Penetration Testing

Module 19

Engineered by Hackers. Presented by Professionals.


SECURITY NEWS
COMPUTERWORLD
December 22, 2010 06:43 AM ET
Researchers reveal attack code for new IE zero-day
Security researchers have released attack code that exploits an unpatched bug in Microsoft's Internet Explorer (IE) and sidesteps defenses baked into Windows 7.
Microsoft said it was looking into the vulnerability.
"Microsoft is investigating new public claims of a possible vulnerability in Internet Explorer," said Dave Forstrom, the director of Microsoft's Trustworthy Computing group, in statement. "We're currently unaware of any attacks trying to use the claimed vulnerability or of customer impact."
The bug first surfaced earlier this month when French security firm Vupen announced it had uncovered a flaw in IE's HTML engine that could be exploited when the browser processed a CSS (Cascading Style Sheets) file that included "@import" rules. The @import rules let Web designers add external style sheets to an existing HTML document.
Vupen issued a bare-bones advisory on Dec. 9 that confirmed the vulnerability in IE8 running on Windows XP, Vista and Windows 7, and in IE6 and IE7 on XP. Attackers could trigger the bug from a rigged Web page, then hijack the PCs to plant malware or pillage its secrets.
http://www.computerworld.com
CEH
2
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

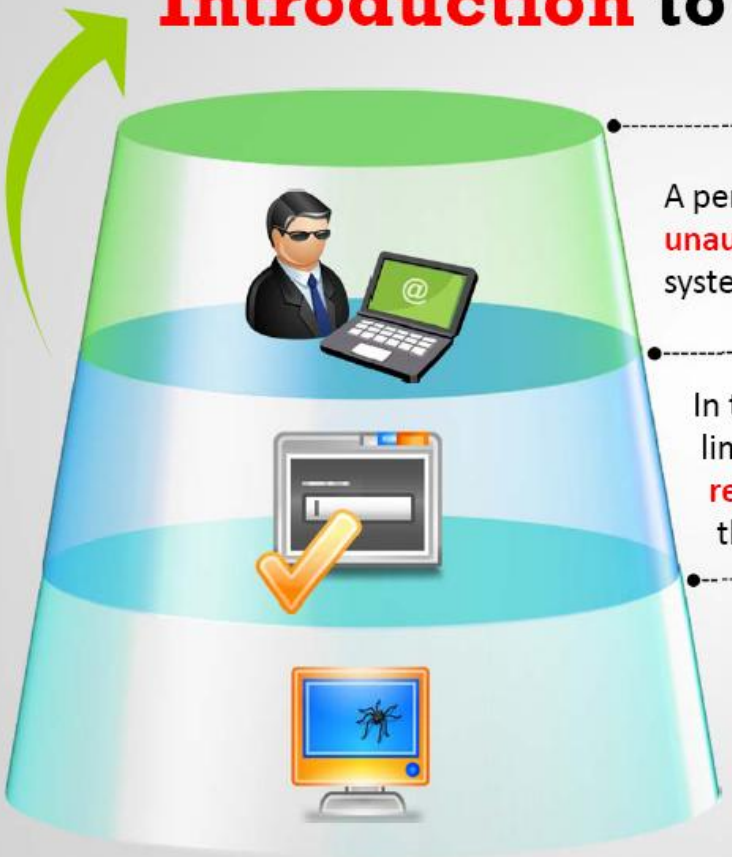
- Penetration Testing (PT)
- Security Assessments
- Risk Management
- Automated Testing
- Manual Testing
- Enumerating Devices

- Denial of Service Emulation
- HackerShield
- Pentest using Various Devices
- VigilENT
- WebInspect
- Tools




Module Flow
Pen Testing Concepts
Types of Pen Testing
Pen Testing Techniques
Pen Testing Phases
Pen Testing Roadmap
Outsourcing Pen Testing Services
Pen Testing Tools
C|EH Certified Ethical Hacker
4
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to Penetration Testing

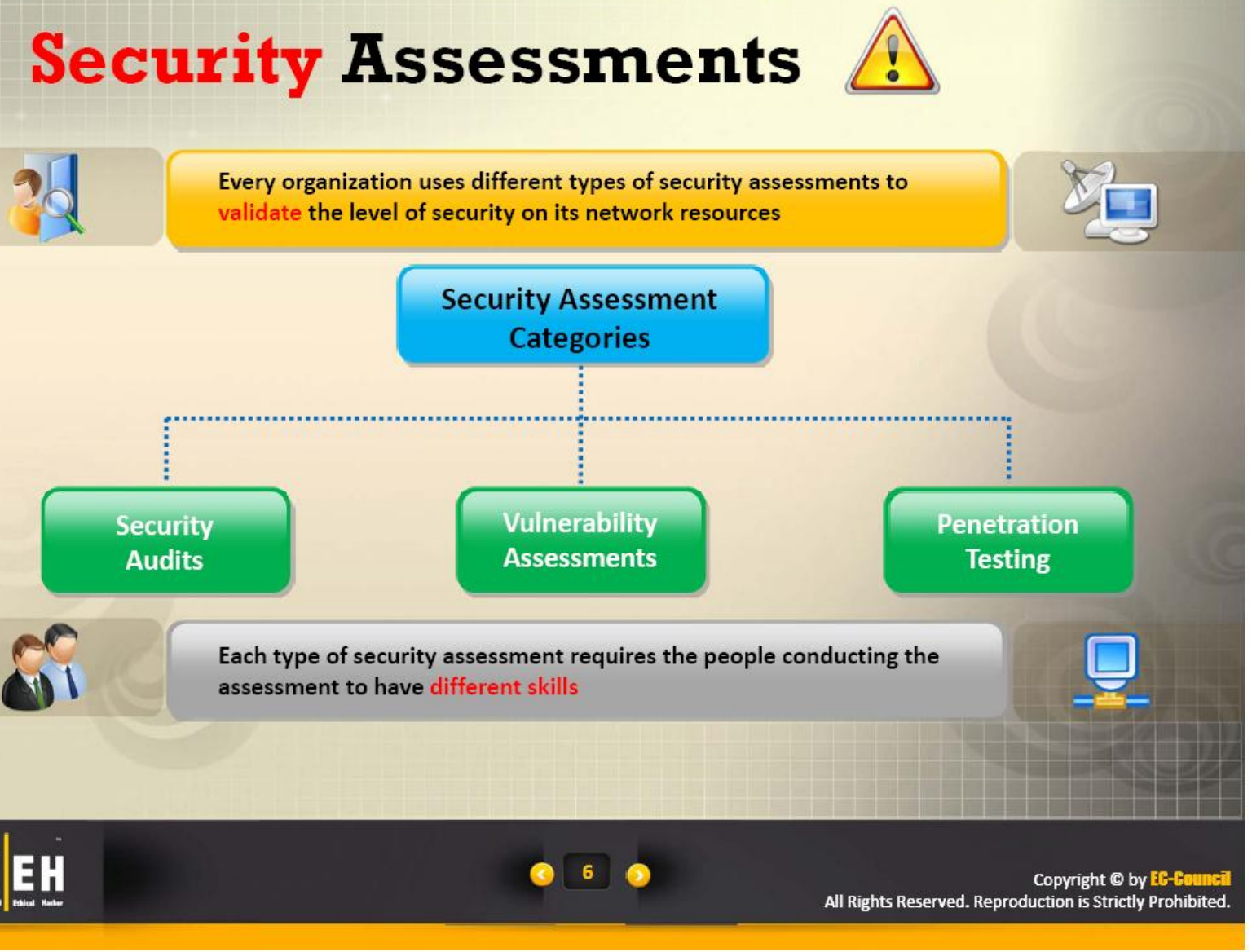


A pentest simulates methods that intruders use to gain **unauthorized access** to an organization's networked systems and then compromise them

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

Security Assessments



Vulnerability Assessment

1 Network Scanning

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

2 Scanning Tools

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

3 Security Mistakes

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

4 Test Systems/Network

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

CEH Certified Ethical Hacker

Limitations of Vulnerability Assessment

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

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

3. This can influence the result of the assessment

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

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

A penetration tester is differentiated from an attacker only by his intent and lack of malice

It reveals potential consequences of a real attacker breaking into the network

Why Penetration Testing?

