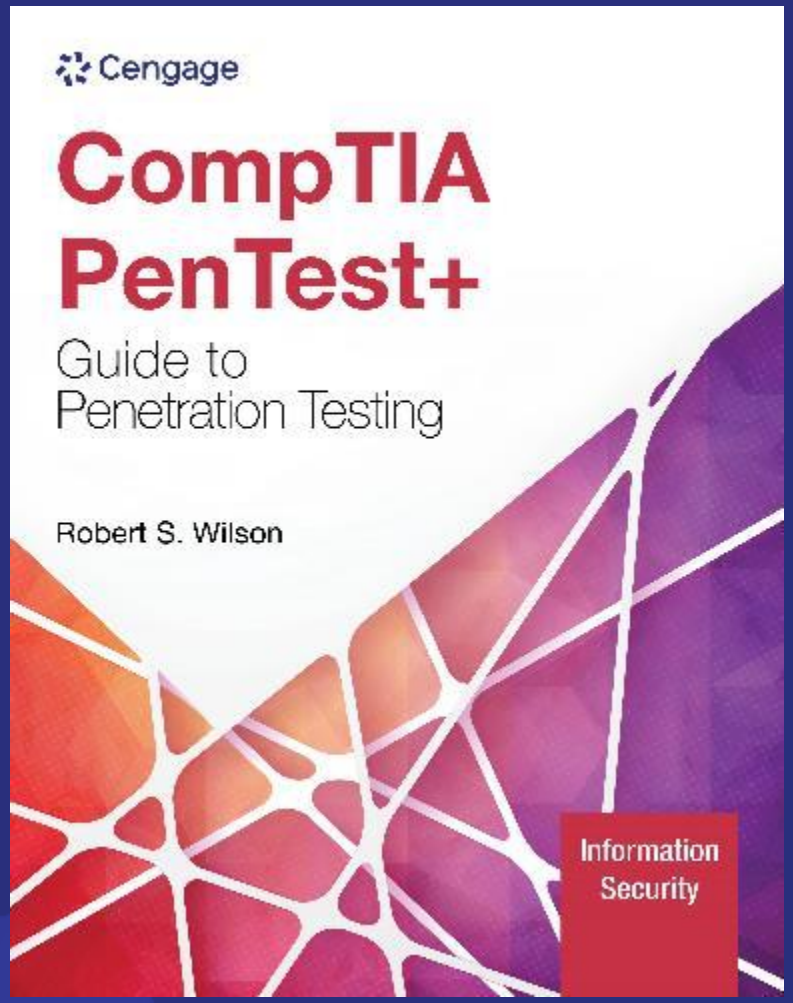


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 3: Planning and Scoping

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Module Objectives

By the end of this module, you should be able to:

1. Describe regulatory compliance requirements, such as those in the PCI DSS and GDPR
2. Define penetration-testing legal documents such as SLAs, SOWs, MSAs, and NDAs
3. Identify penetration-testing standards and methodologies such as the MITRE ATT&CK Framework, OWASP, NIST, OSSTMM, and PTES
4. Describe types of penetration-testing assessments
5. Define the rules of engagement for penetration testing

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (1 of 20)

Key Terms

Governance – ensures that organizational activities are aligned to business goals

Risk – potential for the loss of confidentiality, integrity, or availability of information, data, or systems, and the harm that may come from it

Compliance – businesses or organizations are required to conform to policies, jurisdictional laws, and regulations in the area of business

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (2 of 20)

Regulatory Compliance

- Pen tests may be conducted to meet an obligation to maintain regulatory compliance
- Compliance involves the rules, regulations, and standards an organization must follow to conduct and operate as a business
- Compliance standards and regulations may provide either little or significant direction on pen-test scope and activity
- Best practices in technical, operational, and policy realms may also influence the need for or the scope and targets of a pen test

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (3 of 20)

Payment Card Industry Data Security Standard (PCI DSS)

- PCI DSS managed by PCI Security Standards Council (PCI SSC)
- PCI DSS v4.0 effective March 2022
- Organizations that use credit card services must comply with PCI DSS
- Standard consists of twelve requirements in six categories
- Helps to reduce fraud and provide cardholders with better security

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (4 of 20)

Payment Card Industry Data Security Standard (PCI DSS)

