Information Security Acts: Payment Card Industry Data Security Standard (PCI-DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard** for **organizations** that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
- PCI DSS **applies to all entities involved in payment card processing**, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data.
- High-level overview of the PCI DSS requirements developed and maintained by the **Payment Card Industry (PCI) Security Standards Council.**

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	Implement Strong Access Control Measures
Protect Cardholder Data	Regularly Monitor and Test Networks
Maintain a Vulnerability Management Program	Maintain an Information Security Policy

- Transaksi keuangan dengan menggunakan kartu sudah menjadi aktifitas sehari-hari bagi semua orang, maka dari itu PCI Data Security Standar menjadi tolak ukur sistem keamanan tingkat tinggi.

Information Security Acts: Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act, universally known as HIPAA, deals with personal health data, which is defined as:

- An individual's past, present, or future physical or mental health or condition
- An individual's provision of health care
- Past, present, or future payment for provision of health care to an individual

The primary objective of the security rule is to protect the confidentiality, integrity, and availability of data when it is managed (i.e. stored, maintained, or transmitted) by a health care provider).

Health-care providers must give notice of privacy policies and procedures to patients, obtain consent and authorization for use of information, and tell how information is generally shared, and how patients can access, inspect, copy, and amend their own medical records.

- Health Insurance Portability and Accountability Act (HIPAA) adalah Hukum federal di Amerika Serikat yang menciptakan standar nasional untuk melindungi privasi catatan medis pasien dan informasi kesehatan pribadi lainnya.

Proses Pembentukan CISO

- Sarbanes–Oxley is a United States federal law that set new or enhanced standards for all US public company **boards**, **management**, and **public accounting firms.**
- The rules and enforcement policies outlined by the SOX Act amend or supplement existing legislation dealing with **security regulations.**

Section 302

- A mandate that requires senior management to certify the accuracy of the reported financial statement
- CEOs and CFOs of accounting companies' clients must sign statements verifying the completeness and accuracy of financial reports

Section 404

- A requirement that management and auditors establish internal controls and reporting methods on the adequacy of those controls
- CEOs, CFOs, and auditors must report on and attest to the effectiveness of internal controls for financial reporting

- Sarbanes Oxley Act (Sox) adalah Hukum federal di Amerika Serikat sebagai tanggapan terhadap sejumlah skandal akuntansi perusahaan besar yang mengguncang saham nasional. Sox membentuk PCAOB yang bertugas untuk mengawasi, mengatur, memeriksa, dan mendisiplinkan kantor akuntan dalam peranan mereka sebagai auditor perusahaan publik.

Information Security Acts: Gramm-Leach-Bliley Act (GLBA)

- The objective of the **Gramm-Leach-Bliley Act** was to ease the transfer of **financial** information between **institutions** and **banks** while making the rights of the individual through **security** requirements more specific.

Key Points Include:

- Protecting consumers' **personal financial information** held by financial institutions and their service providers
- The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than **$10,000 for each violation**

Although the penalty is small, it is easy to see how it could impact a bank

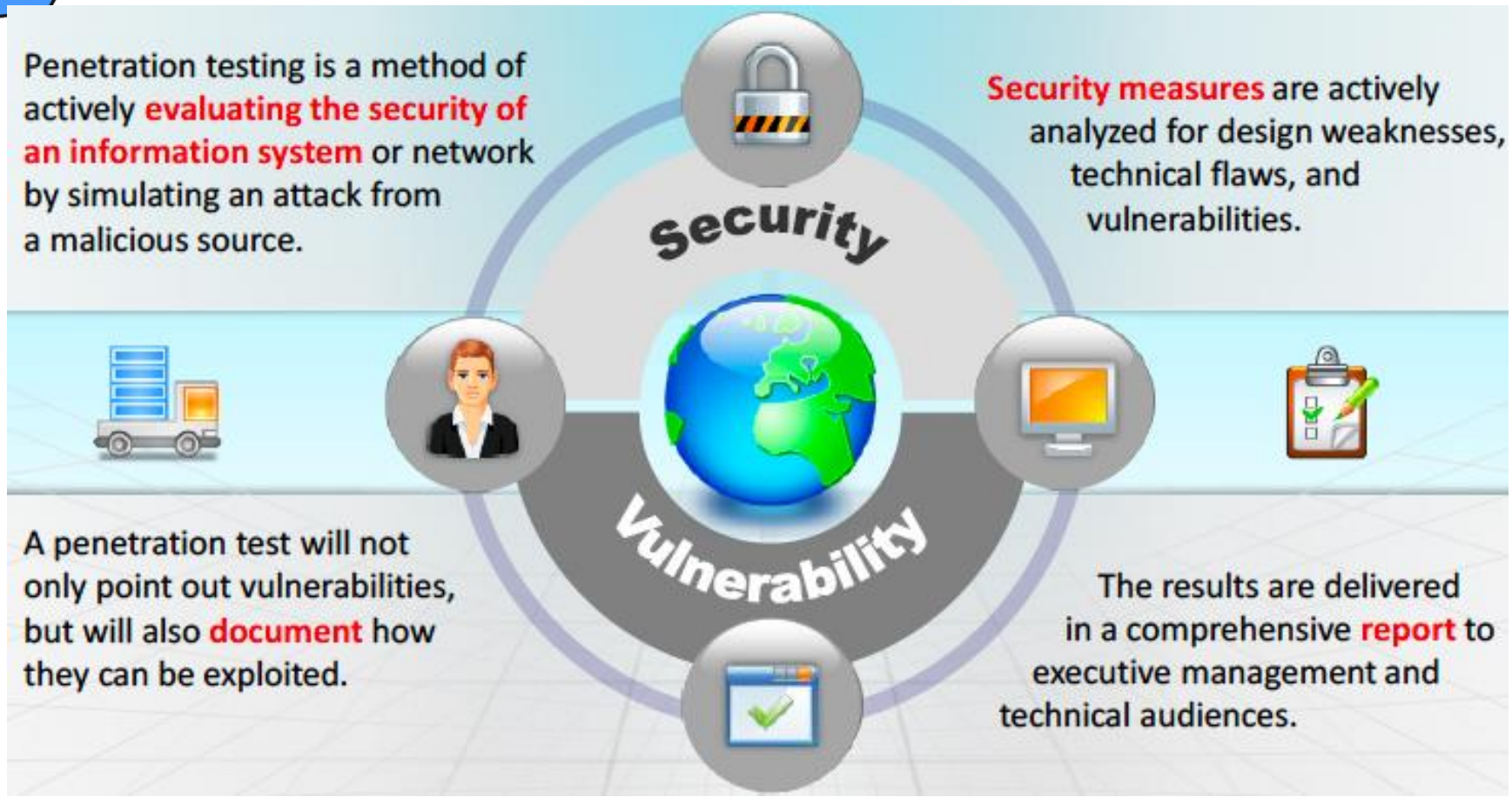
- Gramm-Leach-Bliley Act adalah Hukum federal yang diberlakukan di Amerika Serikat untuk mengontrol kesepakatan lembaga keuangan dengan informasi pribadi pelanggan.

Information Security Acts and Laws

1. USA Patriot Act 2001
2. The Data Protection Act 1998
3. Freedom of Information Act (FOIA)
4. The Electronic Communications Privacy Act
5. The Audit Investigation and Community Enterprise Act 2005
6. The Human Rights Act 1998
7. The Freedom of Information Act 2000
8. Computer Fraud and Abuse Act

- Undang-undang dan Hukum keamanan informasi.

Penetration Testing Methodology



- Penetration testing adalah metode aktif guna mengevaluasikan keamanan sistem informasi atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya.

Why Penetration Testing?

