OBE December 2021

Date and time of Exam :- 15th Dec. 2021, 9:00AM

Examination Roll Number :- 19234757006

Name of Program :- Master of Computer Application

Semester :- V

Unique Paper Code (UPC) :- 223402501

Title of Paper :- Cyber Security

Name of the Dept. :- Dept. of Computer Science

Email-ID :- anubhav.mca19.du@gmail.com

Mobile No. :- 9044490197

No. of Pages used :- 4

192347570006

(3). • Difference b/w penetration testing and vulnerability assesment :-

⇒ Penetration testing replicates the actions of an external or internal cyber attackers that is intented to break the information security and hack the valuable data or disrupt the normal functioning of the organization. So with the help of advanced tools and techniques, a penetration tester ~~makes~~ makes an effort to control the System and acquires data acess to sensitive data.

⇒ Vulnerability Assessment is the technique of identifying and measuring security vulnerability in a given enviroment. It is comprehensive assesment of the information security position. Further, it identifies the potential weakness and provides the proper measure to either remove those weakness or reduce below the risk level.

⇒ Vulnerability assesment doesn't validate results, there's always room for false positives.

⇒ Unlike Vulnerabldity assesment, when performing a penetration test the vulnerabilities are discovered through manual probing using a customized toolset that would otherwise not be uncovered in a Vulnerability assesment.

19234757006

PAGE NO.
DATE :

- Is Penetration testing still important if company has a firewall?

Yes, even if a software system has a firewall, penetration testing is still important. The purpose of firewall penetration testing is to prevent unauthorized access to the internal network from the internet.

Penetration testing can involve the attempted breaching of any no. of system applications (API, frontend/backend servers) to uncover vulnerabilities. Insights provided by the penetration test can be used to find and fine-tune software firewalls weaknesses.

- Who needs Penetration testing and why do they need it?

Organizations with an online presence, web or mobile application or connected digital infrastructure should perform penetration testing.

A penetration test should be performed on any type of connected and even non-connected technology after implementation or development and prior to its go-live phase. It is also recommended to perform penetration test on a periodic basis and also after changes are made as new

19234757006

vulnerabilities are discovered over time and need to be identified and validated as to how they can be exploited or chained with other vulnerabilities. to gain access to a target.

Also, organization that require to meet compliance standards such as PCI-DSS v3.0 requirement 11.3 whose penetration testing is required on a regular basis also need to perform penetration testing.

- Steps Involved in Penetration testing :-

There are five main steps (Stages) in penetration testing :-

(1). Planning and Reconnaissance :- It involves the definitions of the scope of goals of a test and gathering of intelligance to better understand how a target works.

(2). Scanning :- In this step, we understand how the target application will respond to various intrusion attempts. This is typically done using Static & dynamic Analysis.

(3). Gaining Access :- This step uses web-application attacks, such as cross-site scripting etc.

(4). Maintaining Access :- The goal of this step is to see if the vulnerability can be used

to achieve a persistent presence in the exploited system long enough for a bad actor to gain in depth access.

(5). Analysis :- The result of the penetration testing are the compiled into a report detailing specific vulnerabilities, sensitive data and amount of time pen tester was able to remain in the system undetected, etc.

- Hurdles faced during penetration testing :-

1. Penetration testing is facing many hurdles in the information security landscapes. The limited scope of penetration testing with temporal-spule boundaries makes it hard mission, especially in production enviroment.

2. During a penetration testing, we can't cover all the vulnerabilities and threats.

3. Sudden and unexpected techical incidents due to heavy scanning and automated tools.

4. Estimating that the bugs fixed during the test ensure complete security to the system.