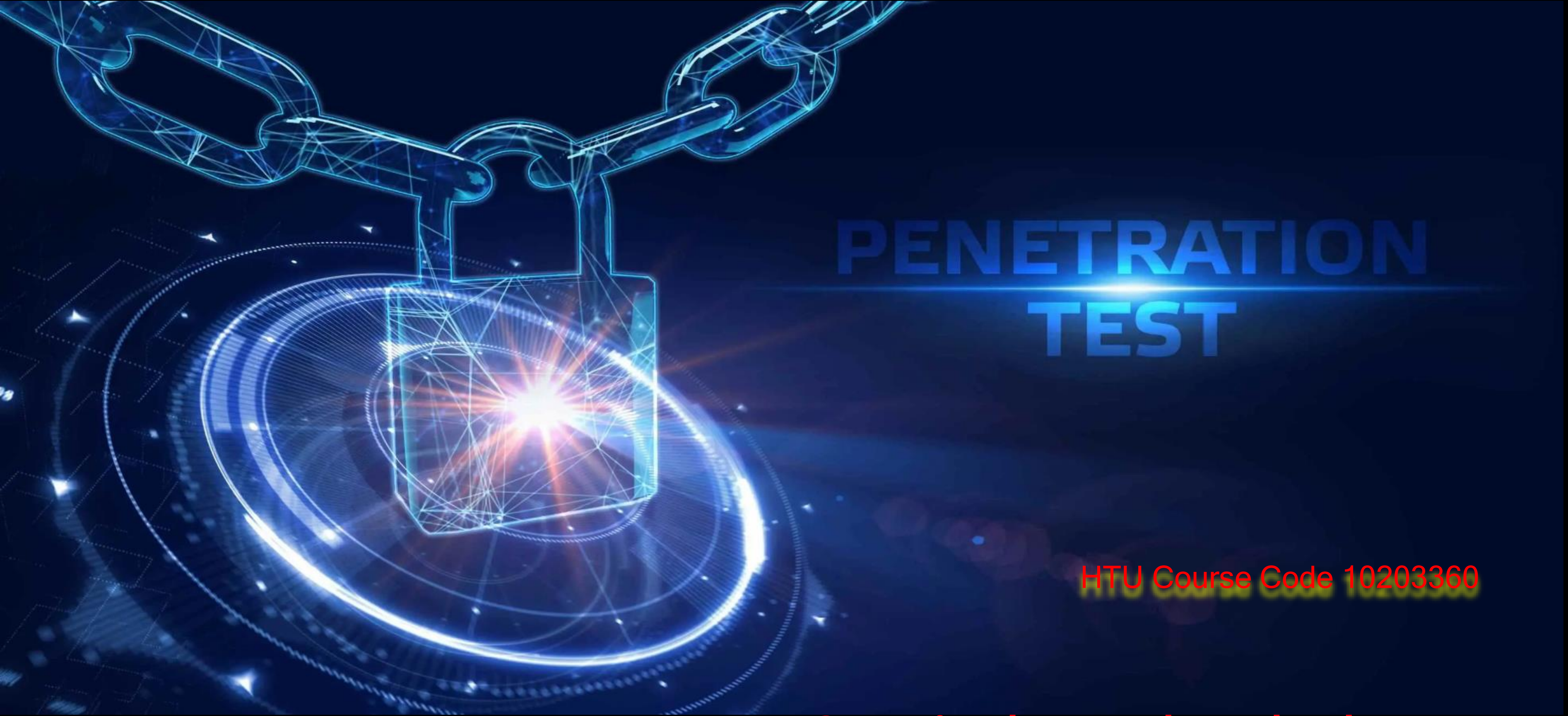


PENETRATION TEST

HTU Course Code 10203360

By: Sami Al-mashaqbeh

ETHICAL STATEMENT

In this course, you will explore and apply various tools and techniques within a controlled virtual machine environment to simulate cyber-attacks and discover, assess, and exploit built-in vulnerabilities. It is crucial to acknowledge that the hands-on labs are meant solely for educational purposes, aiming to equip you with the skills to identify and safeguard against real-world threats. The vulnerabilities and weaknesses demonstrated here must be used responsibly and ethically, exclusively within this designated environment.

Engaging with these tools, techniques, or resources beyond the provided virtual environment or outside your authorized scope may lead to violations of local laws and regulations. We strongly emphasize the **importance** of seeking clarification from your instructor before attempting any experimentation.

It is imperative to comprehend that **unauthorized access to data, computer systems, and networks is illegal** in numerous jurisdictions, **regardless of intentions or motivations**. We emphasize the significance of using your newfound knowledge responsibly and ensuring compliance with all applicable laws and regulations.

By accepting this "Statement," you acknowledge the critical importance of utilizing the skills acquired in this course for ethical and lawful purposes only, and you commit to upholding the principles of responsible cybersecurity practices. Remember, with great power comes great responsibility.

LEARNING OUTCOMES

LO#1: Gain foundational skills in penetration testing:

- Explain the importance of penetration testing in cybersecurity for assessing organizational security and fortifying defences.
- Discuss the types of penetration assessment and penetration testing strategies.
- Discuss common areas of penetration testing and the ethical considerations of a penetration tester.
- Explain how to initiate, engage, and proceed with the penetration testing.
- Analyze in detail the risks associated with penetration testing.

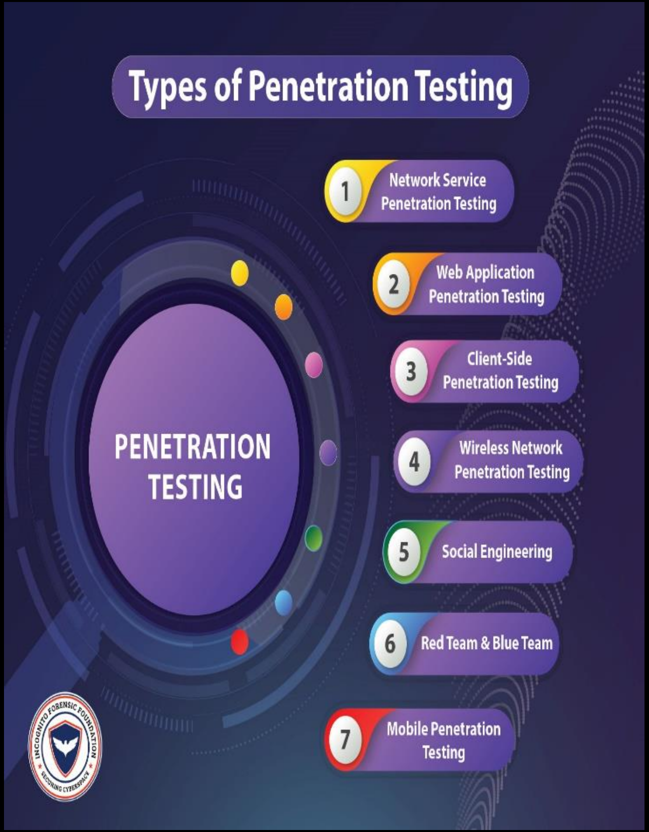
WHY WE NEED PENETRATION TESTING?

- Penetration testing is a type of security testing that evaluates an organization’s ability to protect its infrastructure such as network, applications, systems, and users against external as well as internal threats.
- It is an effective way of determining the efficacy of the organization’s security policies, controls, and technologies.
- It involves the active evaluation of the security of the organization’s infrastructure by simulating an attack similar to those performed by real attacker.
- During a penetration test, security measures are actively analyzed for design weaknesses, technical flaws, and vulnerabilities.
- The test results are documented and delivered in a comprehensive report to executive management and technical audiences.

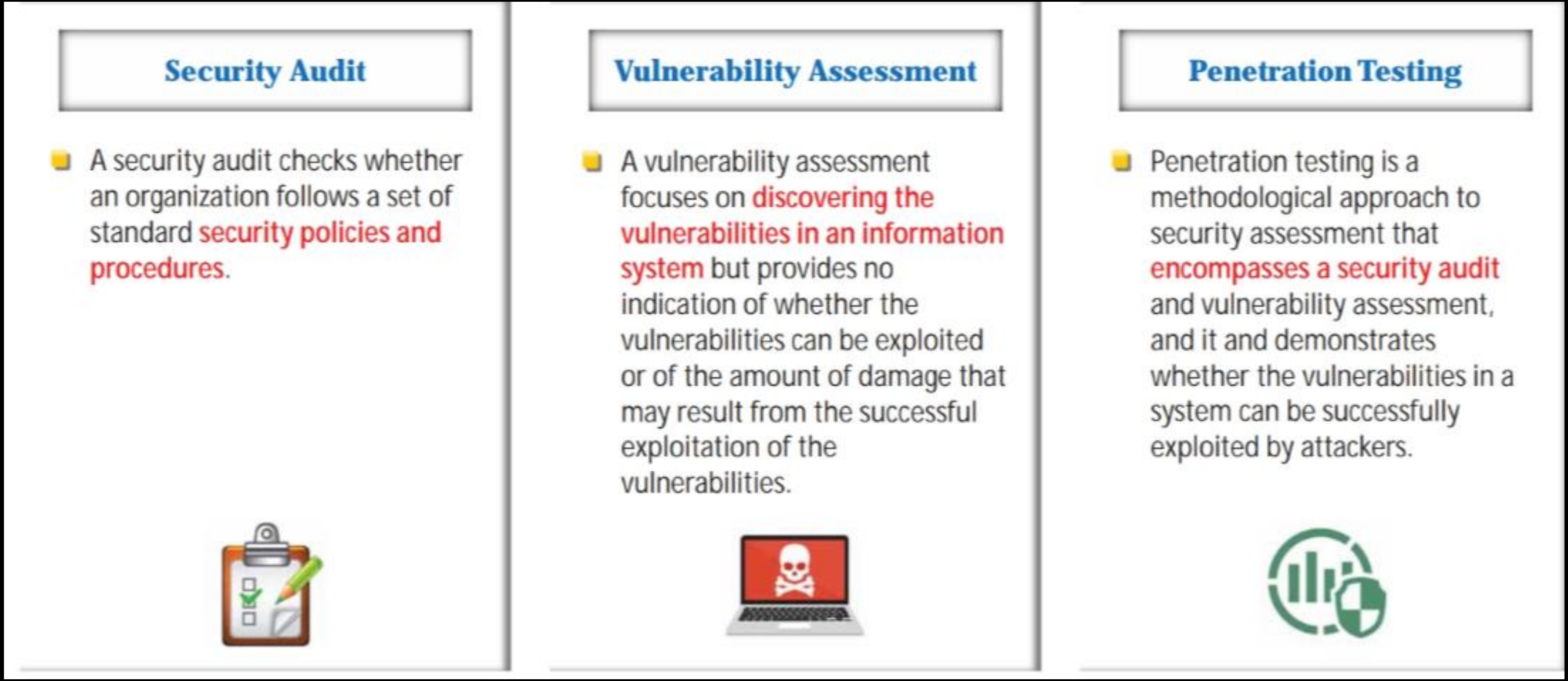
ETHICAL HACKING VS PENETRATION TESTING

- Before we jump into how to perform penetration testing, you first need to understand some core concepts about the “art of hacking”. For example, you need to understand the difference between *ethical hacking* and *unethical hacking*. Understanding the tools and techniques used in this field, understanding the most current threats and attacker motivations is also important.