- Identify the **threats** facing an organization's information assets
- Reduce an organization's IT security costs and provide a better **Return On IT Security Investment** (ROSI) by identifying and resolving vulnerabilities and weaknesses
- Provide an organization with assurance - a thorough and **comprehensive assessment** of organizational security covering policy, procedure, design and implementation
- Gain and maintain **certification** to an industry regulation (BS7799, HIPAA etc.)
- Adopt best practice by conforming 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

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, e-commerce failure, and loss of confidential information
- Public facing systems; websites, email gateways, and remote access platforms
- Mail, DNS, firewalls, passwords, FTP, IIS, and web servers

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

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 

ROI on Penetration Testing

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

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

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

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

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 Locations

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

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

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

CEH Certified Ethical Hacker

15

Module Flow


Pen Testing Concepts
Types of Pen Testing
Pen Testing Techniques
Pen Testing Phases
Pen Testing Roadmap
Outsourcing Pen Testing Services
Pen Testing Tools
C|EH Certified Ethical Hacker
16
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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

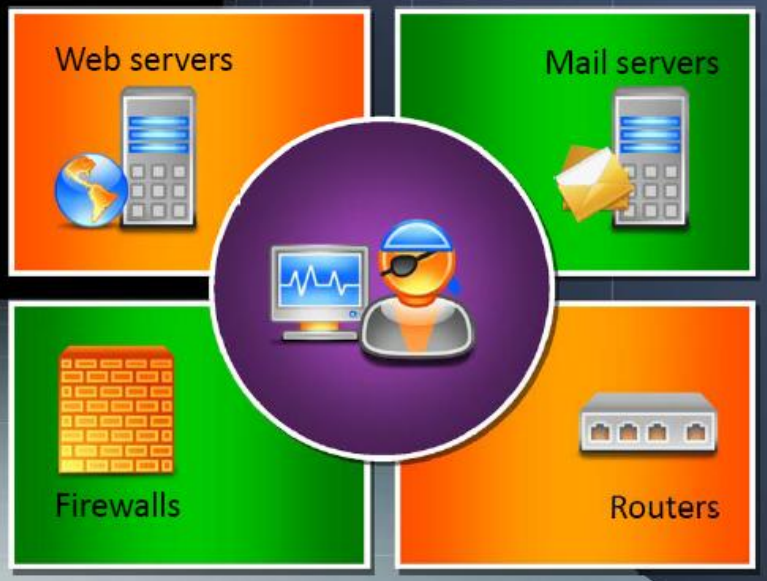
Internal testing will be performed from a number of **network access points**, representing each logical and physical segment

- 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

1	It is the **traditional** approach to penetration testing
2	The testing is focused on the servers, infrastructure and the underlying software **comprising the target**
3	It may be performed with no **prior knowledge** of the site (black box)
4	Full disclosure of the **topology** and **environment** (crystal/white box)

External penetration testing involves a **comprehensive analysis** of publicly available information about the target, such as



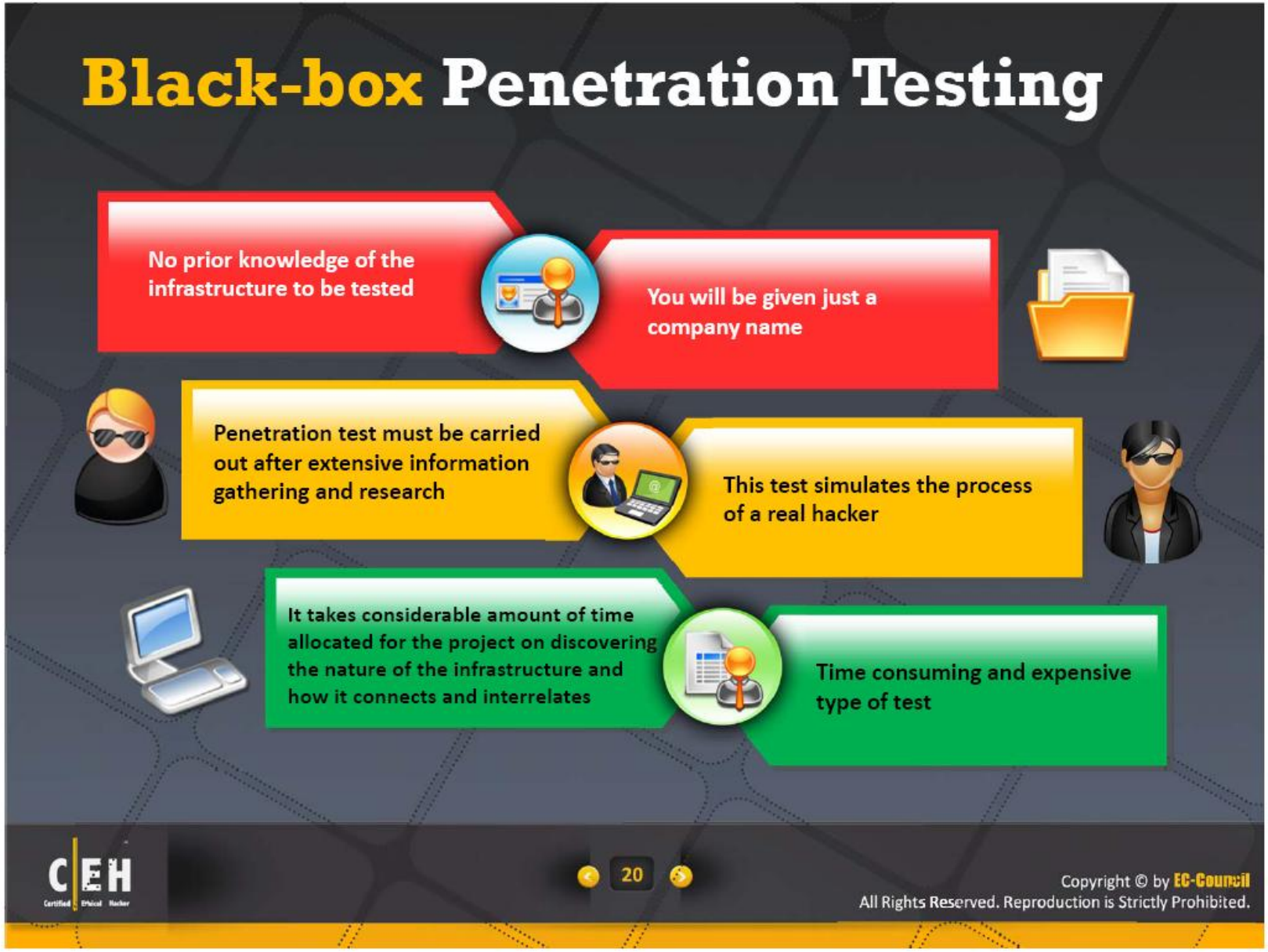
Internal Security Assessment

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

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

Black-box Penetration Testing



Grey-box Penetration Testing

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

It performs security assessment and testing internally

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

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

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

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

Automated Testing

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

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

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

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

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

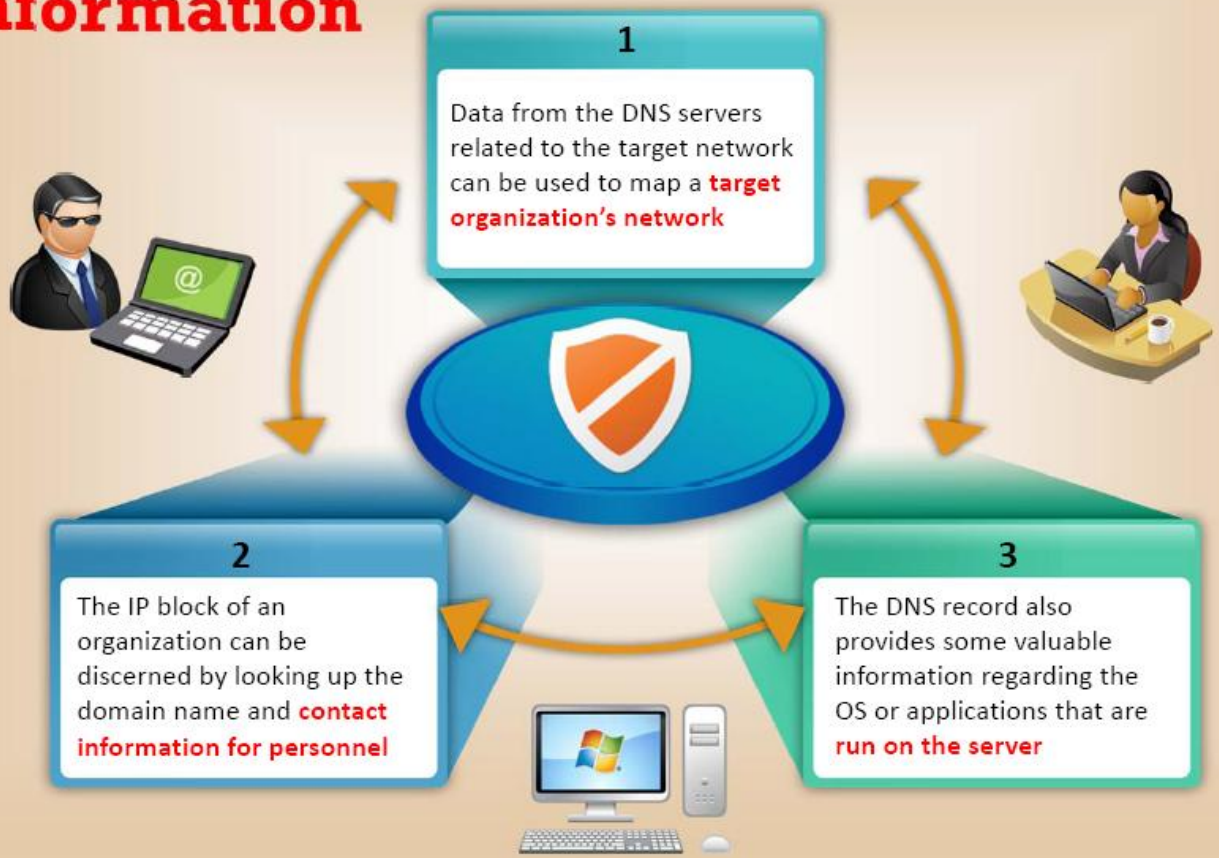
Module Flow


Pen Testing Concepts
Types of Pen Testing
Pen Testing Techniques
Pen Testing Phases
Pen Testing Roadmap
Outsourcing Pen Testing Services
Pen Testing Tools
CEH
Certified Ethical Hacker
26
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Penetration Testing Techniques

