Introduction To Penetration Testing

Contents

- Introduction to Penetration testing.
- Types of Penetration testing.
- The objects of Penetration testing.
- Benefits of Penetration Testing.
- The locations of Penetration testing.
- Penetration test Process overview.
- Penetration testing standards.
- Setting up virtual lab.

1. Introduction to Penetration testing

How to improve your system security?

- Vulnerability Assessment
- Penetration Testing

Vulnerability Assessment

- A vulnerability is an assessment where you identify areas in the configuration that make your system vulnerable to an attack or security incident.
- Using tools: Nessus, Nexpose, Microsoft Baseline Security Analyzer, …
- The software is not performing attacks on the system, it simply checks the configuration of the system => Passive Assessment

nexpose®

acunetix

Vulnerability Assessment

Vulnerability assessment for Operating system:

- Unused accounts
- Administrative accounts
- Unpatched operating system
- Unpatched software
- Vulnerability software

Characteristics of vulnerability assessment

- **Passively testing security controls:** you are not actually trying to hack into the system or exploit it.
- **Identify vulnerability:** identify vulnerabilities, or weaknesses
- **Identify lack of security controls:** when performing a vulnerability assessment, you are looking to identify of there are any security controls that should be used that are not currently being used

Characteristics of vulnerability assessment

- **Identify common misconfigurations**
- **False positive:** somethings that is being reported as a vulnerability, but it is not.

Penetration Testing

- **Penetration testing or pentesting**: involves simulating real attacks to assess the risk associated with potential security breaches.
- Using many tools and techniques, the penetration tester attempts to exploit critical systems and gain access to sensitive data.

Penetration Testing characteristics

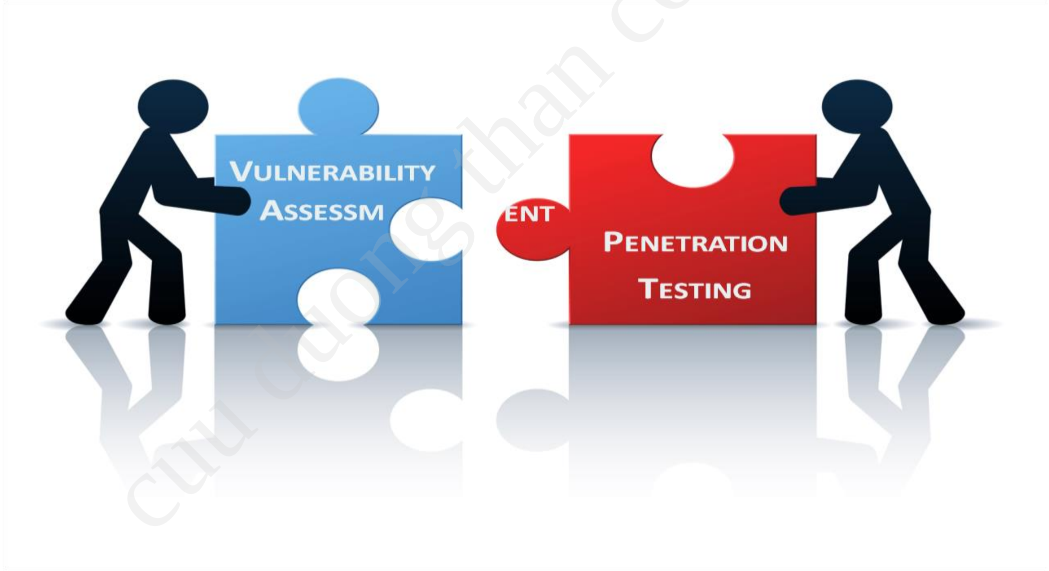
- Verify a threat exists
- Bypass security controls
- Actively test security control
- Exploiting vulnerabilities

Difference: Penetration Testing vs Vulnerability Assessment?

