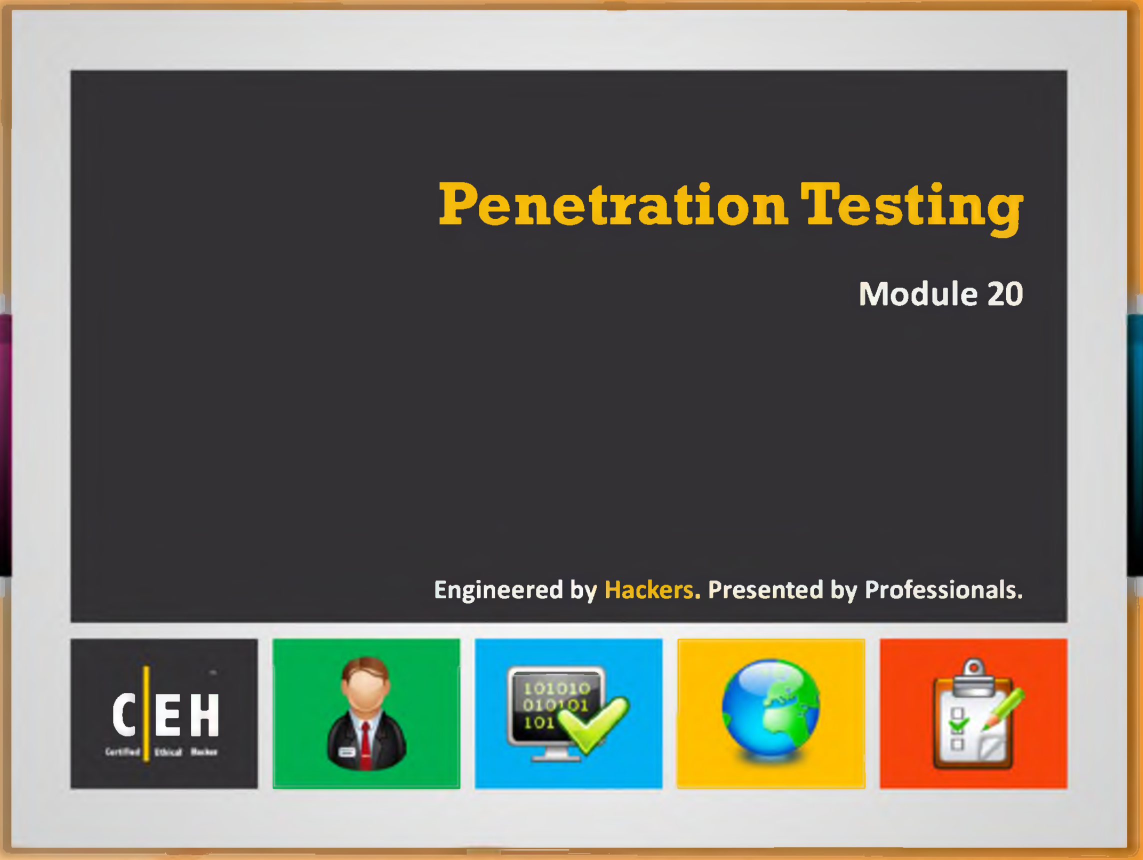
Penetration Testing

Module 20



Penetration Testing

Module 20

Engineered by Hackers. Presented by Professionals.

Ethical Hacking and Countermeasures v8

Module 20: Penetration Testing

Exam 312-50

October 02, 2012

City of Tulsa Cyber Attack Was Penetration Test, Not Hack

The City of Tulsa, Oklahoma last week began notifying residents that their personal data may have been accessed -- but it now turns out that the attack was a penetration test by a company the city had hired.

"City officials didn't realize that the apparent breach was caused by the security firm, Utah-based SecurityMetrics, until after 90,000 letters had been sent to people who had applied for city jobs or made crime reports online over the past decade, warning them that their personal identification information might have been accessed," writes Tulsa World's Brian Barber. "The mailing cost the city $20,000, officials said."

"An additional $25,000 was spent on security consulting services to add protection measures to the website," FOX23 News reports.

http://www.esecurityplanet.com

Security News

City of Tulsa Cyber Attack Was Penetration Test, Not Hack

Source: http://www.esecurityplanet.com

The City of Tulsa, Oklahoma last week began notifying residents that their personal data may have been accessed -- but it now turns out that the attack was a penetration test by a company the city had hired.

"City officials didn't realize that the apparent breach was caused by the security firm, Utah-based SecurityMetrics, until after 90,000 letters had been sent to people who had applied for city jobs or made crime reports online over the past decade, warning them that their personal identification information might have been accessed," writes Tulsa World's Brian Barber. "The mailing cost the city $20,000, officials said."

"**An additional $25,000 was spent on security consulting services to add protection measures to the website**," FOX23 News reports.

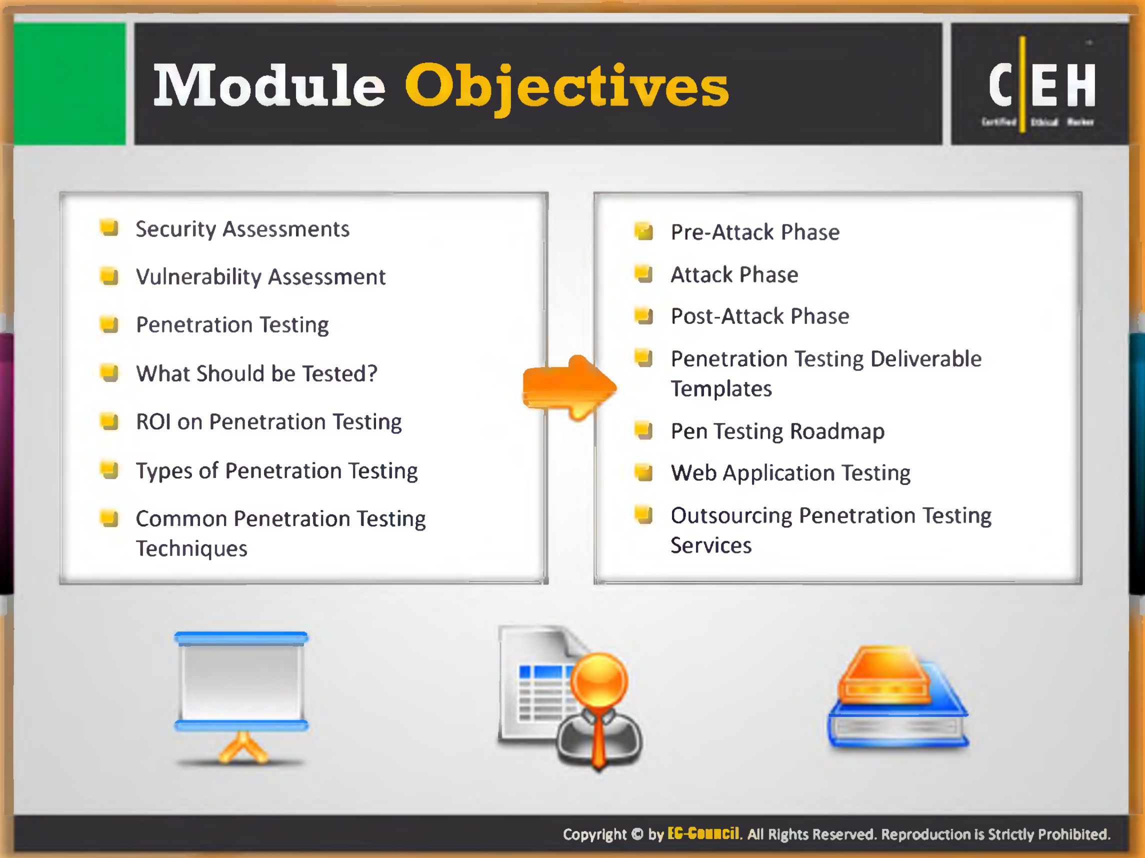
"The third-party consultant had been hired to perform an assessment of the city's network for vulnerabilities," write NewsOn6.com's Dee Duren and Lacie Lowry. "The firm used an unfamiliar testing procedure that caused the City to believe its website had been compromised. 'We had to treat this like a cyber-attack because every indication initially pointed to an attack,' said City Manager Jim Twombly."

"The chief information officer who failed to determine that the hack was actually part of a penetration test has been placed on administrative leave with pay," writes Softpedia's Eduard Kovacs. "In the meantime, his position will be filled by Tulsa Police Department Captain Jonathan Brook."

Copyright 2012 QuinStreet Inc

By Jeff Goldman

http://www.esecurityplanet.com/network-security/city-of-tulsa-cyber-attack-was-penetration-test-not-hack.html



Module Objectives

- Security Assessments
- Vulnerability Assessment
- Penetration Testing
- What Should be Tested?
- ROI on Penetration Testing
- Types of Penetration Testing
- Common Penetration Testing Techniques

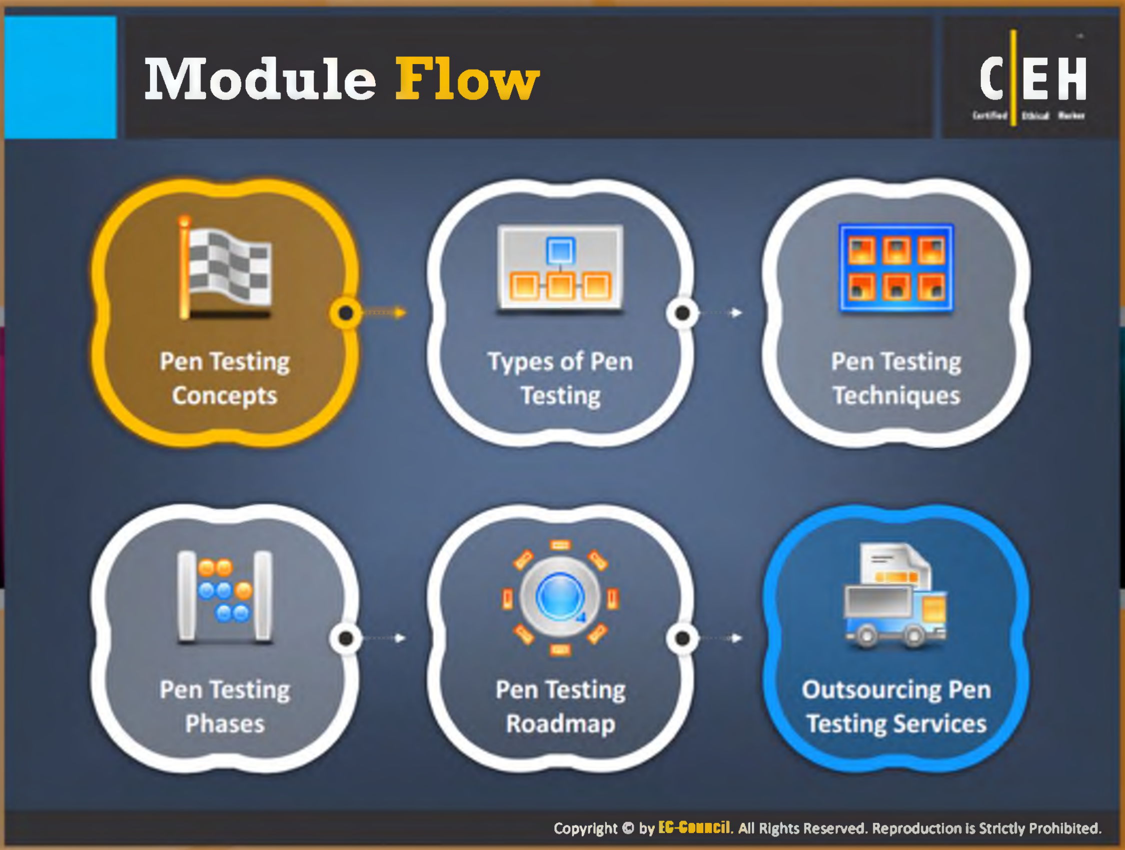
- Pre-Attack Phase
- Attack Phase
- Post-Attack Phase
- Penetration Testing Deliverable Templates
- Pen Testing Roadmap
- Web Application Testing
- Outsourcing Penetration Testing Services

Module Objectives

All the modules discussed so far concentrated on various penetration testing techniques specific to the respective element (web application, etc.), mechanism (IDS, firewall, etc.), or phase (reconnaissance, scanning, etc.). This module summarizes all the **penetration tests**. This module helps you in evaluating the security of an organization and also guides you to make your network or system more secure with its **countermeasures**.

The module will make you familiarize with:

- Security Assessments
- Vulnerability Assessments
- Penetration Testing
- What Should be Tested
- ROI on Penetration Testing
- Types of Penetration Testing
- Common Penetration Testing Techniques
- Pre-attack Phase
- Attack Phase
- Post-attack Phase
- Penetration Testing Deliverable Templates
- Pen Testing Roadmap
- Web Application Testing
- Outsourcing Penetration Testing Services

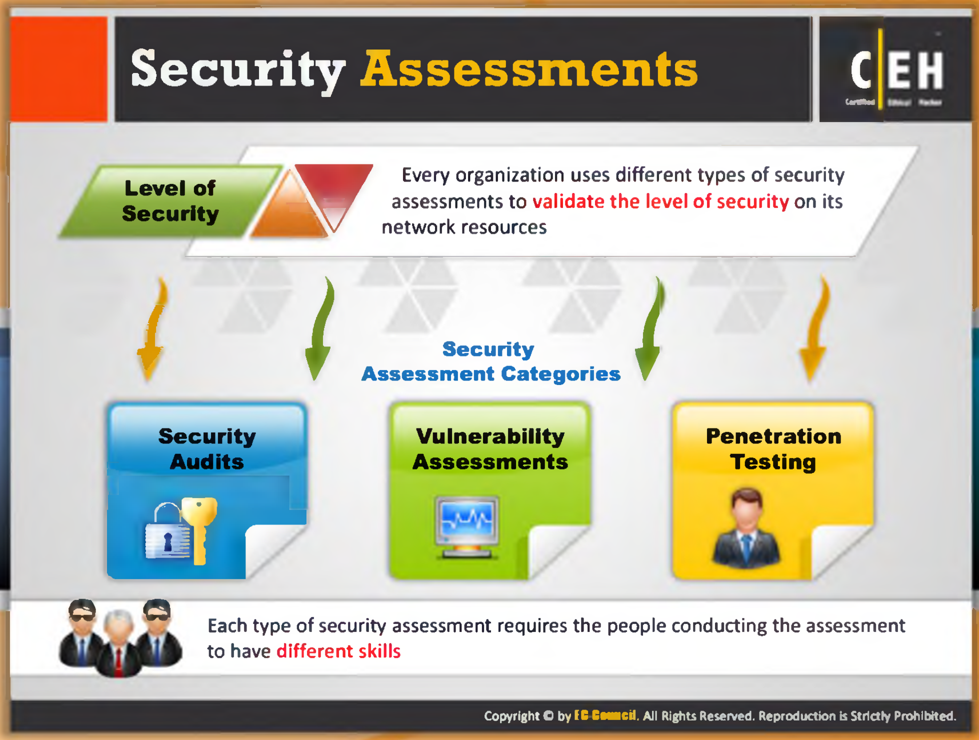


Module Flow

For better understanding of penetration testing, this module is divided into various sections. Let's begin with penetration testing concepts.

Pen Testing Concepts	Types of Pen Testing
Pen Testing Techniques	Pen Testing Phases
Pen Testing Roadmap	Outsourcing Pen Testing Services

This section starts with basic concept of penetration testing. In this section, you will learn the role of penetration testing in the security assessment and why vulnerability assessment alone is not enough to detect and remove vulnerabilities in the network. Later in this section, you will examine why penetration testing is necessary, how to perform a good penetration test, how to determine testing points, testing locations, and so on.



Security Assessments

Level of Security

Every organization uses different types of security assessments to validate the level of security on its network resources

Security Assessment Categories

Security Audits

Vulnerability Assessments

Penetration Testing

Each type of security assessment requires the people conducting the assessment to have different skills

Security Assessments

Every organization uses different types of security assessments to validate the level of security on its network resources. Organizations need to choose the assessment method that suits the requirements of its situation most appropriately. People conducting different types of security assessments must possess different skills. Therefore, pen testers—if they are employees or outsourced security experts—must have a thorough experience of penetration testing. Security assessment categories include security audits, vulnerability assessments, and penetration testing or ethical hacking.

Security Assessment Categories

The security assessment is broadly divided into three categories:

1. **Security Audits:** IT security audits typically focus on the people and processes used to design, implement, and manage security on a network. There is a baseline involved for processes and policies within an organization. In an IT security audit, the auditor and the organization's security policies and procedures use the specific baseline to audit the organization. The IT management usually initiates IT security audits. The National Institute of Standards and Technology (NIST) has an IT security audit manual and associated toolset to conduct the audit; the NIST Automated Security Self-Evaluated Tool (ASSET) can be downloaded at http://csrc.nist.gov/asset/.

In a computer, the security audit technical assessment of a system or application is done manually or automatic.

You can perform a manual assessment by using the following techniques:

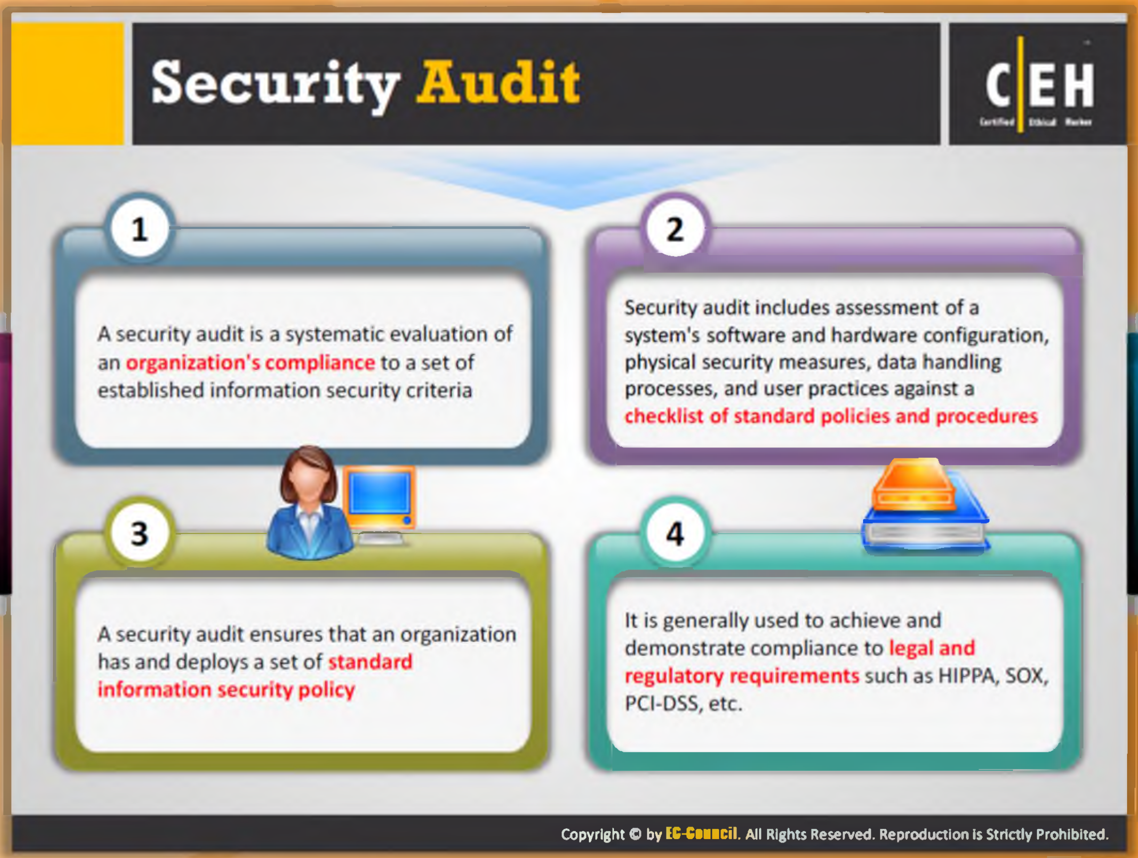
- Interviewing the staff
- Reviewing application and operating systems access controls
- Analyzing physical access to the systems.

You can perform an automatic assessment by using the following techniques:

- Generating audit reports
- Monitoring and reporting the changes in the files

2. **Vulnerability Assessments:** A vulnerability assessment helps you in identifying **security vulnerabilities.** To perform a vulnerability assessment you should be a very skilled professional. Through proper assessment, threats from hackers (outsiders), former employees, internal employees, etc. can be determined.

3. **Penetration Testing:** Penetration testing is the act of testing an **organization's security** by simulating the actions of an attacker. It helps you in determining various levels of vulnerabilities and to what extent an external attacker can damage the network, before it actually occurs.



Security Audit

1. A security audit is a systematic evaluation of an **organization's compliance** to a set of established information security criteria

2. Security audit includes assessment of a system's software and hardware configuration, physical security measures, data handling processes, and user practices against a **checklist of standard policies and procedures**

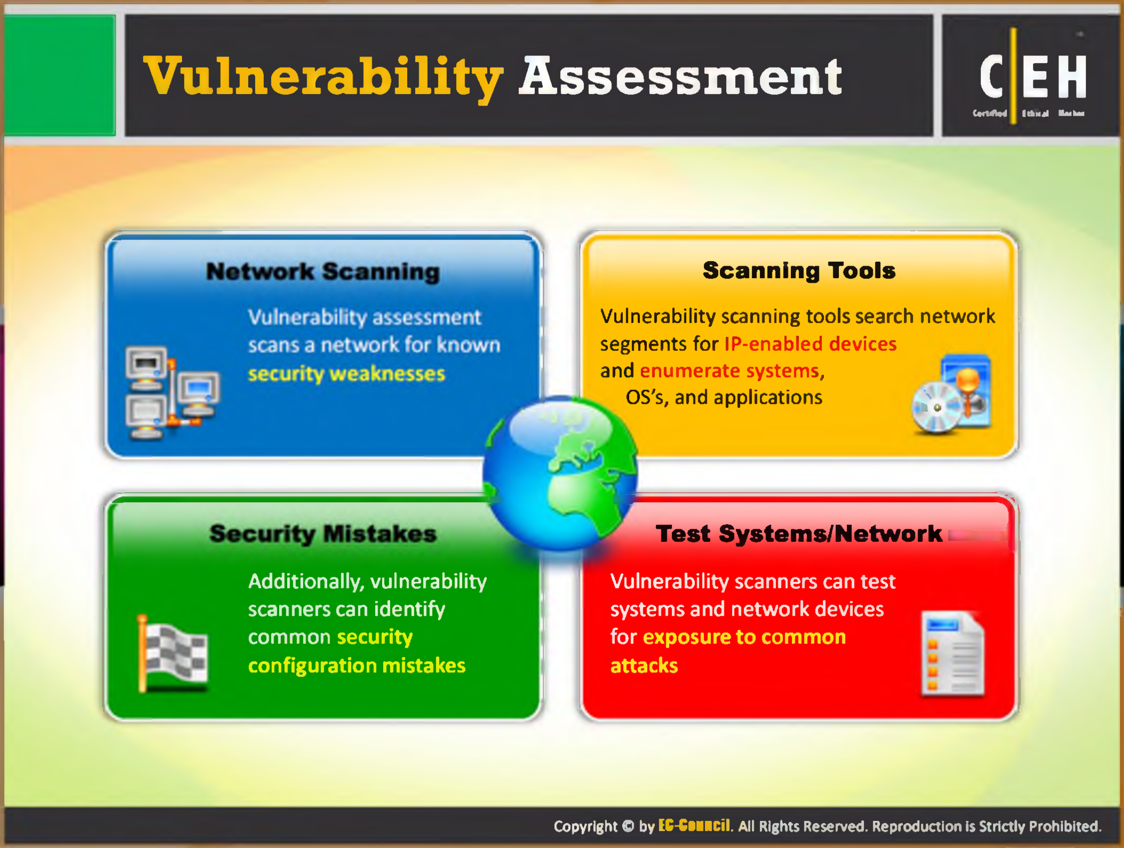
3. A security audit ensures that an organization has and deploys a set of **standard information security policy**

4. It is generally used to achieve and demonstrate compliance to **legal and regulatory requirements** such as HIPPA, SOX, PCI-DSS, etc.

Security Audit

A security audit is a systematic, measurable technical assessment of how the security policy is employed by the organization. A security audit is conducted to maintain the security level of the particular organization. It helps you to identify attacks that pose a threat to the network or attacks against resources that are considered valuable in risk assessment. The security auditor is responsible for **conducting security audits** on the **particular organization**. The security auditor works with the full knowledge of the organization, at times with considerable inside information, in order to understand the resources to be audited.

- A security audit is a systematic evaluation of an organization's compliance to a set of established information security criteria.
- The security audit includes assessment of a system's software and hardware configuration, physical security measures, data handling processes, and user practices against a checklist of **standard policies** and procedures.
- A security audit ensures that an organization has and deploys a set of standard information security policies.
- It is generally used to achieve and demonstrate compliance to legal and regulatory requirements such as **HIPPA, SOX, PCI-DSS**, etc.



Vulnerability Assessment

CEH
Certified Ethical Hacker

Network Scanning

Vulnerability assessment scans a network for known **security weaknesses**

Scanning Tools

Vulnerability scanning tools search network segments for **IP-enabled devices** and **enumerate systems**, OS's, and applications

Security Mistakes

Additionally, vulnerability scanners can identify common **security configuration mistakes**

Test Systems/Network

Vulnerability scanners can test systems and network devices for **exposure to common attacks**

Vulnerability Assessment

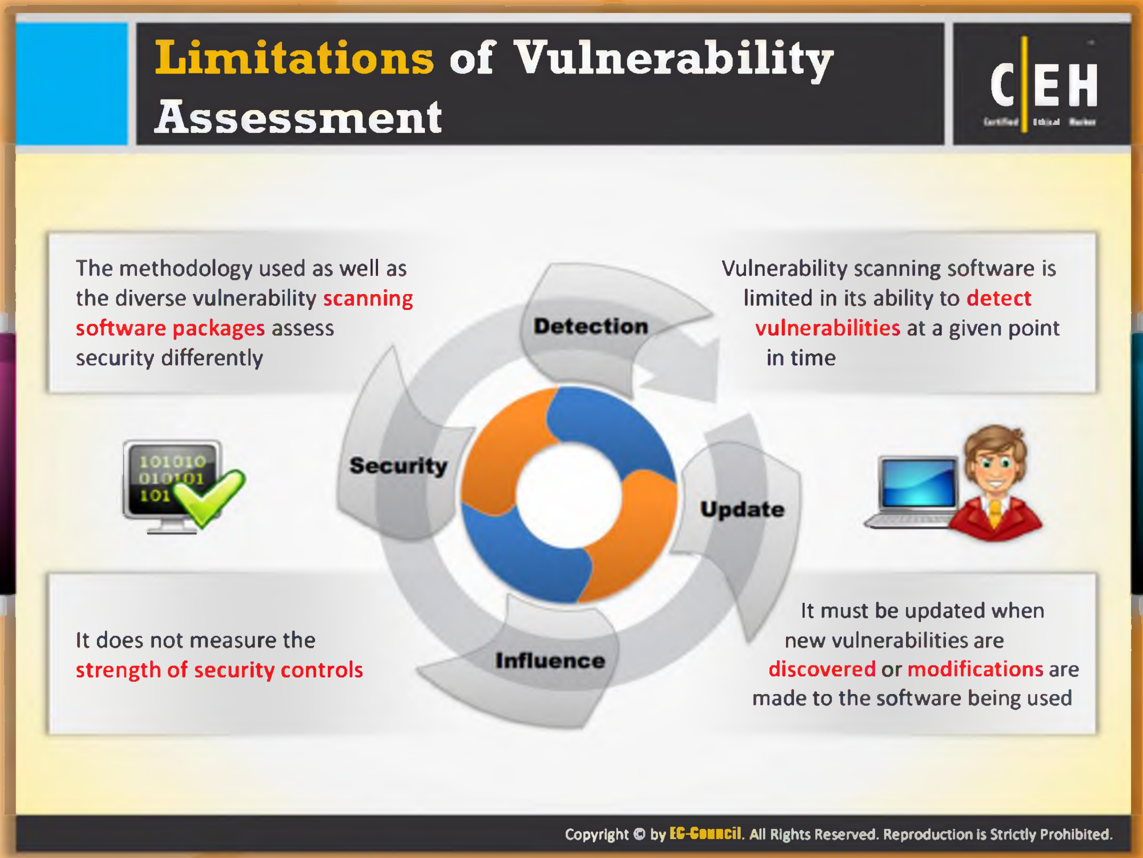
A vulnerability assessment is a basic type of security. This assessment helps you in finding the known security weaknesses by scanning a network. With the help of vulnerability-scanning tools, you can search network segments for **IP-enabled devices** and **enumerate systems, operating systems,** and **applications**. Vulnerability scanners are capable of identifying device configurations including the OS version running on computers or devices, IP protocols and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening, and applications that are installed on computers.

By using vulnerability scanners, you can also identify common security mistakes such as accounts that have weak passwords, files and folders with weak permissions, default services and applications that might need to be uninstalled, and mistakes in the security configuration of common applications. They can search for computers exposed to known or publicly reported vulnerabilities. The software packages that perform vulnerability scanning scan the computer against the Common Vulnerability and Exposures (CVE) index and security bullets provided by the software vendor. The CVE is a **vendor-neutral** listing of reported security vulnerabilities in major operating systems and applications and is maintained at http://cve.mitre.org/.

Vulnerability scanners can test systems and network devices for exposure to common attacks. This includes common attacks such as the enumeration of security-related information and denial-of-service attacks. However, it must be noted that vulnerability scanning reports can expose weaknesses in hidden areas of applications and frequently include many false positives. Network administrators who analyze vulnerability scan results must have sufficient knowledge and experience with the operating systems, network devices, and applications being scanned and their roles in the network.

You can use two types of automated vulnerability scanners depending upon the situation: network-based and host-based. Network-based scanners attempt to detect vulnerabilities from the outside. They are normally launched from a remote system, outside the organization, and without an authorized user access. For example, **network-based scanners examine** a system for such exploits as open ports, application security exploits, and buffer overflows.

Host-based scanners usually require a software agent or client to be installed on the host. The client then reports back the vulnerabilities it finds to the server. Host-based scanners look for features such as weak file access permissions, poor passwords, and logging faults.



Limitations of Vulnerability Assessment

The methodology used as well as the diverse vulnerability scanning software packages assess security differently

Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

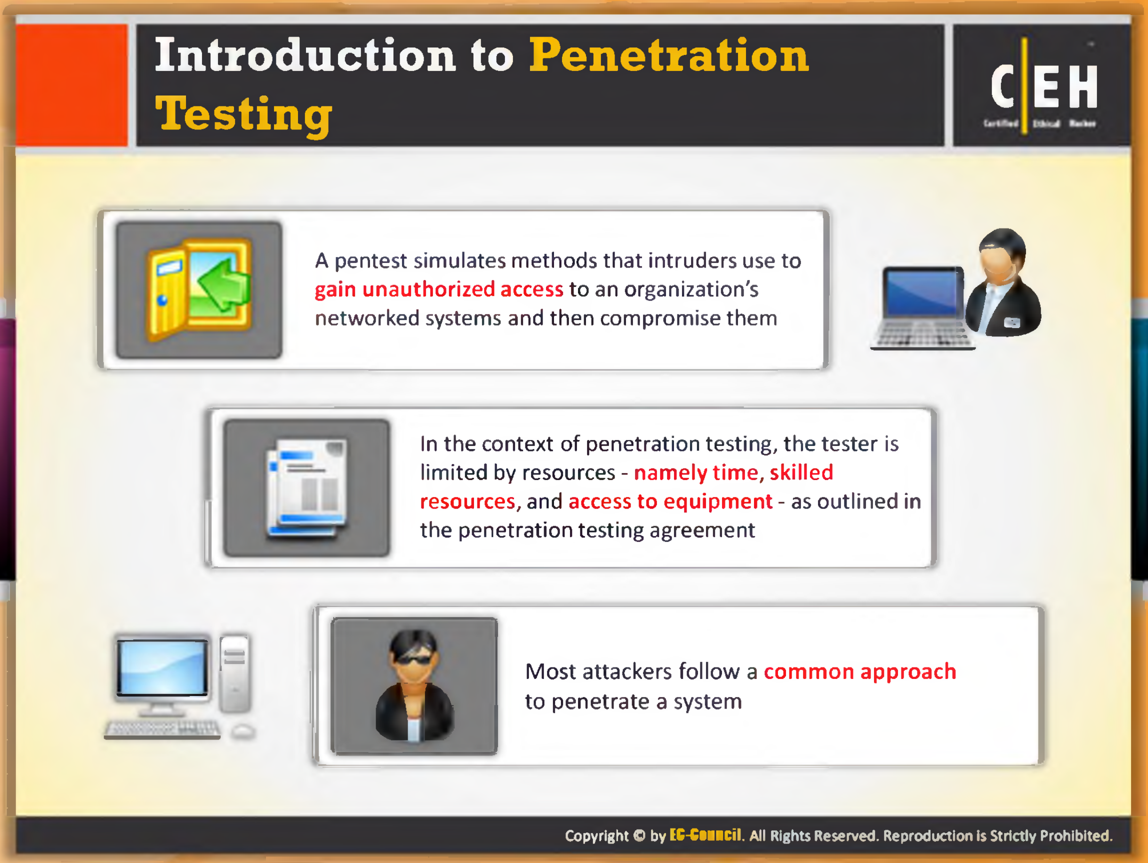
It does not measure the strength of security controls

It must be updated when new vulnerabilities are discovered or modifications are made to the software being used

Limitations of Vulnerability Assessment

Vulnerability scanning software allows you to detect limited vulnerabilities at a given point in time. As with any assessment software, which requires the signature file to be updated, vulnerability scanning software must be updated when new vulnerabilities are discovered or improvements made to the software are being used. The vulnerability software is only as effective as the maintenance performed on it by the software vendor and by the administrator who uses it. Vulnerability scanning software itself is not immune to software engineering flaws that might lead to non-detection of serious vulnerabilities.

Another aspect to be noted is that the methodology used might have an impact on the result of the test. For example, vulnerability scanning software that runs under the security context of the domain administrator will yield different results than if it were run under the security context of an authenticated user or a non-authenticated user. Similarly, diverse vulnerability scanning software packages assess security differently and have unique features. This can influence the result of the assessment. Examples of vulnerability scanners include Nessus and Retina.



Introduction to Penetration Testing

A pentest simulates methods that intruders use to **gain unauthorized access** to an organization's networked systems and then compromise them

In the context of penetration testing, the tester is limited by resources - **namely time**, **skilled resources**, and **access to equipment** - as outlined in the penetration testing agreement

Most attackers follow a **common approach** to penetrate a system

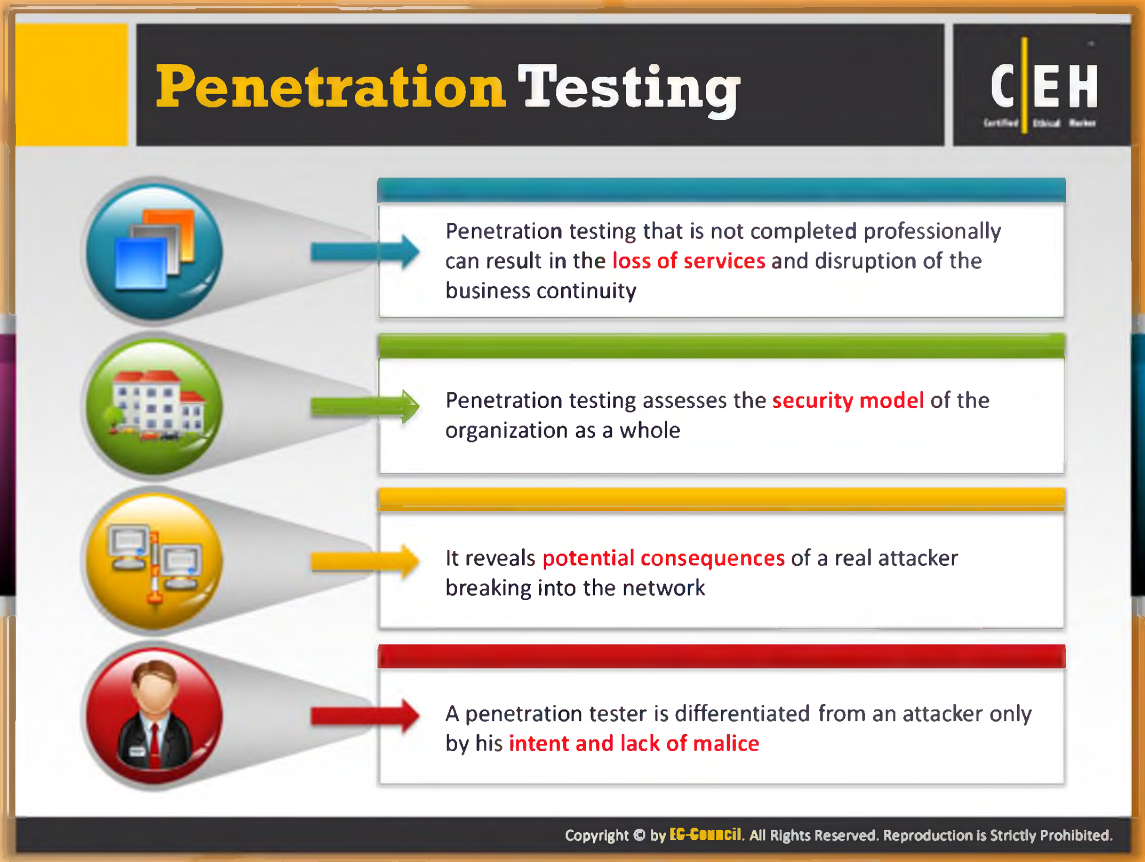
Introduction to Penetration Testing

This module marks a departure from the approach followed in earlier modules; here you will be encouraged to think "**outside** the **box**." Hacking as it was defined originally portrayed a streak of genius or brilliance in the ability to conjure previously unknown ways of doing things. In this context, to advocate a methodology that can be followed to simulate a real-world hack through ethical hacking or penetration testing might come across as a contradiction. Penetration testing is a process of evaluating the security of the network by trying all possible attack vectors like an attacker does. The reason behind advocating a methodology in penetration testing arises from the fact that most attackers follow a common underlying approach when it comes to penetrate a system.