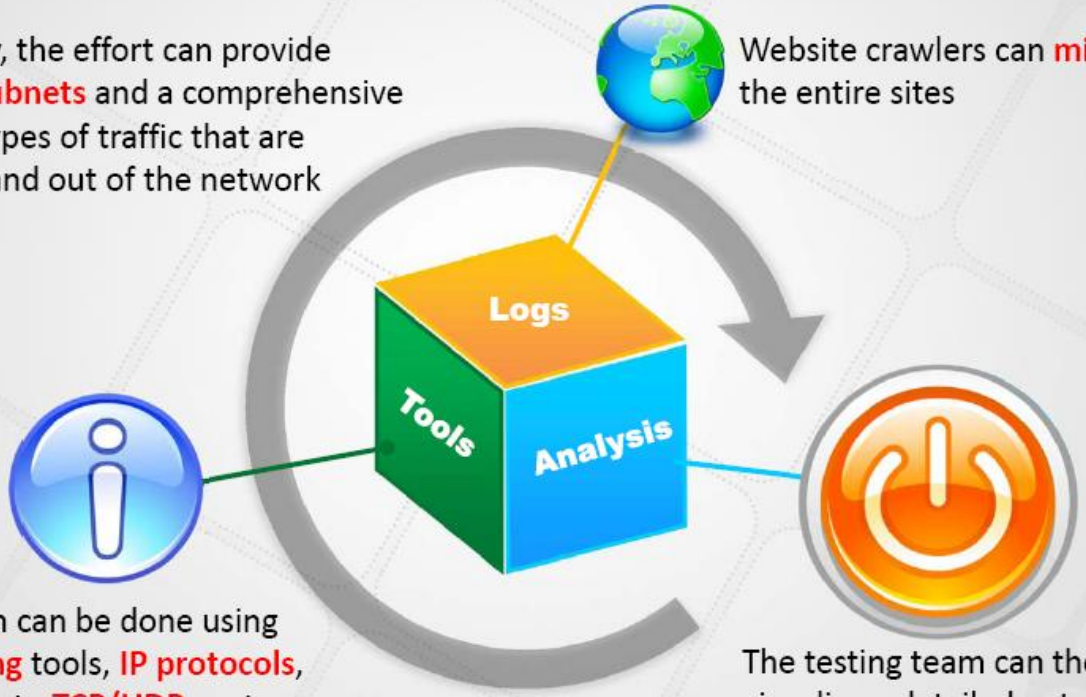
Passive Research Is used to gather all the information about an organization's system configurations	**Open Source Monitoring** Facilitates an organization to take necessary steps to ensure its confidentiality and integrity	**Network Mapping and OS Fingerprinting** Is used to get an idea of the network's 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

Using DNS Domain Name and IP Address Information



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



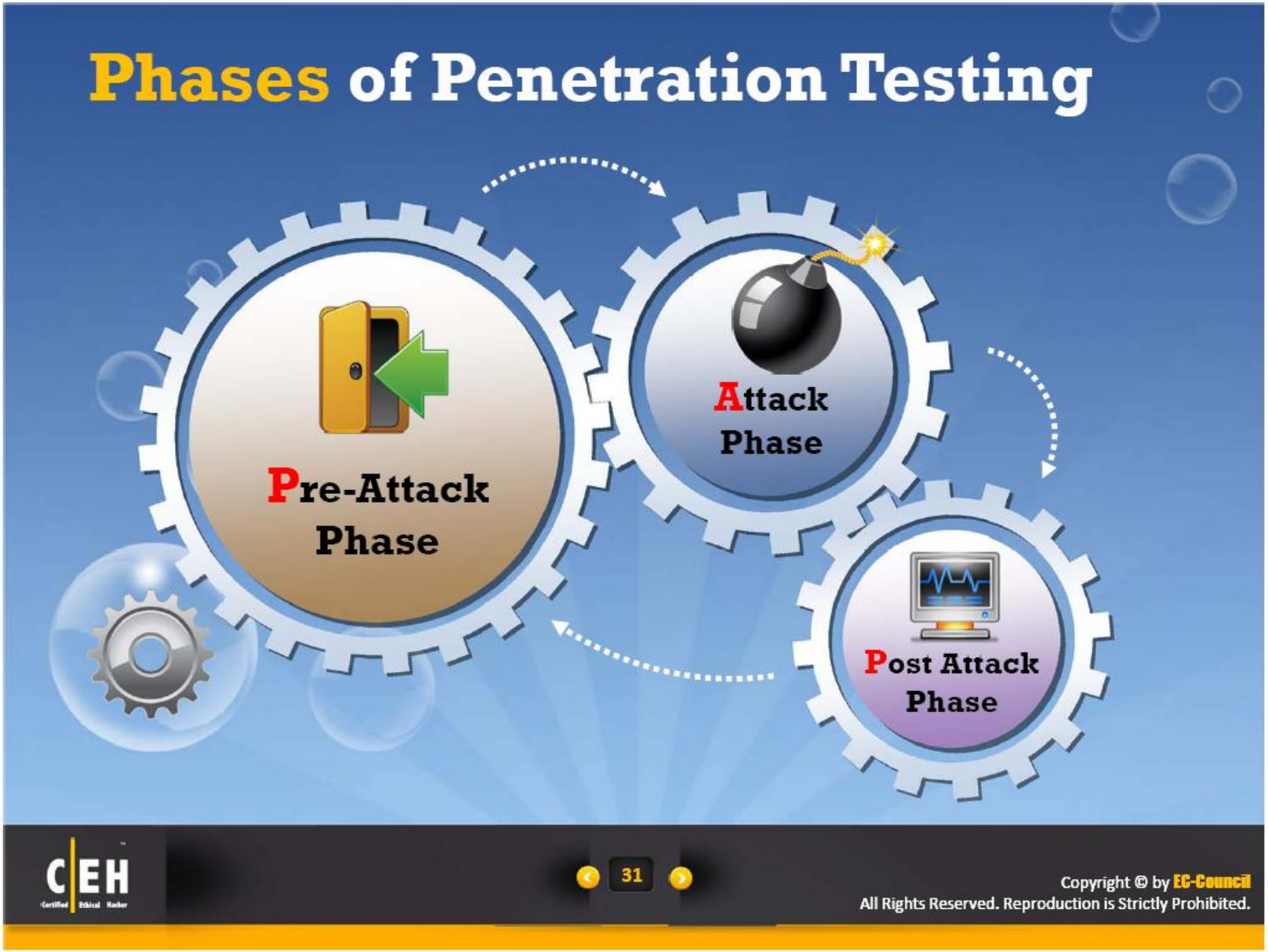
Website crawlers can mirror the entire sites

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

Module Flow


Pen Testing Concepts
Types of Pen Testing
Pen Testing Techniques
Pen Testing Phases
Pen Testing Roadmap
Outsourcing Pen Testing Services
Pen Testing Tools
C|EH Certified Ethical Hacker
30
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.


Phases of Penetration Testing
Pre-Attack Phase
Attack Phase
Post Attack Phase
CEH
31
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pre-Attack Phase

- 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
- Hacker seeks to find out as much information as possible about the victim
- Hackers gather information in different ways that allows them to **formulate a plan** of attack
- It is of two types:

  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

Information retrieved in this 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
Penetrate Perimeter
Acquire Target
Execute, Implant, Retract
Escalate Privileges
101010
010101
101
C|EH
33
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Activity: Perimeter Testing

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

Checking **access control lists** by forging responses with crafted packets

Evaluating **protocol filtering rules** by attempting connections using various protocols such as SSH, FTP, and Telnet

Examining the **perimeter security system's response** to web server scans using multiple methods such as POST, DELETE, and COPY

Evaluating **error reporting** and **error management** with ICMP probes

Measuring the **threshold for denial of service** by attempting persistent TCP connections, evaluating transitory TCP connections, and attempting to stream UDP connections

Evaluating the **IDS's capability** by passing malicious content (such as malformed URL) and scanning the target variously for responding to abnormal traffic

CEH Certified Ethical Hacker

Enumerating 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

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:

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)

- 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
- 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

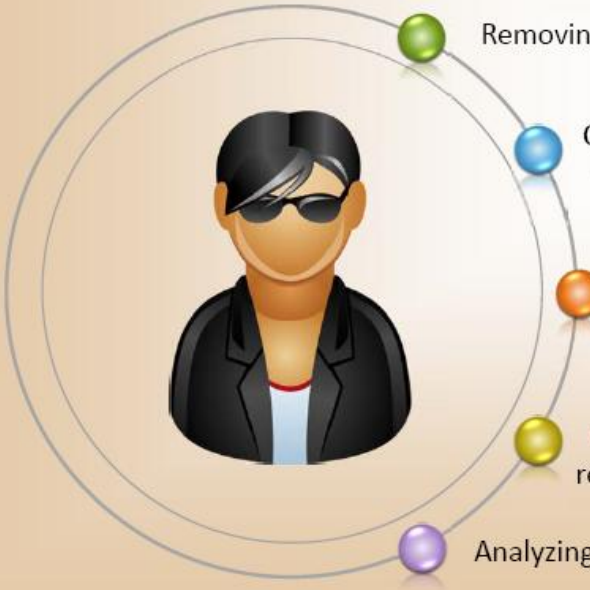
The objective of system penetration is to explore the extent to which the security fails

