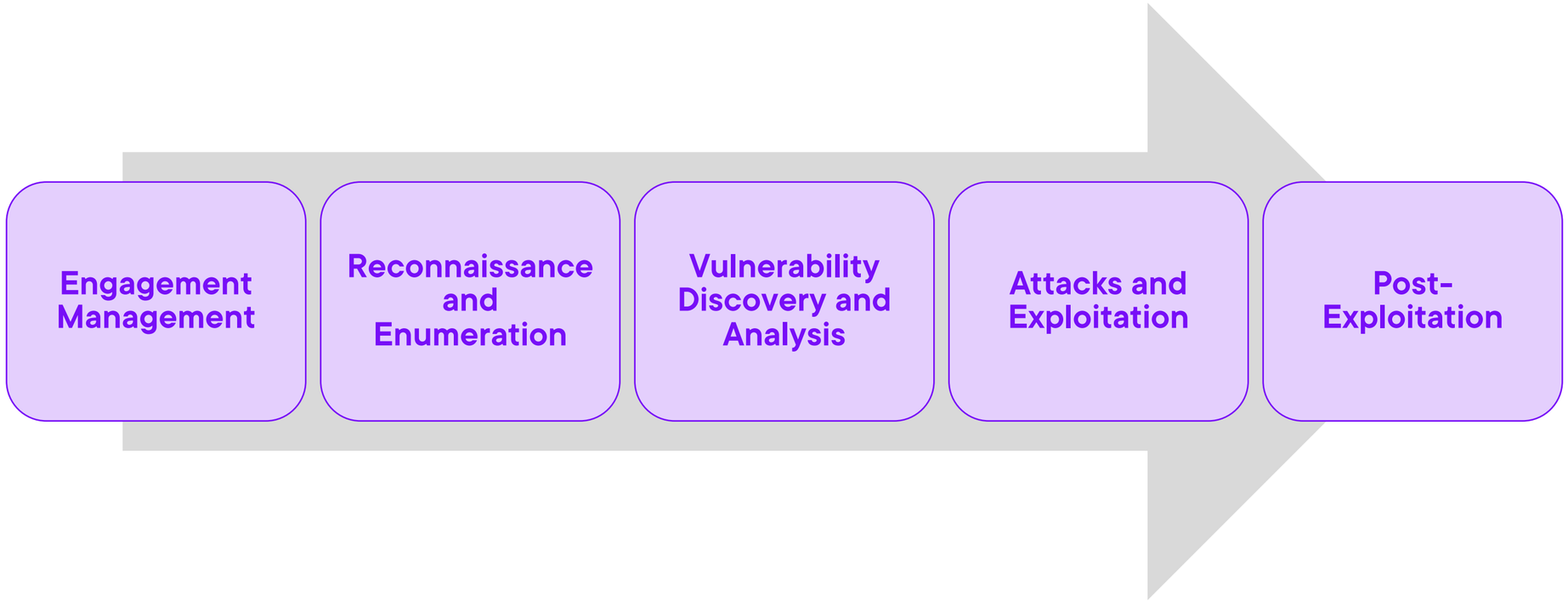
Engagement Management for CompTIA Pentest+

Pre-Engagement Tasks

Ricardo Reimao, OSCP, CISSP
Cybersecurity Consultant

The Overall Pentest Process



CompTIA PenTest+ Certification Exam Objectives (PT003)

Engagement Management

- Understanding the client needs
- Define scope and assessment types
- Sign contracts and agreements
- Define rules of engagement
- Define test frameworks
- Communications
- Reporting

Understanding Client Needs

It is our job to understand their needs and translate them into a technical project

Some stakeholders are non-technical

- The client does not know what they want/need

Understand critical points:

- What they expect
- What triggered
- Who requested

Main Assessment Types

Web Application	External Network	Internal Network
Wireless Testing	Mobile Testing	Etc.

