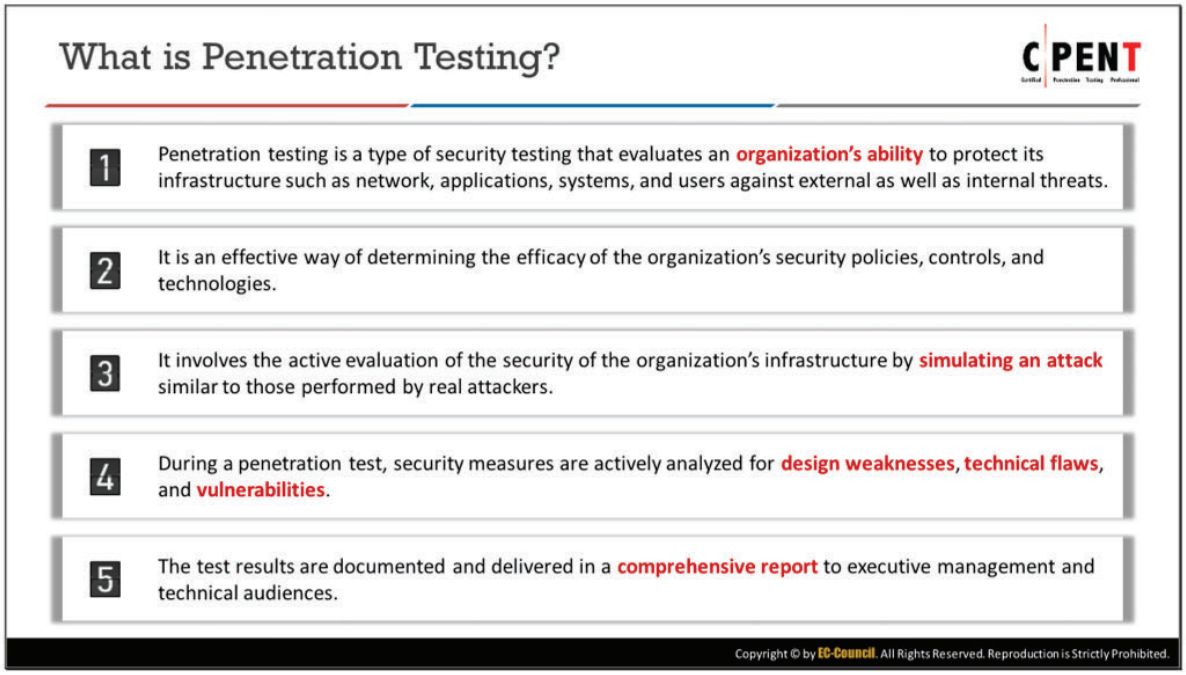


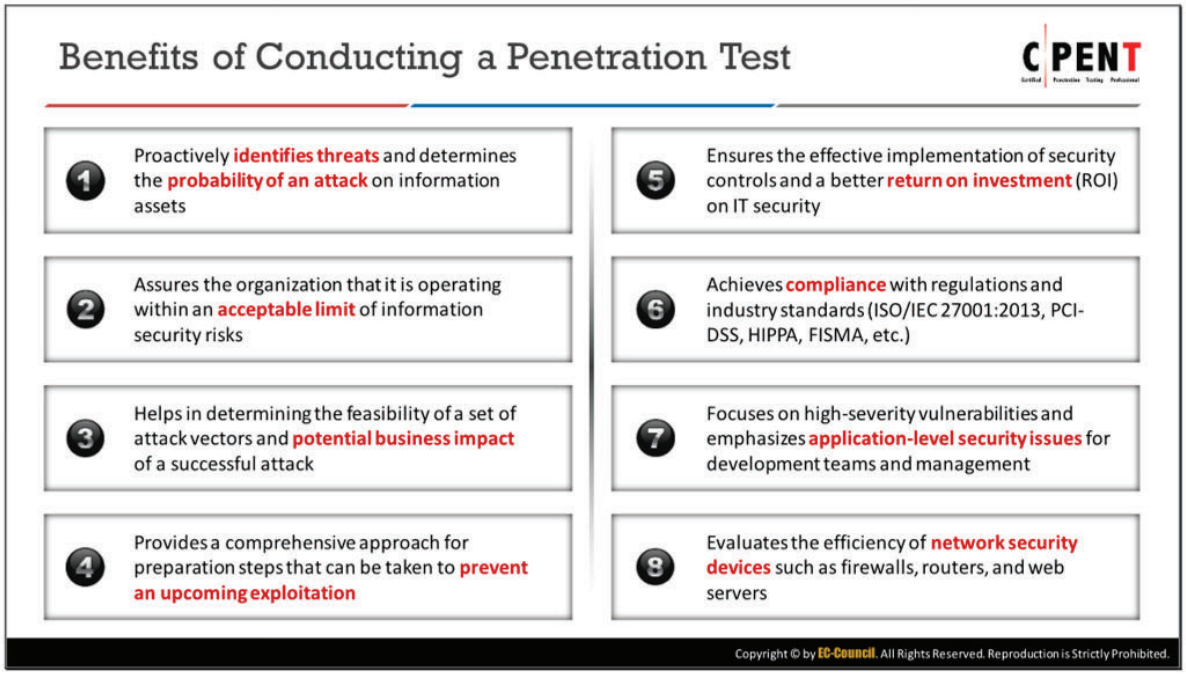
What is Penetration Testing?

Penetration testing, also called pen testing, goes a step ahead of vulnerability scanning in security assessment. Unlike vulnerability scanning, which examines the security of individual computers, network devices, or applications, penetration testing assesses the security model of the network as a whole. Penetration testing can reveal the potential consequences of a real attacker breaking into the accounts of network-to-network administrators, IT managers, and executives. It also sheds light on the security weaknesses missed in typical vulnerability scanning.

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 from 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 attackers. 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.

A penetration test not only documents vulnerabilities but also points out how they can be exploited. It shows how an attacker can exploit several minor vulnerabilities to compromise a computer or network. Penetration testing exposes the gaps in the security model and helps organizations strike a balance between technical prowess and business functionality from the perspective of potential security breaches, which helps in disaster recovery and business continuity planning.

Most vulnerability assessments are conducted solely based on software and do not assess technology-related security. Furthermore, people and processes are as likely as technology and software to be a source of security vulnerabilities. Using social engineering techniques,



Benefits of Conducting a Penetration Test

The following are some of the benefits of conducting a penetration test:

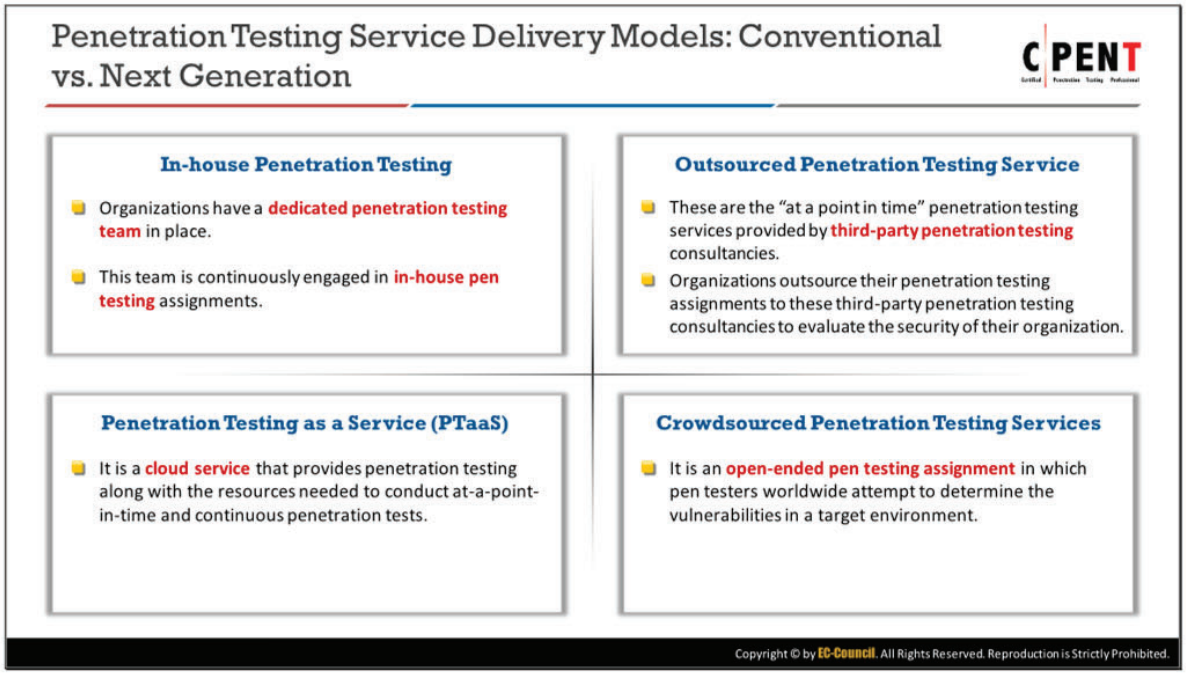
- **Reveal vulnerabilities**: In addition to revealing existing weaknesses in a system or application configurations, a penetration test investigates the action and behavior of an organization's staff that could lead to a data breach. Finally, the tester provides a report containing updates on security vulnerabilities as well as recommendations and policies to improve the overall security.
- **Show real risks**: The tester exploits the identified vulnerabilities to check how a real attacker could behave.
- **Ensure business continuity**: A small interruption can have a great impact on a business. It can cost the company tens to thousands of dollars. Therefore, the availability of the network, access to the resources, and 24/7 communications are necessary to run the business operation. A penetration test discloses potential threats and recommends solutions to ensure that the business operation will not be affected by an unexpected downtime or a loss of accessibility.
- **Reducing client-end attacks**: An attacker can break into an organization's systems from the client side, especially via web and online form services. Companies should be prepared to protect their systems from such attacks. If an organization knows which kind of attacks can be expected, then they know the signs to look out for and must be able to update the application.
- **Establishing the status of the company in terms of security**: Penetration testing provides knowledge of the security level of a company and its status in terms of security. The tester provides a report on the company's overall security system and areas needing

improvements, and the report includes details on the protection of the protection of its infrastructure and effectiveness of existing security measures.

- **Guard the reputation of the company**: It is important for a company to maintain a good reputation with its partners and clients. Gaining the trust and support of even loyal partners is difficult if the company is affected by a data breach or attack. Organizations should regularly perform penetration tests to protect their data and the trust of their partners and clients.

A few additional benefits of conducting a penetration test are as follows:

- Proactively identifies threats and determines the probability of an attack on information assets (IA)
- Assures the organization that it is operating within an acceptable limit of information security risks
- Helps in determining the feasibility of a set of attack vectors and potential business impact of a successful attack
- Provides a comprehensive approach for preparation steps that can be taken to prevent an upcoming exploitation
- Ensures the effective implementation of security controls and a better return on investment (ROI) on IT security
- Achieves compliance with regulations and industry standards (ISO/IEC 27001:2013, PCI-DSS, HIPPA, FISMA, etc.)
- Focuses on high-severity vulnerabilities and emphasizes application-level security issues for development teams and management
- Evaluates the efficiency of network security devices such as firewalls, routers, and web servers



Penetration Testing Service Delivery Models: Conventional vs. Next Generation

An organization can perform penetration testing in-house by hiring a dedicated team of testers or can take help from vendors providing advanced penetration testing services. The following are the penetration testing service delivery models adopted by various organizations.

- **In-house penetration testing service:** In this penetration testing service model, organizations have a dedicated penetration testing team in place, which is continuously engaged in in-house pen testing assignments.

  This model has a shorter response time and can be easily integrated with the application modification system within the organization. An internal testing team is well versed with the organization's environment and can perform better than external penetration testing teams in this respect.

- **Outsourced penetration testing service:** These are "at a point in time" penetration testing services provided by third-party penetration testing consultancies. Organizations outsource their penetration testing assignments to these third-party firms to evaluate their security.

  The organization should have complete trust in the third-party vendor (consultancy). Outsourced penetration testing requires the sharing of a wide range of organizational information to a third-party consultancy and can cause a security breach due to negligence. Therefore, the third-party consultancy must be selected after ensuring that it has good customer service and a good reputation.

- **Penetration testing as a service (PTaaS):** It is a cloud service that provides penetration testing along with the resources needed to conduct at-a-point-in-time and continuous

penetration tests. Using PtaaS, an organization performs continuous testing and remediation.

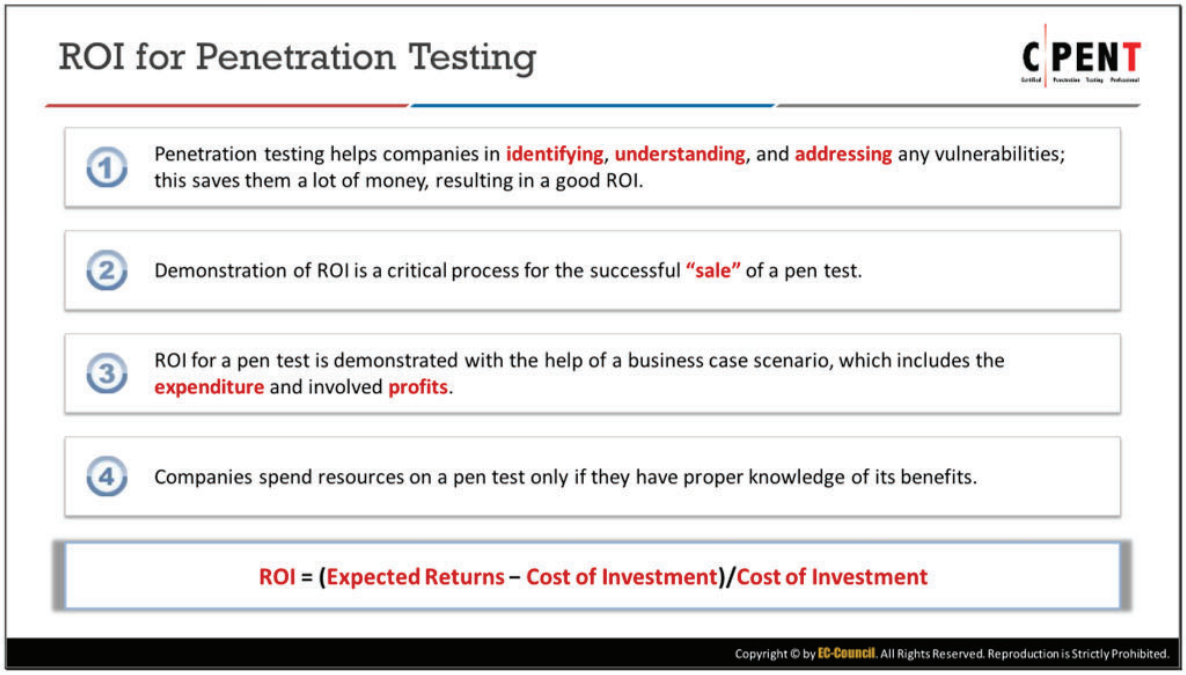
PTaaS has the following benefits:

- PTaaS provides continuous security management of the organization's infrastructure with yearly subscriptions.
- PTaaS providers enable organizations to run live scans on their assets and provide periodic (daily, weekly, bi-weekly, monthly, and/or quarterly) vulnerability scanning reports.
- PTaaS providers have highly qualified security experts to resolve unlimited customer queries.
- The adoption of PTaaS reduces administrative overhead.
- A PTaaS provider keeps the organization updated with the latest security tools and practices.

- **Crowdsourced penetration testing service:** It is an open-ended pen testing assignment in which pen testers worldwide attempt to determine the vulnerabilities in a target environment.

  A crowdsourced penetration testing service is a global community consisting of white hat hackers who work together for cyber security. This penetration service delivery model provides diverse skills for finding hidden vulnerabilities. Since numerous penetration testers are involved in crowdsourced penetration testing, it requires less time than in-house or outsourced penetration testing teams for discovering critical vulnerabilities.

  Crowdsourced penetration testers focus on organizations that promise them high monetary gains. They are paid based on the activity period or number of vulnerabilities found. Therefore, companies with a small testing budget cannot expect skilled crowdsourced penetration testers to work for them.