Execute Exploits

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

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

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

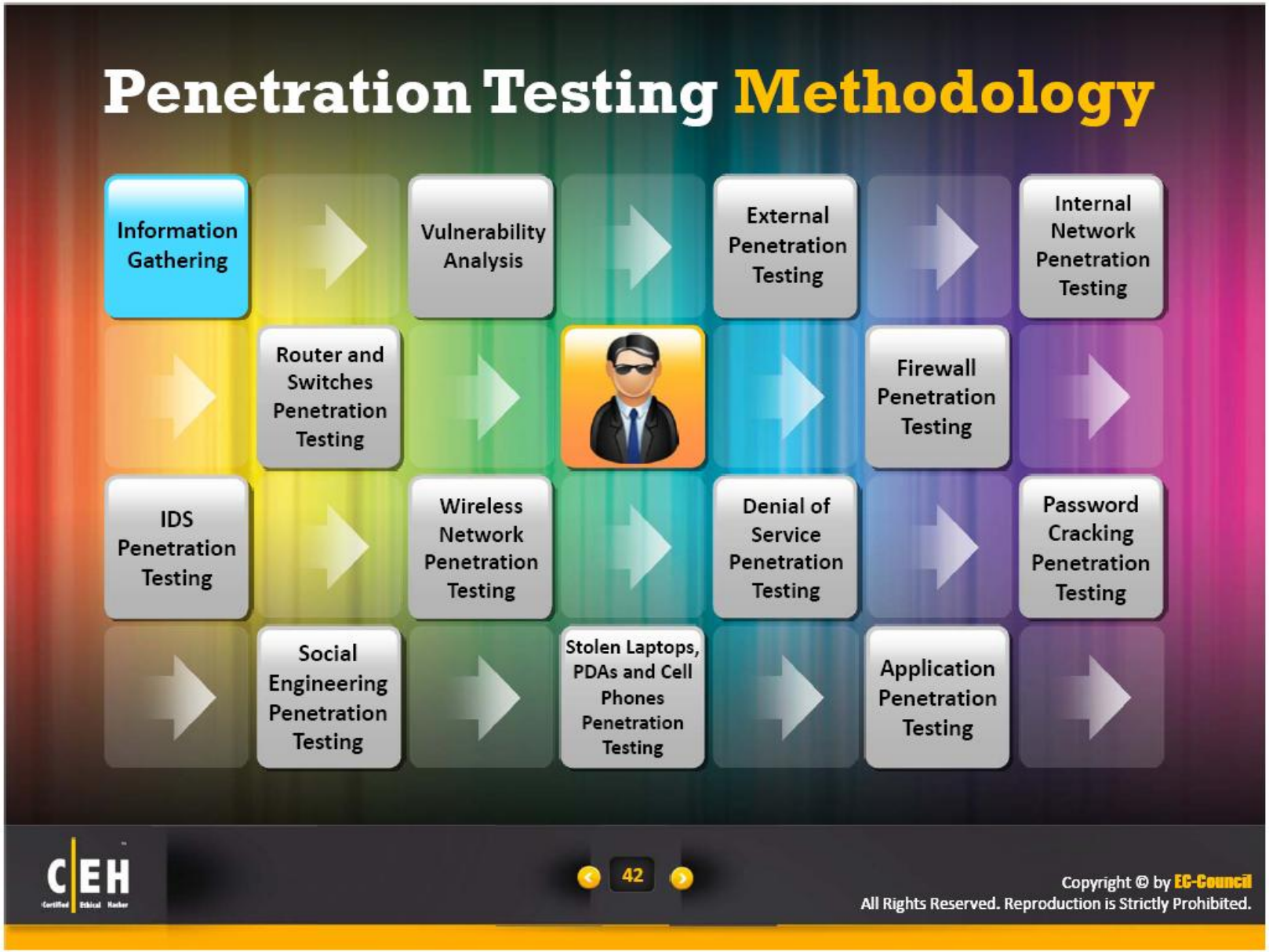
Broad areas covered include objectives, observations, activities undertaken, and incidents reported

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

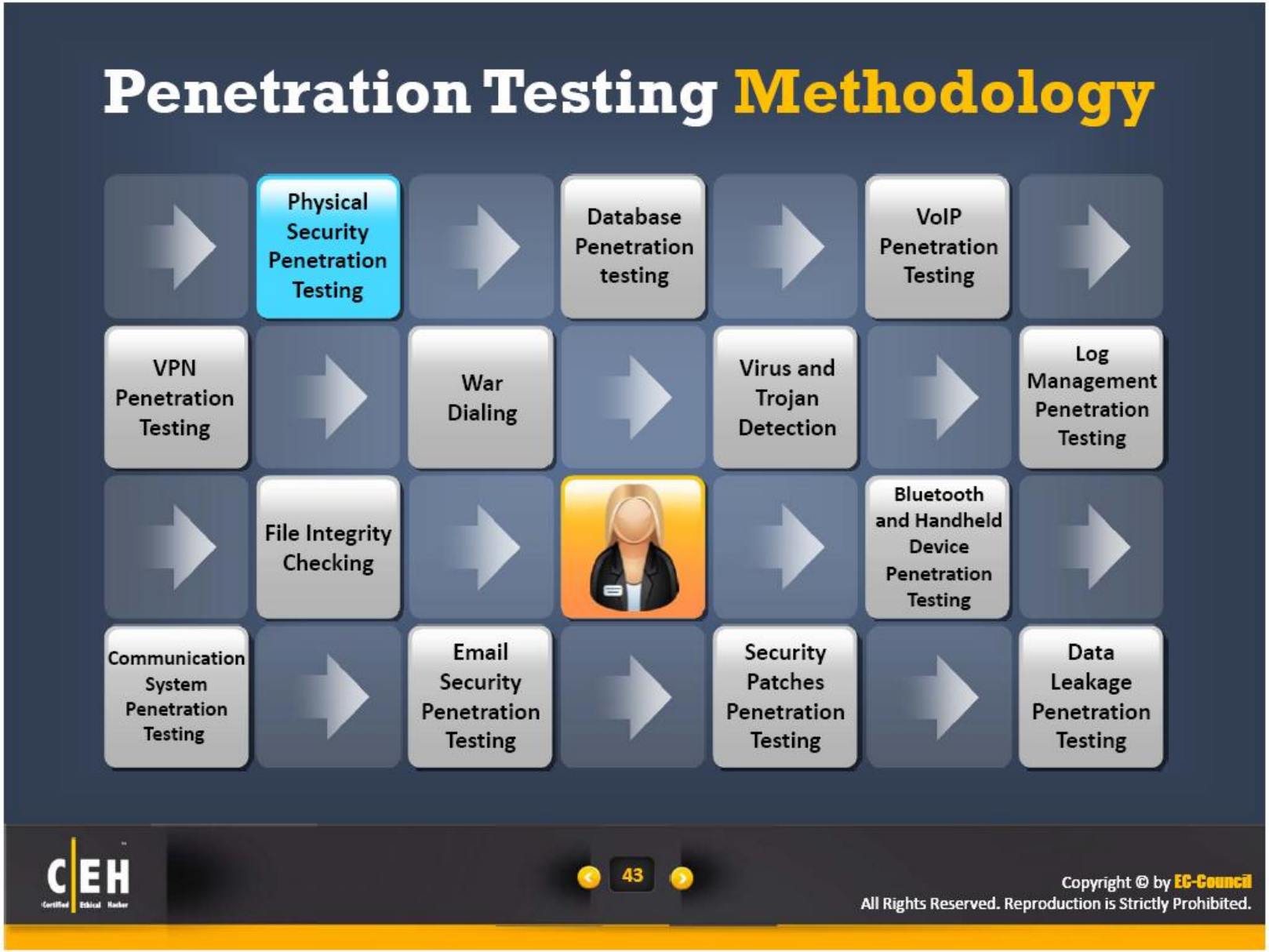
Module Flow


Pen Testing Concepts
Types of Pen Testing
Pen Testing Techniques
Pen Testing Phases
Pen Testing Roadmap
Outsourcing Pen Testing Services
Pen Testing Tools
C|EH Certified Ethical Hacker
41
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing Methodology