Proactively **identify the threats** and determine the **probability of an attack** on information assets	Ensure effective implementation of security controls and a better **Return on Investment** (ROI) on IT security
A comprehensive pen test provides an **assurance** that the organization is operating within an acceptable limit of information security risks	Achieve **compliance** to regulations and industry standards (ISO/IEC 27001:2013, PCI-DSS, HIPPA, FISMA, etc.)
Help in determining feasibility of a set of attack vectors and determine **potential business impact** of a successful attack	Focus on high severity vulnerabilities and **emphasize application-level security issues** to development teams and management
Provide a comprehensive approach for preparation steps that can be taken to **prevent upcoming exploitation**	Evaluate the efficiency of **network security devices** such as firewalls, routers, and web servers

- Penetration Testing dapat mengidentifikasi ancaman dan menentukan probabilitas serangan terhadap aset informasi.

Penetration Test vs. Vulnerability Test

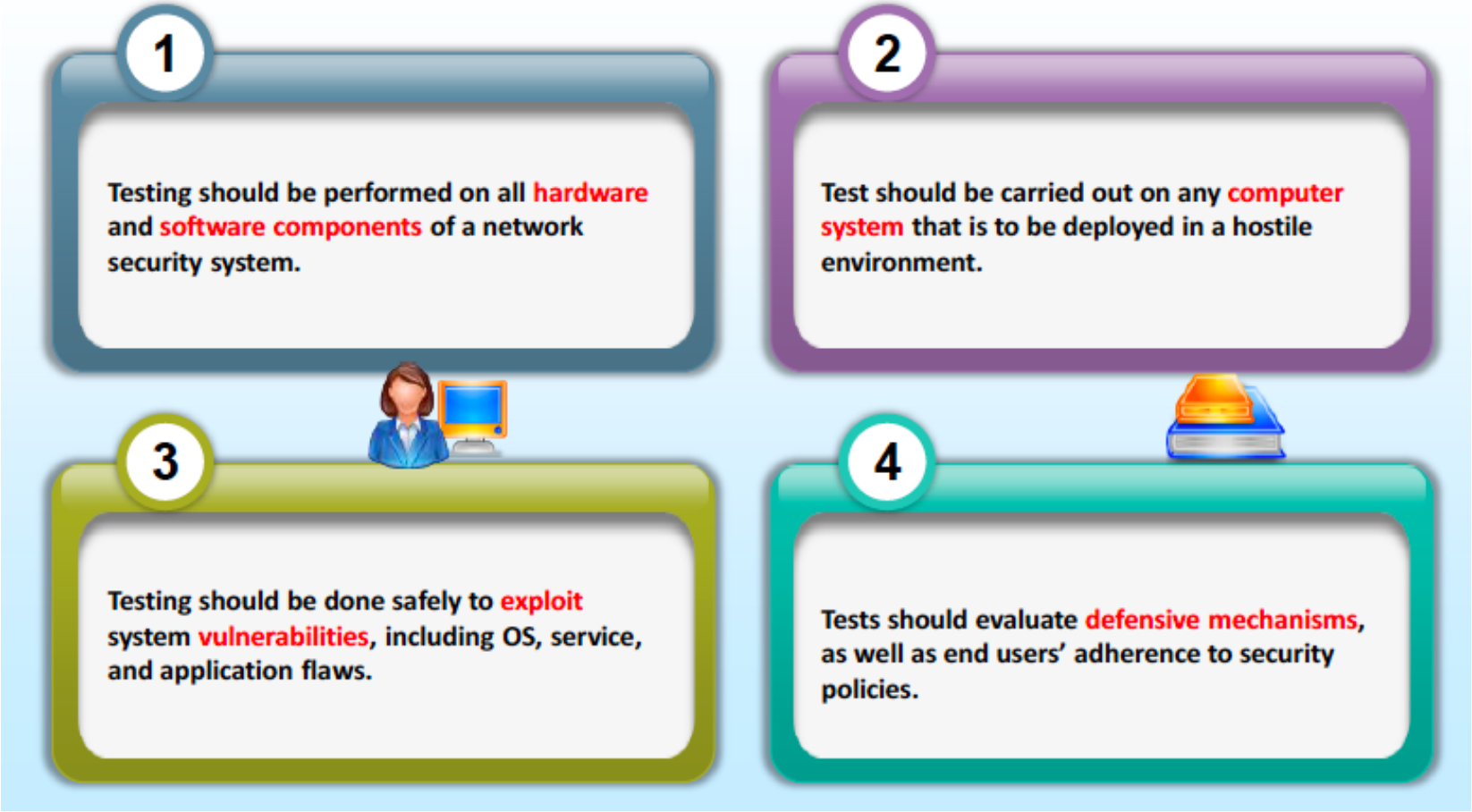
Penetration testing goes one step ahead of vulnerability testing: vulnerability tests verify known vulnerabilities; penetration tests adopt the concept of "**defense in depth.**"

As there are automated tools for vulnerability testing, there are likewise **automated** penetration testing tools.

Penetration testing goes beyond testing for known vulnerabilities and adopts innovative means of **demonstrating where security fails** in an organization.

- Penetration testing satu langkah diatas vulnerability testing yaitu Vulnerability test melakukan verifikasi kerentanan yang dikenal; Penetration tests mengadopsi konsep pertahanan berlapis.

What Should be Tested?



- Pengujian harus dilakukan pada semua komponen hardware dan software sistem keamanan jaringan.

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 the cost and benefits
- Following a methodology with proper planning and documentation
- Documenting the result carefully and making it comprehensible for the client

❖ Untuk melakukan Penetration Test yang baik meliputi; Objectives, Hiring Skilled, tests, methodology, Documenting the result.

Scope of Penetration Testing

Nondestructive Test

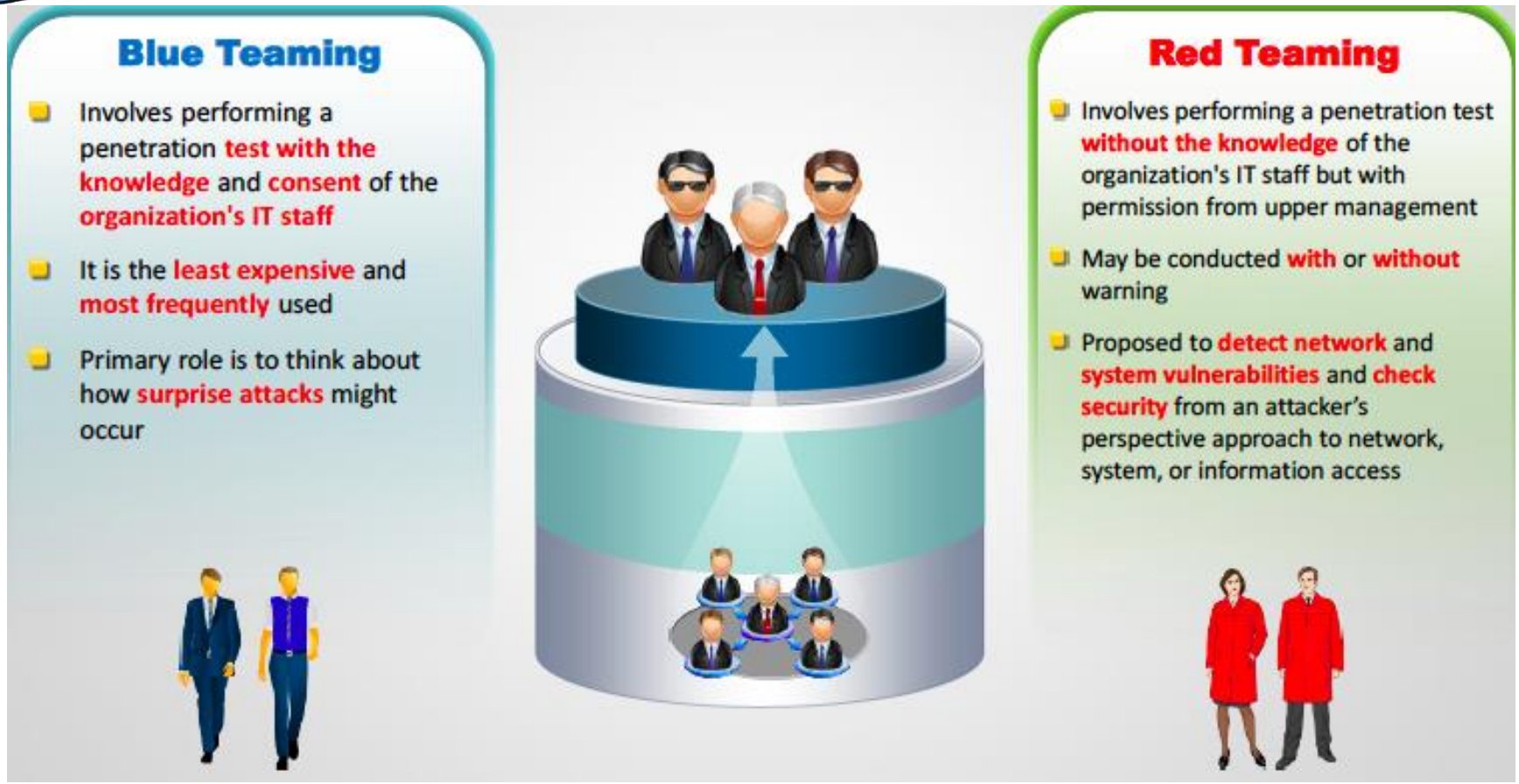
- Scans and identifies the **remote system** for potential vulnerabilities with proper care to avoid disruption
- Scans and identifies the **remote system** for potential vulnerabilities
- It only provides a **proof of concept** of the exploits
- **Does not attempt** a Denial-of-Service (DoS) and Buffer Overflow attacks that may result in disruption