	Vulnerability Assessment:	Penetration Testing
Purpose	Identify, rank, and report vulnerabilities but does not exploit them	Identify ways to exploit vulnerabilities
Tools	Automated	manual
Difficult level	Administrator or inexperienced security professional	Penetration tester (higher skill level)
Price		Higher
Time		longer

Penetration Testing vs Vulnerability Assessment

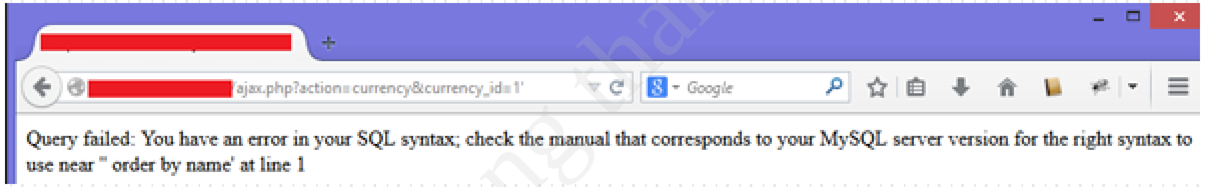
- Vulnerability Assessment is not Penetration Testing
- Penetration testing expands upon vulnerability assessment



Penetration Testing vs Vulnerability Assessment

Example:

- Vulnerability Assessment: using Acunetix tool to discover SQL injection link.

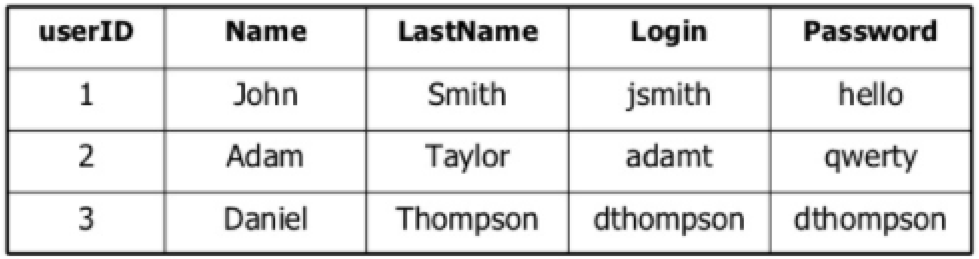


[redacted]

[redacted]/ajax.php?action=currency&currency_id=1'

Query failed: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' order by name' at line 1

- Penetration Testing: Using the result of vulnerability assessment to exploit database

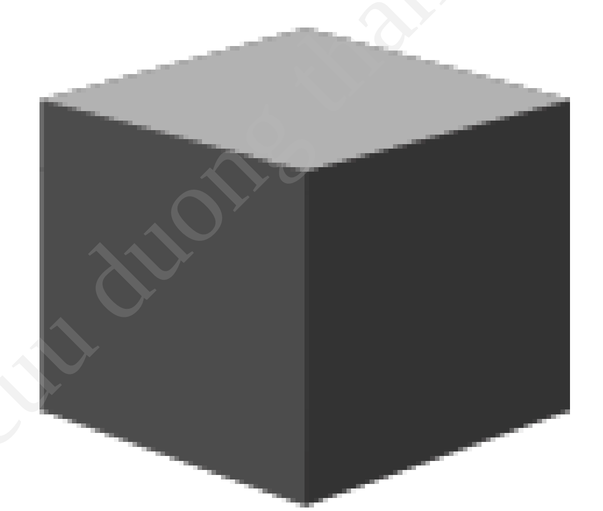


userID	Name	LastName	Login	Password
1	John	Smith	jsmith	hello
2	Adam	Taylor	adamt	qwerty
3	Daniel	Thompson	dthompson	dthompson

2. Types of Penetration testing.

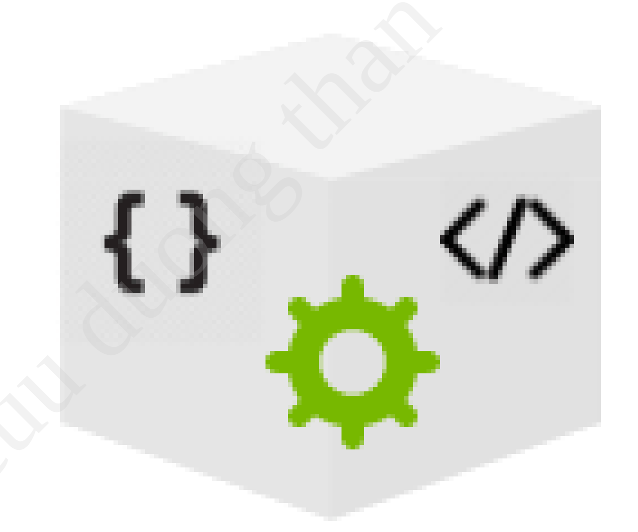
Black-box testing

- Penetration Tester is performed with no knowledge of the target system and tester must perform their own reconnaissance.