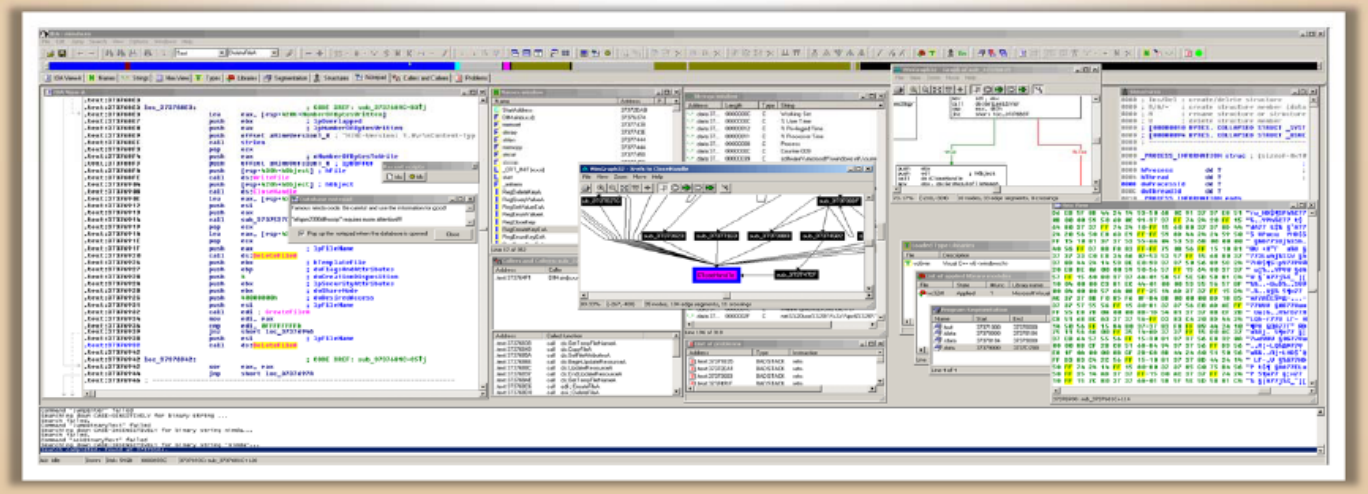


Penetration Testing Methodology

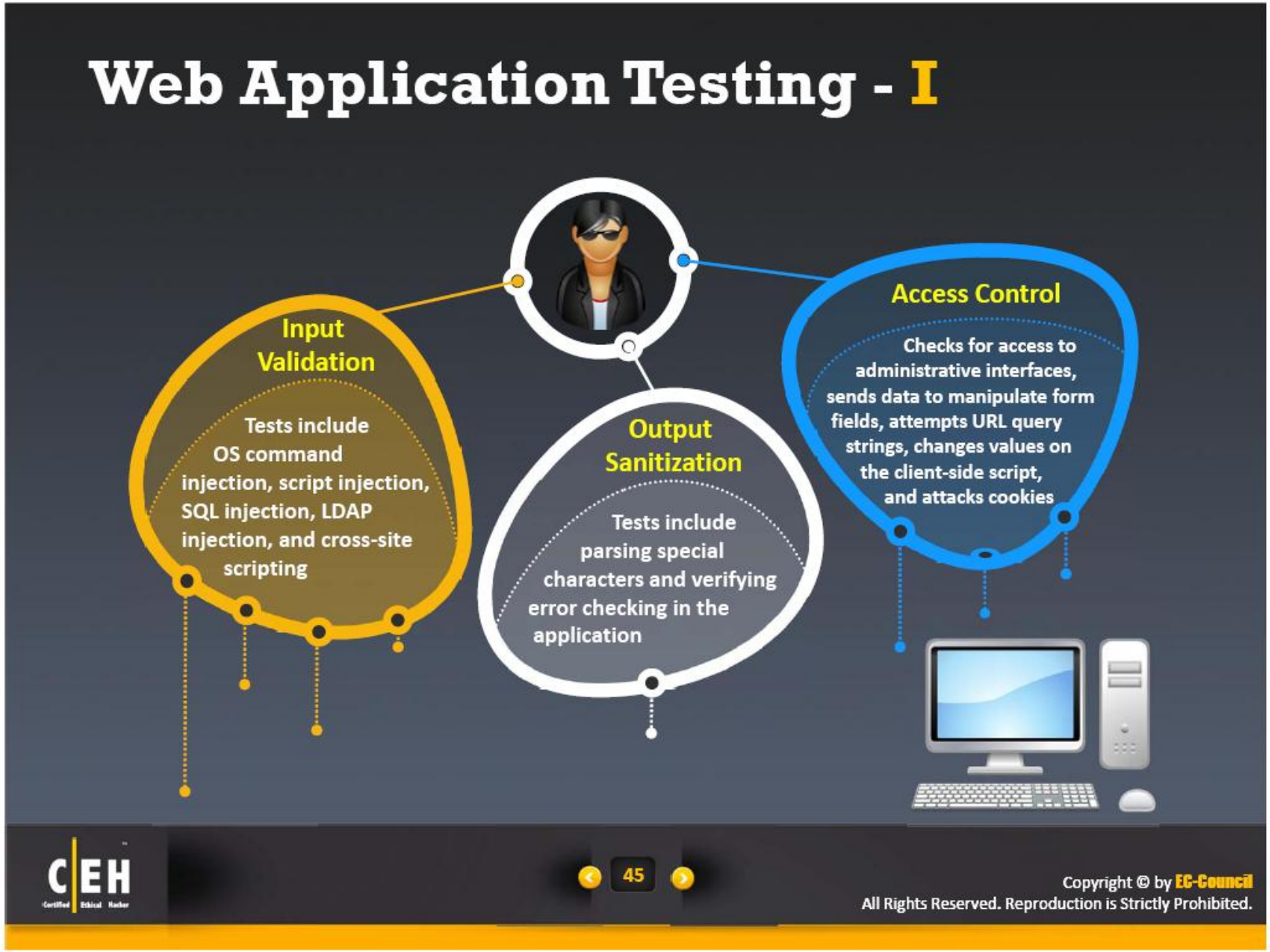


Application Security Assessment

- 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, proprietary applications or systems
- This test checks on application so that a malicious user cannot **access**, **modify** or **destroy data** or **services** within the system



Web Application Testing - I



Web Application Testing - II

- Tests include attacks **against stack overflows, heap overflows**, and format string overflows
- It checks for **security controls on web server/application components** that might expose the web application to vulnerabilities
- It 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
- It 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 - 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

Network Security Assessment

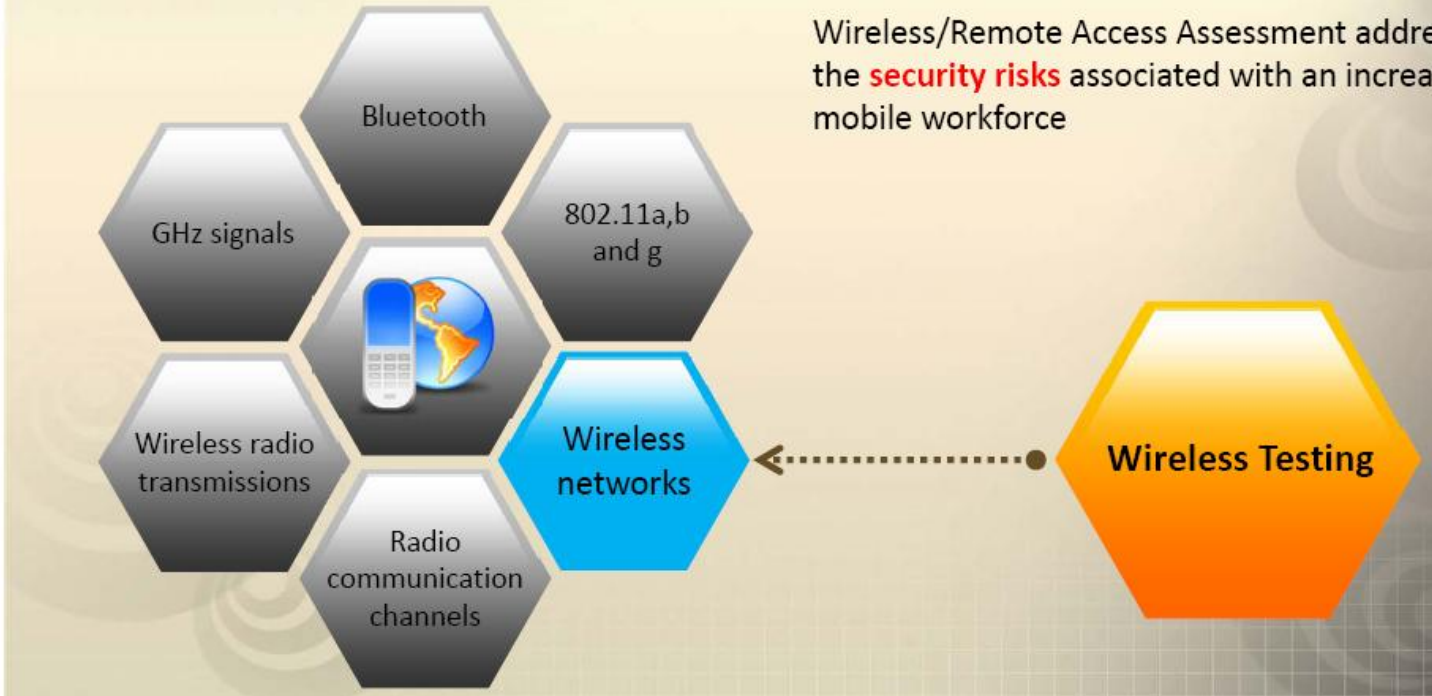
It scans the network environment for identifying vulnerabilities and helps to improve an enterprise's security policy

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 addresses the **security risks** associated with an increasingly mobile workforce