ROI for Penetration Testing

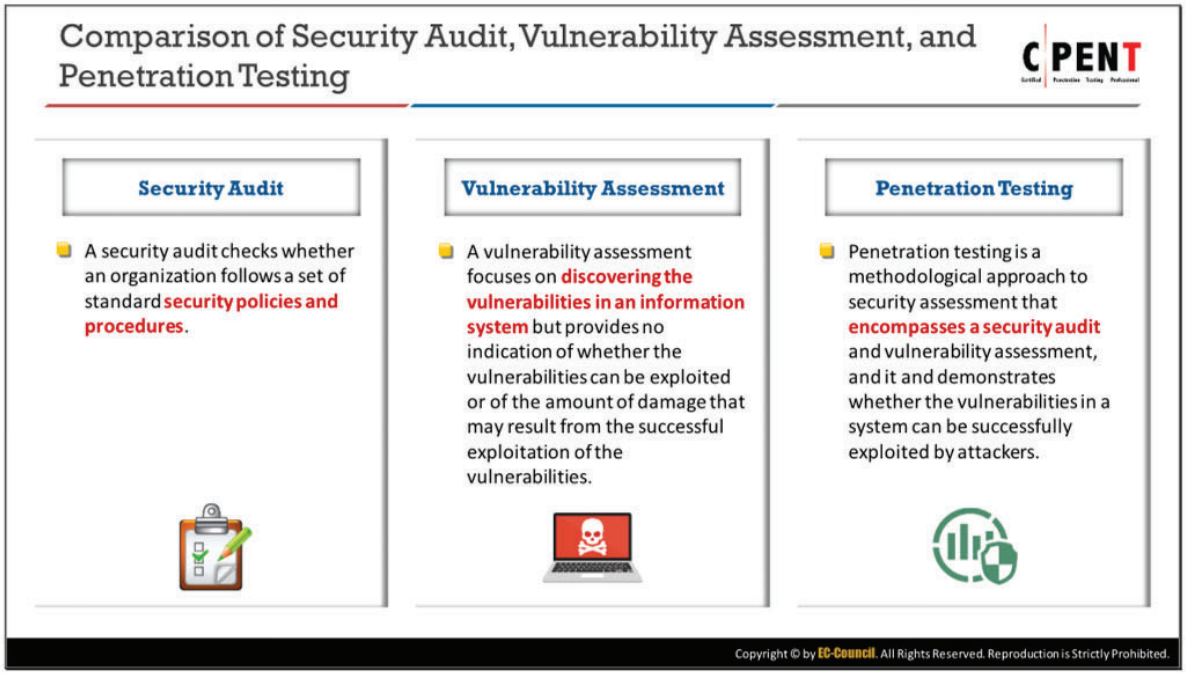
Penetration testing helps companies in identifying, understanding, and addressing any vulnerabilities, which saves a lot of money and, in turn, yields a good ROI. The purpose of penetration testing is to discover and expose vulnerabilities in an organization's security system while considering the company's IA and how those assets are related to the business value of the organization. Through a penetration test, the company acquires knowledge of possible risks, vulnerabilities, or threats to IA, as well as the information required to mitigate those risks.

Companies spend resources on penetration testing only if they have proper knowledge of its benefits. Therefore, the demonstration of ROI is a critical process for the successful "sale" of a penetration test. The ROI for penetration testing is demonstrated with the help of a business case scenario, which includes the expenditure and profits involved. Because ROI is a conventional financial measure based on historical data, it is a retrospective metric that yields no insights into how to improve business results in the future.

In practice, most organizations use one or more "financial metrics" and refer to them individually or collectively as "ROI." These metrics include the following:

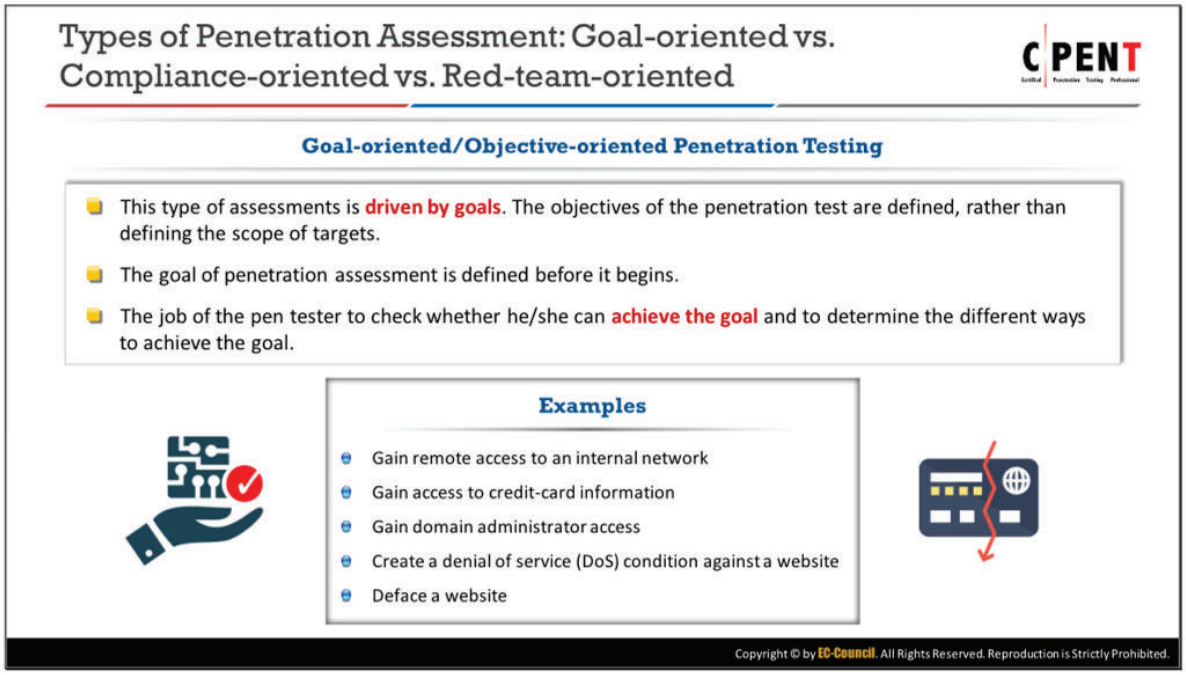
- **Payback period:** Time required for the return on an investment to "repay" the sum of the original investment
- **Net present value**: Present value of future cash flows minus the purchase price
- **Internal rate of return**: Benefits repeated as an interest rate
- **ROI**: Ratio of the net gain from a planned project divided by its total costs, i.e.,

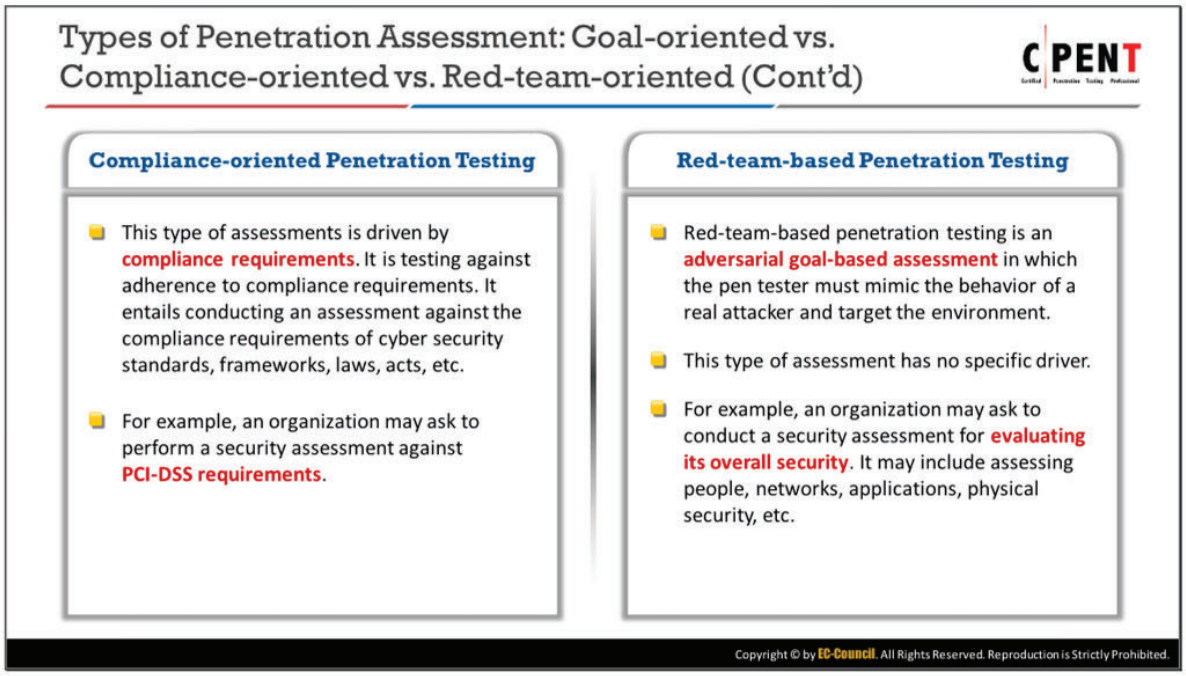
  ROI = (Expected Returns – Cost of Investment)/Cost of Investment



Comparison of Security Audit, Vulnerability Assessment, and Penetration Testing

- **Security audit**: A security audit is used to evaluate whether the security of a company's information fulfills a set of established criteria and to ensure that the company is in compliance with its regulations, security policy, and legal responsibilities. Different types of audits are used to evaluate a company's security processes. A security audit only checks whether the organization follows a set of standard security policies and procedures.
- **Vulnerability assessment**: It is used for identifying and measuring the severity of vulnerability in a system; usually, it is used to identify common vulnerabilities in a system's configuration. Vulnerability assessment provides to organizations a list of vulnerabilities that need to be fixed, without estimating specific goals or scenarios. The list is provided according to the severity level of the vulnerability or business criticality. Vulnerability assessment is suitable for an organization that is not secure, wishes to get started, has a medium-to-high security maturity, and wishes to maintain the security posture of its network. Although vulnerability assessment focuses on discovering the vulnerabilities in an information system, it 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**: A penetration test is a goal-oriented exercise; it focuses on real-time attacks instead of discovering a specific vulnerability. The penetration tester acts as a hacker and follows all the steps a real hacker would to breach a system. This type of testing is suitable for organizations at a high maturity level of security. Penetration testing is a methodological approach to security assessment that encompasses a security audit and vulnerability assessment, and it demonstrates whether the vulnerabilities in the





Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented

Penetration assessment can be performed using the following approaches.

- **Goal-oriented/objective-oriented penetration testing approach**: Goals are the drivers for this penetration testing approach. In this type of assessment, a pen tester tasked with identifying or demonstrating a risk attempts to achieve a goal, rather than find

vulnerabilities. They focus on finding different ways to achieve the goal. In goal-oriented penetration assessment, the goal is defined before the start of pen testing. To achieve the set goals (objective), the pen tester performs multiple serial or parallel processes. Some common goals in goal-oriented/objective-oriented penetration testing are as follows:

- 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

- **Compliance-oriented penetration testing approach**: Compliance requirements are the drivers for this approach. It entails testing against adherence to compliance requirements. It involves conducting assessments against the compliance requirements of cyber-security standards, frameworks, laws, acts, etc. For example, an organization may ask to perform a security assessment against compliance standards such as PCI-DSS, ISO-27001, FISMA, HIPAA, and HITRUST. Compliance-oriented penetration testing also reviews firewall rules for compliance.

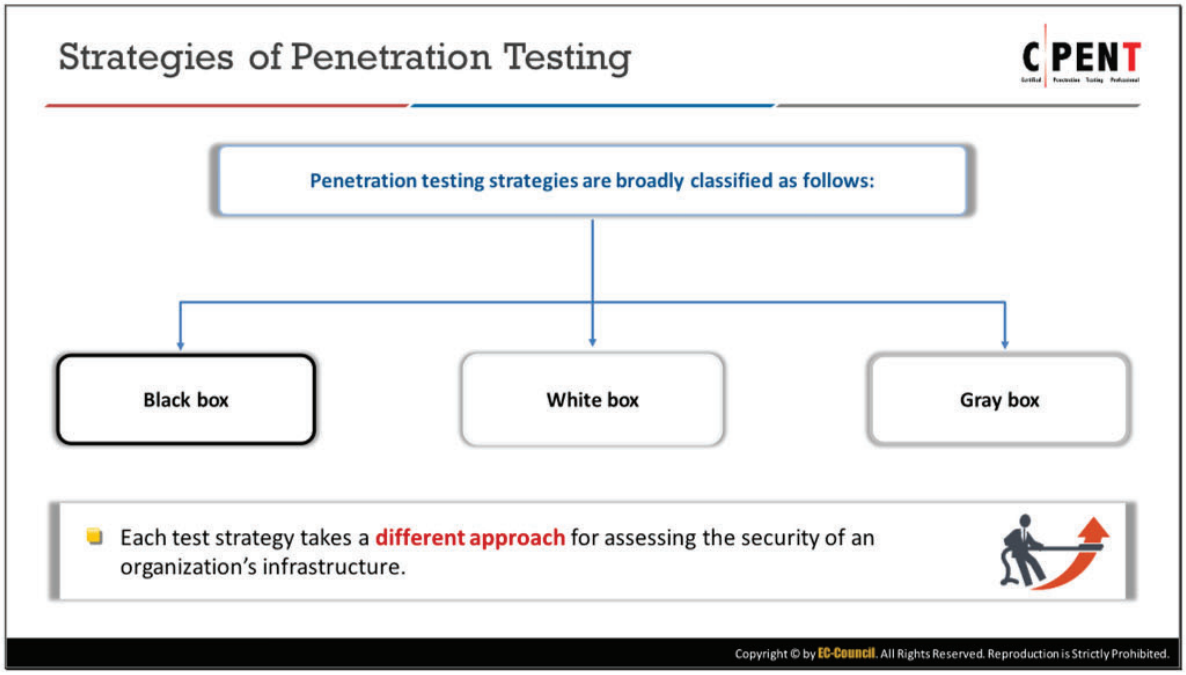
  The compliance-oriented penetration testing approach is a proactive approach to secure and maintain compliance. This enables organizations to do the following:

  - Maintain the security posture of the organization by identifying and preventing attacks before they occur
  - Enhance the security infrastructure or policy framework
  - Evaluate an organization's compliance level in specific areas such as patch management, password policy, and configuration management
  - Protect client data from breaches, which could result in a heavy penalty
  - Verify the system's security with respect to certification and accreditation (C&A) activities

- **Red-team-oriented penetration testing approach**: This approach is an adversarial goal-based assessment in which the pen tester must mimic a real attacker and target an environment. This approach has no specific driver. For example, an organization may ask to conduct a security assessment for evaluating its overall security. It may include the assessment of people, networks, applications, physical security, etc. Furthermore, it is an offensive type of security testing in which a red team works with a blue team and updates the blue team with the tactics, techniques, and procedures (TTPs) used by the read team.

  It enables organizations to do the following:

  - Understand their ability to detect and respond to real-world attacks
  - Assess their organizational security with respect to specific targets



Strategies of Penetration Testing

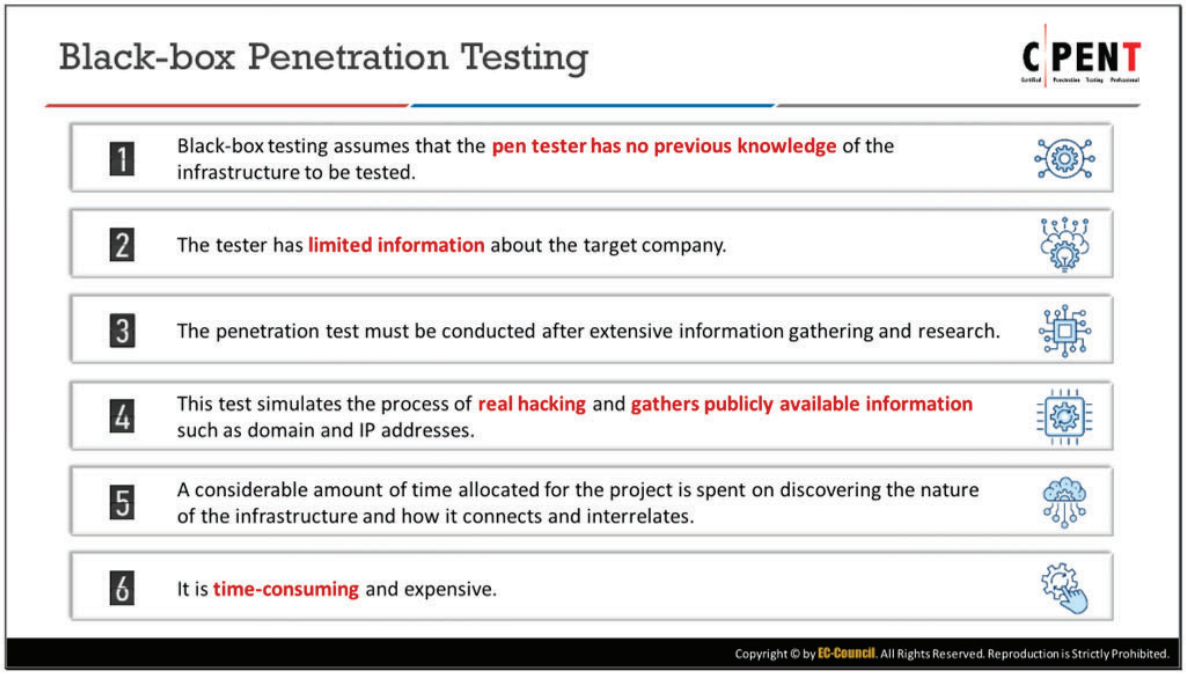
The three types of penetration testing are black-, white-, and gray-box testing. Each test type takes a different approach for assessing the security of an organization's infrastructure.

