# IT3789 Cyber Security Attack & Defence


## L4 – Penetration Testing Methodology

# WITH KNOWLEDGE COMES RESPONSIBILITY

# Penetration Testing Methodology

**Penetration Testing Methodologies**

**PMBOK**

**ISSAF**

**OSSTMM**

# Need for a Methodology

It has been observed that **hackers target networks/systems** in a strategic manner.

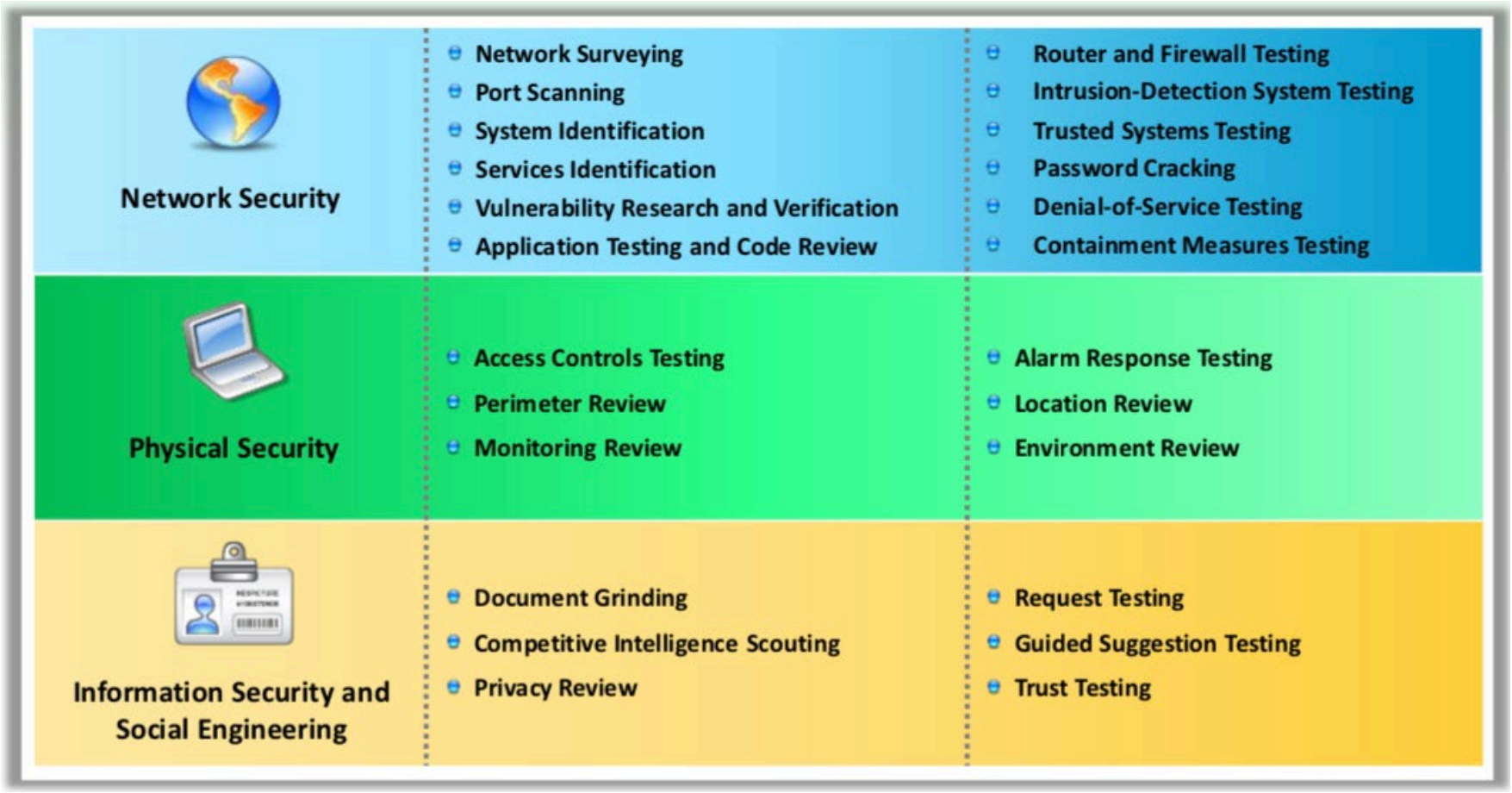
A methodology ensures that the exercise is done in a **standard manner** with **documented** and **repeatable results** for a given security posture.