Assessment Visibility

Black Box Testing

White Box Testing

Grey Box Testing

Main Contracts and Agreements

Master Service Agreement (MSA)

- The overarching contract between a client and a service provider
- Defines how two companies conduct business (e.g. how payments are made)
- Only one MSA per client

Non-Disclosure Agreement (NDA)

- One-time agreement to enforce privacy between the two parties
- Heavy fines for disclosing sensitive data

Statement of Work (SoW)

- The agreement to perform an engagement
- Defines the scope of a pentest and the prices for the specific services
- One SOW per engagement

Terms of Service (ToS)

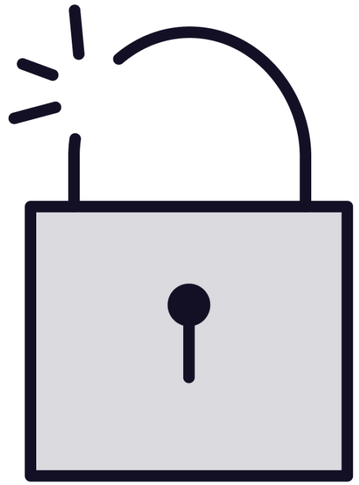
- Defines how the engagement will be performed, including testing hours and methodology

Course Scenario: The Globomantics Pentest

	Statement of Work – OK

Regulatory Considerations

Importance of Compliance Considerations



Compliance directly impacts your pentest

- How it will be executed
- What will be delivered in the report
- Who can execute the tests

Most Common Compliance Standards

PCI-DSS	GDPR	HIPAA
SOX	NERC-CIP	ISO27001

PCI-DSS

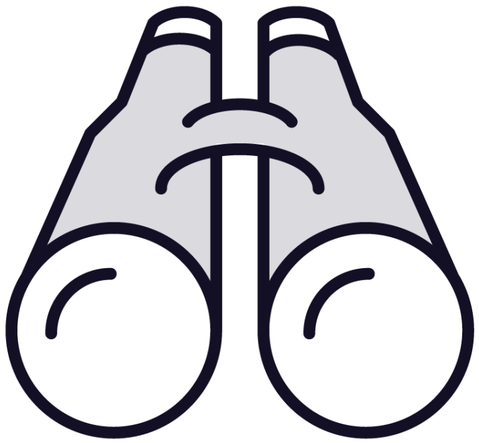
Payment Card Industry – Data Security Standards (PCI-DSS)

Mandatory for any company that processes credit card transactions

Detailed “Penetration Testing Guidance” document

- Required pentest scope and frequency
- Segmentation tests
- Cleaning up tasks
- etc.

GDPR



General Data Protection Regulation (GDPR)

A cybersecurity standard to protect customer data in Europe

Requires periodic pentests

- “(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.”

Discuss applicable regulations with your client.

Local Restrictions

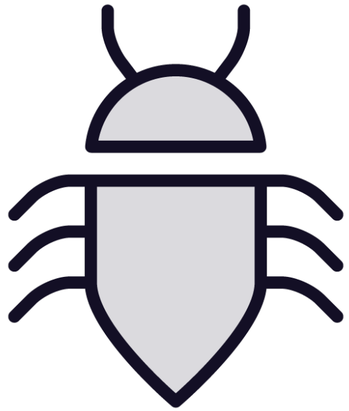
Each country (or even region) might have their own restrictions in terms of scope

Examples:

- Keylogging
- Recording audio/video

Varies from country to country. Do your own research!

Attacks/Tools Restrictions



In addition to local restrictions, the client (or any third-party) might have additional restrictions

Examples:

- DoS attacks
- Heavy scanning tools
- Password brute forcing

Discuss with your client what attacks should not be performed

Privacy Requirements

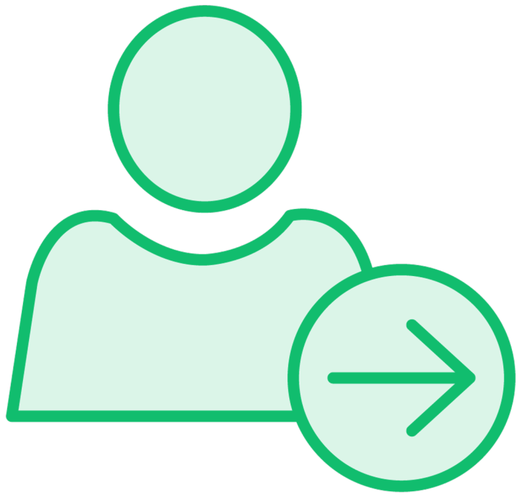
- Ensure that no sensitive data leaves the company
- Pentester location requirements
- Minimum-access requirements
- Discuss with your client any additional privacy requirements