In the context of penetration testing, as a tester you will be limited by resources such as time, skilled resources, and access to equipment, as outlined in the penetration testing agreement. The paradox of penetration testing is the fact that the inability to breach a target does not necessarily indicate the absence of **vulnerability**. In other words, to maximize the returns from a penetration test, you must be able to apply your skills to the resources available in such a manner that the attack area of the target is reduced as much as possible.

A pen test simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them. It involves using proprietary and open source tools to test for known and unknown technical vulnerabilities in networked systems. Apart from automated techniques, penetration testing involves manual techniques for conducting targeted testing on specific systems to ensure that there are no **security flaws** that may have gone undetected earlier.

The main purpose behind **footprinting** pen testing is to gather data related to a target system or network and find out its vulnerabilities. You can perform this through various techniques such as DNS queries, network enumeration, network queries, **operating system identification**, organizational queries, ping sweeps, point of contact queries, port scanning, registrar queries, and so on.



Penetration Testing

- Penetration testing that is not completed professionally can result in the loss of services and disruption of the business continuity
- Penetration testing assesses the security model of the organization as a whole
- It reveals potential consequences of a real attacker breaking into the network
- A penetration tester is differentiated from an attacker only by his intent and lack of malice

Penetration Testing

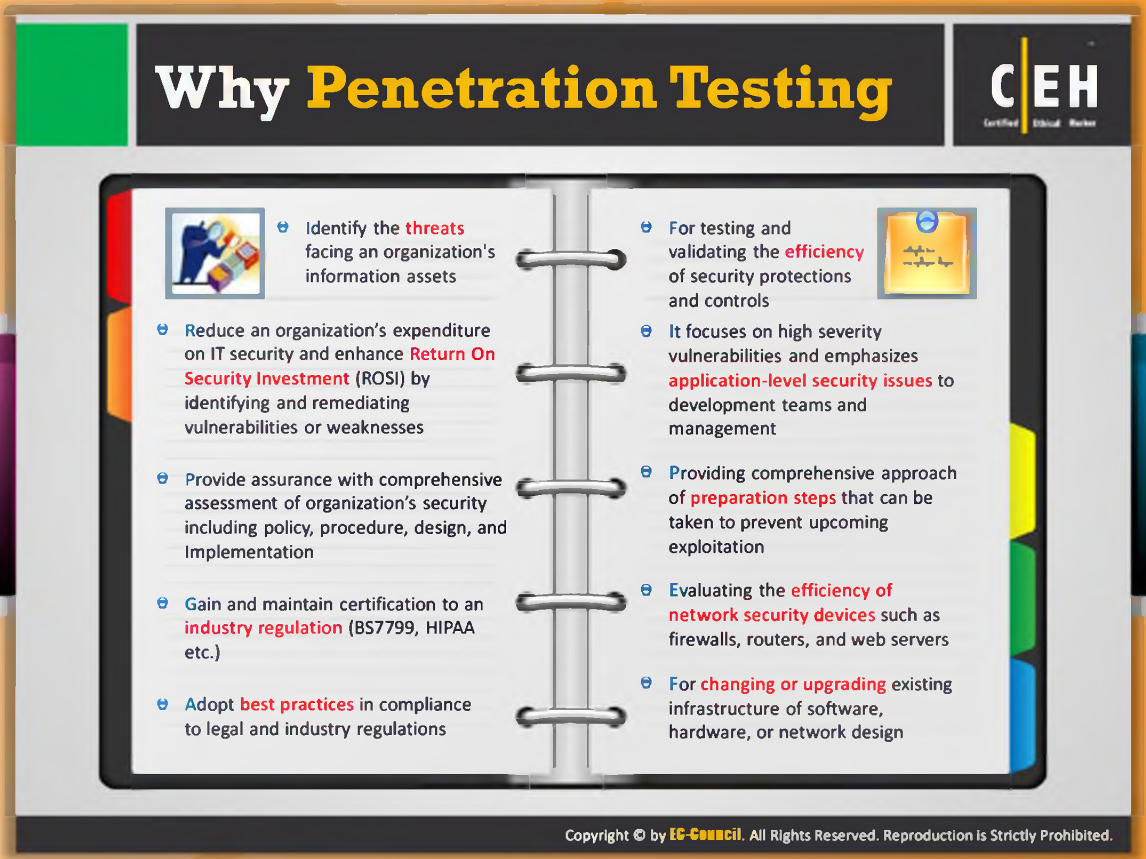
Penetration testing goes a step beyond vulnerability scanning in the category of security assessments. With vulnerability scanning, you can only examine the security of the individual computers, network devices, or applications, but penetration testing allows you to assess the security model of the network as a whole. Penetration testing can help you to reveal potential consequences of a real attacker breaking into the network to **network administrators, IT managers, and executives**. Penetration testing also reveals the security **weaknesses** that a typical vulnerability scanning misses.

A penetration test will not only point out vulnerabilities, it will also document how the weaknesses can be exploited and how several minor vulnerabilities can be escalated by an attacker to compromise a computer or network. Penetration testing must be considered as an activity that shows the holes in the security model of an organization. Penetration testing helps organizations to reach a balance between technical prowess and business functionality from the perspective of **potential security breaches**. This test can help you in disaster recovery and **business continuity planning**.

Most vulnerability assessments are carried out solely based on **software** and cannot assess security that is not related to technology. Both people and processes can be the source of security vulnerabilities as much as the technology can be. Using social engineering techniques, penetration tests can reveal whether employees routinely allow people without identification to enter company facilities and where they would have physical access to computers. Practices such as patch management cycles can be evaluated. A penetration test can reveal process problems, such as not applying security updates until three days after they are released, which would give attackers a **three-day window** to exploit known vulnerabilities on servers.

You can differentiate a penetration tester from an attacker only by his ot her intent and lack of malice. Therefore, employees or external experts must be cautioned against conducting penetration tests without proper authorization. Penetration testing that is not completed professionally can result in the loss of services and **disruption** of **business continuity**.

Management needs to give written approval for penetration testing. This approval should include a clear scoping, a description of what will be tested, and when the testing will take place. Because of the nature of penetration testing, failure to obtain this approval might result in committing computer crime, despite the best intentions.



Why Penetration Testing

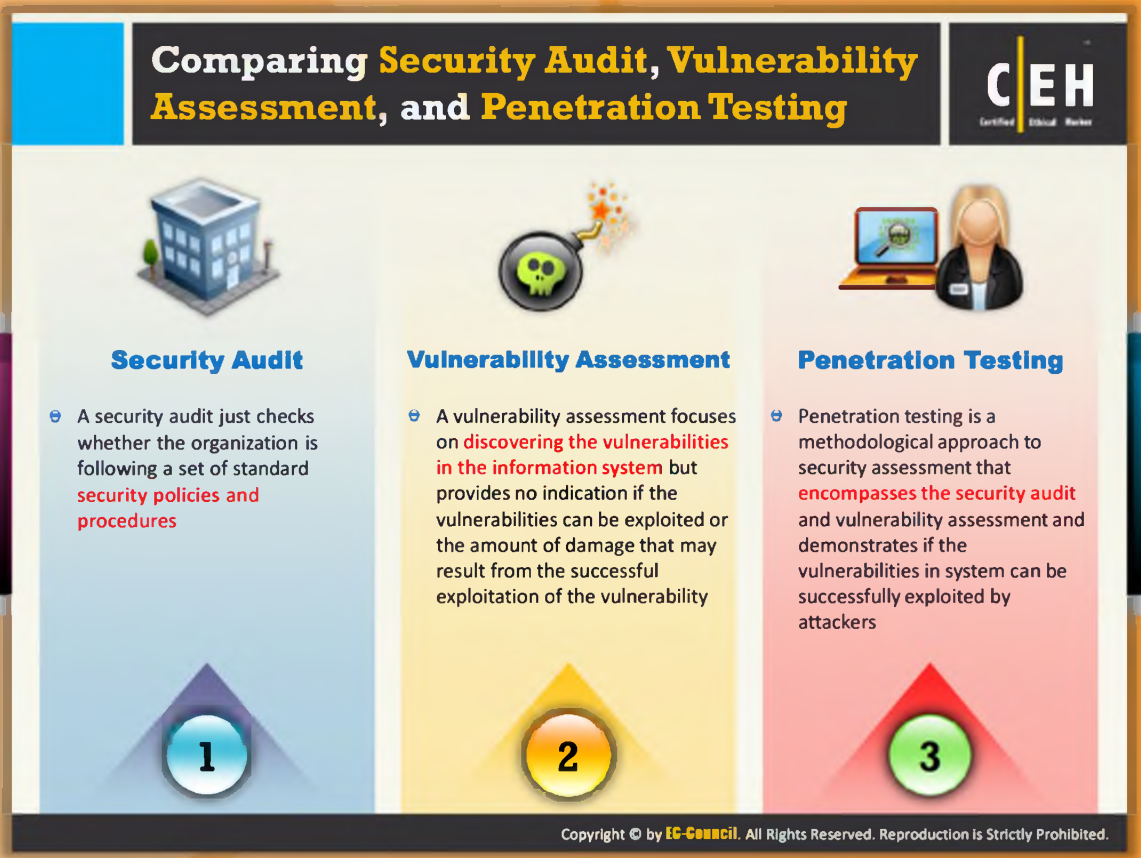
- Identify the threats facing an organization's information assets
- Reduce an organization's expenditure on IT security and enhance Return On Security Investment (ROSI) by identifying and remediating vulnerabilities or weaknesses
- Provide assurance with comprehensive assessment of organization's security including policy, procedure, design, and Implementation
- Gain and maintain certification to an industry regulation (BS7799, HIPAA etc.)
- Adopt best practices in compliance to legal and industry regulations
- For testing and validating the efficiency of security protections and controls
- It focuses on high severity vulnerabilities and emphasizes application-level security issues to development teams and management
- Providing comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
- Evaluating the efficiency of network security devices such as firewalls, routers, and web servers
- For changing or upgrading existing infrastructure of software, hardware, or network design

Why Penetration Testing?

Penetration testing plays a vital role in evaluating and maintaining security of a system or network. It helps you in finding out the loopholes by deploying attacks. It includes both script-based testing as well as human-based testing on networks. A penetration test not only reveals network security holes, but also provides risk assessment. Let's see what you can do with the help of penetration testing:

- You can identify the threats facing an organization's information assets.
- You can reduce an organization's IT security costs and provide a better Return On IT Security Investment (ROSI) by identifying and resolving vulnerabilities and weaknesses.
- You can provide an organization with assurance: a thorough and comprehensive assessment of organizational security covering policy, procedure, design, and implementation.
- You can gain and maintain certification to an industry regulation (BS7799, HIPAA, etc.).
- You can adopt best practices by conforming to legal and industry regulations.
- You can test and validate the efficiency of security protections and controls.
- It focuses on high-severity vulnerabilities and emphasizes application-level security issues to development teams and management.

- It provides a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation.
- You can evaluate the efficiency of network security devices such as firewalls, routers, and web servers.
- You can use it for changing or **upgrading existing infrastructure** of software, hardware, or network design.



Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

Security Audit

- A security audit just checks whether the organization is following a set of standard security policies and procedures

Vulnerability Assessment

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

Penetration Testing

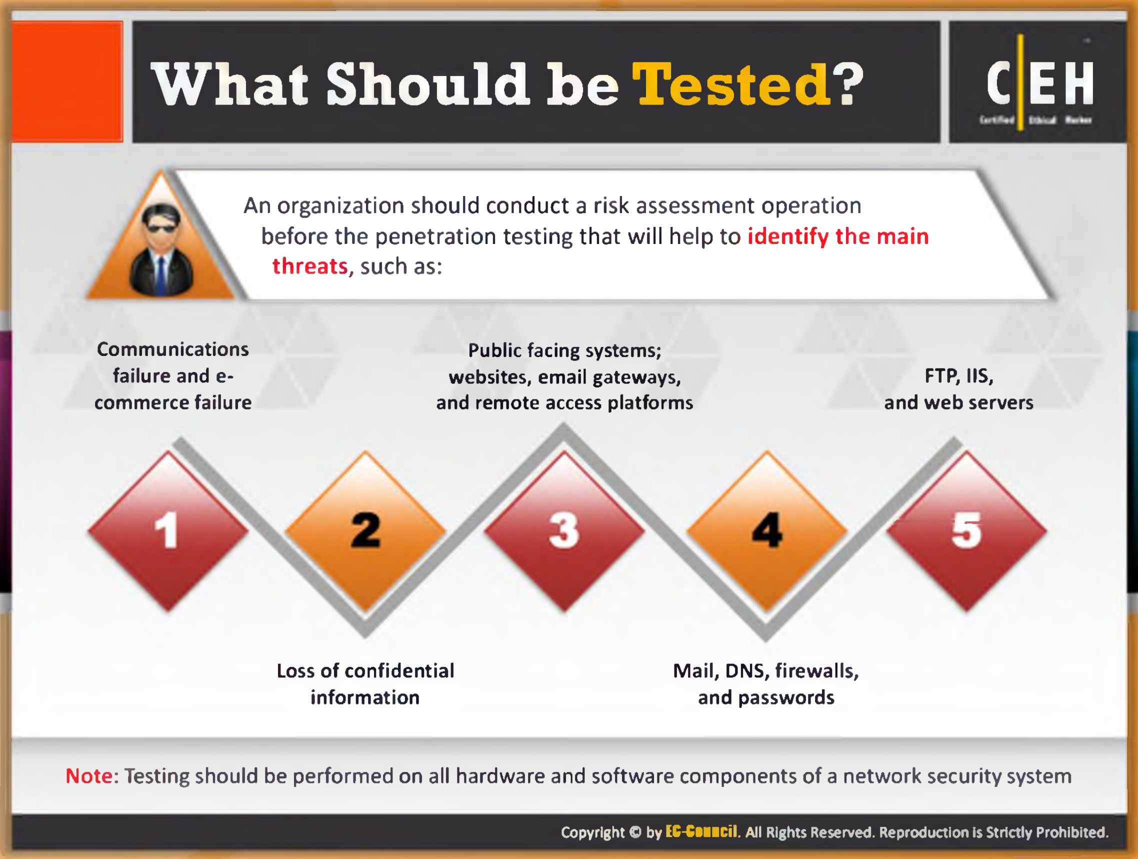
- Penetration testing is a methodological approach to security assessment that encompasses the security audit and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attackers

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

Although a lot of people use the terms security audit, vulnerability assessment, and penetration test interchangeably to mean security assessment, there are considerable differences between them.

Security Audit	Vulnerability Assessment	Penetration Testing
A security audit just checks whether the organization is following a set of standard security policies and procedures	A vulnerability assessment focuses on discovering the vulnerabilities in the information system but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability	Penetration testing is a methodological approach to security assessment that encompasses the security audit and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attackers

TABLE 20.1: Comparison between Security Audit, Vulnerability Assessment, and Penetration Testing



What Should be Tested?

An organization should conduct a risk assessment operation before the penetration testing that will help to **identify the main threats**, such as:

Communications failure and e-commerce failure

Public facing systems; websites, email gateways, and remote access platforms

FTP, IIS, and web servers

Loss of confidential information

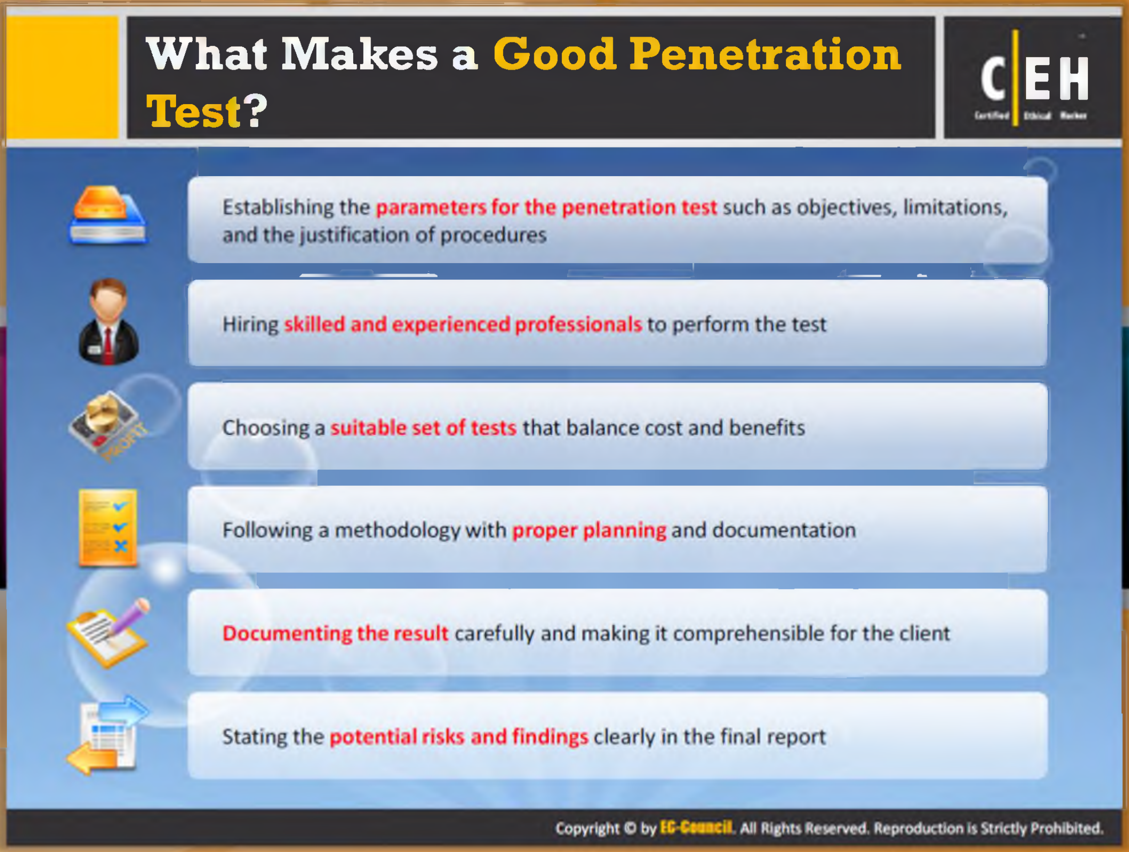
Mail, DNS, firewalls, and passwords

Note: Testing should be performed on all hardware and software components of a network security system

What Should be Tested?

It is always ideal to conduct a vulnerability assessment in an organization so that various potential threats can be known well before they occur. You can test various network or system components for **security vulnerabilities**, such as:

- Communication failure
- E-commerce failure
- Loss of confidential information
- Public facing systems websites
- Email gateways
- Remote access platforms
- Mail
- DNS
- Firewalls
- Passwords
- FTP
- IIS
- Web servers



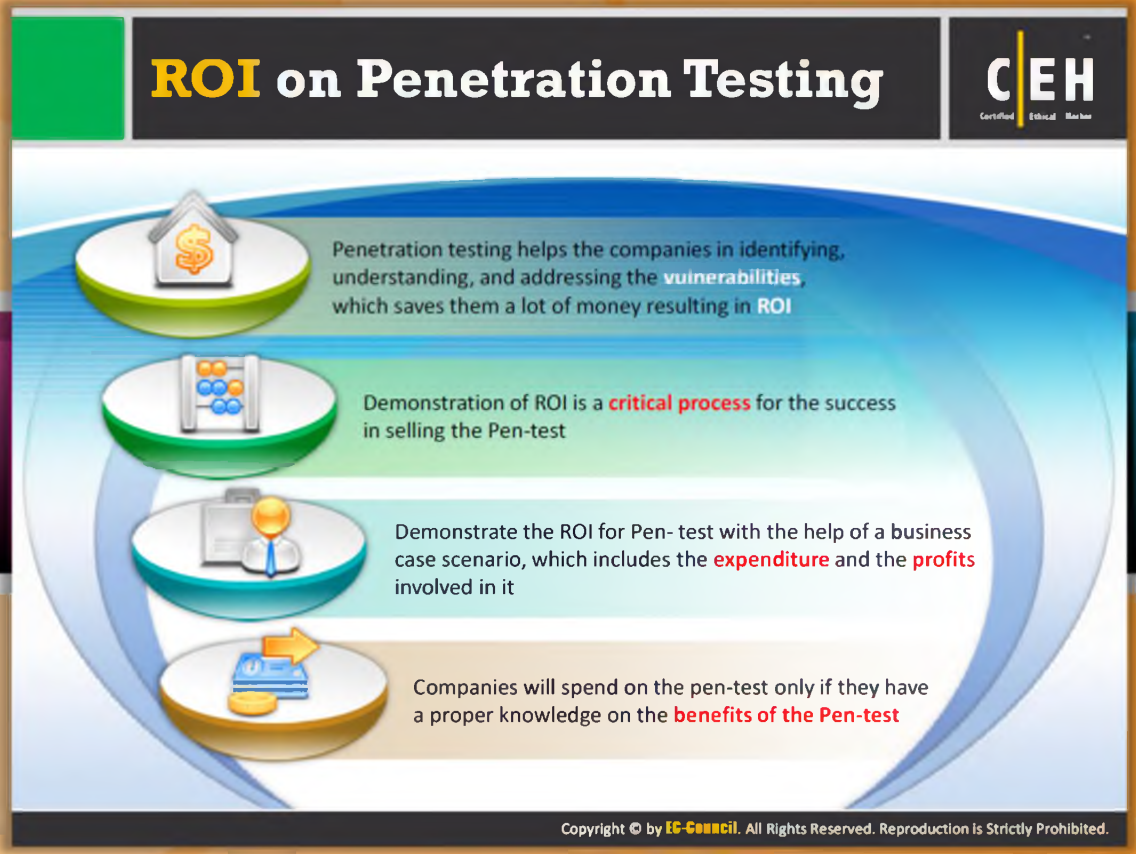
What Makes a Good Penetration Test?

- Establishing the parameters for the penetration test such as objectives, limitations, and the 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
- Stating the potential risks and findings clearly in the final report

What Makes a Good Penetration Test?

Consider the following factors to perform a good penetration test:

- Establish the parameters for the penetration test such as objectives, limitations, and the justification of procedures. The establishment of these parameters helps you in know the purpose of conducting penetration test.
- Hire skilled and experienced professionals to perform the test. If the penetration testing is not done by the skilled and experienced professionals there are chances of damaging the live data and more harm can happen than the benefits.
- Choose a suitable set of tests that balance cost and benefits.
- Follow a methodology with proper planning and documentation. It is very important to document the test at each phase for the further references.
- Document the result carefully and making it comprehensible for the client.
- State the potential risks and findings clearly in the final report.



ROI on Penetration Testing

CEH
Certified Ethical Hacker

Penetration testing helps the companies in identifying, understanding, and addressing the vulnerabilities, which saves them a lot of money resulting in ROI

Demonstration of ROI is a critical process for the success in selling the Pen-test

Demonstrate the ROI for Pen- test with the help of a business case scenario, which includes the expenditure and the profits involved in it

Companies will spend on the pen-test only if they have a proper knowledge on the benefits of the Pen-test

ROI on Penetration Testing

ROI (return on investment) is a traditional financial measure. It is used to determine the business results of for the future based on the calculations of historical data. The ROI is calculated based on three things:

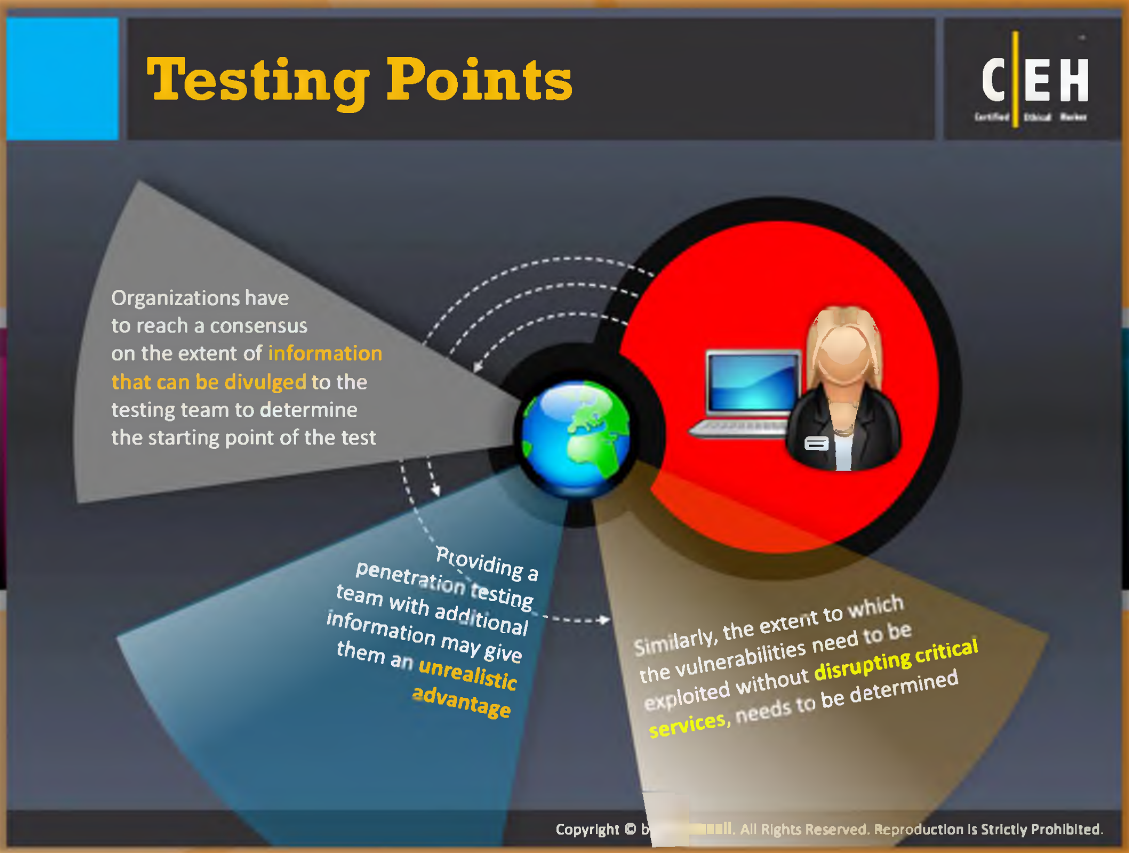
- **Payback period:** In this method the time taken to get the pay back (getting the amount invested) on a particular project is calculated.
- **Net present value:** Future benefits are calculated in the terms of today's money.
- **Internal rate of return:** The benefits based on the interest rate.

So whenever a penetration test is conducted, a company checks what kinds of benefits are there associated with the penetration testing. What could be the costs to be incurred for the for penetration testing? Costs related to the hiring of skilled professionals?

All these things to be kept in view and penetration testing should be conducted through proper planning.

- Penetration testing helps companies in identifying, understanding, and addressing vulnerabilities, which saves them a lot of money resulting in ROI.

- Demonstrate the ROI for a pen test with the help of a **business case scenario**, which includes the expenditure and the profits involved in it.



Testing Points

Organizations have to reach a consensus on the extent of information that can be divulged to the testing team to determine the starting point of the test

Providing a penetration testing team with additional information may give them an unrealistic advantage

Similarly, the extent to which the vulnerabilities need to be exploited without disrupting critical services, needs to be determined

Testing Points

Every penetration test will have a start- and end-point, irrespective of whether it is zero knowledge or partial knowledge test. How does a pen test team or an organization determine this? While providing a penetration-testing team with information such as the exact configuration of the firewall used by the target network may speed up the testing, it can work negatively by providing the testers with an unrealistic advantage.

If the objective of the penetration effort is to find as much vulnerability as possible, it might be a good idea to opt for white box testing and share as much information as possible with the testers. This can help in detecting hidden vulnerabilities that are often undetected because of obscurity. On the other hand, if the purpose of the penetration test is to evaluate the effectiveness of the security posture of the organization—irrespective of any "security by obscurity" measures—withholding information will derive more realistic results.

Similarly, by making highly sensitive information, such as the names and user IDs of system administrators, the organization may be defeating the purpose of a comprehensive pen test. Therefore, balance must be reached between assisting the testing team in conducting their test faster and providing a more realistic testing environment by restricting information.

Some organizations may choose to get the initial pen test audited by a second pen test team so that there is a third party assurance on the results obtained.

Testing Locations

The pentest team may have a choice of doing the test either remotely or on-site

A remote assessment may simulate an external hacker attack. However, it may miss assessing internal guards

An on-site assessment may be expensive and may not simulate an external threat exactly

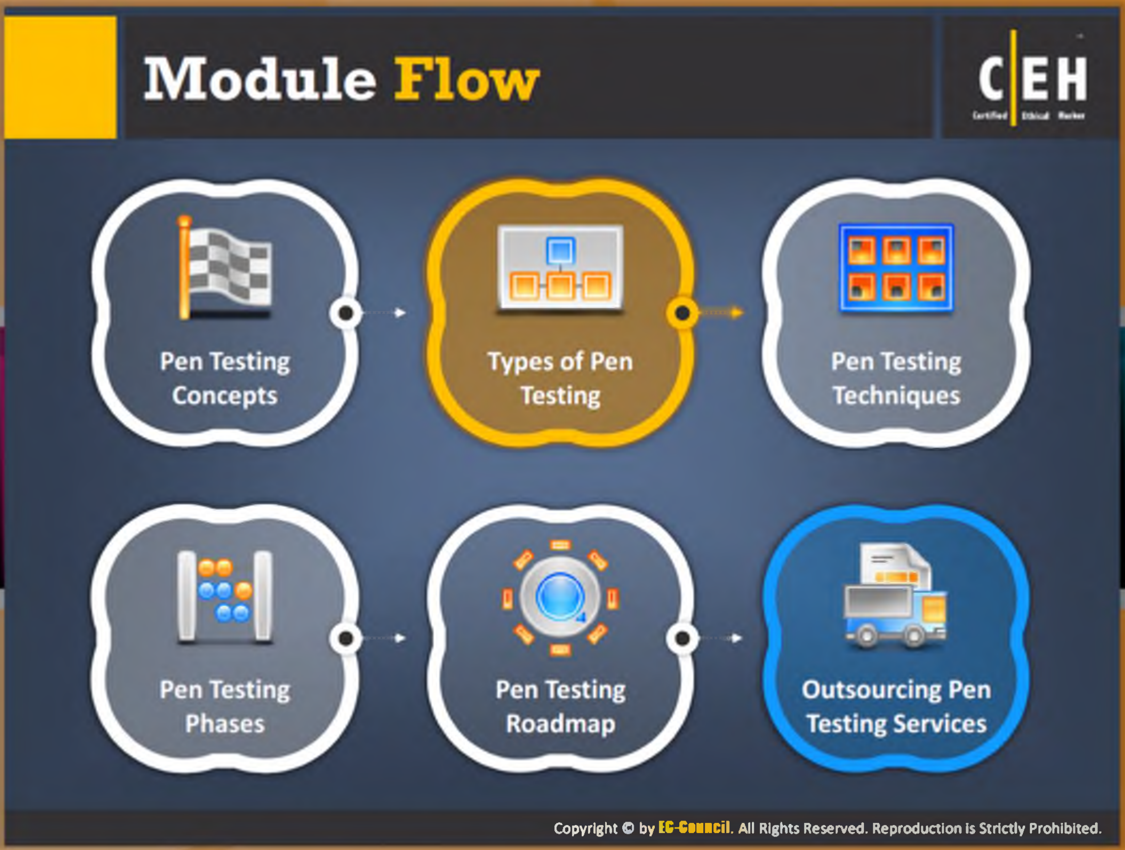
Testing Locations

The penetration test team may have a preference on the location from where they would probe the network. Alternatively, the organization may want the network to be assessed from a remote location. If the pen test team is based overseas, an **onsite assessment** may be expensive than a remote one.

The location of the assessment has an influence on the test results. Testing over the Internet may provide a more realistic test environment. However, the pen test team may learn little if there is a well-configured perimeter firewall and robust web application defenses. A purely external assessment may not be able to test any additional inner network defenses put in place to guard against an internal intruder.

Sometimes, the organization may have a network that is dispersed geographically across locations and that contains several systems. In this case, the organization may choose to prioritize locations or the team may choose locations depending on **critical applications**.

If a complete knowledge test is being undertaken, the pen test team can undertake an asset audit to determine which systems are critical to the business, and plan the test accordingly.

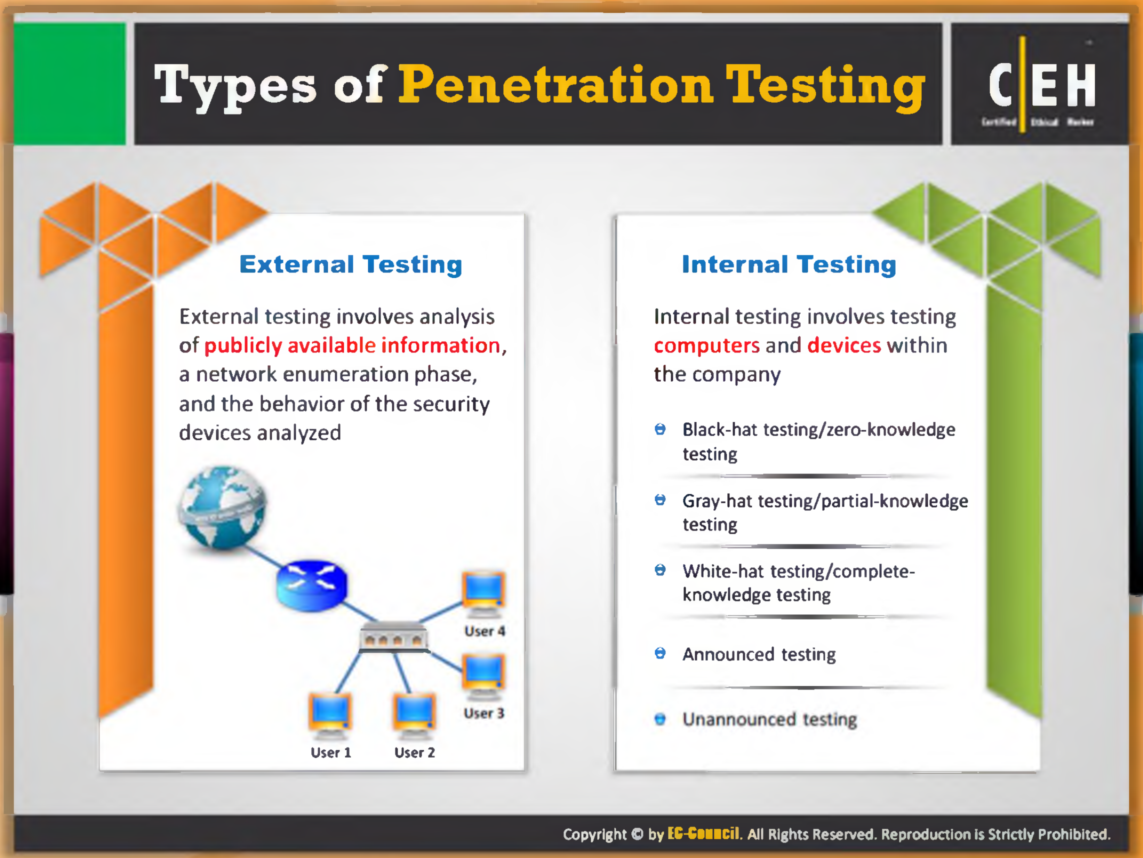


Module Flow

So far, we have discussed various pen testing concepts. Depending on the scope of operation and time required for conducting a pen test, the tester can choose the appropriate type of penetration testing. The selection of the particular type of penetration testing depends upon the type of resources to be protected against attacks. Now, we will discuss various types of pen testing.

Pen Testing Concepts	Types of Pen Testing
Pen Testing Techniques	Pen Testing Phases
Pen Testing Roadmap	Outsourcing Pen Testing Services

In this section, you will learn different types of penetration testing such as external testing, internal testing, Black-box, gray-box penetration testing, white-box penetration testing, announced/unannounced testing, automated testing, and manual testing.



Types of Penetration Testing

External Testing

External testing involves analysis of publicly available information, a network enumeration phase, and the behavior of the security devices analyzed

Internal Testing

Internal testing involves testing computers and devices within the company

- Black-hat testing/zero-knowledge testing
- Gray-hat testing/partial-knowledge testing
- White-hat testing/complete-knowledge testing
- Announced testing
- Unannounced testing

Types of Penetration Testing

Penetration testing is broadly divided into two types. They are:

External Testing

External penetration testing is the conventional approach to penetration testing. The testing is focused on the servers, infrastructure, and underlying software pertaining to the target. It may be performed with no prior knowledge of the site (black box) or with full disclosure of the topology and environment (white box). This type of testing will take in a comprehensive analysis of publicly available information about the target.

