	Penetration Testing
1- Regularity	After every two months or specially when the system got out of patched or out dated or when new plugins or softwares are installed.	Twice a year, when the network goes into a subsequent changes or depends on a client .
2-Reports	Generate a concise report about the Vulnerabilities exists in the assets and prioritize the vulnerabilities based on the CVSS and mitigate accordingly	Focuses more on what information was compromised and how it is compromised, and what payload was used.
3- Focus	Known Application and software vulnerabilities that can be exploited	Focuses more on unknown vulnerabilities or zero day vulnerabilities on the application
4-Value	Detects when a web application or a system could be compromised	It reduces the risk associated with the system or network by identifying unknown vulnerabilities
5- Process	Only a single step is involved - find vulnerabilities	It is a two step process find vulnerabilities and later exploit.
6-Protection	High	Low
7-Cost	Low to moderate	High

4. Exploitation-

If the pen-tester have done all the above steps correctly and if the payload executed on the client machine then it comes to the exploitation phase. Where the pen-tester starts gaining access to the system and install it like malware or malicious file in the web application.

5. Post exploitation

As the exploitation phase is completed, the pen-tester will enter to the last phase where the documentation part actually starts or whether it could move latterly in the network.

6. Reporting –

It is again the most important phase, because from this phase the client will understand where did the problem exists in the network or system and what steps should the stakeholders take to mitigate them, if we see from the start then the main objective of a penetration test is to make the system more secure right ?

So a pen-tester scores the vulnerabilities based on CVSS as extreme, High, Moderate and low.

So a good report is very important.

7. Re-test

Not all pen-testers do this phase but if you are a really good pen-tester than this phase is important too. The pen-testers conduct a quick re check of all the network and server again for any vulnerability.

Resource and Hardware Requirements

Generally the resource requirements for carrying out both the methods is pretty much the same. It requires a system with at-least 8 GB of ram and preferably the operating system should be KaliLinux or parrot security because these operating system comes with pre installed set of vulnerability assessment and penetration testing tools.

The Final Result

As we come to the end of our paper we have discussed each technique in details and understood that both have their own specific way of conducting a security test. These both services would be definitely worth to be taken for any organization to find probable vulnerability and different ways of exploits.

Vulnerability Assessment is good for maintaining the security and health checkup of the servers where as Penetration testing is good for finding unknown vulnerabilities and security miscon figurations which are not known to the users.

So, coming to the conclusion, I would choose penetration testing is more preferable way for any organization to find

the loopholes or any security misconfiguration in the servers because a good pen-tester is required to have prerequisite knowledge of all the vulnerabilities and server misconfiguration to perform a test, It is also required for a pen-tester to have programming knowledge as well as networking knowledge to penetrate into the network and programming language to find the flaws in the programming structure of any software or web applications.

Because some of the vulnerabilities exists in the flaw of programming code such as Cross site scripting, SQL injection, External XML entity, where as some vulnerabilities also exists in the networking part protocols such as Service message block (SMB), transport layer security (TLS), secured shell (SSH).

This a penetration testing is overall a good choice to make the servers secure.

Conclusion

We have discussed the two most important ways of security scanning in cyber security in detailed and also learned about the life cycle of each process namely - VAPT lifecycle and Penetration testing life cycle and also how to execute both the process systematically.

Both the process are equally important for any organization to persists but when it comes to the budget and result Penetration testing is always superior to vulnerability management because in penetration testing one can

- Detect
- Analyze
- Confirm vulnerabilities

Even unknown vulnerabilities but in the case of vulnerability assessment the tool which is designed to scan the web servers and the network only finds the vulnerabilities within the discovered vulnerabilities only, but networks and systems can still be exploited with zero day vulnerabilities.

It is always better to think like a attacker for a pen-tester only then he can secure the web servers and other network misconfigurations present in the system and also mitigate it.

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] Du, W., & Mathur, A. P. (2002). Testing for software vulnerability using environment perturbation. Quality and Reliability Engineering International, 18(3), 261-272.

[5] Reddy, M. R., & Yalla, P. (2016, March). Mathematical analysis of Penetration Testing and vulnerability countermeasures. In Engineering and Technology (ICETECH), 2016 IEEE International Conference on (pp. 26-30). IEEE.

[6] Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques, 11(1), 27-49.

[7] Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. Procedia Computer Science, 57, 710-715.

[8] CVSS documentation, Forum of Incident Response and Security Teams, http://www.first.org/cvss/cvss-guide.html.

[9] http://www.ist-magnet.org/ MAGNET beyond/D4.4.2 "Analysis, Verification and Evaluation", June 2008

[10] S. A. Butler, "Security attribute evaluation method: a cost-benefit approach", Proceedings of the 24th ICSE, May 2002