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

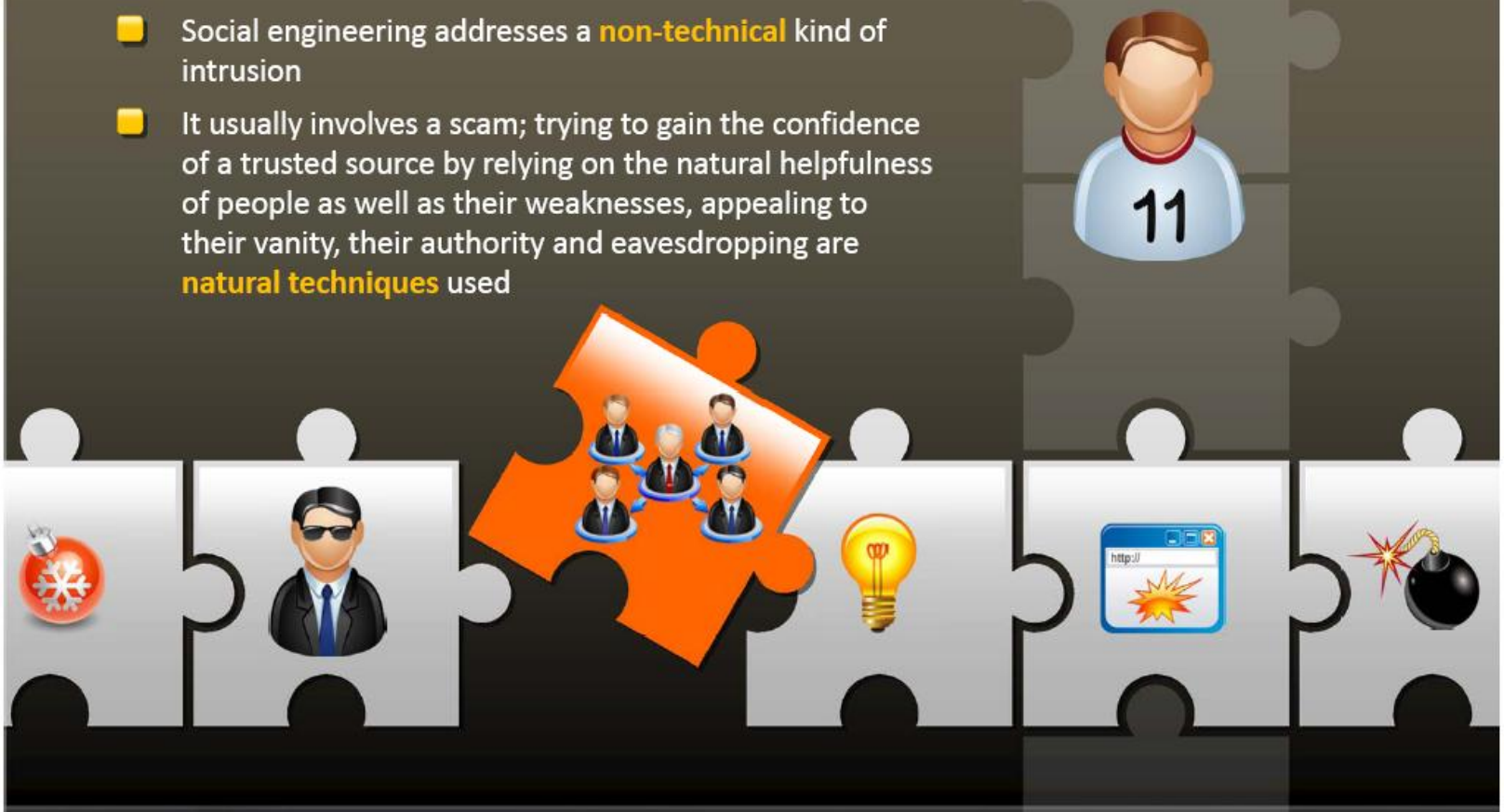
Telephony Security Assessment

A telephony security assessment addresses security concerns relating to corporate voice technologies

This includes 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

Social Engineering

- Social engineering addresses a **non-technical** kind of intrusion
- It usually involves a scam; trying to gain the confidence of a trusted source by relying on the natural helpfulness of people as well as their weaknesses, appealing to their vanity, their authority and eavesdropping are **natural techniques** used



Testing Network-Filtering Devices

The objective of the pentest team is to ascertain that all **legitimate traffic** flows through the filtering device

Proxy servers may be subjected to stress tests to evaluate their ability to filter out **unwanted packets**

Testers can also check for any **remote login** capability that might have been enabled

Testing for default installations of the firewall can be done to ensure that default **user IDs** and **passwords** have been disabled or changed

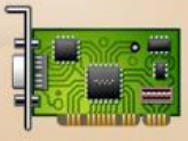
Denial of Service Emulation

Emulating DoS attacks can be resource intensive

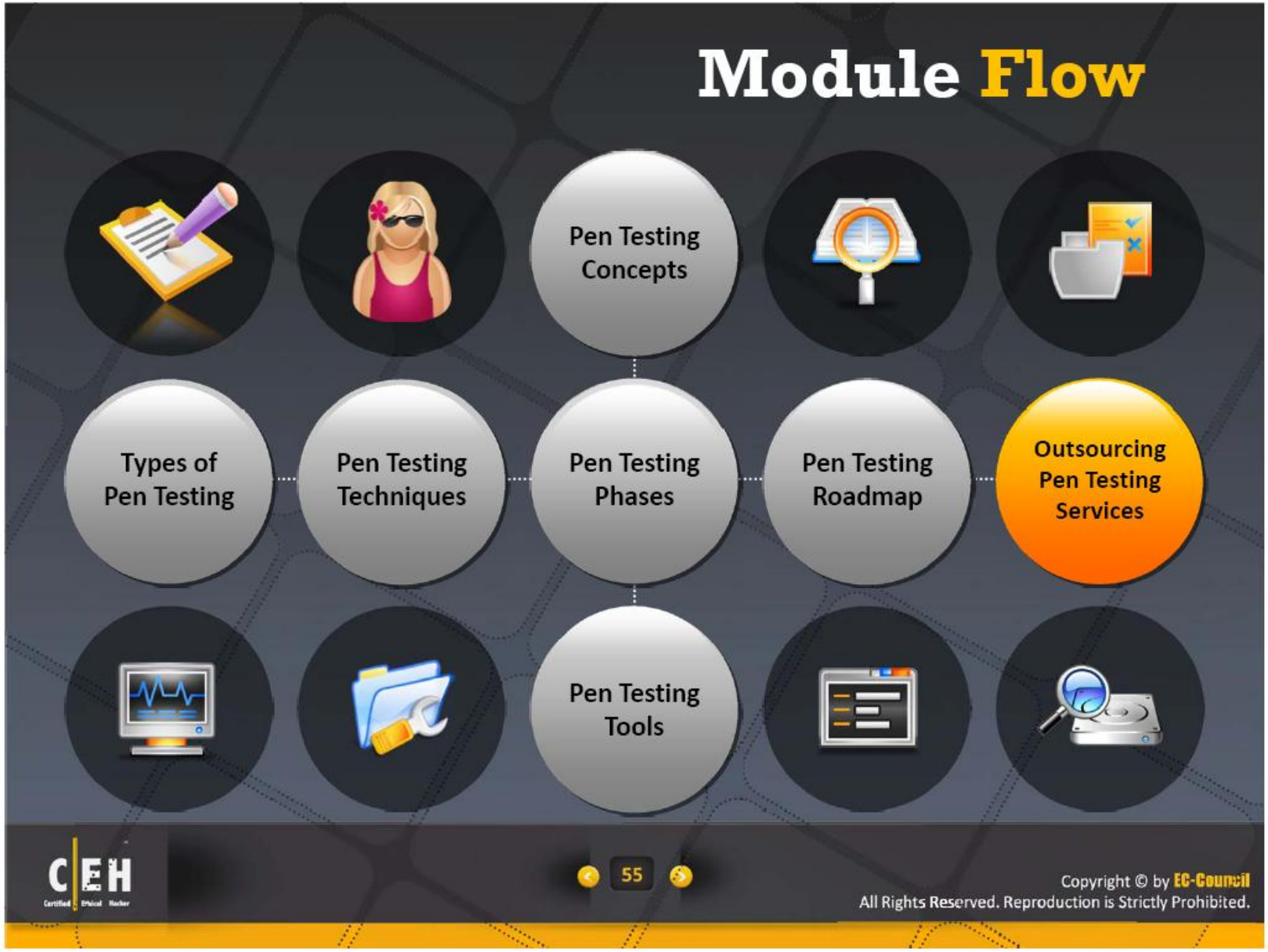
These tests are meant to check the effectiveness of anti-DoS devices

DoS attacks can be emulated using hardware

Some online sites simulate DoS attacks for a nominal charge



Module Flow



Outsourcing Penetration Testing Services

Drivers for outsourcing pentest services

To get the network audited by an external agency to acquire an **intruder's point** of view

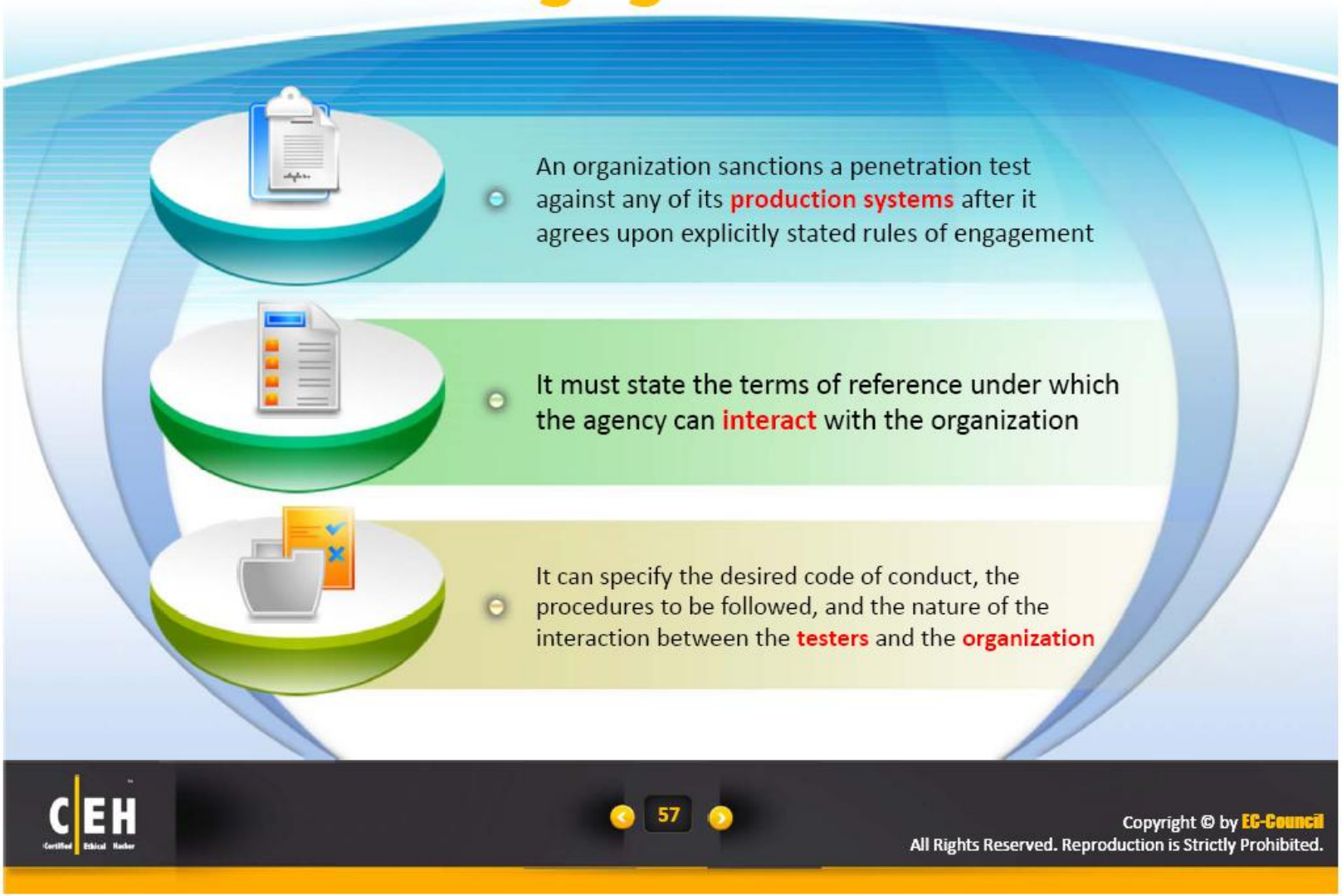
The organization may require a specific **security assessment** and **suggestive corrective measures**