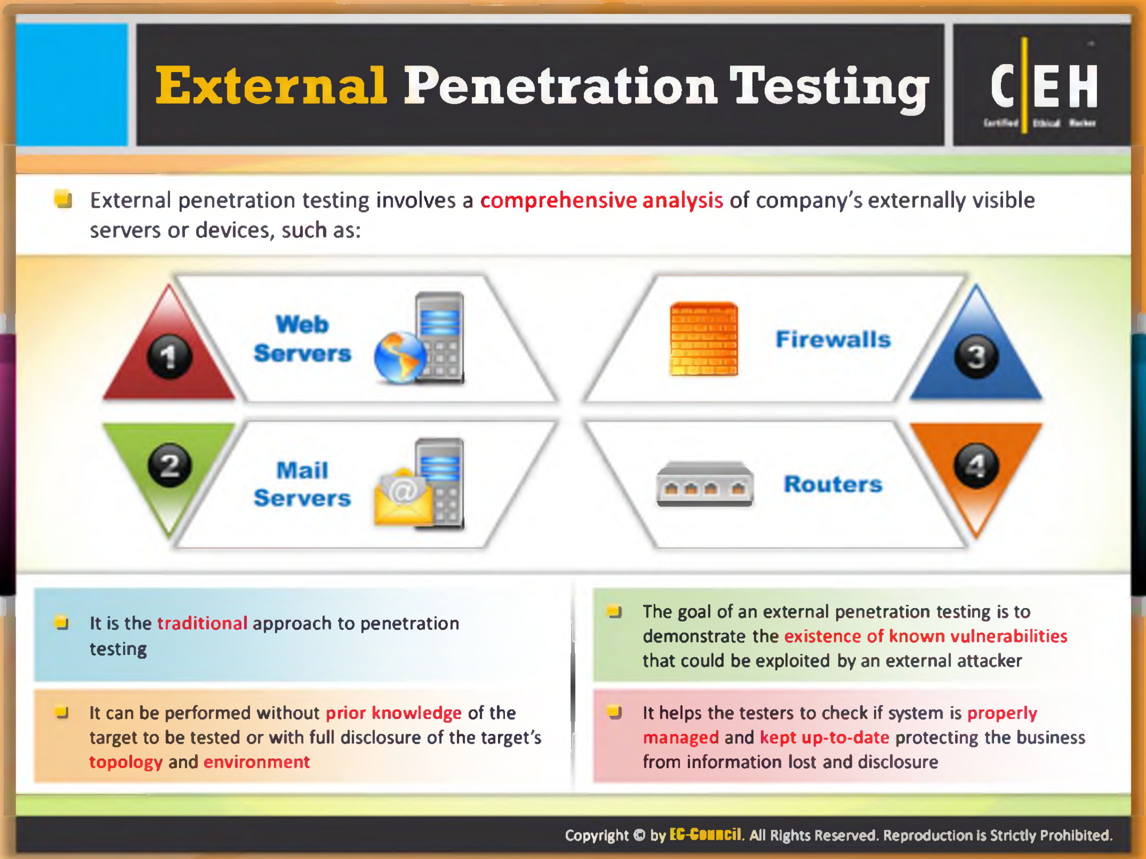
Internal Testing

Internal testing makes use of similar methods as the external testing, and it is considered to be a more versatile view of the security. Testing will be performed from several network access points, including both logical and physical segments.

It is critical to note that despite everything, information security is an ongoing process and penetration testing only gives a snapshot of the security posture of an organization at any given point in time.

Internal testing will be performed from a number of network access points, representing each logical and physical segment. The following tests comes fall under internal testing:

- Black-hat testing/zero-knowledge testing
- Gray-hat testing/partial-knowledge testing
- White-hat testing/complete-knowledge testing
- Announced testing
- Unannounced testing



External Penetration Testing

- External penetration testing involves a comprehensive analysis of company's externally visible servers or devices, such as:

1
Web Servers
2
Mail Servers
3
Firewalls
4
Routers

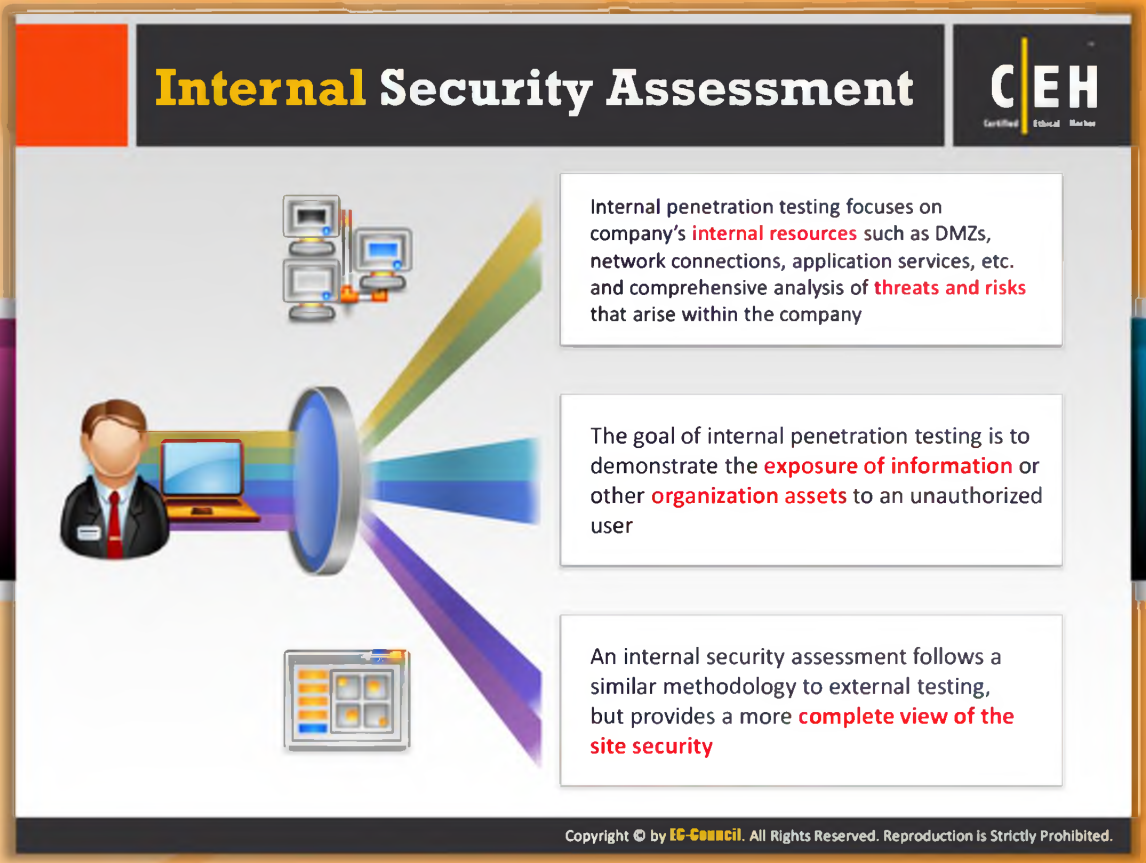
- It is the traditional approach to penetration testing
- It can be performed without prior knowledge of the target to be tested or with full disclosure of the target's topology and environment
- The goal of an external penetration testing is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker
- It helps the testers to check if system is properly managed and kept up-to-date protecting the business from information lost and disclosure

External Penetration Testing

A pen tester conducts external penetration test for determining the external threats to the network or system. The attacker can perform an external attack without accessing a system by using credentials or the appropriate rights. The main aim behind conducting this pen test is to **identify potential weaknesses** in the security of target network system.

External testing is focused on the servers, infrastructure, and underlying software pertaining to the target. It may be performed with no prior knowledge of the site (black box) or with full disclosure of the topology and environment (white box).

This type of testing will take in a comprehensive analysis of publicly available information about the target, a network enumeration phase where target hosts are identified and analyzed, and the behavior of security devices such as **screening network-filtering devices**. Vulnerabilities are then identified and verified, and the implications assessed. It is the traditional approach to penetration testing.



Internal Security Assessment

Internal penetration testing focuses on company's internal resources such as DMZs, network connections, application services, etc. and comprehensive analysis of threats and risks that arise within the company

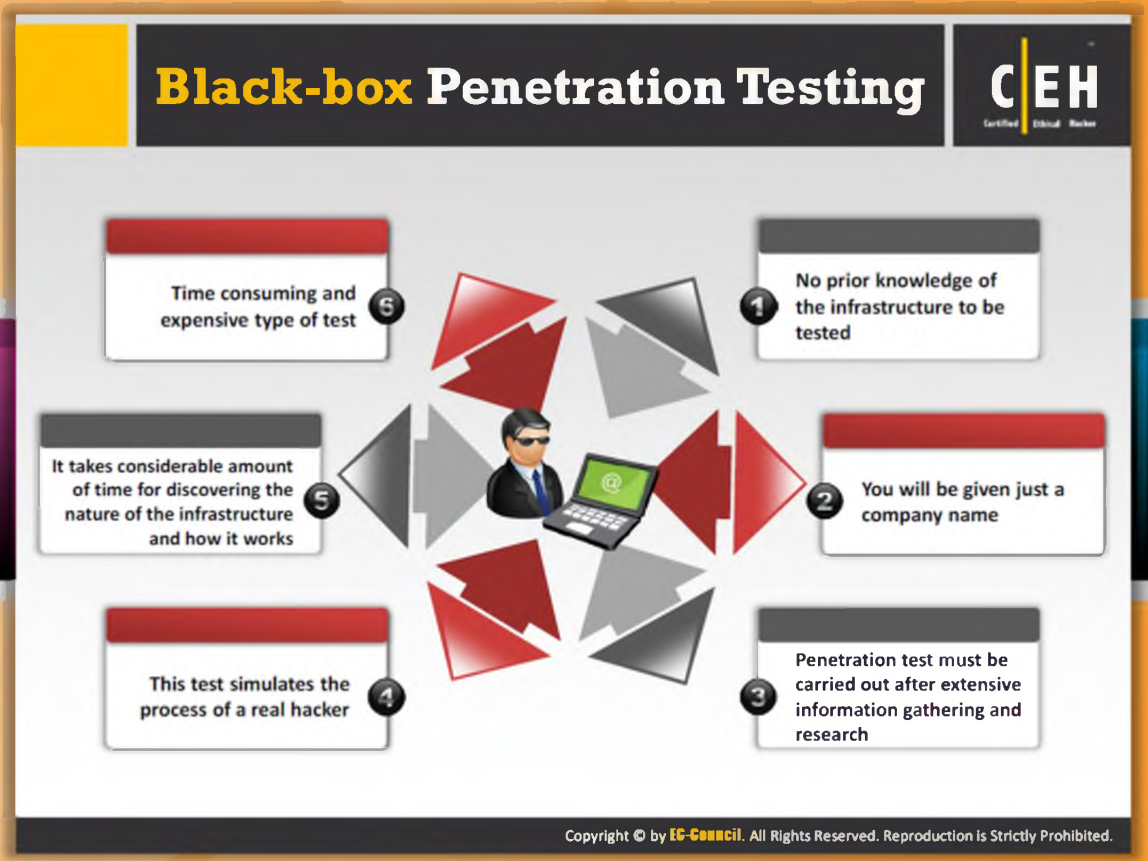
The goal of internal penetration testing is to demonstrate the exposure of information or other organization assets to an unauthorized user

An internal security assessment follows a similar methodology to external testing, but provides a more complete view of the site security

Internal Security Assessment

A pen tester conducts internal penetration testing in order to ensure nobody can access the system inside network by misusing user privileges. It is used to identify the weaknesses of computer system inside the particular network. The internal security assessment gives a clear view of the site's security. Internal security assessment has similar methodology like external penetration testing. The main purpose behind the **internal penetration testing** is to find out the various vulnerabilities inside the network. Risks associated with security aspects are carefully checked. Exploitation can be done by a hacker, a malicious employee, etc.:

- Testing will be performed from a number of network access points, representing each logical and physical segment.
- For example, this may include tiers and DMZs within the environment, the corporate network, or partner company connections.



Black-box Penetration Testing

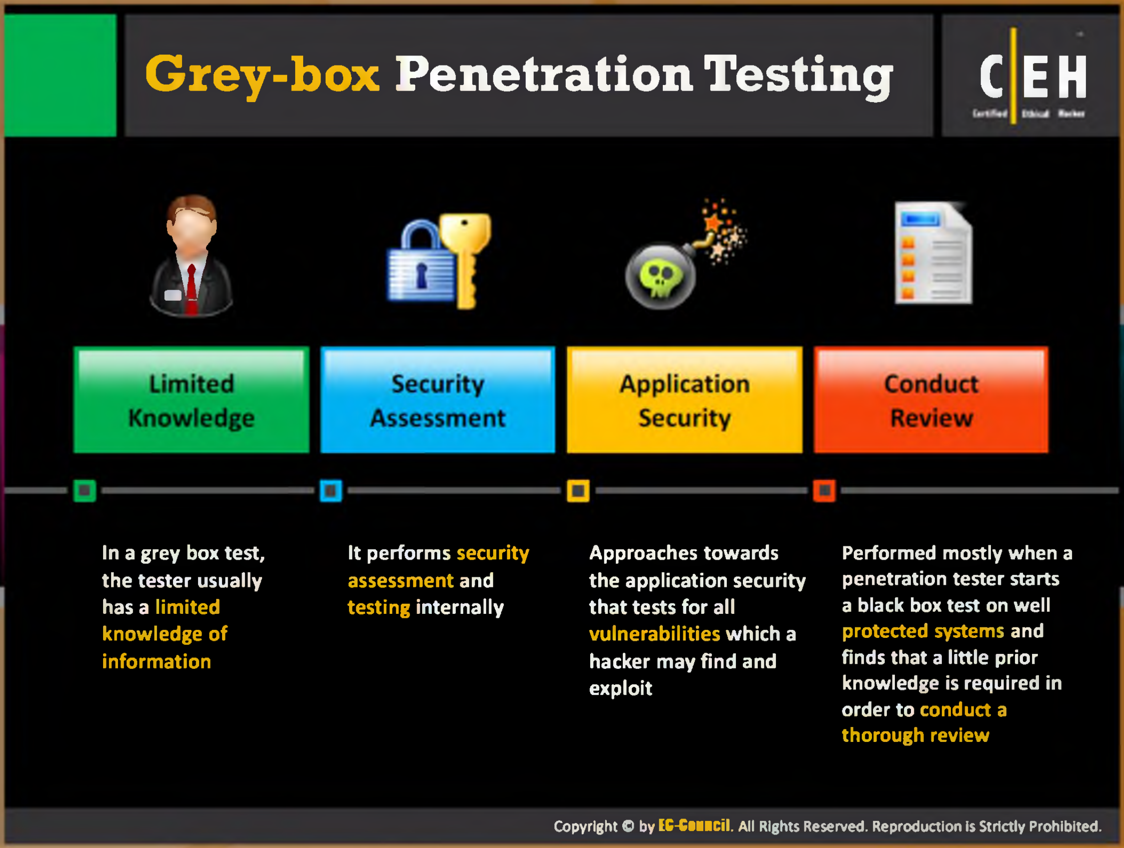
1. No prior knowledge of the infrastructure to be tested
2. You will be given just a company name
3. Penetration test must be carried out after extensive information gathering and research
4. This test simulates the process of a real hacker
5. It takes considerable amount of time for discovering the nature of the infrastructure and how it works
6. Time consuming and expensive type of test

Black-box Penetration Testing

In black-box testing, a pen tester carries out the test without having any prior knowledge the target. In order to simulate **real-world attacks** and minimize false positives, pen testers can choose to undertake black-hat testing (or a zero-knowledge attack, with no information or assistance from the client) and map the network while enumerating services, shared file systems and operating systems discreetly. Additionally, the pen tester can undertake war dialing to detect listening modems and war driving to discover vulnerable access points if it is legal and within the scope of the project.

The following points summarize the black-box pen testing:

- It does not require prior knowledge of the infrastructure to be tested
- Penetration test must be carried out after extensive information gathering and research
- It takes a considerable amount of time for the project to discover the nature of the **infrastructure** and how it connects and **interrelates**
- You will be given only a company name
- This test simulates the process of a real hacker
- Time consuming and expensive type of test



Grey-box Penetration Testing

Limited Knowledge

In a grey box test, the tester usually has a limited knowledge of information

Security Assessment

It performs security assessment and testing internally

Application Security

Approaches towards the application security that tests for all vulnerabilities which a hacker may find and exploit

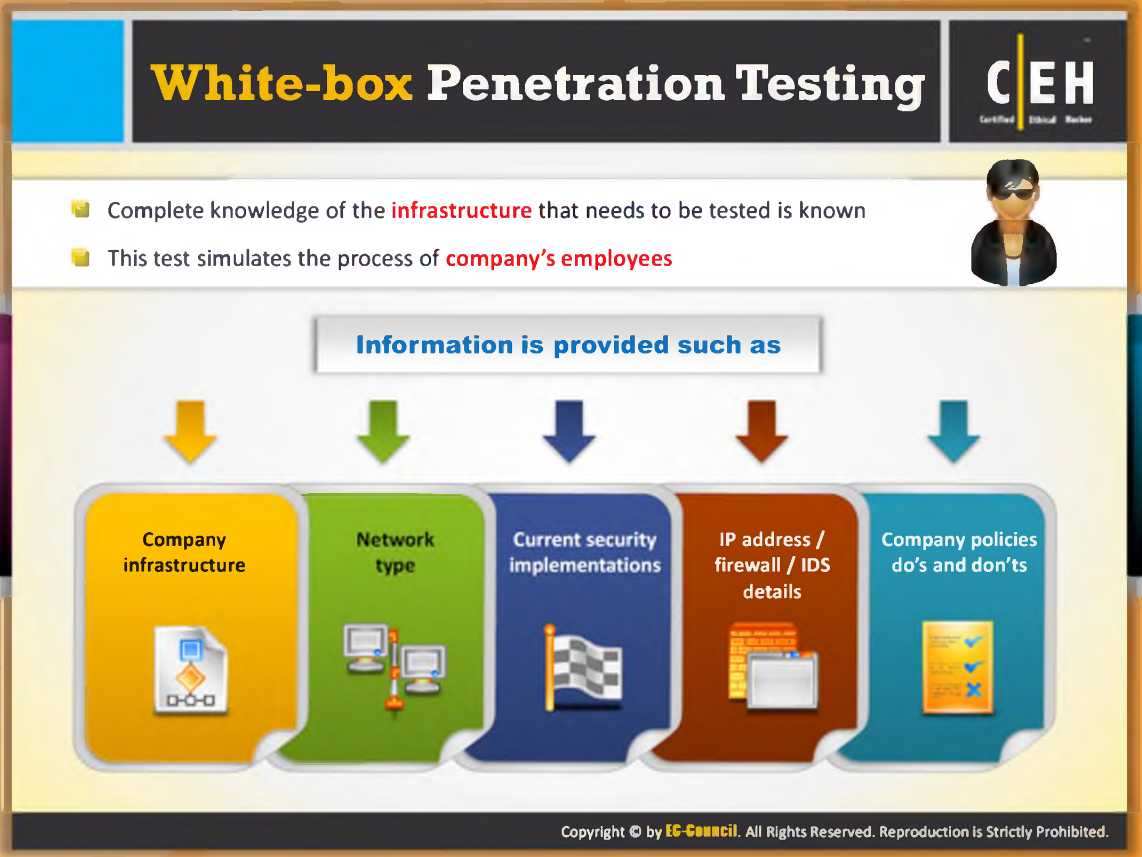
Conduct Review

Performed mostly when a penetration tester starts a black box test on well protected systems and finds that a little prior knowledge is required in order to conduct a thorough review

Gray-box Penetration Testing

In gray-box penetration testing, the test is conducted with limited knowledge about infrastructure, defense mechanism, and communication channels of the target on which test is to be conducted. It is simulation of those attacks that is performed by the insider or outsider with limited accesses privileges.

In this case, organizations would prefer to provide the pen testers with partial knowledge or information that hackers could find such as domain name server. This can save time and expenses of the organization. In gray-box testing, pen testers may also interact with system and network administrators.



White-box Penetration Testing

- Complete knowledge of the infrastructure that needs to be tested is known
- This test simulates the process of company's employees

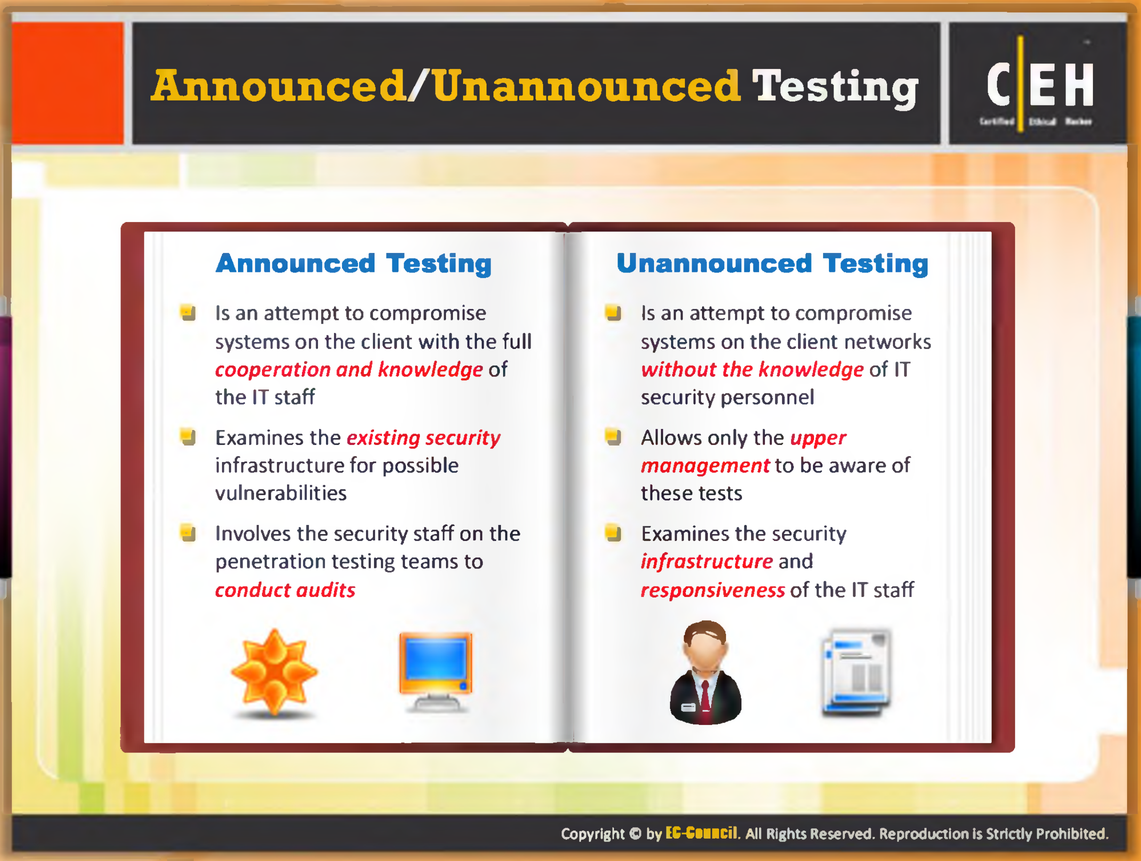
Information is provided such as

- Company infrastructure
- Network type
- Current security implementations
- IP address / firewall / IDS details
- Company policies do's and don'ts

White-box Penetration Testing

In white-box penetration testing, the test is conducted with full knowledge of infrastructure, defense mechanism, and communication channels of the target on which test is being conducted. This test simulates the insider attacker who has full privileges and unlimited access to the **target system**.

This type of penetration test is being conducted when the organization needs to assess its security against a specific kind of attack or a specific target. In this case, the complete information about the target is given to the pen testers. The information provided can include network topology documents, asset inventory, and valuation information. Typically, an organization would opt for this when it wants a complete **audit** of its security.



Announced/Unannounced Testing

Announced Testing

- Is an attempt to compromise systems on the client with the full ***cooperation and knowledge*** of the IT staff
- Examines the ***existing security*** infrastructure for possible vulnerabilities
- Involves the security staff on the penetration testing teams to ***conduct audits***

Unannounced Testing

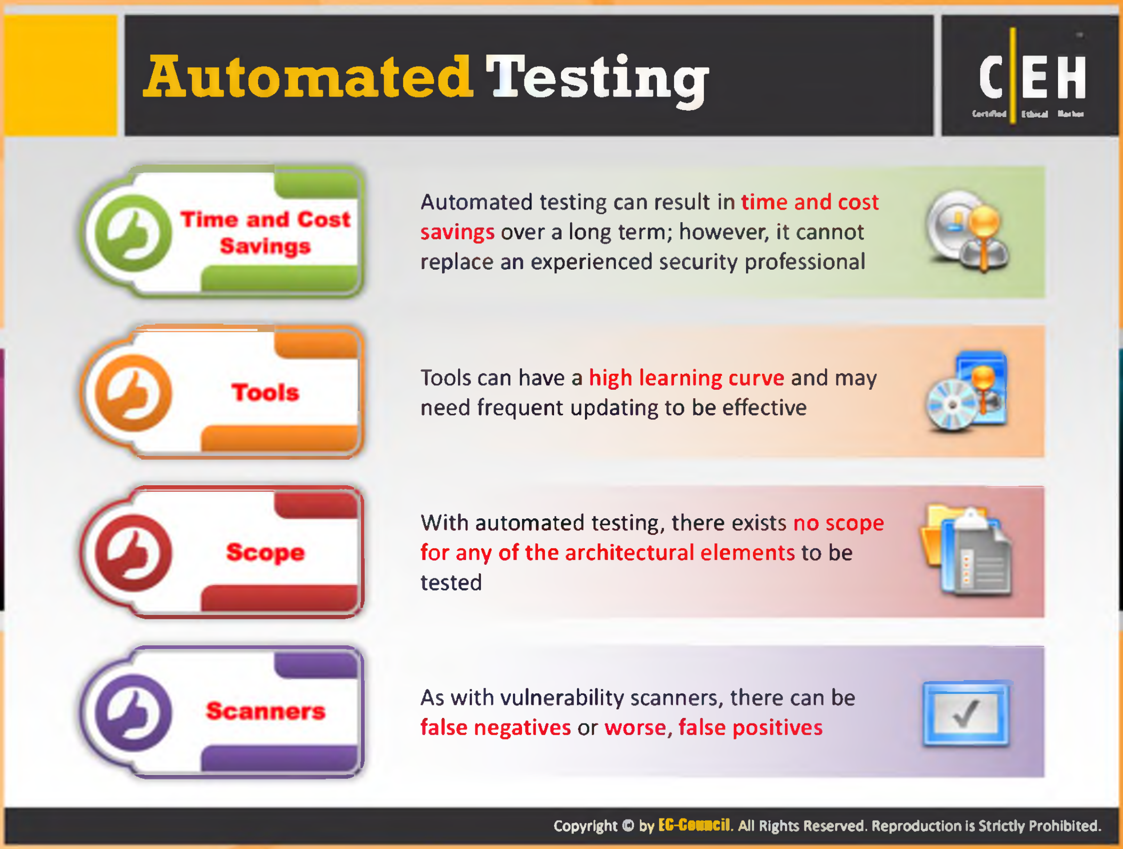
- Is an attempt to compromise systems on the client networks ***without the knowledge*** of IT security personnel
- Allows only the ***upper management*** to be aware of these tests
- Examines the security ***infrastructure*** and ***responsiveness*** of the IT staff

Announced/Unannounced Testing

Announced testing is an attempt to access and retrieve pre-identified flag file(s) or to compromise systems on the client network with the full cooperation and knowledge of the IT staff. Such testing examines the existing security infrastructure and individual systems for possible vulnerabilities. Creating a **team-oriented environment** in which members of the organization's security staff are part of the penetration team allows for a targeted attack against the most worthwhile hosts.

Unannounced testing is an attempt to access and **retrieve pre-identified flag file(s)** or to compromise systems on the client network with the awareness of only the upper levels of management. Such testing examines both the existing security infrastructure and the responsiveness of the staff. If intrusion detection and incident response plans have been created, this type of test will identify any weaknesses in their execution. Unannounced testing offers a test of the organization's security procedures in addition to the security of the infrastructure.

In both cases, the IT representative in the organization who would normally report security breaches to legal authorities should be aware of the test to prevent escalation to law enforcement organizations.



Automated Testing

CEH Certified Ethical Hacker

Time and Cost Savings — Automated testing can result in time and cost savings over a long term; however, it cannot replace an experienced security professional

Tools — Tools can have a high learning curve and may need frequent updating to be effective

Scope — With automated testing, there exists no scope for any of the architectural elements to be tested

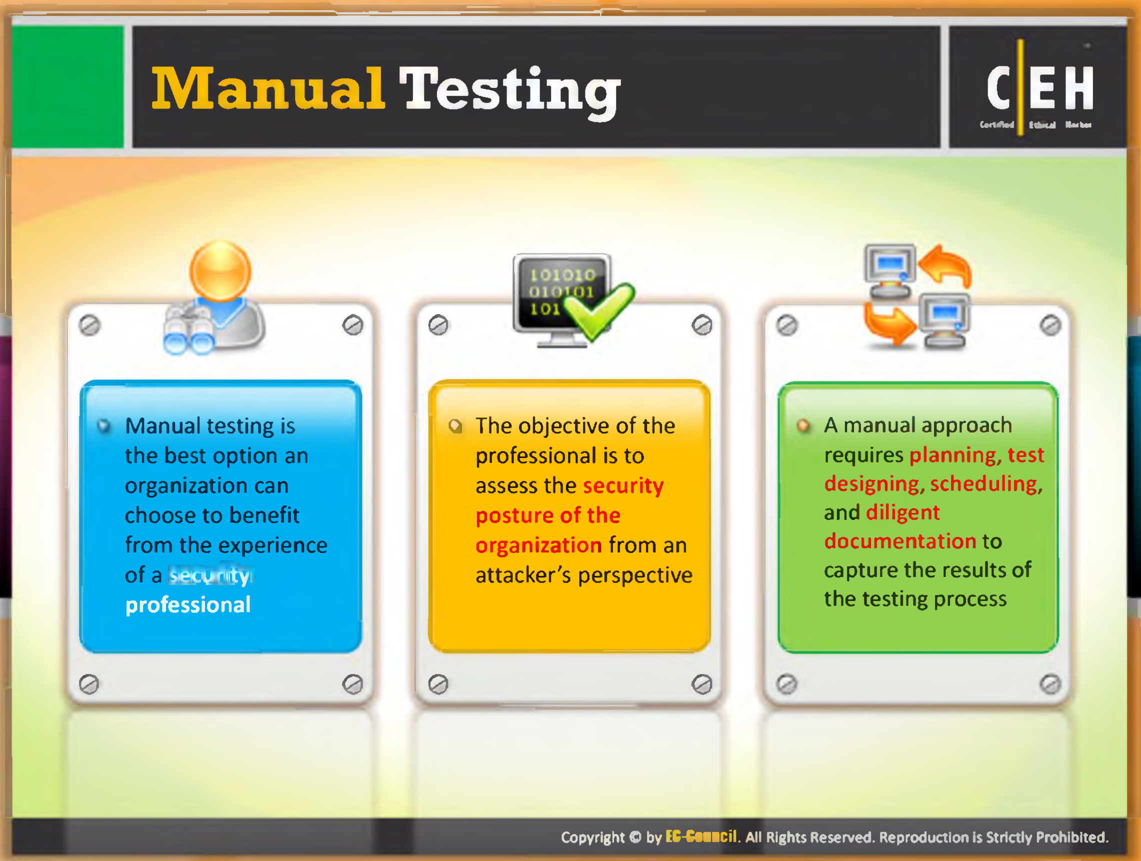
Scanners — As with vulnerability scanners, there can be false negatives or worse, false positives

Automated Testing

Instead of relying on security experts, some organizations and security-testing firms prefer to automate their security assessments. Here, a security tool is run against the target and the security posture is assessed. The tools attempt to replicate the attacks that intruders have been known to use. This is similar to vulnerability scanning. Based on the success or failure of these attacks, the tool attempts to assess and report security vulnerabilities.

However, it must be noted that a thorough security assessment also includes elements of **architectural review, security policy, firewall rule-base analysis, application testing, and general benchmarking**. Automated testing is generally limited to external penetration testing using the black-box approach and does not allow an organization to profit completely from the exercise. As an automated process, there is no scope for any of the policy or architectural elements in the testing, and it may need to be supplemented by a security professional's expertise.

One advantage attributed to automated testing is that it reduces the volume of traffic required for each test. This gives an impression that the organization can service its customers concurrently for the same overhead structure. Organizations need to evaluate if this indeed serves the purpose of the test. A **non-automated security assessment** will always be more flexible to an organization's requirements and more cost effective, as it will take into account other areas such as security architecture and policy, and will most likely be more thorough and therefore secure. In addition, testing at frequent intervals allows the consultants to explain to the management of the organization and the technical audiences what they have discovered, the processes they used, and the **ramifications** of all the **recommendations**. Additionally, they can inform in person, as an individual entity helping to support the IT security department augmenting the budgets required.



Manual Testing

- Manual testing is the best option an organization can choose to benefit from the experience of a security professional

- The objective of the professional is to assess the security posture of the organization from an attacker's perspective

- A manual approach requires planning, test designing, scheduling, and diligent documentation to capture the results of the testing process

Manual Testing

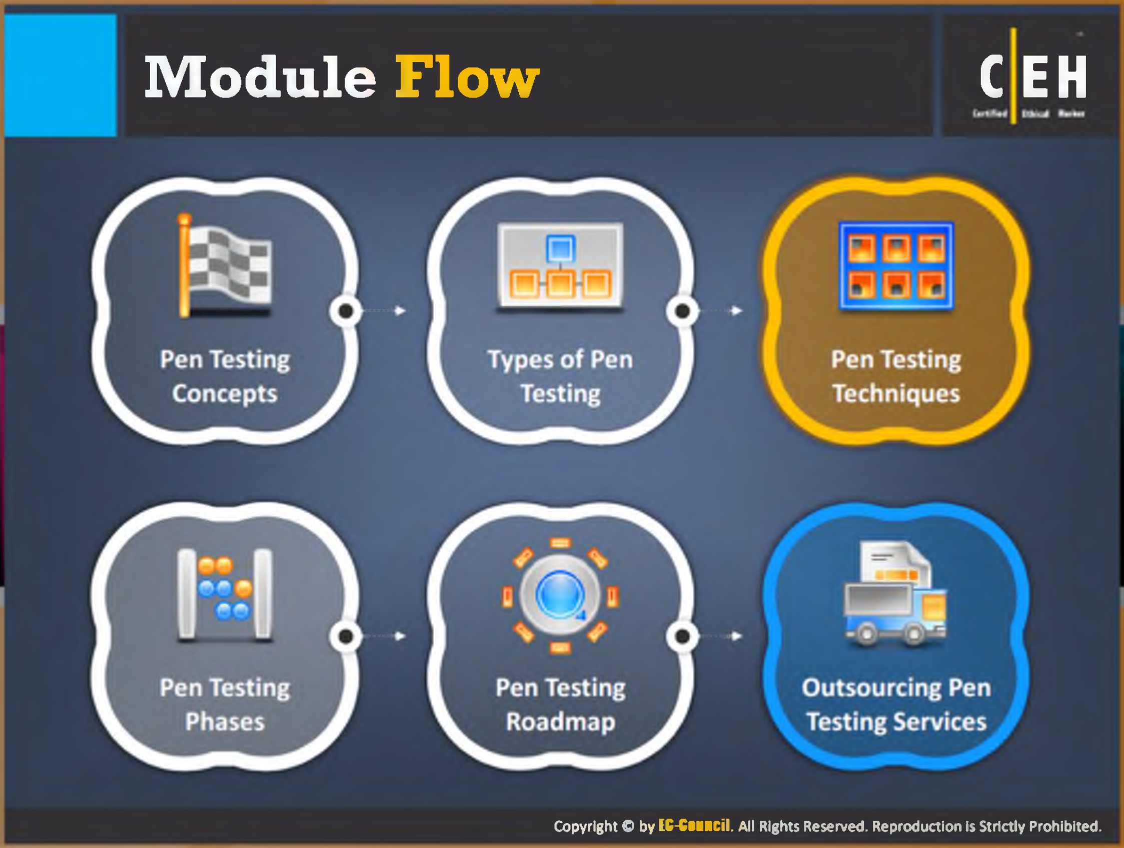
Several organizations choose to have a manual assessment of their security and benefit from the experience of a seasoned security professional. The objective of the professional is to assess the security posture of the organization from an attacker's perspective.

Under the manual approach, the security professional attempts to unearth holes in the security model of the organization by approaching it in a methodical manner. The phases of testing can involve **basic information gathering, social engineering, scanning, vulnerability assessment, exploiting vulnerabilities**, etc.

A manual approach requires planning, test designing and scheduling, and diligent documentation to capture the results of the testing process in its entirety. Documentation plays a significant role in deciding how well the team has been able to assess the security posture of the organization.

Some organizations may choose to have their own internal team to do the manual assessment and an external agency audit at the same time. Some others may choose to get a second external team to audit the findings of the **first external team**.

The rules of engagement and the expected deliverables should be clearly defined. In the long term, the management will benefit more from a manual approach as the team would be able to explain the gravity of the situation from an unbiased viewpoint and make recommendations on improving the security posture.

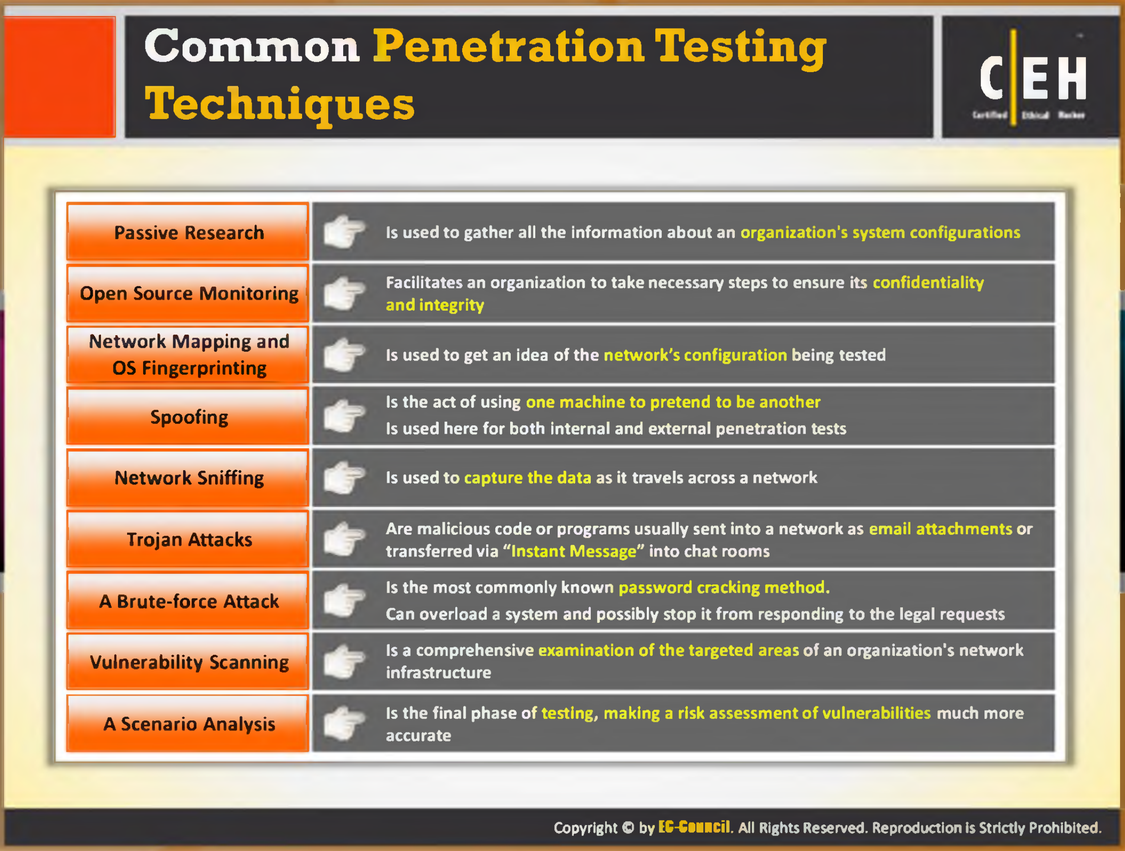

Module Flow
CEH
Pen Testing Concepts
Types of Pen Testing
Pen Testing Techniques
Pen Testing Phases
Pen Testing Roadmap
Outsourcing Pen Testing Services
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Considering that you became familiar with pen testing concepts and the types of penetration testing, we will move forward to penetration testing techniques.