Methodology plays a crucial role in the success of a pen test; lack of a pen test methodology results in **no consistency**.

It helps testers to **plan their testing/attack strategy** according to the input gained in the preceding phases of the testing process.

# Penetration Testing Methodology

- A full project should include some or all of the following areas:



# Methodologies for Penetration Testing

- Improve the chance of successfully completing penetration testing project.
- Methodologies and frameworks that have large support within the penetration testing community.
  - Project Management Book of Knowledge (PMBOK)
  - Information System Security Assessment Framework (ISSAF)
  - Open Source Security Testing Methodology Manual (OSSTMM)

# Penetration Testing Methodology

**Penetration Testing Methodologies**

**PMBOK**

**ISSAF**

**OSSTMM**

# Project Management Body of Knowledge (PMBOK)

- Standardize project management practices and information.
- Process-based
  - Describes work as being accomplished by processes.
  - Processes overlap and interact throughout a project.
- Processes are described in terms of:
  - Inputs (documents, plans, designs, etc)
  - Tools and techniques (mechanisms applied to inputs)
  - Outputs (documents, products, etc)

# PMBOK

- Five Process Groups
  - Initiating
  - Planning
  - Executing
  - Closing
  - Monitoring and Controlling
- These groups are chronological in sequence during the project

# PMBOK

- Ten Knowledge Areas
  - Project Integration Management
  - Project Scope Management
  - Project Schedule Management
  - Project Cost Management
  - Project Quality Management
  - Project Resource Management
  - Project Communications Management
  - Project Risk Management
  - Project Procurement Management
  - Project Stakeholder Management
- These above knowledge areas must be considered at all process groups during the project

# PMBOK - Initiating Process Group

- Attempt to gain approval for the project.
- Client needs to precisely know what is included and excluded as penetration testing is costly.
- Identify Stakeholders
  - Penetration tests affects a large number of individuals.
    - System owners, network administrators, management, etc.
  - Communication among stakeholders is more effective.

# PMBOK - Initiating Processes

- Develop Project Charter
  - Authorizes the launch of the project.
  - Defines the scope of the project.
  - Incorporate Statement of Work (SOW)
    - Defines the work activities, deliverables and timeline.
  - Incorporate the contract and industry standards.
  - Ensure that project meets business needs of stakeholders means greater chance of success.

# PMBOK - Planning Process Group

- Within the scope of a penetration test, the project manager needs to know…
  - Duration of the project
  - Size of team
  - Estimated cost of project
  - Resources needed
- Planning Processes help define the project to finer level of granularity.

# PMBOK - Planning Processes

| | | | | |
|---|---|---|---|---|
| Develop project management plan | Collect requirements | Define scope | Create work breakdown structure (WBS) | Define activities |
| Sequence activities | Estimate activity resources | Estimate activity durations | Develop schedule | Estimate costs |
| Determine budget | Plan quality | Develop human resource plan | Plan communications | Plan risk management |
| Identify risks | Perform qualitative analysis | Plan risk responses | Plan Procurement | |

# PMBOK - Planning Process Group

- Some planning issues within penetration testing involves the use of resources.
  - e.g. software tools
  - Commercial PenTest tools often have tight licensing agreements.
    - Limits the number of users and IP address range of targets.
- Planning documents are modified throughout the project lifecycle.