- PCI DSS applies to all entities involved in payment card processing
  - Merchants
  - Processors
  - Acquirers
  - Issuers
  - Service providers
- Applies to all other entities that process, store, or transmit cardholder data (CHD) and sensitive authentication data (SAD)

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (5 of 20)

PCI DSS – Requirements Scope

Cardholder data environment (CDE) is defined as “the people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data” and includes:

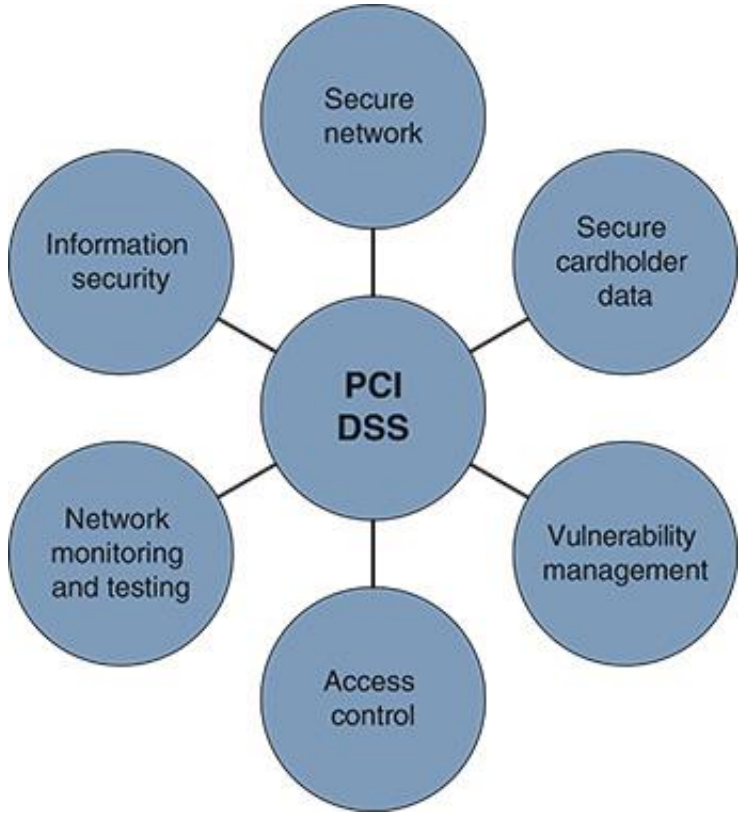
- Security systems
- Virtual devices
- Networking devices
- Servers
- Applications

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (6 of 20)

PCI DSS – Requirement Categories

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy



PCI DSS requirement categories

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (7 of 20)

PCI DSS – Pen Testing Guidelines

PCI DSS provides a document that outlines pen-test components, methodologies, and reports

- Items addressed in Penetration Testing Guidelines document include:
  - Isolating the CDE from the network and encrypting it during transmission
  - Using strong passwords and encryption and prohibiting default passwords
  - Conducting annual pen tests from internal and external locations

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (8 of 20)

Real World Criminal Breaches of Credit Card Data

- Warner Music Group – In 2020 a cybercriminal group used infected software to skim customer data over three months
- Target Corporation – Lost 40 million credit card numbers in 2013 costing over $220 million in legal fees and settlements
- Adobe – 38 million login details and card numbers from three million customer resulted in $1 million fine and undisclosed settlements
- Equifax – suffered breach in 2017 involving over 143 million people in three countries, settlements over $425 million

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (9 of 20)

General Data Protection Regulation (GDPR)

- GDPR protections of European Union (EU) citizens' online activity and data, regardless of the activity's country of origin
- GDPR requires that data associated with the EU citizen must be stored in EU country
- Noncompliance can result in fines over $11 million or more

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (10 of 20)

General Data Protection Regulation (GDPR) Requirements

- Organizations collecting or processing EU citizen data must address GDPR requirements related to:
  - Data protection officers
  - Report and disclosure
  - Lawfulness, fairness, and transparency
  - Accountability and governance
  - Data security
  - Privacy rights

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (11 of 20)

General Data Protection Regulation and Pen Testing

While the GDPR doesn't specifically mandate pen testing, the following questions should be answered for pen tests supporting GDPR compliance:

- Is the security of the systems sufficient to prevent breaches?
- Can your security measures detect a breach so that it can be reported within 72 hours?
- Does your organization store EU citizen data only on servers located in the EU, as required?
- Are you using encryption and strong authentication to protect data at rest and in transit?

