IT3789 Cyber Security Attack & Defence

L1 - Introduction to Penetration Testing

NANYANG POLYTECHNIC

WITH KNOWLEDGE COMES RESPONSIBILITY

Introduction to Penetration Testing

Enterprise Security Assessment

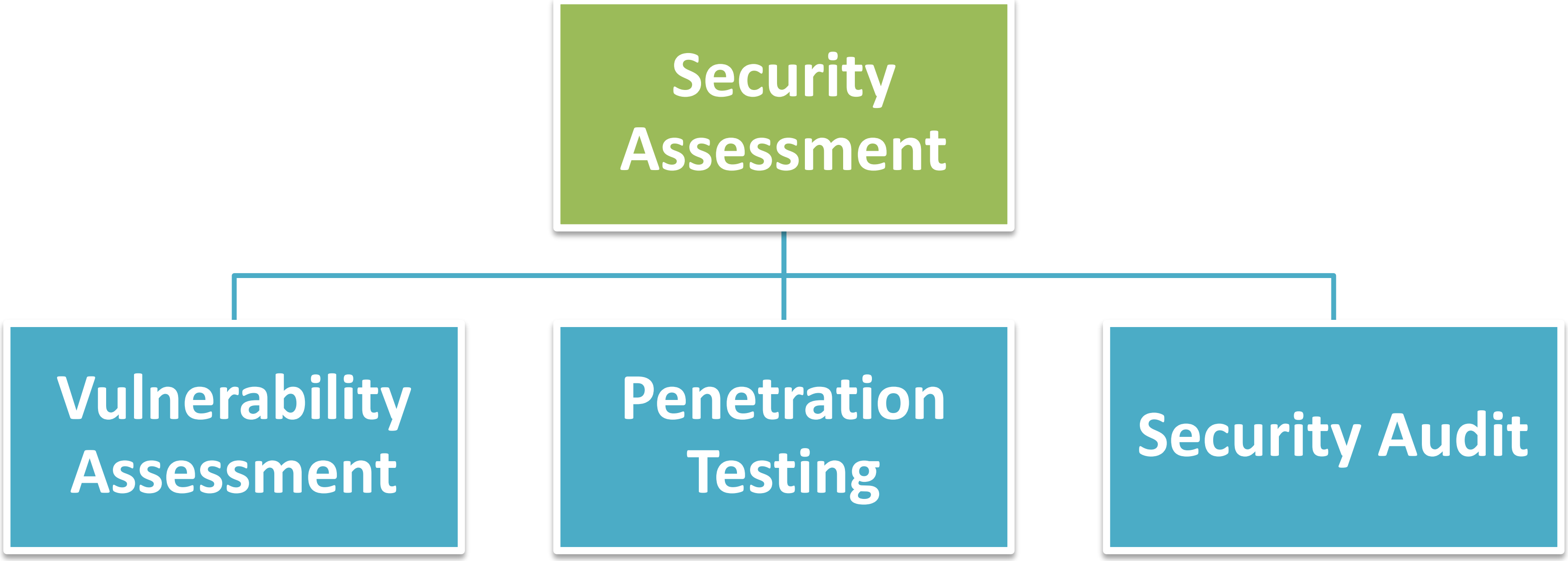
Penetration Testing

Code of Ethics

Enterprise Security Assessment

- Why?
  - – To assess an organization's security standards, processes and procedures.
  - – To discover vulnerabilities and risks that exist within an organization.
- Goal
  - – Ensure that necessary security controls are integrated into the systems within the organization.

Enterprise Security Assessment



Security Assessment

Vulnerability Assessment

Penetration Testing

Security Audit

Enterprise Security Assessment

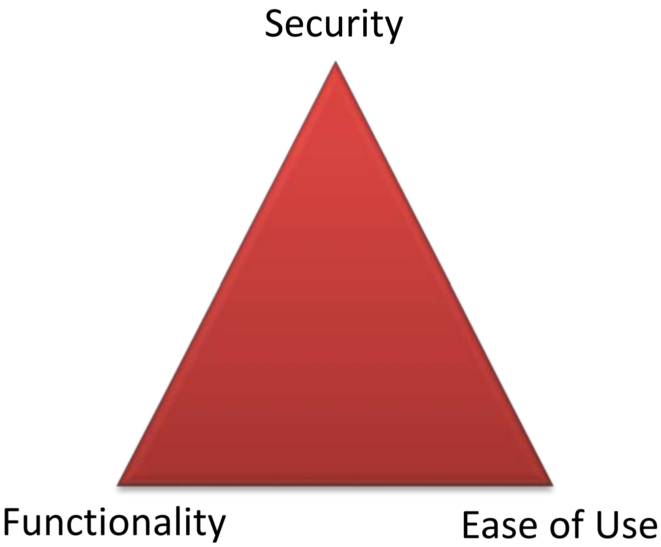
- Vulnerability Assessment
  - Focus on finding security vulnerabilities in systems.
  - Often does not involve exploitation of the discovered flaws.
  - Usually includes policy and procedure reviews.
- Penetration Testing
  - Focus on gaining access or obtaining information in target systems.