# PMBOK - Executing Process Group

- Within a penetration test project, this is when the attacks are conducted.
  - Information gathering
  - Vulnerability identification
  - Vulnerability verification
  - Compromising steps
- Results are compared to expectation listed in the documents in the planning processes.
  - May result in project expectation change.
  - Causes activities in executing processes to change.

# PMBOK - Executing Processes

Direct and manage project execution

Perform quality assurance

Acquire project team

Develop project team

Manage project team

Distribute information

Manage stakeholder expectations

Conduct procurements

# PMBOK - Closing Process Group

- Final documents are released to the client.
- Contractual agreements concluded.
- Closing Processes
  - Close project or phase
    - Release of final assessment to the client which includes…
      - Details of vulnerabilities identified and exploited.
      - Suggested solutions.
  - Close Procurements
    - Release resources for other projects.

# PMBOK - Monitoring & Controlling Process Group

- Discoveries are made during the entire process.
  - Affects the direction of the project including changes in scope.
  - Changes need to managed in a systematic way.
    - So that time, budget, scope and quality are not negatively affected.
- In penetration testing, project are often brief (1-2 months).
  - Can be less formal depending on organization requirements.
  - However, all the processes need to be addressed within a penetration test.

# PMBOK - Monitoring & Controlling Processes

| | | | |
|---|---|---|---|
| Monitor and control project work | Perform integrated change control | Verify scope | Control scope |
| Control schedule | Control costs | Perform quality control | Report performance |
| | Monitor and control risks | Administer procurement | |

# Penetration Testing Methodology

**Penetration Testing Methodologies**

**PMBOK**

**ISSAF**

**OSSTMM**

# Information System Security Assessment Framework (ISSAF)

- Peer-reviewed process that provides in-depth information about how to conduct a penetration test.
- Contains two separate documents.
  - Engagement Management & Good Practices (ISSAF0.2.1A)
  - Penetration Testing (ISSAF0.2.1B)
- Checklists for auditing & hardening systems.
- Tool-Centric
  - Connection between distinct tasks within a penetration test with penetration test tools.
  - Effective learning tool

# ISSAF

Phase 1: Planning & Preparation

Phase 2: Assessment

Phase 3: Reporting, Clean-up & Destroy Artifacts

# ISSAF – Phase 1: Planning & Preparation

- This phase comprises of steps to exchange information, plan and prepare for the test.
  - Identification of contact individuals from both sides.
  - Opening meeting to confirm scope, approach and methodology.
  - Agree to specific test cases and escalation paths.
- Not useful for penetration test project manager as not much information found in ISSAFv0.2b.
  - May need to use a different methodology for planning and preparation phase.

# ISSAF – Phase 2: Assessment

- Steps in penetration testing are referred to as layers.
- Layers defined in ISSAF:
  - Information gathering
  - Network mapping
  - Vulnerability identification
  - Penetration
  - Gaining access and privilege escalation
  - Enumerating further
  - Compromise remote users/sites
  - Maintaining access
  - Covering tracks

# ISSAF – Phase 2: Assessment

- The layers can be applied to the following targets
  - Networks
  - Hosts
  - Applications
  - Databases
- ISSAF also discusses about many older and well known social engineering techniques.

# ISSAF – Phase 3: Reporting, Clean-up & Destroy Artifacts

- Deals with generating the reports and securing any data that was obtained during the test.
- Report should include:
  - Management summary
  - Project scope
  - Penetration test tools used
  - Exploits used
  - Date and time of tests
  - All outputs of tools and exploits
  - A list of identified vulnerabilities
  - Recommendations to mitigate identified vulnerabilities
- Not much details regarding clean-up and destroy artifacts are included in ISSAF.

# ISSAF

- Advantages
  - Does not assume previous knowledge.
  - Provides examples of penetration test tool use.
- Disadvantages
  - Out of date quickly.
  - Penetration test tool examples are not extensive.
  - Last update: May 2006

# Penetration Testing Methodology

**Penetration Testing Methodologies**

**PMBOK**

**ISSAF**

**OSSTMM**

# Open Source Security Testing Methodology Manual (OSSTMM)

- "…to provide a scientific methodology for the accurate characterization of operational security (OpSec) through examination and correlation of test results in a consistent and reliable way."
- Adaptable to almost any audit type including penetration testing.