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**

Underwriting penetration testing

Terms of Engagement



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**

Pentest Service Level Agreements

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

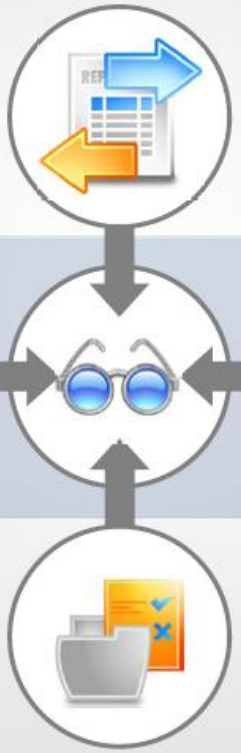
The bottom line is that SLAs define the minimum levels of availability from the testers and determine what actions will be taken in the event of **serious disruption**

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

Penetration Testing Consultants

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

A penetration test of a corporate network will examine **numerous different hosts** (with a number of different operating systems), **network architecture**, **policies** and **procedures**



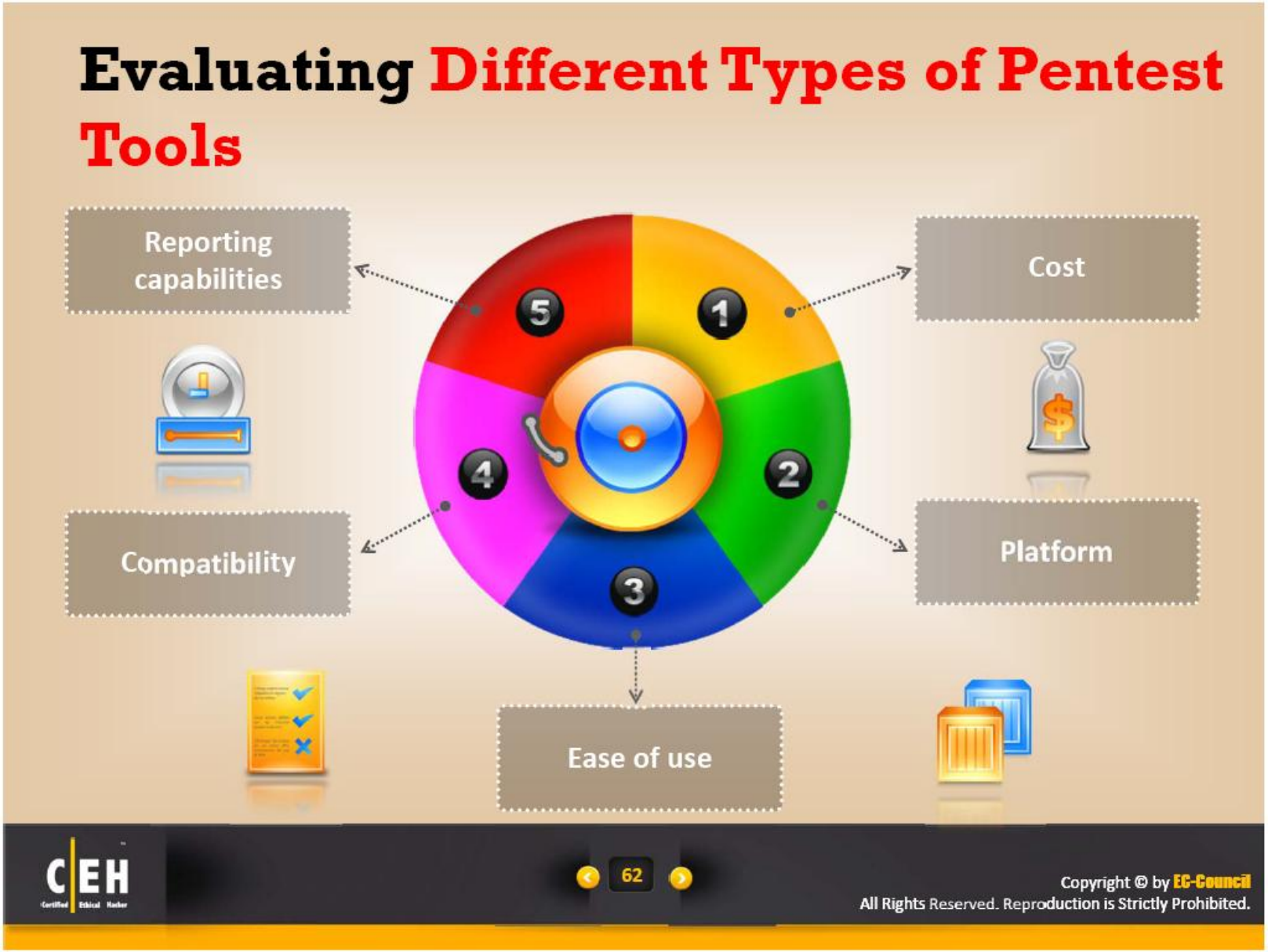
Each area of the network must be examined **in-depth**

Penetration testing skills cannot be obtained without years of experience in **IT fields**, such as development, systems administration, or consultancy

Module Flow

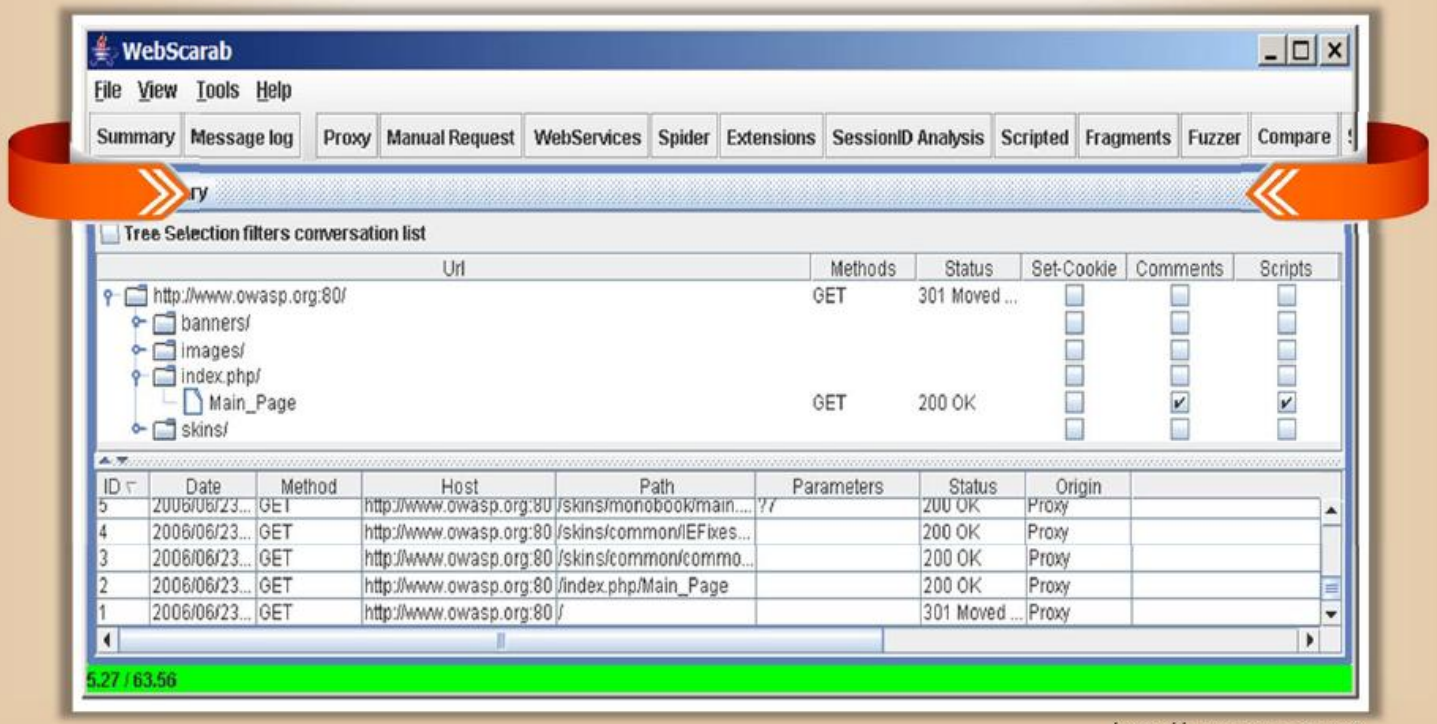

Pen Testing Concepts
Types of Pen Testing
Pen Testing Techniques
Pen Testing Phases
Pen Testing Roadmap
Outsourcing Pen Testing Services
Pen Testing Tools
CEH
Certified Ethical Hacker
61
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Evaluating Different Types of Pentest Tools