Enterprise Security Assessment

- Security Audit
  - Assess security risks faced by an organization.
  - Countermeasures against risks are tested against set of standards.
    - Example: ISO 27000 series (www.27000.org)
  - Reveals weaknesses in systems, practices and other key areas.

Security/Functionality/Ease of Use

- Increase and decrease in any one of the factors will impact the other 2 factors.
- Need to find a balance between the 3 factors.



Introduction to Penetration Testing

Enterprise Security Assessment

Penetration Testing

Code of Ethics

Penetration Testing

- Purpose
  - See things from an attacker’s perspective.
  - Use hacking skills and toolsets for defensive purpose.
  - Test systems and network for weaknesses.
    - Help to find mistakes that other approaches miss.
    - Fewer in-depth interviews but more debriefings and scope check.
  - Propose countermeasures for any vulnerabilities identified.

Hackers

- Can be classified into 3 groups.
  - White Hats
    - Ethical hackers who use their skills for defensive purpose.
  - Black Hats
    - Malicious hackers or crackers who use their skills for illegal or malicious purpose.
  - Gray Hats
    - Hackers who may work offensively or defensively depending on the situation.
    - May just be interested in hacking tools and technologies.
    - Self-proclaimed ethical hackers.
      - Usually have no permission to perform penetration testing.

Terminologies

- Threat
  - Environment or situation that could lead a potential breach of security.
  - Example: Hackers with malicious intent.
- Vulnerability
  - A flaw in system that may lead to execution of damaging instructions.
- Exploit
  - A code that takes advantage of a vulnerability in a system
  - Leads to unauthorized access, privilege escalation and denial of service.

Terminologies

- Target of evaluation (TOE)
  - System, application or network that is subjected to security analysis or attack.
- Attack
  - Occurs when a system is compromised by exploiting a vulnerability.
- Remote
  - Exploit is sent over network.
  - No prior access to target system or network.
- Local
  - Exploit is directly executed on the system or network.
  - Requires prior access.

Penetration Test Types

- Various types of penetration testing can be performed.
- Each types simulate an attacker with different levels of knowledge about target organization.
- Penetration test types
  - White box testing
  - Black box testing
  - Gray box testing

Penetration Test Types

- Black Box Testing
  - No prior knowledge of the infrastructure or system to be tested.
  - Testers must determine the locations and system configurations.
  - Simulates a real malicious attacker.
  - More time spent on information gathering.

