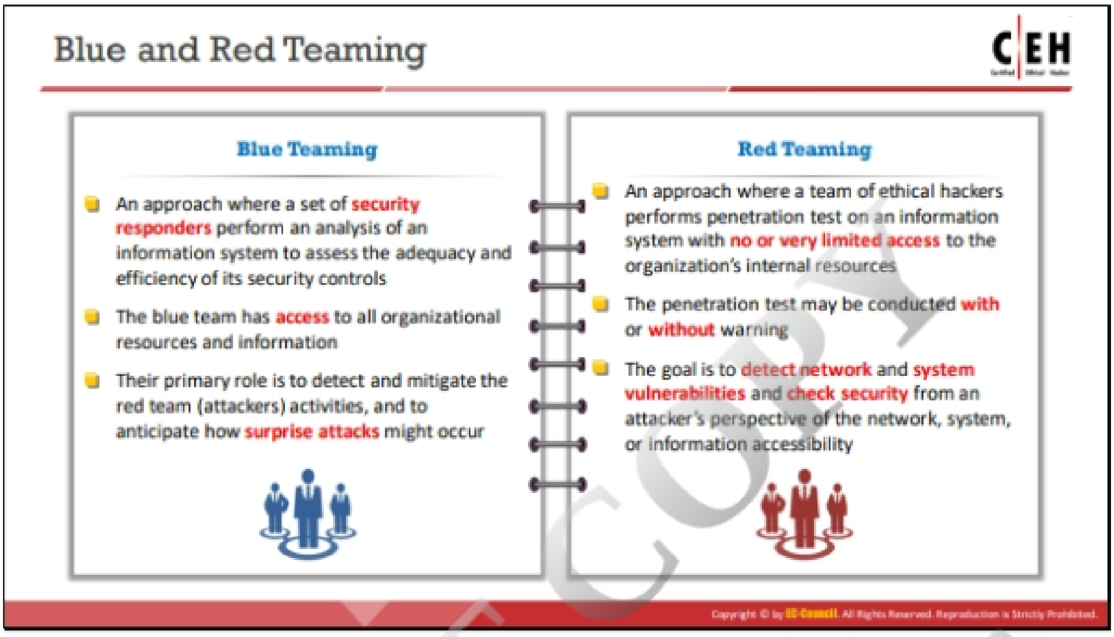


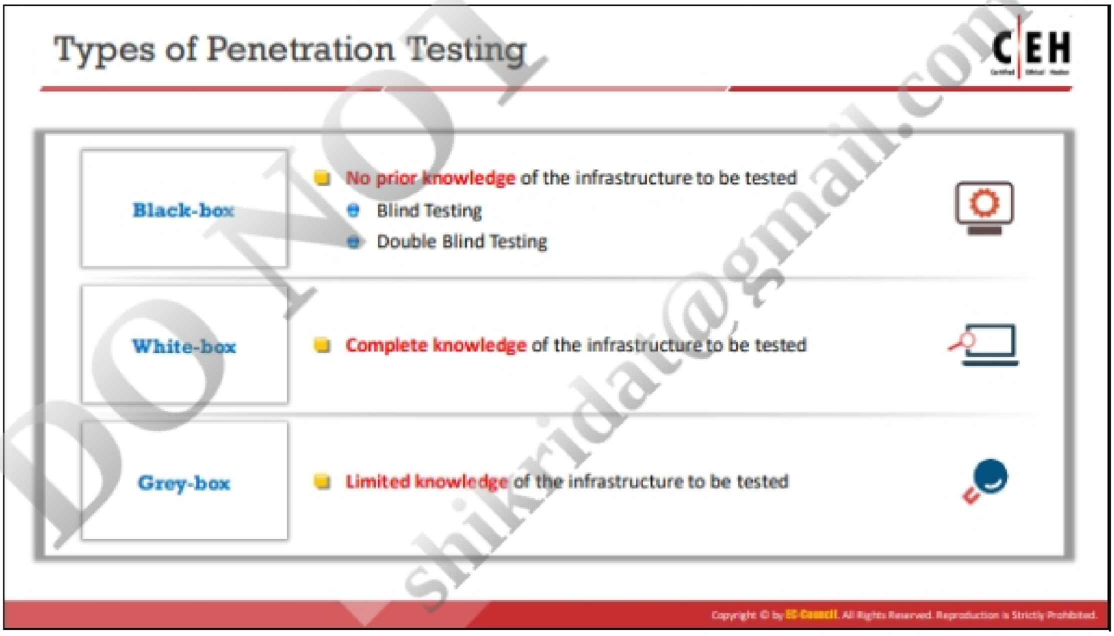
Blue and Red Teaming

Blue Teaming

- An approach where a set of security responders perform an analysis of an information system to assess the adequacy and efficiency of its security controls
- The blue team has access to all organizational resources and information
- Their primary role is to detect and mitigate the red team (attackers) activities, and to anticipate how surprise attacks might occur

Red Teaming

- An approach where a team of ethical hackers performs penetration test on an information system with no or very limited access to the organization's internal resources
- The penetration test may be conducted with or without warning
- The goal is to detect network and system vulnerabilities and check security from an attacker's perspective of the network, system, or information accessibility



Types of Penetration Testing

Black-box	No prior knowledge of the infrastructure to be tested Blind Testing Double Blind Testing
White-box	Complete knowledge of the infrastructure to be tested
Grey-box	Limited knowledge of the infrastructure to be tested