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (12 of 20)

Other Important United States Compliance Standards*

- HIPAA –Governs the security and privacy of sensitive health info
- GLBA – Controls financial institutions' handling of sensitive data
- SOX – Protects investors from fraudulent practices
- FIPS- Federal security requirements for data and encryption for U.S. government and contractors
- ISO 27001- International standards and best practices on info security

**Current CompTIA PenTest+ exam only covers PCI DSS and GDPR*

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Discussion Activity 3-1

Pen-testing activities that are legally allowed may vary based on the location and jurisdiction in which the pen tester and clients are located. Laws governing computer security activities can vary from state to state. Surprisingly, “ethical hacking” and “anti-hacking tools” are punishable by fines and imprisonment in Germany.

- How can pen testers provide security testing and ethical hacking services to clients without putting themselves at legal risk?
- How might a law covering pen testing be written to allow the ethical use of hacking tools and protections for authorized security testers working for a client on a pen test?

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (13 of 20)

Legal Concepts and Documents – Common Pen Test Documents

These are common pen test documents. Many others exist and may be used in specific circumstances based on client or tester needs.

- Service-Level Agreement (SLA)
- Statement of Work (SOW)
- Master Service Agreement (MSA)
- Nondisclosure Agreement (NDA)

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (14 of 20)

Legal Concepts and Documents – Service Level Agreement (SLA)

Agreement between client and service provider listing services being provided; may include details such as:

- Description of services
- How to measure services
- Responsibilities of parties
- Actions if service level is not met
- Authorizations

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (15 of 20)

Legal Concepts and Documents – Statement of Work (SOW)

- Purpose of the SOW is to clearly communicate what is expected and allowed
- Covers work to be performed for client by pen-test team
- May specify activities that are prohibited
- Must be agreed upon and signed by all stakeholders before work begins

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (16 of 20)

Legal Concepts and Documents – Statement of Work (SOW)

- Includes details about but not limited to:
  - Scope of pen test
  - Deliverables
  - Price and payment schedule
  - Change in management procedure
  - Project timeline
  - Location(s) of work
  - Liability disclaimers

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (17 of 20)

Legal Concepts and Documents – Statement of Work (SOW)

The scope of the pen-testing project must address the pen-test activities and parameters surrounding the work and may include areas such as:

- Reconnaissance/Info gathering
- Targets allowed and off limits
- Scanning tools and process
- Vulnerability discovery methods
- Exploitation of vulnerabilities
- Privilege escalation
- Compliance testing standards
- Procedures for critical vulnerability discovery
- Incident handling and notification

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (18 of 20)

Legal Concepts and Documents – Master Service Agreement (MSA)

High-level document governing the relationship between pen tester and client; optional but useful

- One MSA can cover many separate SOWs and SLAs
  - Operational procedures
  - Future SOWs
  - Expectations
  - General payment terms
  - Legal jurisdiction, dispute resolution
  - Warranties and work standards
  - Liability disclaimers
  - Purchase order process

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (19 of 20)

Legal Concepts and Documents – Nondisclosure Agreement (NDA)

Legal, enforceable agreement covering sensitive and confidential information potentially uncovered as a result of pen test

- Includes client system flaws and vulnerabilities
- Protects client from damage caused by improper info disclosure

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Governance, Risk, and Compliance Concepts (20 of 20)

Legal Concepts and Documents – Additional Documents

Data Ownership and Retention – covers who owns the data created and discovered during pen-test process

Permission to Attack – signed and authorized agreement detailing possible attack scenarios; protects pen tester from possible legal action as result of pen-test activities

Third-Party Authorization – addresses interaction and requirements necessary for pen tester to conduct testing that may involve third-party services or systems such as cloud hosting providers

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Discussion Activity 3-2

Identifying the scope of a penetration test is perhaps the most important pre-engagement activity. The questions on the next slide are examples of questions to ask a client to gather information needed to properly develop the SOW for a pen-test client.

The types of clients contracting penetration test services varies as widely as the specific pen-test needs of those clients.

In small groups, discuss and write a list of additional questions that a pen-test group might ask potential clients as part of the scoping process.