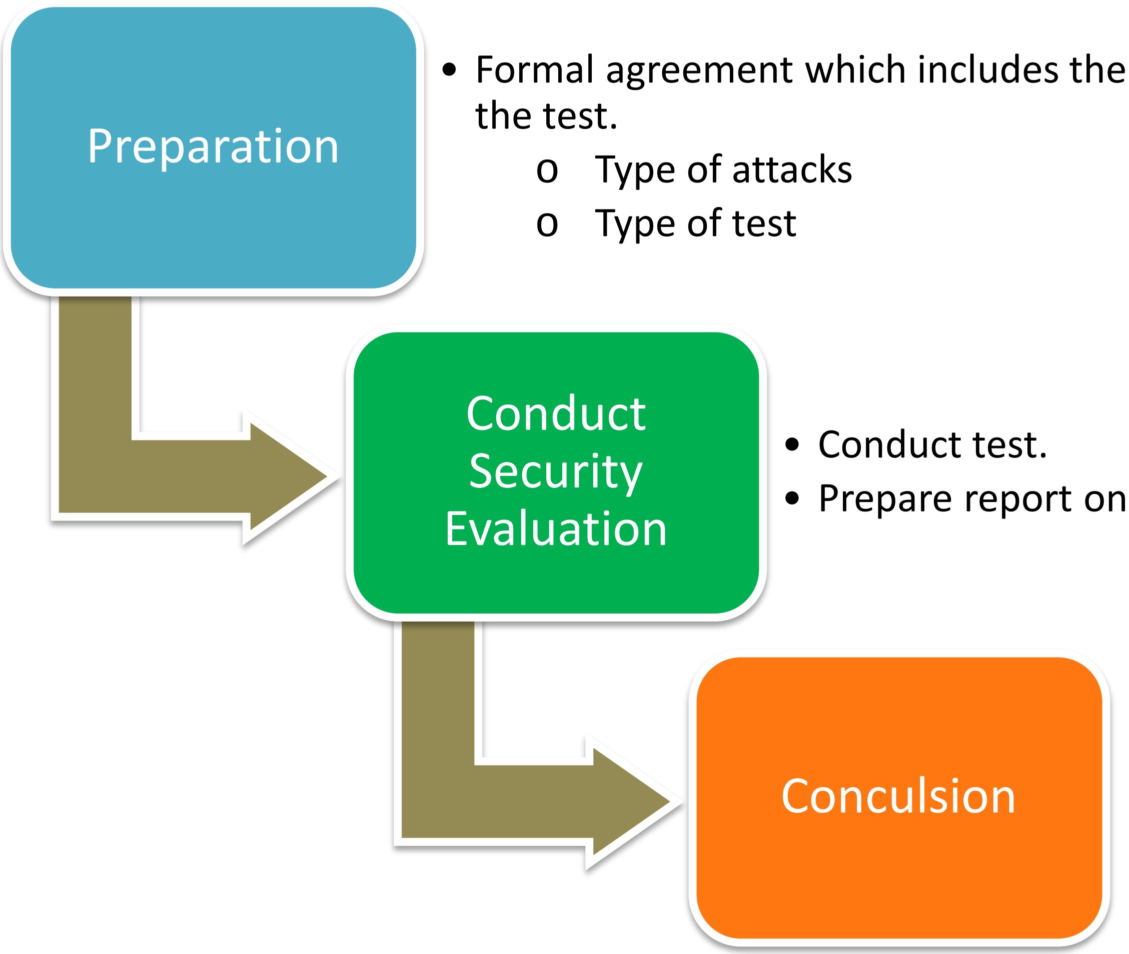
Penetration Test Types

- White Box Testing
  - Complete knowledge of network infrastructure.
  - Jumps right into the attack phase.
  - Avoid additional time and expense of black box testing.

Penetration Test Types

- Gray Box Testing
  - Perform a security evaluation and testing internally to examine the extent of access by insiders.
  - To simulate attacks that are initiated from within the network.
  - Test and audit level of access for employees and contractors.
    - Can privilege be escalated?

Performing Penetration Test



- Formal agreement which includes the full scope of the test.
    - Type of attacks
    - Type of test

- Conduct test.
- Prepare report on findings.

- Present findings.
- Recommend countermeasures.

Performing Penetration Test

- Penetration Tester **DOES NOT**…
  - fix or patch the vulnerabilities found.
  - Implement countermeasures.
- Deliverables of penetration testing.
  - Findings of test.
  - Analysis of associated risks.
  - Document findings by…
    - screenshots.
    - hacking tool output.
    - important log files.

Introduction to Penetration Testing

Enterprise Security Assessment

Penetration Testing

Code of Ethics

Keeping it Legal

- An penetration tester should know the penalties of unauthorized access into a system.
- Network penetration testing or security audit should not start till a signed legal document has been received.
- Consult lawyer.
- Need to find out the laws in various countries if penetration testing is performed across international borders.

Cyber Crime Laws in Singapore

- Computer Misuse and Cybersecurity Act (Chapter 50A)
  - Unauthorized access to computer material.
  - Access with intent to commit or facilitate commission of the offence.
  - Unauthorized modification of computer material.
  - Unauthorized use or interception of computer science.
  - Unauthorized obstruction of the use of computer.
  - Unauthorized disclosure of access code.
  - Enhanced punishment for offences involving protected computers.
  - Abetments and attempts punishable as offences.

Reference: http://statuts.agc.gov.sg

Getting Permission to Hack

- Gain authorization from client.
  - Signed contract for permission to perform test.
- Maintain and follow non-disclosure agreement (NDA) with client.
  - Maintain confidentiality when performing test.
  - No sensitive information gathered during test should be disclosed.
  - Information and results of the test should not be disclosed. Why?
- Perform the test up to the agreed-upon limits.

Company Obligations

- Ensure penetration tester is given just the necessary access to perform the test.
- Place safeguards to protect organization.
  - Network and system monitoring and logging targeted at penetration tester.
  - Escort the tester while on organization property.
  - Restrict data from leaving organization.
    - Usually in sensitive environments (e.g. military).
    - Documentations and equipment are not allow to enter or leave the organization.
    - If equipment are allowed, then they must be sanitized before leaving.