This section covers various penetration testing techniques.

Pen Testing Concepts	Types of Pen Testing
Pen Testing Techniques	Pen Testing Phases
Pen Testing Roadmap	Outsourcing Pen Testing Services



Common Penetration Testing Techniques

Passive Research	Is used to gather all the information about an organization's system configurations
Open Source Monitoring	Facilitates an organization to take necessary steps to ensure its confidentiality and integrity
Network Mapping and OS Fingerprinting	Is used to get an idea of the network's configuration being tested
Spoofing	Is the act of using one machine to pretend to be another Is used here for both internal and external penetration tests
Network Sniffing	Is used to capture the data as it travels across a network
Trojan Attacks	Are malicious code or programs usually sent into a network as email attachments or transferred via "Instant Message" into chat rooms
A Brute-force Attack	Is the most commonly known password cracking method. Can overload a system and possibly stop it from responding to the legal requests
Vulnerability Scanning	Is a comprehensive examination of the targeted areas of an organization's network infrastructure
A Scenario Analysis	Is the final phase of testing, making a risk assessment of vulnerabilities much more accurate

Common Penetration Testing Techniques

The following are a few common techniques that can be used for penetration testing:

Passive research

Passive research is used to gather information about an organization related to the configuration from public domain sources such as DNS records, name registries, ISP looking-glass servers, Usenet newsgroups, etc.

Open source monitoring

Open source monitoring facilitates an organization to take necessary steps to ensure its confidentiality and integrity. Monitoring includes alerting in the following situations:

- When the database is not available
- When a database error occurs
- The file system is running out of space etc.

Graphing and seeing trends for:

- Database

- Table locks
- Replication lag
- Table cache efficiency etc.

Network mapping and OS fingerprinting

Network mapping and OS fingerprinting gives an idea about the configuration of the entire network being tested. This technique is designed to specify different types of services present on the target system.

Spoofing

Spoofing is an attempt by someone or something to masquerade as someone else. For example: one machine pretends to be another. Spoofing is used here for both internal and external penetration tests.

Network sniffing

Network spoofing occurs when the attacker forges the source or destination IP address in the IP header. It is used to capture data as it travels across a network.

Trojan attacks

A Trojan attack is installing a Trojan (malicious software) onto the victim's system. It gets installed through **email, CD-ROM, Internet Explorer**, etc.

Brute force attacks

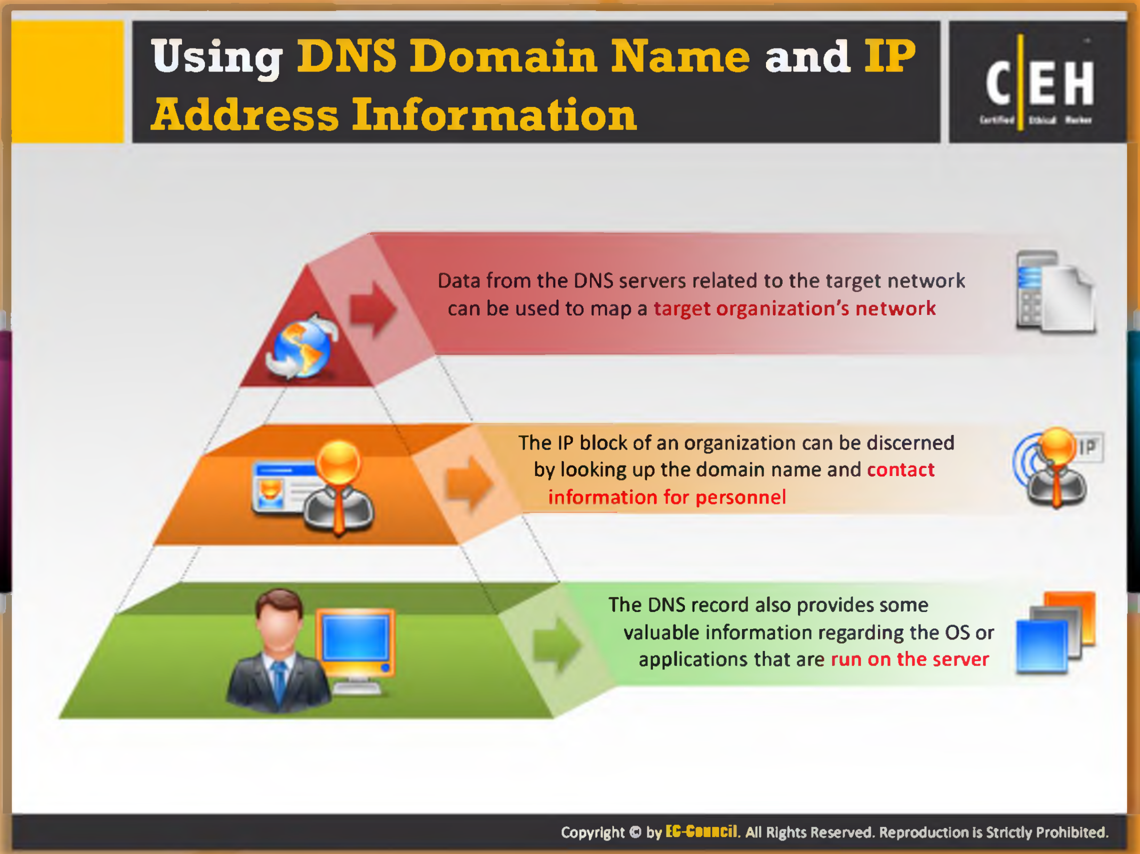
Session IDs can be guessed by using the brute force technique. It tries multiple possibilities of patterns until a session ID works. An attacker using a DSL line can make up to 1000 session IDs per second. This technique is used when the algorithm that produces session IDs is not random.

Vulnerability scanning

Vulnerability scanning is used to discover weaknesses in a security system in order to improve or repair before a breach occurs. It is a comprehensive examination of the targeted areas of an organization's network infrastructure

Scenario analysis

Scenario analysis helps in dealing with uncertainties. It is the final phase of testing, making a risk assessment of vulnerabilities much more accurate.



Using DNS Domain Name and IP Address Information

Data from the DNS servers related to the target network can be used to map a **target organization's network**

The IP block of an organization can be discerned by looking up the domain name and **contact information for personnel**

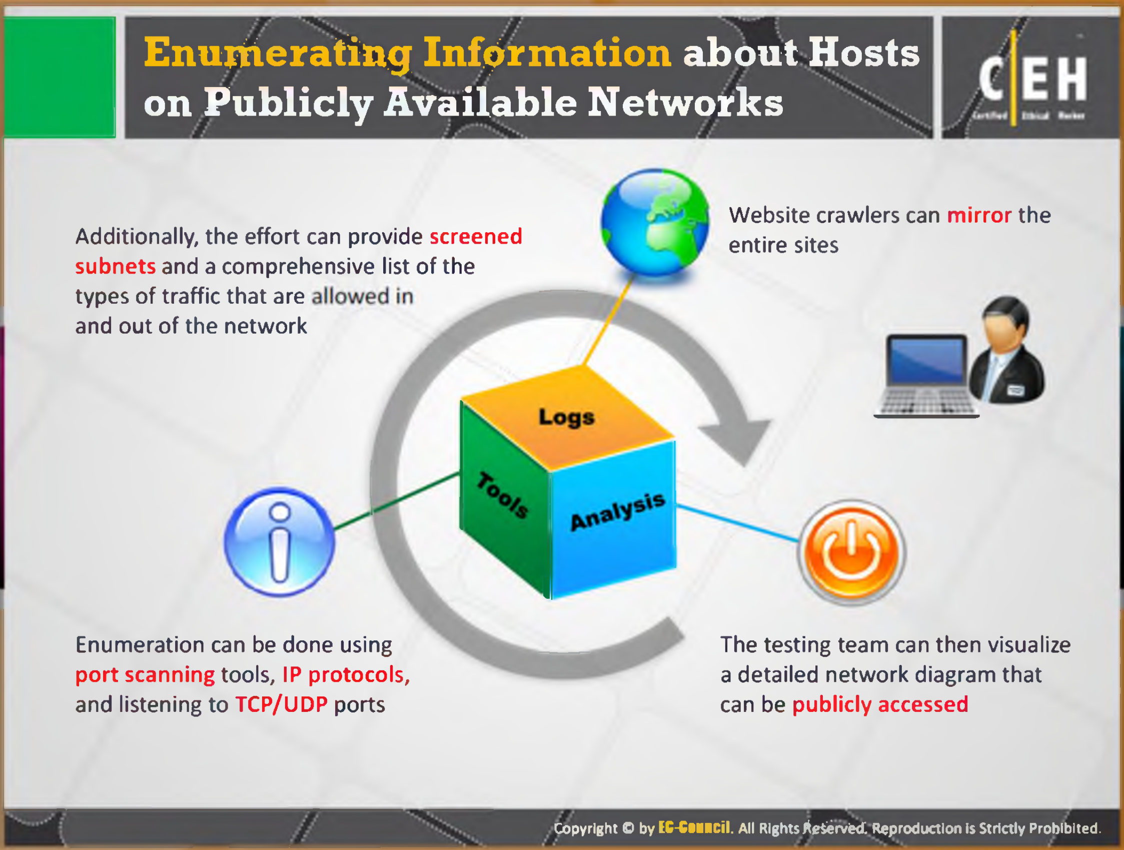
The DNS record also provides some valuable information regarding the OS or applications that are **run on the server**

Using DNS Domain Name and IP Address Information

Data from the DNS servers related to the target network can be used to map a target organization's network. DNS zones can be analyzed for information about the target organization's network. This can result in obtaining further data, including the **server host's names, services offered by particular servers, IP addresses**, and contact data for the members of the IT staff.

Many attackers have been known to use software, which is easily available to the general public, to create well-organized network diagrams of the target network. IP address data regarding a particular system can be gained from the DNS zone or the American Registry of Internet Numbers (ARIN). Another way of obtaining an IP address is by using port-scanning software to deduce a **target organization's network diagram**.

By examining the DNS records, you can get a good understanding about where the servers of the target network are located. The DNS record also provides some valuable information regarding the OS or applications that are being run on the server. The IP block of an organization can be discerned by looking up the domain name and contact information for personnel can be obtained.



Enumerating Information about Hosts on Publicly Available Networks

Additionally, the effort can provide screened subnets and a comprehensive list of the types of traffic that are allowed in and out of the network

Website crawlers can mirror the entire sites

Enumeration can be done using port scanning tools, IP protocols, and listening to TCP/UDP ports

The testing team can then visualize a detailed network diagram that can be publicly accessed

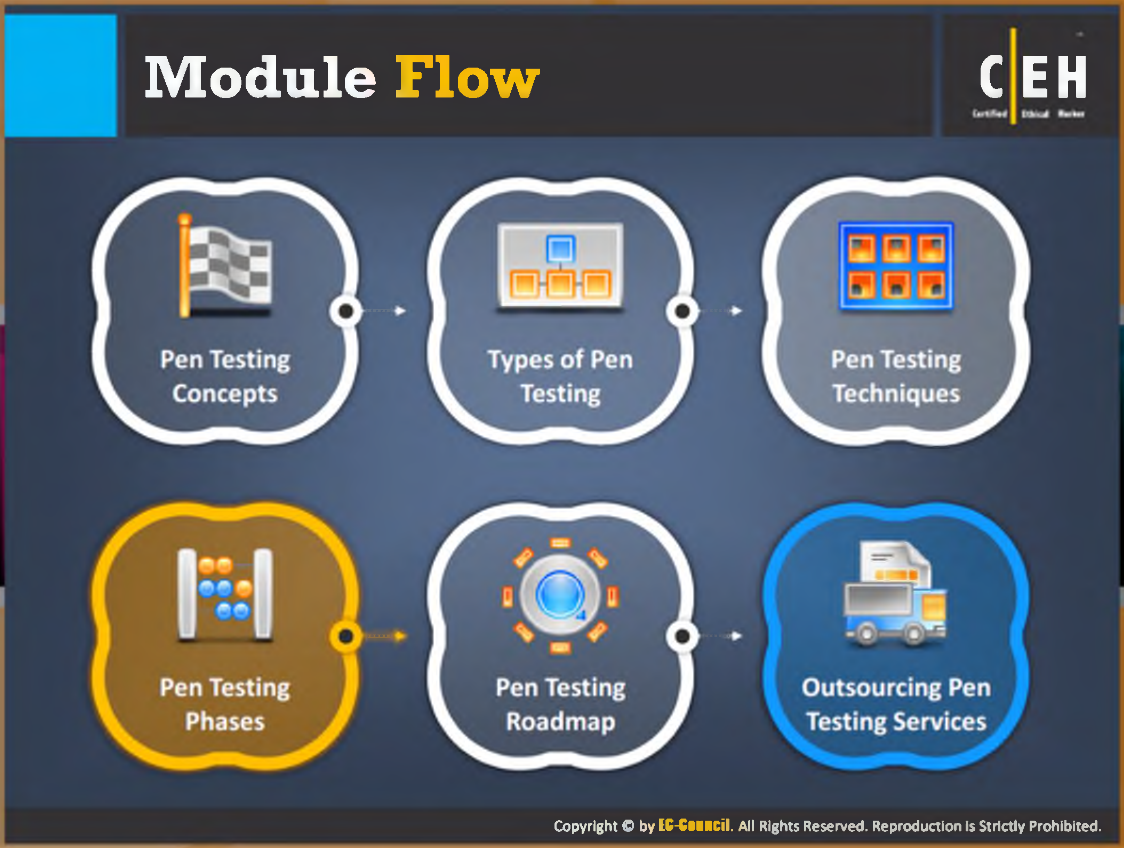
Enumerating Information about Hosts on Publicly Available Networks

With the IP addresses obtained in the preceding step, the pen-test team can outline the network to explore possible points of entry from the perspective of an attacker. Testers achieve this by analyzing all data about the hosts that are uncovered to the Internet by the target organization. They can use port-scanning tools and IP protocols, and they can listen to TCP/UDP ports.

Port scans will also reveal information about hosts such as the current operating system that is running on the system and also other applications. An effective port-scanning tool can also help to deduce how the router and firewall IP filters are configured. The testing team can then visualize a detailed network diagram that can be publicly accessed.

Additionally, the effort can provide screened subnets and a comprehensive list of the types of traffic that is allowed in and out of the network. Website crawlers can mirror entire sites and allow the testing group to check for faulty source code or inadvertent inclusions of sensitive information. Many times, organizations have given information that is not intended for use by the public, but is posted on the website.

- If the rules of engagement permit, the pen-test team may purchase research reports on the organization available for sale and use the information available therein for comprising the security of the target organization. These can include covert means, such as social engineering, as well. It is necessary to point out that prior approval from management is a critical aspect to be considered before indulging in such activities.



Module Flow

CEH
Certified Ethical Hacker

Pen Testing Concepts → Types of Pen Testing → Pen Testing Techniques

Pen Testing Phases → Pen Testing Roadmap → Outsourcing Pen Testing Services

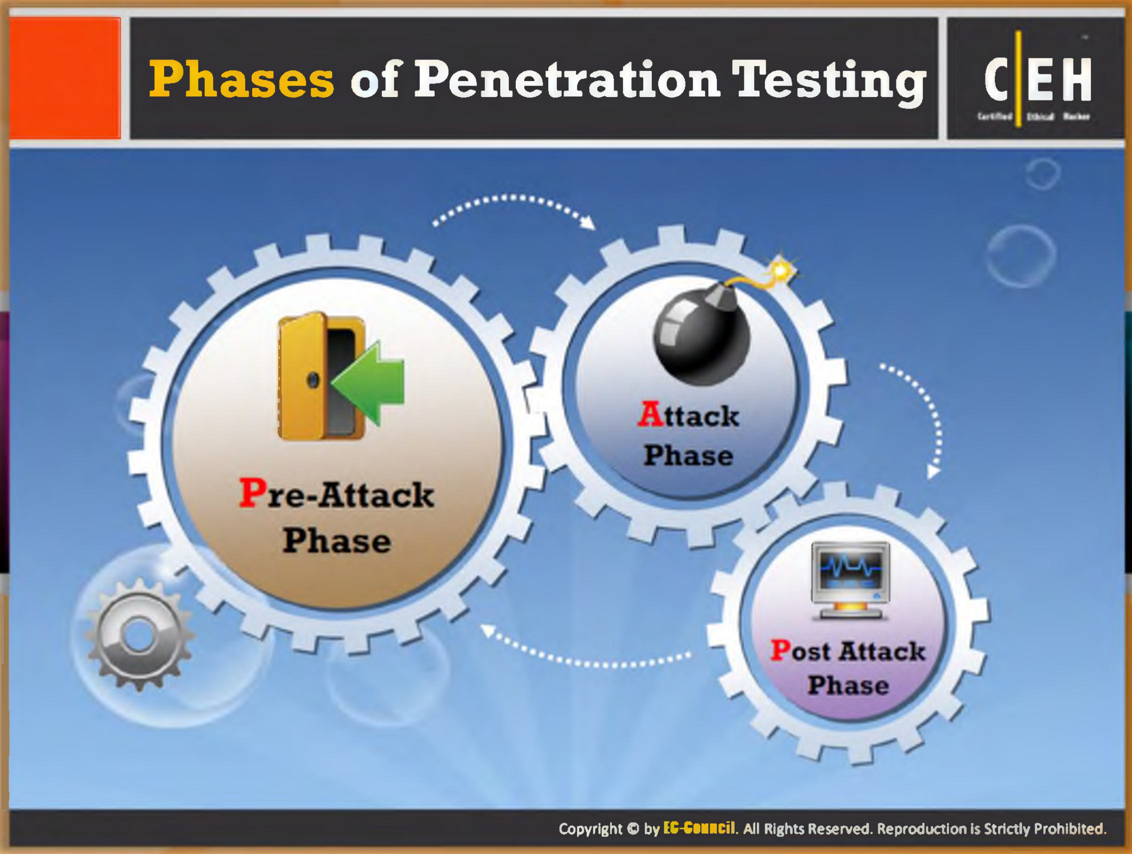
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Pen testing is the test conducted in three phases for discovering the vulnerabilities or weakness in an organization's systems. The three phases are the **pre-attack phase, attack phase, and post-attack phase**.

Pen Testing Concepts	**Types of Pen Testing**
Pen Testing Techniques	**Pen Testing Phases**
Pen Testing Roadmap	**Outsourcing Pen Testing Services**

This section highlights the three phases of pen testing.



Phases of Penetration Testing

Pre-Attack Phase

Attack Phase

Post Attack Phase

Phases of Penetration Testing

These are three phases of penetration testing.

Pre-attack Phase

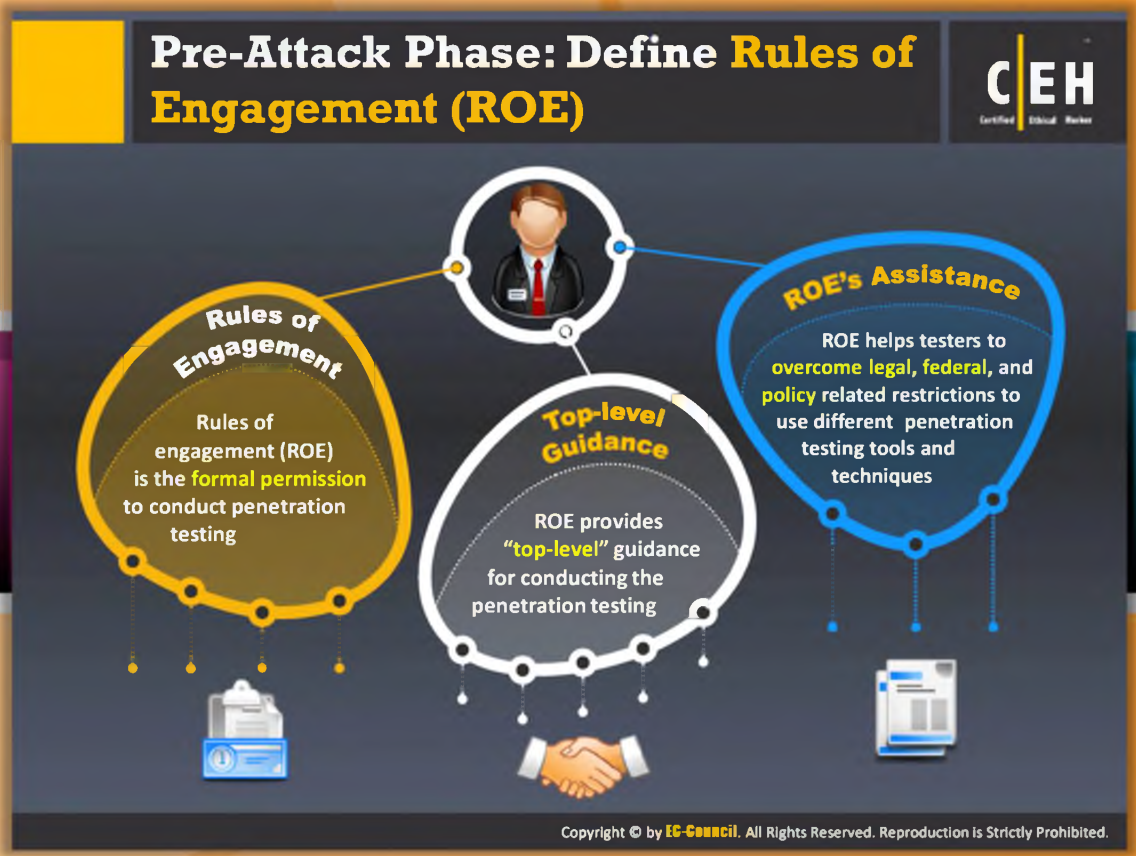
This phase is focused on gathering as much information as possible about the target organization or network to be attacked. This can be non-invasive or invasive.

Attack Phase

The information gathered in the pre-attack phase forms the basis of the attack strategy. Before deciding the attack strategy, the tester may choose to carry out an invasive information gathering process such as scanning.

Post-attack Phase

This is a crucial part of the testing process, as the tester needs to restore the network to its original state. This involves cleanup of testing processes and removal of vulnerabilities created (not those that existed originally), exploits crafted, etc.

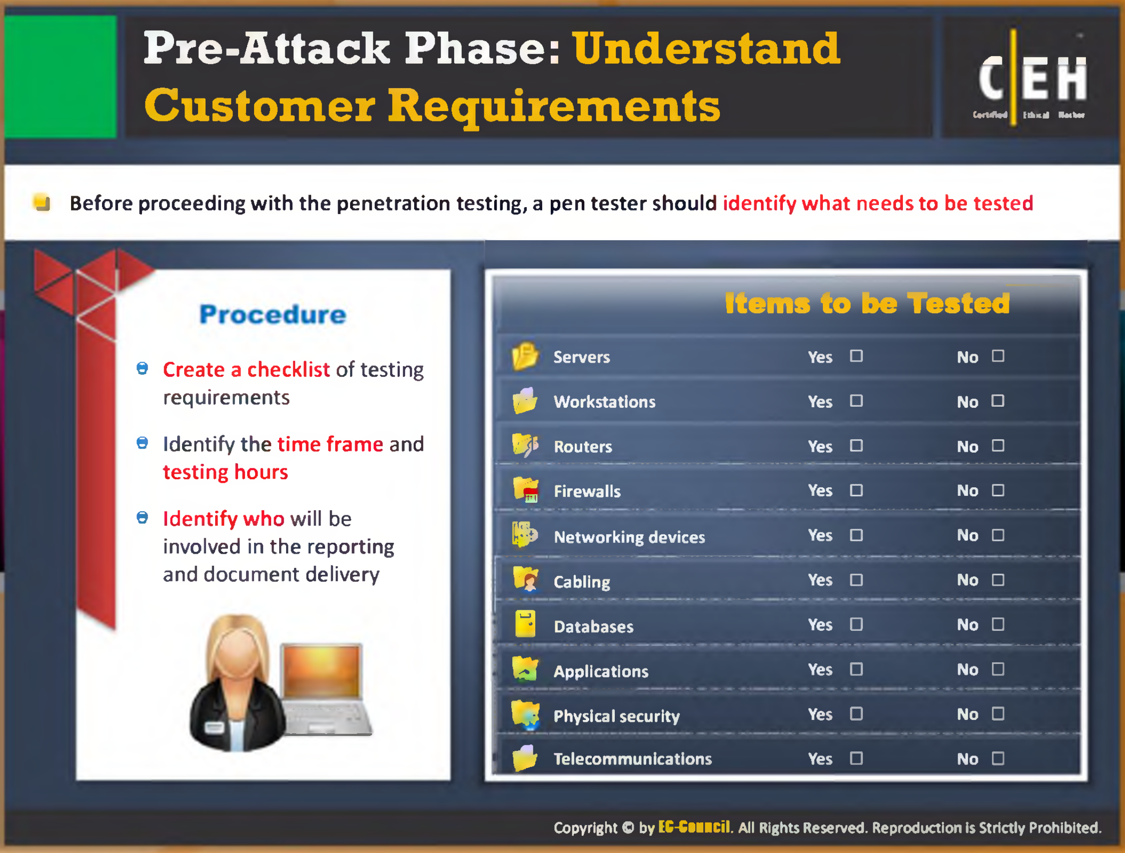


Pre-Attack Phase: Define Rules of Engagement (ROE)

CEH
Certified Ethical Hacker
Rules of Engagement
Rules of engagement (ROE) is the formal permission to conduct penetration testing
Top-level Guidance
ROE provides "top-level" guidance for conducting the penetration testing
ROE's Assistance
ROE helps testers to overcome legal, federal, and policy related restrictions to use different penetration testing tools and techniques

Pre-attack Phase: Define Rules of Engagement (ROE)

Rules of engagement (ROE) are the guidelines and constraints about the execution of penetration testing. It should be developed and presented before conducting the penetration test. It gives authority to the pen tester to conduct defined activities without the need for additional permissions. ROE helps pen testers to overcome **legal-, federal-, and policy-related restrictions** to use different penetration testing tools and techniques



Pre-Attack Phase: Understand Customer Requirements

Before proceeding with the penetration testing, a pen tester should identify what needs to be tested

Procedure

- Create a checklist of testing requirements
- Identify the time frame and testing hours
- Identify who will be involved in the reporting and document delivery

Items to be Tested

Servers	Yes □	No □
Workstations	Yes □	No □
Routers	Yes □	No □
Firewalls	Yes □	No □
Networking devices	Yes □	No □
Cabling	Yes □	No □
Databases	Yes □	No □
Applications	Yes □	No □
Physical security	Yes □	No □
Telecommunications	Yes □	No □

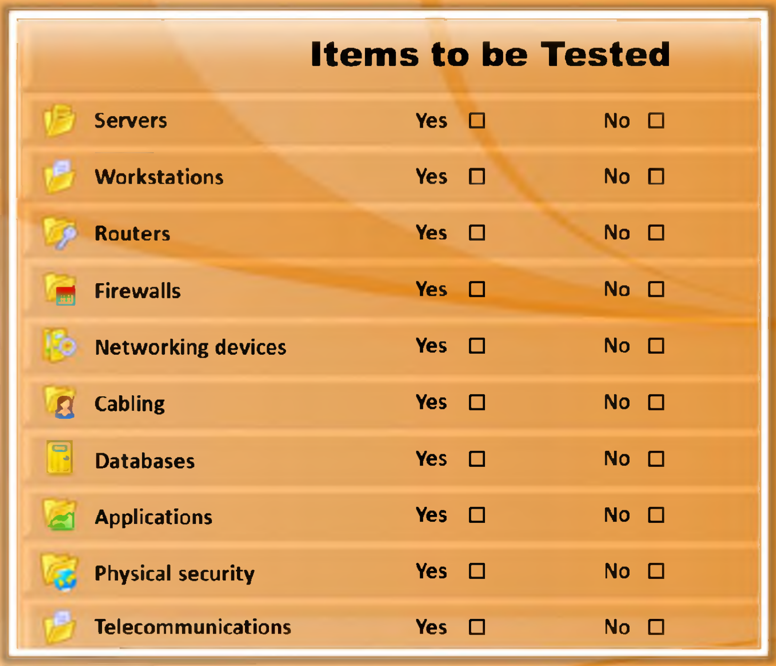
Pre-attack Phase: Understand Customer Requirements

Once ROE is defined to conduct penetration test, the second step in the pre-attack phase, you should clearly understand the customer requirements, i.e., what the customer expects from the penetration test. Before proceeding with the penetration testing, a pen tester should identify what needs to be tested in the target organization.

To clearly identify the customer requirements, do the following things:

- Create a checklist of testing requirements
- Identify the time frame and testing hours
- Identify who will be involved in the reporting and document delivery

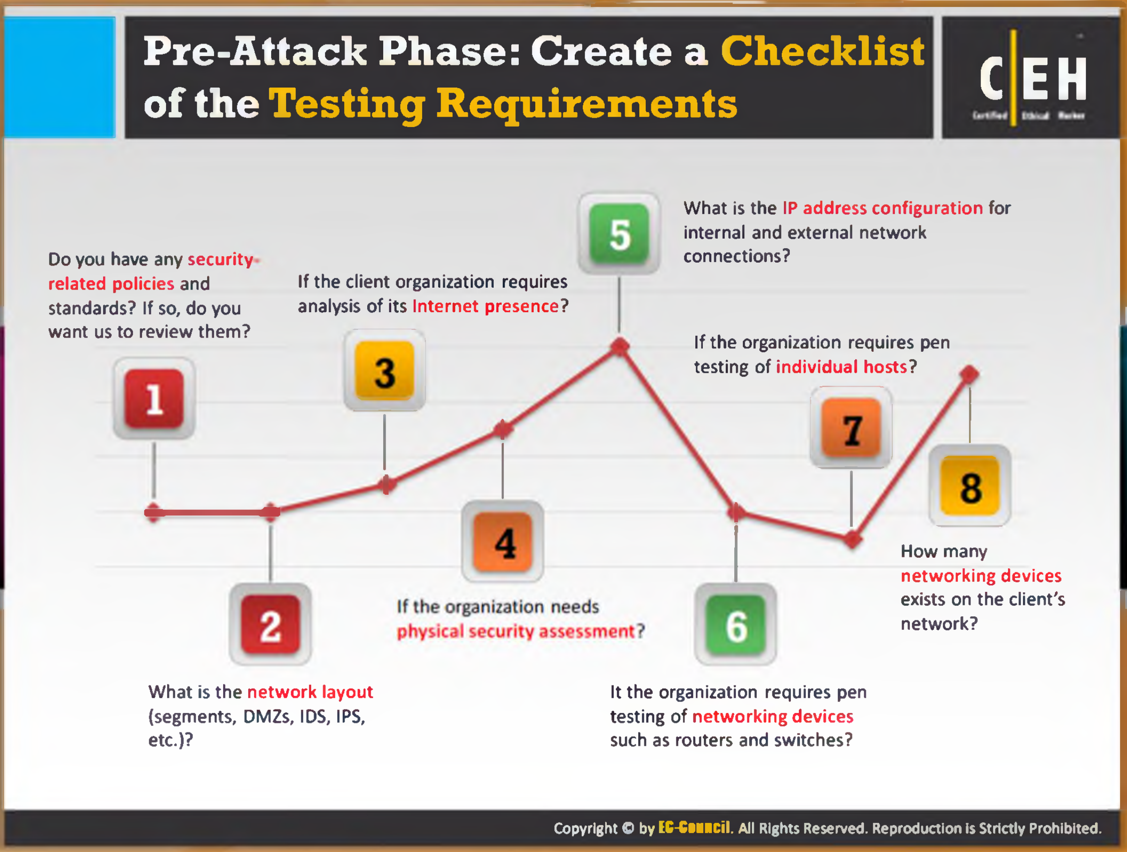
Prepare the check list for the items that need to be tested in target organization as shown in following figure:



Items to be Tested

Servers	Yes □	No □
Workstations	Yes □	No □
Routers	Yes □	No □
Firewalls	Yes □	No □
Networking devices	Yes □	No □
Cabling	Yes □	No □
Databases	Yes □	No □
Applications	Yes □	No □
Physical security	Yes □	No □
Telecommunications	Yes □	No □

FIGURE 20.1: Check list of the items that need to be tested



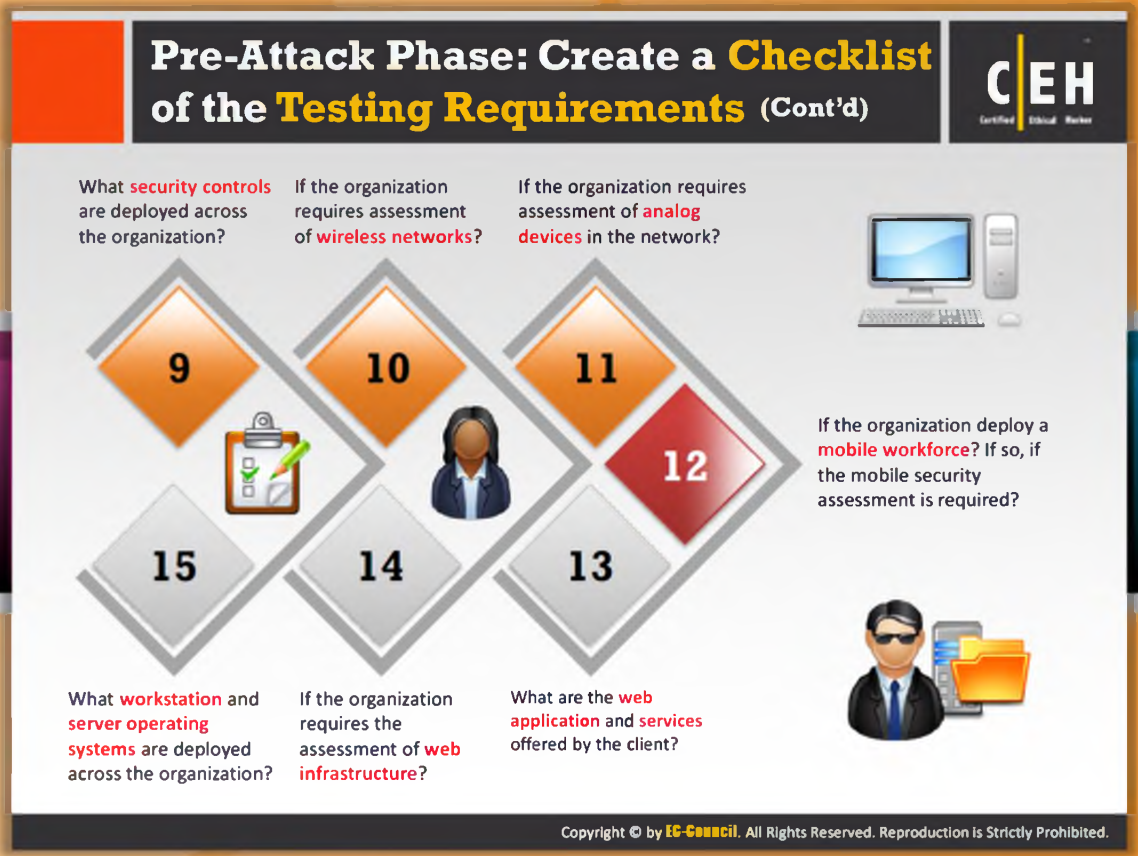
Pre-Attack Phase: Create a Checklist of the Testing Requirements

1. Do you have any security-related policies and standards? If so, do you want us to review them?
2. What is the network layout (segments, DMZs, IDS, IPS, etc.)?
3. If the client organization requires analysis of its Internet presence?
4. If the organization needs physical security assessment?
5. What is the IP address configuration for internal and external network connections?
6. It the organization requires pen testing of networking devices such as routers and switches?
7. If the organization requires pen testing of individual hosts?
8. How many networking devices exists on the client's network?

Pre-attack Phase: Create a Checklist of the Testing Requirements

To collect the **penetration test** requirements from the customer, ask the customer the following questions. The answers of these questions will help you to define the scope of the test.

- Do you have any security-related policies and standards? If so, do you want us to review them?
- What is the network layout (segments, DMZs, IDS, IPS, etc.)?
- If the client organization requires analysis of its Internet presence?
- If the organization needs **physical security assessment**?
- What is the IP address configuration for internal and external network connections?
- It the organization requires pen testing of networking devices such as routers and switches?
- If the organization requires pen testing of individual hosts?
- How many networking devices exists on the client's network?