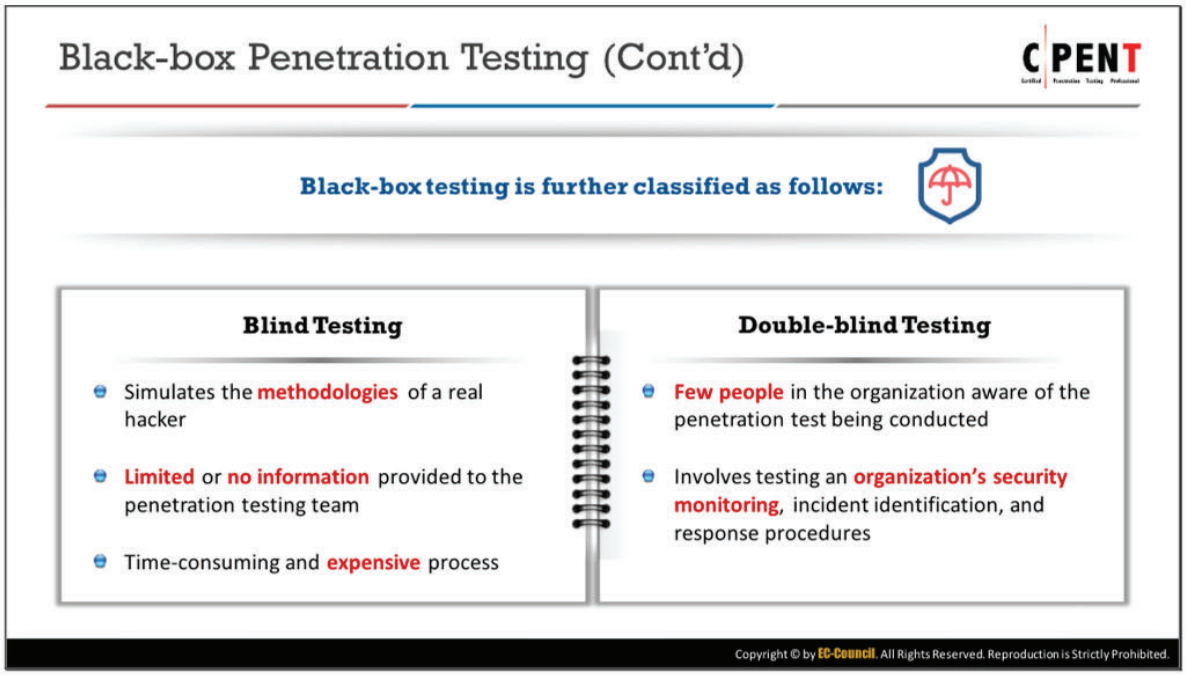
- **Black-box testing**

  To simulate real-world attacks and minimize false positives, penetration testers can choose to undertake black-box testing (or zero-knowledge attack, with no information or assistance from the client) and map the network while enumerating services, shared file systems, and operating systems (OSes) discreetly. Additionally, the penetration tester can undertake war dialing to detect listening modems and war driving to discover vulnerable access points, provided it is legal and within the project scope.

- **White-box testing**

  If the organization needs to assess its security against a specific kind of attack or a specific target, complete information about the same may be given to pen testers. The information provided can include network topology documents, asset inventory, and valuation information. An organization typically opts for white-box testing when it requires a complete audit of its security. It is critical to note that despite all of this, information security is an ongoing process, and penetration testing only provides a snapshot of the security posture of an organization at any given point in time. White-box testing can be performed with and without the knowledge of the IT staff. When a test is conducted without the involvement of the organization's IT staff, only the top management is informed of it.





Black-box Penetration Testing

Black-box testing is one of the ways in which penetration testing can be performed. The following are some of the features of black-box pen testing:

- Black-box testing assumes that the pen tester has no previous knowledge of the infrastructure to be tested.
- The tester only knows the company name.

- The penetration test must be conducted after extensive information gathering and research.
- This test simulates the process of real hacking and gathers publicly available information such as domain and Internet Protocol (IP) addresses.
- A considerable amount of time allocated for the project is spent on discovering the nature of the infrastructure and how it connects and interrelates.
- It is time-consuming and expensive.

Black-box testing is further classified into blind and double-blind testing.

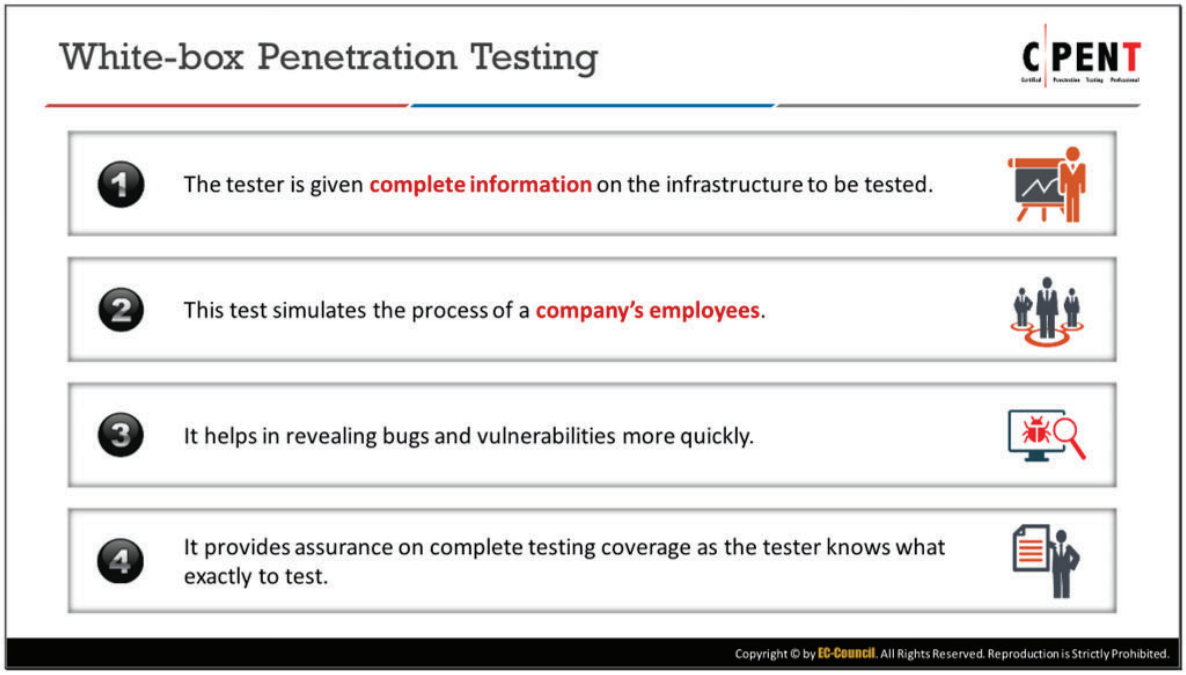
- **Blind testing**

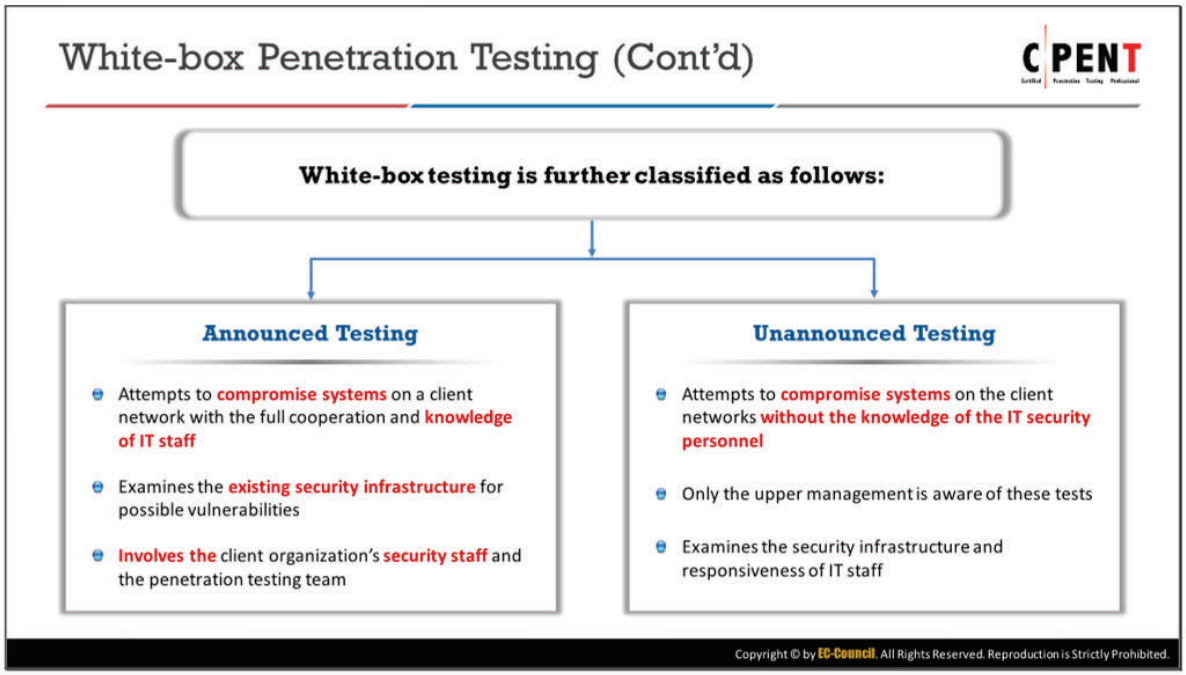
  A blind-testing process focuses on and simulates the methodologies of a real attacker. It is a time-consuming and expensive process. The penetration test team is provided with limited or no knowledge of the organization before conducting the test. To conduct the test, the penetration testing team gathers publicly available information on the target from the following sources:

  - Websites
  - Domain name registries
  - Online discussion boards
  - Usenet

- **Double-blind testing**

  A double-blind test is a step beyond blind testing. Here, the IT and security staff of the organization are not informed of the planned testing activities. It is an important component of testing. This strategy tests the organization's security monitoring issues, incident identification, and response procedures. In double-blind testing, few people in the organization are aware of the test conducted. The individual responsible is the project manager, who observes the whole procedure of penetration testing.





White-box Penetration Testing

White-box testing is also known as structural testing. In this type of testing, the tester is provided with various information of the organization before the start of the test. This test simulates the process of the company's employees and provides assurance on complete testing coverage as the tester knows what exactly to test. This helps in revealing bugs and vulnerabilities more quickly.

The following are some of the information that could be provided through this type of test:

- **Company infrastructure**

  This includes information related to the different departments of the organization. Information related to hardware, software, and controls is also revealed to the penetration tester.

- **Network type**

  The network-type information can be related to the local area network (LAN) of the organization and the topology used to connect the systems. It can also be related to access to remote networks or the Internet.

- **Current security implementations**

  Current security implementations are the various security measures adopted by the organization to safeguard vital information from any kind of damage or theft.

- **IP address/firewall/IDS details**

  This information includes details of the organization's IPs and firewalls used to protect data from unauthorized access. The firewall and intrusion detection system (IDS) policies are made available to the penetration tester.

- **Company policies: do's and don'ts**

  The various policies adopted by the organization to conduct business are made available depending on the nature of the test. These policies could be related to the security policies, legal policies, labor policies, and so on.

White-box testing is further classified as follows:

- **Announced testing**

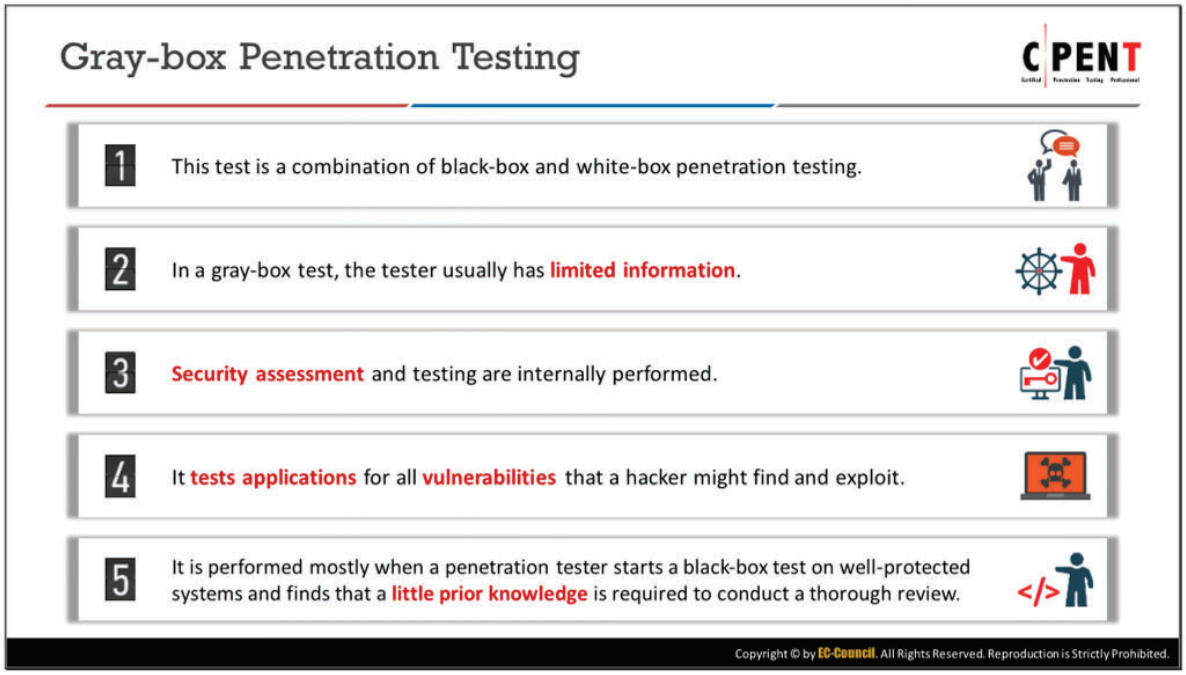
  Announced testing is an attempt to compromise the client's network systems with the knowledge and cooperation of the IT staff. This type of testing examines the existing security infrastructure for possible vulnerabilities. The security staff usually joins the penetration testing team to conduct these audits. This type of penetration testing is effective for the physical security of the penetration test.

  Announced penetration testing may help a penetration tester in the following ways:

  - A penetration tester can acquire a complete overview of the infrastructure of the organization.
  - A penetration tester may be able to know the kind of physical access provided to different employees in the organization.
  - A penetration tester may acquire a clear picture of measures applied for the information and system security of the organization.

- **Unannounced testing**

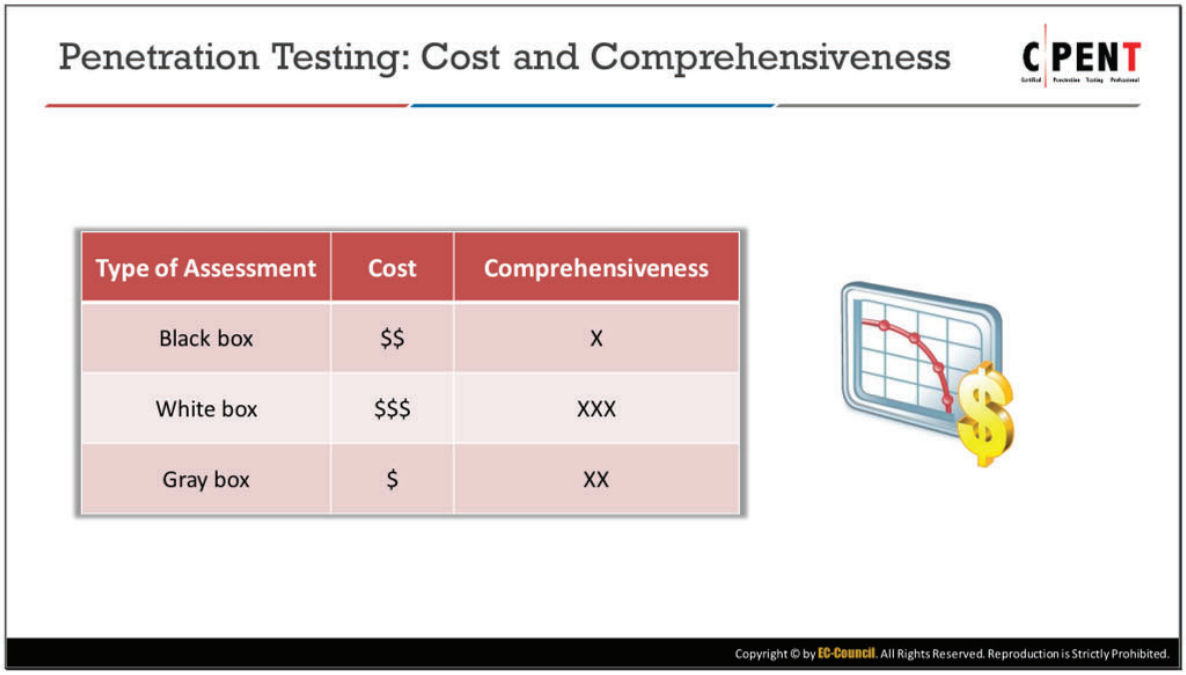
  Unannounced testing is an attempt to compromise systems on the client's networks without the knowledge of IT security personnel. Unannounced penetration testing is



Gray-box Penetration Testing

In gray-box penetration testing, security assessment and testing are internally performed; the process of testing examines the scope of access by insiders within the organization's network. It is the most common approach toward application security that tests the vulnerabilities an attacker can exploit. This testing process functions in a manner similar to black-box testing. Both the attacking team and normal application users are provided the same privileges, and the purpose is to simulate an attack by a malicious insider.