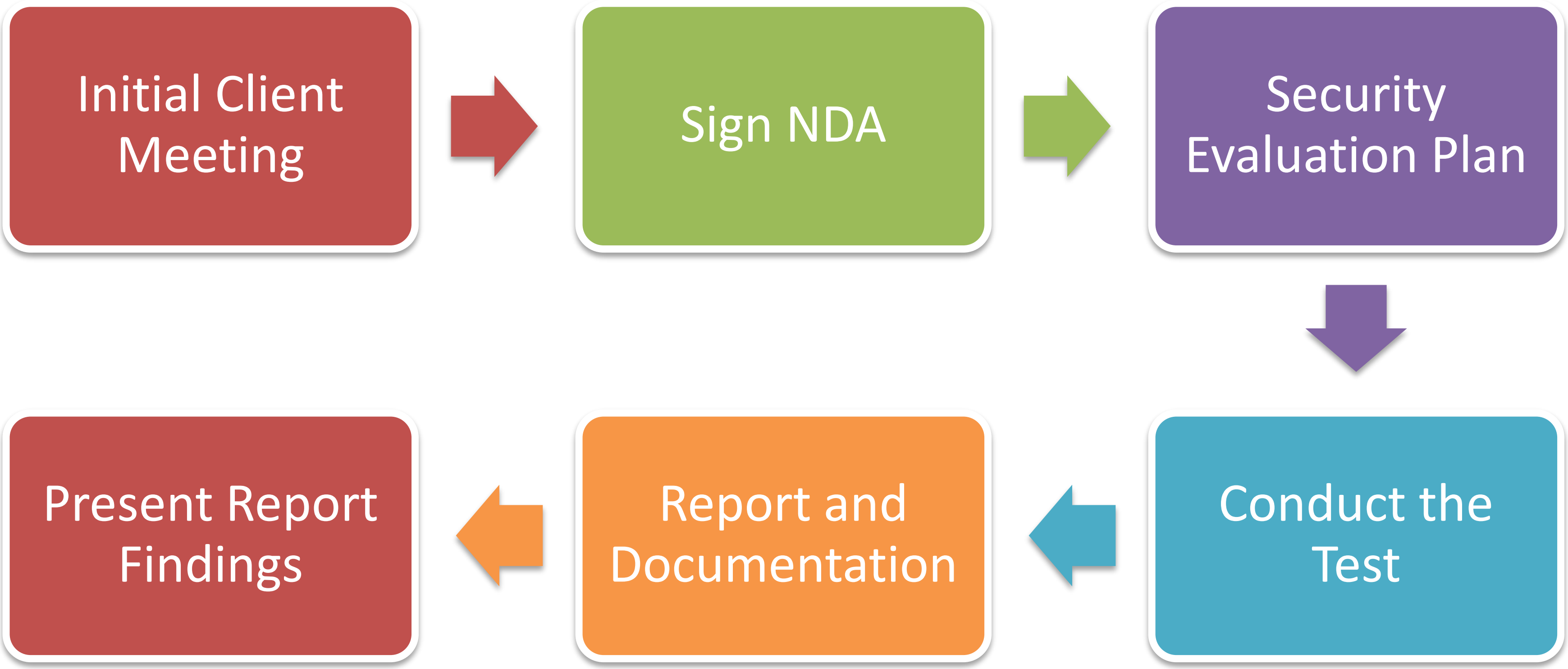
Contractor Obligations

- There should be a clause to indicate how can penetration tester use the information gathered.
  - Tester will only disclose information to employees with a “need to know”.
- Delivery and destruction of data.
  - Test must be completed within agreed time frame.
  - Present client with certificate of destruction.
    - Certificate contains detailed list
      - Information disposed.
      - Date of destruction.
      - Who authorized the destruction?
      - Who witness the destruction?
  - Method of destruction.
    - Maybe dictated by client.

Auditing & Monitoring

- Client audits tester’s systems to ensure that the tester is compliant with the contract.
  - How are data managed, store and transferred?
- Monitoring is done so that client feels confident that the tester is only performing tests that is stated in the contract.
  - If tester realized that there is a need to step outside contracted boundaries, he has to stop all activities and negotiates agreement.
    - A new contract may be required.

Security Audit Steps



Initial Client Meeting

Sign NDA

Security Evaluation Plan

Conduct the Test

Report and Documentation

Present Report Findings

Introduction to Penetration Testing

Enterprise Security Assessment

- Why?
- Goal
- Security Assessment

Penetration Testing

- Penetration Test Types
- Performing Penetration Testing

Code of Ethics

- Cyber Crime Laws in Singapore
- Getting Permission to Hack