IJARSCT

ISSN (Online) 2581-9429

IJARSCT
Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 3, Issue 1, January 2023

Penetration Testing Mechanisms

Nimala S
Instructor, Department of Computer Applications
Standard Fireworks Rajaratnam College for Women, Sivakasi, Tamil Nadu, India

Abstract: *In this paper we have to see Penetration Testing as the security testing which imitates cyber-attacks to identify the vulnerabilities of a system or a network to breach the system's security controls, by a pseudo-enemy attack by a friendly evaluation team on a computer system of interest to discover ways, it covers many protocols like HTTP, SIP, TCP/IP.*

Keywords: Vulnerability Assessment, Penetration Testing, Portfolio, Scrutinizing.

I. INTRODUCTION

Penetration testing is a part of cyber security which mainly deals with an attack simulation intended to expose the effectiveness of an application's security controls by highlighting risks posed by actual exploitable vulnerabilities Vulnerability assessment is an important techniques which ensure that our system is secure, this process is actually identify vulnerability and making a report. In penetration testing it is the process of evaluating and exploiting the vulnerability in any system, It is the extended process of vulnerability assessment also it includes scanning, enumerating, reporting the vulnerabilities.

1.1 Scanning

- Scanning includes different target, different websites, and different techniques when we scanning the open ports open service is running and their version number will do the vulnerability assessment.
- It provides a touch of various contexts to the results.
- Generally, vulnerability scans are per- formed either via unauthenticated or authenticated means. In an unauthenticated scan, a system is checked by the net- work point of view by trying to find open ports and testing for the utilization of exploits and attacks.
- An authenticated scan will perform a credentialed scan of the OS and applications trying to find misconfigurations and missing patches which will be taken advantage of by threat actors, like weak passwords, application vulnerabilities and malware.
- Part of the vulnerability assessment is only done from the attitude of getting an honest security posture.

1.2 Reporting

- After exploit the vulnerability then we reports all.
- Reporting vulnerability is critical because it indicates the output of the scan, the risk and importance of the devices and systems scanned, and the future steps that should be taken to patch the vulnerability. In vulnerability assessment, it's important that reporting must be actionable.

II. WHY PENETRATION TESTING

It is essential because identifies a simulation environment i.e. how an intruder may attack the system through white hat attack. It helps to find weak areas where an intruder can attack to gain access to the computer's features and data. It supports to avoid black hat attack and protects the original data. It estimates the magnitude of the attack on potential business. It provides evidence to suggest, why it is important to increase investments in security aspect of technology. Important goal of vulnerability assessment is to identify security vulnerabilities under controlled circumstances so they can be eliminated before unauthorized users exploit them. Computing System professionals use penetration testing to address problems inherent in vulnerability assessment, focusing on high-severity vulnerabilities. Penetration testing is a valued imprisonment, or ultimate failure Penetration testing, as a proactive service, provides unassailable information that helps the organization to meet the auditing or

DOI: 10.48175/IJARSCT-7842

compliance aspects of regulations. A single incident of compromised client data can be devastating. Loss of consumer confidence and business reputation can put the entire organization at risk. Penetration testing creates heightened awareness of security's importance at all levels of the organization. This helps the organization avoid security incidents that threaten its corporate image, put its reputation at risk and impact customer loyalty assurance assessment tool that benefits both business and its operations. Industry has mandated regulatory requirements for computing systems. Non-compliance can result in the organization's receiving heavy fines

Using the results of penetration testing requires proper interpretation. Neither testers nor sponsors should assert that the penetration test has found all possible flaws, or that the failure to find flaws means that the system is secure. All types of testing can show only the presence of flaws and never the absence of them. The best that testers can say is that the specific flaws they looked for and failed to find aren't present; this can give some idea of the overall security of the system's design and implementation. Penetration testing is effective because it lets us consider a system as it's actually used, rather than as it's expected to be used. It's some-thing to which all computer security students should be exposed

2.1 Strategies of Penetration Testing

- External testing: This involves attacks on the organization's network perimeter using procedures performed from outside the organization's systems, e.g., the Extranet and Internet.
- Internal testing: Performed from within the organization's environment, this test attempts to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network.
- Blind testing: In this case, the tester tries to simulate the actions of a real hacker. The testing team has little or no information about the organization but instead must rely on publicly available information (such as corporate website, domain name registry, etc.) to gather information about the target and conduct its penetration tests.
- Double blind testing: In this exercise, only a few people within the organization are made aware of the testing. The IT and security staff are not notified or informed beforehand, and as such, they are "blind" to the planned testing activities. Double-blind testing helps test an organization's security monitoring and incident identification processes, as well as its escalation and response procedures.
- Targeted testing: Also known as the lights-turned-on approach, target testing involves both IT and penetration testing teams. Testing activities and information concerning the target and the network design are known going in. Targeted tests require less time and effort than a blind test, but typically don't provide as complete a picture of an organization's security vulnerabilities and response capabilities as other testing strategies.

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyber attacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.

2.2 Applications

- Find if someone could change the votes recorded on the system.
- Find if someone could alter the firmware on the system to display votes correctly but store them incorrectly.
- Find if specific policies and procedures sufficiently prevent attackers from changing the results.

III. RESULT

At the result, of this are you need to detect where you weak, this test eliminates the window of opportunity for those with ill intent. That's when penetration testing comes into play. Penetration job entail scrutinizing every nook and cranny of your systems

DOI: 10.48175/IJARSCT-7842

IV. CONCLUSION

The goal of the test is high level overview of the findings, we must convey our findings to a customer in a meaningful way, we have to tell them what they are doing correctly, where they need to improve secure their posture, and how you got in, what you find, how to fix problems, and so on, so overall conclusion is the write the good penetration report is an art that takes practice to master.

REFERENCES

[1]. Wikipedia

[2]. https://www.ijert.org/vulnerability-assessment-and-penetration-testing

[3]. https://sci-hub.se/10.1109/MSP.2007.159

[4]. Georgia widman foreword by Peter Van Eeckhoutte "Hands on Introduction to Hacking" ISBN-10:1-59327-564-1, ISBN-13:978-1-59327-564-8