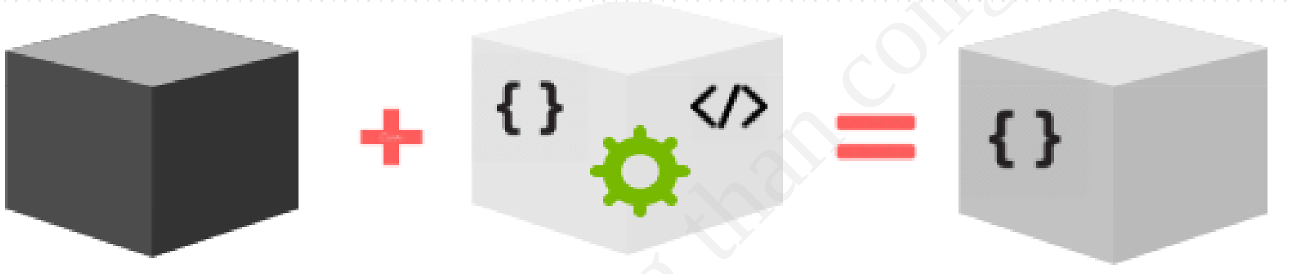
White-box testing

- Penetration Tester is given access to the source code and other relevant information that the company provides.



Gray-box testing

- Gray means partial knowledge



Black box White box Gray box

3. The objects of Penetration testing

The objects of penetration testing

- Network Penetration Testing
- Application Penetration Testing
- Web Application Penetration Testing
- Physical Penetration Testing
- Social Engineering