This type of testing is a combination of black-box and white-box penetration testing. In a gray-box test, the tester usually has limited information. The tester performs security assessment and testing internally and tests applications for all vulnerabilities that a hacker might find and exploit. It is performed primarily 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.



Penetration Testing: Cost and Comprehensiveness

- **Black-box assessment**

  In this type of assessment, no background information is given to the testing analyst. They need to spend a large amount of time in researching the environment and organization.

- **White-box assessment**

  In this type of assessment, the analyst is given all the information required to penetrate the organization's environment. Consequently, the analyst spends more time on testing and exploitation than on acquiring information. Based on the type of test performed, the information includes data flow charts, network diagrams, the source code of applications, server descriptions and configurations, and credentials to access all login panels.

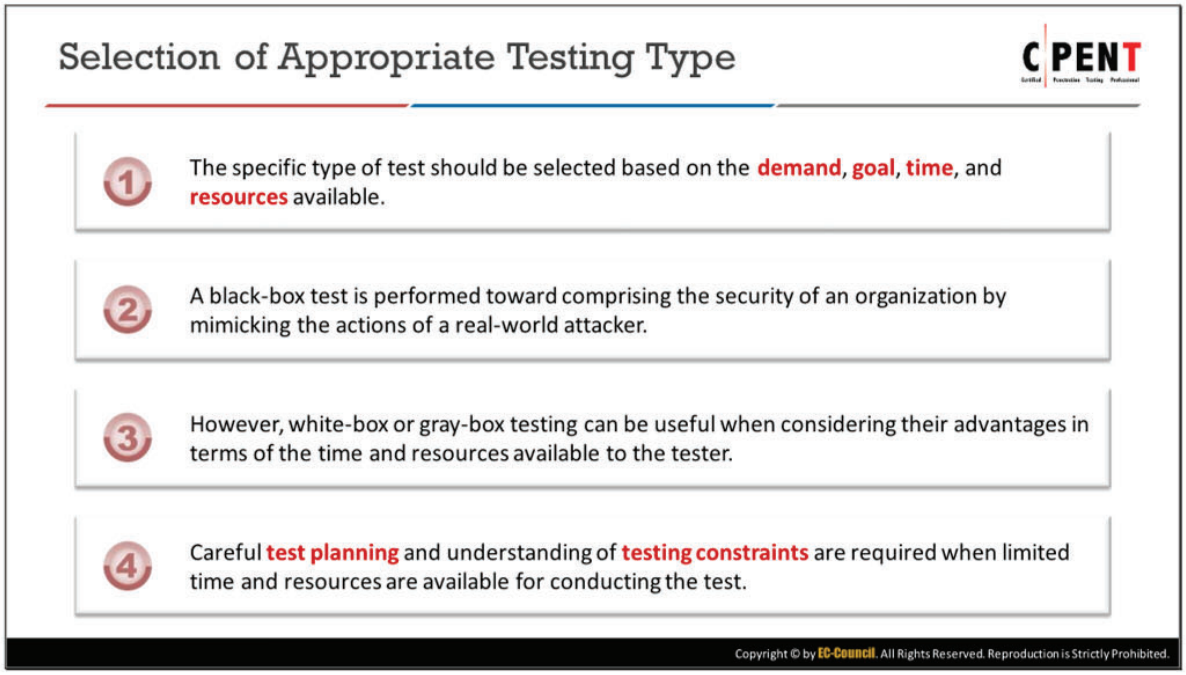
- **Gray-box assessment**

  In this type of assessment, some information is given to the analyst to assist in their research. It is the most cost-effective type. The analyst obtains most of the same results as they would in white-box assessment.

The following are some of the factors that affect the cost of a penetration test:

- **Complexity**

  The most important factor is the company's infrastructure; the cost depends on the size of the environment and number of network devices involved. More complex environments need more work for the tester to find every possible vulnerability.

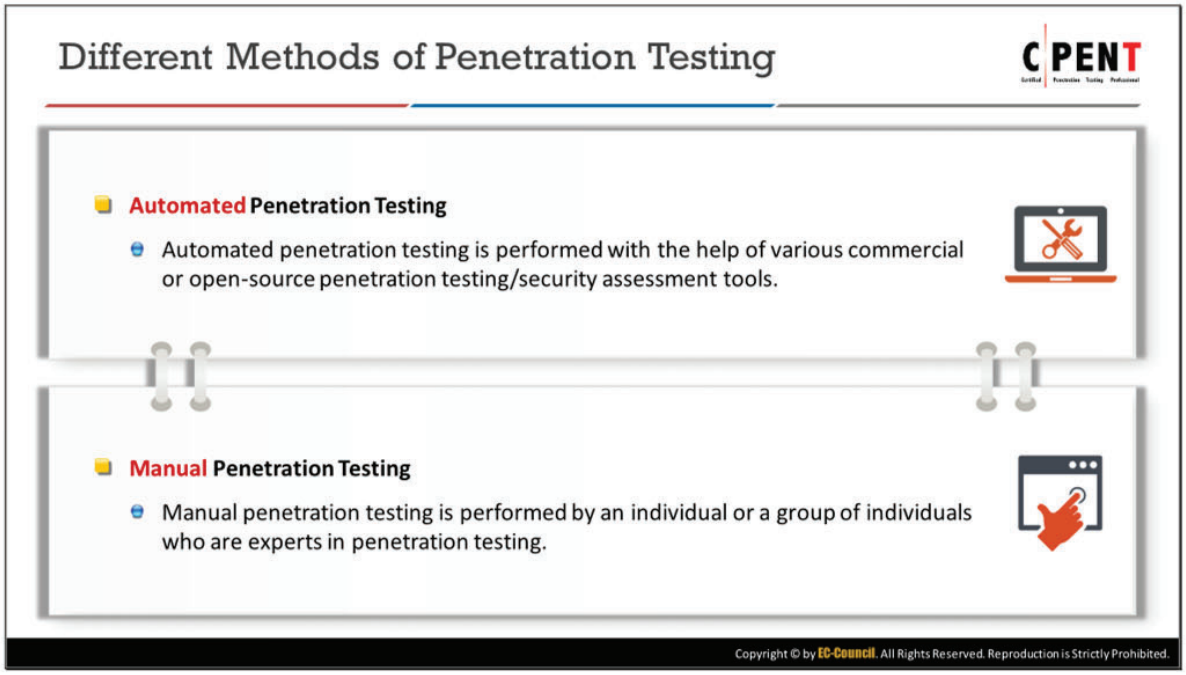


Selection of Appropriate Testing Type

Usually, the type of test is selected based on the organization's requirement, demand, scope, goal, time, resources available, and budget. If penetration testing is compulsory and performed regularly, then the company may be tempted to find the lowest-cost automated pen testing service. However, the company may have already allocated the funds to perform a penetration test. Therefore, it is important to select the appropriate test to obtain good results. If not, the company may incur losses in terms of not only spending but also the time and resources spent on the pen test.

Not every test can be performed for every organization; therefore, the type of test depends on the organization's infrastructure, network, and devices involved. Occasionally, the type of test depends on the organization's budget. Further, it depends on how the organization wishes to conduct the test; if it wishes to focus more on a specific application or network where a chance of exploit exists or if it is more worried about real-world attacks or risks, then a more skilled tester is required to perform a thorough test. Thus, it is advisable to choose the optimal type of test for penetration testing.

A black-box test is performed toward comprising the security of an organization by mimicking the actions of a real-world attacker. However, white-box or gray-box testing can be useful when considering their advantages in terms of the time and resources available to the tester. Careful test planning and understanding of testing constraints are required when limited time and resources are available for conducting the test.



Different Methods of Penetration Testing

The following are different methods of penetration testing:

- **Automated penetration testing**

  A person with minimal knowledge of testing can run an automated penetration test. This technology is remarkably simple, fast, efficient, and reliable, and it tests vulnerabilities and risks automatically. Automated penetration testing is performed with the help of various commercial or open-source penetration testing/security assessment tools. Some tools used for automated penetration testing are Metasploit, OpenID, Nessus, and backtrack.

- **Manual penetration testing**

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

  The following are the different types and steps of manual pen testing.

  - **Types of manual penetration testing**

    - **Focused**

      This type is used to test only specific vulnerabilities and risks. The test is performed only by human experts who examine specific applications within the given domain.

    - **Comprehensive**

      In this type, all systems that are connected to a shared network are tested to identify a wide range of risks and vulnerabilities.

- **Steps involved in manual penetration testing**
  - **Data collection**

    Data can be collected either manually or by using tools freely available online. Information that can be gathered with the help of tools include database versions, software, table names, hardware, and third-party plugins.
  - **Vulnerability assessment**

    After gathering the information, the tester identifies weakness and accordingly takes preventive steps.
  - **Actual exploit**

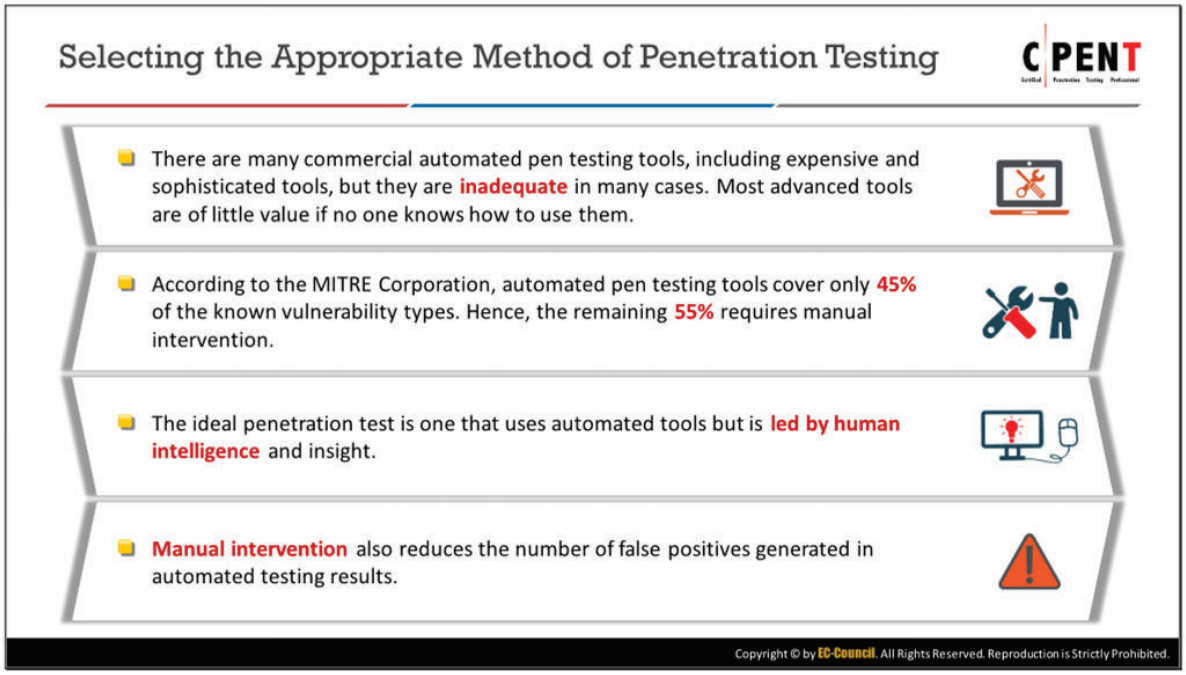
    Now, the tester launches an attack on the target system. This is a very difficult step that requires an expert tester to execute.
  - **Report preparation**

    Finally, the tester prepares a final report that describes the overall pros and cons of the system. The report is analyzed to take corrective steps to secure the target system.

The table summarizes the differences between manual and automated penetration testing.

Manual penetration testing	Automated penetration testing
An expert engineer is required to perform the test.	Because it is automated, a person with minimal knowledge of testing can perform it.
The results may vary between tests.	The results are fixed.
It is very time-consuming and exhaustive.	It is fast and efficient.
The tester can think like a hacker, focus on areas they can attack, analyze the situation accordingly, and recommend appropriate security measures.	It cannot analyze the situation.
Multiple tests can be run as per the requirement.	Multiple automated tests cannot be run.
The test is especially useful in critical conditions.	It cannot be used in critical conditions.
The tester must remember to clear the memory.	The memory is automatically cleared.

Table 1.2: Differences between manual and automated penetration testing



Selecting the Appropriate Method of Penetration Testing

Selecting the appropriate penetration testing technique is another important aspect to consider before performing the test. By using an automated pen test tool, only some standard vulnerabilities that are present in an application can be identified. Scanning tools are used to check the presence of any malicious code that can lead to a potential security breach and encryption tools that can examine the system and determine hard-coded values such as usernames and passwords.

Numerous commercial automated pen testing tools are available, 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.

A commercial pen testing tool must satisfy the following criteria to merit selection:

- Easy to deploy, configure, and use
- Easily scans the entire system
- Categorizes vulnerabilities based on severity level and need for an immediate fix
- Reverifies previously found vulnerabilities or exploits
- Generates detailed vulnerability reports and logs
- Automates verification of vulnerabilities

It is sometimes difficult to find all vulnerabilities using automated tools. Vulnerability to social engineering is one such type that can only be tested manually. 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

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

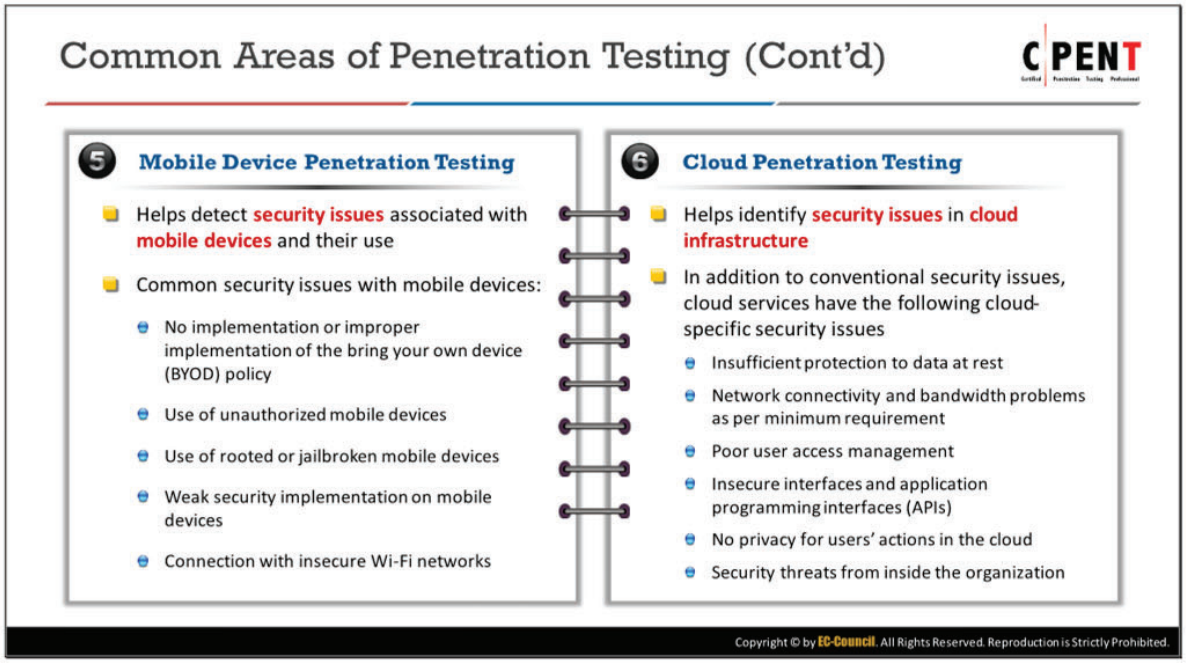
Common Areas of Penetration Testing (Cont'd)

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

Some of the common areas of penetration testing include networks, web applications, wireless networks, mobile devices, and cloud computing. Social engineering is another common area of penetration testing.