Application Security Assessment Tool: Webscarab

It is a framework for analyzing applications that communicate using the HTTP and HTTPS protocols



http://www.owasp.org

Application Security Assessment Tools

Acunetix
http://www.acunetix.com

Wapiti
http://www.ict-romulus.eu

Netsparker
http://www.mavitunasecurity.com

Watcher
http://websecuritytool.codeplex.com

NStalker
http://nstalker.com

Websecurify
http://www.websecurify.com

skipfish
http://code.google.com

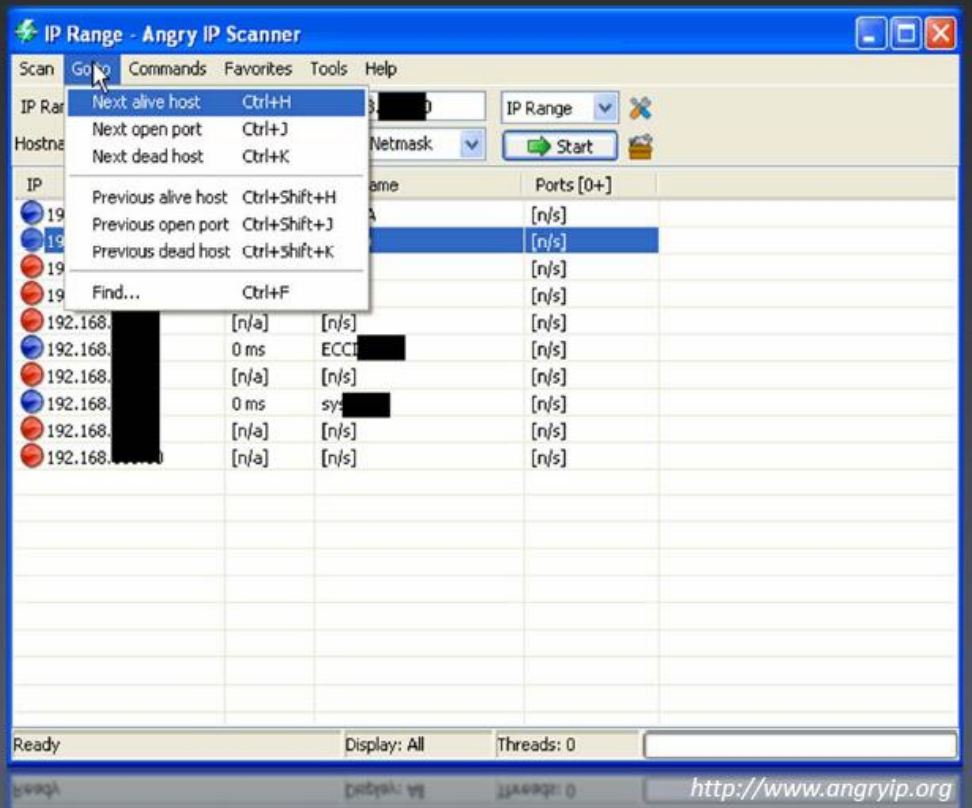
x5s
http://xss.codeplex.com

Network Security Assessment Tool:
Angry IP scanner

Scans **IP addresses** as well as **ports** in any range

Features:

- NetBIOS information
- Favorite IP address ranges
- Web server detection
- Customizable openers



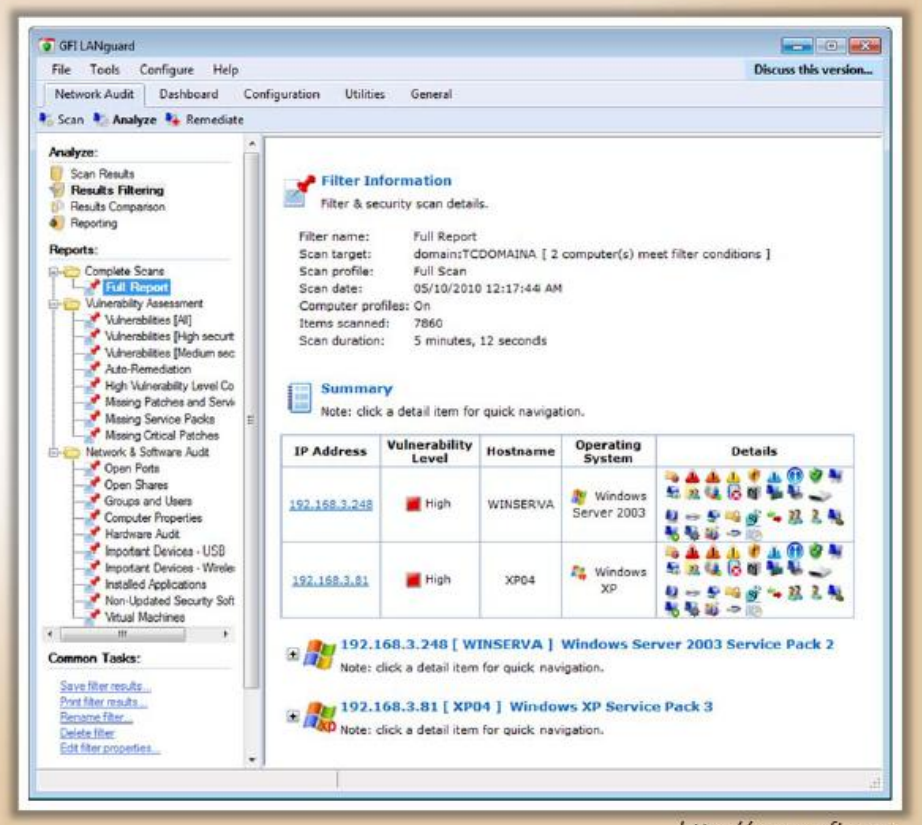
CEH

Network Security Assessment Tool:
GFI LANguard

GFI LANguard is a **network security scanner** and patch management solution

GFI LANguard assists in the areas:

- Patch management
- Vulnerability management
- Network and software auditing
- Assets inventory
- Change management
- Risk analysis and compliance



http://www.gfi.com

Network Security Assessment Tools

Cain and Abel
http://www.oxid.it

Nessus
http://www.nessus.org

John the Ripper
http://www.openwall.com

Snort
http://www.snort.org

Kismet
http://www.kismetwireless.net

Tcpdump
http://www.tcpdump.org

Ntop
http://www.ntop.org

Wireshark
http://www.wireshark.org

Wireless/Remote Access Assessment Tool: Kismet

- It is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system
- Identifies networks by passively collecting packets
- Detects hidden networks and presence of nonbeaconing networks via data traffic

http://www.kismetwireless.net

Wireless/Remote Access Assessment Tools

Aircrack
http://www.aircrack-ng.org

WiFi scanner
http://netsecurity.about.com

Airsnot
http://airsnort.shmoo.com

FakeAP
http://netsecurity.about.com

KisMAC
http://trac.kismac-ng.org

TigerII WAP Tool
http://tigerii-wap-tools.findmysoft.com

Netstumbler
http://www.stumbler.net

Blueauditor
http://www.wirelessnetworktools.com

Telephony Security Assessment Tool: Omnipeek

Omnipeek is a **network analyzer** offering real-time **VoIP monitoring and analysis** combined with Ethernet, Wireless, 10GbE, Gigabit, and WAN

http://www.wildpackets.com

Telephony Security Assessment Tools

VLANping
http://www.hackingvoip.com

VoIPER
http://voiper.sourceforge.net

VoIP Hopper
http://sourceforge.net

Vo²IP
http://www.voipsa.org

Voipong
http://www.enderunix.org

NSAUDITOR - SIP UDP Traffic Generator - Flooder
http://www.nsauditor.com

Vomit
http://vomit.xtdnet.nl

VoIPaudit
http://www.voipshield.com

Testing Network-Filtering Device Tool: Traffic IQ Professional

Traffic IQ Professional enables security professionals to **audit and validate the behavior of security devices** by generating the **standard application traffic or attack** traffic between two virtual machines

Traffic IQ Professional can be used to **assess, audit,** and **test the behavioral characteristics** of any non-proxy packet-filtering device including:

- **Application layer firewalls**
- **Intrusion detection systems**
- **Intrusion prevention systems**
- **Routers and switches**

http://www.blade-software.com

Module Summary

- A pentest simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them
- Security assessment categories are security audits, vulnerability assessments, and penetration testing
- Vulnerability scanners can test systems and network devices for exposure to common attacks
- Penetration testing reveals potential consequences of a real attacker breaking into the network
- Risk = Threat x Vulnerability
- The Abyss Web server application is a small personal web server that can support HTTP/1.1 CGI scripts, partial downloads, caching negotiation, and indexing files

Quotes

"All of the biggest technological inventions created by man - the airplane, the automobile, the computer - says little about his intelligence, but speaks volumes about his laziness."

- Mark Kennedy,
An American Businessman and Politician