Pre-Attack Phase: Create a Checklist of the Testing Requirements (Cont'd)

9. What security controls are deployed across the organization?

10. If the organization requires assessment of wireless networks?

11. If the organization requires assessment of analog devices in the network?

12. If the organization deploy a mobile workforce? If so, if the mobile security assessment is required?

13. What are the web application and services offered by the client?

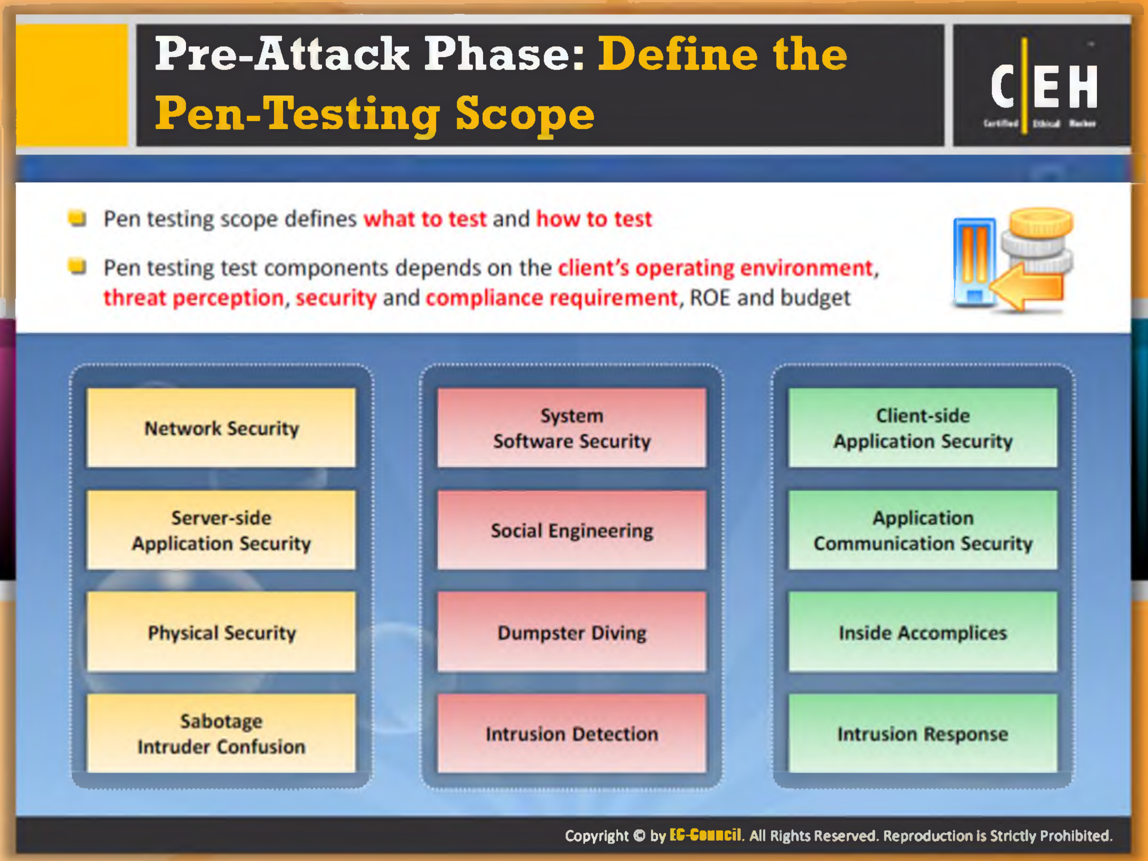
14. If the organization requires the assessment of web infrastructure?

15. What workstation and server operating systems are deployed across the organization?

Pre-attack Phase: Create a Checklist of the Testing Requirements (Cont'd)

The following are a few more questions that you should ask the customer to complete the checklist of penetration testing requirements:

- What security controls are deployed across the organization?
- If the organization requires assessment of wireless networks?
- If the organization requires assessment of analog devices in the network?
- If the organization deploy a mobile workforce? If so, if the mobile security assessment is required?
- What are the web application and services offered by the client?
- If the organization requires the assessment of web infrastructure?
- What workstation and server operating systems are deployed across the organization?



Pre-Attack Phase: Define the Pen-Testing Scope

- Pen testing scope defines what to test and how to test
- Pen testing test components depends on the client's operating environment, threat perception, security and compliance requirement, ROE and budget

Network Security

Server-side Application Security

Physical Security

Sabotage Intruder Confusion

System Software Security

Social Engineering

Dumpster Diving

Intrusion Detection

Client-side Application Security

Application Communication Security

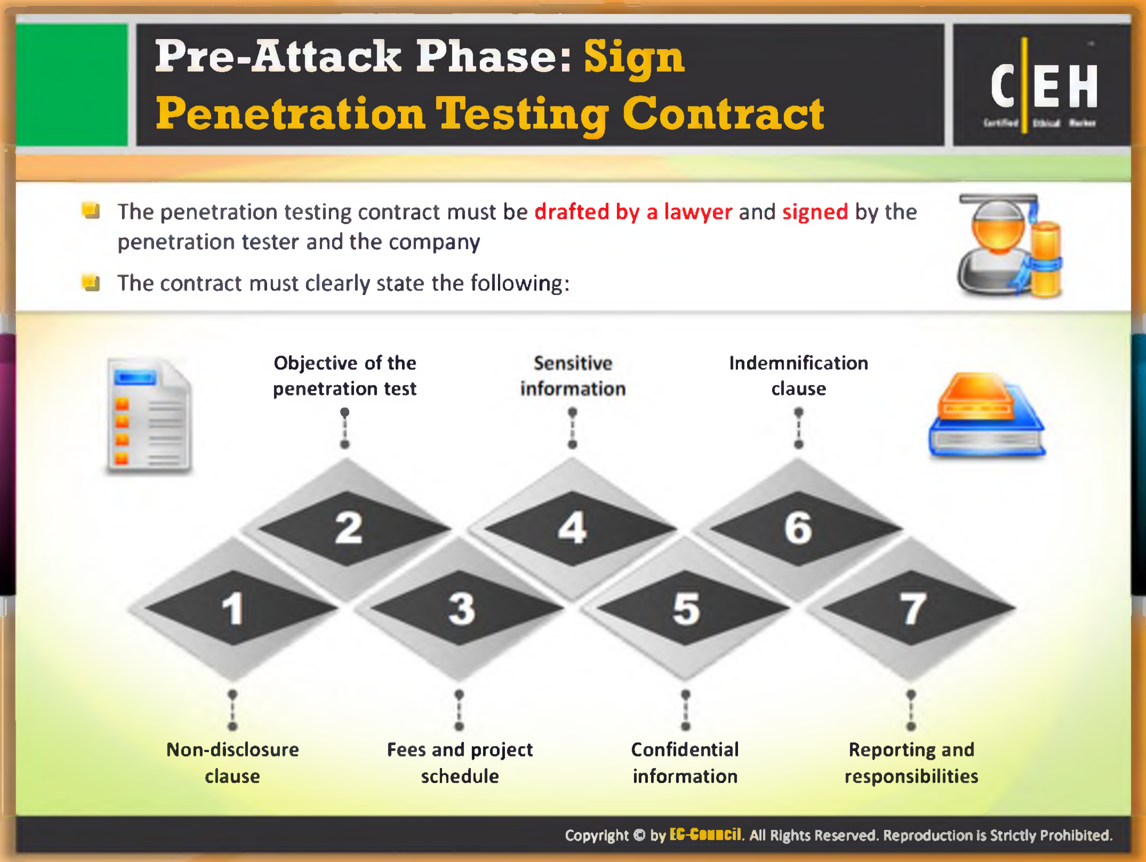
Inside Accomplices

Intrusion Response

Pre-attack Phase: Define the Pen-testing Scope

You should define the scope of your penetration test explicitly and in writing. This will help you to identify what needs to be tested in the target organization, and help to develop the procedure to test particular component once identified. This also help you to identify limitations, i.e., what should not be tested. Pen testing test components depend on **the client's operating environment, threat perception, security and compliance requirements, ROE, and budget**. The following are the possible areas of the scope of the penetration test:

- Network Security
- System Software Security
- Client-side Application Security
- Server-side Application Security
- Social Engineering
- Application Communication Security
- Physical Security
- Dumpster Diving
- Inside Accomplices
- Sabotage Intruder Confusion
- Intrusion Detection
- Intrusion Response



Pre-Attack Phase: Sign Penetration Testing Contract

- The penetration testing contract must be drafted by a lawyer and signed by the penetration tester and the company
- The contract must clearly state the following:

1 Non-disclosure clause

2 Objective of the penetration test

3 Fees and project schedule

4 Sensitive information

5 Confidential information

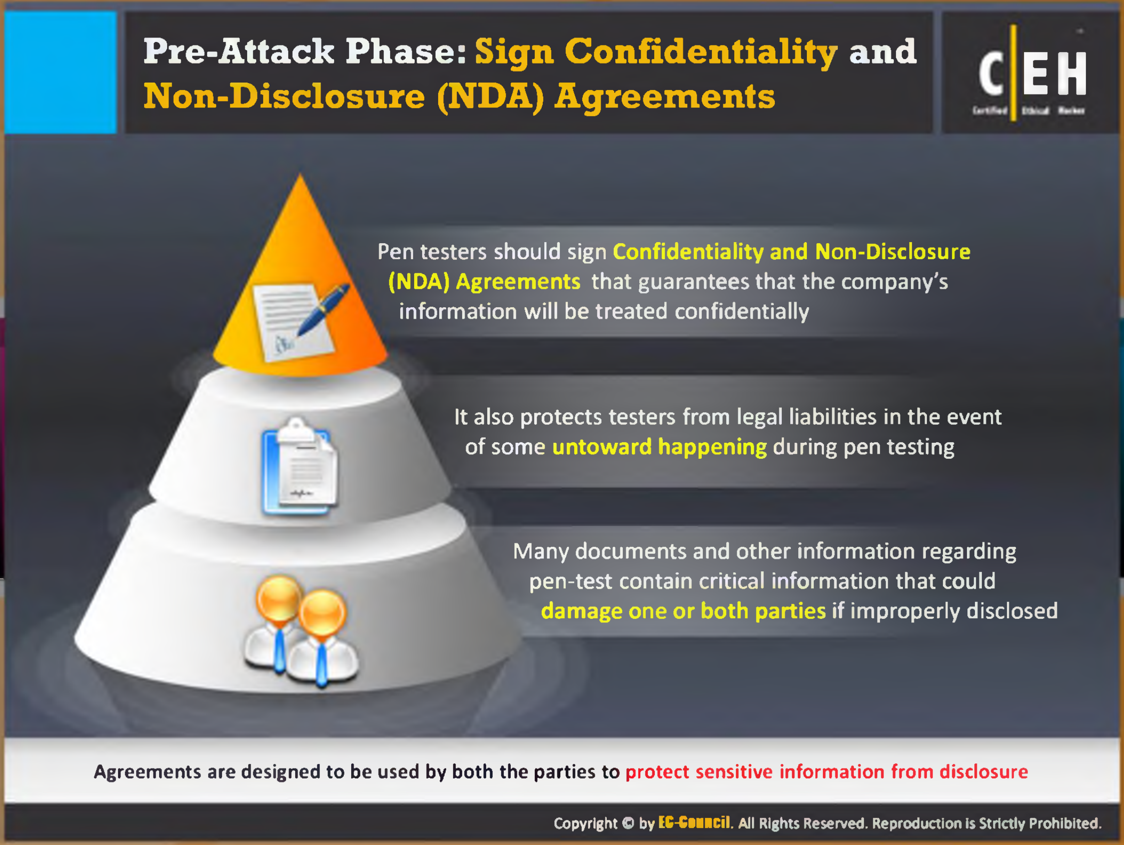
6 Indemnification clause

7 Reporting and responsibilities

Pre-attack Phase: Sign Penetration Testing Contract

Once the requirements and scope of the penetration test is confirmed from the client, you need to sign the contract with the company to conduct the penetration test. This contract must be drafted by a lawyer and duly signed by the penetration tester and the company. The contract should include the following terms and conditions:

- Non-disclosure clause
- Objective of the penetration test
- Fees and project schedule
- Sensitive information
- Confidential information
- Indemnification clause
- Reporting and responsibilities



Pre-Attack Phase: Sign Confidentiality and Non-Disclosure (NDA) Agreements

CEH
Certified Ethical Hacker

Pen testers should sign Confidentiality and Non-Disclosure (NDA) Agreements that guarantees that the company's information will be treated confidentially

It also protects testers from legal liabilities in the event of some untoward happening during pen testing

Many documents and other information regarding pen-test contain critical information that could damage one or both parties if improperly disclosed

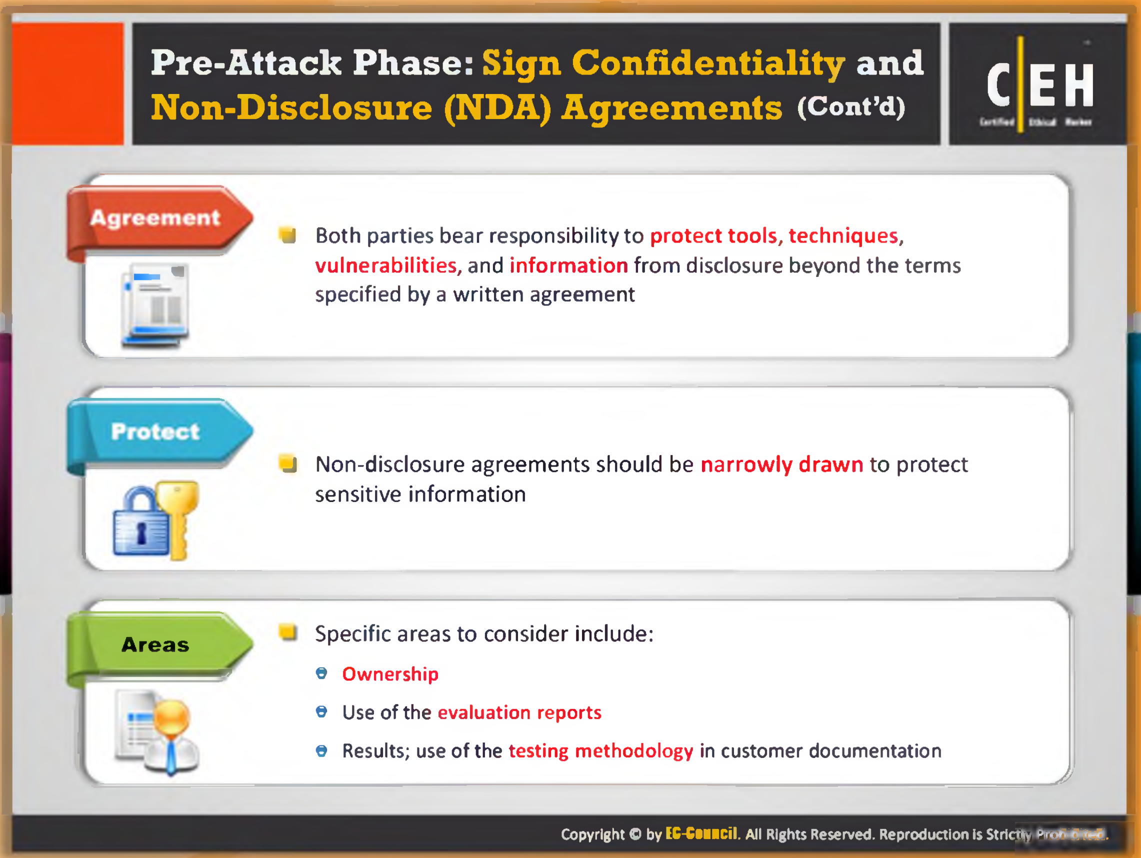
Agreements are designed to be used by both the parties to protect sensitive information from disclosure

Pre-attack Phase: Sign Confidentiality and Non-Disclosure (NDA) Agreements

As a pen tester, you will also need to sign Confidentiality and Non-Disclosure (NDA) Agreements to maintain the confidentiality of the company's sensitive information. Many documents and other information regarding the pen test contain critical information that could damage one or both parties if disclosed to other parties. Both (pen tester and company) parties should agree and duly signed on the terms and conditions included in the Confidentiality and Non-Disclosure (NDA) Agreements before conducting penetration test.

The following are the advantages of signing Confidentiality and Non-Disclosure (NDA) Agreements:

- They ensure that the company's information will be treated confidentially.
- They will also help to provide cover for a number of other key areas, such as negligence and liability in the event of something untoward happening.



Pre-Attack Phase: Sign Confidentiality and Non-Disclosure (NDA) Agreements (Cont'd)

CEH
Certified Ethical Hacker

Agreement

- Both parties bear responsibility to protect tools, techniques, vulnerabilities, and information from disclosure beyond the terms specified by a written agreement

Protect

- Non-disclosure agreements should be narrowly drawn to protect sensitive information

Areas

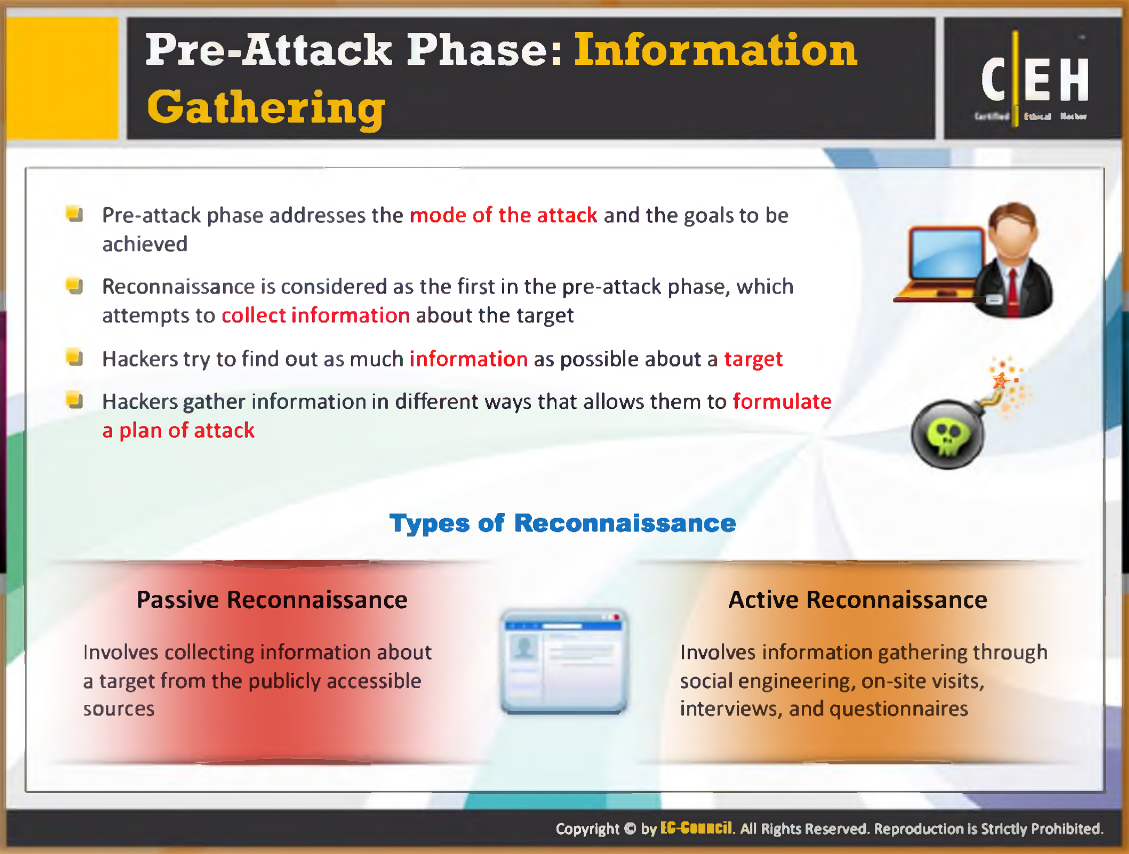
- Specific areas to consider include:
  - Ownership
  - Use of the evaluation reports
  - Results; use of the testing methodology in customer documentation

Pre-attack Phase: Sign Confidentiality and Non-Disclosure (NDA) Agreements (Cont'd)

The Confidentiality and Non-Disclosure agreements document is a powerful tool. Once you sign the NDA agreement, the company has the right to file a lawsuit against you even if you disclose the information to third party either intentionally or unintentionally. The following points should be considered while crafting Confidentiality and Non-Disclosure (NDA) Agreements:

- Both parties should bear responsibility to **protect tools, techniques, vulnerabilities**, and information from disclosure beyond the terms specified by a written agreement
- Non-disclosure agreements should be narrowly drawn to protect sensitive information.
- Specific areas to consider include:
  - Ownership
  - Use of the evaluation reports

Results; use of the testing methodology in customer documentation



Pre-Attack Phase: Information Gathering

- Pre-attack phase addresses the mode of the attack and the goals to be achieved
- Reconnaissance is considered as the first in the pre-attack phase, which attempts to collect information about the target
- Hackers try to find out as much information as possible about a target
- Hackers gather information in different ways that allows them to formulate a plan of attack

Types of Reconnaissance

Passive Reconnaissance

Involves collecting information about a target from the publicly accessible sources

Active Reconnaissance

Involves information gathering through social engineering, on-site visits, interviews, and questionnaires

Pre-attack Phase: Information Gathering

The pre-attack phase addresses the mode of the attack and the goals to be achieved. Reconnaissance is considered as the first in the pre-attack phase and is an attempt to locate, gather, identify, and record information about the target. An attacker seeks to find out as much information as possible about the victim. Attackers gather information in different ways that allows them to formulate a plan of attack. There are two types of reconnaisance:

Passive reconnaissance

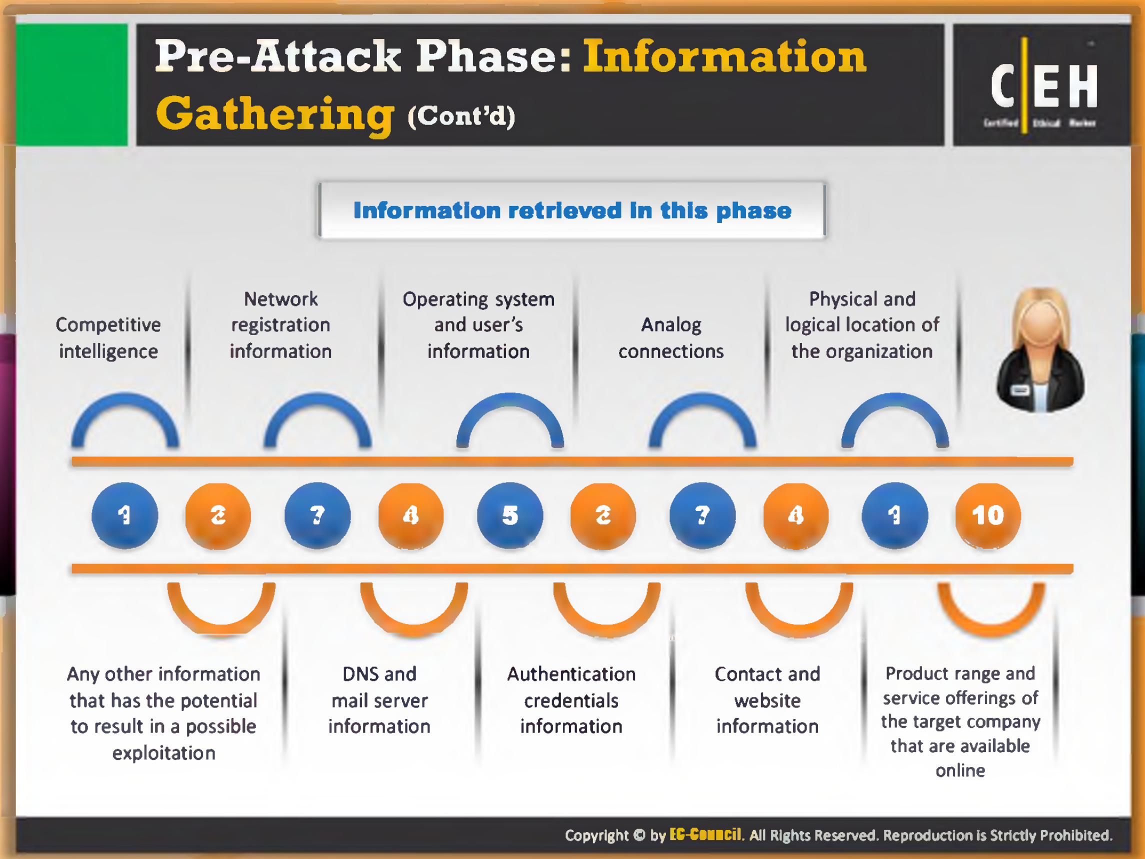
It comprises the attacker's attempts to scout for or survey potential targets and investigations or explorations of the target. It also includes information gathering and may involve competitive intelligence gathering, social engineering, breaching physical security, etc. Attackers typically spend more time on the pre-attack or reconnaissance activity than the actual attack.

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

With regard to publicly available information, access to this information is independent of the organization’s resources, and can therefore be effectively accessed by anyone. Information is often contained on systems unrelated to the organization.

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, etc. The attacker may adopt techniques such as **social engineering**, employing tools such as **scanners** and **sniffers** that automate these tasks. The footprints that the attacker leaves are larger, and novices can be easily identified.



Pre-Attack Phase: Information Gathering (Cont'd)

Information retrieved in this phase

Competitive intelligence

Network registration information

Operating system and user's information

Analog connections

Physical and logical location of the organization

Any other information that has the potential to result in a possible exploitation

DNS and mail server information

Authentication credentials information

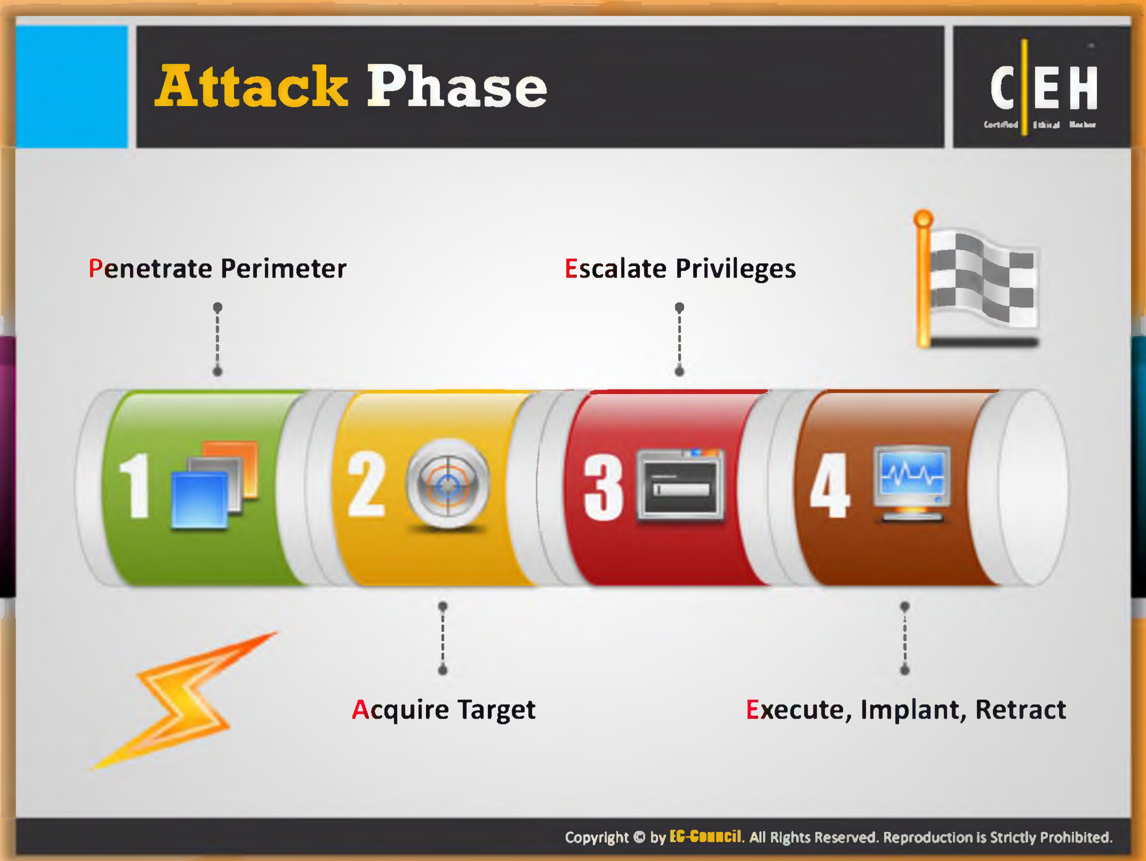
Contact and website information

Product range and service offerings of the target company that are available online

Pre-attack Phase: Information Gathering (Cont'd)

The following information is retrieved during the pre-attack phase:

- Competitive intelligence
- Network registration information
- DNS and mail server information
- Operating system information
- User's information
- Authentication credentials information
- Analog connections
- Contact information
- Website information
- Physical and logical location of the organization
- Product range and service offerings of the target company that are available online
- Any other information that has the potential to result in a possible exploitation

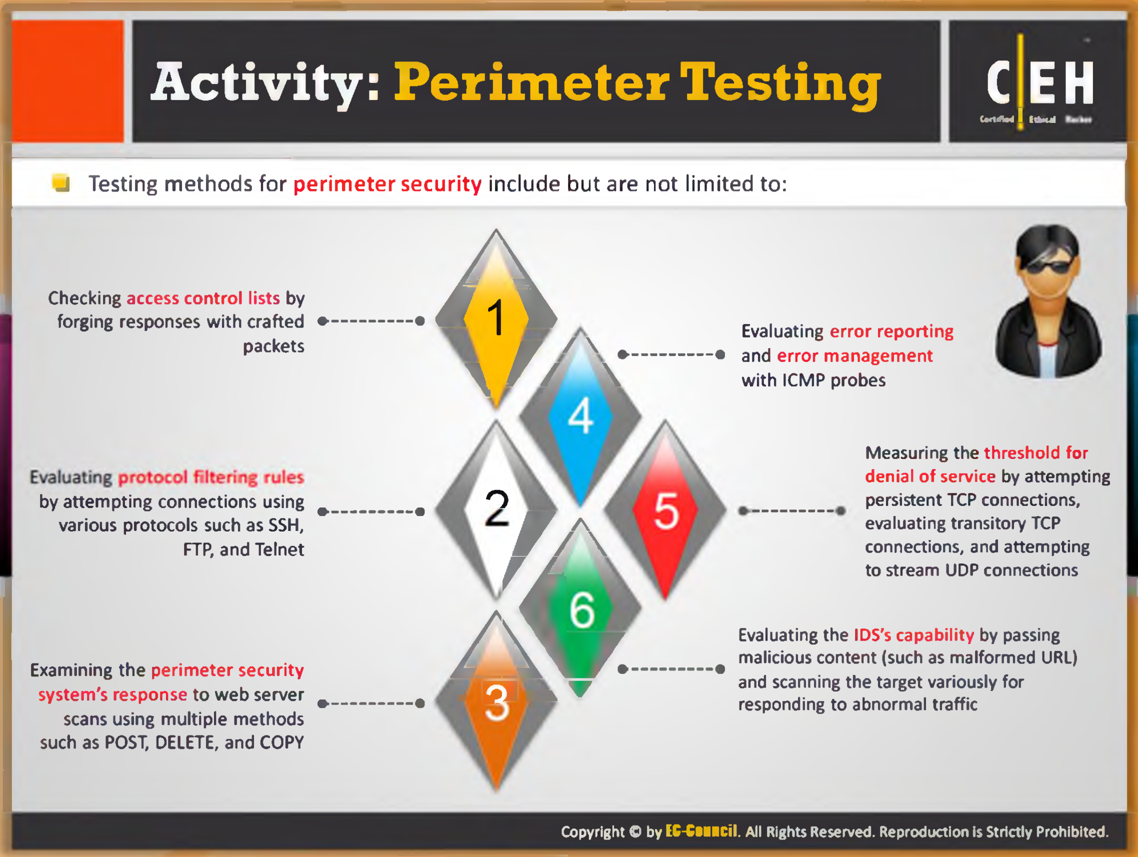

Attack Phase
CEH
Certified Ethical Hacker
Penetrate Perimeter
Escalate Privileges
1
2
3
4
Acquire Target
Execute, Implant, Retract
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attack Phase

This stage involves the actual compromise of the target. The attacker may exploit a vulnerability discovered during the pre-attack phase or use **security loopholes** such as a weak security policy to gain rights to the system. The important point here is that the attacker needs only one port of entry, whereas the organizations are left to defend several. Once inside, the attacker may escalate his privileges and install a backdoor so that he or she sustains access to the system and exploits it in order to achieve his/her **malicious** intent.

During the attack phase, the attacker or pen tester needs to:

- Penetrate perimeter
- Execute, implant, retract
- Acquire target
- Escalate rrivileges



Activity: Perimeter Testing

- Testing methods for perimeter security include but are not limited to:

1. Checking access control lists by forging responses with crafted packets
2. Evaluating protocol filtering rules by attempting connections using various protocols such as SSH, FTP, and Telnet
3. Examining the perimeter security system's response to web server scans using multiple methods such as POST, DELETE, and COPY
4. Evaluating error reporting and error management with ICMP probes
5. Measuring the threshold for denial of service by attempting persistent TCP connections, evaluating transitory TCP connections, and attempting to stream UDP connections
6. Evaluating the IDS's capability by passing malicious content (such as malformed URL) and scanning the target variously for responding to abnormal traffic

Activity: Perimeter Testing

Social engineering is an ongoing activity through the testing phase as sensitive information can be acquired at any stage of testing. The tests that can be carried out in this context include (but are not limited to) impersonating or mocking phone calls to capture sensitive information, verifying information gathered through activities such as dumpster diving. Other means include email testing, trusted person acquisition, and attempts to retrieve legitimate authentication details such as passwords and access privileges. Information gathered here can be used later in web application testing also.

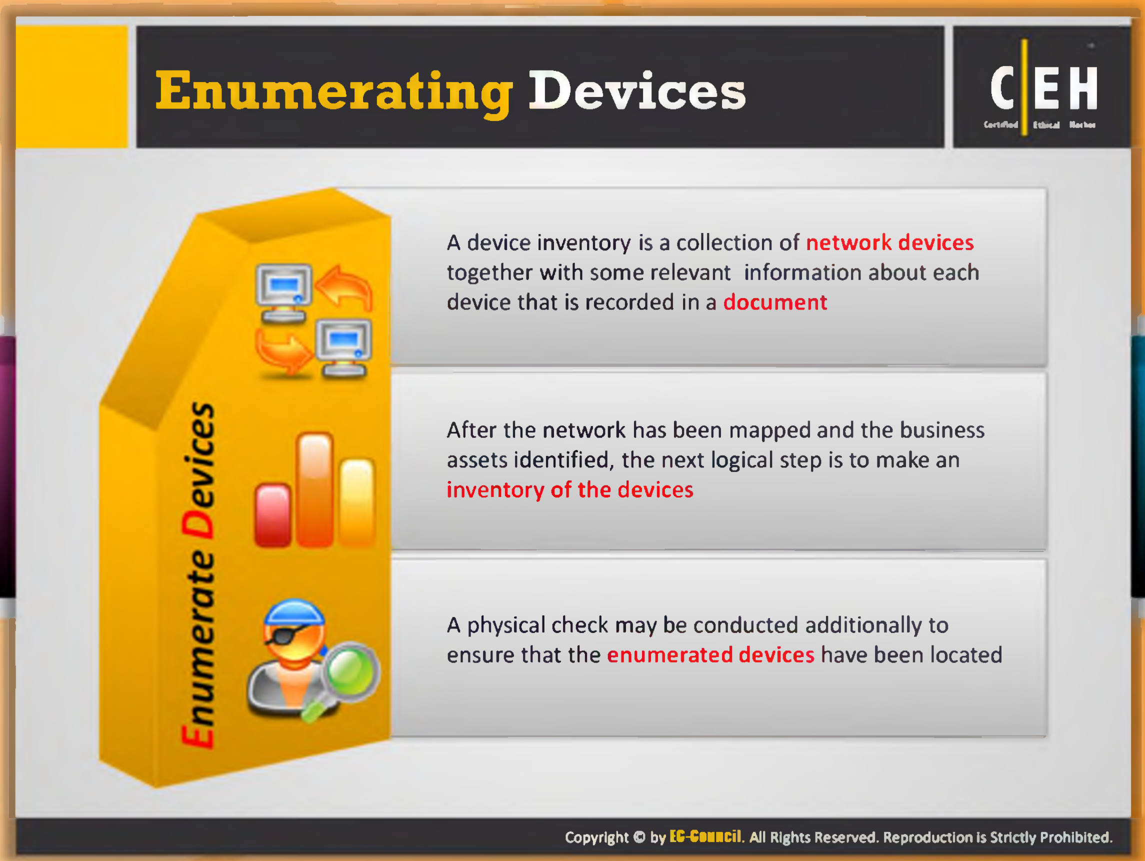
Firewall Testing: The information gained during the pre-attack phase using techniques such as firewalking is further exploited here. Attempts are made to evade the IDS and bypass the firewall.

The processes include but are not limited to:

Crafting and sending packets to check firewall rules. For example, sending SYN packets to test stealth detection. This determines the nature of various packet responses through the firewall. A SYN packet can be used to enumerate the target network. Similarly, other port scans with different flags set can be used to attempt enumeration of the network. This also gives an indication of the source port control on the target.

Usually, perimeter testing measures the firewall's ability to handle fragmentation: big packet fragments, overlapping fragments, flood of packets, etc. Testing methods for **perimeter security** include but are not limited to:

- Evaluating error reporting and error management with ICMP probes
- Checking access control lists with crafted packets
- Measuring the threshold for denial-of-service by attempting persistent TCP connections, evaluating transitory TCP connections, and attempting streaming UDP connection
- Evaluating protocol-filtering rules by attempting connections using various protocols such as SSH, FTP, and Telnet
- Evaluating IDS capability by passing malicious content (such as malformed URLs) and scanning the target for response to abnormal traffic



Enumerating Devices

Enumerate Devices

A device inventory is a collection of network devices together with some relevant information about each device that is recorded in a document

After the network has been mapped and the business assets identified, the next logical step is to make an inventory of the devices

A physical check may be conducted additionally to ensure that the enumerated devices have been located

Enumerating Devices

A device inventory is a collection of network devices, together with some relevant information about each device, which is recorded in a document. After the network has been mapped and the business assets identified, the next logical step is to make an inventory of the devices.