- **Network Penetration Testing**

  In this test, a network professional imitates the process a hacker would use to launch an attack on network devices, applications, or a business website. The main purpose of imitation is to identify security loopholes before a hacker locates them and performs an exploit. The pen testing is performed without any malicious intent; this is the reason why network professionals should take prior authorization or permission from the organization management before conducting a pen test on the network.

  Network penetration testing helps the organization identify security issues in the network design and implementation. It must be planned correctly; otherwise, the result may be disruptive and can lead to business losses.

  Common network security issues include the following:

  - Use of insecure protocols
  - Unused open ports and services
  - Unpatched OS and software
  - Misconfiguration in firewalls, IDS, servers, workstations, network services, and so on.

  Network penetration testing works in the following manner.

Network penetration test involves various steps and plays a crucial role in the planning phase. During the planning phase, the network professional gathers and reviews network specifications, user documentation, network usage, and other relevant documentation. Based on the information gathered, the tester designs a series of test cases for penetration testing.

- **Network interfaces**

  In this case, the tester gathers information from the network interfaces, user interfaces, and application programming interfaces (APIs) present between the software and external environment. If this is not designed correctly, it creates a loophole for the hacker to breach the network. Therefore, it is a good place to start the test of a network interface.

- **Errors and user alerts**

  User errors are quite common; these errors are usually communicated via a software application to an external user. It is important to note all the dialogs associated with user alerts and error messages. If an external user has an intention to hack, then it is important to identify what information is revealed to the external user and how.

- **Disaster scenario identification**

  Network professionals come across various disaster scenarios during the planning phase. These scenarios could provide a good idea of how a network attack would occur and guide the professionals to the actual penetration testing process. The network environment consists of files, applications and system resources, data, and internal logic in the system; the actual security issues usually lie within user input. If any information varies during a penetration test, security issues are confirmed. Based on this, an appropriate measure can be taken to fix the problem.

- **Web Application Penetration Testing**

  Web application penetration testing helps in detecting security issues in web applications due to insecure design and development practices. It uses either manual or automated pen testing to identify security flaws, vulnerabilities, or threats in a web application.

  Common web-application security issues include the following:

  - Injection vulnerabilities
  - Broken authentication and authorization
  - Broken session management
  - Weak cryptography
  - Improper error handling

- **Social Engineering Penetration Testing**

  This type of testing is intended to test the employees' compliance with the security policies and practices predefined by the management. It helps in identifying employees

that do not properly authenticate, follow, validate, or handle the processes and technology. This type of testing provides information to the company regarding how easily an intruder can trick employees to break security rules, reveal confidential data, or provide access to sensitive data. The company must also understand the efficacy and shortcomings of the security training provided to its employees.

The following are some common employee behavioral issues that can cause 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

Following are some effective social engineering techniques:

- **Phishing**

  The tester simply sends an email that tricks users into clicking on something. The tester records that activity or installs a program. For a successful phishing campaign, the tester must remember to check grammar and spelling and try to make the mail appear genuine, believable, and short. The best tool for phishing attacks is the open-source Social-Engineer Toolkit (SET).

- **Pretexting**

  In this technique, the hacker calls the target person and asks for information while pretending to be an authentic user that needs assistance. By performing this technique, the penetration tester can target nontechnical users who may disclose sensitive data.

- **Media dropping**

  This technique involves the dropping of a USB flash drive near a parking lot or entrance area where people can easily see it. This drive contains some interesting music or movie files that the victim can easily download; when it is opened, however, it launches a client-side attack. To implement such a technique in penetration testing, the tester must develop custom attacks and programs in a USB drive or purchase USB drives that are prebuilt for this purpose.

- **Tailgating**

  In this technique, an unauthorized person can enter the company's premises by fooling the staff or simply walking in. To prove the success of this test, the tester must obtain sensitive data or install a device quickly; they can even take photographs of exposed files or documents left on desks or printers.

- **Wireless Network Penetration Testing**

  Hackers mostly consider a wireless network an ideal entry point to an organization's systems. It is very difficult to monitor, control, and protect information from unauthorized penetration. Thus, most businesses, organizations, government offices, and institutions opt for the services of a third-party wireless network security expert to help them identify misconfigurations in wireless network infrastructure.

  The following are usually included in a wireless network penetration test:

  - Identification of hardware and software weaknesses
  - Testing of applications prone to attacks
  - Discovery of new bugs in updated software
  - Increase of general awareness regarding the importance of proper technical controls

  Common security issues in wireless network infrastructure include the following:

  - Unauthorized/rogue/open access points
  - Insecure wireless encryption standards
  - Weak encryption passphrases
  - Unsupported wireless technology

- **Mobile Device Penetration Testing**

  The use of mobile devices and apps is increasing rapidly in every personal/private and business scenario. Accordingly, the need for mobile security is also increasing. In addition to personal and financial data, highly sensitive corporate data are saved on mobile devices, which are exposed to mobile developers via APIs. Most users and organizations are unaware of mobile-app security guidelines, and hackers easily exploit mobile vulnerabilities. Now, most organizations are concentrating on mobile security and on increasing regulatory studies.

  Mobile penetration testing is similar to conventional penetration testing in that it follows the concept of "think like a hacker," but it is different in many ways because modern mobile devices are significantly different from the familiar Intel platform. Further, mobile devices have growing levels of random access memory (RAM) and persistent storage, resulting in capabilities compared to those of conventional computing environments.

  Regardless of the differences between mobile and conventional platforms, a few familiar competencies from web-app security apply to mobile penetration testing; they range from risk analysis, threat modeling, bug tracking, and report preparation to the analysis and remediation of mobile device vulnerabilities. Mobile penetration testing helps in detecting security issues associated with mobile devices and their use.

  Common security issues with mobile devices include the following:

  - 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

- **Cloud Penetration Testing**

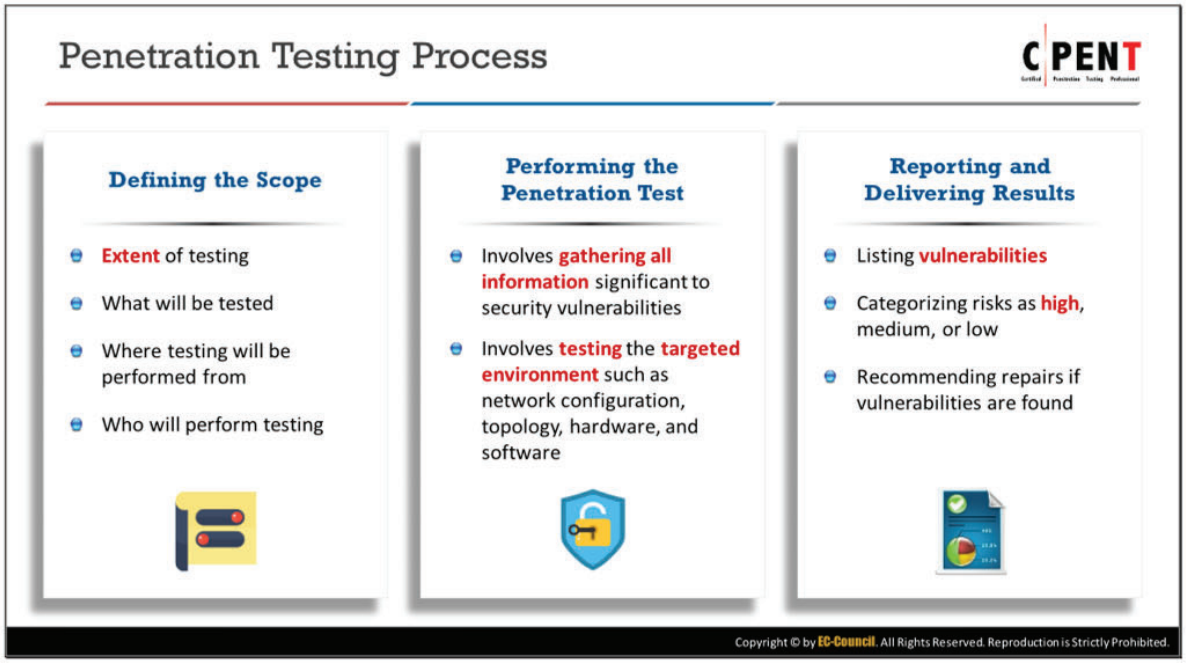
  Cloud computing is one of the fastest-growing technologies. Most organizations are moving their data to the cloud. Organizations can choose from different models of cloud computing: public, private, hybrid, and service models such as software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). The increasing demand for cloud computing can increase the chance of breaches, vulnerabilities, and threats. Enterprises face new challenges every day to protect their resources over the various cloud-computing models.

  To secure its data, an organization must perform vulnerability assessment and penetration tests of critical resource to determine the presence of vulnerabilities or the kind of risks they pose. However, such pen tests and scans are different from those executed on a network or application. First, it is necessary to identify which types of service allow pen testing on the organization's applications and infrastructure. PaaS and IaaS clouds permit user pen testing, whereas SaaS providers do not allow users to pen test their application. If pen testing is permitted, the following steps must be followed to perform a pen test:

  - The first step is to contact the cloud service provider (CSP), which can be done in two ways. The first is via the contractual text stating that pen testing is allowed, the kind of testing, and how often the test can be performed. Alternatively, if no such explicit text exists in a customer contract or as per the CSP's published policies, then testing can be negotiated, if possible.
  - After overcoming legal and contractual hurdles, the next step is to coordinate with the CSP for scheduling and performing the test.

  Another aspect must be considered while performing cloud pen tests: the types of tests that a customer is allowed to perform as per the CSP's policies. Because cloud resources are hosted on multitenant platforms, attacks on such a platform can cause an increase in bandwidth, resource consumption, and system memory, which can negatively affect other customers' resources. Therefore, most CSPs explicitly forbid any kind of DoS attacks or scans, which may affect local resource availability.

  Testers can use the "pivoting" technique, which exploits one system or application and then uses that system as a staging point for additional attacks against other systems or applications. This technique is usually allowed on resources hosted within a CSP environment.



Penetration Testing Process

The process for performing a penetration test in an organization consists of some critical decisions regarding the actions taken before testing the networking devices and system vulnerabilities.

The process is defined for all the operations performed during and prior to the penetration test, and it entails defining the scope, performing the penetration test, and reporting and delivering results.

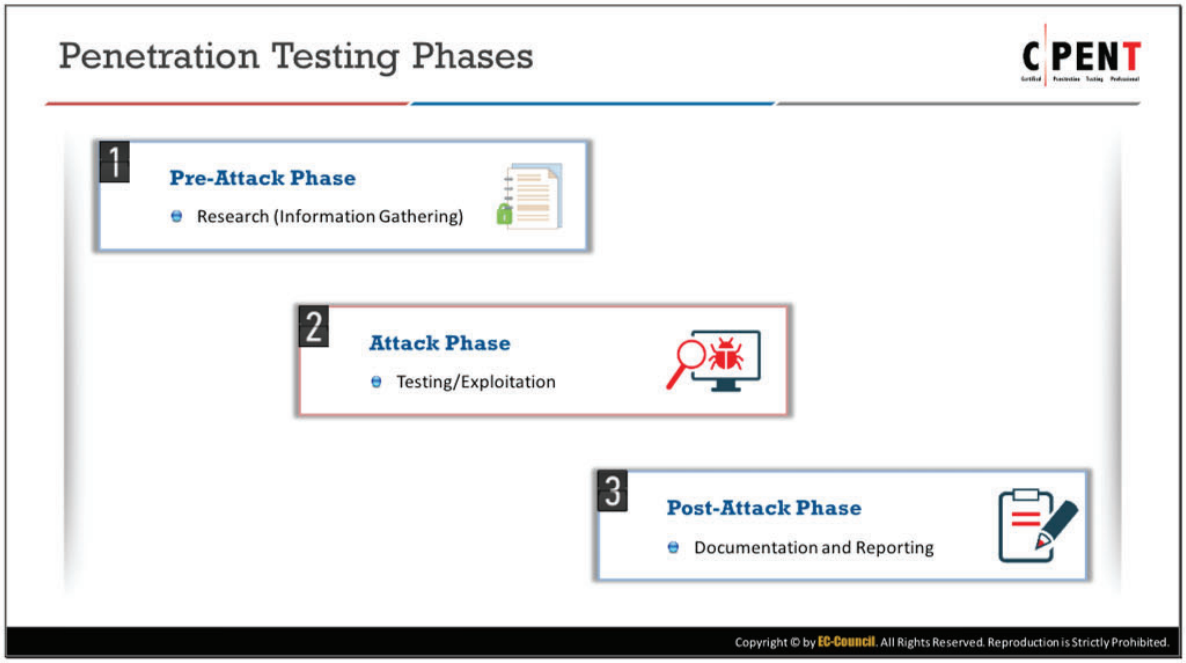
- **Defining the Scope**

  Before performing a penetration test, it is necessary to first define the range of testing. For different types of penetration testing, different types of network devices exist. The test can either be a full-scale test for the entire network and systems or for target devices such as web servers, routers, firewalls, Domain Name System (DNS) servers, mail severs, and File Transfer Protocol (FTP) servers. The scope of penetration testing covers the following:

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

- **Performing the Penetration Test**

  Each company ensures that the processes they implement for penetration testing are appropriate. Therefore, proper methodologies must be used for performing a good penetration test. The tester is responsible for checking the system for any existing or new



Penetration Testing Phases

There are three phases in penetration testing: the pre-attack, attack, and post-attack phases.

- **Pre-attack Phase**

  This phase focuses on gathering as much information as possible about the target. Information can be gathered invasively through, for example, passive and active reconnaissance, port scanning, service scanning, and OS scanning, or it can be gathered noninvasively by, for example, reviewing public records.

  Beginning with passive and active reconnaissance, the tester gathers as much information as possible about the target company. Most leaked information is related to the network topology and types of services running within. The tester can use this information to provisionally map out the network for planning a more coordinated attack strategy.

  Passive reconnaissance involves the following:

  - Mapping the directory structure of the web servers and FTP servers.
  - Gathering competitive intelligence over newsgroups for references to and submissions from within the organization, bulletin boards, and industry feedback sites. Related information can be obtained from job postings, number of personnel, published resumes, and responsibilities. This can also include estimating the cost of support infrastructure.
  - Determining the value of infrastructure interfacing with the web. Asset classification as described under ISO 17799 may also be carried out here. This is to ensure that the penetration test can quantify the acceptable risk to the business.

- Retrieving network registration information from Whois databases and financial websites to identify the critical assets, and searching for business services related to the registered party.
- Determining the product range and service offerings of the target company that are available online or can be requested offline. The threat level posed to these can be estimated by checking for available documentation, associated third-party product vulnerabilities, cracks, and versions.
- Document sifting, which refers to gathering information solely from published material. This includes skimming through the source code of web pages; identifying key personnel; and investigating them further through background checks based on published resumes, affiliations, and publicly available information such as personal web pages, personal email addresses, job databases, and property pages of soft copies of any documents.
- Social engineering can be performed by identifying a conduit (a person who can be targeted easily based on the information gained about personnel) and profiling them. The profiling may be based on position, habits, preferences, weak traits, and so on. The objective here is to remove and catalog sensitive information.

