PT INTRO

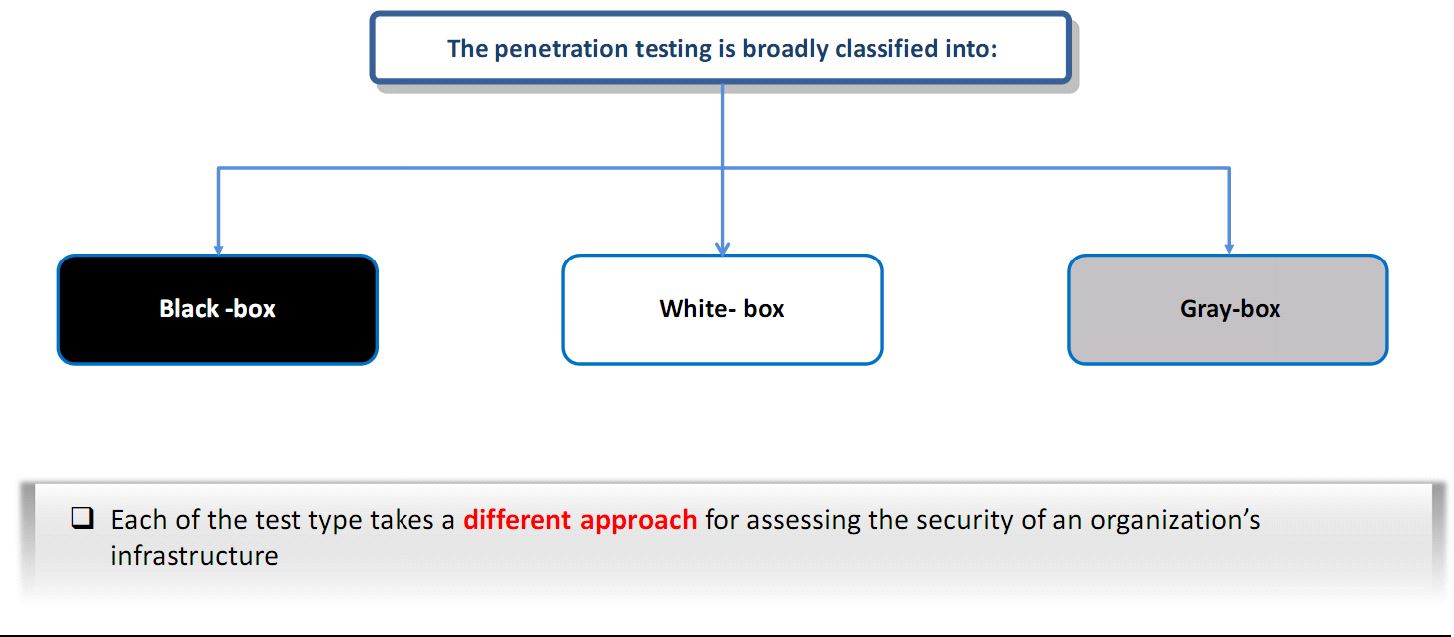
14 June 2021

23:44

**What is Penetration Testing**

* + Penetration testing is one of the types of security testing which evaluates an organization's ability to protect its infrastructure such as network, applications, systems and users from external as well as internal threats.
  + It is an effective way of determine how well the organization's security policies, control and technologies are working.
  + It involves the active evaluation of the security of the organization's infrastructure by simulating an attack like what an attack does.
  + During Penetration test, security measures are actively analyze for design weaknesses, technical flaws, and vulnerabilities.
  + The results of test are documented and delivered in a comprehensive report to executive management and technical.

**Types of Penetration testing**

* + 

* + **Black-box Penetration testing**
    - In a black box penetration test, no information is provided to the tester at all.
    - Black-box testing assumes that the pen tester has no previous knowledge of the infrastructure to be tested.
    - Tester only know the limited information about the target company.
    - Penetration test must be carried out after extensive information gathering and research
    - This test simulates the process of real hacking and gathers publicly information such as domain name and IP address.
    - It is time consuming and expensive.

* + **White-box Penetration Testing**

White box penetesting involves sharing full network and system information with the tester, including network maps and credentials. A white box penetration test is useful for simulating a targeted attack on a specific system utilizing as many attack vectors as possible.