- Penetration testing is a subset of ethical hacking, where security experts attempt to exploit identified vulnerabilities to determine the potential impact of a successful attack. The focus of penetration testing is on actively exploiting vulnerabilities to assess the effectiveness of security controls and to understand the extent to which an attacker can gain unauthorized access, steal data, or disrupt services. Penetration testing provides actionable insights into specific security flaws and helps organizations prioritize remediation efforts.


Types of Penetration Testing
PENETRATION TESTING
1 Network Service Penetration Testing
2 Web Application Penetration Testing
3 Client-Side Penetration Testing
4 Wireless Network Penetration Testing
5 Social Engineering
6 Red Team & Blue Team
7 Mobile Penetration Testing
INCOGNITO FORENSIC FOUNDATION
SECURING CYBERSPACE

SECURITY AUDIT, VULNERABILITY ASSESSMENT, AND PENETRATION TESTING



Security Audit

- A security audit checks whether an organization follows a set of standard security policies and procedures.

Vulnerability Assessment

- A vulnerability assessment focuses on discovering the vulnerabilities in an information system but provides no indication of whether the vulnerabilities can be exploited or of the amount of damage that may result from the successful exploitation of the vulnerabilities.

Penetration Testing

- Penetration testing is a methodological approach to security assessment that encompasses a security audit and vulnerability assessment, and it and demonstrates whether the vulnerabilities in a system can be successfully exploited by attackers.

SECURITY AUDIT, VULNERABILITY ASSESSMENT, AND PENETRATION TESTING

- Penetration testing should not be simply ticking check boxes to meet security requirements.

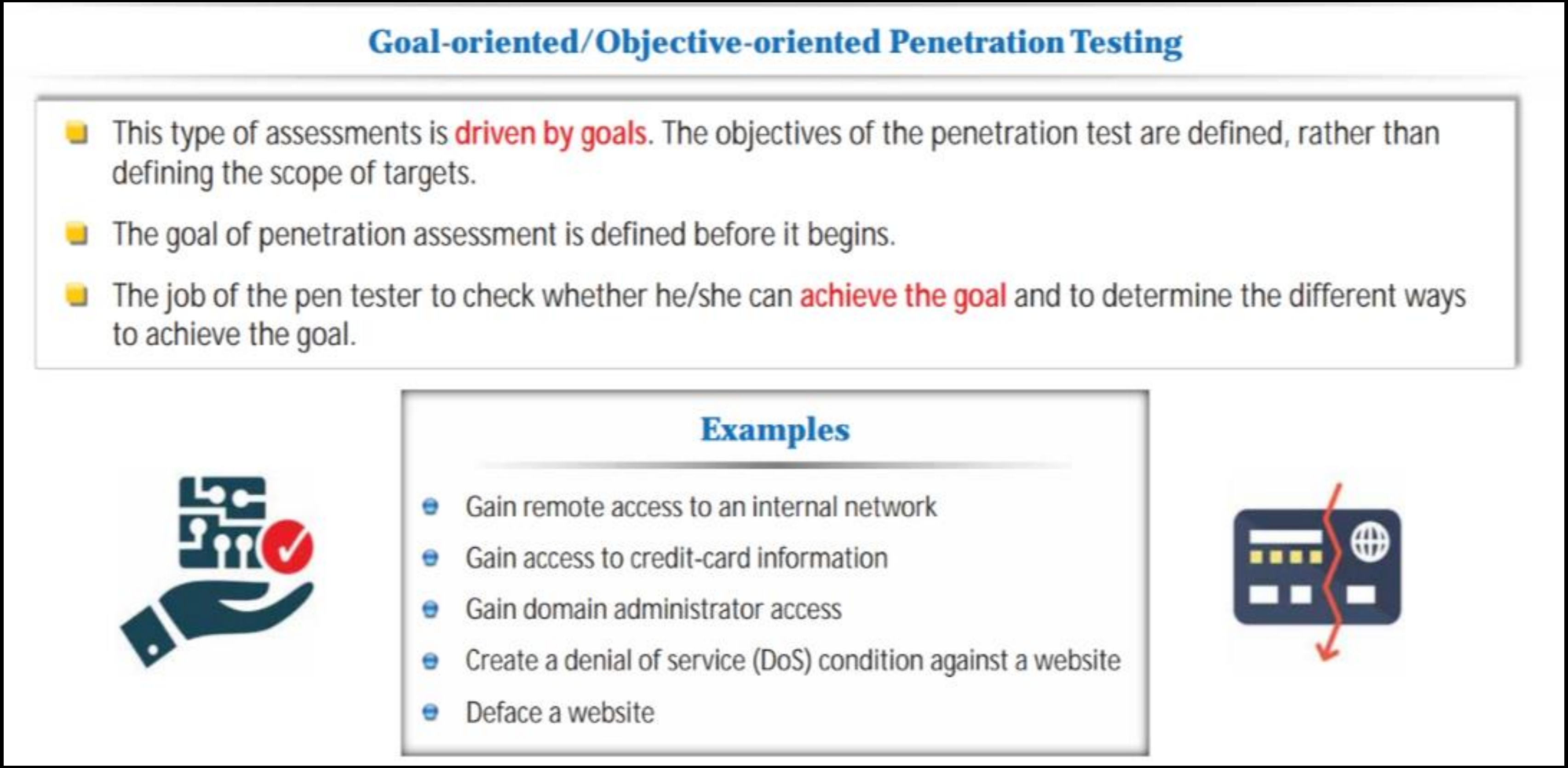
- Vulnerability scanning should be a part of a pen testing program but is not a substitute.

- Penetration testing focuses on achieving goals and not on finding vulnerabilities.

TYPES OF PENETRATION ASSESSMENT

- Goal-oriented
- Compliance-oriented
- Red-team-oriented

TYPES OF PENETRATION ASSESSMENT



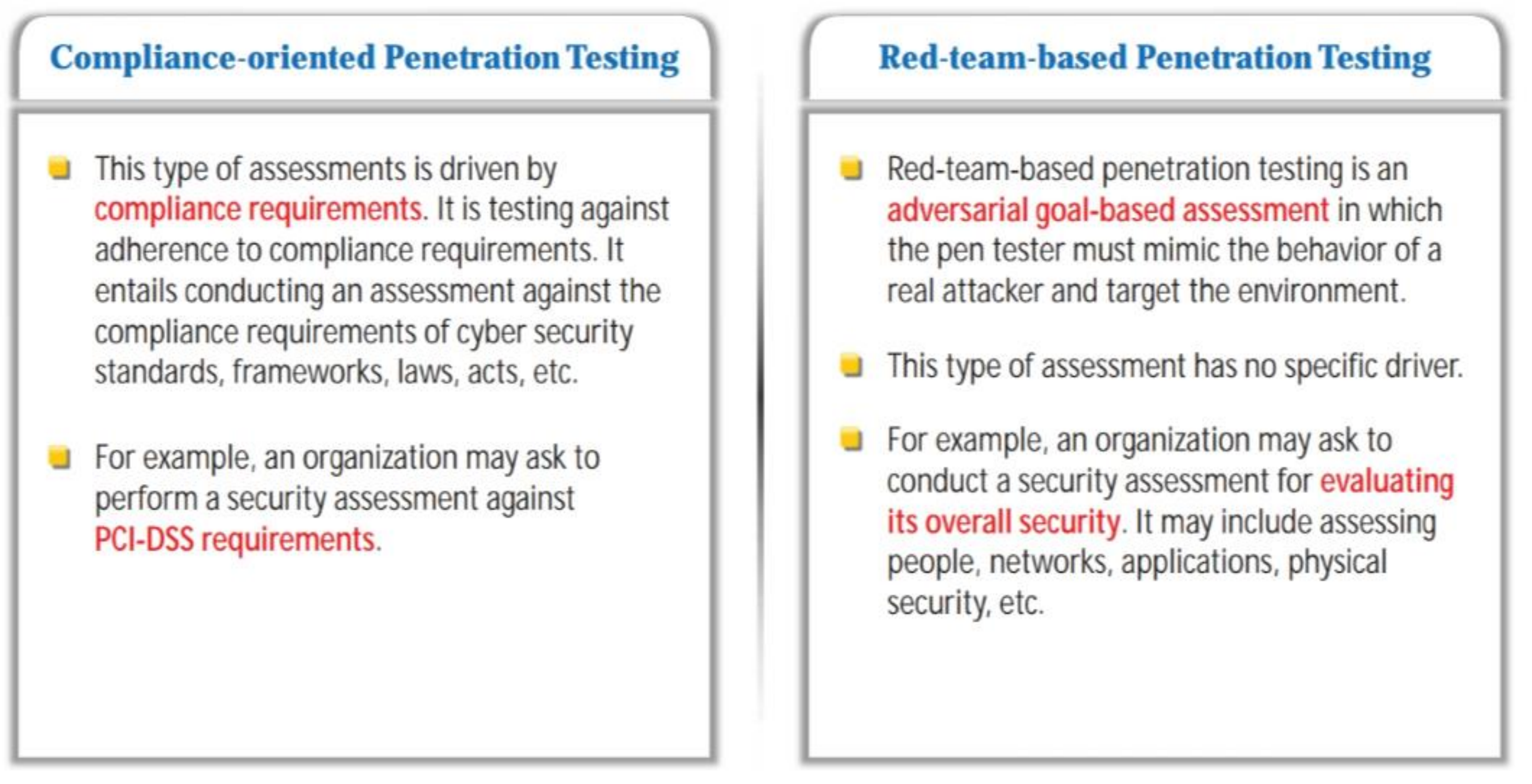
Goal-oriented/Objective-oriented Penetration Testing

- This type of assessments is driven by goals. The objectives of the penetration test are defined, rather than defining the scope of targets.
- The goal of penetration assessment is defined before it begins.
- The job of the pen tester to check whether he/she can achieve the goal and to determine the different ways to achieve the goal.