In active reconnaissance, the information-gathering process encroaches on the target territory. Here, the perpetrator may send probes to the target in the form of port scans, network sweeps, enumeration of shares and user accounts, and so on. The tester may adopt techniques such as social engineering and use tools that automate these tasks such as scanners and sniffers. Active reconnaissance also involves the following:

- Web profiling
- Perimeter mapping
- System and service identification through port scans

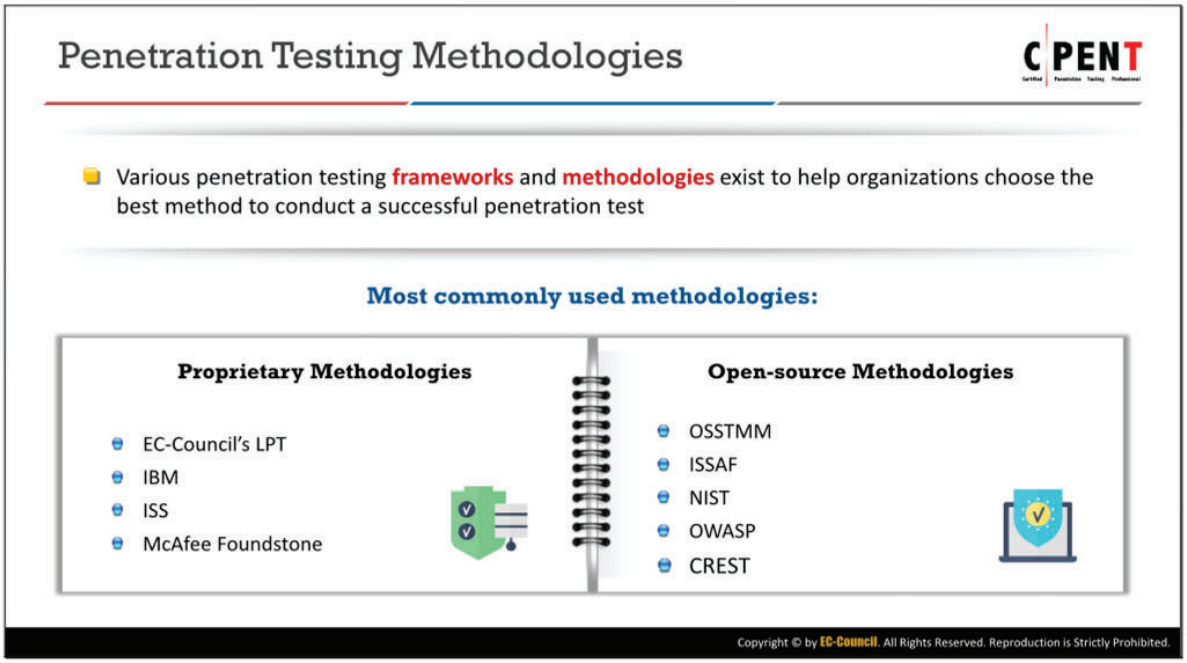
- **Attack Phase**

The information gathered in the pre-attack phase forms the basis of the attack strategy. During the attack phase, the attack strategy is developed and executed. The attack phase involves the actual compromise of the target. The tester may exploit a vulnerability discovered during the pre-attack phase or use security loopholes such as a weak security policy to gain access to the system. The important point here is that while the tester needs only one port of entry, organizations must defend several. Once inside, the tester may escalate their privileges, install a backdoor to sustain access to the system, and exploit it to achieve their goal.

Following are the various activities performed during the attack phase:

- **Perimeter testing**: Perimeter testing measures the firewall's ability to handle fragmentation. It provides an understanding of how Internet-connected networks are vulnerable to hacking.

- **Web application testing**: It provides a security assessment of various kinds of applications.
- **Wireless testing**: Wireless testing activity involves checking all wireless routers, access points, and gateways for vulnerabilities.
- **Application security assessment**: Application security assessment has a methodology similar to that of external penetration testing.
- **Network security assessment**: Network security assessment identifies risks and vulnerabilities that may harm network and security policies. It also provides information needed to make network security decisions.
- **Wireless/remote access security assessment**: Wireless/remote access security assessment identifies the security risks of wireless devices. Some of the wireless technologies with security risks are 802.11 wireless networking, broadband Internet access, and so on. Hence, precautions must be taken so that the architecture, design, and deployment of such solutions are secure.
- **Database penetration testing**: Database penetration testing identifies security issues in databases. The database penetration tester tests the database layer by layer and documents the security weaknesses in every layer. As the database is the most critical asset of an organization, each component is valuable for the success of the entire system. This type of penetration test is conducted to find security breaches in the whole system and to assist in the implementation of the required safeguards.
- **File integrity checking**: File integrity checking focuses on the size, version, and modifications in files. It checks the login details of the users who modify existing files. Further, it adopts integrity checking techniques.
- **Log management penetration testing**: Log management penetration testing focuses on the security issues in log files. Organizations use log data for strengthening information security with the help of advanced audits and data correlation. It is also used for troubleshooting and meeting compliance initiatives. This type of penetration test scans for log files and checks whether the logs are encrypted.
- **Telephony security assessment:** Telephony security assessment checks the security issues of voice technologies used in organizations. In telephony security assessment, penetration testers exploit private branch exchanges (PBXs) to check mailbox deployment and security, routing of calls at the target's expense, unauthorized modem use, voice over IP integration, and associated risks.
- **Data leakage penetration testing**: Data leakage is one of the most debilitating problems that occur within an organization. An organization needs to perform data leakage penetration testing to protect its confidential data from malicious users.
- **Social engineering**: Social engineering is an intrusion process associated with human interactions and deception that involves the breach of simple and basic security procedures. This process exploits the weaknesses and amicability of people. The eavesdropping technique plays a vital role in the process of social engineering. Other



Penetration Testing Methodologies

Various penetration testing frameworks and methodologies exist to help organizations choose the best method to conduct a successful penetration test. The cornerstone of a successful penetration test is the methodology involved in devising it. The underlying methodology should help the tester by providing a systematic approach to the testing pattern. The test must satisfy adjectives such as consistency, accuracy, and efficiency, and the testing methodology should be adequate. This does not mean that the entire framework should be restrictive.

The two types of penetration testing methodologies are as follows:

- **Proprietary methodologies**

  There are many organizations that work on penetration testing and offer services and certifications. Network security organizations have their own methodologies that are to be kept confidential. The following are some proprietary methodologies:

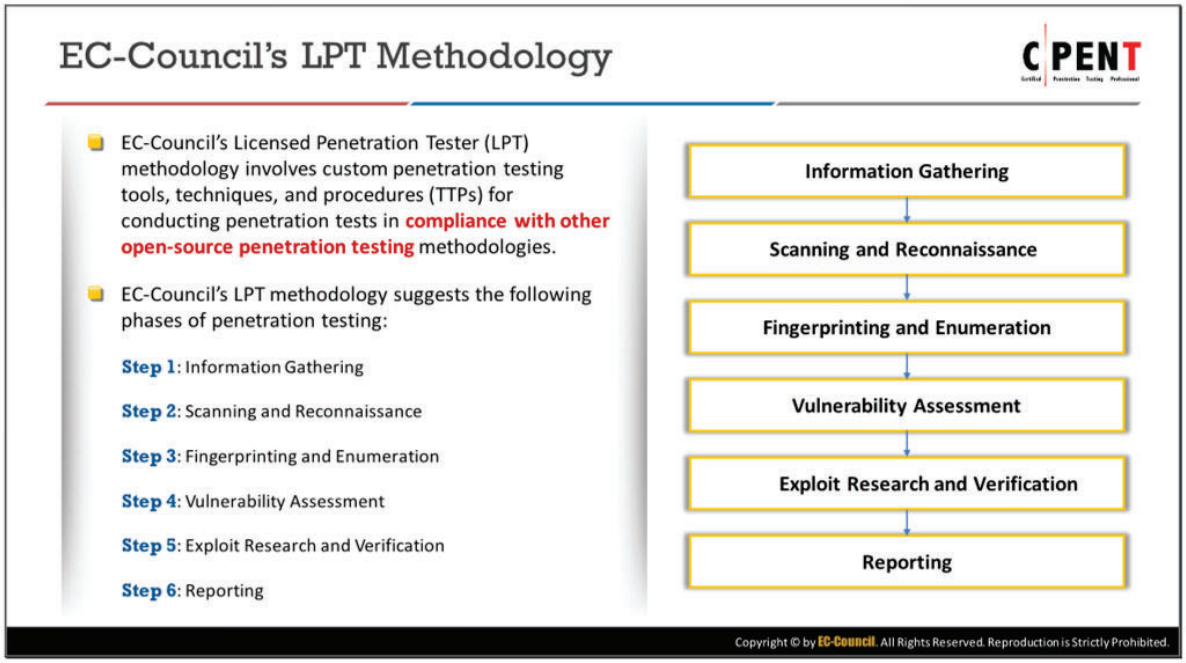
  - EC-Council's Licensed Penetration Tester (LPT)
  - IBM
  - ISS
  - McAfee Foundstone

- **Open-source and public methodologies**

  A wide range of methodologies are publicly available. They can be used by anybody and are intended for public use only.

  - **Open Source Security Testing Methodology Manual**

    The Open Source Security Testing Methodology Manual was compiled by Pete Herzog. It is a standard set for penetration testing to achieve security metrics. It is considered



EC-Council's LPT Methodology

EC-Council's LPT methodology involves custom penetration testing TTPs for conducting penetration tests in compliance with other open-source penetration testing methodologies.

As shown in the figure, EC-Council's LPT methodology suggests the following phases of penetration testing:

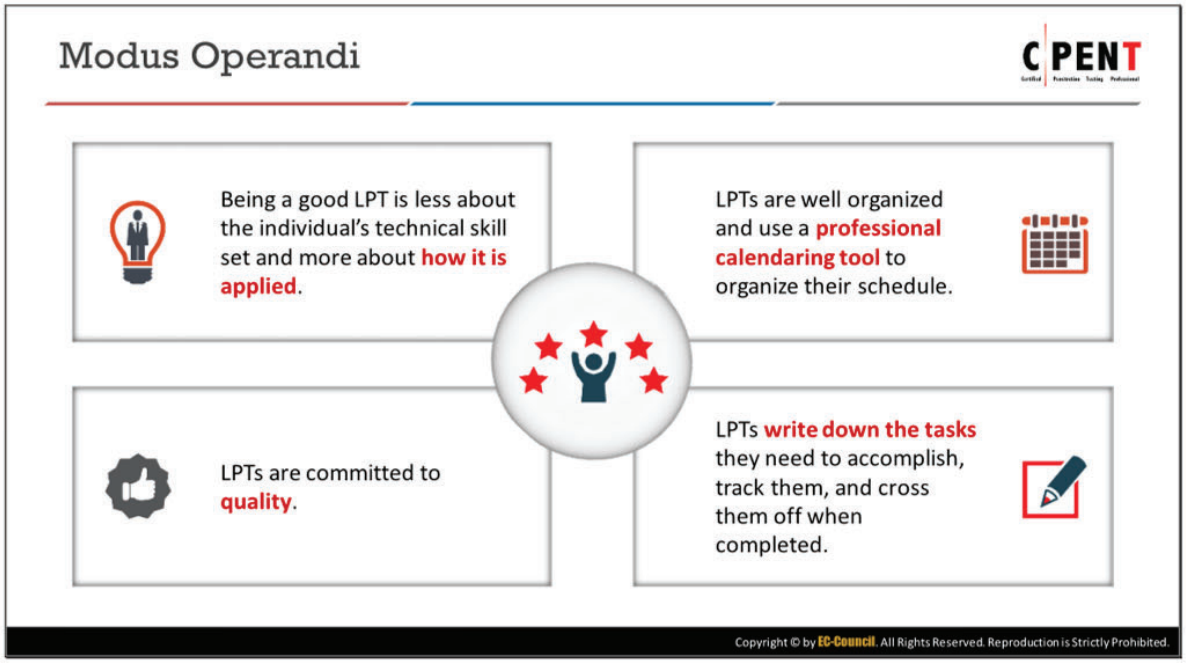
- **Step 1**: Information Gathering
- **Step 2**: Scanning and Reconnaissance
- **Step 3**: Fingerprinting and Enumeration
- **Step 4**: Vulnerability Assessment
- **Step 5**: Exploit Research and Verification
- **Step 6**: Reporting

Figure 1.1: Flowchart of LPT methodology

Qualities of a Licensed Penetration Tester

The following are some qualities of a licensed penetration tester:

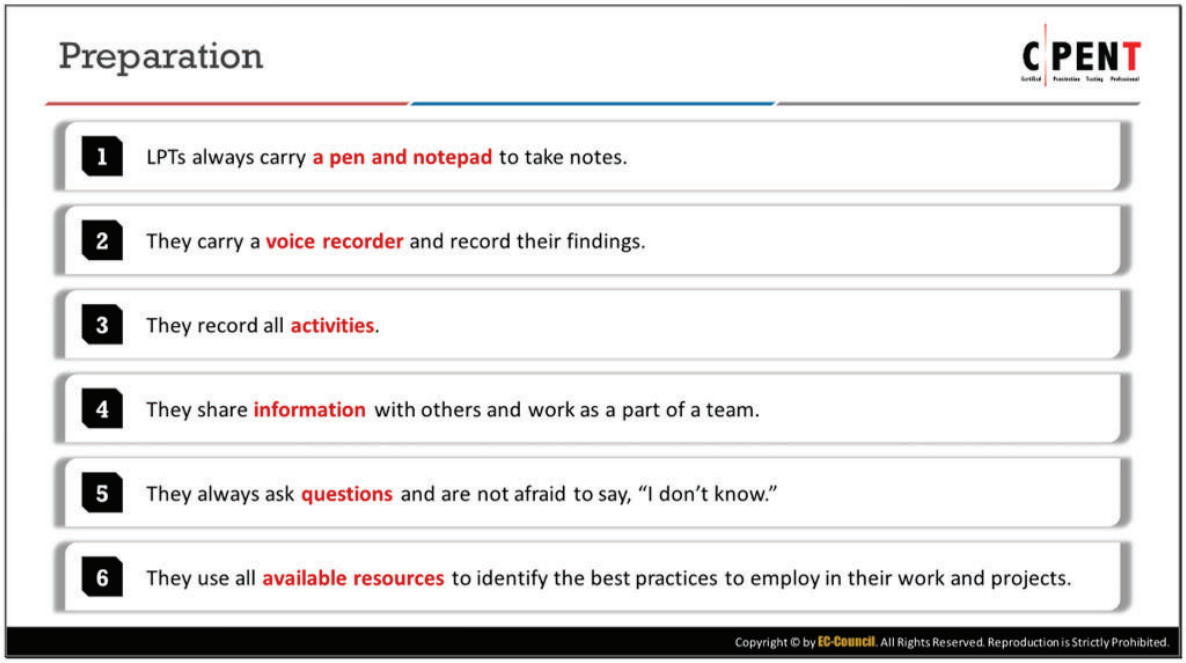
- LPTs constantly analyze their work.
- They motivate, complement, and reward team members for doing good work.
- LPTs approach the work in an effort to improve security.
- LPTs understand not only what to do and what not to do but also why things are done in a certain manner.
- LPTs do not consider themselves indispensable to the project.
- LPTs understand the goal of a project and work toward the goal, rather than merely follow orders.
- LPTs learn from their successes and mistakes, as well as those of others.
- LPTs are capable of solving problems or working toward a solution.
- LPTs provide support for information security programs.
- LPTs keep themselves updated with the current vulnerabilities, attacks and countermeasures, and the possibilities or techniques to respond effectively to attacks.
- LPTs research and document global threats to business execution, intellectual property, and service availability.



Modus Operandi

The following constitute the modus operandi of an LPT:

- Being a good LPT is less about the individual's technical skill set and more about how it is applied.
- LPTs are committed to quality; they ensure the deployment and integration of network security.
- LPTs are well organized and use a professional calendaring tool to organize their schedule.
- LPTs write down the tasks they need to accomplish, track them, and cross them off when completed.
- LPTs assess the security posture of an organization using policies and judgment and report the security events in a timely fashion.
- LPTs develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- LPTs perform risk assessments to ensure that there are no flaws in the security measures of an organization.
- LPTs document computer security and emergency measures policies, procedures, and tests.
- LPTs lead the execution of assessments and audits.

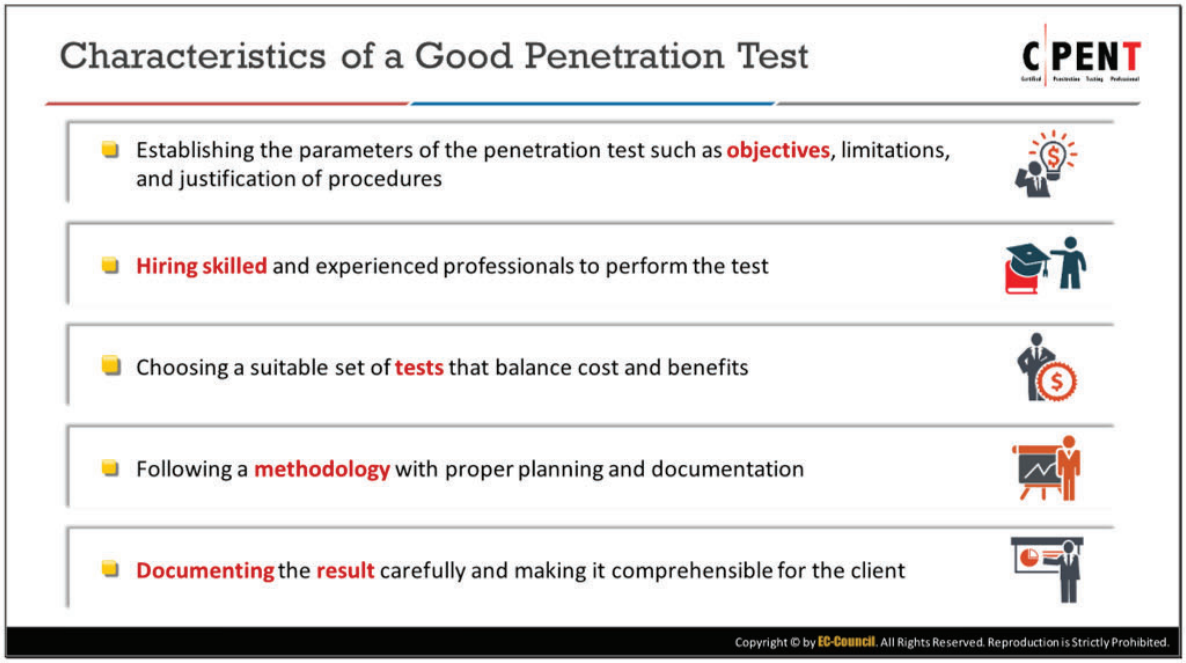


Preparation

A few preparation steps must be taken before performing a penetration test so that every minor issue can be noted and nothing is missed during a test.

