Information Security: Level #4

Module #12

Penetration testing: An Introduction

Different Terms used by an organization interchangably:

Security Audit or Network/Risk Assessment or

Penetration testing

Definition of:

Security Audit: Measurable Technical assessment of system(s) or application(s)

Network Assessment: Evaluation of risks/vulnerabilities in systems/applications/processes

Penetration Testing: Goes beyond. Would don the hat of a malicious hacker and attack those vulnerabilities

Penetration testing: An Introduction

Penetration testing would attempt to verify which vulnerabilities are genuine – Real positive vs. false positive

Effective Penetration tests are those which target a specific system with a specific goal

Quality over Quantity is true test of a successful Penetration test

By carefully choosing valuable targets, a Penetration Tester can determine the entire security infrastructure and associated risk for a valuable asset.

Does Penetration testing make networks secure?

This is a common MYTH!!

Penetration testing evaluates ONLY the effectiveness of existing security

Penetration testing should be done ONLY after the customer has exhausted all efforts for securing the system

Scope of work for penetration testing defining what systems and applications are going to be targeted clearly

Over the next few sessions….

We will try to learn and answer the following questions:

How should the "possible targets" be researched?

How to identify potential vulnerabilities in different types of applications

How to defend applications against common attacks?

How can one offer a suite of penetration testing services?

Penetration testing: Web application

Web Application

Defined as an application that would use a web browser as a client.

Could vary from a simple messaging application to storage in a cloud

Access to these applications would typically be through an industry standard web browser

Web applications are the standard for most of the Internet based applications

Even in hand held devices like Smart phones/tablet devices web applications are what is running

Web Application Penetration testing: Scope

Scope could drastically vary owing to the types of application usages as well as the number of possible business use case combinations

E.g. For performing penetration testing of a mobile device web application hosted on a Linux server

The following could be the scope:

a) Evaluating the Linux server (OS, NW config etc.)

b) Applications on the server

c) Authentication mechanism of users

d) Communication mechanism between the nodes

Web Application Penetration testing: Scope

Non-technical areas of this project scope could include:

- Acquisition mechanisms of devices by the users
- Possible uses of device usage other than this application
- Policies related to the maintenance of the server/network

Penetration testing: Methodology

- Black box testing
- White box testing
- Gray box testing
  - Blend between black box and white box testing

Penetration testing: Black box testing

- Tester does not possess any knowledge of target network, company processes or services
- Requires a lot of reconnaissance
- Longer engagement since the real hacker can spend a lot of time studying targets before launching attacks

Penetration testing: White box testing

- Tester has intimate knowledge of the system.
- Tester is provided with a lot of details about the system, network topology, company processes etc.
- More focussed on meeting a compliance need rather than a generic assessment
- Typically performed by inner security testing groups

Penetration testing: Gray box testing

- Falls in between black box and white box testing
- Owner feels that some unknown information might be discovered by the penetration tester and tells a particular part to be skipped.
- Provided basic details of the target but privileged information is not shared

Real attackers: Profile

- Tend to have some information about a target before making attacks
- Attackers choose a specific target
- Highly motivated and would have interacted with the target in some way possibly before the attack
- Since Real attackers use the Gray box attack typically, the penetration testers also tend to follow the gray box testing methodology

Penetration testing : Scope contents

- Target System(s) identification
- Workframe time requirement
- Evaluation of targets
- Software and Tools used for penetration testing
- Stakeholders of this penetration testing
- Initial access level that is provided to tester
- Target space definition – What parts of the target is the testing to target?
- What is the level of compromise on the targeted system?
- Deliverable from the penetration testing

Thank You