Module 2, Booklet 2

Ethical hacker

Planning and Scoping a Penetration Testing Assessment

By BELKHIR Selma

Governance, Risk, and Compliance in Penetration Testing

Regulatory Compliance Considerations

Understanding industry regulations is essential in penetration testing:

- **PCI DSS – Protects digital payments and cardholder data.**
- **HIPAA – Ensures security and privacy of electronic health information.**
- **FedRAMP – Regulates cloud services for U.S. government use.**
- **GDPR – Strengthens data protection and privacy rights in the EU.**

Governance, Risk, and Compliance in Penetration Testing

Local Restrictions & Legal Considerations

Penetration testing laws vary by country, requiring clear authorization and compliance with local regulations (e.g., CFAA in the U.S.). Always obtain written consent and document constraints such as:

- **Restricted tools or techniques.**
- **Out-of-scope systems.**
- **Legal limitations on data handling.**

Governance, Risk, and Compliance in Penetration Testing

Contracts & Legal Agreements

Key documents ensure clarity and legal protection:

- **Statement of Work (SOW) – Defines scope, tasks, and deliverables.**
- **Service-Level Agreement (SLA) – Outlines expectations and response times.**
- **Non-Disclosure Agreement (NDA) – Protects sensitive client information.**
- **Master Service Agreement (MSA) – Governs long-term business relationships.**

Governance, Risk, and Compliance in Penetration Testing

Disclaimers & Risk Awareness

Pen testers should include disclaimers in pre-engagement documentation and reports, clarifying that:

- Findings are based on the state of systems at a specific date.
- The report does not guarantee security against future threats.
- No legal or compliance guarantees are provided.

Scoping and Requirements

Rules of Engagement

- **What's Included:** Testing timelines, IP ranges, permitted tools, and more.

- **Agreement:** Must be approved by the client before testing begins.

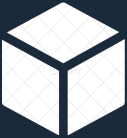
Scoping and Requirements

Target List & In-Scope Assets:

- **What to Test:** Systems, apps, networks, and APIs (e.g., SOAP, Swagger, WSDL).

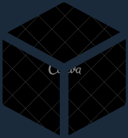
- **Documentation:** Clearly define IP ranges, wireless networks (SSIDs), and API details.

Testing Strategies



- **Unknown-Environment:** Simulates an external attacker with minimal info.

- **Known-Environment:** Full knowledge of the target for comprehensive testing.



Key Takeaways for Penetration Testers

- **Know the Rules:** Stay compliant with regulations like PCI DSS, HIPAA, and GDPR.
- **Scope Carefully:** Define and validate testing boundaries with the client.
- **Legal Protection:** Use contracts, disclaimers, and written permissions to avoid risks.
- **Adapt Strategies:** Choose between unknown and known-environment testing based on client needs.

Stay secure, stay curious because in cybersecurity, every vulnerability patched is a step toward a safer digital world

By BELKHIR Selma