Destructive Test

- Scans and identifies the **remote system** for potential vulnerabilities
- It relies on the **actual exploitation** of the vulnerabilities
- **Attempts** Denial-of-Service (DoS) and Buffer Overflow attacks

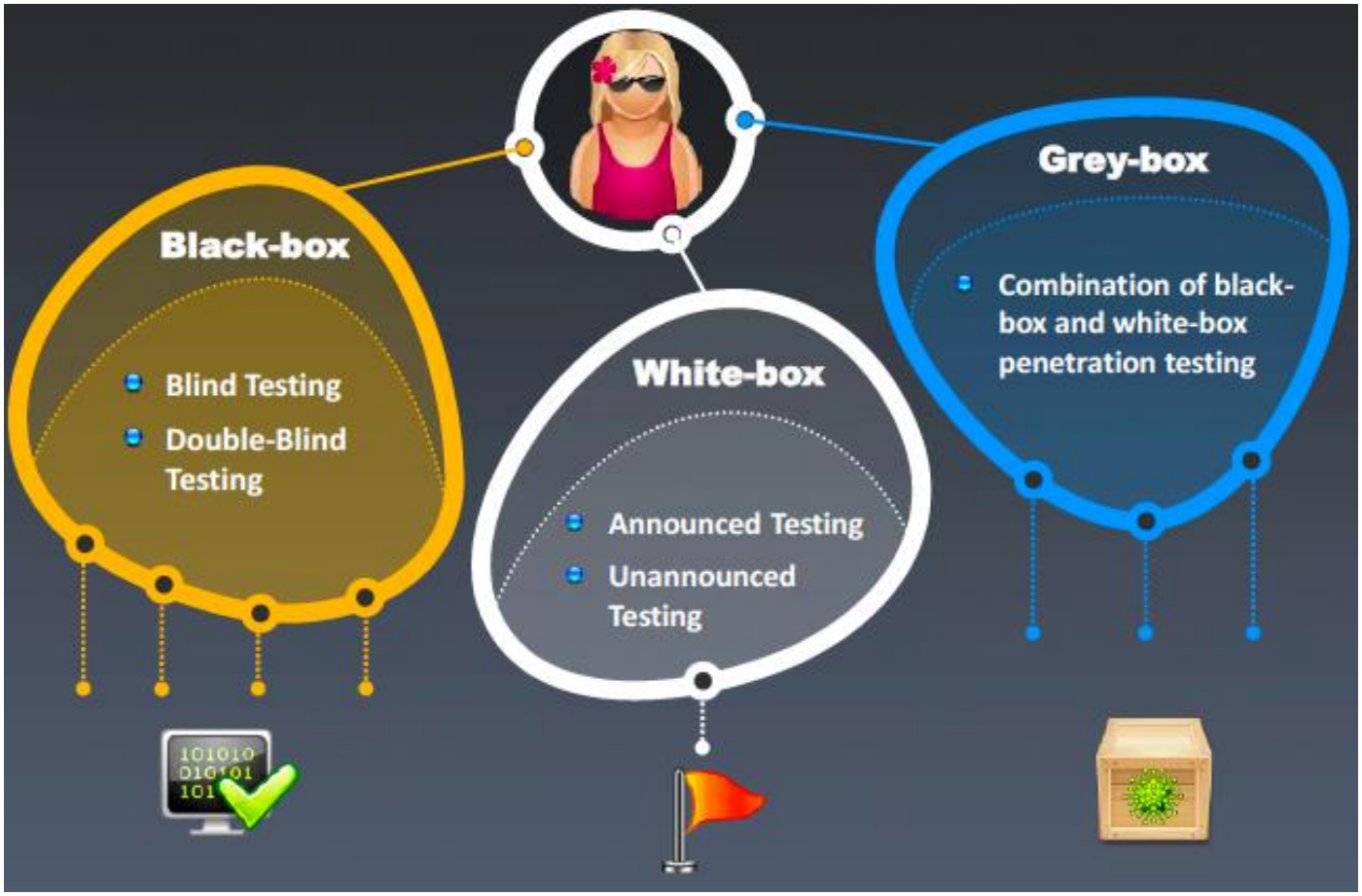
❖ Jangkauan dari Penertration Testing yaitu Nondestructive Test dan Destructive Test

Blue Teaming/Red Teaming



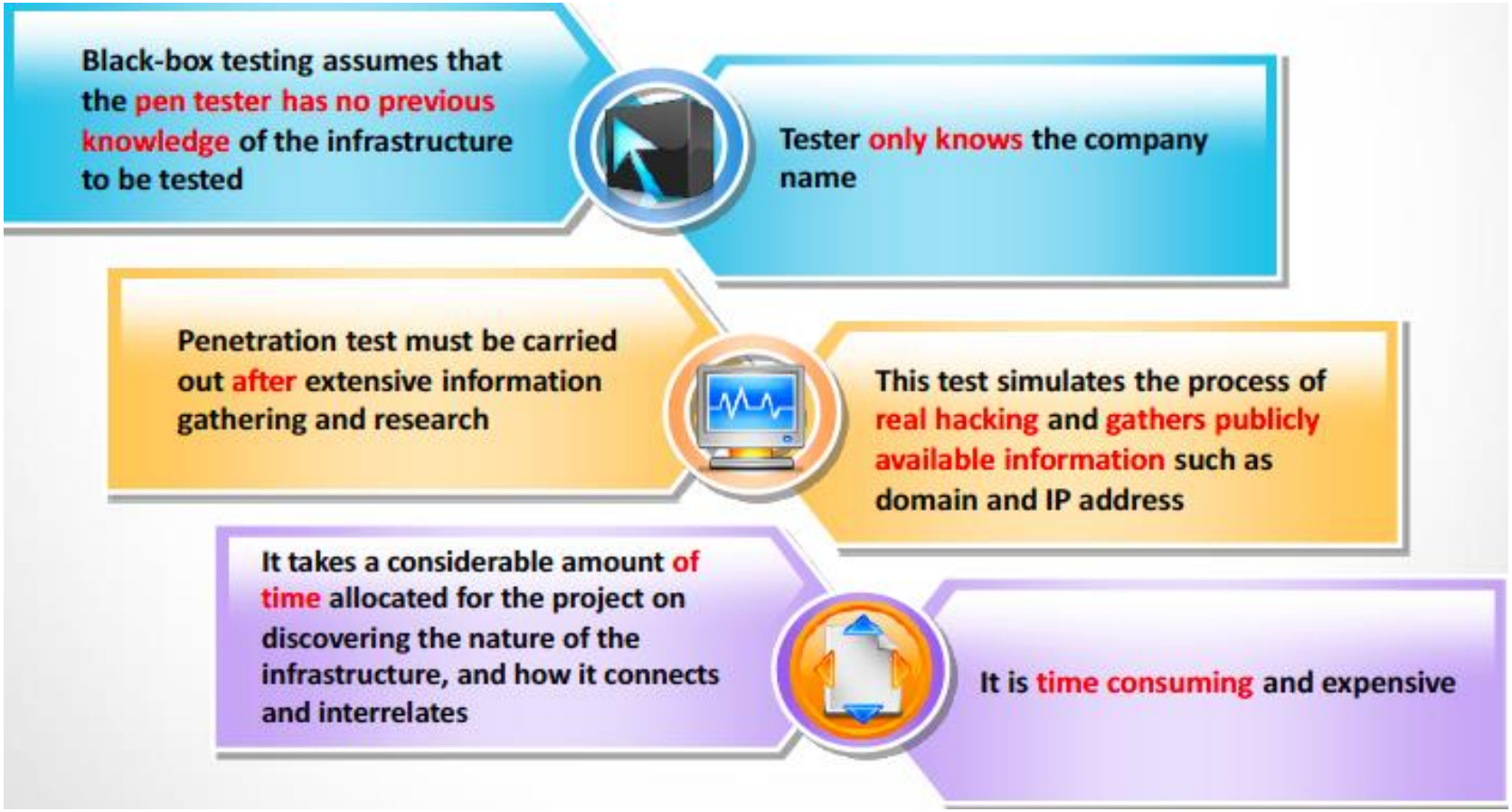
❖ Penetration Test biasanya terbagi menjadi 2 Tim yaitu Blue Teaming dan Red Teaming

