PENETRATION TESTING SERVICE

EXECUTIVE SUMMARY

A penetration test, more commonly known as a ‘Pen Test’ or ‘Ethical Hacking’, is a simulated attack on a computer system with the intention of finding security weaknesses that could be exploited.

Penetration tests and vulnerability assessments we are providing offer an independent view of your existing security processes. It also help establish whether critical processes such as patching and configuration management have been followed correctly.

Once the Penetration Test project is completed, You will achieve the following goals:

- Compliance with relevant standards and regulations
- Identification of weak points requiring urgent action
- Planning of security treatment from the perspective of risk assessment (optional)

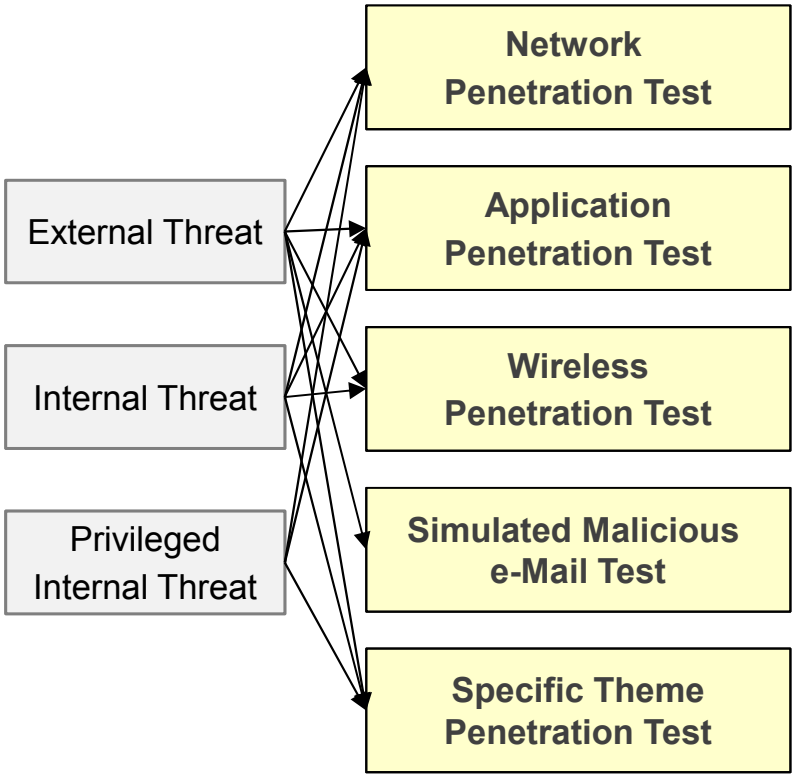
Related international standards and regulations

- ISO/IEC 27002:2013 : A12.6 Technical Vulnerability Management
- PCI-DSS Requirements: Requirement 11.3: Regularly test security systems and processes
- EU GDPR Regulation: Article 32 Security of Processing
- Rwanda RURA Regulation: Article 21 Vulnerability Assessment

SERVICE STRATEGY

In international standards such as ISO, ITU, USA NIST, EU ENISA and NATO CCD-COE, the type of network security threat is divided into internal threat, external threat, and privileged threat.

- External Threat: occurs when someone outside your network creates a security threat to your network
- Internal Threat: occurs when someone from inside your network creates a security threat to your network
- Privileged Threat: occurs when someone from privileged inside your network creates a security threat to your network



Identifies security problems within your network infrastructure. Network penetration testing is likely to involve scanning your network.

Detects security issues within a website or Mobile APP that could be exploited by a malicious attacker, resulting in irreparable damage or data theft..

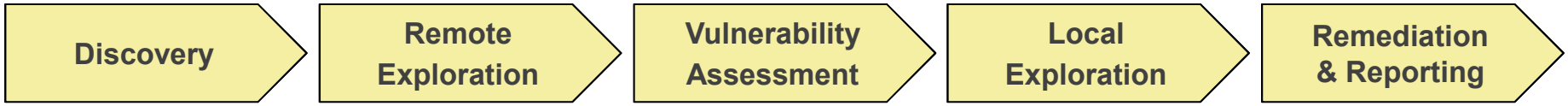
The objective of a wireless penetration test is to detect access points and rogue devices, analyze your configurations and test for vulnerabilities..

Detects security issues within a website or application that could be exploited by a malicious attacker, resulting in irreparable damage or data theft.

To test the security strength of specific services such as IP Telephony, Bank's ATM, and Air Traffic Control, attack scenarios for the target service have been designed and conducts.

METHODOLOGY

Penetration Testing consists of 5 phases from Discovery to Reporting. Depending on the Penetration Test Topic, many testing techniques are used in the detailed steps of each phase.



- Port Scanning
- Gathering Information
- Network Mapping

- Host Exploration
- Service Exploration
- Platform Exploration

- Vulnerability Research(CVE*, CWE**, etc.)
- Vulnerability Discovery
- Threat Classification

- Local Exploit Development
- Local Exploit PoC
- Privilege Escalation

- Risk Assessment
- Risk Treatment Plan
- Future Planning
- Reporting

PT-NW	Network Penetration Test
PT-AP	Application Penetration Test
PT-WR	Wireless Penetration Ttest
PT-ME	Simulated Malicious e-Mail Test
PT-SP	Specific Theme Penetration Test

* CVE: Common Vulnerabilities and Exposures
** CWE: Common Weakness Enumeration

CASES

- **Penetration Test Type**: External Penetration Test
- **Attack target**:
  A website for registering and managing SSN, Passport, etc. information of all citizens
- **Testing Results**
  : Remotely takeover Web administrator privileges and all DBMS Administrator's privileges of the target system via the Internet
- **Attack Narrative**
  a. Check opened TCP / 8580 with port scanning
  b. Vulnerability Information search for ‘JBoss JMX Console'(TCP/8580)
  c. Exploit Code Development (CVE-2010-0738)
  d. Exploit Code injection, and remote login
  e. Upload and execute Web shells(war file) with the Console Administrator privileges
  f. Web Console and DBMS administrator's authority takeover
- **Cause of attack success**
  - Open ‘JBoss JMX Console' service port
  - ‘JBoss JMX Console' patch not available

CASES

- **Penetration Test Type**: Specific-theme Penetration Test
  Tested employee's security awareness by randomly distributing CD with inserted malicious code in office
- **Attack target**:
  Any employee at headquarters
- **Testing Results**:
  Malicious code is inserted and randomly distributed CD is executed on its own PC, so that about 72% of employees infected with malicious code are collected in the logger server
- **Attack Narrative**
  a. Consultation for test scenario with a person in charge of client
  b. Malicious code development and safety testing with Excel file
  c. Insert malicious code into the CD entitled "2016 Internal Personnel Assessment Results"
  d. Developed Logger Server to collect infected PC information
  e. Randomly distribute a specially-produced CD to the head office
  f. Monitoring infection records on Logger server for 1 week
  g. Collecting Infection PC Information from the Logger Server
  h. Infection information analysis(by host, organizational unit) on the Logger Server
- **Cause of attack success**
  - Lack of information security awareness on treatment of removable media of employees