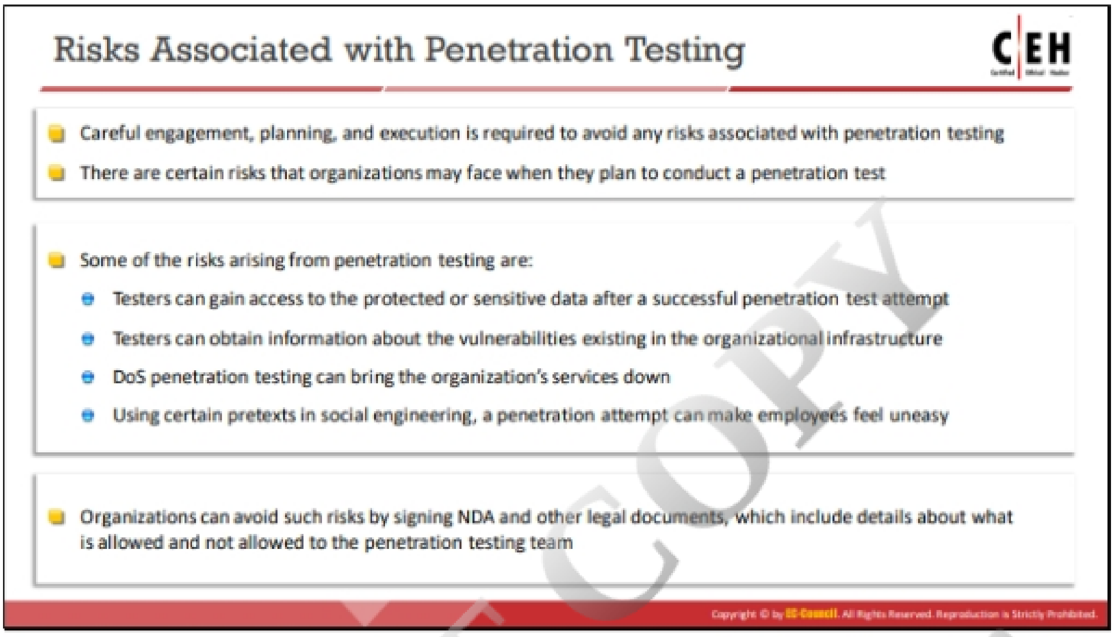
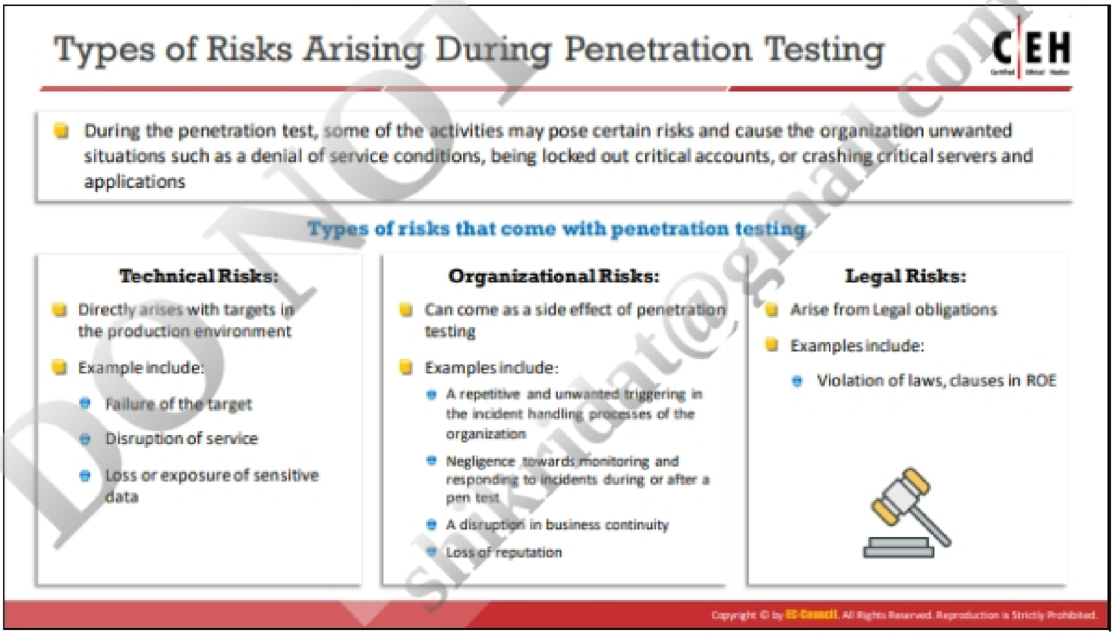