Types of Penetration Testing



- Tipe-tipe Penetration Testing ada 3; Black-box, white-box dan grey-box.

Black-box Penetration Testing



- Pengujian dengan tipe black-box yaitu Mengasumsikan si pen tester (penguji) tidak memiliki pengetahuan sebelumnya mengenai infrastruktur yang akan diuji, Pentester hanya mengetahui nama perusahaan saja.

Black-box Penetration Testing (Lanjutan)

Blind Testing

- Simulates the **methodologies** of a real hacker
- **Limited** or **no information** is provided to the penetration testing team
- Time-consuming and **expensive** process

Double-Blind Testing

- **Few people** in the organization are aware of the penetration test being conducted
- Involves testing an **organization's security monitoring**, incident identification, and response procedures

❖ Pada pengujian black-box kita biasanya ada 2 tipe pengujian lagi yaitu Blind Testing dan Double-blind Testing.

White-box Penetration Testing

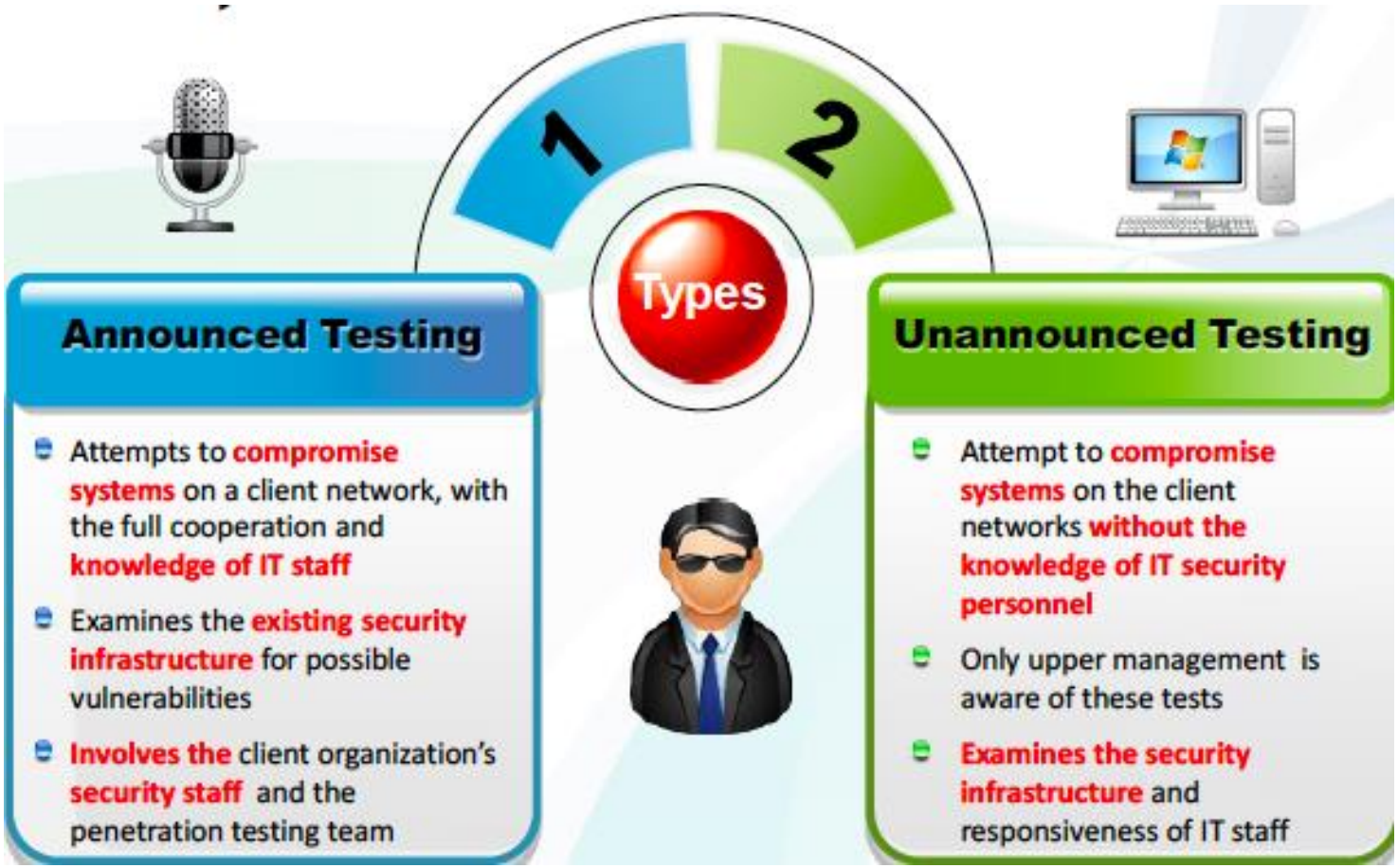
- You will be given **complete knowledge** of the infrastructure to be tested.
- This test simulates the process of a **company's employees.**

You will be provided information such as:

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

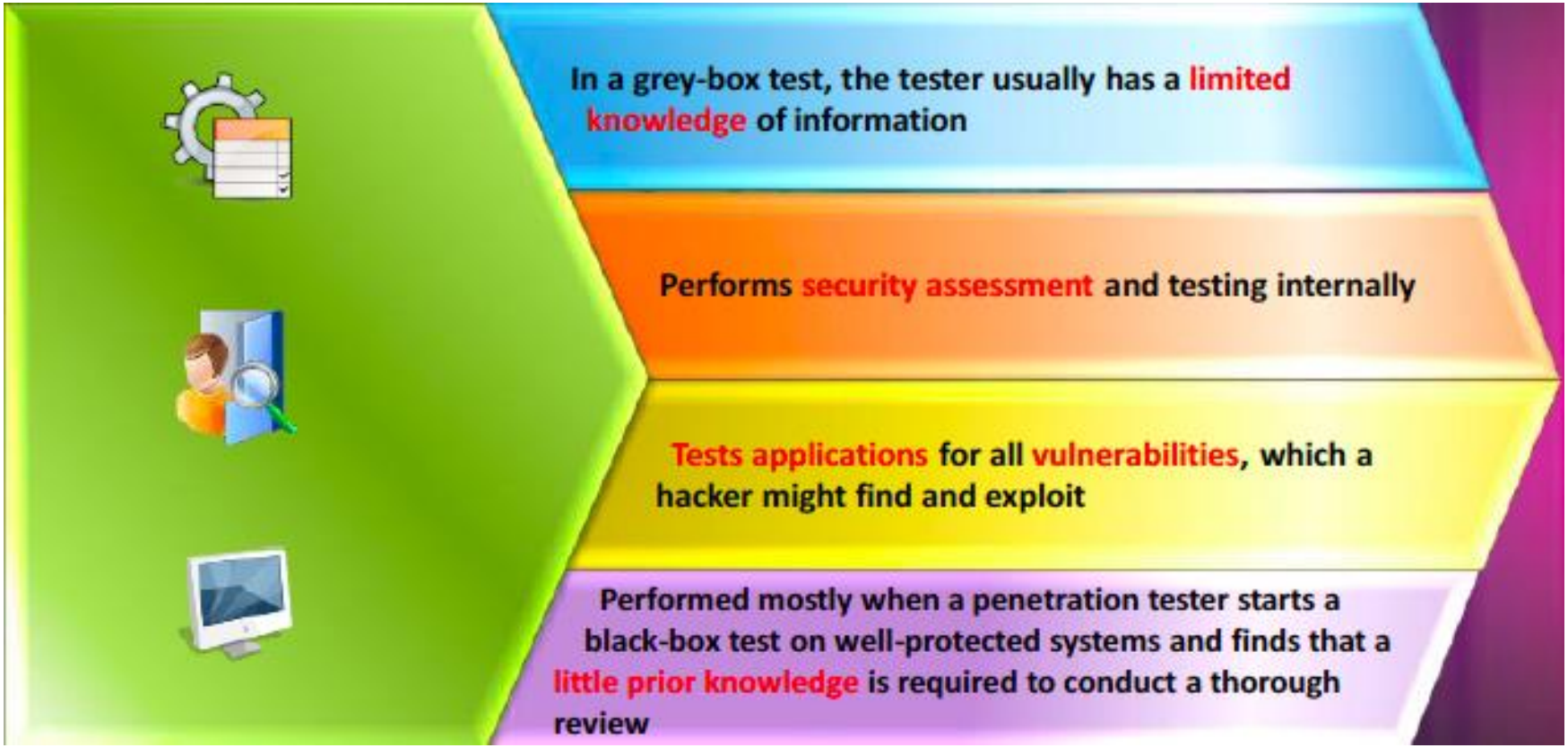
❖ Pada tipe pengujian White-box Penetration Testing; Pentesters diberikan pengetahuan yang lengkap mengenai infrastruktur yang akan diuji.

White-box Penetration Testing (Lanjutan)



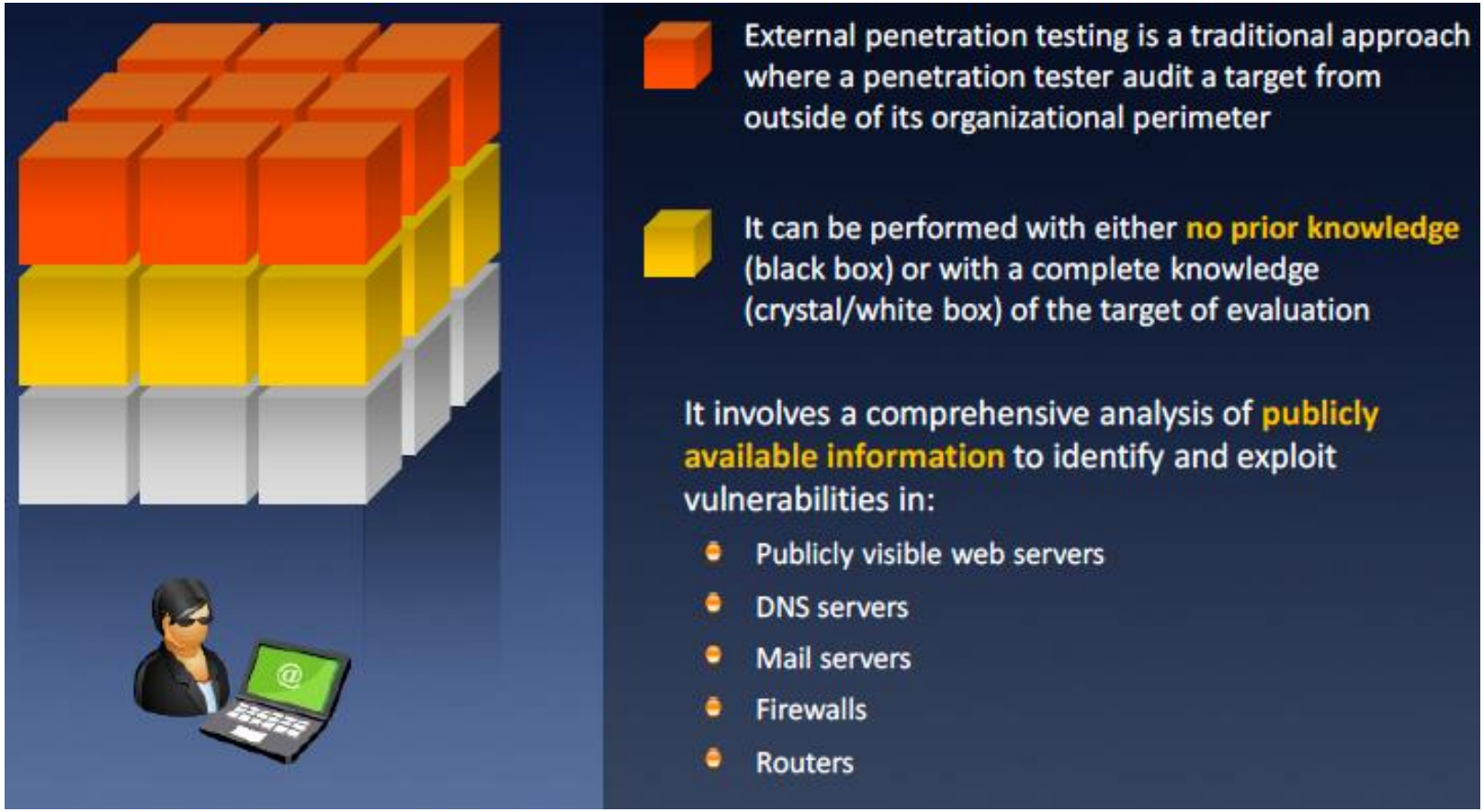
- Pada pengujian white-box kita biasanya ada 2 tipe pengujian lagi yaitu Announced Testing dan Unannounced Testing.