The following are the preparation steps:

- LPTs always carry a pen and notepad to take notes.
- They carry a voice recorder and record their findings.
- They record all activities.
- They share information with others and work as a part of a team.
- They always ask questions and are not afraid to say, "I don't know."
- They use all available resources to identify the best practices to employ in their work and their projects.



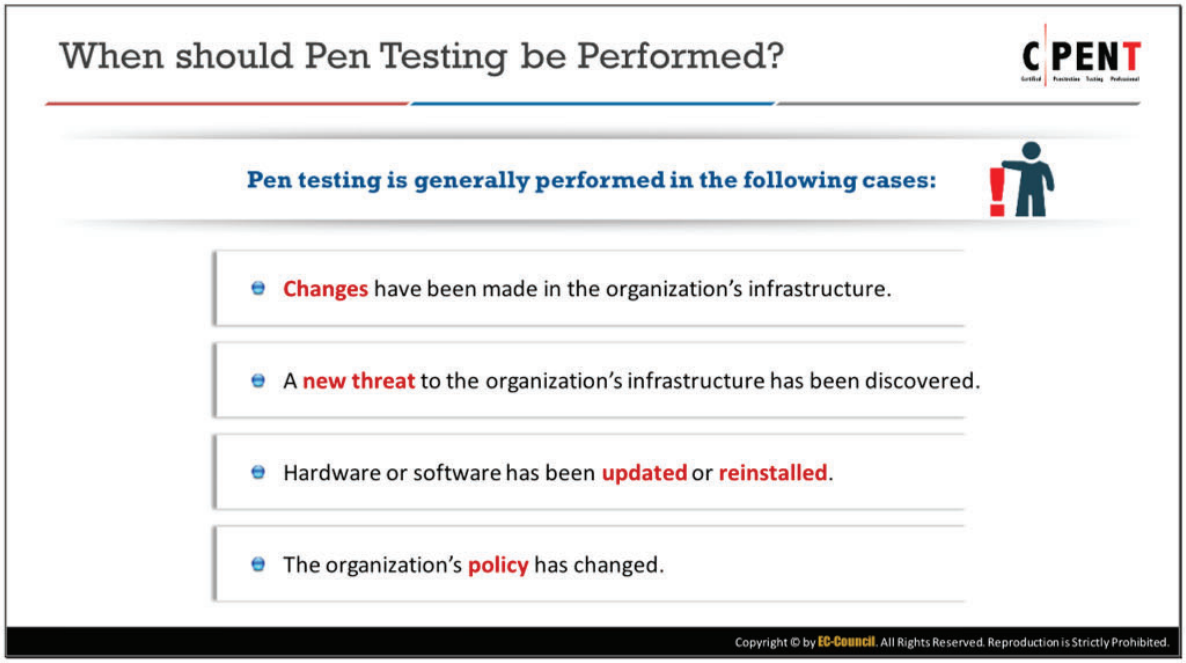
Characteristics of a Good Penetration Test

Before performing any pen test in an organization, the tester must follow some steps to ensure success. First, the organization must call for a meeting, in which they must discuss the scope and objectives of the penetration test and the parties involved in it. The objectives are important because they describe that exploitable vulnerabilities exist within the organization's infrastructure. The objectives of the penetration test must be clear; if the objective is unclear, then the results will inevitably be inaccurate. Next, the systems, machines, network, staff involved, and operational requirements are identified to perform the penetration test.

Another important agenda is the time and duration of the penetration test; these factors should be decided in such a manner that the daily operations and normal business of the organization will not be disturbed. No organization wants their businesses to be affected by a penetration test. Therefore, the organization must ensure that the penetration test is conducted at a particular time of the day because, at times, penetration testing can lead to unusual network traffic, which may cause some systems on the network to crash and affect other working systems on the network. To overcome such situations, the organization must draw a clear plan before proceeding.

The following are a few more points on the characteristics of a good penetration test:

- Establishing the parameters of the penetration test such as objectives, limitations, and justification of procedures
- Hiring skilled and experienced professionals to perform the test
- Choosing a suitable set of tests that balance cost and benefits
- Following a methodology with proper planning and documentation
- Documenting the result carefully and making it comprehensible for the client



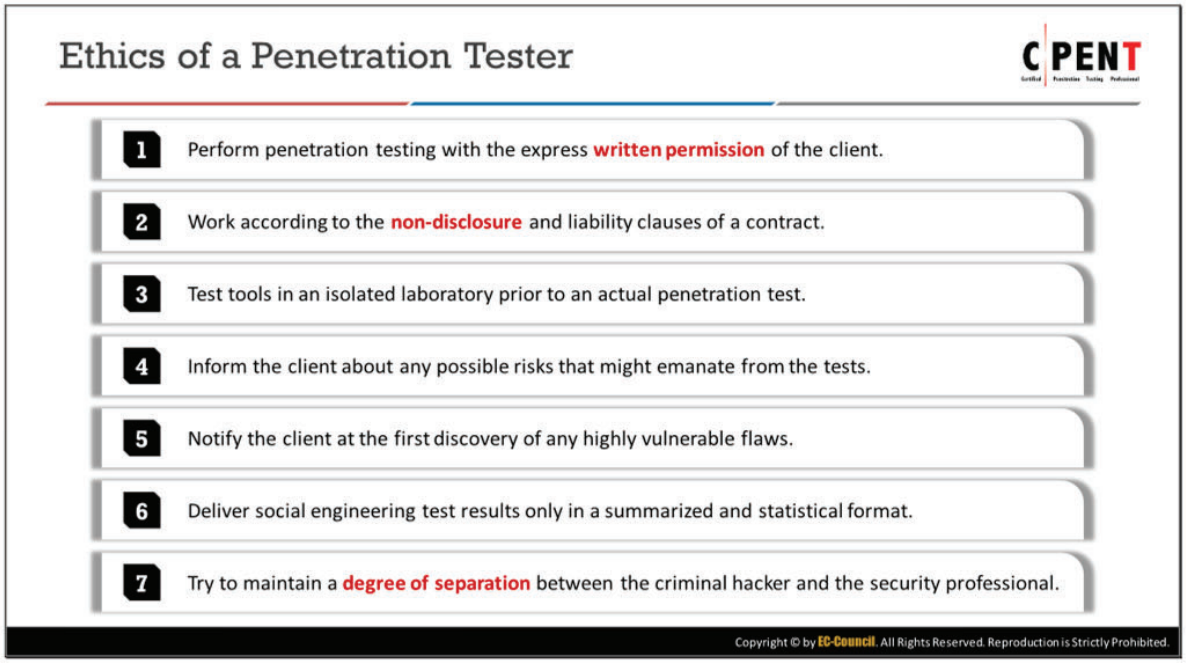
When Should Pen Testing Be Performed?

Penetration testing must be performed on a regular basis to ensure that all existing and newly discovered vulnerabilities are identified and fixed before a cybercriminal exploits them. In recent times, many new attacks have been reported, which indicates that even hackers are attempting new methodologies and techniques. An organization must be prepared with solutions for any new kind of attack. However, most companies neglect the possibility of such a situation and wait too long to conduct penetration testing; they conduct tests either when it is required by law or, in the worst case, only when a company has already been breached.

The question of when pen testing should be performed is difficult to answer because the answer depends on the company. For instance, high-profile companies that are often mentioned in the media are the most prone to attacks. Such companies must regularly perform penetration testing.

The following are some scenarios where penetration testing is required:

- Changes have been made in the organization's infrastructure.
- A new threat to the organization's infrastructure has been discovered.
- Hardware or software has been updated or reinstalled.
- The organization's policy has changed.

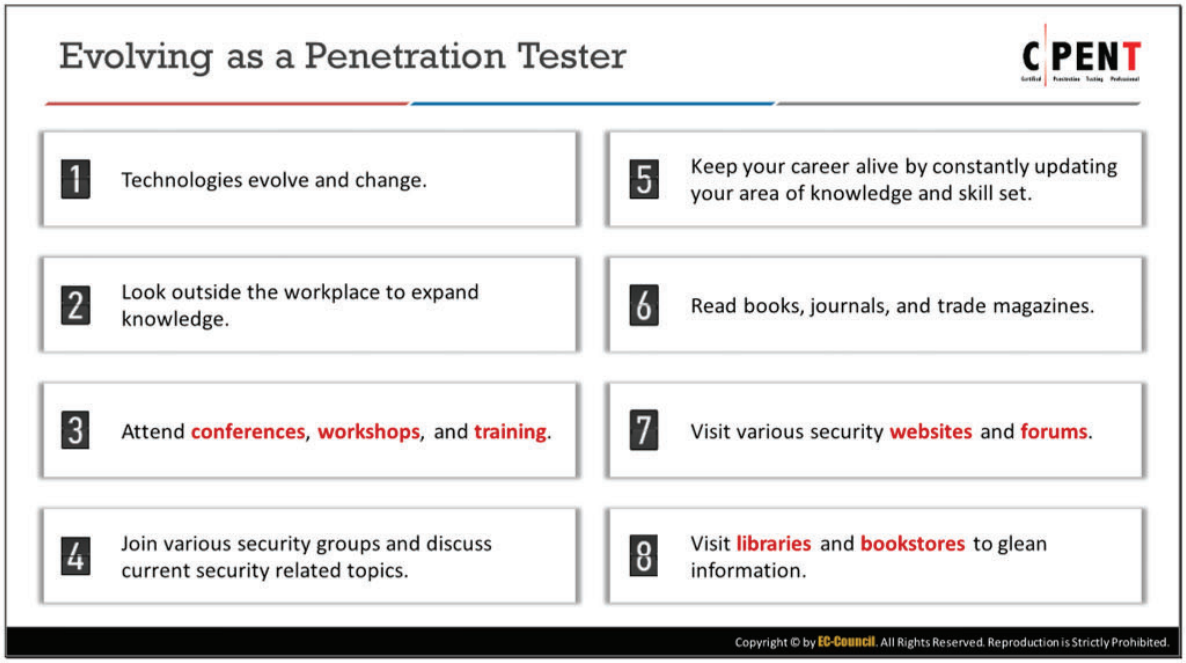


Ethics of a Penetration Tester

Every penetration tester must have ethics that help them avoid illegal activities and serve their clients in a better way. Most organizations make the tester sign an agreement to clarify the current laws and protect their clients. The laws can differ from country to country. Therefore, it is very important for a penetration tester to be aware of the current laws and legal agreement with an organization, and the tester must be highly ethical and fully professional at all times.

The following are some of the ethical requirements of a penetration tester:

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

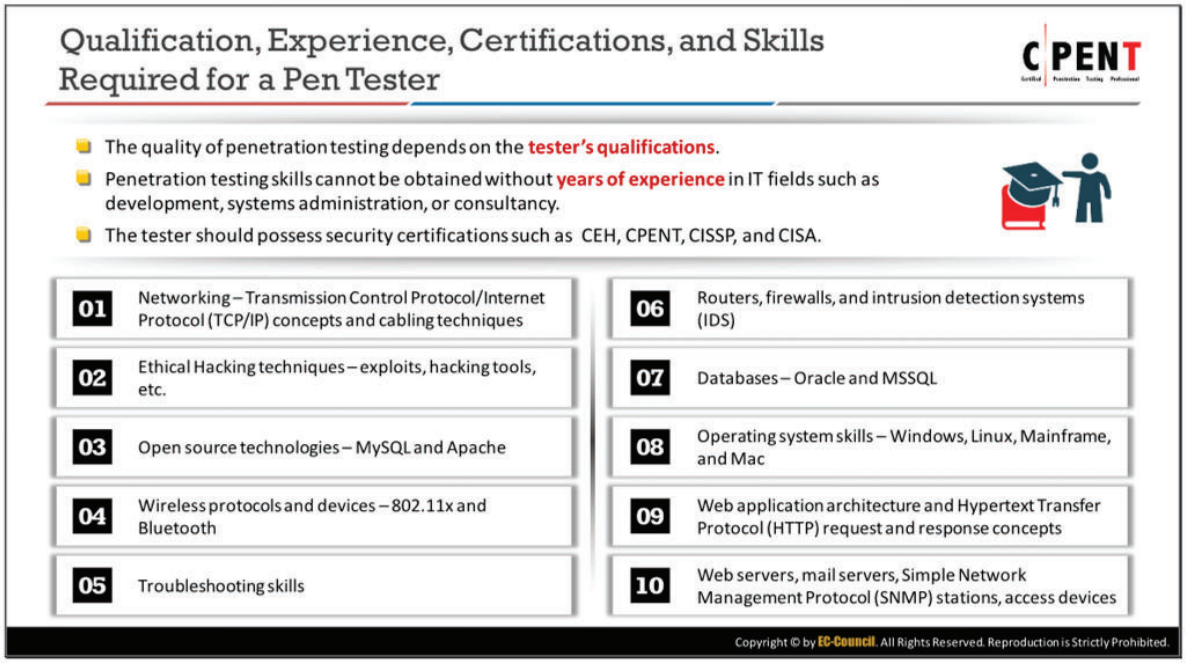


Evolving as a Penetration Tester

If you wish to become a pen tester, the first and foremost requirement is the willingness to continuously study and perform research in this field. Because the IT field is continuously evolving and engaged in the process of modernizing user experience to keep up with rapidly advancing technology, a penetration tester must be up-to-date and have sharp skills to remain one step ahead of malicious hackers. Even hackers keep themselves updated with new technology and develop new methods and techniques. Before they successfully exploit a vulnerability, the penetration tester must be prepared to tackle their attacks and be aware of new technologies and tools. The tester should look outside their workplace to expand their knowledge.

Even an experienced penetration tester must go through free guides, videos, tutorials, books, journals, trade magazines, and so on and attend webinars, conferences, workshops, and training. Pen testers join various security groups and discuss current security-related topics, and they regularly visit various security websites and forums. They also visit libraries and bookstores to glean information. Pen testers keep your career alive by constantly updating their area of knowledge and skill set.

There are multiple ways to perfect the craft of pen testing. In addition to a formal degree, a computer science degree with a certified penetration testing program can help a pen tester become more advanced and gain expertise in specialized area.



Qualification, Experience, Certifications, and Skills Required for a Pen Tester

The quality of penetration testing depends on the tester's qualifications. Penetration testing skills cannot be obtained without years of experience in IT fields such as development, systems administration, or consultancy. A pen tester should possess security certifications such as CEH, CPENT, CISSP, and CISA.

- **Qualification**

  The professional penetration tester must possess the following qualifications:

  - Certified Register of Ethical Security Testers (CREST)
  - Cyber-security certifications (CHECK, CTM, CTL, CREST, TIGER, OSCP)
  - A degree in computer security, computer science, or equivalent
  - Recognized security testing certifications (GIAC and CEH)

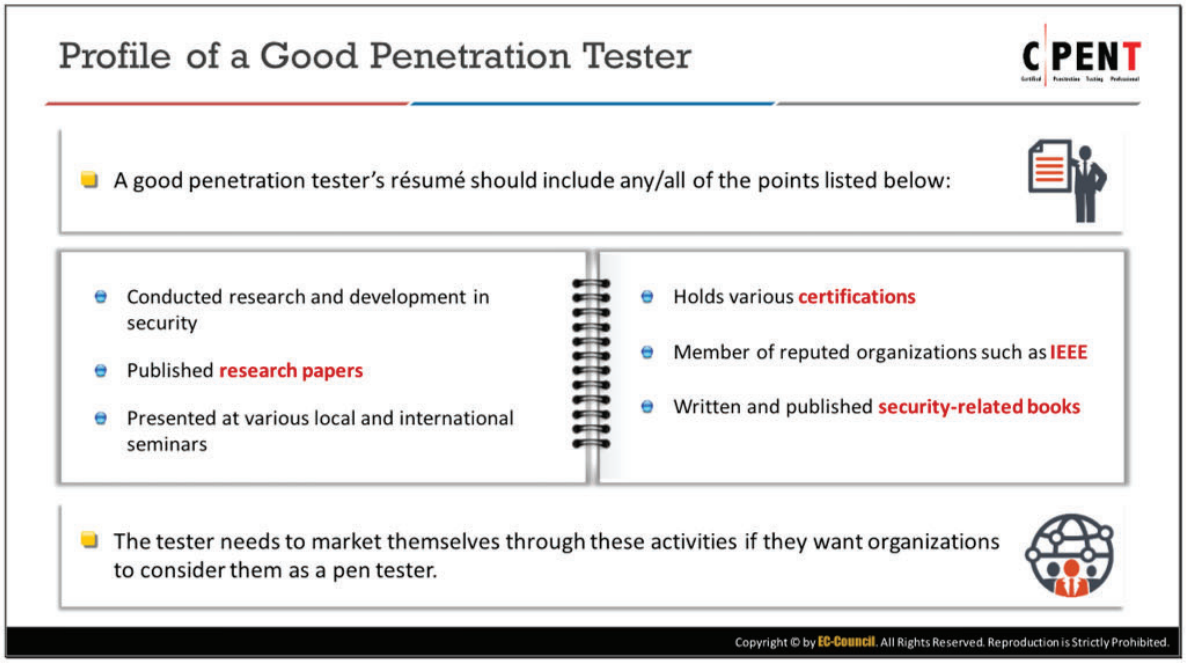
- **Experience**

  - The professional pen tester must have sound knowledge and experience in handling various penetration test tools including open and commercial mapping.
  - They must possess experience in systems, networks, and web-based applications.
  - It is desirable to have experience in using problem-solving techniques and developing a solution to meet vulnerability threats.
  - They must possess good communication skills to explain technical details to nontechnical parties.