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Discussion Activity 3-2 (continued)

- Will staff be queried to gather information?
- Will networks be scanned to gather target information?
- Which systems are targeted, and which are not?
- Should a type of system be targeted, such as all web servers?
- What type of scanning is agreed upon?
- Can privilege escalation be attempted as part of exploitation testing?
- Are compliance standards being tested?
- What procedure should be followed when a critical vulnerability is discovered?
- Who should be notified?

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (1 of 2)

Standards and Methodologies

Scoping – determining targets to pen test and how to test them

Scope of the pen test is determined by many factors:

- Organizational requirements
- Standards and methodologies
- Compliance requirements
- Types of test
- Rules of engagement
- Environmental considerations
- Identified targets

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

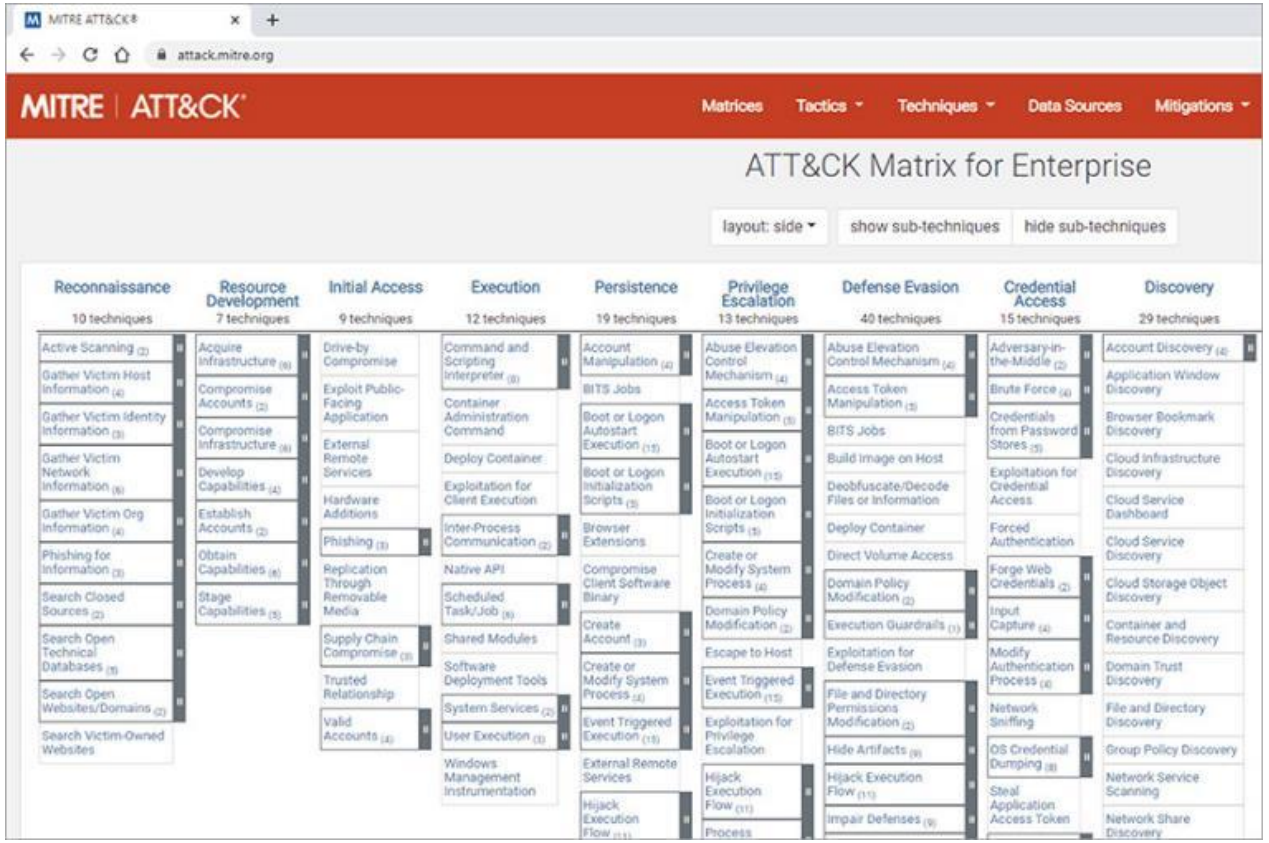
Scoping and Requirements (2 of 2)