Risks Associated with Penetration Testing

- Careful engagement, planning, and execution is required to avoid any risks associated with penetration testing
- There are certain risks that organizations may face when they plan to conduct a penetration test

- Some of the risks arising from penetration testing are:
  - Testers can gain access to the protected or sensitive data after a successful penetration test attempt
  - Testers can obtain information about the vulnerabilities existing in the organizational infrastructure
  - DoS penetration testing can bring the organization's services down
  - Using certain pretexts in social engineering, a penetration attempt can make employees feel uneasy

- Organizations can avoid such risks by signing NDA and other legal documents, which include details about what is allowed and not allowed to the penetration testing team



Types of Risks Arising During Penetration Testing

- During the penetration test, some of the activities may pose certain risks and cause the organization unwanted situations such as a denial of service conditions, being locked out critical accounts, or crashing critical servers and applications

Types of risks that come with penetration testing

Technical Risks:

- Directly arises with targets in the production environment
- Example include:
  - Failure of the target
  - Disruption of service
  - Loss or exposure of sensitive data

Organizational Risks:

- Can come as a side effect of penetration testing
- Examples include:
  - A repetitive and unwanted triggering in the incident handling processes of the organization
  - Negligence towards monitoring and responding to incidents during or after a pen test
  - A disruption in business continuity
  - Loss of reputation

Legal Risks:

- Arise from Legal obligations
- Examples include:
  - Violation of laws, clauses in ROE

