Penetration Testing:- Also known Pen Testing. Penetration Testing is aprocess of Hacking a System, to evaluate Security, Hack value attacks, exploits, Zero-day vulnerability & Other components such as threats, vulnerabilities and daisy Chaining

Penetration Testing is use to find weakness/vulnerability of System, Device and Application S/w to protect Hacker attack

Most of time Hacker enter in a System through port (65535)

Penetration Testing help developer to secure the System/Application

Types of Penetration Testing:-

(i) Black Box:- The black box is a type of penetration testing or double blind testing in which Pen tester have no prior knowledge of System.

(ii) Gray Box:- ~~G~~ In this type of testing, ~~for~~ tester have little bit information about targets such as IP Address

(iii) White box:- Tester have complete information about target like ~~open~~ Port, IP Address, MAC Address.

Major Tool for Penetration Testing

(i) Kali Linux:- Find technical weakness of System, Application, Network & Wi-fi

(ii) viasat:- ~~I~~ Network Protocol analyzer. Available for Windows, MAC & Linux OS.

(iii) Nessus:- This is automated Penetration Testing tool

Penetration Testing Stages:-

(i) Planning & reconnaissance:- The first stage involved

(a) Defining the Scope & goal of a Test.

Gathering Intelligence (eg Network & domain Names, mail Server) to understand how a target works & its potential weakness.

(ii) Scanning :- This Step help to understand how the target application will respond to various intrusion attempts This is typically done using

(a) Static analysis :- Inspecting an application code to estimate the way it behaves while running

(b) Dynamic Analysis :- Inspecting an application's code in a running State. This is more practical way of Scanning

(iii) Exploitation :- This Stage uses web application attacks, such as cross-site Scripting, SQL Injection and backdoors to uncover a target's vulnerabilities. Testers try and exploit these ~~vad~~ weakness, typically by escalating privileges, stealing data, intercepting traffic etc, to understand the damage they can cause.

(iv) Post Exploitation & Maintaining Access : The goal of this stage is to see if the vulnerability can be used to achieve a persistence presence in the exploited system - Long enough for a bad actor to gain in-depth access. The result of the penetration test are then compiled into a report dialing

- Specific vulnerabilites that were exploited.
- Sensitive data that was accessed.
- The amount of time the Pen tester was able to remain in the System undetected.

Sumit Agarwal
9968132130