Grey-box Penetration Testing



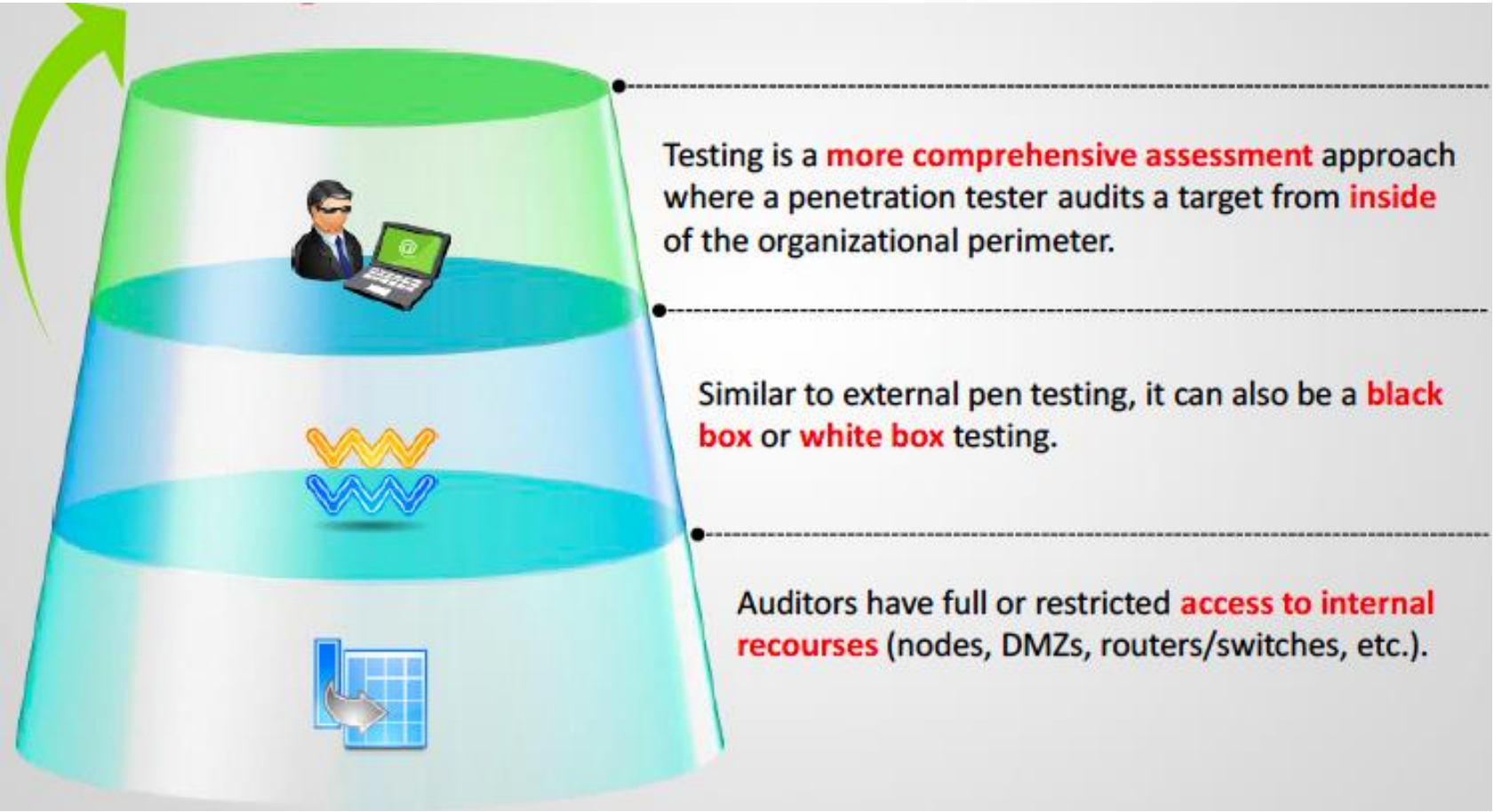
- Pada Pengujian menggunakan grey-box, pentester biasanya mendapatkan Informasi yang terbatas, melakukan pengujian keamanan dan pengjujian secara internal.

Penetration Testing Strategies: External Penetration Testings



- Eksternal Penetration Testing yaitu Pendekatan secara tradisional dimana seorang Pentester mengaudit sasaran dari luar perimeter organisasi tersebut.

Penetration Testing Strategies: Internal Penetration Testing



- Internal Penetration Testing yaitu Pendekatan secara komprehensif dimana seorang Pentester mengaudit sasaran dari dalam perimeter organisasi tersebut.

Penetration Testing Process

Defining the Scope

- The extent of testing
- What will be tested
- From where it will be tested
- By whom it will be tested

Performing the Penetration Test

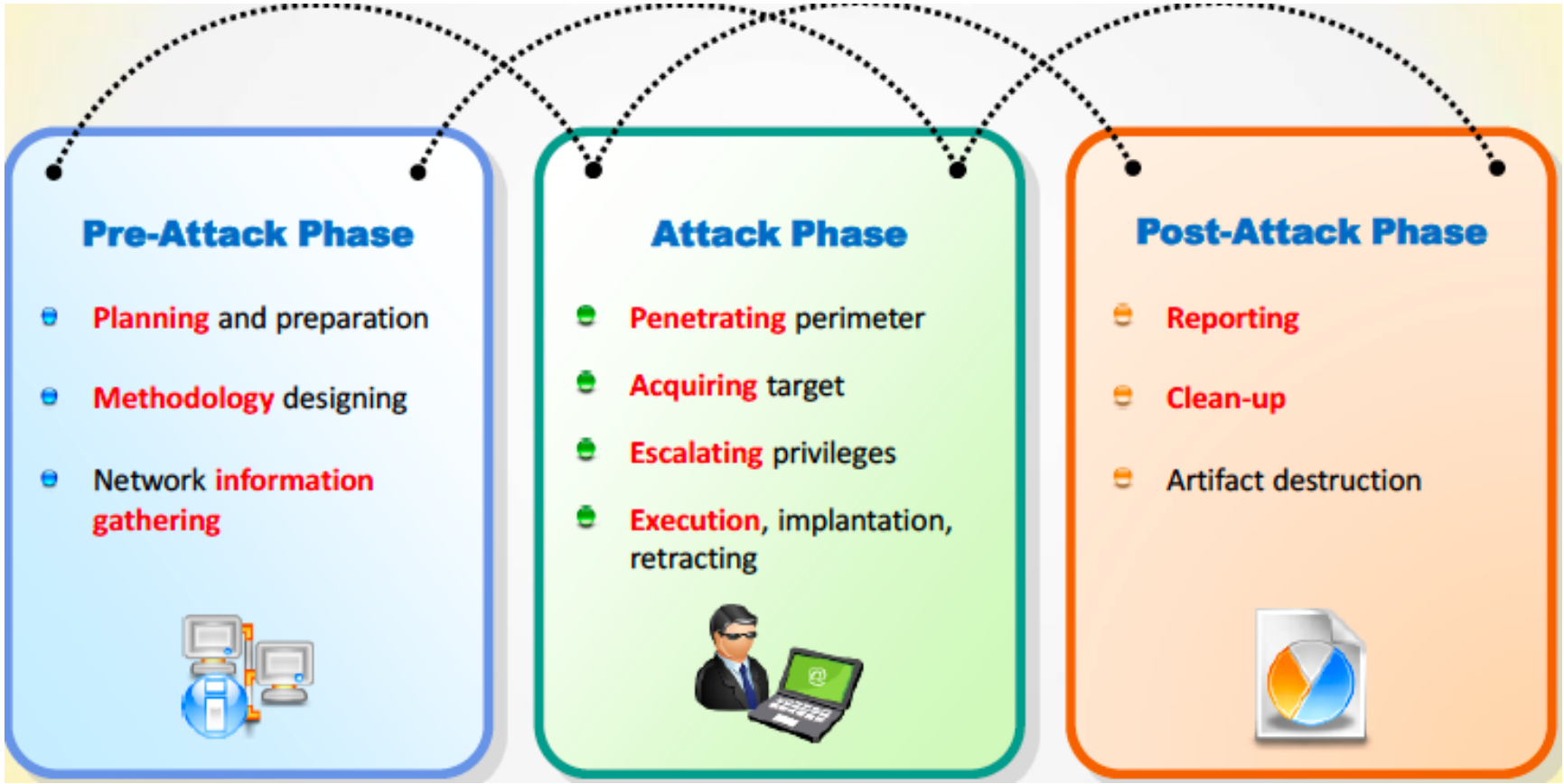
- Involves gathering all the information significant to security vulnerabilities
- Involves testing the targeted environment, such as network configuration, topology, hardware, and software

Reporting and Delivering Results

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

- Proses PenTest meliputi; mendefinisikan lingkup, melakukan PenTest, pelaporan dan memberikan hasil.

Penetration Testing Phases



- Fase-fase PenTest meliputi; Fase sebelum penyerangan, Fase Penyerangan, dan Fase setelah penyerangan.