Examples

- Gain remote access to an internal network
- Gain access to credit-card information
- Gain domain administrator access
- Create a denial of service (DoS) condition against a website
- Deface a website

TYPES OF PENETRATION ASSESSMENT



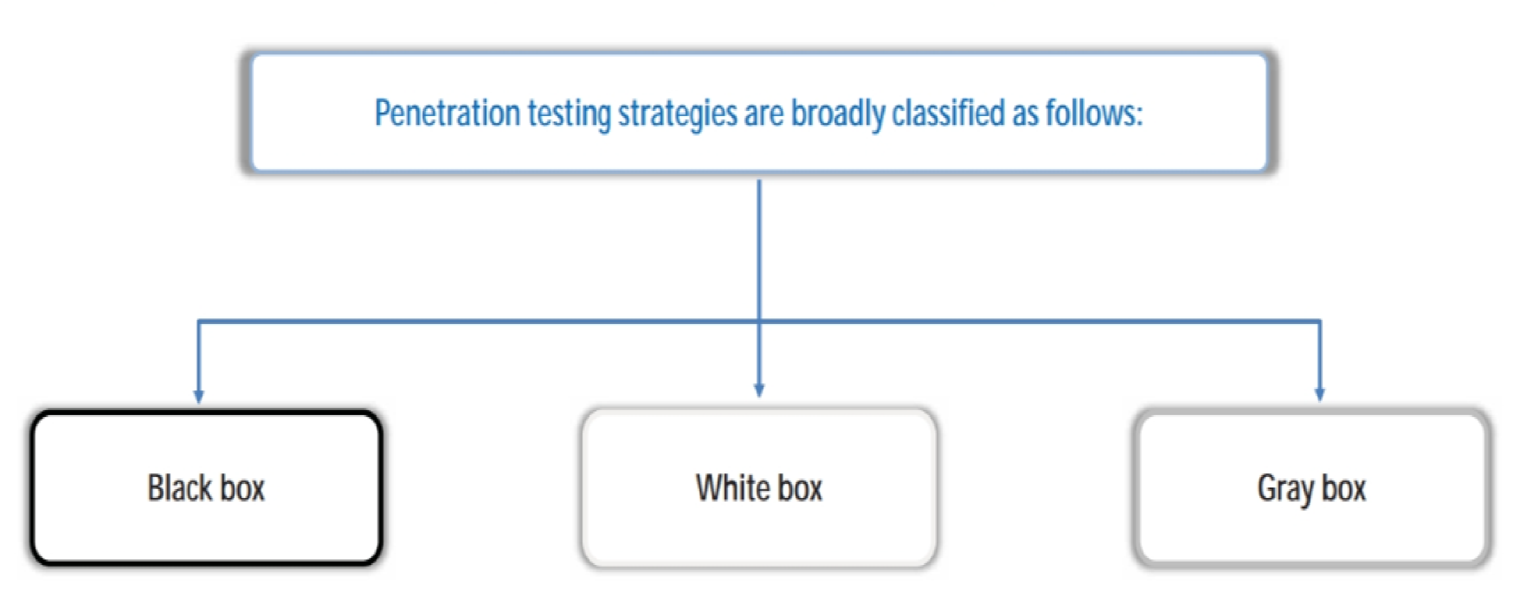
Compliance-oriented Penetration Testing

- This type of assessments is driven by compliance requirements. It is testing against adherence to compliance requirements. It entails conducting an assessment against the compliance requirements of cyber security standards, frameworks, laws, acts, etc.
- For example, an organization may ask to perform a security assessment against PCI-DSS requirements.

Red-team-based Penetration Testing

- Red-team-based penetration testing is an adversarial goal-based assessment in which the pen tester must mimic the behavior of a real attacker and target the environment.
- This type of assessment has no specific driver.
- For example, an organization may ask to conduct a security assessment for evaluating its overall security. It may include assessing people, networks, applications, physical security, etc.

STRATEGIES OF PENETRATION TESTING



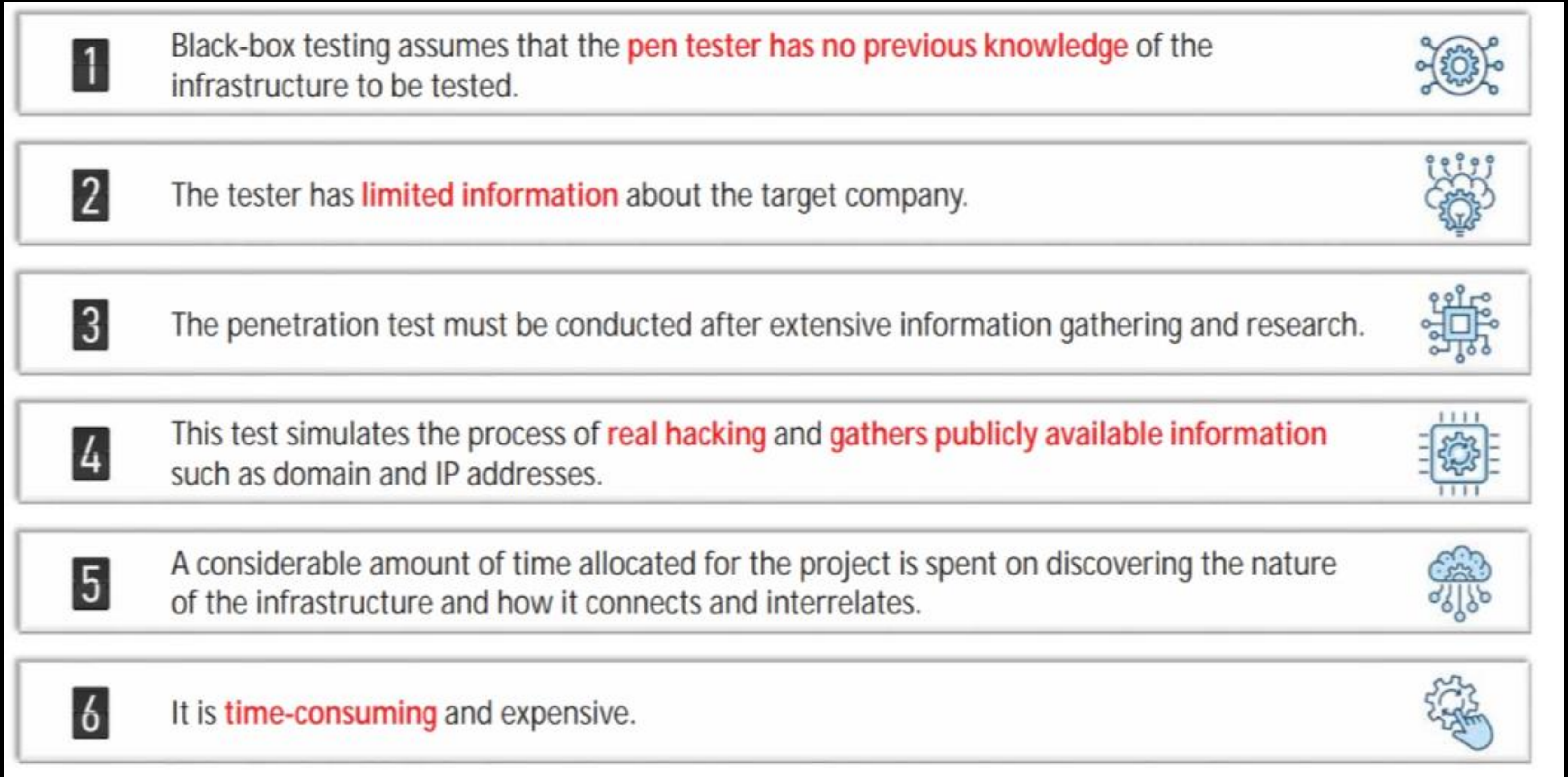
Penetration testing strategies are broadly classified as follows:

Black box

White box

Gray box

BLACK-BOX PENETRATION TESTING



1 Black-box testing assumes that the pen tester has no previous knowledge of the infrastructure to be tested.

2 The tester has limited information about the target company.

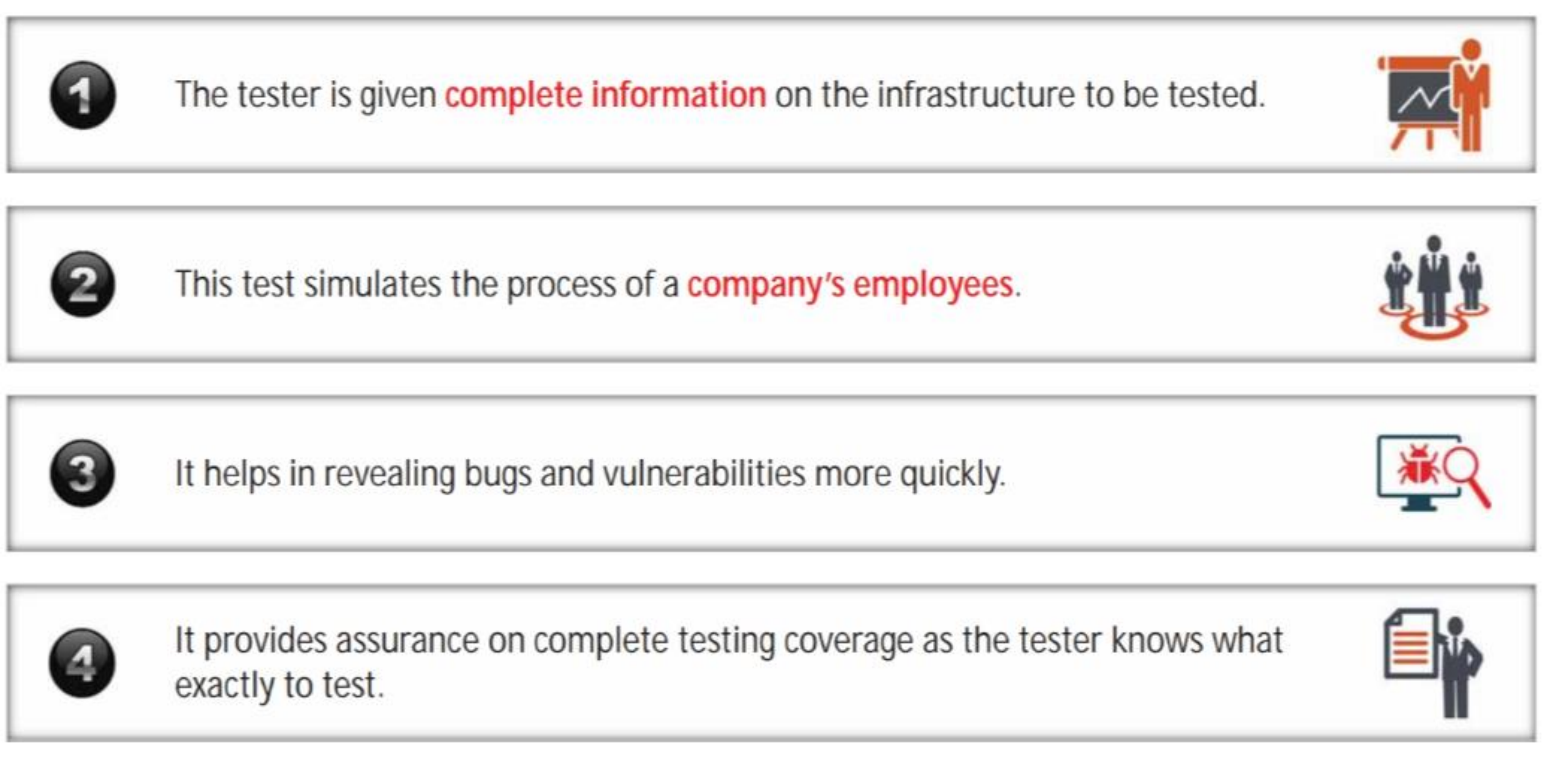
3 The penetration test must be conducted after extensive information gathering and research.