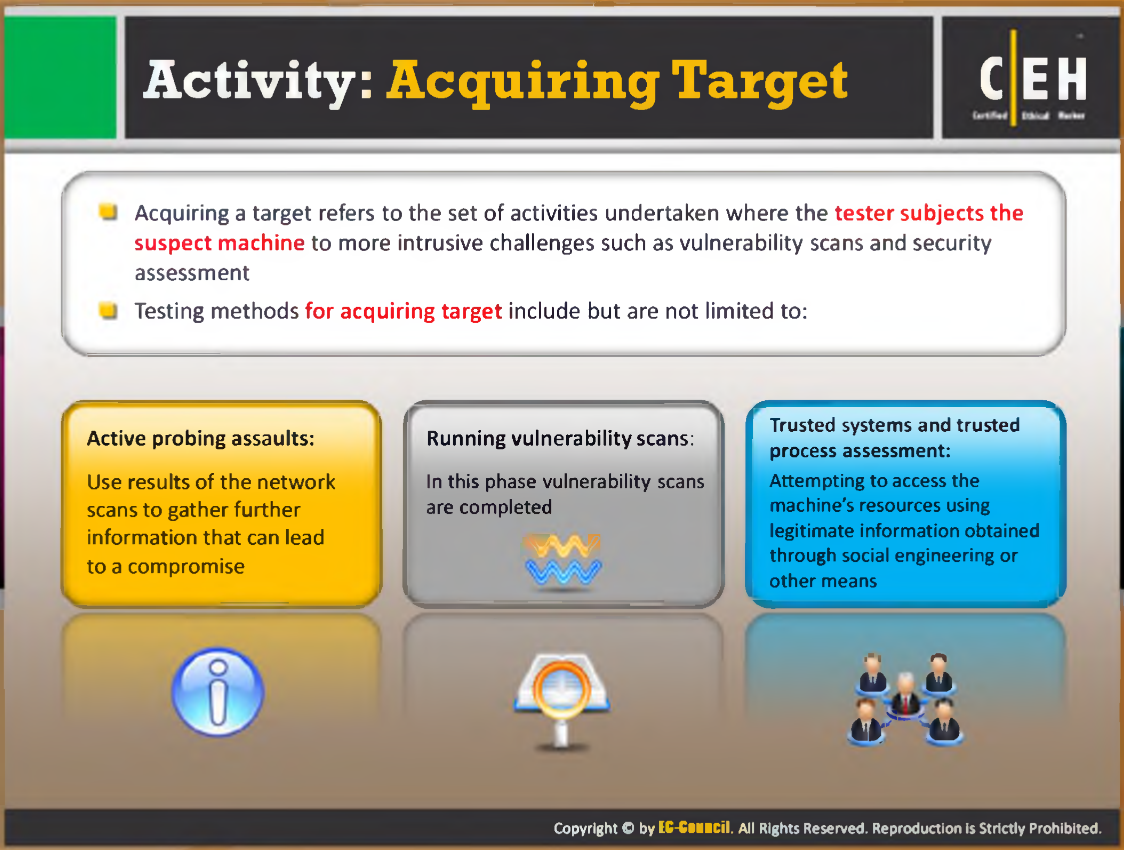
During the initial stages of the pen test, the devices may be referred to by their identification on the network such as IP address, MAC address, etc. This can be done by pinging all devices on the network or by using device enumeration tools.

Later, when there is a physical security check, devices may be cross checked regarding their location and identity. This step can help to identify unauthorized devices on the network. The other method is to do ping sweeps to detect responses from devices and later correlate the results with the actual inventory.

The likely parameters to be captured in an inventory sheet would be:

- Device ID
- Description
- Hostname
- Physical location
- IP address
- MAC address

- Network accessibility



Activity: Acquiring Target

- Acquiring a target refers to the set of activities undertaken where the tester subjects the suspect machine to more intrusive challenges such as vulnerability scans and security assessment
- Testing methods for acquiring target include but are not limited to:

Active probing assaults:

Use results of the network scans to gather further information that can lead to a compromise

Running vulnerability scans:

In this phase vulnerability scans are completed

Trusted systems and trusted process assessment:

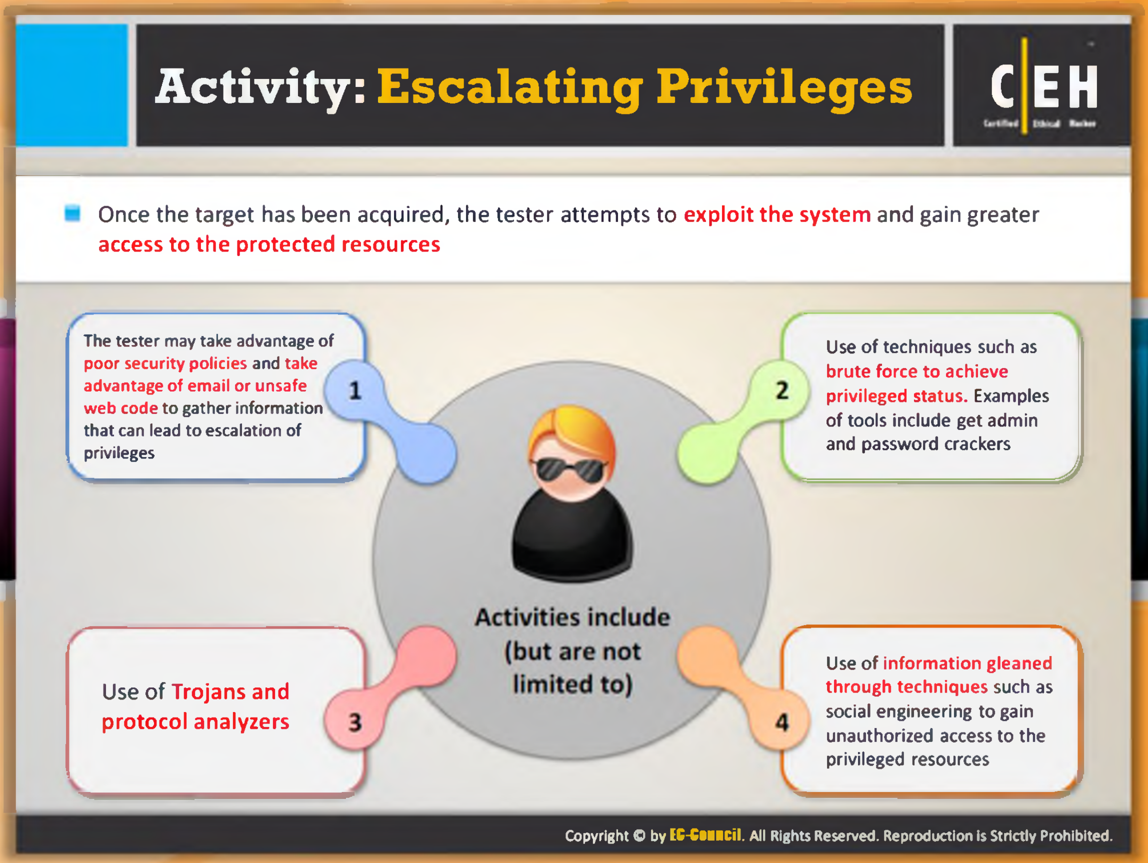
Attempting to access the machine's resources using legitimate information obtained through social engineering or other means

Activity: Acquiring Target

Usually, target acquisition refers to all the activities that are undertaken to unearth as much information as possible about a particular machine or systems so that it can be used later in the actual process of exploitation. Here, acquiring a target is referred to as the set of activities undertaken where the tester subjects the targeted machine to more intrusive challenges such as vulnerability scans and security assessment. This is done to obtain more information about the target and can be used in the exploit phase.

Examples of such activities include subjecting the machine to:

- **Active probing assaults**: Use the results of network scans to gather further information that can lead to a compromise.
- **Running vulnerability scans**: Vulnerability scans are completed in this phase.
- **Trusted systems and trusted process assessment**: Attempting to access the machine's resources using legitimate information obtained through social engineering or other means.



Activity: Escalating Privileges

- Once the target has been acquired, the tester attempts to exploit the system and gain greater access to the protected resources

Activities include (but are not limited to)

1. The tester may take advantage of poor security policies and take advantage of email or unsafe web code to gather information that can lead to escalation of privileges
2. Use of techniques such as brute force to achieve privileged status. Examples of tools include get admin and password crackers
3. Use of Trojans and protocol analyzers
4. Use of information gleaned through techniques such as social engineering to gain unauthorized access to the privileged resources

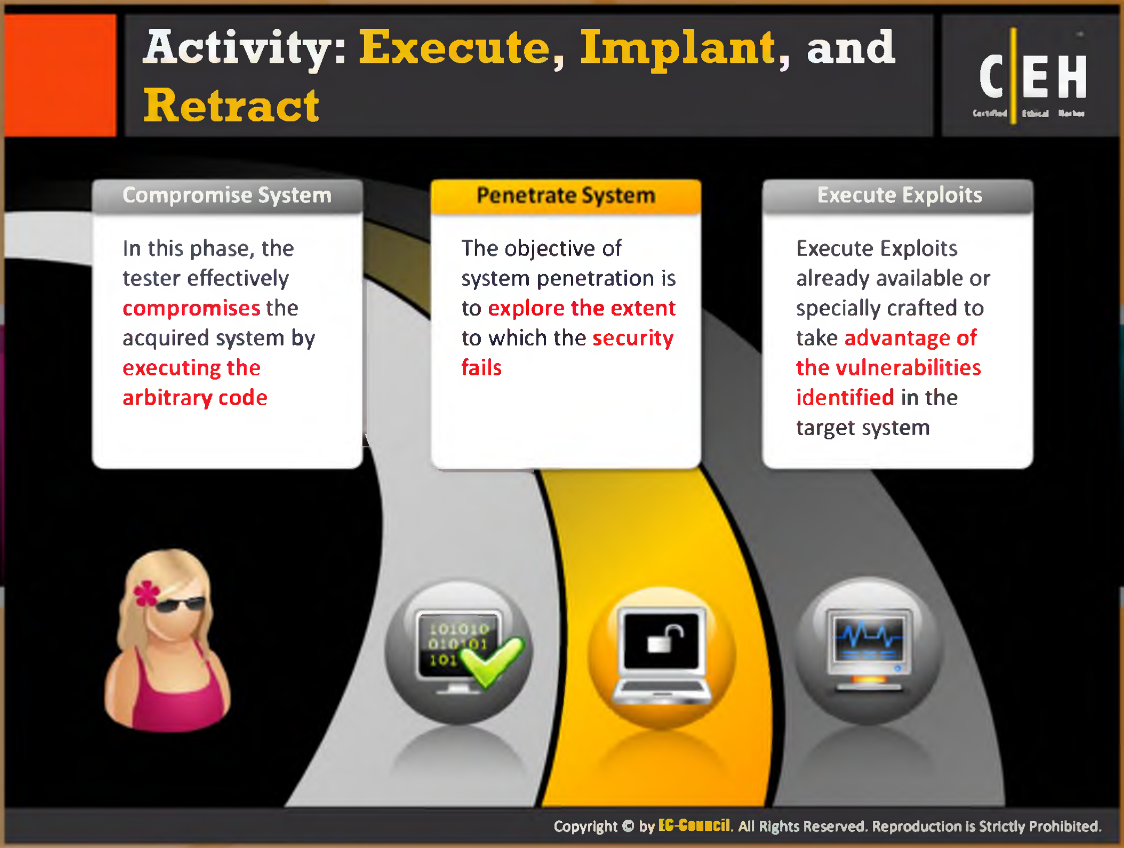
Activity: Escalating Privileges

When an attacker succeeds in gaining unauthorized access into a system or network, the degree of escalation depends on the various authorizations possessed by an attacker. The ultimate aim of an attacker would be to gain the highest possible administration privilege that gives access to the **entire network, sensitive information, online banking** etc.

Once the target has been acquired, the tester attempts to exploit the system and gain greater access to the protected resources

Activities include (but are not limited to):

- The tester may take advantage of poor security policies and take advantage of email or unsafe web code to gather information that can lead to the escalation of privileges
- Use of techniques such as brute force to achieve privileged status. Examples of tools include get admin and password crackers
- Use of Trojans and protocol analyzers
- Use of information gleaned through techniques such as social engineering to gain **unauthorized access** to the privileged resources



Activity: Execute, Implant, and Retract

Compromise System

In this phase, the tester effectively **compromises** the acquired system by **executing the arbitrary code**

Penetrate System

The objective of system penetration is to **explore the extent** to which the **security fails**

Execute Exploits

Execute Exploits already available or specially crafted to take **advantage of the vulnerabilities identified** in the target system

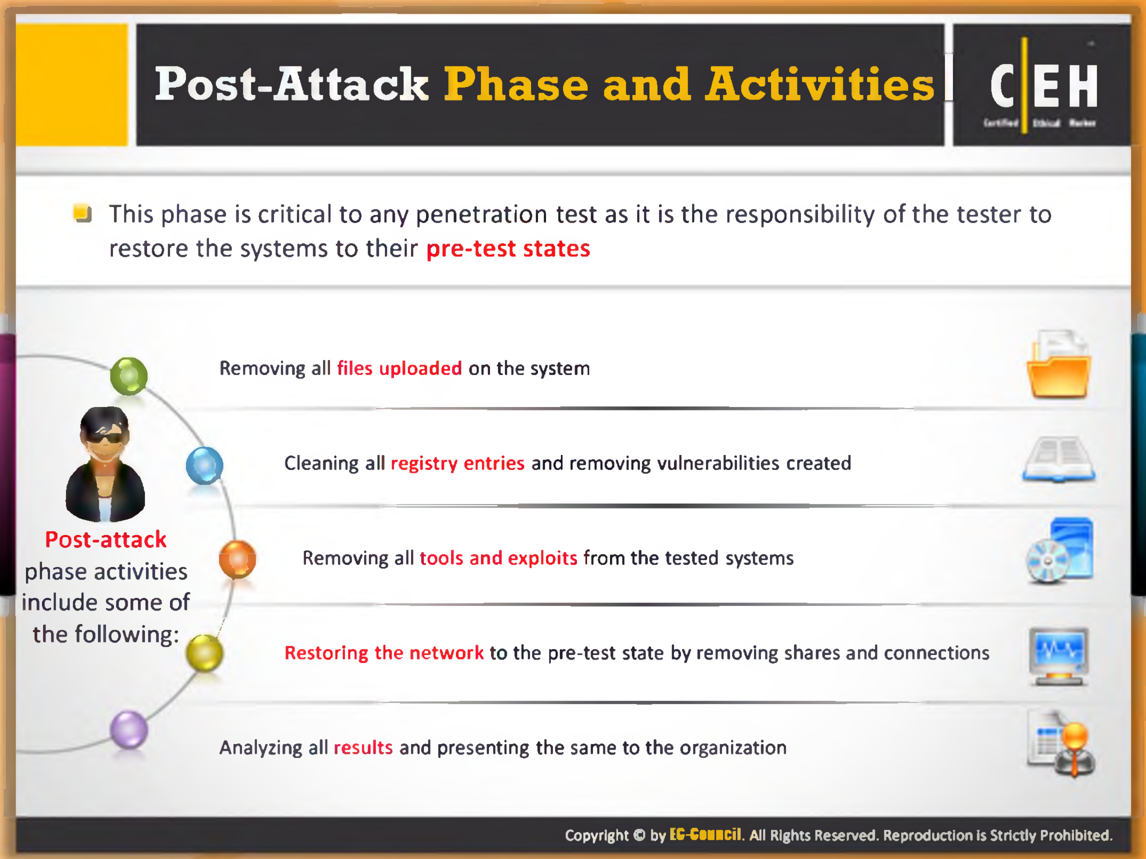
Activity: Execute, Implant, and Retract

In this phase, the tester effectively compromises the acquired system by executing the arbitrary code. The objective here is to explore the extent to which security fails. The tester attempts to execute the **arbitrary code**, hides files in the compromised system, and leaves the system without raising alarms. He or she then attempts to re-enter the system **stealthily**. Activities include:

- Executing exploits to take advantage of the vulnerabilities identified on the target system.
- Exploiting buffer overflows in order to trick the system into running arbitrary code.
- Executing activities that are usually subjected to containment measures such as the use of **Trojans** and **rootkits**.

Activities in the retract phase include manipulation of audit log files to remove traces of the activities:

- Examples include use of tools such as audit poll. The tester may also change settings within the system to remain inconspicuous during a re-entry and change log settings.
- The tester may re-enter the system using the backdoor implanted by the tester.



Post-Attack Phase and Activities

- This phase is critical to any penetration test as it is the responsibility of the tester to restore the systems to their **pre-test states**

Post-attack phase activities include some of the following:

- Removing all **files uploaded** on the system
- Cleaning all **registry entries** and removing vulnerabilities created
- Removing all **tools and exploits** from the tested systems
- **Restoring the network** to the pre-test state by removing shares and connections
- Analyzing all **results** and presenting the same to the organization

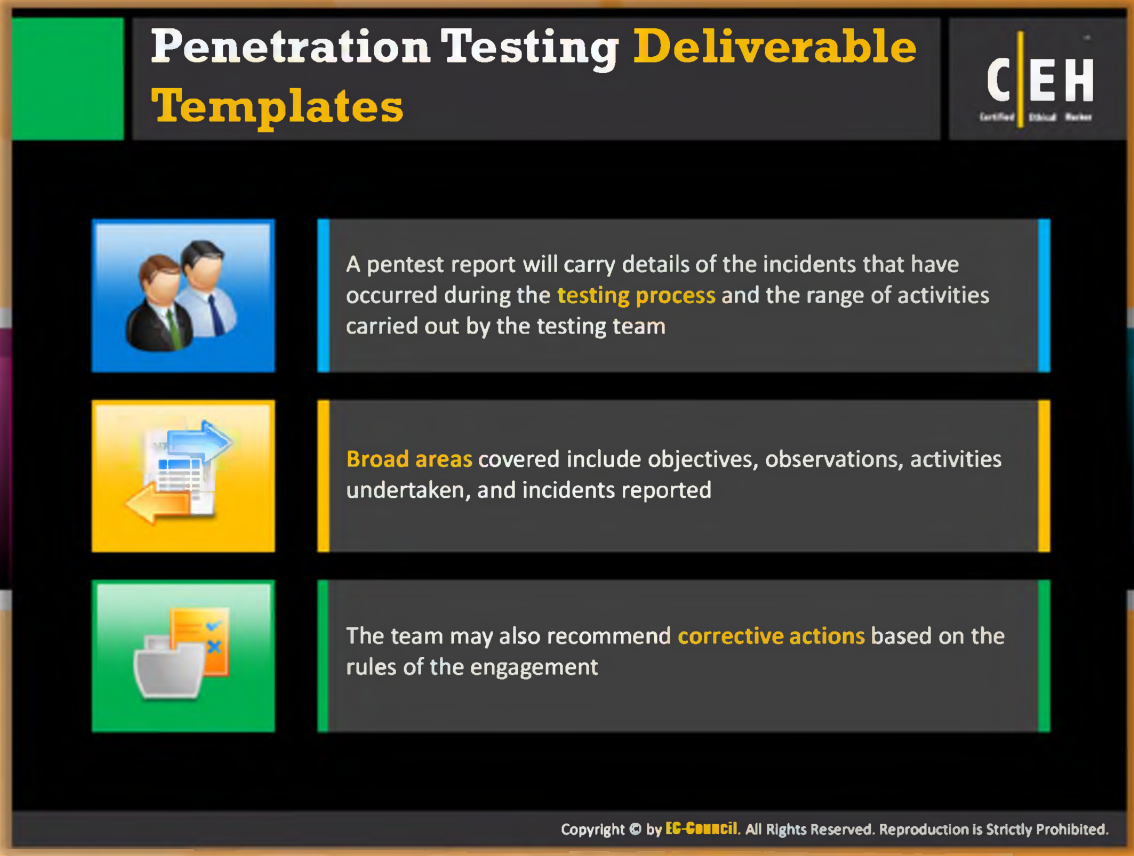
Post-attack Phase and Activities

This phase is critical to any penetration test as it is the responsibility of the tester to restore the systems to a pre-test state. The objective of the test is to show where **security fails**, and unless there is a scaling of the penetration test agreement, whereby the tester is assigned the responsibility to correct the security posture of the systems, this phase must be completed.

Activities in this phase include (but are not restricted to):

- Removing all files uploaded on the system
- Cleaning all registry entries and removing vulnerabilities created
- Reversing all file and setting manipulations done during the test
- Reversing all changes in privileges and user settings
- Removing all tools and exploits from the tested systems
- Restoring the network to the pre-test stage by removing shares and connections
- Mapping of the network state
- Documenting and capturing all logs registered during the test
- Analyzing all results and presenting them to the organization

The penetration tester should document all his or her activities and record all observations and results so that the test can be repeatable and verifiable for the given **security posture** of the organization. For the organization to quantify the security risk in business terms, it is essential that the tester should identify critical systems and critical resources and map the threat to these.



Penetration Testing Deliverable Templates

A pentest report will carry details of the incidents that have occurred during the testing process and the range of activities carried out by the testing team

Broad areas covered include objectives, observations, activities undertaken, and incidents reported

The team may also recommend corrective actions based on the rules of the engagement

Penetration Testing Deliverable Templates

A pen test report carries details of the incidents that have occurred during the testing process and the range of activities that the testing team carries out.

It captures the objectives as agreed upon in the rules of engagement and provides a brief description of the observations from the **testing engagement**.

Under the activities carried out will be all the tests, the devices against which the tests were conducted, and the preliminary observations. These are usually **cross-referenced** to the appropriate **test log entry**.

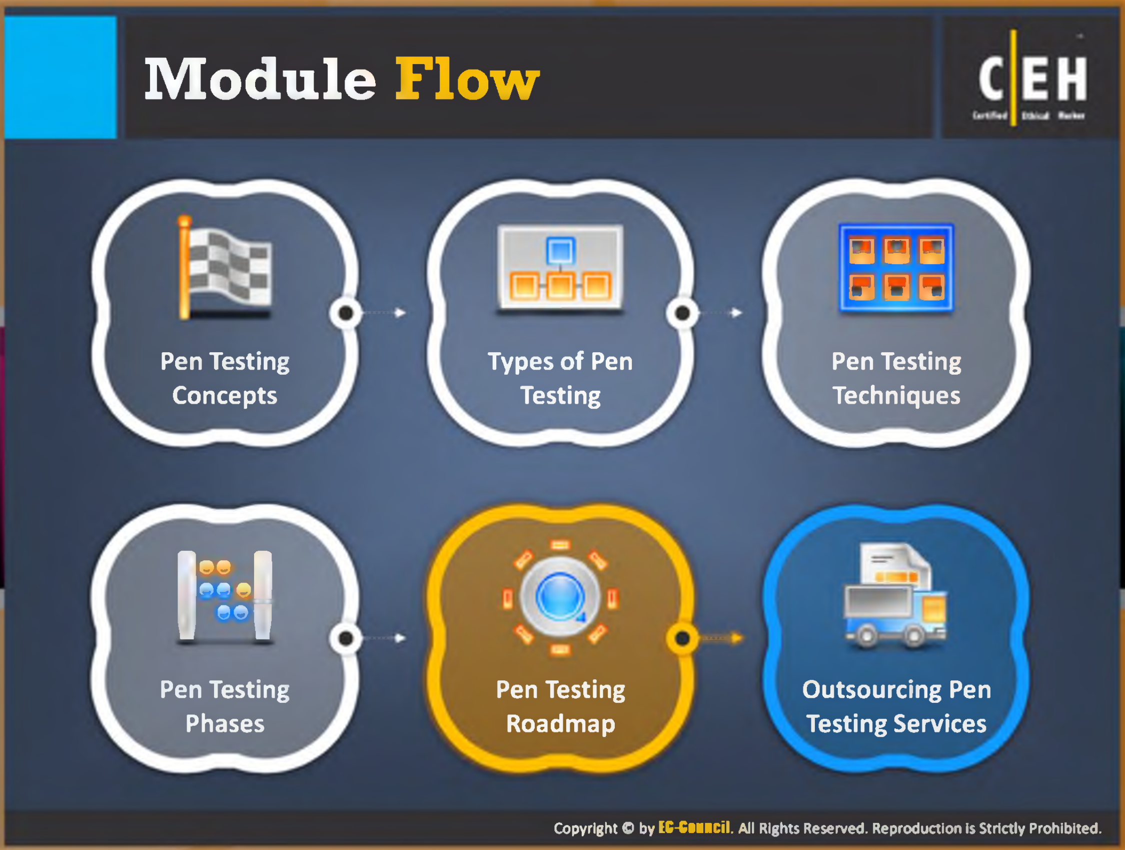
Other information that can be captured under incident description can include:

- A detailed description of the incident
- The date and time when the incident occurred
- Contact information for the person who observed the incident
- The stage of testing during which the incident occurred
- A description of the steps taken to create the incident. This can be supplemented by screen captures
- Observations on whether the incident can be repeated or not

- Details on the tool (if detected), the name and version of the tool, and if relevant, any custom configuration settings

Under risk analysis, the impact of the test is captured from a business perspective. The information included is:

- The initial estimate of the relative severity of the incident to the business
- The initial estimate of the relative likelihood (or frequency) of the incident reoccurring in production
- The initial estimate of the cause of the incident

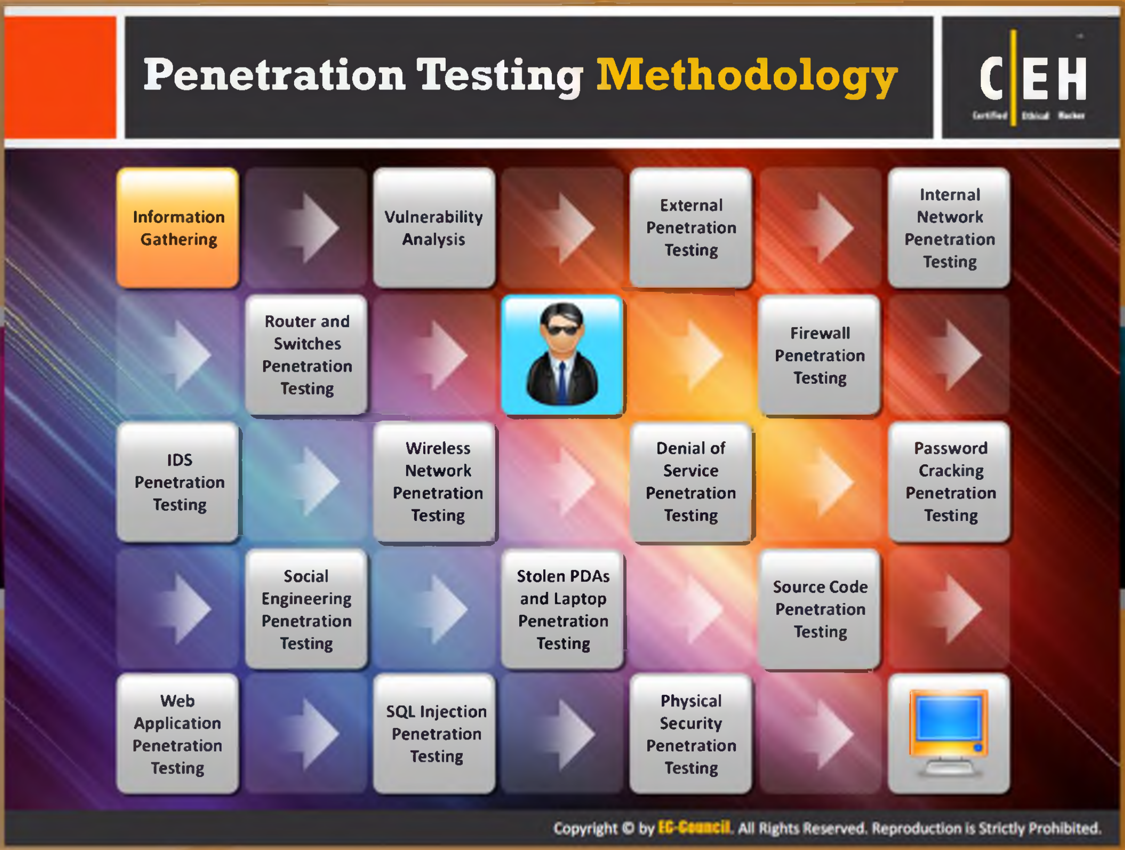


Module Flow

Pen Testing Roadmap

A penetration test is a technique that evaluates or audits the security of a computer system or other facility by launching an attack from a malicious source. It also proves how vulnerable that a computer system would be in the event of the real attack. The rules, practices, methods as well as procedures implemented, followed during the course of any information security audit program are defined by pen testing methodology. This methodology defines you a roadmap with proven practices as well as practical ideas that are to be handled with care for assessing the system security correctly. A detailed explanation about the pen testing roadmap is given in the next slides.

Pen Testing Concepts	Types of Pen Testing
Pen Testing Techniques	Pen Testing Phases
Pen Testing Roadmap	Outsourcing Pen Testing Services



Penetration Testing Methodology

Information Gathering

Vulnerability Analysis

External Penetration Testing

Internal Network Penetration Testing

Router and Switches Penetration Testing

Firewall Penetration Testing

IDS Penetration Testing

Wireless Network Penetration Testing

Denial of Service Penetration Testing

Password Cracking Penetration Testing

Social Engineering Penetration Testing

Stolen PDAs and Laptop Penetration Testing

Source Code Penetration Testing

Web Application Penetration Testing

SQL Injection Penetration Testing

Physical Security Penetration Testing

Penetration Testing Methodology

The following are the various phases in the penetration testing methodology:

Information Gathering

Information gathering is one of the major steps of the penetration testing. It is the first phase in the penetration testing process. It is done using various tools, scanners, online sources, sending simple http requests, specially crafted requests, etc.

Vulnerability Analysis

Vulnerability analysis is a method of identifying vulnerabilities on a network. It provides an overview of the flaws that exist in a system or network.

External Penetration Testing

An external penetration test is conducted to know whether the external network is secure or not. In external penetration testing, hacking is done in the same way the actual attacker does but without causing any harm to the network. This helps in making the network more secure. Various methods used in external penetration testing are:

- Footprinting
- Public Information & Information Leakage

- DNS Analysis & DNS Brute forcing
- Port Scanning
- System Fingerprinting
- Services Probing
- Exploit Research
- Manual Vulnerability Testing and Verification of Identified Vulnerabilities
- Intrusion Detection/Prevention System Testing
- Password Service Strength Testing
- Remediation Retest (optional)

Internal Network Penetration Testing

In internal network penetration testing, all the possible internal network flaws are identified and simulated as if a real attack has taken place. Various methods used for the internal network penetration testing are:

- Internal Network Scanning
- Port Scanning
- System Fingerprinting
- Services Probing
- Exploit Research
- Manual Vulnerability Testing and Verification
- Manual Configuration Weakness Testing and Verification
- Limited Application Layer Testing
- Firewall and ACL Testing
- Administrator Privileges Escalation Testing
- Password Strength Testing
- Network Equipment Security Controls Testing
- Database Security Controls Testing
- Internal Network Scan for Known Trojans
- Third-Party/Vendor Security Configuration Testing

Router and Switches Penetration Testing

Router switches penetration is carried out to determine:

- End to end router security
- Bandwidth and speed of the internet connection

- Data transfer speed
- Router performance
- Router Security assessment

Firewall Penetration Testing

Firewall penetration testing is one of the most useful methods in analyzing security effectiveness. Through this method, you can identify how secure your firewall network is against the attacks performed by network intruders.

IDS Penetration Testing

An intrusion detection system (IDS) can be software or hardware. IDS penetration testing helps you to test the strength of the IDS. It can be performed with the help of tools such as IDS informer, an evasion gateway, etc.

Wireless Network Penetration Testing

Wireless networks are more economical than wired networks. Though wireless networks are cheaper, there are various risks associated with them. A wireless network is less protected than a wired one. Therefore, wireless networks must be tested strictly and the respective security enhancements must be applied.

Denial-of-Service Penetration Testing

The main purpose of a denial-of-service (DoS) attack is to slow down the website or even to crash it by sending too many requests, more than a particular server can handle. If the attacker knows the details of the server and its technical specifications, it becomes more vulnerable. Sometimes DoS is done on a trial and error basis. So the penetration tester must check how much the website or server can withstand. It is also necessary to provide an alternative way to react to the situation when the limit exceeds.

Password Cracking Penetration Testing

Passwords are used to protect computer resources from unauthorized access. Password cracking penetration testing identifies the vulnerabilities associated with password management. This helps in avoiding various kinds of malicious attacks such as brute force attacks, hybrid attacks, and dictionary attacks, etc.

Social Engineering Penetration Testing

Social engineering is a method used by attackers to get crucial information of a company. Attackers especially target individuals within the organization to gather as much information as possible about the company. This is completely documented and then the employees are educated about possible social engineering attacks and cautioned about various threats.

Stolen Laptops, PDAs, and Cell Phones Penetration Testing

The penetration tester should find out the possible loopholes in physical locality and identify the various ways that an intruder can enter into the company. Once the important electronic devices that contain sensitive information of the company are stolen, you can extract information from these stolen devices. Therefore, such penetration testing proves very beneficial. Penetration tests are done especially on senior members of the company as their PDAs, laptops and mobile phones often contain sensitive information.

Source Code Penetration Testing

The penetration tester should perform source code analysis by using some source code analysis tools. These tools will help the pen tester to detect the vulnerabilities in the source code.

Application Penetration Testing

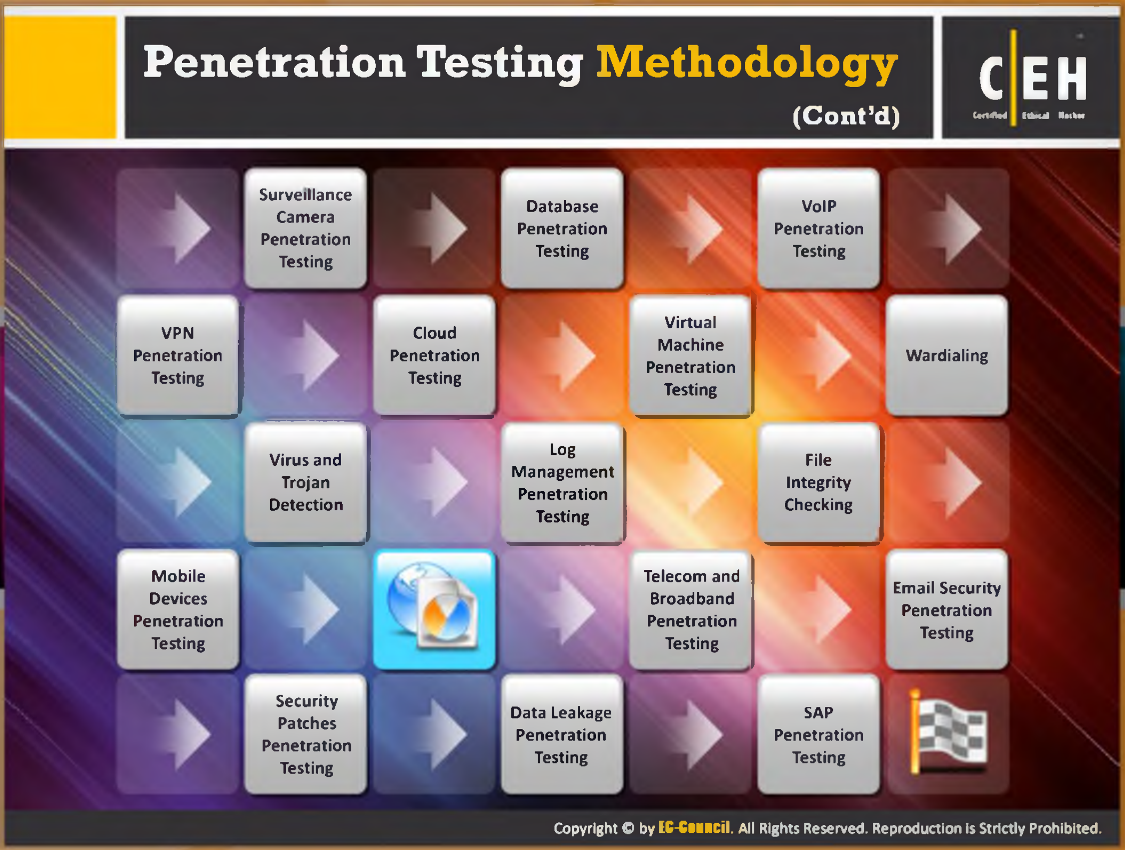
Programmers may make some mistakes at the time of software creation. Those mistakes can become potential vulnerabilities. Application penetration testing helps in determining the design error of the software.

SQL Injection Penetration Testing

The penetration tester should perform SQL injection penetration testing on the application in order to find out vulnerabilities in the application. The pen tester should try to simulate different types of SQL injection attacks to find the possible vulnerabilities.

Physical Security Penetration Testing

Here the penetration tester tries to gain physical access to the organizational resources before, during, and after business hours. All the physical security controls must be properly tested.



Penetration Testing Methodology (Cont'd)

Surveillance Camera Penetration Testing

Database Penetration Testing

VoIP Penetration Testing

VPN Penetration Testing

Cloud Penetration Testing

Virtual Machine Penetration Testing

Wardialing

Virus and Trojan Detection

Log Management Penetration Testing

File Integrity Checking

Mobile Devices Penetration Testing

Telecom and Broadband Penetration Testing

Email Security Penetration Testing

Security Patches Penetration Testing

Data Leakage Penetration Testing

SAP Penetration Testing

Penetration Testing Methodology

Surveillance Camera Penetration Testing

A surveillance camera can be used to monitor the live target. The surveillance camera can be prone to security flaws due to non-robust design of the **web interface** created for the surveillance camera activities. As a pen tester, you should try to find out vulnerabilities in the web interface of the surveillance camera. You should do the following things to test the surveillance camera:

- The web interface should be completely debugged
- Try to look for the injection points from where the motion images are included remotely
- Validate the image path
- Create the different motion picture recorder and editor in order to validate motion or picture recoded by the surveillance camera whether they are same or not

Database Penetration Testing

In this process, a penetration tester tries to directly access data contained in the database or indirectly accessing the data through triggers or stored procedures executed by a database engine. This method helps in avoiding **unauthorized access** of **data**.

VoIP Penetration Testing

In VoIP penetration testing, access to the VOIP network is attempted to record the conversations and even a DoS attack may also be used to find out the company's security policies.