# OSSTMM

- **Scope** encompasses the systems and networks that are subjected to the audit.
- The assets within the scope are linked through the direction of interactions. These are called **vectors**.
  - e.g. Department A to B, internal to external, etc.
- Different security areas of interest within an organisation are classified into **channels**.
  - There are five channels:
    - Human
    - Physical
    - Wireless
    - Telecommunications
    - Data networks

# OSSTMM

- High level objectives for security testing in each **channels** are provided in OSSTMM.
  - Methods to be used is not dictated.
- Each **channel** must be separately tested for each **vector**.
- **Attack surface** is the unprotected part of the **Scope** from a defined **Vector**.

# OSSTMM – Common Test Types

## Blind

- Analyst engages the target with no prior knowledge of its defenses, assets or channels.
- Target is prepared and knows details of audit.

## Double Blind

- Analyst engages the target with no prior knowledge of its defences, assets or channels.
- Target is not notified in advance of the scope of the audit, the channels tested, or the test vectors.

## Gray Box

- Analyst engages the target with limited knowledge of its defenses and assets and full knowledge of channels.
- Target is prepared for the audit, knowing in advance all the details of the audit.

# OSSTMM – Common Test Types

## Double Gray Box

- Analyst engages the target with limited knowledge of its defenses and assets and full knowledge of channels.
- Target is notified in advance of the scope and time frame of the audit but not the channels tested or the test vectors.