4 This test simulates the process of real hacking and gathers publicly available information such as domain and IP addresses.

5 A considerable amount of time allocated for the project is spent on discovering the nature of the infrastructure and how it connects and interrelates.

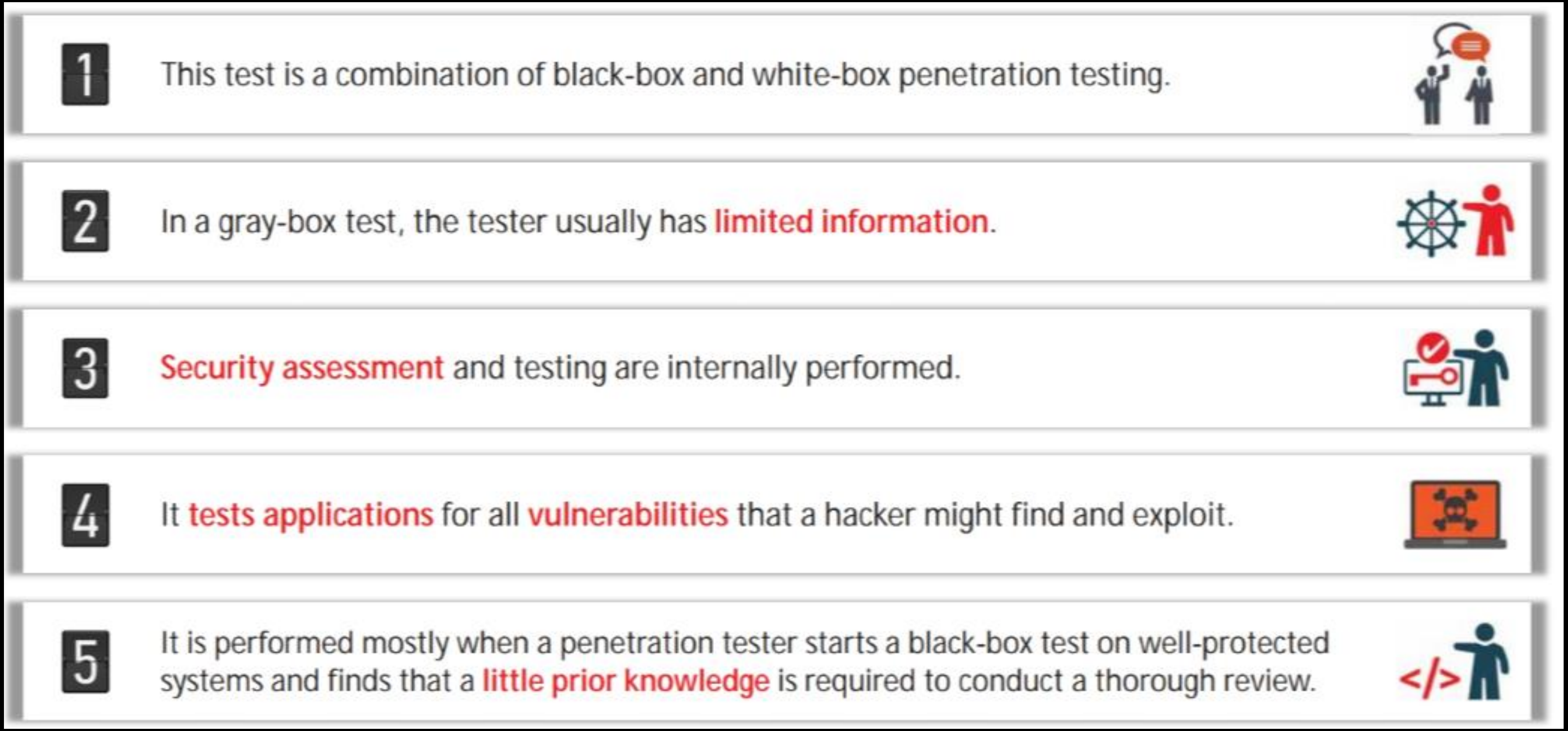
6 It is time-consuming and expensive.

WHITE-BOX PENETRATION TESTING



1. The tester is given **complete information** on the infrastructure to be tested.
2. This test simulates the process of a **company's employees**.
3. It helps in revealing bugs and vulnerabilities more quickly.
4. It provides assurance on complete testing coverage as the tester knows what exactly to test.

GRAY-BOX PENETRATION TESTING



1 This test is a combination of black-box and white-box penetration testing.

2 In a gray-box test, the tester usually has limited information.

3 Security assessment and testing are internally performed.

4 It tests applications for all vulnerabilities that a hacker might find and exploit.

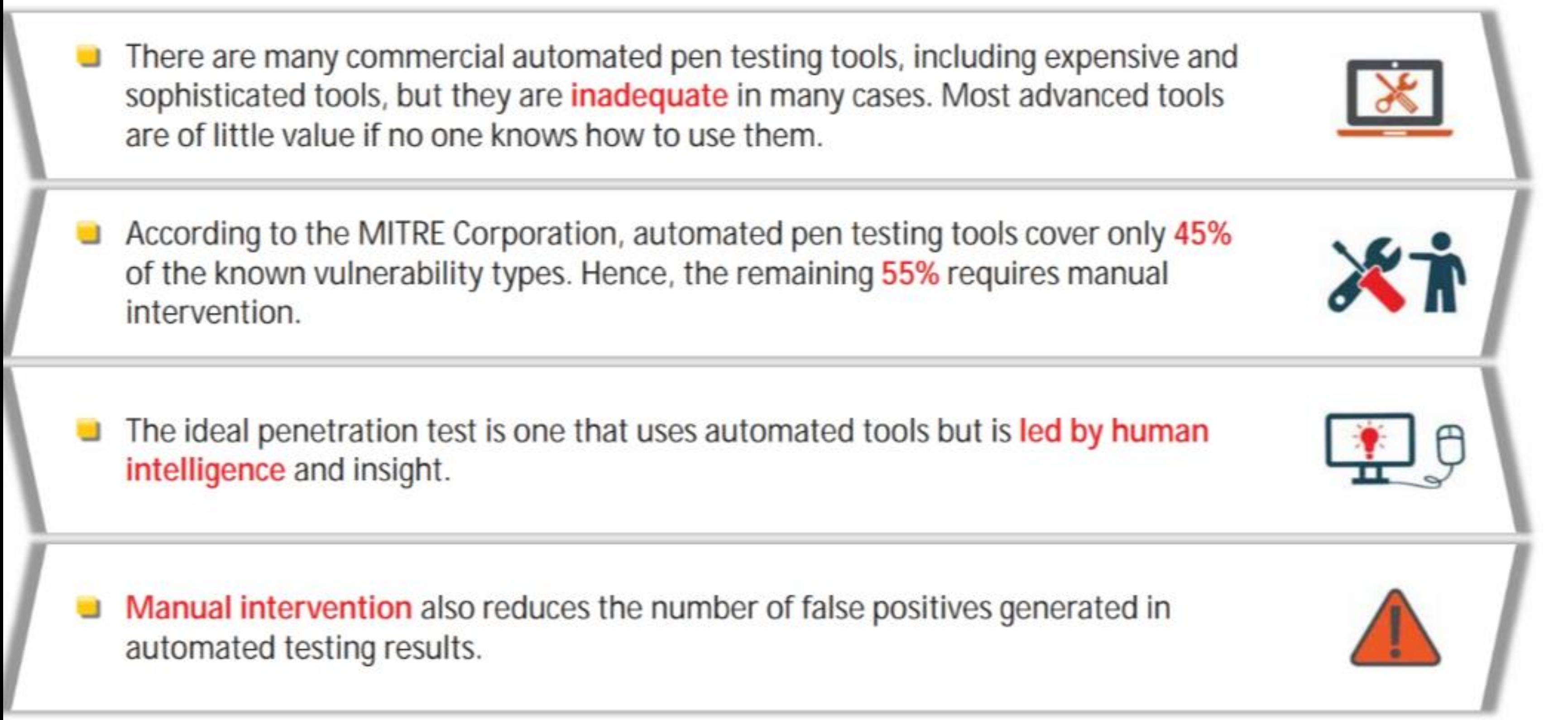
5 It is performed mostly when a penetration tester starts a black-box test on well-protected systems and finds that a little prior knowledge is required to conduct a thorough review.

METHODS OF PENETRATION TESTING

- **Automated Penetration Testing:** is performed with the help of various commercial or opensource penetration testing/security assessment tools.