VPN Penetration Testing

Sometimes, employees are allowed to work from home or remotely and in such situations, there are lot of security issues associated with VPN. So the penetration team attempts to gain access to the VPN through a remote endpoint or a VPN tunnel and check the vulnerabilities.

Cloud Penetration Testing

Cloud computing systems are widespread today. There are risks associated with cloud computing. The organizations must figure out these risks and apply proper security mechanisms to protect against potential risks. To find out the vulnerabilities in a cloud-based application, conduct a penetration test on the cloud.

Virtual Machine Penetration Testing

An attacker can exploit the virtual machine security flaw by running malicious code on the virtual machine. The pen tester needs to find out the vulnerabilities in the VM by simulating the actions of an attacker before a real attack occurs.

War Dialing

Dial-up modems used by the companies have various vulnerabilities. These allow attackers to hack a system or network easily. Wardialing penetration testing will be useful:

- To identify the vulnerabilities of the modems.
- To know the passwords related vulnerabilities.
- To know whether there is any open access to organizations systems or not.

Virus and Trojan Detection

Viruses and Trojans are the most widespread malicious software today. Once on the system and networks, these are very dangerous. Early detection of viruses and Trojans is very important.

Log Management Penetration Testing

A management log contains a record of all the events that use a data grid network. It contains the complete track of events such as status of node, agent transmission, job request, etc. Therefore, proper log management helps in tracking any malicious activity such as unauthorized access from outside attackers at an early stage.

File Integrity Checking

Checking the integrity of a file is the best way to tell whether it is corrupted or not. It involves checking the following things:

- File size
- Version
- When it was created
- When it was modified
- The login name of any user who modifies the file
- Its attributes (e.g., Read-Only, Hidden, System, etc.)

Mobile Devices Penetration Testing

In mobile penetration testing, the pen tester tries to access and manipulate the data on the particular mobile device simulating all possible attacks such as using social engineering, uploading malicious code, etc. Mobile device penetration pinpoints and addresses gaps in end-user awareness and security exposures in these devices before attackers actually misuse and compromise them.

Telecom and Broadband Penetration Testing

The pen tester tries to determine the vulnerabilities in the broadband connection of the particular corporate network. The pen tester simulates different types of attacks such as unauthorized access, installation of malicious software, DoS attacks on broadband connections to check whether the network withstands these types of attacks.

Email Security Penetration Testing

Email security penetration testing helps to check all the vulnerabilities associated with an email mechanism.

Security Patches Penetration Testing

Unless the system or software is updated with the latest security patches, it is vulnerable to attacks. Poorly designed security patches have more vulnerability so testing them helps in resolving such issues.

Data Leakage Penetration Testing

Penetration testing of data leakage helps in the following ways:

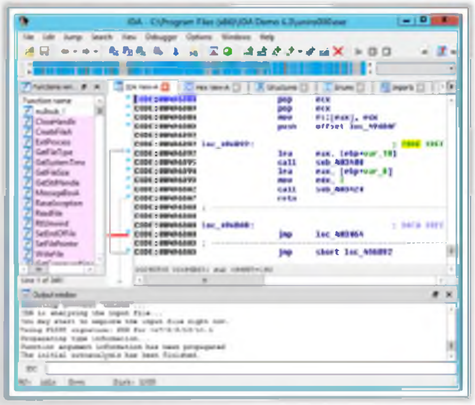
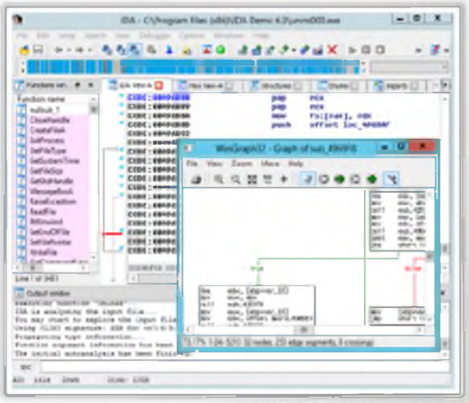
- Preventing confidential information from going out to the market or to competitors
- Allows increasing internal compliance level for data protection
- Improvesawareness amongst employees on Safe Practices
- Will be useful to easily demonstrates compliance to regulations
- Controls exposure with workflows for mitigation

SAP Penetration Testing

Attackers may be able to break into SAP platform and can perform espionage, sabotage, and **fraud attacks on business-critical information**. The SAP penetration testing service simulates the process performed by an attacker. In SAP penetration testing, the pen tester tries to find the vulnerabilities in the SAP platform by conducting different types of attacks, and then checks whether he or she is able to break into the SAP platform.

Application Security Assessment

- Application security assessment is an in-depth analysis of applications to identify and assess security vulnerabilities that can expose the organization's sensitive information
- This test checks on application so that a malicious user cannot access, modify, or destroy data or services within the system

http://www.hex-rays.com

Application Security Assessment

Application security assessment is done by a security professional to identify security vulnerabilities and significant issues.

Application security assessment involves:

- Inspection of application validation and bounds checking for both accidental and mischievous input.
- Manipulation of client-side code and locally stored information such as session information and configuration files.
- Examination of application-to-application interaction between system components such as the web service and back-end data sources.
- Discovery of opportunities that could be utilized by an attacker to escalate their permissions.
- Examination of event logging functionality.
- Examination of authentication methods in use for their robustness and resilience to various subversion techniques.

Even in a well-deployed and secured infrastructure, a weak application can expose the organization's crown jewels to unacceptable risk.

Application security assessment is designed to identify and assess threats to the organization through **bespoke** or proprietary applications or systems. This test checks the application so that a malicious user cannot access, modify, or destroy data or services within the system.

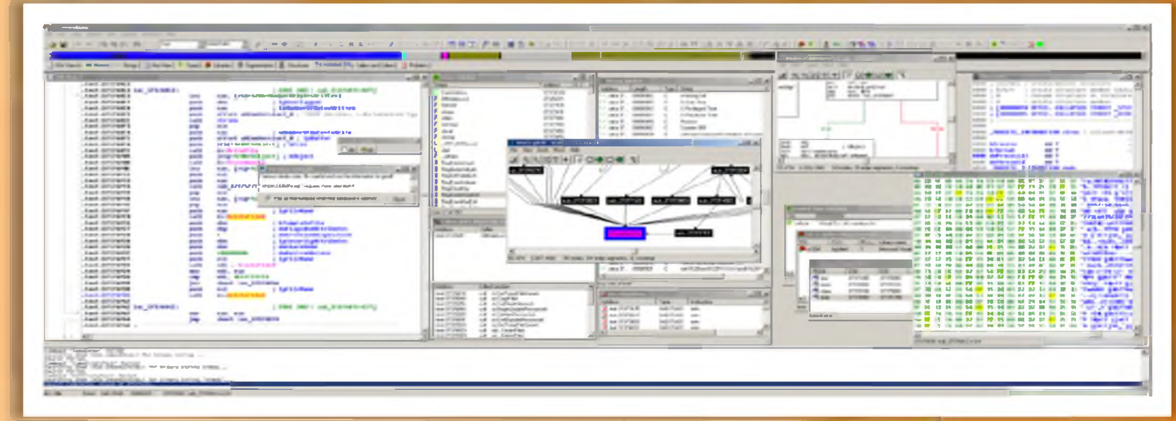
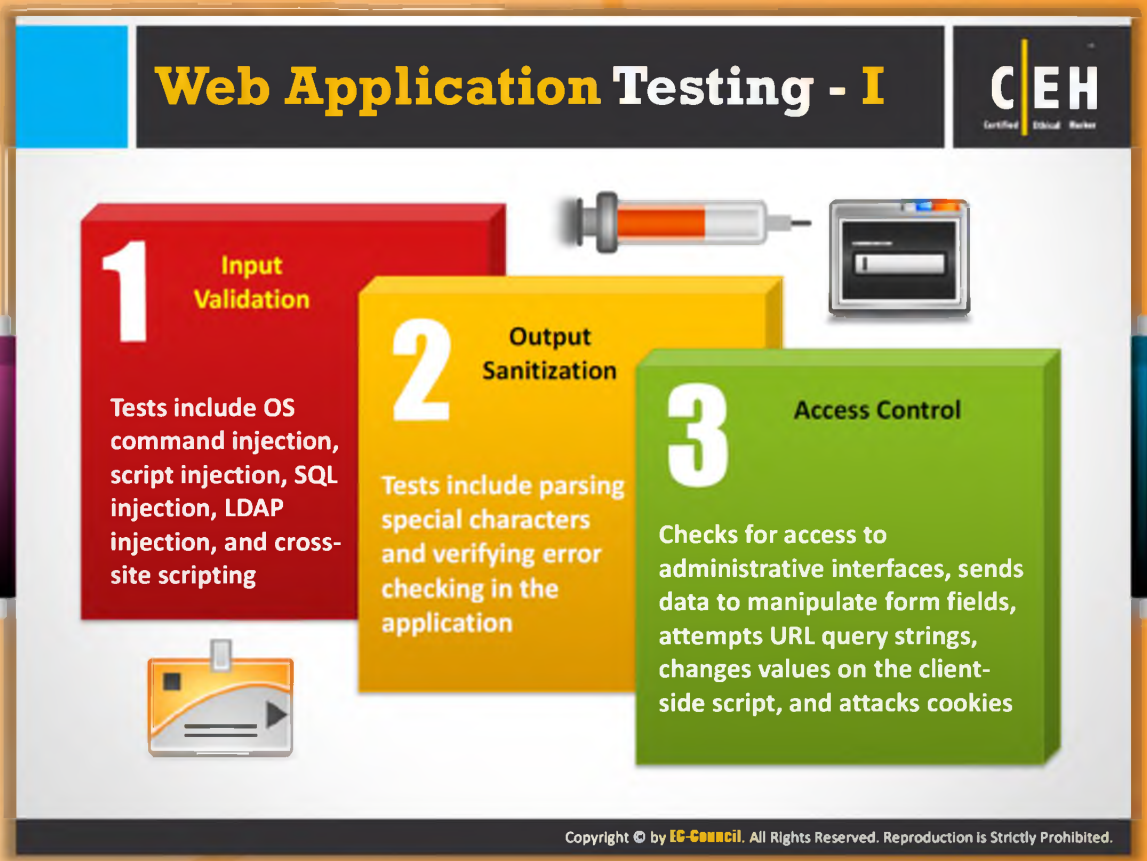


FIGURE 20.2: Application security assessment screenshot



Web Application Testing - I

1 Input Validation

Tests include OS command injection, script injection, SQL injection, LDAP injection, and cross-site scripting

2 Output Sanitization

Tests include parsing special characters and verifying error checking in the application

3 Access Control

Checks for access to administrative interfaces, sends data to manipulate form fields, attempts URL query strings, changes values on the client-side script, and attacks cookies

Web Application Testing – I

This test phase can be carried out as the tester proceeds to acquire the target.

Input validation

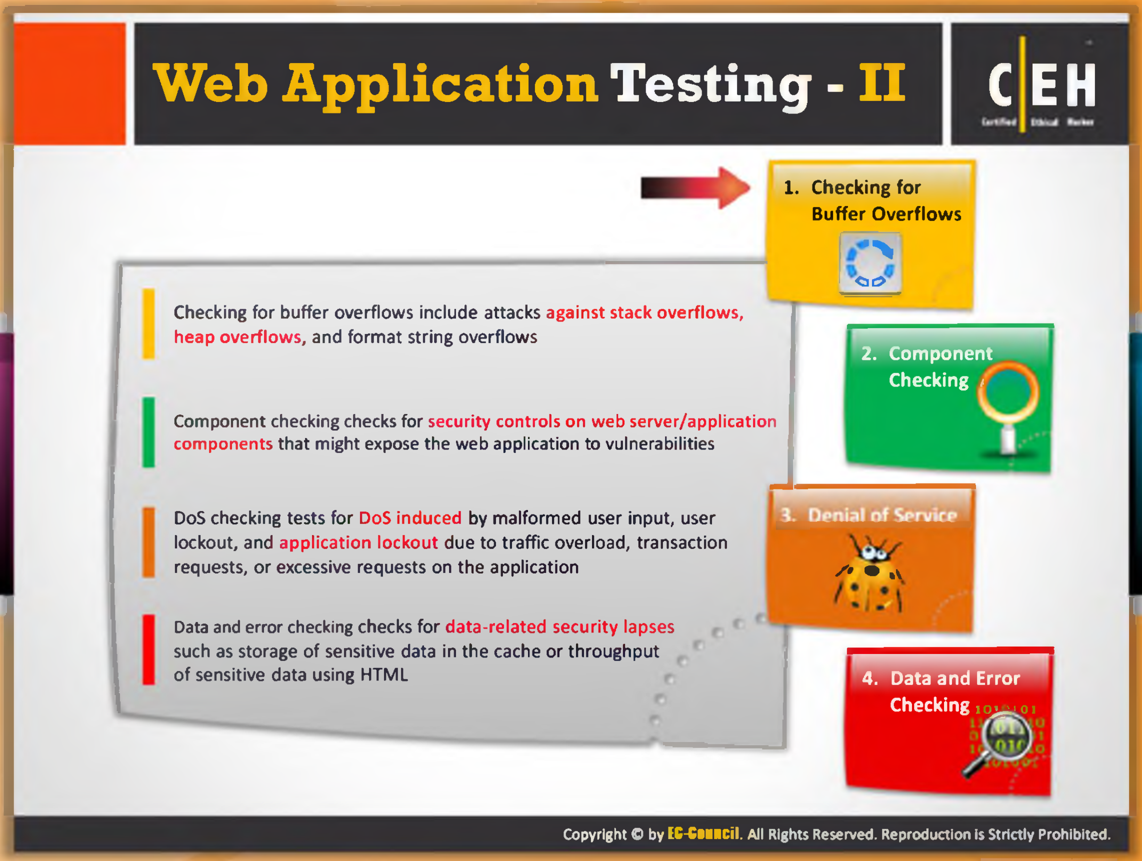
Tests include OS command injection, script injection, SQL injection, LDAP injection, and cross-site scripting. Other tests include checking for dependency on the external data and the source verification.

Output sanitization

Tests include parsing special characters and verifying error checking in the application.

Access control

The tester checks access to administrative interfaces, transfers data for manipulating form fields, checks URL query strings, changes the values of client-side script, and attacks cookies. Other tests include checking for authorization breaches, enumerating assets accessible through the application, lapses in event handling sequences, proxy handling, and compliance with least privilege access rule.



Web Application Testing - II

Checking for buffer overflows include attacks against stack overflows, heap overflows, and format string overflows

Component checking checks for security controls on web server/application components that might expose the web application to vulnerabilities

DoS checking tests for DoS induced by malformed user input, user lockout, and application lockout due to traffic overload, transaction requests, or excessive requests on the application

Data and error checking checks for data-related security lapses such as storage of sensitive data in the cache or throughput of sensitive data using HTML

Web Application Testing - II

Checking for Buffer Overflows

Tests include attacks against stack overflows, heap overflows, and format string overflows.

Denial–of-service

Test for DoS is induced due to malformed user input, user lockout, and application lockout due to traffic overload, transaction requests, or excessive requests on the application.

Component checking

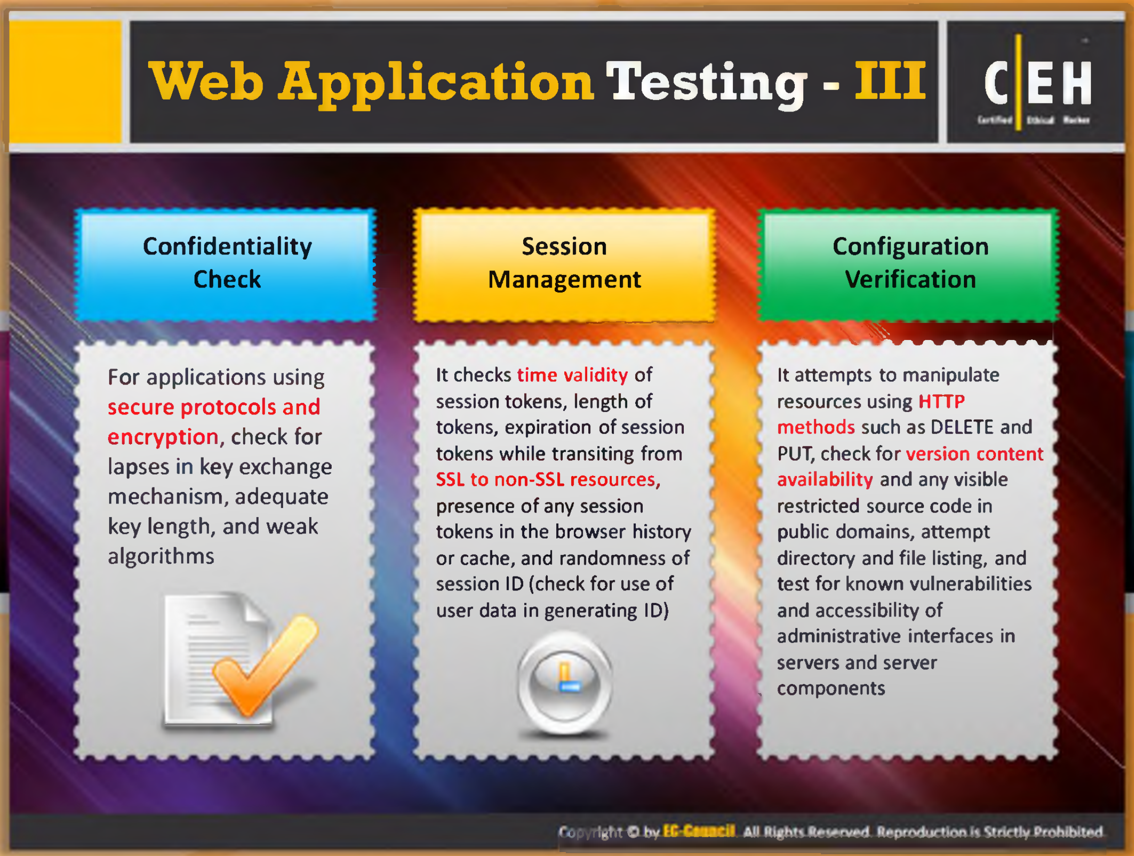
Check for security controls on web server/application components might expose the web application to vulnerabilities, such as basic authentication.

Data and error checking

Check for data-related security lapses such as storage of sensitive data in the cache or input of sensitive data using HTML. Check for verbose error messages that give away more details of the application than necessary and error type.

SQL injection techniques

SQL injection may be attempted against web applications to gain access to the **target system**.



Web Application Testing - III

Confidentiality Check

For applications using secure protocols and encryption, check for lapses in key exchange mechanism, adequate key length, and weak algorithms

Session Management

It checks time validity of session tokens, length of tokens, expiration of session tokens while transiting from SSL to non-SSL resources, presence of any session tokens in the browser history or cache, and randomness of session ID (check for use of user data in generating ID)

Configuration Verification

It attempts to manipulate resources using HTTP methods such as DELETE and PUT, check for version content availability and any visible restricted source code in public domains, attempt directory and file listing, and test for known vulnerabilities and accessibility of administrative interfaces in servers and server components

Web Application Testing - III

Confidentiality check

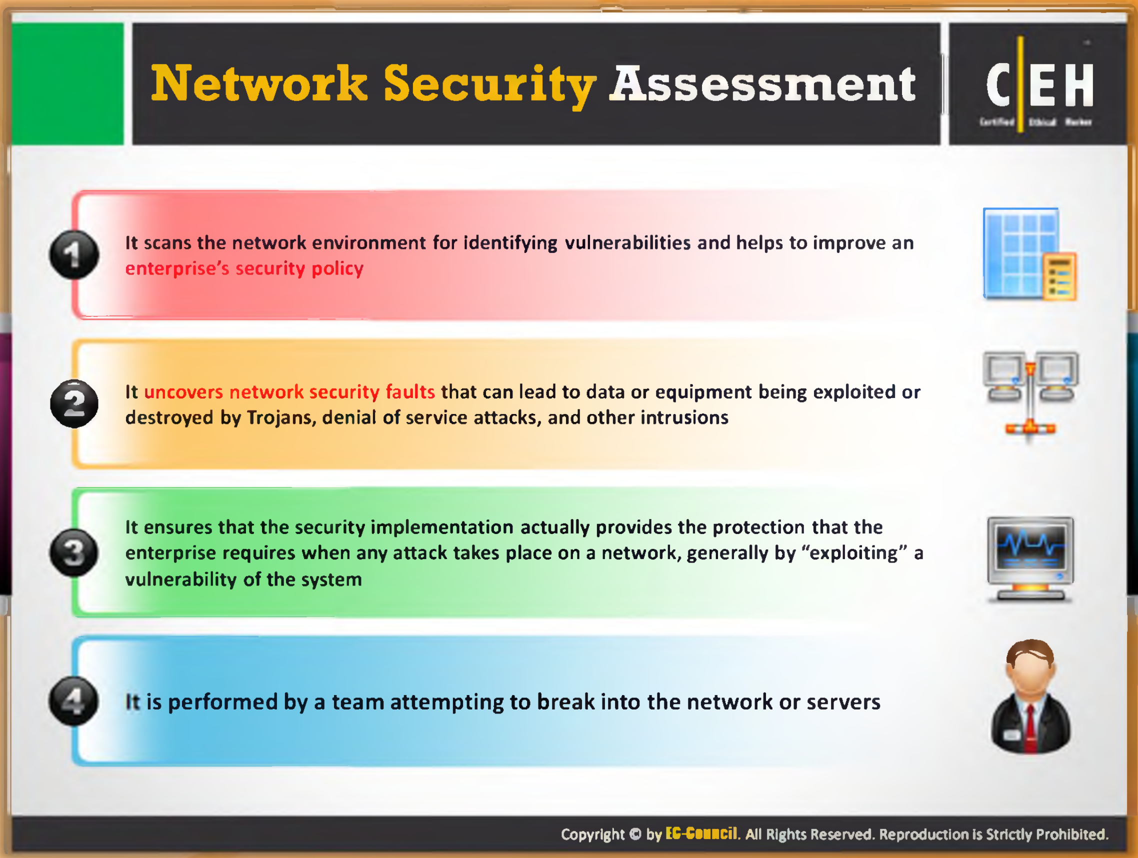
For applications using secure protocols and encryption, check for lapses in key exchange mechanism, inadequate key length, and weak algorithms. Validate authentication schemes by attempting user enumeration through login or a recovery process. Check digital certificates and use a signature verification process.

Session management

Check time validity of session tokens, length of tokens, and expiration of session tokens while transiting from SSL to non-SSL resources, presence of any session tokens in the browser history or cache, and randomness of session ID (check for use of user data in generating an ID).

Configuration verification

Attempt manipulation of resources using HTTP methods such as DELETE and PUT, check for version content availability, and any visible restricted source code in public domains, attempt directory, and file listing, test for known vulnerabilities, and accessibility of administrative interfaces in the server and server components.



Network Security Assessment

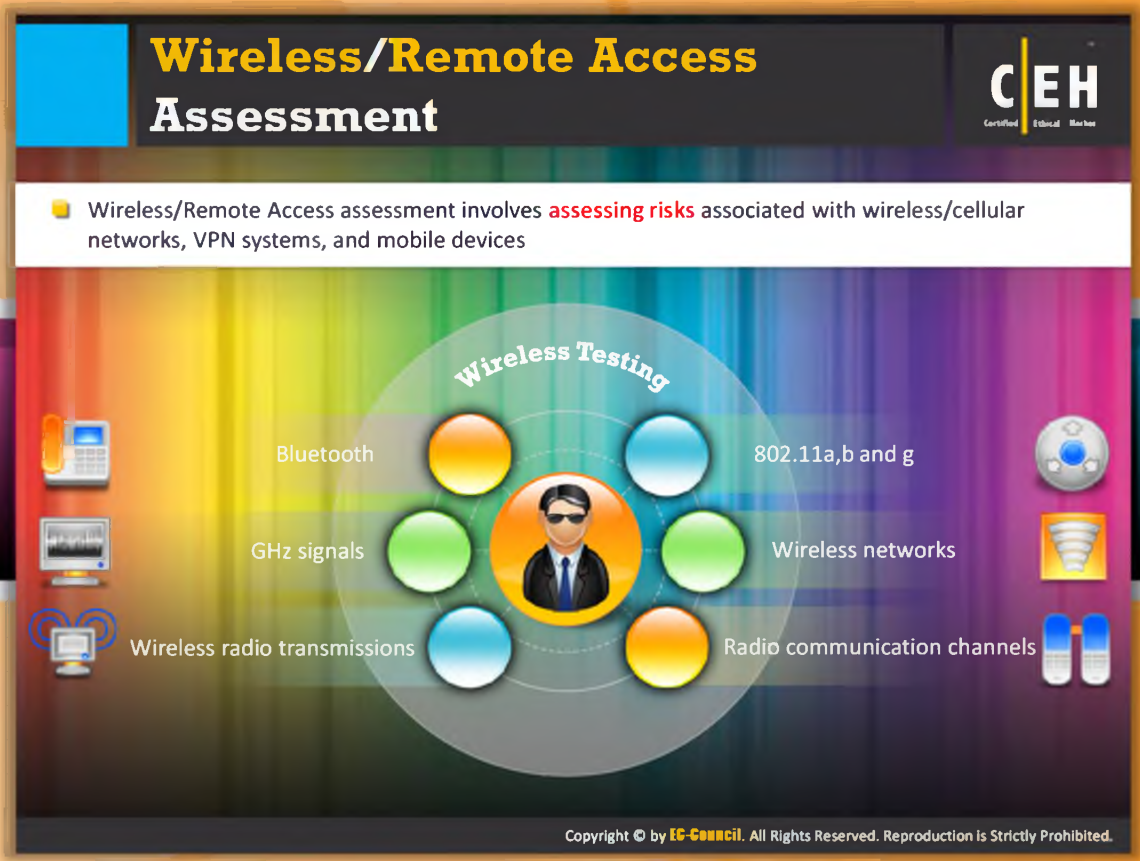
CEH
Certified Ethical Hacker

1. It scans the network environment for identifying vulnerabilities and helps to improve an enterprise's security policy
2. It uncovers network security faults that can lead to data or equipment being exploited or destroyed by Trojans, denial of service attacks, and other intrusions
3. It ensures that the security implementation actually provides the protection that the enterprise requires when any attack takes place on a network, generally by "exploiting" a vulnerability of the system
4. It is performed by a team attempting to break into the network or servers

Network Security Assessment

Network security assessment is an effective method to protect the systems from external attacks. Vulnerabilities present in routers, firewalls, DNS, web and database servers, and other systems become a doorway to attackers to perform attacks. Network assessment helps in reducing the risks related to networks. It gives a more clear idea about the risks posed by external and internal attackers.

- It scans the network environment for identifying vulnerabilities and helps to improve an enterprise's security policy
- It uncovers network security faults that can lead to data or equipment being exploited or destroyed by Trojans, denial-of-service attacks, and other intrusions
- It ensures that the security implementation actually provides the protection that the enterprise requires when any attack takes place on a network, generally by "exploiting" a vulnerability of the system
- It is performed by a team attempting to break into the network or servers



Wireless/Remote Access Assessment

- Wireless/Remote Access assessment involves assessing risks associated with wireless/cellular networks, VPN systems, and mobile devices

Wireless Testing

Bluetooth

802.11a,b and g

GHz signals

Wireless networks

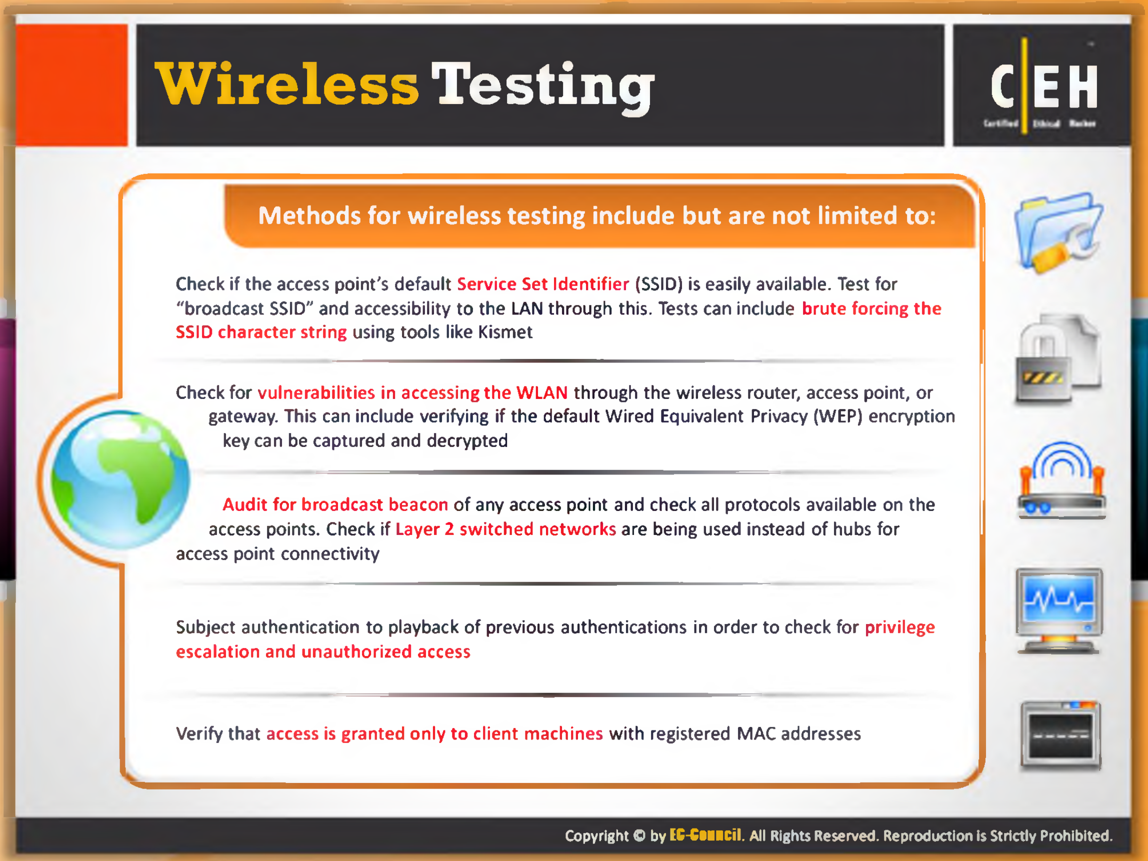
Wireless radio transmissions

Radio communication channels

Wireless/Remote Access Assessment

Wireless/remote access assessment addresses the security risks associated with an increasing mobile workforce. Wireless networking has various benefits as well as security risks. Assessment includes testing the following things:

- Bluetooth
- 802.11a,b and g
- Wireless networks
- Radio communication channels
- Wireless radio transmissions
- GHz signals



Wireless Testing

Methods for wireless testing include but are not limited to:

- Check if the access point's default Service Set Identifier (SSID) is easily available. Test for "broadcast SSID" and accessibility to the LAN through this. Tests can include brute forcing the SSID character string using tools like Kismet
- Check for vulnerabilities in accessing the WLAN through the wireless router, access point, or gateway. This can include verifying if the default Wired Equivalent Privacy (WEP) encryption key can be captured and decrypted
- Audit for broadcast beacon of any access point and check all protocols available on the access points. Check if Layer 2 switched networks are being used instead of hubs for access point connectivity
- Subject authentication to playback of previous authentications in order to check for privilege escalation and unauthorized access
- Verify that access is granted only to client machines with registered MAC addresses

Wireless Testing

A wireless network can be attacked in **multiple ways** and conducting a penetration test is difficult process here, compared to a wired network. To launch the attack against wireless networks, attackers use various methods such as:

- Denial-of-service attacks
- Man-in-the-middle attacks
- ARP poisoning attacks

Methods for wireless testing include but are not limited to:

- Check if the access point's default **Service Set Identifier (SSID)** is easily available. Test for "broadcast SSID" and accessibility to the LAN through this. Tests can include brute forcing the SSID character string using tools like Kismet
- Check for vulnerabilities in accessing the WLAN through the wireless router, access point, or gateway. This can include verifying if the default Wired Equivalent Privacy (WEP) encryption key can be captured and decrypted

- Audit for a **broadcast beacon** of any access point and check all protocols available on the access points. Check if Layer 2 switched networks are being used instead of hubs for access point connectivity
- Subject authentication to playback of previous authentications in order to check for privilege escalation and unauthorized access
- Verify that access is granted only to client machines with registered MAC addresses

Telephony Security Assessment

A telephony security assessment is performed to identify vulnerabilities in corporate voice technologies that might result in toll fraud, eavesdropping on calls, unauthorized access to voice mail systems, DoS attack, etc.

Telephone security assessment includes security assessment of PBXs, Voice over IP (VoIP) systems, modems, mailboxes, etc.

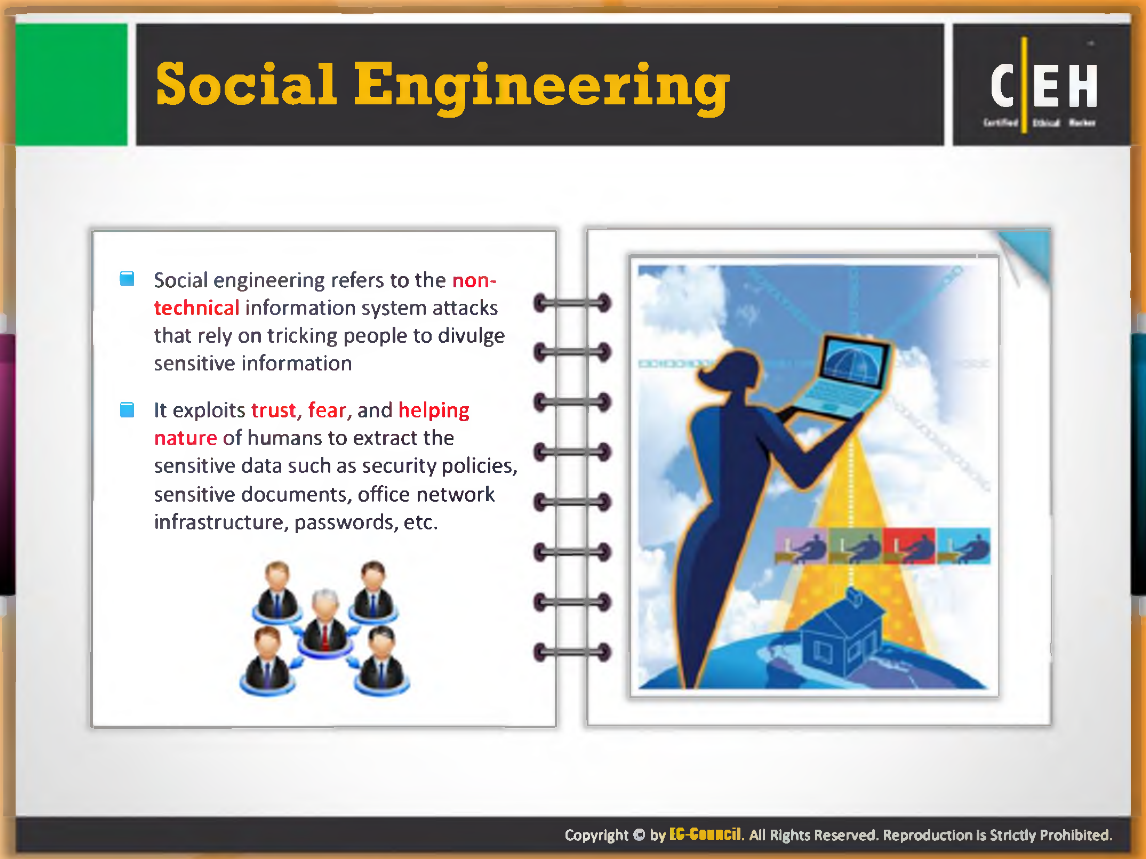
Telephony Security Assessment

The main objective of a telephony assessment is to conduct:

- Toll fraud
- Eavesdropping on telephone calls
- Unauthorized access to voicemail system

A telephony security assessment addresses security concerns relating to **corporate voice technologies.** This includes the abuse of PBXs by outsiders to route calls at the **target's expense**, mailbox deployment and security, voice over IP (VoIP) integration, unauthorized modem use, and associated risks. Telephony security assessment consists of:

- PBX testing
- Voicemail testing
- FAX review
- Modem testing



Social Engineering

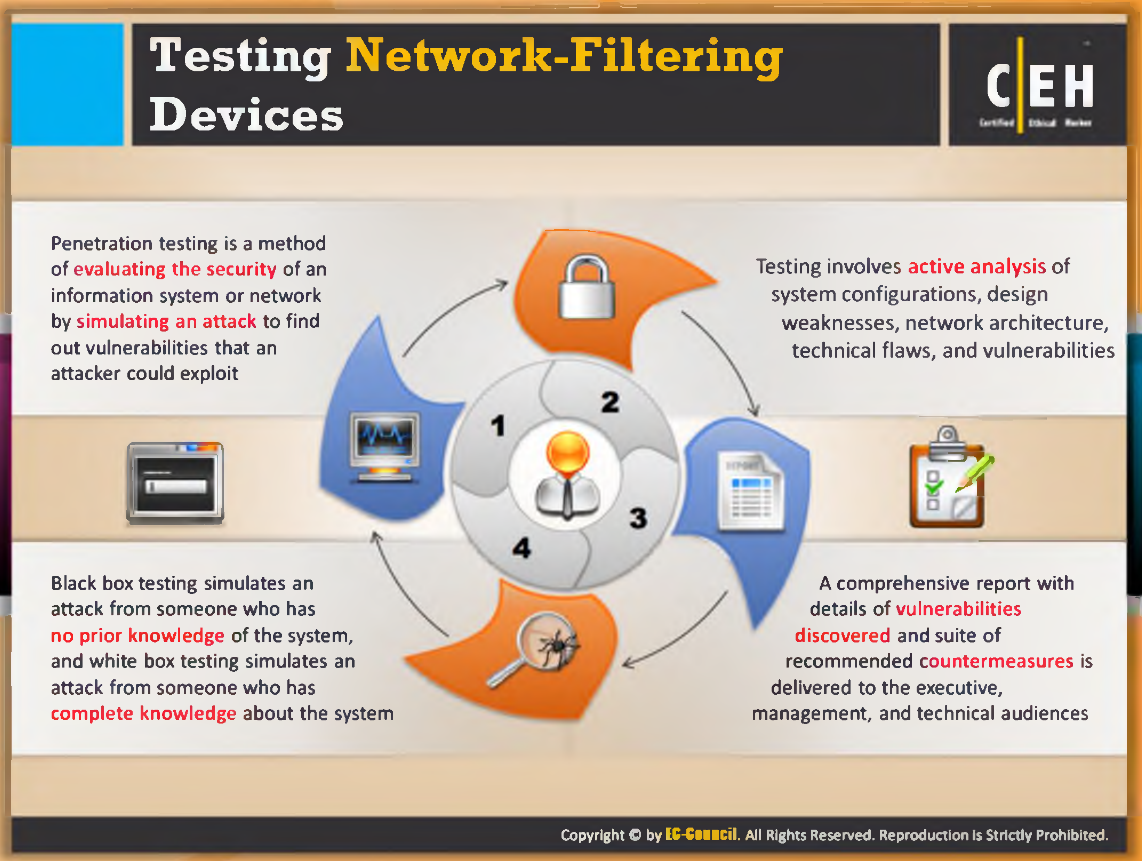
- Social engineering refers to the non-technical information system attacks that rely on tricking people to divulge sensitive information
- It exploits trust, fear, and helping nature of humans to extract the sensitive data such as security policies, sensitive documents, office network infrastructure, passwords, etc.