4. Benefits of Penetration Testing

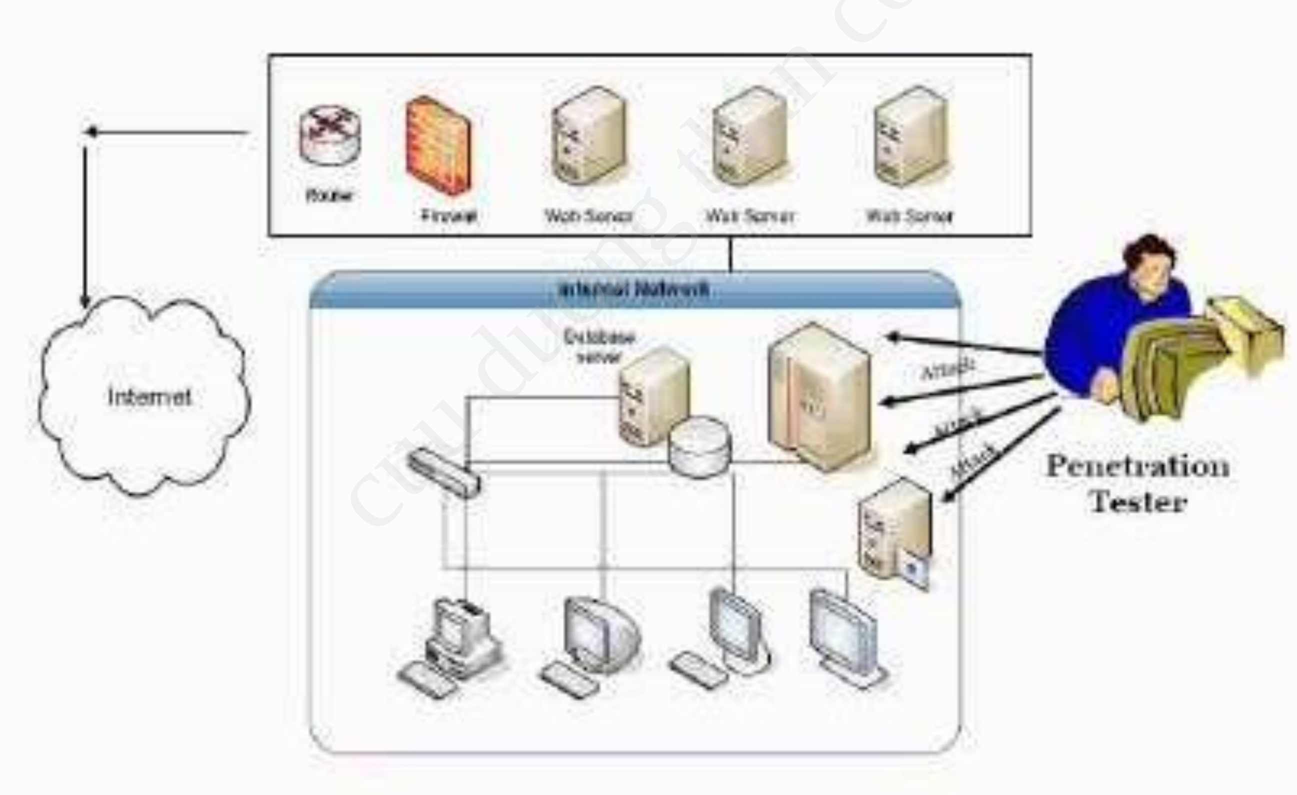
4. Benefits of Penetration Testing

- Penetration testing lists a set of vulnerabilities.
- Penetration testing shows the real risk of vulnerabilities.
- It tests your cyber-defense capability.
- It offers a third party expert opinion.
- It helps comply with regulations and certifications

5. The locations of penetration testing

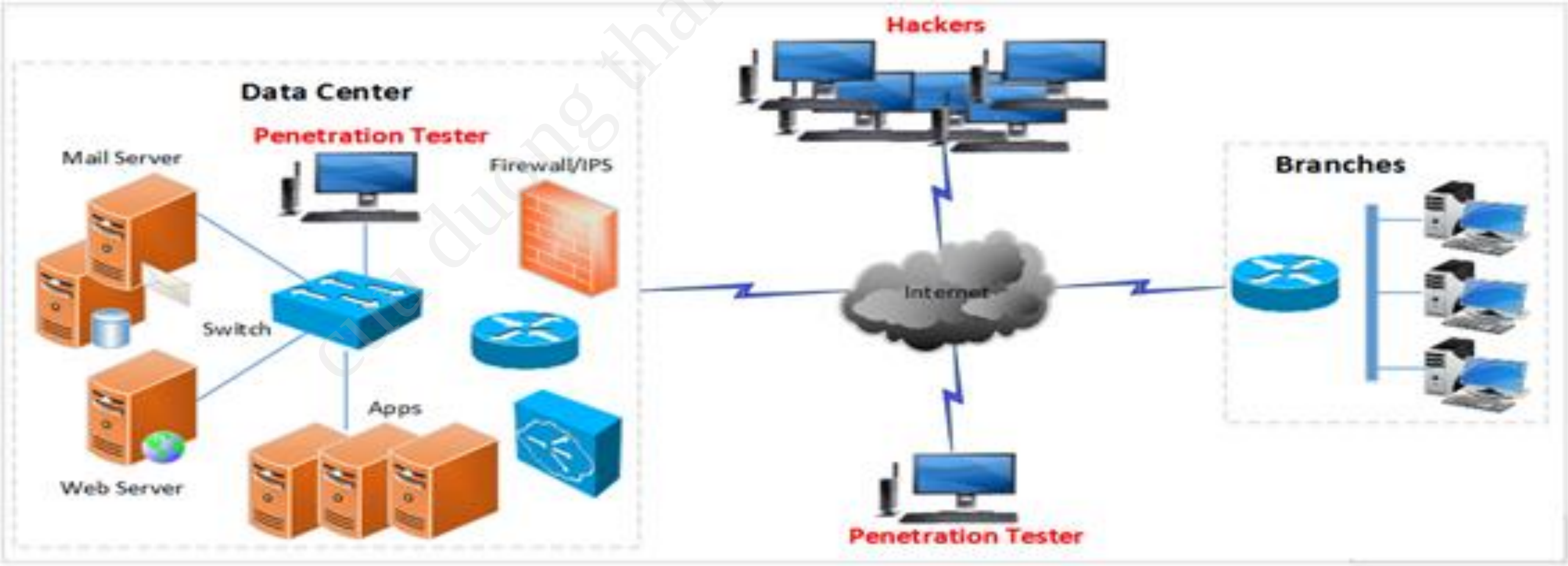
Internal Penetration testing

- Internal Penetration Test is to determine what systems a malicious insider would be able to access from within the internal structure of the network