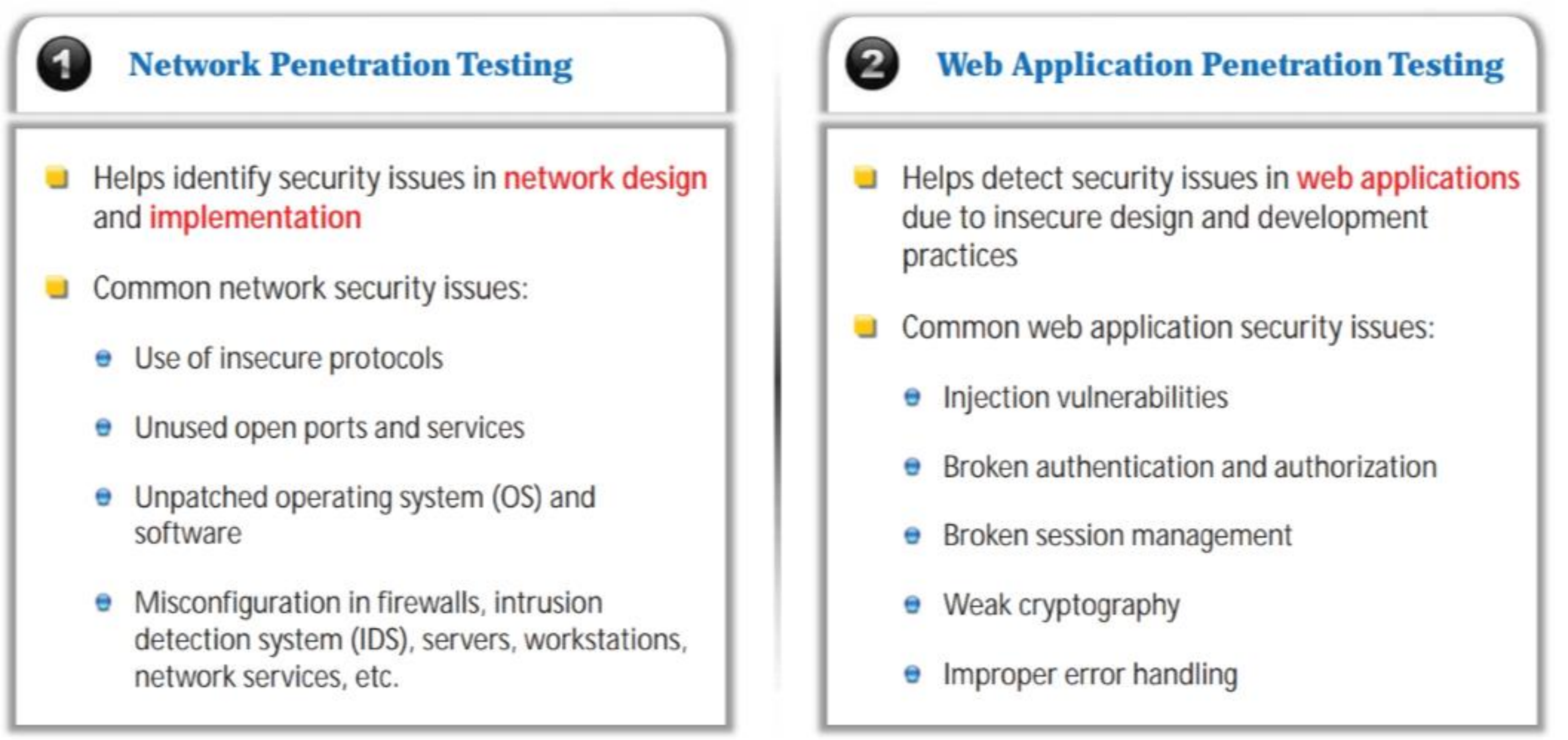
- **Manual penetration testing :** is performed by an individual or a group of individuals who are experts in penetration testing.

SELECTING THE APPROPRIATE METHOD OF PENETRATION TESTING



- There are many commercial automated pen testing tools, including expensive and sophisticated tools, but they are inadequate in many cases. Most advanced tools are of little value if no one knows how to use them.
- According to the MITRE Corporation, automated pen testing tools cover only 45% of the known vulnerability types. Hence, the remaining 55% requires manual intervention.
- The ideal penetration test is one that uses automated tools but is led by human intelligence and insight.
- Manual intervention also reduces the number of false positives generated in automated testing results.

COMMON AREAS OF PENETRATION TESTING



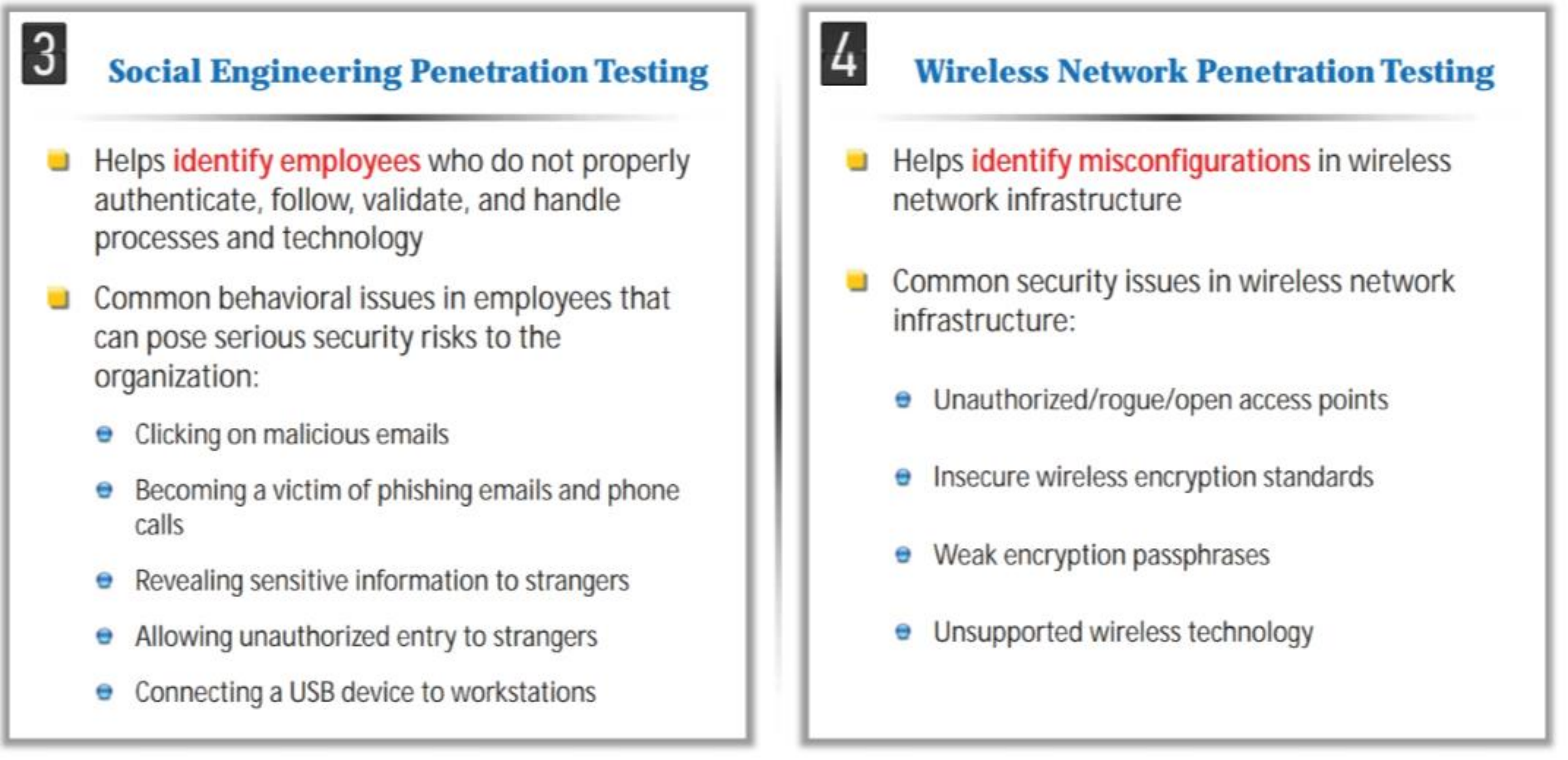
1 Network Penetration Testing

- Helps identify security issues in network design and implementation
- Common network security issues:
  - Use of insecure protocols
  - Unused open ports and services
  - Unpatched operating system (OS) and software
  - Misconfiguration in firewalls, intrusion detection system (IDS), servers, workstations, network services, etc.

2 Web Application Penetration Testing

- Helps detect security issues in web applications due to insecure design and development practices
- Common web application security issues:
  - Injection vulnerabilities
  - Broken authentication and authorization
  - Broken session management
  - Weak cryptography
  - Improper error handling

COMMON AREAS OF PENETRATION TESTING



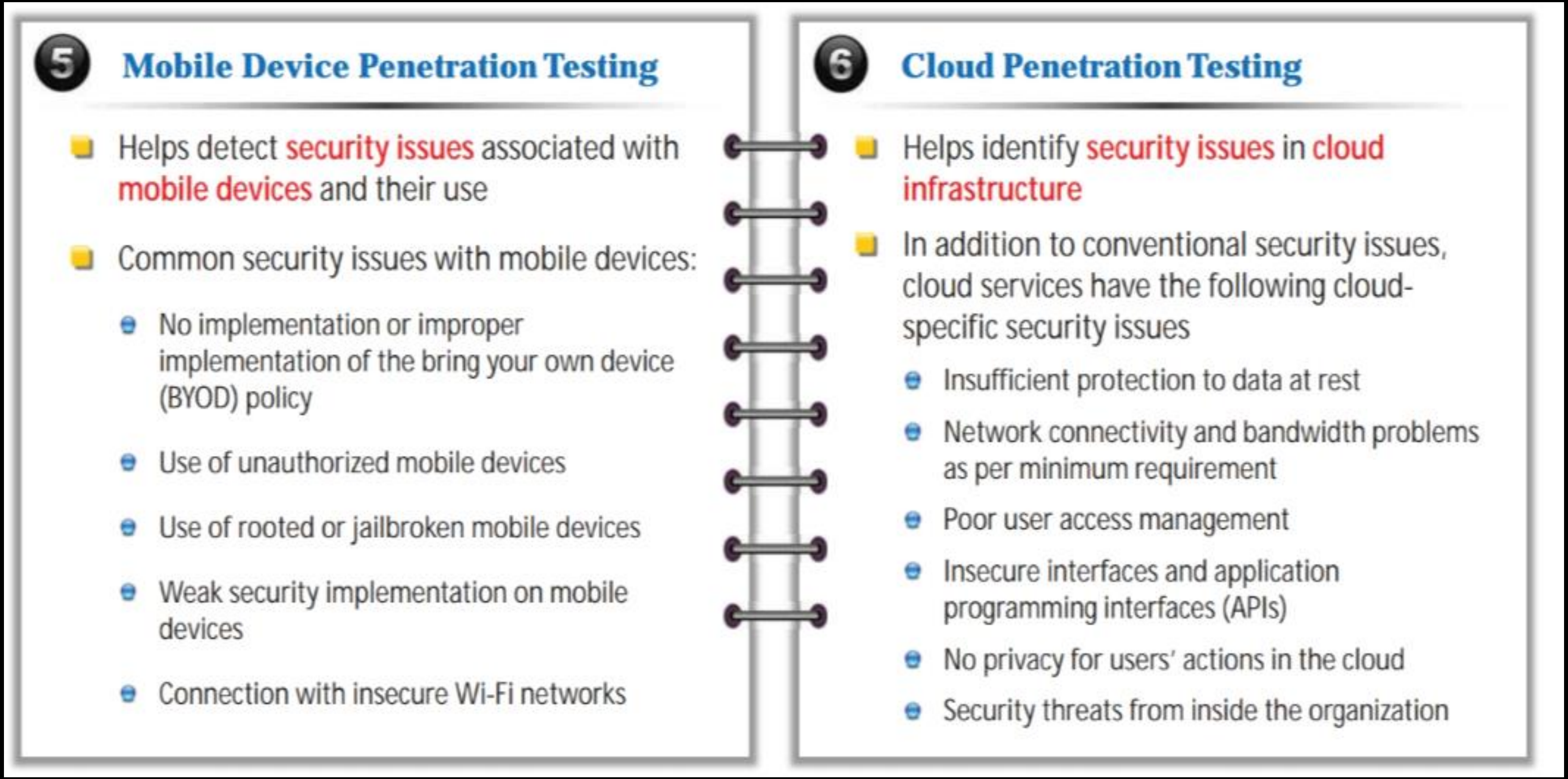
3 Social Engineering Penetration Testing