Social Engineering

Social engineering refers to the method of influencing and persuading people to reveal sensitive information in order to perform some malicious action. You can use this to gather confidential information, authorization details, and access details by deceiving and manipulating people.

All security measures adopted by the organization are in vain when employees get "socially engineered" by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam emails, and bragging in front of co-workers.

Most often, people are not even aware of a security lapse on their part. Possibilities are that they divulge information to a potential attacker inadvertently. Attackers take special interest in developing social engineering skills, and are so proficient that their victims don't even realize that they have been scammed. Despite having security policies in the organization they can be compromised because social engineering attacks target the weakness of people to be helpful for launching their attack. Attackers always look for new ways to gather information; they ensure that they know the people on the perimeter—security guards, receptionists, and help desk workers—in order to exploit the human's oversight. People have been conditioned not to be overly suspicious; they associate certain behavior and appearances with known entities.



Testing Network-Filtering Devices

Penetration testing is a method of evaluating the security of an information system or network by simulating an attack to find out vulnerabilities that an attacker could exploit

Testing involves active analysis of system configurations, design weaknesses, network architecture, technical flaws, and vulnerabilities

Black box testing simulates an attack from someone who has no prior knowledge of the system, and white box testing simulates an attack from someone who has complete knowledge about the system

A comprehensive report with details of vulnerabilities discovered and suite of recommended countermeasures is delivered to the executive, management, and technical audiences

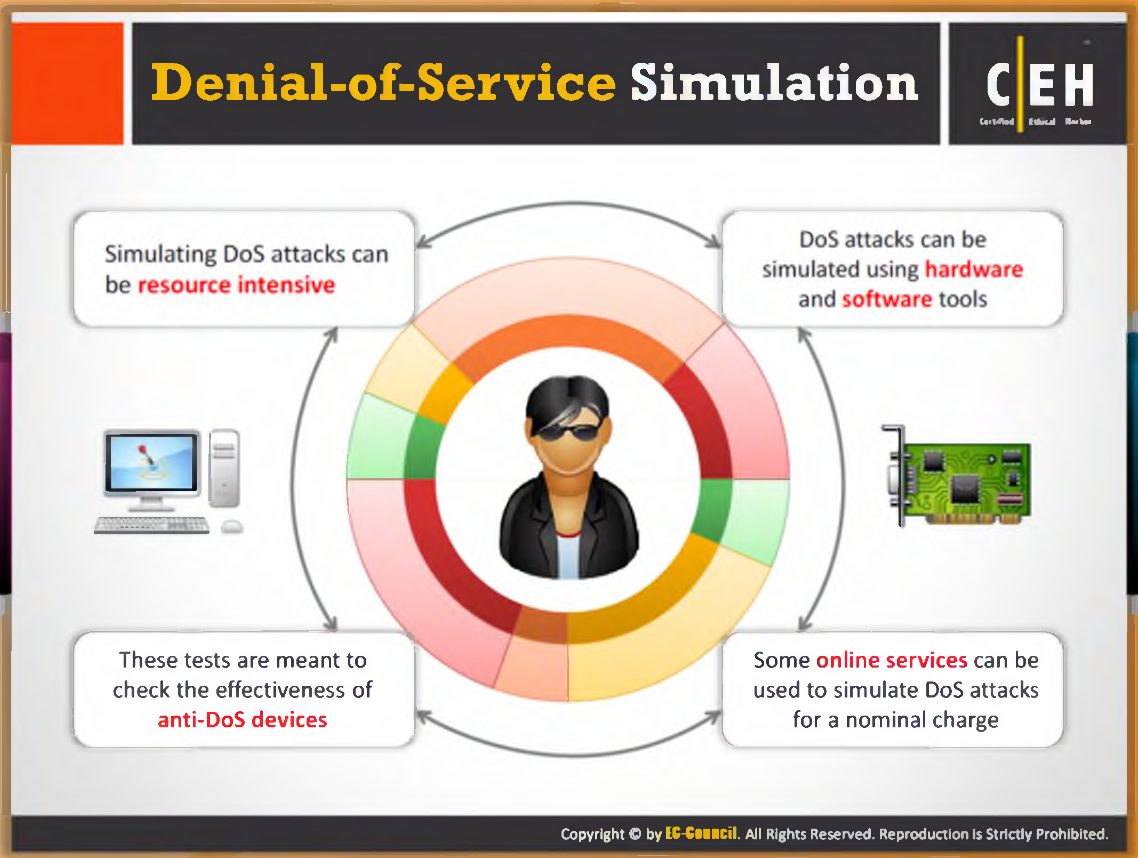
Testing Network-filtering Devices

There are various ways to configure network-filtering devices. In some instances, they may be careless to check malicious traffic, while in others; they may be strict to allow legitimate traffic. The objective of the pen test team would be to ascertain that only **legitimate traffic flows** through the filtering device. However, if multiple filters are used, like a DMZ configuration that uses two firewalls, each filter has to be tested to make sure that it has been configured in the correct way.

It is a fact, however, that even the most preventive firewall cannot restrict network intrusion when the intrusion is initiated within the organization. Most firewalls have the ability to log all activities. But, if the logs are unmonitored over a period of time, they may hinder the functionality of the firewall. Pen testers may test the firewall for endurance by checking the logs and ensuring that the logging activity does not interfere with the firewall's primary activity.

Proxy servers may be subjected to tests to determine their ability to filter out unwanted packets. The pen testers may recommend the use of a load balancer if the traffic load seems to be affecting the filtering capabilities of the devices.

Testing for default installations of the firewall can be done to ensure that default user IDs and passwords have been disabled or changed. Testers can also check for any **remote login capability** that are enabled and allow an intruder to disable the firewall.



Denial-of-Service Simulation

Simulating DoS attacks can be **resource intensive**

DoS attacks can be simulated using **hardware** and **software** tools

These tests are meant to check the effectiveness of **anti-DoS devices**

Some **online services** can be used to simulate DoS attacks for a nominal charge

Denial-of-Service Emulation

There are two classes of DoS: magic packet attacks and resource-exhaustion attacks.

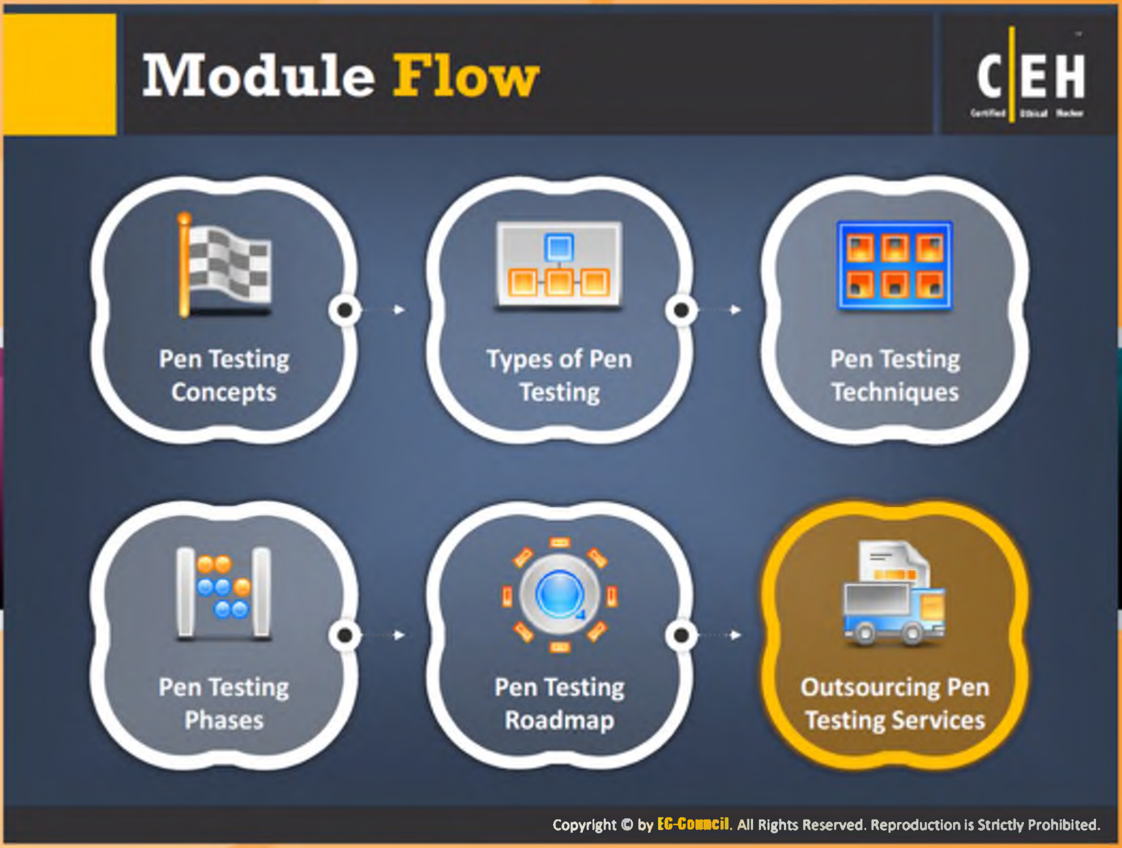
Magic packet attacks usually take advantage of the existing vulnerability in the OS or application for vast abnormal response and excessive CPU utilization or a full system crash by sending one or a few particular packets, for example, **WinNuke** and **Ping** of **Death**.

Resource-exhaustion attacks do not completely rely on the vulnerabilities; instead they make use of the available computer resources. A resource-exhaustion DoS attack is implemented by intentional utilization of the maximum resources and then stealing them.

While small DoS attacks can be duplicated by running DoS from one machine connected to the target network, large tests that seek to duplicate DoS attacks may need to utilize many machines and large amounts of network bandwidth. These may prove to be time consuming and resource intensive, as well. Instead of **deploying several generic servers**, hardware devices may be used to create large volumes of network traffic. They can also come with attack/testing modules that are designed to emulate the most common DoS attacks.

Simulating hacker attacks can include spoofing the DoS source address to that of a router or device on the network itself so that if the IDS are triggered, the network cuts itself off and the objective is achieved. Another option is to emulate the DoS from an online site over the Internet. Some firms offer this service for a charge and **route traffic** over the Internet to emulate the attack.

There are several tools available to simulate a denial-of-service attack and assess the effectiveness of anti-DoS devices. For example, Web Avalanche can be configured to increase the **connection-per-second** rate and bandwidth usage. This formulates connections which is less latent and usually faster than the average user's HTTP connection. However, this may not essentially affect the capabilities of the devices that are tested to study traffic.

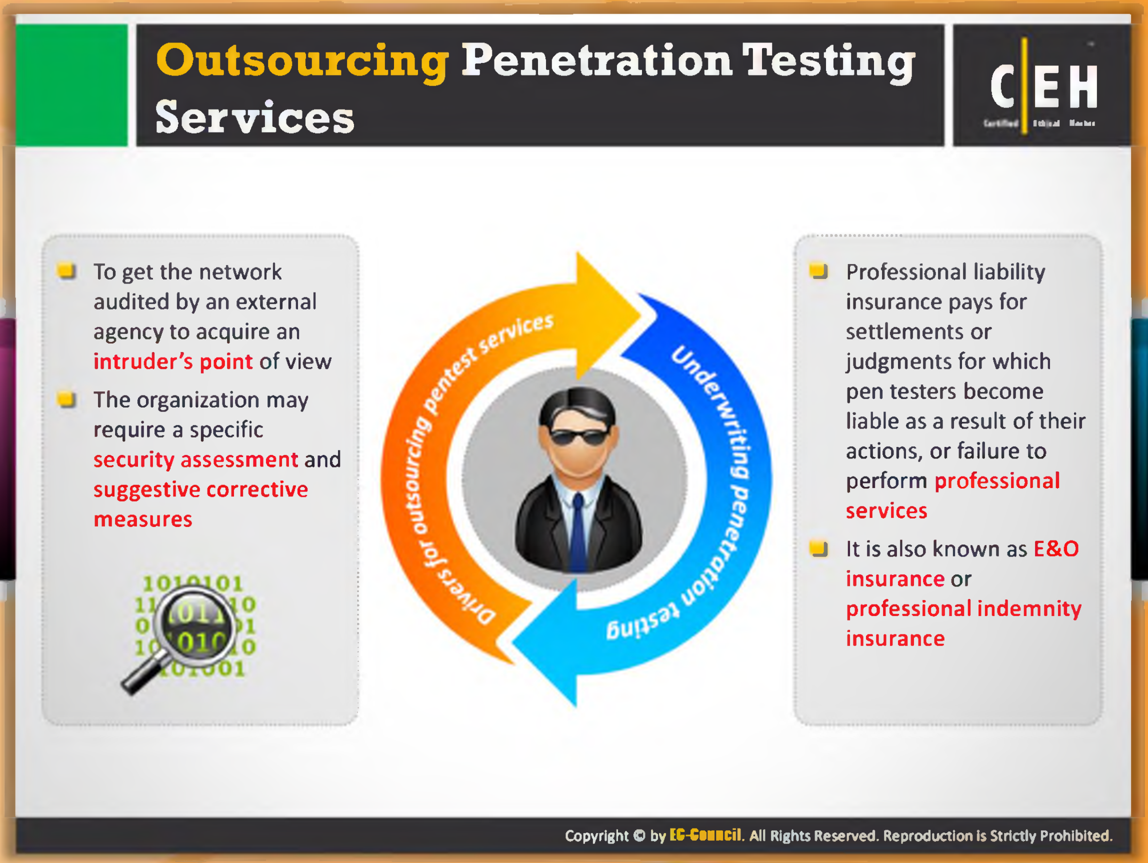


Module Flow

Pen testing results can be effective when the test is performed by a skilled pen tester. Hiring a highly skilled professional on permanent basis may be a huge investment; therefore, most companies prefer outsourcing their pen testing services. Outsourcing the pen testing can increase the frequency, scope, and consistency of its security evaluations.

Pen Testing Concepts	Types of Pen Testing
Pen Testing Techniques	Pen Testing Phases
Pen Testing Roadmap	Outsourcing Pen Testing Services

A detailed explanation about outsourcing penetration testing services is explained on the next slides.



Outsourcing Penetration Testing Services

- To get the network audited by an external agency to acquire an **intruder's point** of view
- The organization may require a specific **security assessment** and **suggestive corrective measures**

Drivers for outsourcing pentest services
Underwriting penetration testing

- Professional liability insurance pays for settlements or judgments for which pen testers become liable as a result of their actions, or failure to perform **professional services**
- It is also known as **E&O insurance** or **professional indemnity insurance**

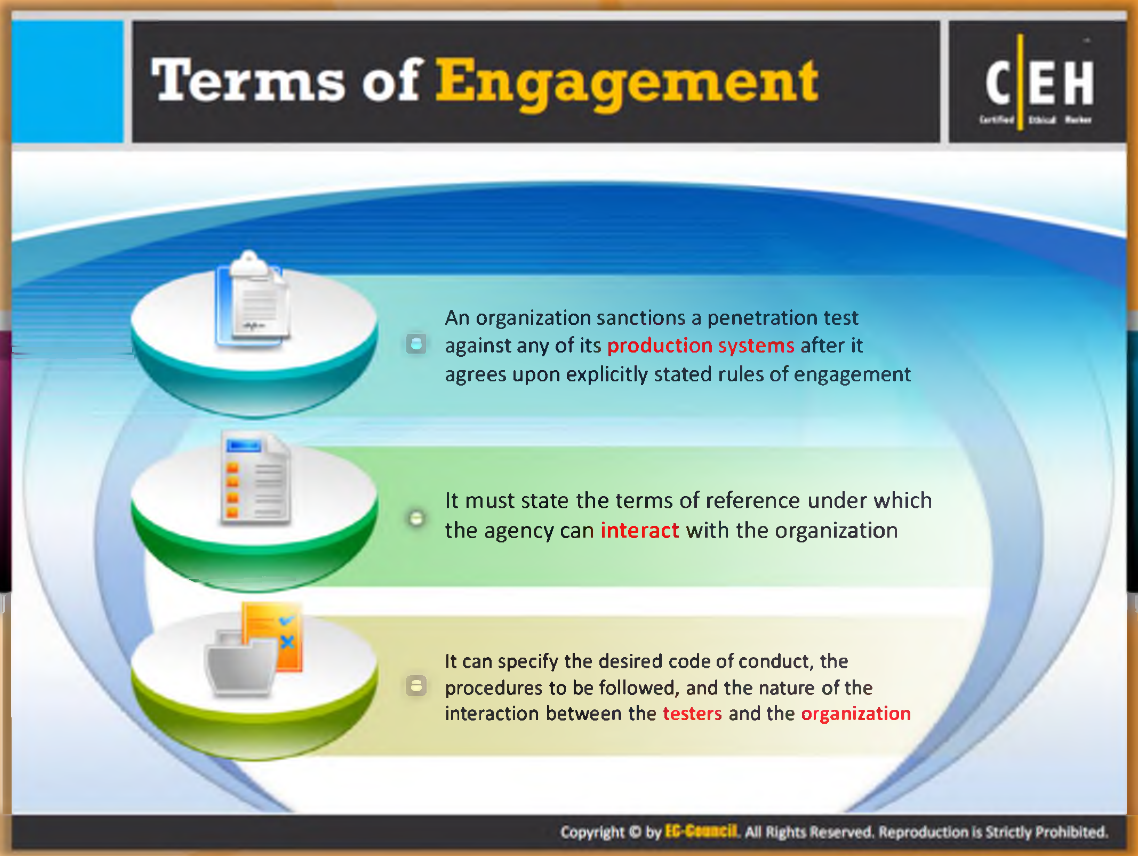
Outsourcing Penetration Testing Services

An organization may choose to outsource **penetration-testing** services if there is a lack of specific technical knowledge and expertise within the organization. The organization may require a specific security assessment and suggested corrective measures. Alternatively, the organization may choose to get its network audited by an **external** agency to acquire an intruder's point of view. The need to outsource may also be due to insufficient staff time and resources. The baseline audit may require an ongoing external assessment or the organization may want to build customer and **partner confidence**.

From an organization's perspective, it would be prudent to appoint a cutout. A cutout is a company's in-house monitor over the course of the test. This person will be fully aware of how the test will be conducted, the time frame involved, and the comprehensive nature of the test. The cutout will also be able to intervene during the test to save both pen testers and crucial production systems from **unacceptable damage**.

Underwriting Penetration Testing

- There is an inherent risk involved in undertaking a penetration test. Most organizations would like to know if the penetration testing organization has professional liability insurance. Professional liability insurance pays for settlements or judgments for which pen testers become liable as a result of their actions or failure to perform **professional services**. They take care of the costs involved in defending against the claim, which includes the attorney’s fees, court costs, and other related expenditures involved in investigation, and this also includes the expenditure of the settlement process. From a pen tester’s perspective, professional liability insurance is malpractice insurance for professional service providers. It is also known as E&O insurance or professional indemnity insurance.



Terms of Engagement

C|EH
Certified Ethical Hacker

- An organization sanctions a penetration test against any of its production systems after it agrees upon explicitly stated rules of engagement
- It must state the terms of reference under which the agency can interact with the organization
- It can specify the desired code of conduct, the procedures to be followed, and the nature of the interaction between the testers and the organization

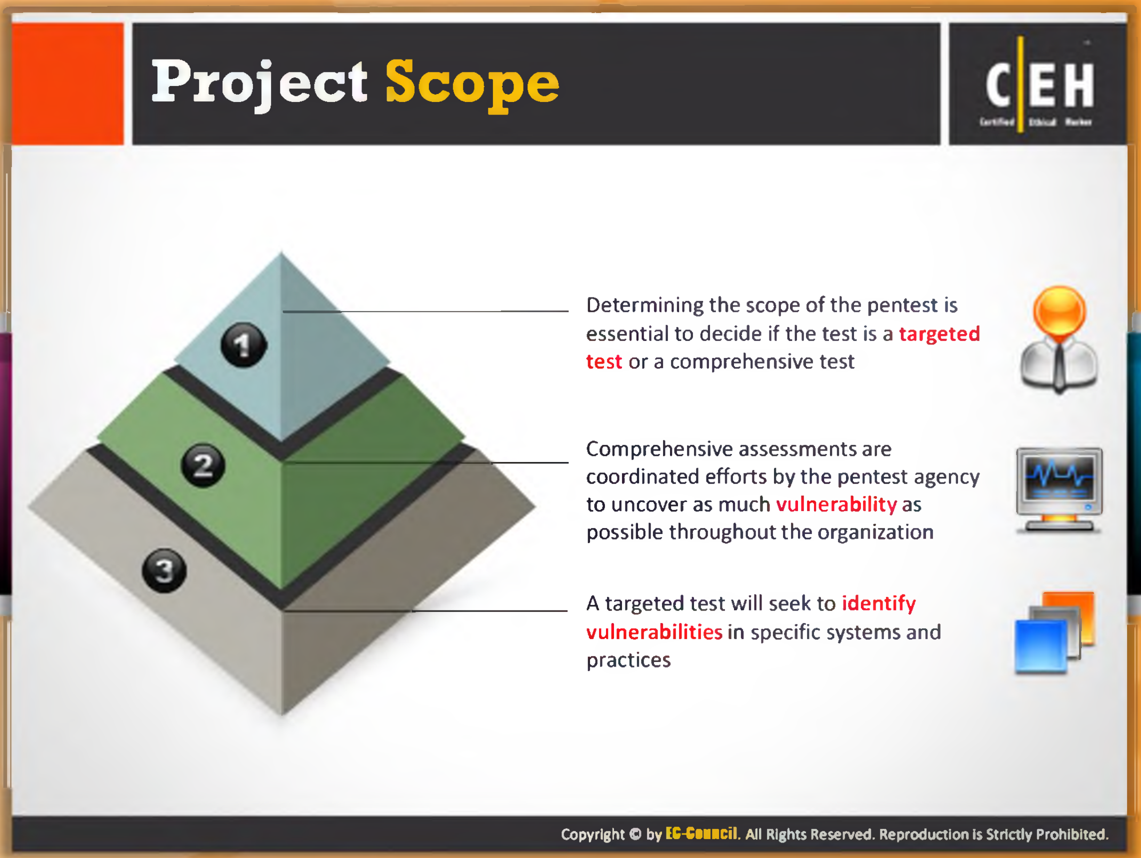
Terms of Engagement

Source: http://seclists.org

Terms of engagement are essential to protect both the **organization's interests** and the pen tester's liabilities. The terms lay down clearly defined guidelines within which the testers can test the systems. They can specify the desired code of conduct, the procedures to be followed, and the nature of interaction between the testers and the organization.

It is prudent for an organization to sanction a penetration test against any of its production systems only after it agrees upon explicitly stated rules of engagement. This contract agreed upon with the pen test agency must state the terms of reference under which the agency can interact with the organization.

For instance, if the pen test agency is undertaking network mapping, the rules of engagement may read as follows: "Pen test agency can obtain much of the required information regarding the site's network profile, such as IP address ranges, telephone number ranges, and other general network topology through public information sources, such as Internet registration services, web pages, and telephone directories. More detailed information about the site's network architecture can be obtained through the use of **domain name server (DNS**) queries, ping sweeps, port scans, and connection route tracing. Informal inquiries, not related to organization, may also be attempted to gather information from users and administrators that could assist in gaining access to network resources.”



Project Scope

Determining the scope of the pentest is essential to decide if the test is a targeted test or a comprehensive test

Comprehensive assessments are coordinated efforts by the pentest agency to uncover as much vulnerability as possible throughout the organization

A targeted test will seek to identify vulnerabilities in specific systems and practices

Project Scope

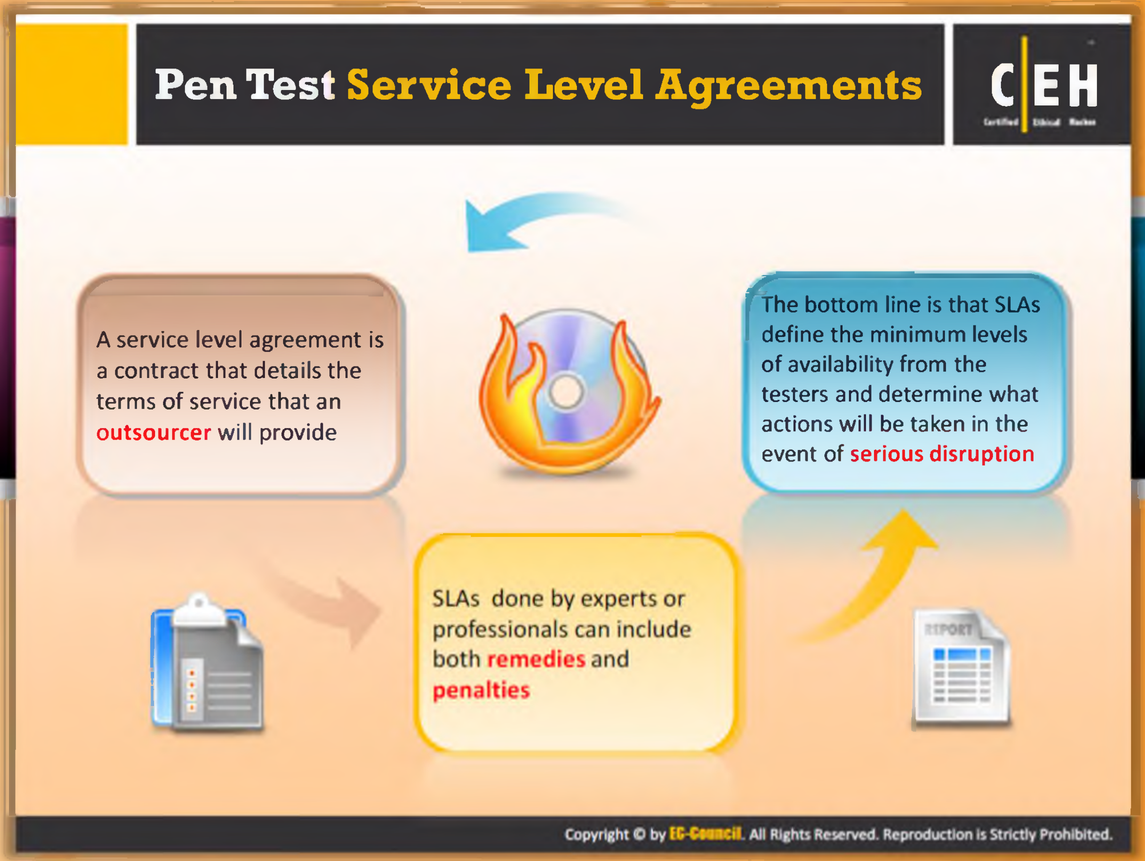
Determining the scope of the pen test is essential to decide if the test is a targeted test or a comprehensive test. One of the factors that have a significant effect on the effort estimation and cost component of the penetration test is whether or not the pen test agency can undertake a zero knowledge test or a partial knowledge test.

Providing even partial knowledge to the pen testers results in time and cost savings. The burden is on the client to make sure that the information provided is complete to the extent intended to be. This is important because if sensitive system data about critical systems is given beforehand, it might defeat the purpose of the penetration test.

If the agency is going to undertake a targeted test, it can seek to identify vulnerabilities in specific systems and practices such as:

- Remote access technologies such as dial-in modems, wireless, and VPN
- Perimeter defenses of Internet-connected systems
- Security of web applications and database applications
- Vulnerability to denial-of-service attacks

On the other hand, comprehensive assessments are coordinated efforts by the pen test agency to uncover as much vulnerability as possible throughout an organization's IT practices and networked infrastructure.



Pen Test Service Level Agreements

A service level agreement is a contract that details the terms of service that an outsourcer will provide

The bottom line is that SLAs define the minimum levels of availability from the testers and determine what actions will be taken in the event of serious disruption

SLAs done by experts or professionals can include both remedies and penalties

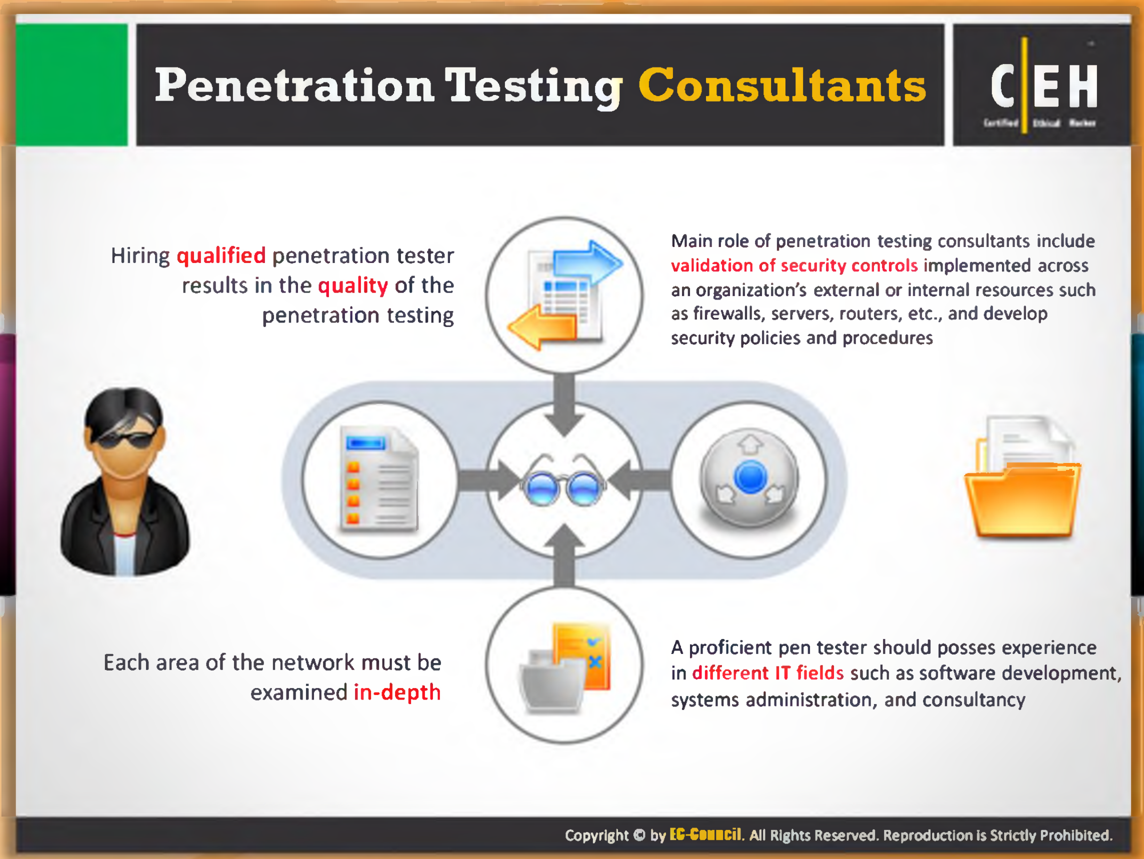
Pen Test Service Level Agreements

The contract agreement that describes the terms of service that an outsourcer provides is known as a Service Level Agreement (SLA). SLAs should match the testing requirements as closely as possible. Proficiently done SLAs can include **remedies** and **penalties** for missing particular service levels.

These penalties encourage the pen test team to achieve the objectives, and make sure that they get back on track quickly. Many organizations also ask for referrals and examples of SLAs they have used with other customers who had similar testing needs. The organization may want to verify the metrics used and the quality of the results achieved to assess the ability of the pen-test team to meet its requirements.

From a pen tester's perspective, it may be difficult to provide examples of real-world SLAs because they are considered confidential business information, similar to other contract terms. The bottom line is that **SLAs** define the minimum levels of availability from the testers and determine what actions can be taken in the event of serious disruption.

Normally, the contract covers those issues as compensation, warranties and remedies, resolution of disputes, and legal compliance. It basically frames the **relationship**, and determines the **major responsibilities**, both during normal testing and in an emergency situation.



Penetration Testing Consultants

Hiring qualified penetration tester results in the quality of the penetration testing

Main role of penetration testing consultants include validation of security controls implemented across an organization's external or internal resources such as firewalls, servers, routers, etc., and develop security policies and procedures

Each area of the network must be examined in-depth

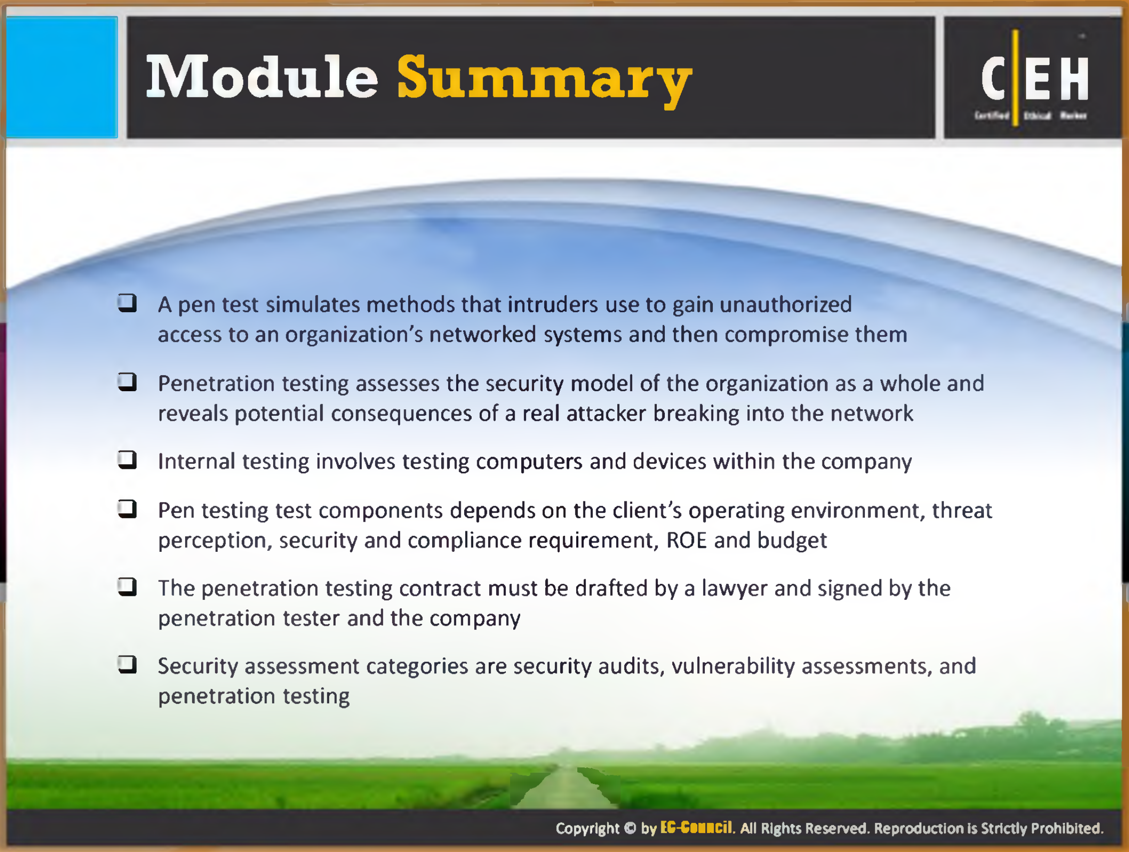
A proficient pen tester should posses experience in different IT fields such as software development, systems administration, and consultancy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing Consultants

When companies outsource penetration testing, though it is a bit costly to hire qualified professionals who are exclusively trained, it usually yields good results. More qualitative work can be done and desired goals can be achieved.

- Hiring a qualified penetration tester results in the quality of the penetration testing.
- A penetration test of a corporate network can examine numerous different hosts (with a number of different operating systems), network architecture, policies, and procedures.
- Each area of the network must be examined in-depth.
- Penetration testing skills cannot be obtained without years of experience in IT fields, such as development, systems administration, or consultancy.



Module Summary

CEH
Certified Ethical Hacker

- ❑ A pen test simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them
- ❑ Penetration testing assesses the security model of the organization as a whole and reveals potential consequences of a real attacker breaking into the network
- ❑ Internal testing involves testing computers and devices within the company
- ❑ Pen testing test components depends on the client's operating environment, threat perception, security and compliance requirement, ROE and budget
- ❑ The penetration testing contract must be drafted by a lawyer and signed by the penetration tester and the company
- ❑ Security assessment categories are security audits, vulnerability assessments, and penetration testing

Module Summary

- A pen test simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them.
- Penetration testing assesses the security model of the organization as a whole and reveals potential consequences of a real attacker breaking into the network.
- Internal testing will be performed from a number of network access points, representing each logical and physical segment.
- Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirement, ROE, and budget.
- The penetration testing contract must be drafted by a lawyer and signed by the penetration tester and the company.
- Security assessment categories are security audits, vulnerability assessments, and penetration testing.