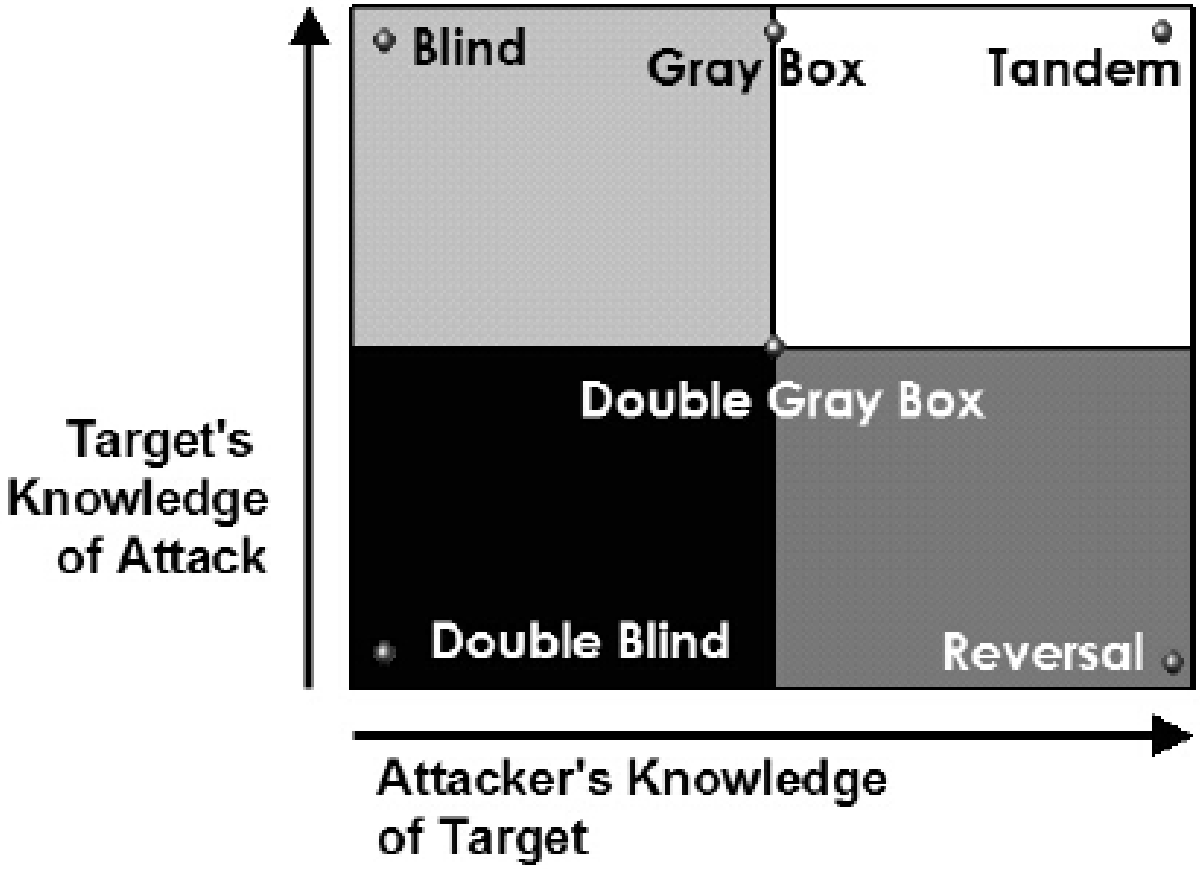
## Tandem

- The analyst and the target are prepared for the audit, both knowing in advance all the details of the audit.

## Reversal

- Analyst engages the target with full knowledge of its processes and operational security.
- Target knows nothing of what, how, or when the analyst will be testing.

# OSSTMM – Common Test Types



# Error Types

| | |
|---|---|
| False Positive | • The target response indicates a particular state as true although in reality the state is not true. |
| False Negative | • The target response indicates a particular state as not true although in reality the state is true. |
| Gray Positive | • The target response indicates a particular state as true, however the target is designed to respond to any cause with this state whether it is true or not. |
| Gray Negative | • The target response indicates a particular state as not true, however the target is designed to respond to any cause with this state whether it is true or not. |

# Error Types

| | |
|---|---|
| Specter | • The target response indicates a particular state as either true or false although in reality the state cannot be known. |
| Indiscretion | • The target response indicates a particular state as either true or false but only during a particular time, which may or may not follow a pattern. |
| Entropy Error | • The target response cannot accurately indicate a particular state as either true or false due to a high noise to signal ratio. |
| Falsification | • The target response indicates a particular state as either true or false although in reality the state is dependent upon largely unknown variables due to target bias. |

# Error Types

| | |
|---|---|
| Sampling Error | • The target is a biased sample of a larger system or a larger number of possible states. |
| Constraint | • The limitations of human senses or equipment capabilities indicate a particular state as either true or false although the actual state is unknown. |
| Propagation | • The Analyst does not make a particular test or has a bias to ignore a particular result due to a presumed outcome. |
| Human Error | • An error caused by lack of ability, experience, or comprehension is not one of bias and is always a factor that is present, regardless of methodology or technique. |

# OSSTMM – Rules of Engagement

- These rules define the operational guidelines of acceptable practices in the following areas.
  - *Sales and Marketing*
  - *Assessment / Estimate Delivery*
  - *Contracts and Negotiations*
  - *Scope Definition*
  - *Test Plan*
  - *Test Process*
  - *Reporting*

# OSSTMM

- Advantages
  - More flexibility for Pentesters.
  - Frequent updates.
- Disadvantages
  - Assumes tester have necessary knowledge beforehand.
  - Latest version requires paid subscription.

# Penetration Testing Methodology

**Penetration Testing Methodologies**

**PMBOK**

- Initiating Process Group
- Planning Process Group
- Executing Process Group
- Closing Process Group
- Monitoring & Controlling Process Group

**ISSAF**

- Phase 1: Planning & Preparation
- Phase 2: Assessment
- Phase 3: Reporting, Clean-up & Destroy Artefacts
- Advantages & Disadvantages

**OSSTMM**

- Scope, channels, vectors
- Common Test Types
- Error Types
- Rules of Engagement
- Advantages & Disadvantages