- Helps identify employees who do not properly authenticate, follow, validate, and handle processes and technology
- Common behavioral issues in employees that can pose serious security risks to the organization:
  - Clicking on malicious emails
  - Becoming a victim of phishing emails and phone calls
  - Revealing sensitive information to strangers
  - Allowing unauthorized entry to strangers
  - Connecting a USB device to workstations

4 Wireless Network Penetration Testing

- Helps identify misconfigurations in wireless network infrastructure
- Common security issues in wireless network infrastructure:
  - Unauthorized/rogue/open access points
  - Insecure wireless encryption standards
  - Weak encryption passphrases
  - Unsupported wireless technology

COMMON AREAS OF PENETRATION TESTING



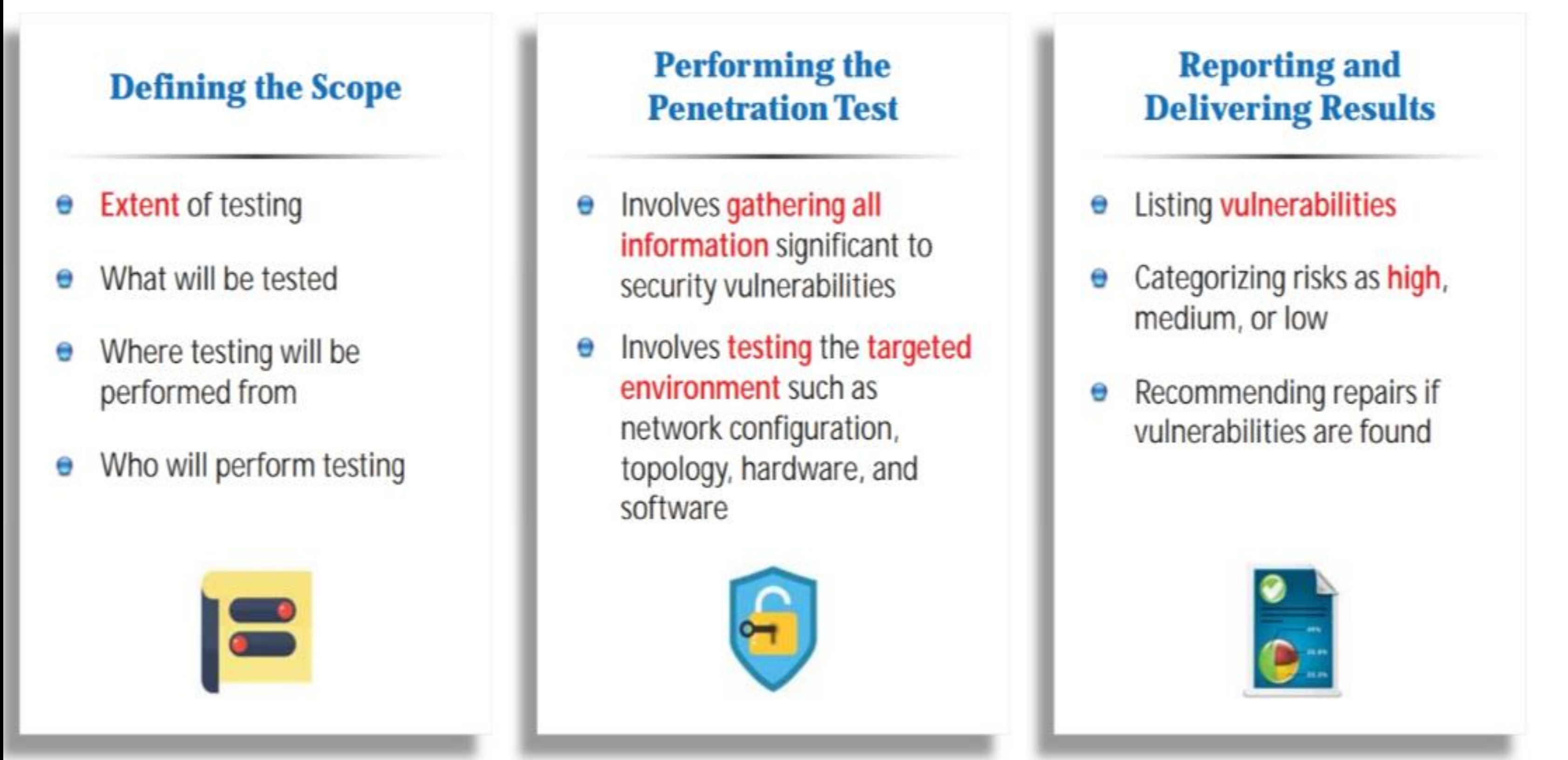
5 Mobile Device Penetration Testing

- Helps detect security issues associated with mobile devices and their use
- Common security issues with mobile devices:
  - No implementation or improper implementation of the bring your own device (BYOD) policy
  - Use of unauthorized mobile devices
  - Use of rooted or jailbroken mobile devices
  - Weak security implementation on mobile devices
  - Connection with insecure Wi-Fi networks

6 Cloud Penetration Testing

- Helps identify security issues in cloud infrastructure
- In addition to conventional security issues, cloud services have the following cloud-specific security issues
  - Insufficient protection to data at rest
  - Network connectivity and bandwidth problems as per minimum requirement
  - Poor user access management
  - Insecure interfaces and application programming interfaces (APIs)
  - No privacy for users' actions in the cloud
  - Security threats from inside the organization

PENETRATION TESTING PROCESS



Defining the Scope

- Extent of testing
- What will be tested
- Where testing will be performed from
- Who will perform testing

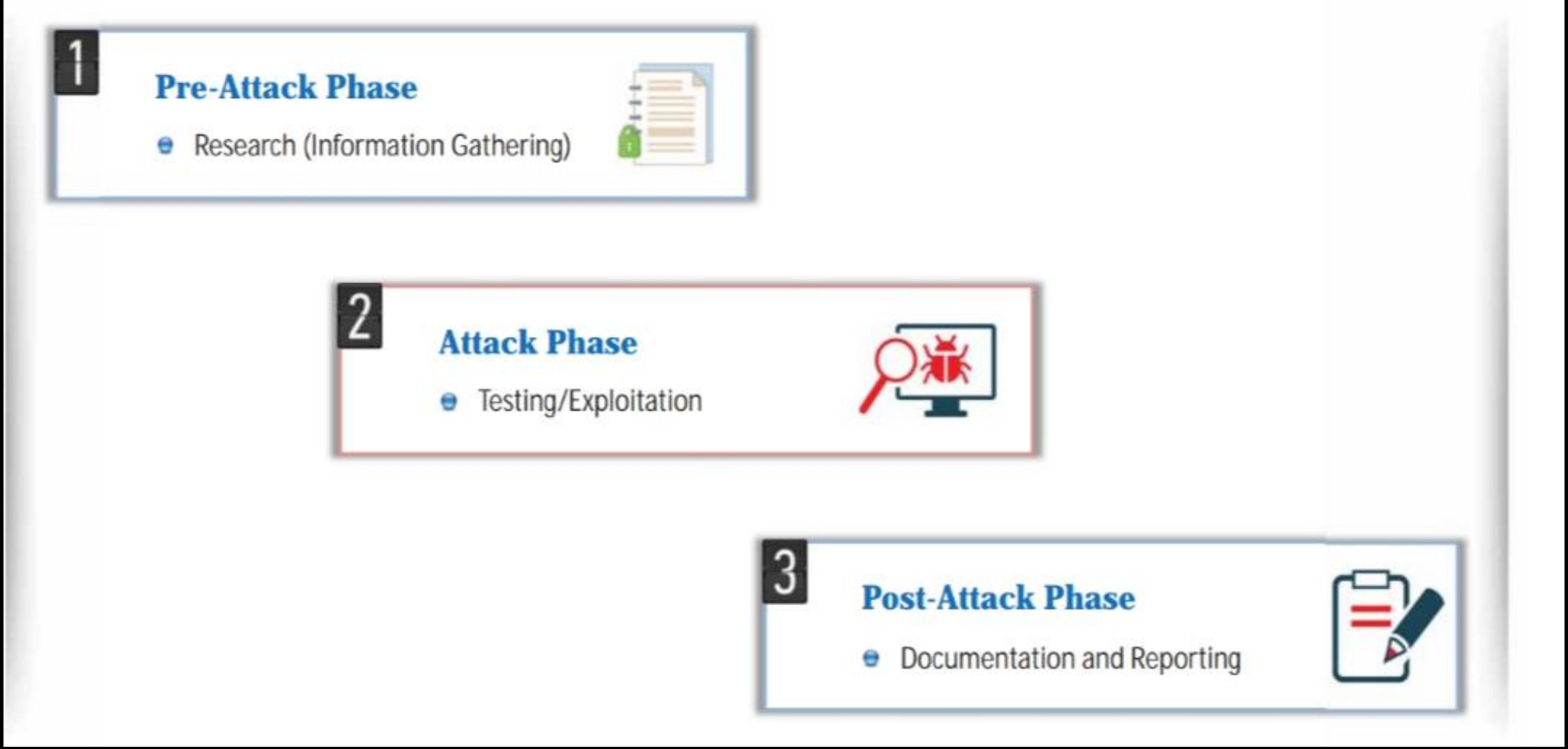
Performing the Penetration Test

- Involves gathering all information significant to security vulnerabilities
- Involves testing the targeted environment such as network configuration, topology, hardware, and software

Reporting and Delivering Results

- Listing vulnerabilities
- Categorizing risks as high, medium, or low
- Recommending repairs if vulnerabilities are found

PENETRATION TESTING PHASES



1

Pre-Attack Phase

- Research (Information Gathering)