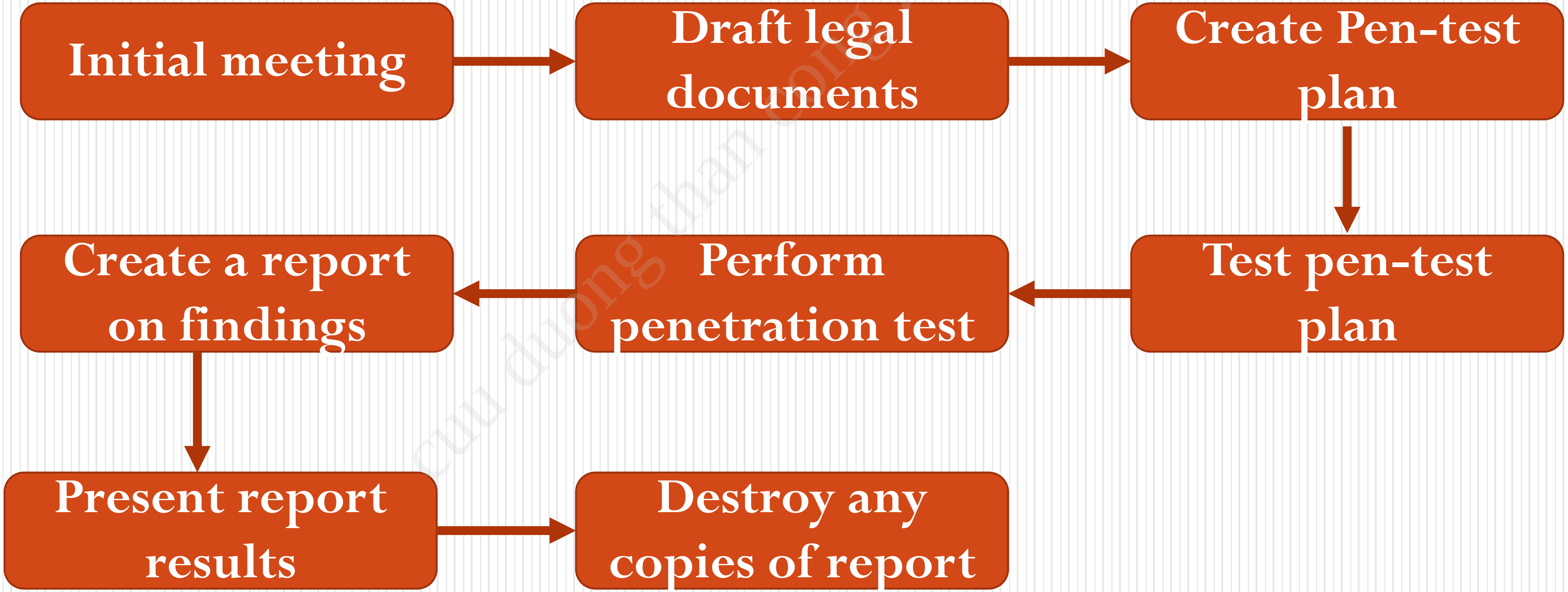
External Penetration testing

- External penetration testing is to identify vulnerabilities that are present for connections that have been established through the organization connected to the internet



6. Penetration test Process overview

Penetration test Process overview



Initial meeting

Draft legal documents

Create Pen-test plan

Test pen-test plan

Perform penetration test

Create a report on findings

Present report results

Destroy any copies of report

Determination of scope

Before you can accurately determine the scope of the test, you will need to gather as much information as possible:

- Does your customer understand the difference between a vulnerability assessment and a penetration test?
- What is the purpose of the test?
- Who has the authority to authorize testing?
- What is the proposed timeframe for the testing?

Determination of scope

- Are there any restrictions as to when the testing can be performed?
- Will you be conducting this test with, or without cooperation of the IT Security Operations Team?
- Is social engineering permitted?
- How about Denial of Service attacks?
- Are you allowed to see the network documentation or to be informed of the network architecture prior to testing to speed things along?

Determination of scope

- What are the IP ranges that you are allowed to test against?
- What are the physical locations of the company?
- Will additional permission be required once a vulnerability has been exploited?
- How are databases to be handled? Are you allowed to add records, users, and so on?

Determination of scope

Rules of engagement documentation:

- Proper permissions by appropriate personnel.
- Begin and end dates for your testing.
- The type of testing that will be performed.
- Limitations of testing (DDOS, Social engineering, …)
- IP ranges and physical locations to be tested.

Determination of scope

- How the report will be transmitted at the end of the test
- Which tools will be used during the test?
- Let your client know how any illegal data that is found during testing would be handled.
- How sensitive information will be handled.
- Contact information for both your team and for the key employees of the company you are testing.