Globomantics Scenario: Regulatory Considerations

No access to HR databases

Rules of Engagement

Escalation Process



Defines how issues will be escalated to the client

- Critical vulnerabilities
- Pentest impact

Defines the contact point on the client side and a potential escalation point (manager) if required

Testing Window

Some clients might have restrictions on the time that the tests can be performed

Minimize the impact of a pentest

Formalize the test hours on the rules of engagement

Examples:

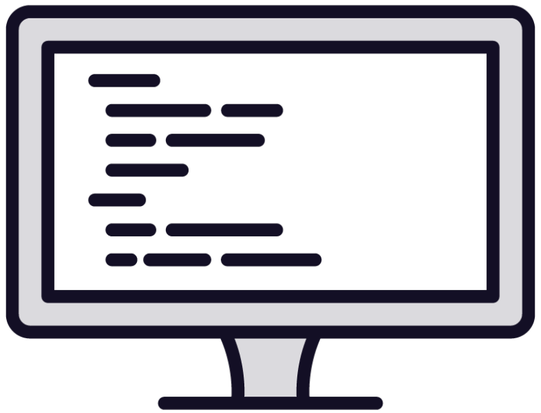
- Business hours only
- Non-business hours only

Exclusions

Critical assets

Explicitly defines what should not be touched during a pentest

Test Cases



In some specific cases, clients might want to stick to a set of test cases

Example:

- Test only for authentication vulnerabilities
- Test only for session management risks

In this case, it is important to document what will be tested and how it will be tested

Scenario: Rules of Engagement

Target Selection

Requesting Asset Information

Request information about the assets in scope, and how to access them

- IP addresses, URLs, APIs, etc.

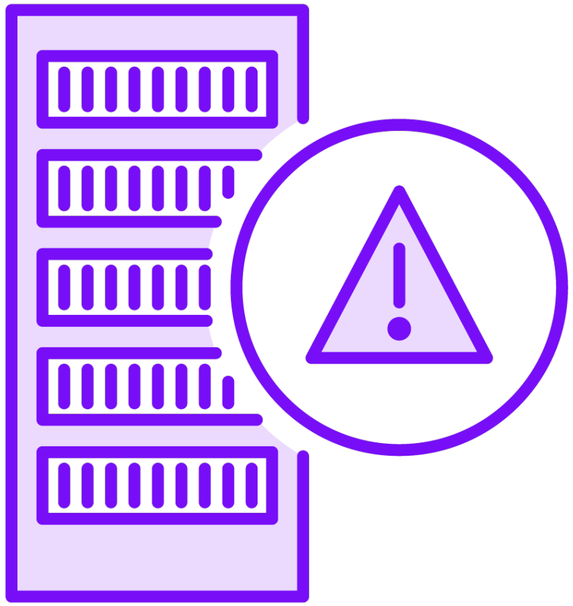
Request essential information about the assets

- Asset owners, contact information, time for testing

Ensure you have ways to access the assets

- E.g. VPN for internal assets

Out of Scope Assets



As important as defining the assets in scope, is defining what is out of scope

Ask the client for a list of assets that should not be tested

- Especially if IP ranges were provided

Ensure that we are not testing servers that are out of scope

Potential Assets in Scope

- Specific Servers
- APIs
- Entire Internal Surface
- Specific URLs
- Physical Locations
- Third-party Hosted
- IP Ranges (CIDR)
- DNS
- SaaS
- Domains
- Entire External Surface
- Cloud Environments

On-prem vs. Cloud Testing

For on-prem, you should gather all information discussed in this module

For cloud testing, you should also gather:

- Information about the cloud provider
- Shared responsibility model
- Authorization from cloud provider

Ensure you're targeting ONLY targets related to your client

- Common for several companies to share the same IP ranges

Third-party applications

Gather information about the third-party provider

Define communications

Get approvals and align testing times

Contacting Owners and Stakeholders

Depending on the test scope, the asset owner should be contacted prior the tests

- Discuss dates and attacks in scope

Work with the asset owner to minimize the impact of the test

- Example: Testing in non-business hours

If security directors do NOT want to inform asset owners, this should be formalized and documented

Globomantics Scenario: Assets in Scope

Legal and Ethical Considerations

A pentest is a serious engagement

Without proper authorization, you might be committing a crime

- Ensure in-writing authorizations
- Have the client sign on the scope
- Stay in scope during the test

If your pentest is part of a legal case, confirm the reporting requirements

Up Next:

Assessment Frameworks