Notes: ______________________________

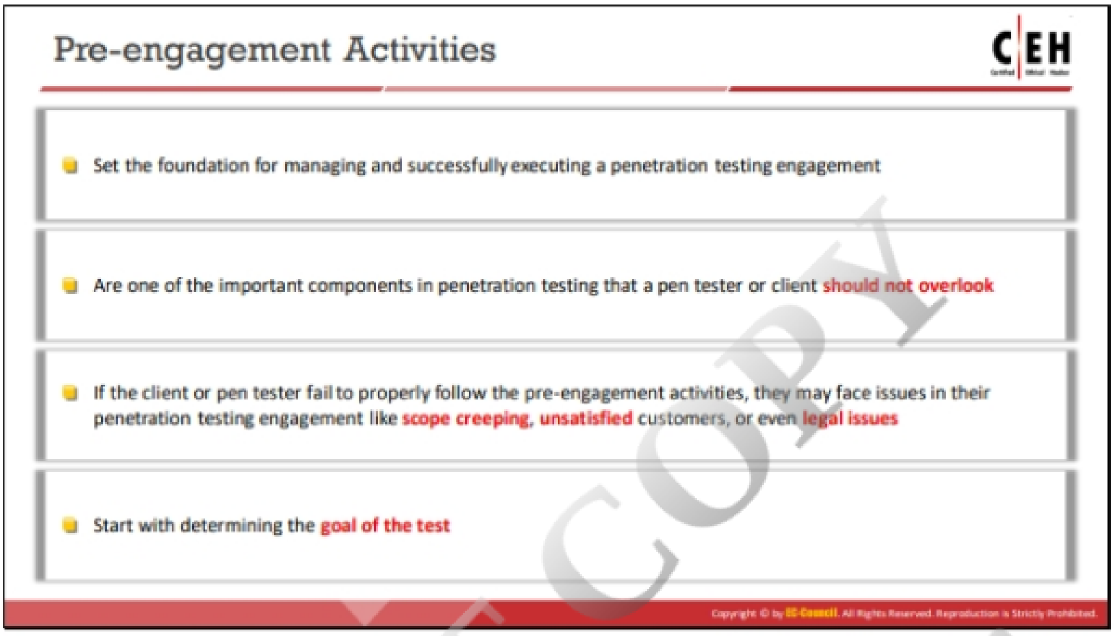
____

____

____

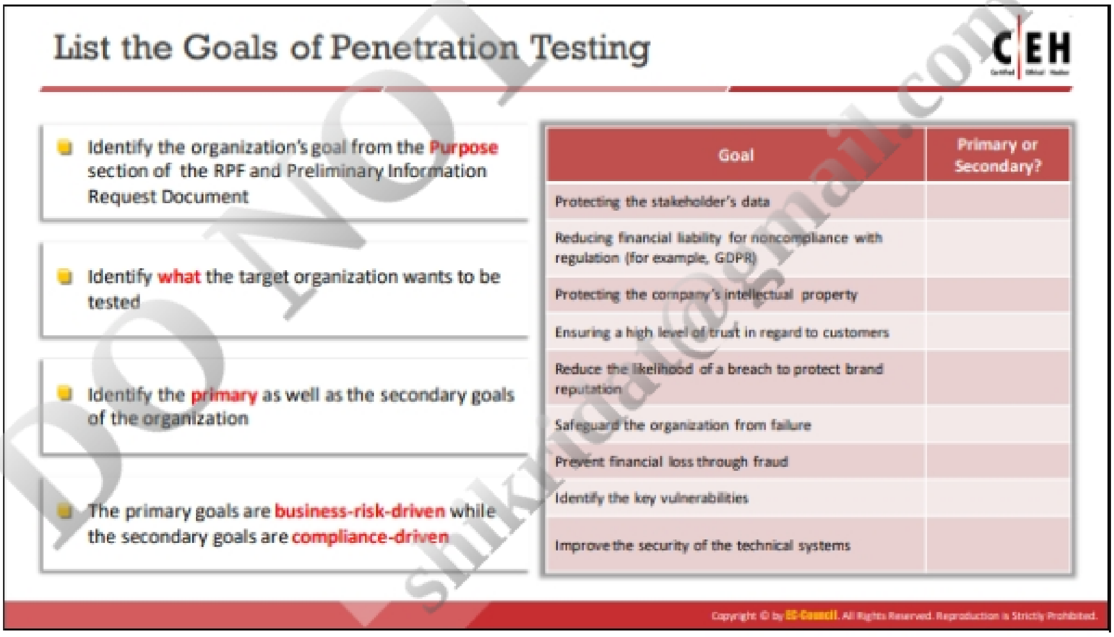
____

____



Pre-engagement Activities

- Set the foundation for managing and successfully executing a penetration testing engagement
- Are one of the important components in penetration testing that a pen tester or client **should not overlook**
- If the client or pen tester fail to properly follow the pre-engagement activities, they may face issues in their penetration testing engagement like **scope creeping**, **unsatisfied** customers, or even **legal issues**
- Start with determining the **goal of the test**



List the Goals of Penetration Testing

- Identify the organization's goal from the **Purpose** section of the RPF and Preliminary Information Request Document
- Identify **what** the target organization wants to be tested
- Identify the **primary** as well as the secondary goals of the organization
- The primary goals are **business-risk-driven** while the secondary goals are **compliance-driven**

Goal	Primary or Secondary?
Protecting the stakeholder's data	
Reducing financial liability for noncompliance with regulation (for example, GDPR)	
Protecting the company's intellectual property	
Ensuring a high level of trust in regard to customers	
Reduce the likelihood of a breach to protect brand reputation	
Safeguard the organization from failure	
Prevent financial loss through fraud	
Identify the key vulnerabilities	
Improve the security of the technical systems	

Notes: ____

____

____

____

____

____