Determination of scope

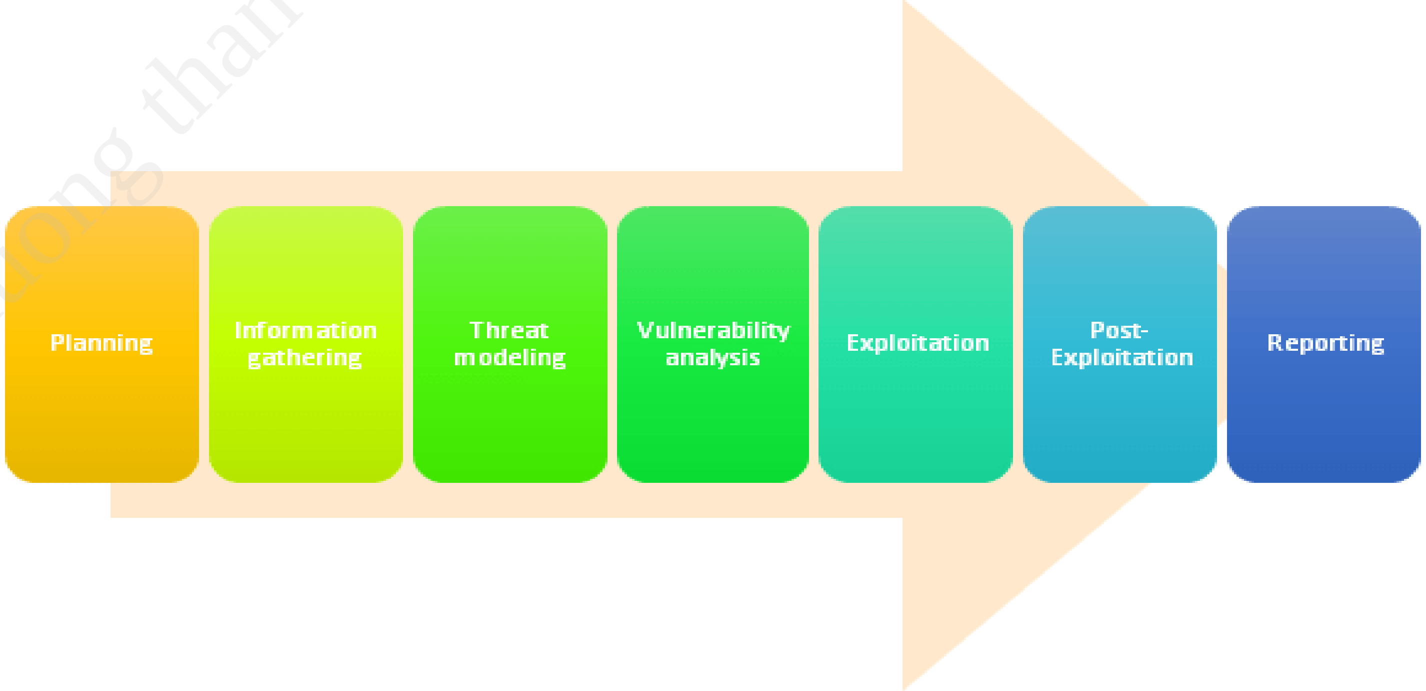
- An agreement of what you will do to ensure the customer's system information does not remain on unsecured laptops and desktops used during testing.