- They must be proficient at report writing and scripting skills and have good experience at reverse engineering.
- Consulting experience is an added advantage because they must understand the client's needs and build a positive relationship with them.

- **Certifications**
  - CEH: Certified Ethical Hacker
  - CPENT: Certified Penetration Testing Professional
  - CEPT: Certified Expert Penetration Tester
  - GPEN: GIAC Certified Penetration Tester
  - OSCP: Offensive Security Certified Professional
  - CISSP: Certified Information Systems Security Professional
  - GCIH: GIAC Certified Incident Handler
  - GCFE: GIAC Certified Forensic Examiner
  - GCFA: GIAC Certified Forensic Analyst
  - CCFE: Certified Computer Forensics Examiner
  - CREA: Certified Reverse Engineering Analyst
  - CPTC: Certified Penetration Testing Consultant
  - CPTE: Certified Penetration Testing Engineer
  - CompTIA: Security+
  - CSTA: Certified Security Testing Associate
- **Required skills sets of a penetration tester**

  A professional penetration tester should possess the following skill sets:
  - Strong knowledge of current and emerging technology, methodologies, and tools in the security industry
  - Familiarity with network security concepts, software architecture and design, and engineering processes
  - Knowledge of hardware concepts such as the following:
    - Networking: Transmission Control Protocol/Internet Protocol (TCP/IP) concepts and cabling techniques
    - Ethical hacking techniques: exploits, hacking tools, and so on.
    - Open-source technologies: MySQL and Apache
    - Wireless protocols and devices: 802.11x and Bluetooth

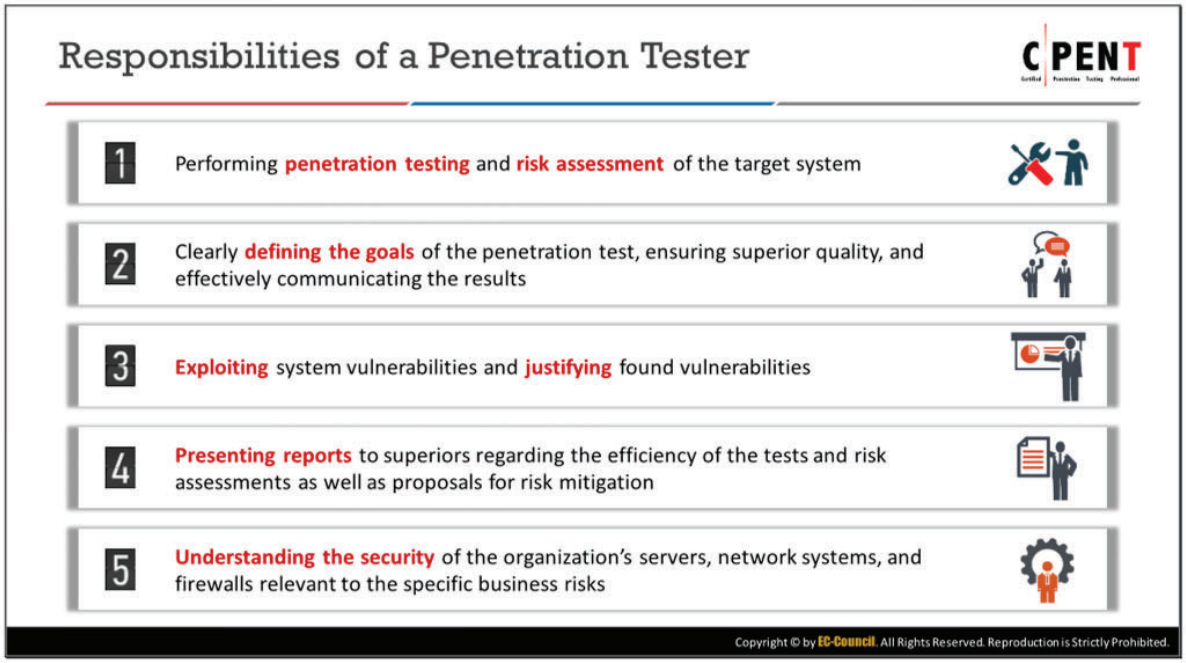


Profile of a Good Penetration Tester

It is very important to prepare a good résumé before applying for any job; it must precisely describe the skills and experiences of the candidate that are suitable for the job. The profile forms the first impression for the employer to judge whether a candidate is a good fit as a penetration tester. A few aspects need to be highlighted in the résumé so that the employer can quickly go through it, and the résumé must be short and precise.

A good penetration tester will have the following in their résumé:

- Conducted research and development in security
- Published research papers
- Presented at various local and international seminars
- Holds various certifications
- Member of many reputed organizations such as IEEE
- Written and published security-related books
- Previous experience as a pen tester
- Developed open-source security software tools
- Participated in "capture the flag" competitions and hackathons
- Achievements such as appreciation from an organization for work in improving their security
- Conducted a talk in an international security conference for a chosen topic of relevance
- Has code configurations in open-source security projects



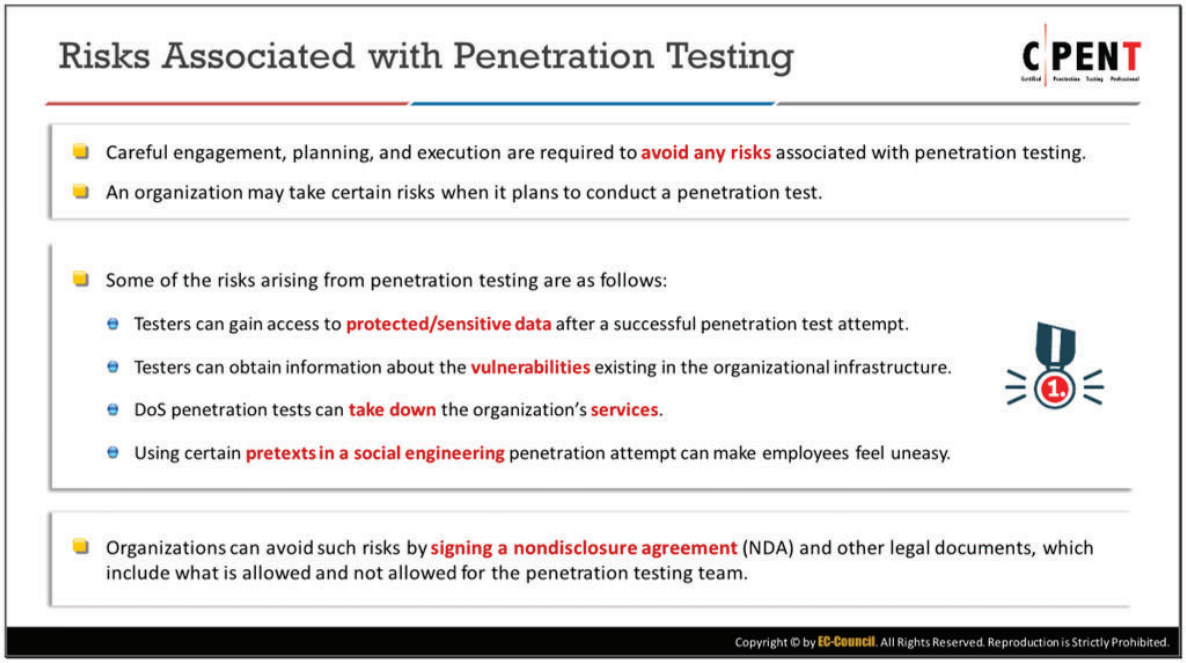
Responsibilities of a Penetration Tester

Often, penetration testers are called ethical hackers because they breach into a network or system with prior permission from or agreement of the concerned person or organization; without prior permission or agreement, they are simply hackers. Companies mainly hire penetration testers to know if any part of their infrastructure or network is vulnerable to attacks and determine the existence of security holes that a hacker can easily exploit.

Therefore, a penetration tester must run several tests and prepare an assessment report about the tests and their results. Often, the tester runs predefined types of tests and design their own tests as well to exploit vulnerabilities; to design a custom test, the tester requires a lot of creativity and imagination with a high level of technical knowledge.

In addition, a penetration tester has the following responsibilities:

- Perform the penetration testing and risk assessment of the target system.
- Clearly define the goals of the penetration test, ensure superior quality, and effectively communicate the results.
- Exploit system vulnerabilities and justify found vulnerabilities.
- Present reports to superiors on the efficiency of the tests and risk assessments, as well as proposals for risk mitigation.
- Understand the security of the organization's servers, network systems, and firewalls relevant to specific business risks
- Create and design new penetration tools for testing vulnerabilities.
- Identify the methods and techniques that an attacker could use to exploit weaknesses and logic flaws.



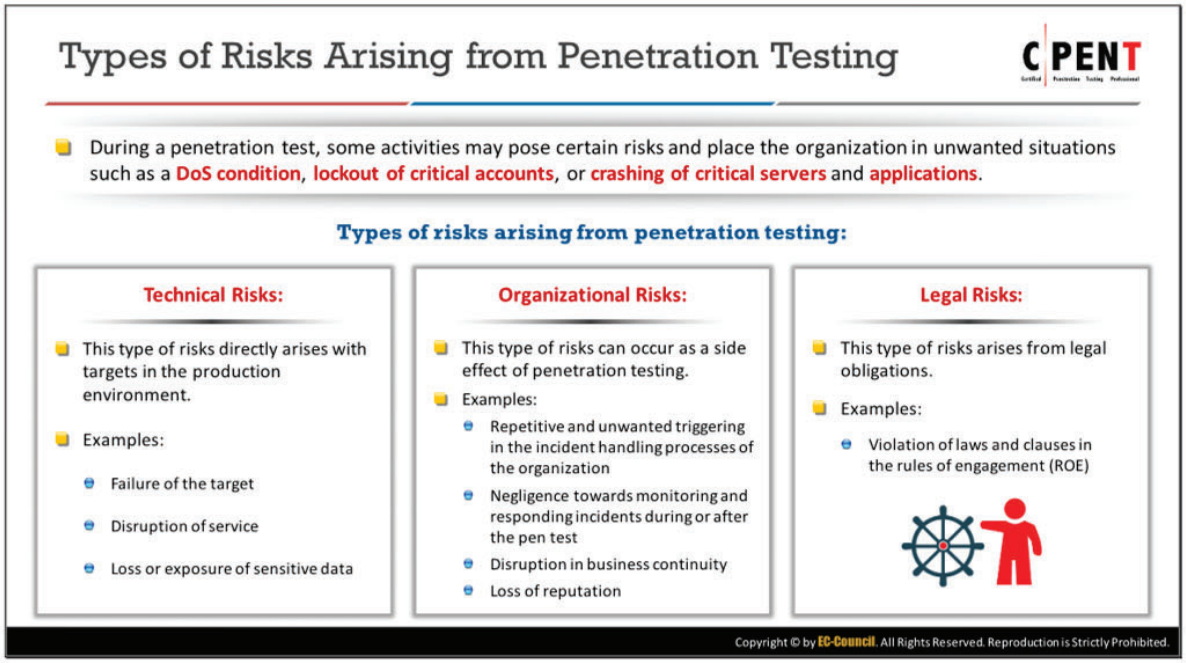
Risks Associated with Penetration Testing

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 vulnerabilities existing in the organization infrastructure.
- DoS penetration tests can take down the organization's services.
- Using certain pretexts in a social engineering penetration attempt can make employees feel embarrassed, uneasy, and uncomfortable.

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.

The following are the types of risks arising from penetration testing:

- **Technical risks**

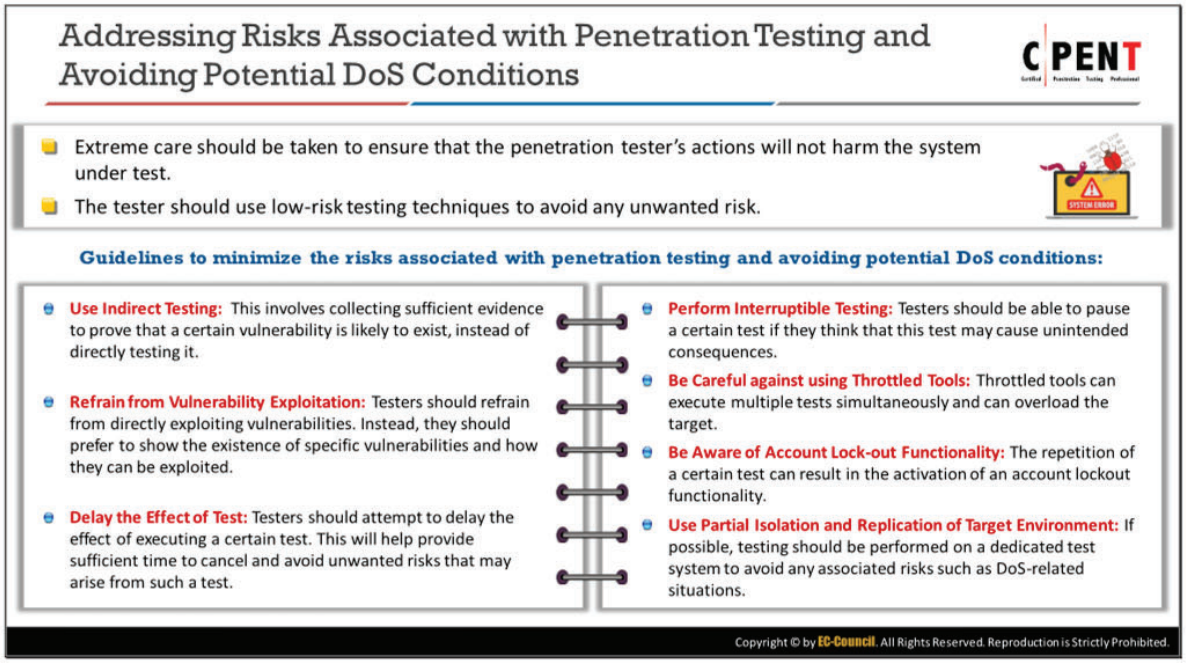
  This type of risks directly arises with targets in the production environment. It includes the following.

  - **Failure of the target**: Testing continuously consumes a large amount of resources of the target system. This may result in the unavailability of services of the target machine.
  - **Disruption of service**: The testing process can disrupt some critical services.
  - **Loss or exposure of sensitive data**: The organization needs to share sensitive data with the pen testers, which may result in the exposure of sensitive data.

- **Organizational risks**

  This type of risks can occur as a side effect of penetration testing. It includes the following.

  - Repetitive and unwanted triggering in the incident-handling processes of the organization
  - Negligence toward monitoring and responding incidents during or after the pen test
  - Disruption in business continuity



Addressing Risks Associated with Penetration Testing and Avoiding Potential DoS Conditions

Extreme care should be taken to ensure that the penetration tester's actions will not harm the system under test. The tester should use low-risk testing techniques to avoid any unwanted risk.

The following are the guidelines to minimize the risks associated with penetration testing and avoiding potential DoS conditions:

- **Use indirect testing**: This involves collecting sufficient evidence to prove that a certain vulnerability is likely to exist, instead of directly testing it.
- **Refrain from vulnerability exploitation**: Testers should refrain from directly exploiting vulnerabilities. Instead, they should prefer to show the existence of specific vulnerabilities and how they can be exploited.
- **Delay the effect of a test**: Testers should attempt to delay the effect of executing a certain test. This will help provide sufficient time to cancel and avoid unwanted risks that may arise from the test.
- **Perform interruptible testing**: Testers should be able to pause a certain test if they think that this test may cause unintended consequences.
- **Be careful of using throttled tools**: Throttled tools can execute multiple tests simultaneously and can overload the target.
- **Be aware of account lockout functionality**: The repetition of a certain test can result in the activation of an account lockout functionality.