Pre-Attack Phase

- This phase is **focused on gathering** as much information as possible about the target to be attacked
- The pre-attack phase can be categorized into **two types**:
  - Passive reconnaissance
  - Active reconnaissance

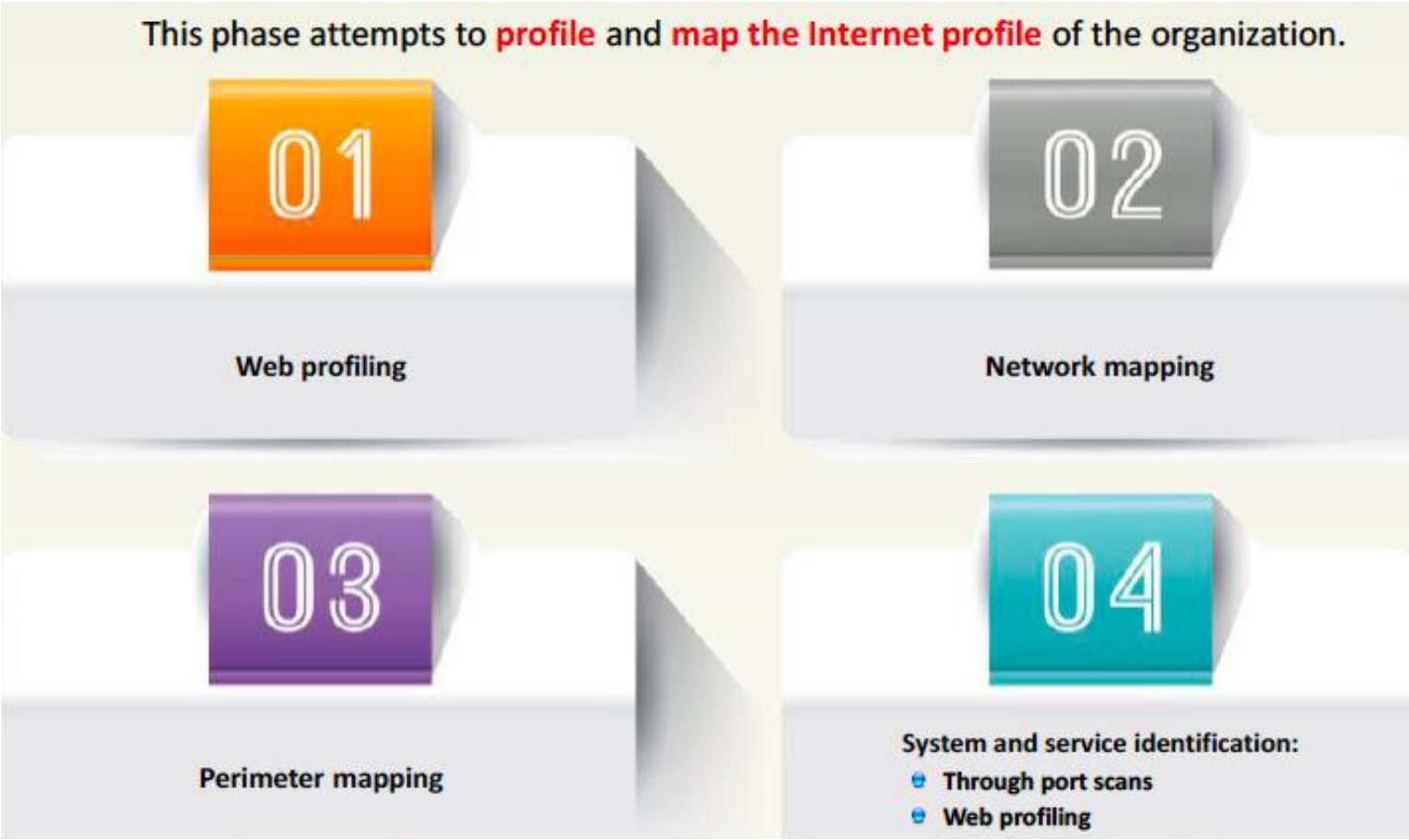
❖ Fase ini berfokus pada pengumpulan informasi target sebanyak mungkin untuk diserang.

Pre-Attack Phase: Passive Reconnainssance

- Using passive reconnaissance, the tester gathers information about an intended target.
- Information related to the network topology and the types of services running within are mostly gathered here.

❖ Menggunakan pengintaian pasif, Penguji mengumpulkan semua informasi tentang target yang akan diserang.

Pre-Attack Phase: Active Reconnaissance



- Pada fase ini kita mencoba untuk memetakan internet pada jaringan internet, seperti web, network, perimeter bahkan sistem dan servis

Attack Phase

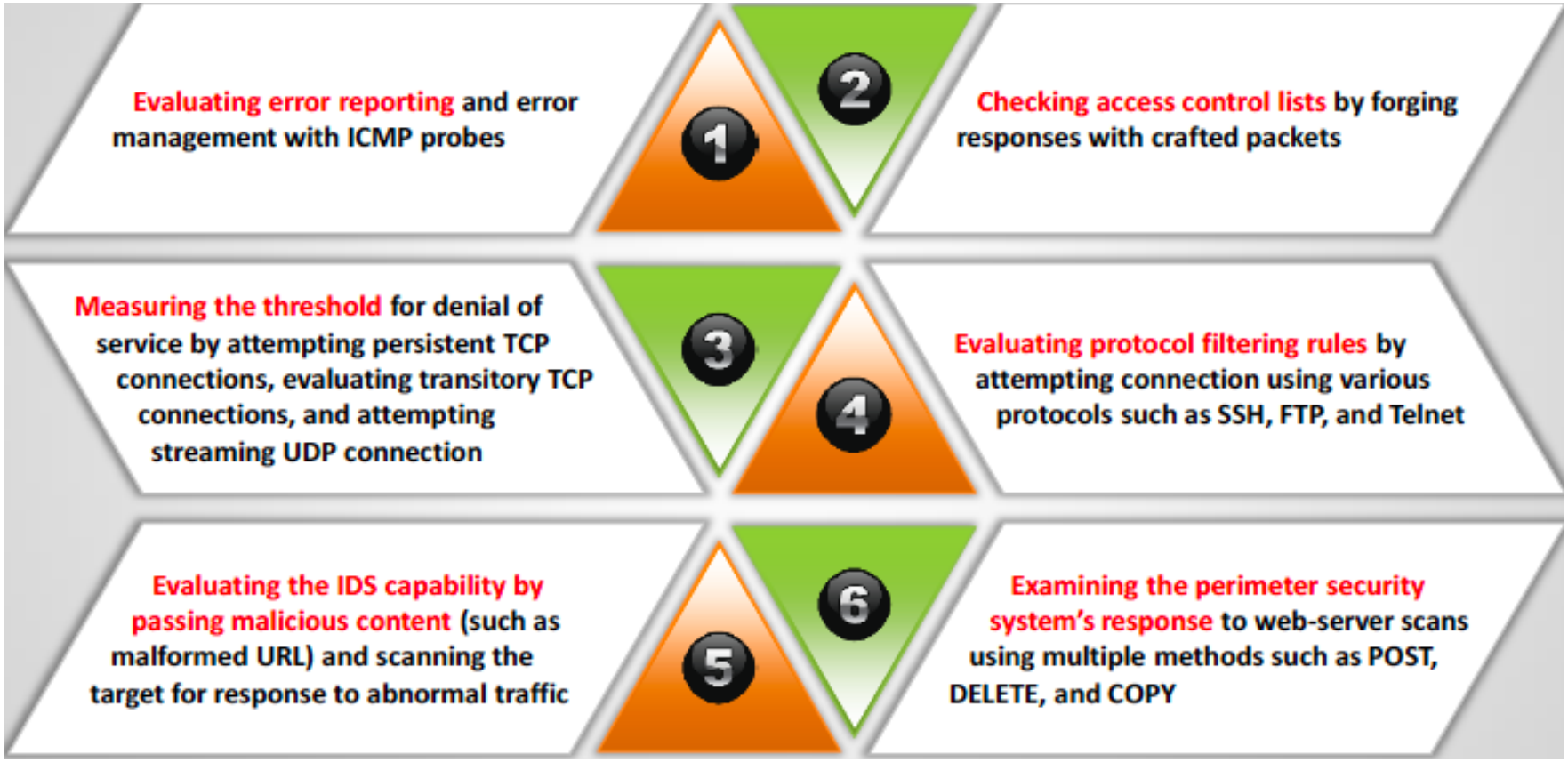
- This is the **actual phase** during which a pen tester tries to **exploit** vulnerabilities identified during the previous phase.
- This phase can be completed after a pen tester does the following:

❖ Pada Fase ini adalah Fase dimana pentester mencoba untuk mengekspoitasi kerentanan yang sudah terindentifikasi di fase sebelummnya.