7. Penetration Testing Standards

Penetration Testing Execution Standard - PTES

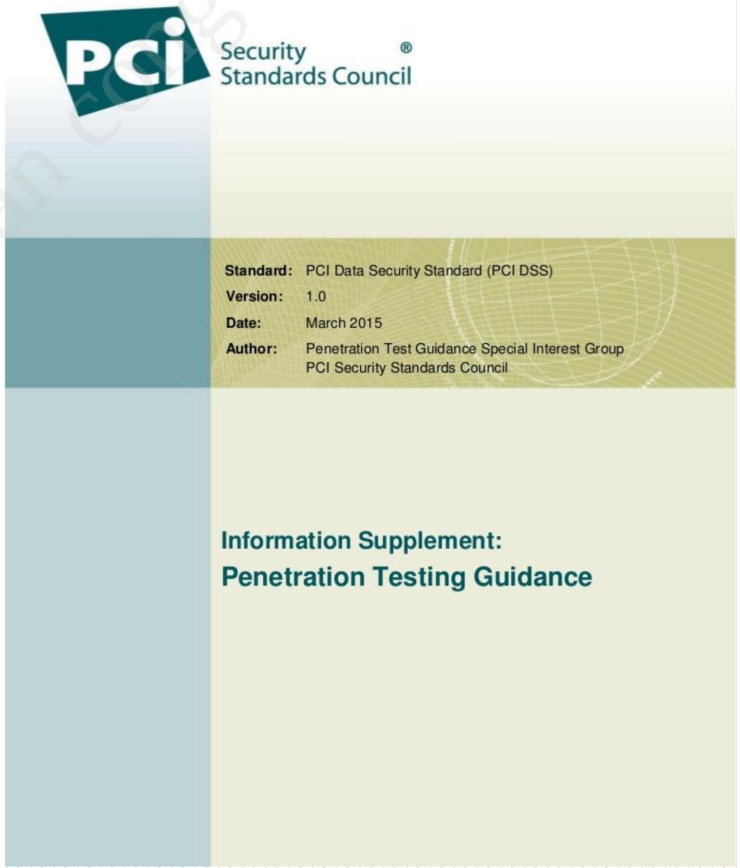
PTES (old but good)

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting



Payment Card Industry Data Security Standard

- PCI Information Supplement: Penetration Testing Guidance March 2015


PCI Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)
Version: 1.0
Date: March 2015
Author: Penetration Test Guidance Special Interest Group
PCI Security Standards Council

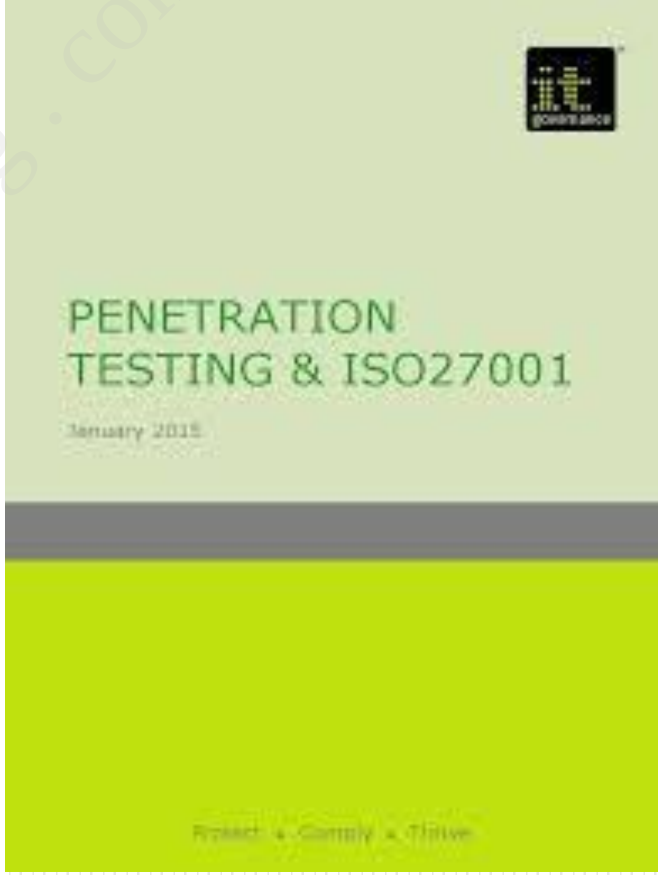
Information Supplement:
Penetration Testing Guidance

OWASP Testing Guide

- Web Application Security
- Excellent resource
- Detailed, practical methods

ISO 27001

- A component for obtaining an ISO 27001 certification is performing a penetration test. It provides insight into the current status of your security and shows where you need to improve.



PENETRATION
TESTING & ISO27001

January 2015

Protect • Comply • Thrive

8. Setting up virtual lab

Setting up virtual lab

- Installing VMware
- Setting Up Kali Linux
  - Configuring the Network for Your Virtual Machine
  - Installing Nessus
  - Installing Additional Software (mingw32, Hyperion, Veil-Evasion, Ettercap
  - Setting Up Android Emulators
  - Smartphone Pentest Framework

Setting up virtual lab

- Target Virtual Machines
  - Creating the Windows XP Target
  - Setting Up the Ubuntu 8 .10 Target
  - Creating the Windows 7 Target

Thanks