Standards and Methodologies – MITRE ATT&CK Framework

- The MITRE Corporation manages federally funded research and development centers (FFRDCs) in fields such as cybersecurity
- MITRE ATT&CK Framework is a freely available service that offers cyber threat info to organizations
- Used by the FBI and Cybersecurity and Infrastructure Security Agency (CISA) and many companies
- MITRE publishes the common vulnerabilities and exposures (CVEs) database of known vulnerabilities

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

MITRE ATT&CK (1 of 2)

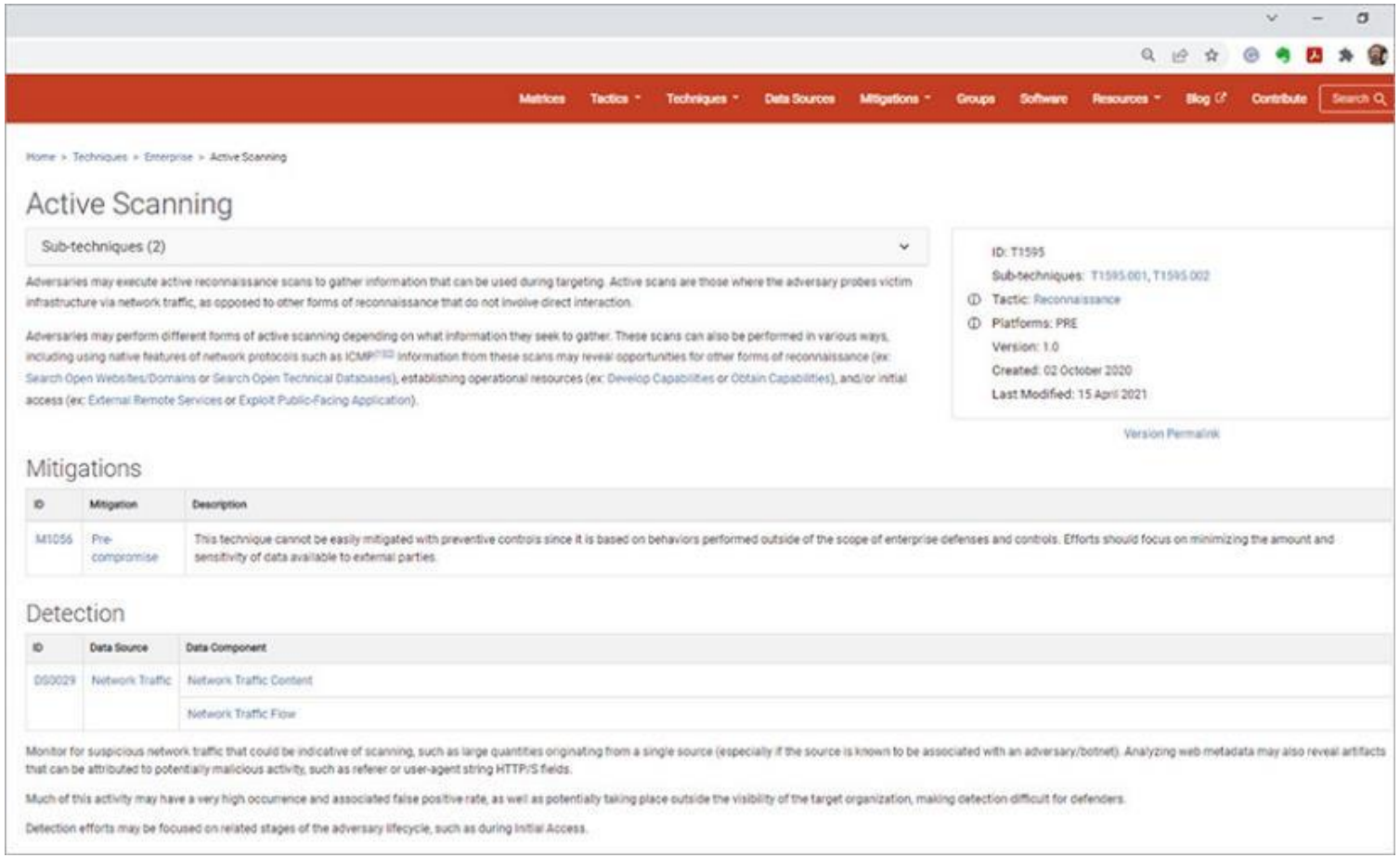


MITRE ATT&CK website

Cengage

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

MITRE ATT&CK (2 of 2)