Notes: ____

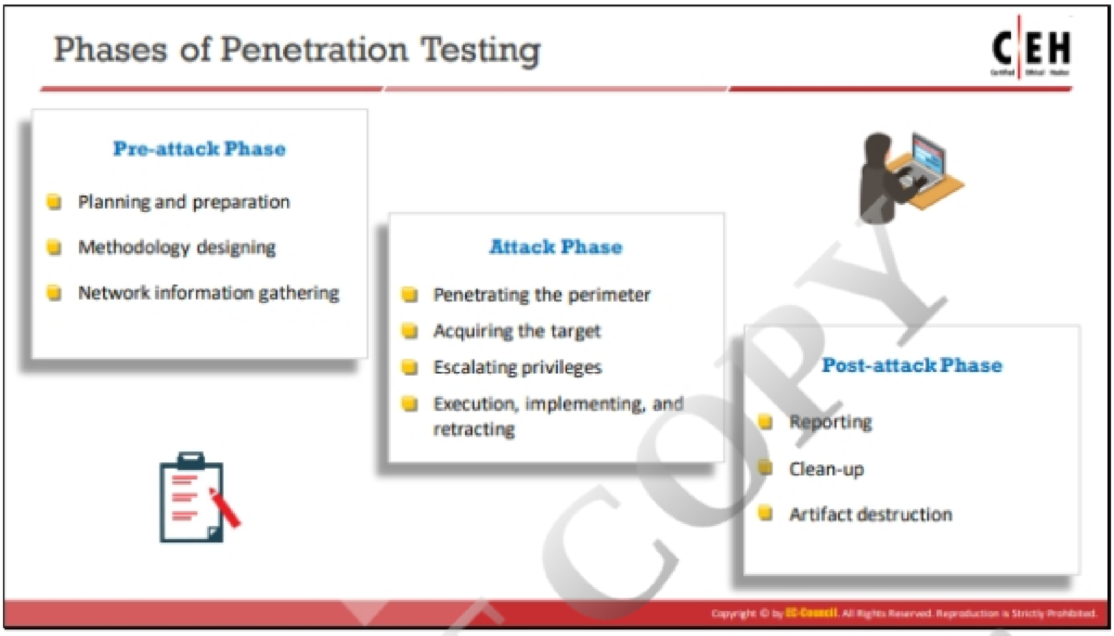
____

____

____

____

____



Phases of Penetration Testing

Pre-attack Phase

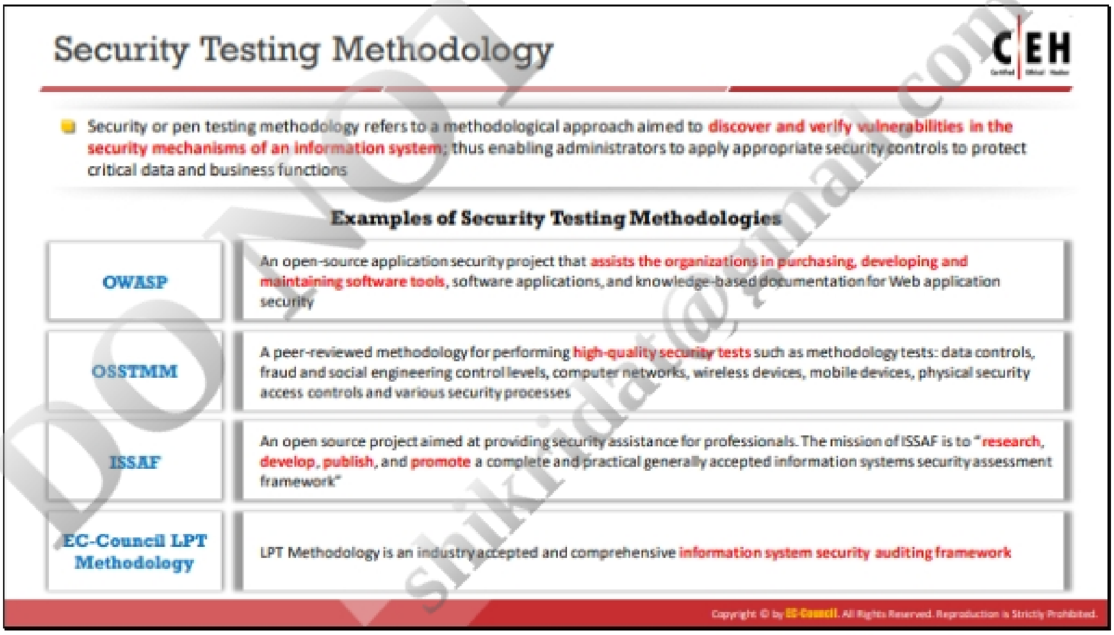
- Planning and preparation
- Methodology designing
- Network information gathering

Attack Phase

- Penetrating the perimeter
- Acquiring the target
- Escalating privileges
- Execution, implementing, and retracting

Post-attack Phase

- Reporting
- Clean-up
- Artifact destruction



Security Testing Methodology

- Security or pen testing methodology refers to a methodological approach aimed to **discover and verify vulnerabilities in the security mechanisms of an information system**; thus enabling administrators to apply appropriate security controls to protect critical data and business functions

Examples of Security Testing Methodologies

OWASP	An open-source application security project that **assists the organizations in purchasing, developing and maintaining software tools**, software applications, and knowledge-based documentation for Web application security
OSSTMM	A peer-reviewed methodology for performing **high-quality security tests** such as methodology tests: data controls, fraud and social engineering control levels, computer networks, wireless devices, mobile devices, physical security access controls and various security processes
ISSAF	An open source project aimed at providing security assistance for professionals. The mission of ISSAF is to "**research**, **develop**, **publish**, and **promote** a complete and practical generally accepted information systems security assessment framework"
EC-Council LPT Methodology	LPT Methodology is an industry accepted and comprehensive **information system security auditing framework**

Notes: ____

____

____

____

____

____