* + You will be given complete knowledge of the infrastructure to be tested
  + It helps in revealing bugs and vulnerabilities more quickly

* + **Grey box penetration testing**
    - This test is the combination of black-box and white-box penetration testing.
    - The tester usually has a limited knowledge of information.
    - Test applications for all vulnerabilities, which a hacker might find and exploit.
    - Grey box testing is useful to help understand the level of access a privileged user could gain and the potential damage they could cause.

**Common Area of Penetration Testing**

* + **Network Penetration Testing**
    - Helps you identify security issues in network design and implementation.
    - Common network security issues:
      * Use of insecure protocols
      * Unused open ports and services
      * Unpatched OS and software
      * Misconfiguration in firewalls, IDS, Servers, workstation, network services, etc.

* + **Web Application Penetration Testing**
    - Web application penetration testing is the process of using penetration testing techniques on a web application to detect its vulnerabilities.
    - It is similar to a penetration test and aims to break into the web application using any penetration attacks or threats.
    - Common Web application security issues:
      * Injection vulnerabilities
      * Broken session management
      * Weak Cryptography

* + **Social Engineering Penetration Testing**
    - Helps you identify Employees that do not properly authenticate, follow, validate, handle, the process and technology.
    - Common issues with employees that can pose serious security risk to the organization.
      * Clicked on malicious emails.
      * Becoming victim of phishing emails and phone calls.
      * Revealing sensitive information to strangers
      * Connecting a USB to workstation.

* + **Wireless Network Penetration Testing**
    - Helps you identify misconfiguration in wireless network infrastructure.
    - Common security issues in wireless network infrastructure
      * Insecure wireless encryption standards
      * Default password
      * Misconfiguration

* + **Mobile Device Penetration Testing**
    - Helps you detect security issues associated with mobile devices and their uses
    - Common security issues with mobile devices
      * Use of unauthorized mobile device
      * Ise of rooted or jailbroken mobile devices
      * Weak security implementation on mobile devices
      * Getting connected with insecure WIFI network

* + **Cloud Penetration Testing**
    - Helps you to identify security issues in cloud infrastructure
    - Despite the traditional security issues, cloud services also face the following cloud specific security issues.
      * Insufficient protection to data at rest
      * Insecure interface and APIs
      * Security threats from insider
      * Poor user access management

**Penetration Testing Process**

* + **Define the scope**
    - The extent of testing
    - What will be tested
    - From where it will be tested
    - By whom it will be tested

* + **Performing the penetration test**
    - Involves gathering all the information significant to security vulnerabilities
    - Involves testing the targeted environment, such as network configuration, topology, hardware, and software.

* + **Reporting and Delivering results**
    - Listing the vulnerabilities
    - Categorizing risks as high, medium, and low
    - Recommending repairs, if vulnerabilities are found

**Penetration Testing Phases**

* + **Pre-Attack Phase :-** Research (information gathering)
  + **Attack Phase:-** Testing/Exploiting
  + **Post-Attack Phase:-** Documentation and Reporting

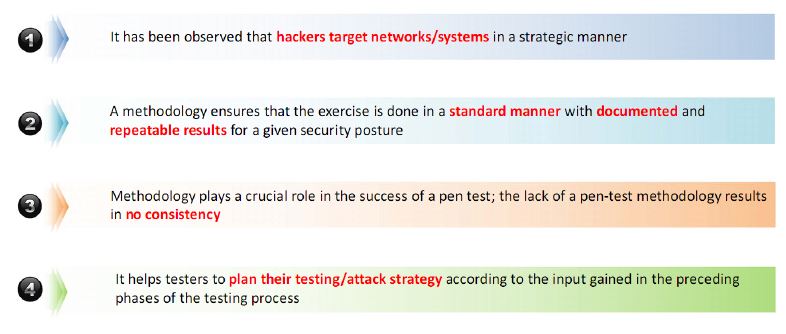
**Penetration Testing Methodologies**

Various penetration testing framework and methodologies exist to help organization choose the best method to conduct a successful penetration test.

**Most commonly used methodologies:**



**Need for a Methodology**



**LPT Penetration Testing Methodology**