Active scanning attack info

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (1 of 15)

Standards and Methodologies – Open Web Application Security Project (OWASP)

- Online community providing methodologies, documentation, and tools for web application security
- Creator of OWASP security learning and testing tool

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (2 of 15)

Standards and Methodologies – National Institute of Standards and Technology (NIST)

- NIST Cybersecurity Framework published in 2014; defines five functions of cybersecurity program to guide risk management:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Mandatory for U.S. government agencies
- 2018 – Version 1.1 published

Functions of the NIST Cybersecurity Framework

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (3 of 15)

Standards and Methodologies –Open Source Security Testing Methodology Manual (OSSTMM)

- Peer-reviewed security testing methodology

"*This manual provides test cases that result in verified facts. These facts provide actionable information that can measurably improve your operational security. By using the OSSTMM you no longer have to rely on general best practices, anecdotal evidence, or superstitions…*"

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (4 of 15)

Standards and Methodologies –Penetration Testing Execution Standard (PTES)

- Pen-testing methodology developed by team of infosec experts, organized into seven sections
  - Pre-engagement interactions
  - Intelligence gathering
  - Threat modeling
  - Vulnerability analysis
  - Exploitation
  - Post-exploitation
  - Reporting

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (5 of 15)

Standards and Methodologies –Information Systems Security Assessment Framework (ISSAF)

- Identifies phases a threat actor follows to breach a target
  - Planning and preparation
  - Assessment
  - Reporting and clean-up
- Out of date, no longer maintained, not to be used as sole methodology
- Links pen-test steps with pen-test tools

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (6 of 15)

Types of Assessments and Tests – Goals, Compliance and Red Team Assessments

Goal-based - conducted to test specific goals

- Test all web servers to check for current security patches

Compliance-based – dictated by compliance requirements such as those required of PCI DSS or GDPR

Red team – targeted attacks simulating how malicious actors may compromise systems

- Useful for testing defensive capabilities of systems and personnel

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (7 of 15)

Types of Assessments and Tests – Black Box, White Box, Gray Box Tests

Black box – Pen tester has "zero knowledge" of target test items; tester must gather info on targets

- Simulates typical real-world attacker

White box– Client provides tester with full knowledge of targets

- Can include network diagrams, IP addresses, OS versions, and more

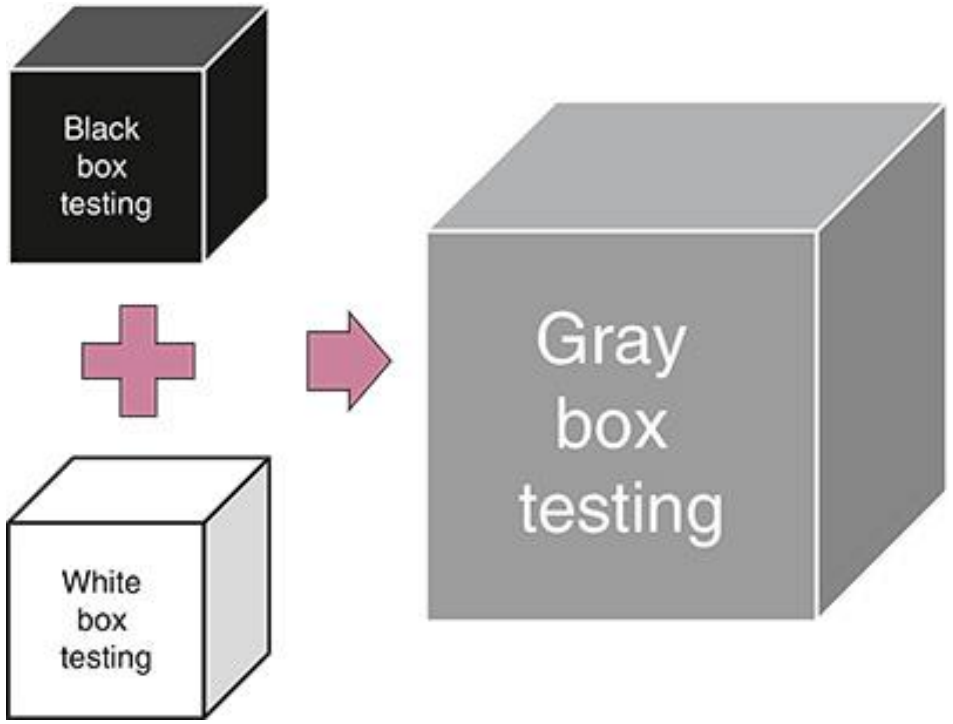
Gray box – Tester has some info about targets but must discover remaining test details on their own