2

Attack Phase

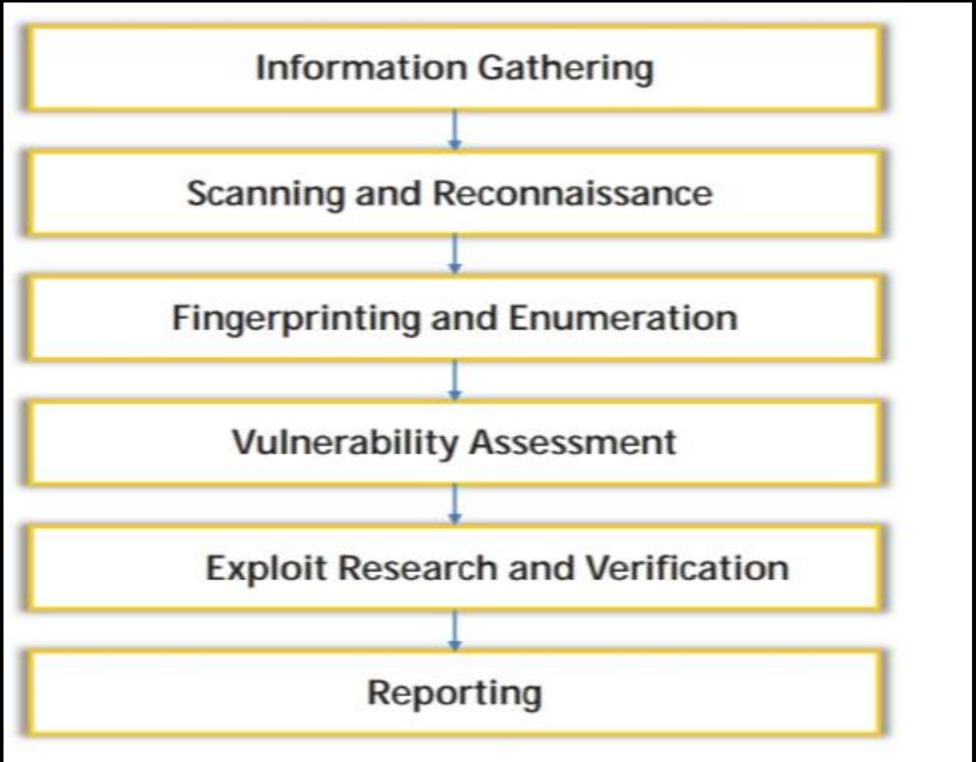
- Testing/Exploitation

3

Post-Attack Phase

- Documentation and Reporting

PENETRATION TESTING METHODOLOGY



Information Gathering

Scanning and Reconnaissance

Fingerprinting and Enumeration

Vulnerability Assessment

Exploit Research and Verification

Reporting

HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Preparation and Planning:

- Clearly define the scope of the penetration test, including systems, networks, and applications to be tested.
- Obtain necessary permissions from relevant stakeholders, such as system owners and management.
- Assemble a skilled and qualified penetration testing team or hire a reputable third-party firm with experienced professionals.
- Establish rules of engagement, including the timing, methods, and limitations of the test.
- Ensure that all necessary legal and compliance requirements are met.

HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Information Gathering:

- Gather as much information as possible about the target system or network using both passive and active reconnaissance techniques.
- Identify potential entry points, such as open ports, services running on the target systems, and any publicly available information about the organization.

HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Vulnerability Analysis:

- Perform a comprehensive assessment of the target environment to identify potential vulnerabilities.

- Utilize automated vulnerability scanning tools as well as manual inspection to uncover vulnerabilities that may be missed by automated tools.

- Prioritize identified vulnerabilities based on their severity and potential impact on the organization.

HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Exploitation:

- Once vulnerabilities are identified, attempt to exploit them to gain unauthorized access to the target systems or sensitive information.

- Exercise caution to avoid causing disruption or damage to the target environment during exploitation.

- Document successful exploitation techniques for later analysis and remediation.

HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Post-Exploitation:

- Once access is gained to the target systems, conduct further exploration to identify additional weaknesses or sensitive data.

- Escalate privileges if possible to simulate the actions of a sophisticated attacker.

- Document all findings, including the compromised systems, data accessed, and potential impact on the organization.

HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Reporting:

- Prepare a detailed report summarizing the findings of the penetration test, including vulnerabilities discovered, their severity, and recommendations for remediation.

- Provide clear and actionable recommendations for improving the security posture of the target environment.

- Present the findings to relevant stakeholders, including technical teams, management, and executives, in a clear and understandable manner.

HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Remediation and Follow-Up:

- Work closely with the organization's IT and security teams to address identified vulnerabilities and weaknesses.

- Verify that remediation efforts are effective in mitigating the identified risks.

- Conduct follow-up assessments periodically to ensure that security improvements are maintained over time.

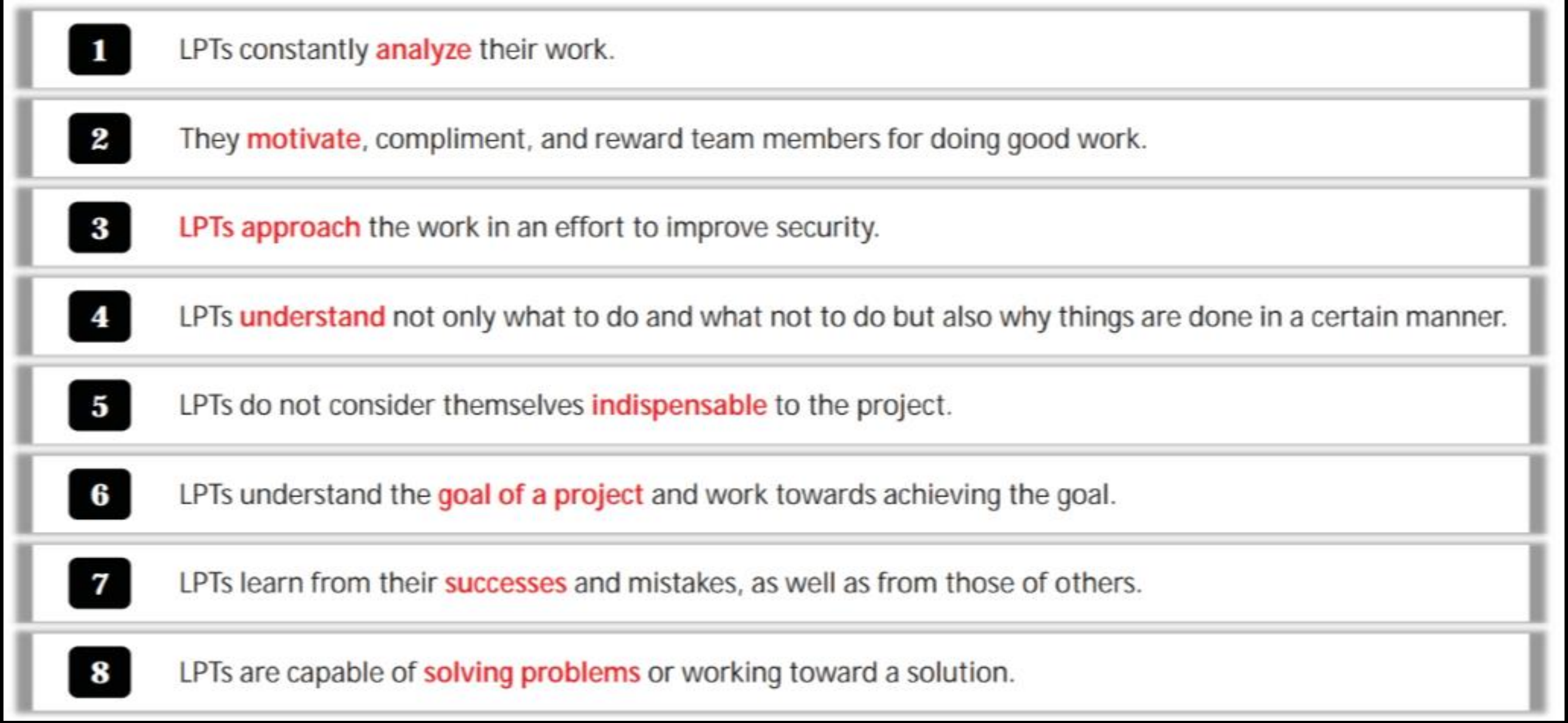
HOW TO INITIATE, ENGAGE, AND PROCEED WITH THE PENETRATION TESTING

Continuous Improvement:

- Learn from each penetration testing engagement to refine and improve future testing methodologies.

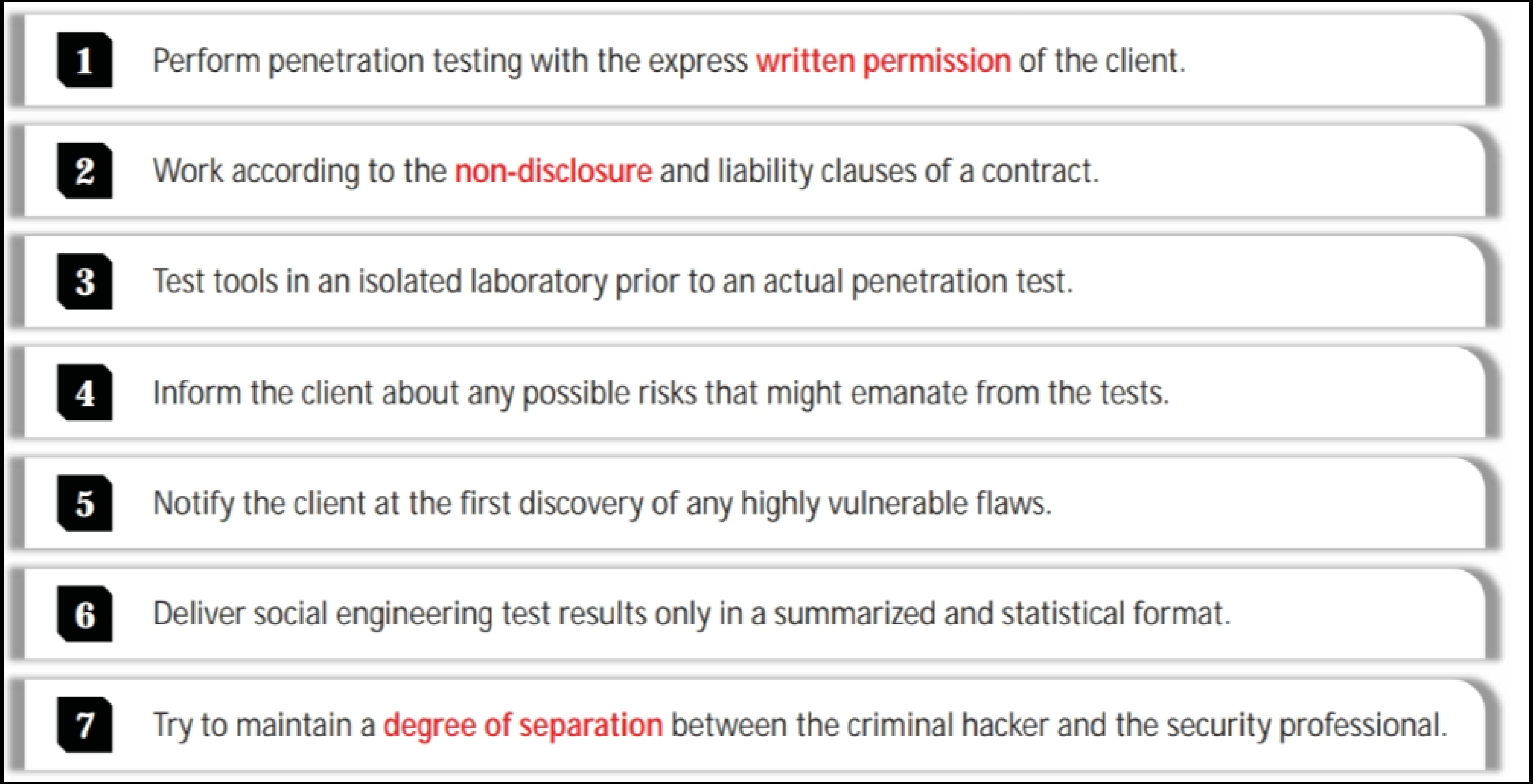
- Stay updated on the latest security threats, vulnerabilities, and exploitation techniques to ensure the effectiveness of penetration testing efforts.