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Discussion Activity 3-3

Pen tests often follow the black, white, and gray box testing models, with each having its benefits and disadvantages.

In small groups, discuss when each model would be most advantageous to a pen-test client. Create three hypothetical, ideal client scenarios, one for each model, and explain the scenarios and reasoning to the other groups.



Black, white, and gray box testing

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (8 of 15)

Rules of Engagement (ROE)

- The rules of engagement are critical to all pen tests and must be established before activities begin
- Explicitly define what is allowable and what is not
- Example – Denial of Service (DOS) attacks likely not permitted on systems providing critical business services
- Many factors to consider when drafting ROE

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (9 of 15)

Rules of Engagement (ROE) – Factors to Consider

- Types of tests being performed:
  - Scanning, probing, attack types, denial of service, etc.
- Types of tests prohibited
- Timing – when tests begin and end, times of day, days allowed
- Handling of sensitive data when discovered or created
- Communication of project status and updates
- Emergency contacts and scenarios for contact

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (10 of 15)

Rules of Engagement (ROE) – Factors to Consider

- Handling of critical and sensitive vulnerabilities
- Actions if prior compromises are discovered
- Targets in scope of pen test
- Client personnel involved in or aware of testing activities
- Red team attack system IP address
- Passive reconnaissance activities allowed
- Social engineering parameters, if allowed

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (11 of 15)

Environmental Considerations

Pen-test target systems rarely function in isolation; high level, big picture must be considered when planning and executing pen-test activities

- Computing Environment – virtualized and cloud hosted services
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- ROE Environment – Particular limitations on tools or testing methods

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (12 of 15)

Environmental Considerations

- Legal Environment – encompasses local, regional, and national laws
  - Import and export restrictions
  - Data storage regions
  - Industry or government compliance requirements
- Organization Testing Environment – test or nonproduction systems and networks available for pen-testing activities
- Communication Environment – client contacts and communication rules
  - Executives, public relations, tech support, legal, admin, third-party

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (13 of 15)

Defining Target Lists

Targets may be computers, networks, applications, processes, and people and must be explicitly defined to protect pen tester and client

- Networks
- Domain controllers and authentication systems
- IP address ranges
- Physical locations
- Data and databases
- Domain Name System (DNS) services
- External targets
- Internal targets
- Third-party or cloud services

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (14 of 15)

Defining Target Lists – Social Engineering Targets and Methods

People are often security's weakest link; social engineering targets them

- There are many types of social engineering that may be used in pen tests
  - Phishing, spear phishing, and whaling
  - Impersonation
  - Shoulder surfing
  - Many other social engineering tactics and scenarios exist

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Scoping and Requirements (15 of 15)

Validating Scope of Engagement

Before pen testing, revisit pen-test plan and documents to ensure they meet client's requirements; consider the following areas and items:

- Client requirements
- Budget
- Threat modeling
- Time management
- Risk acceptance
- Goal prioritization
- Impact tolerance

Sufficient review of SOE can limit potential of **scope creep**, when testing leads to discovery of items to test not in original scope; requires amendment to scope and proper authorization to do so

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Summary

By the end of this module, you should be able to:

1. Describe regulatory compliance requirements, such as those in the PCI DSS and GDPR
2. Define penetration-testing legal documents such as SLAs, SOWs, MSAs, and NDAs
3. Identify penetration-testing standards and methodologies such as the MITRE ATT&CK Framework, OWASP, NIST, OSSTMM, and PTES
4. Describe types of penetration-testing assessments
5. Define the rules of engagement for penetration testing

Robert Wilson, CompTIA PenTest+: Guide to Penetration Testing, 1st Edition. © 2024 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.