QUALITIES OF A LICENSED PENETRATION TESTER



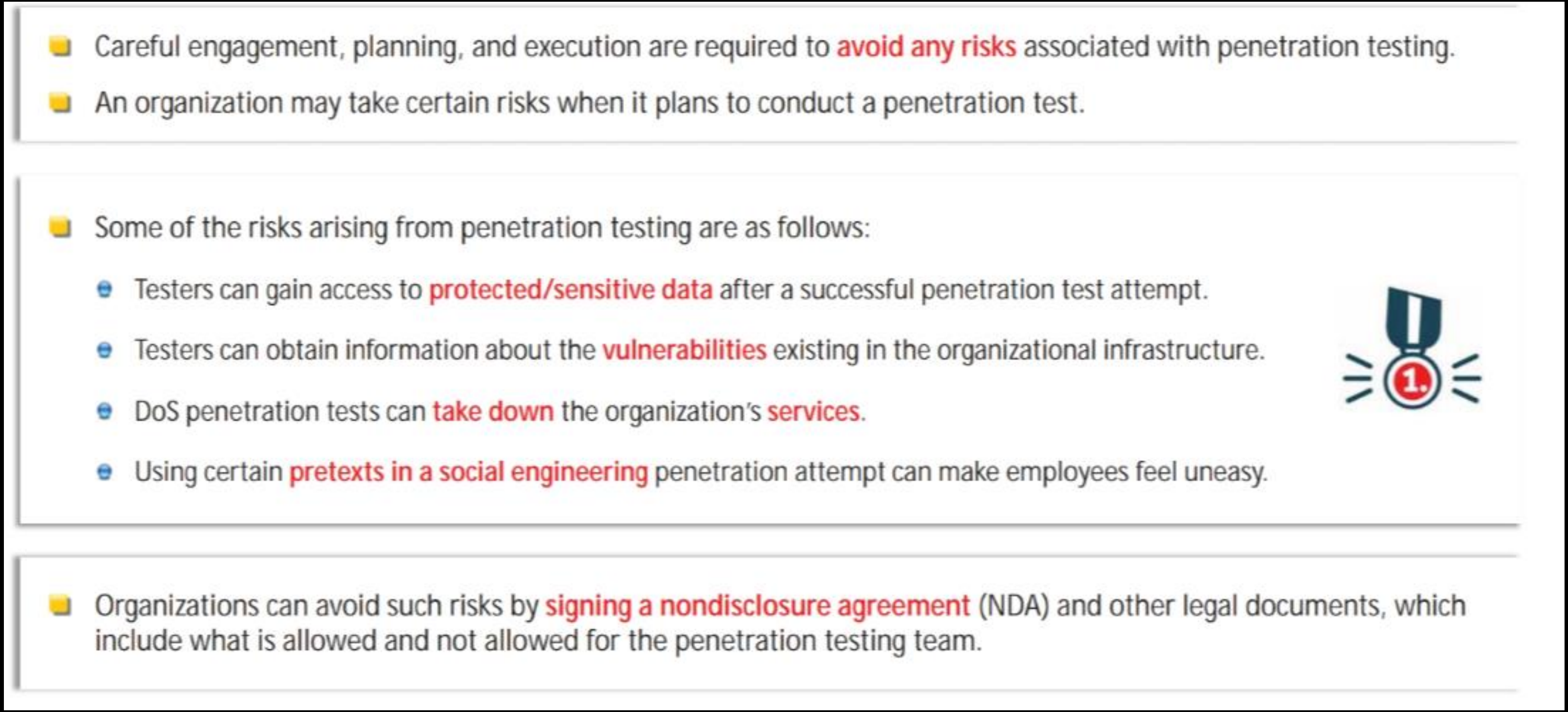
1. LPTs constantly analyze their work.
2. They motivate, compliment, and reward team members for doing good work.
3. LPTs approach the work in an effort to improve security.
4. LPTs understand not only what to do and what not to do but also why things are done in a certain manner.
5. LPTs do not consider themselves indispensable to the project.
6. LPTs understand the goal of a project and work towards achieving the goal.
7. LPTs learn from their successes and mistakes, as well as from those of others.
8. LPTs are capable of solving problems or working toward a solution.

ETHICS OF A PENETRATION TESTER



1. Perform penetration testing with the express written permission of the client.
2. Work according to the non-disclosure and liability clauses of a contract.
3. Test tools in an isolated laboratory prior to an actual penetration test.
4. Inform the client about any possible risks that might emanate from the tests.
5. Notify the client at the first discovery of any highly vulnerable flaws.
6. Deliver social engineering test results only in a summarized and statistical format.
7. Try to maintain a degree of separation between the criminal hacker and the security professional.

RISKS ASSOCIATED WITH PENETRATION TESTING

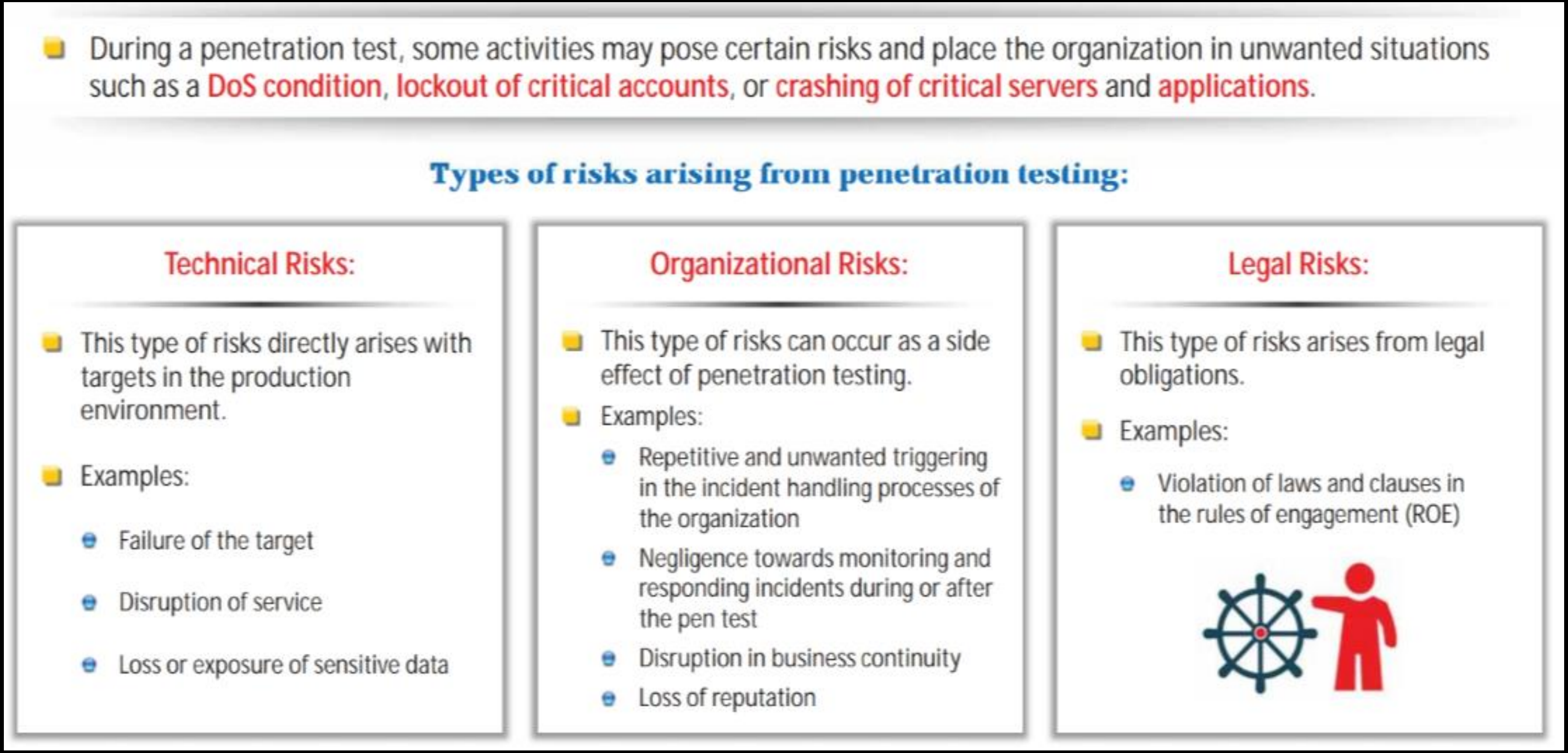


- Careful engagement, planning, and execution are required to avoid any risks associated with penetration testing.
- An organization may take certain risks when it plans to conduct a penetration test.

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

- Organizations can avoid such risks by signing a nondisclosure agreement (NDA) and other legal documents, which include what is allowed and not allowed for the penetration testing team.

TYPES OF RISKS ARISING FROM PENETRATION TESTING



- During a penetration test, some activities may pose certain risks and place the organization in unwanted situations such as a DoS condition, lockout of critical accounts, or crashing of critical servers and applications.

Types of risks arising from penetration testing:

Technical Risks:

- This type of risks directly arises with targets in the production environment.
- Examples:
  - Failure of the target
  - Disruption of service
  - Loss or exposure of sensitive data

Organizational Risks:

- This type of risks can occur as a side effect of penetration testing.
- Examples:
  - Repetitive and unwanted triggering in the incident handling processes of the organization
  - Negligence towards monitoring and responding incidents during or after the pen test
  - Disruption in business continuity
  - Loss of reputation

Legal Risks:

- This type of risks arises from legal obligations.
- Examples:
  - Violation of laws and clauses in the rules of engagement (ROE)