Attack-Phase Activities

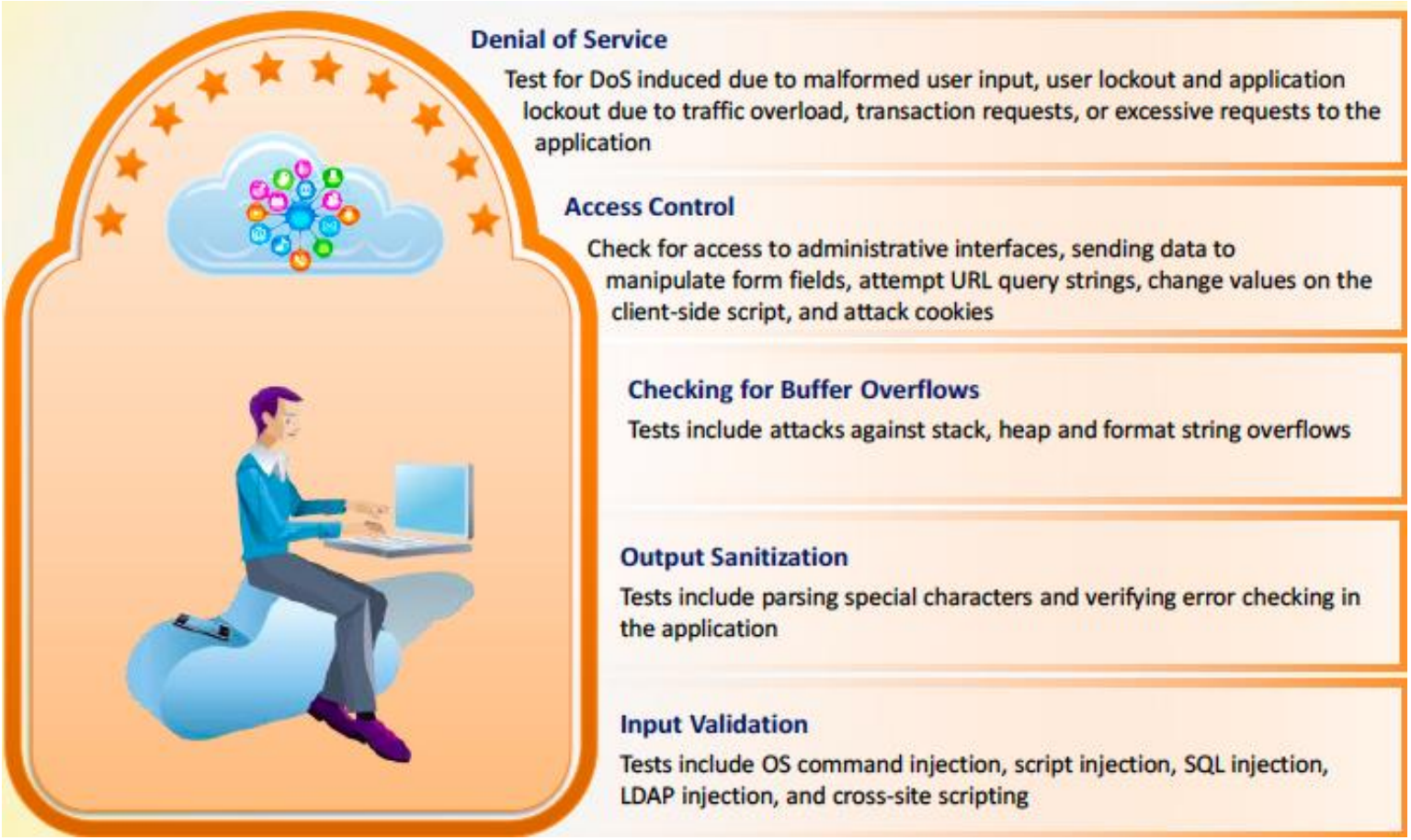
- Pada Fase penyerangan Aktifitas, Pentester menguji semua aktifitas-aktiftas yang ada pada jaringan internet di organisasi tersebut.

Activity: Perimeter Testing



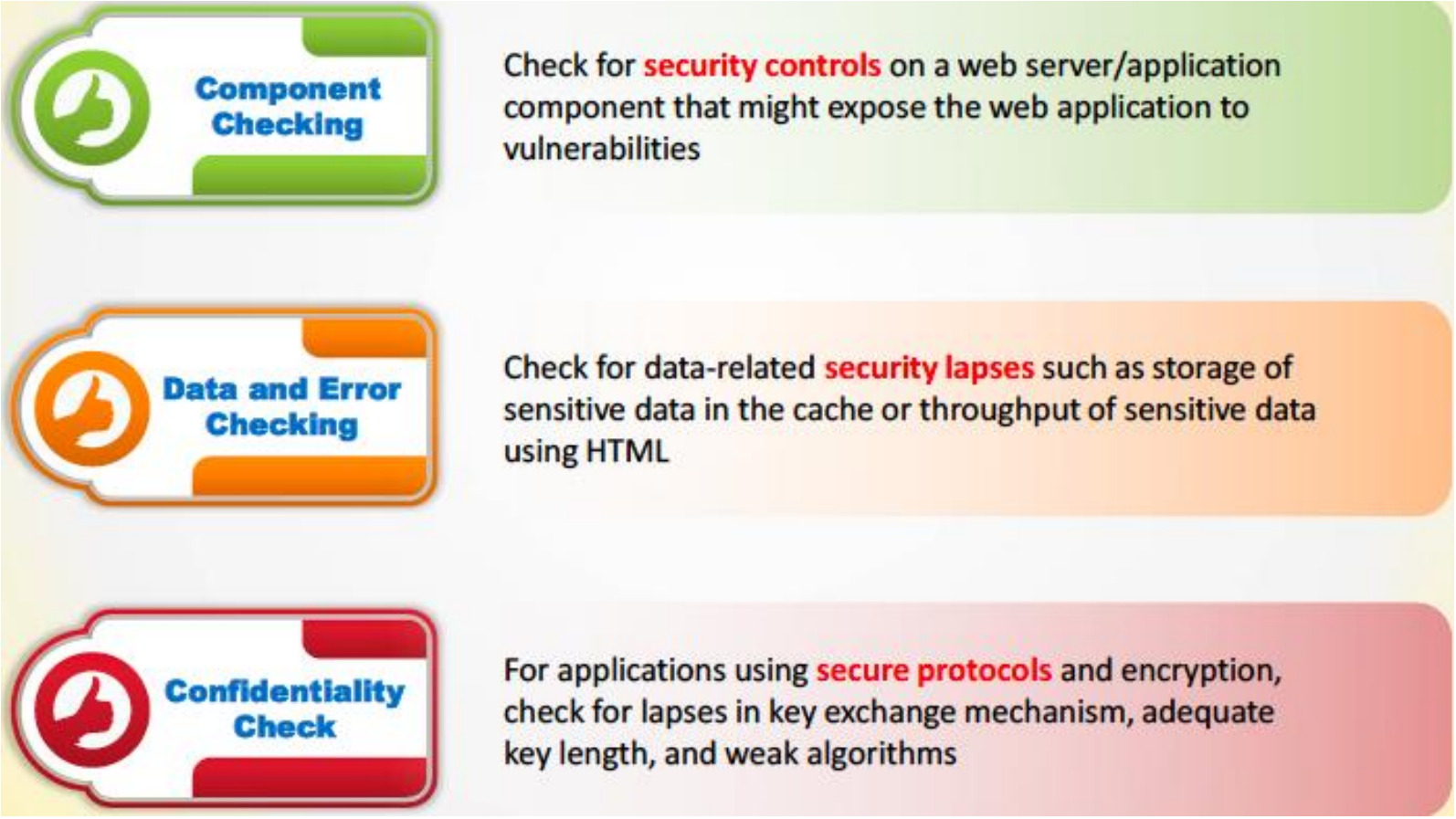
- Pentester mencoba untuk menguji perimeter yang ada di organisasi tersebut.

Activity: Web Application Testing - I



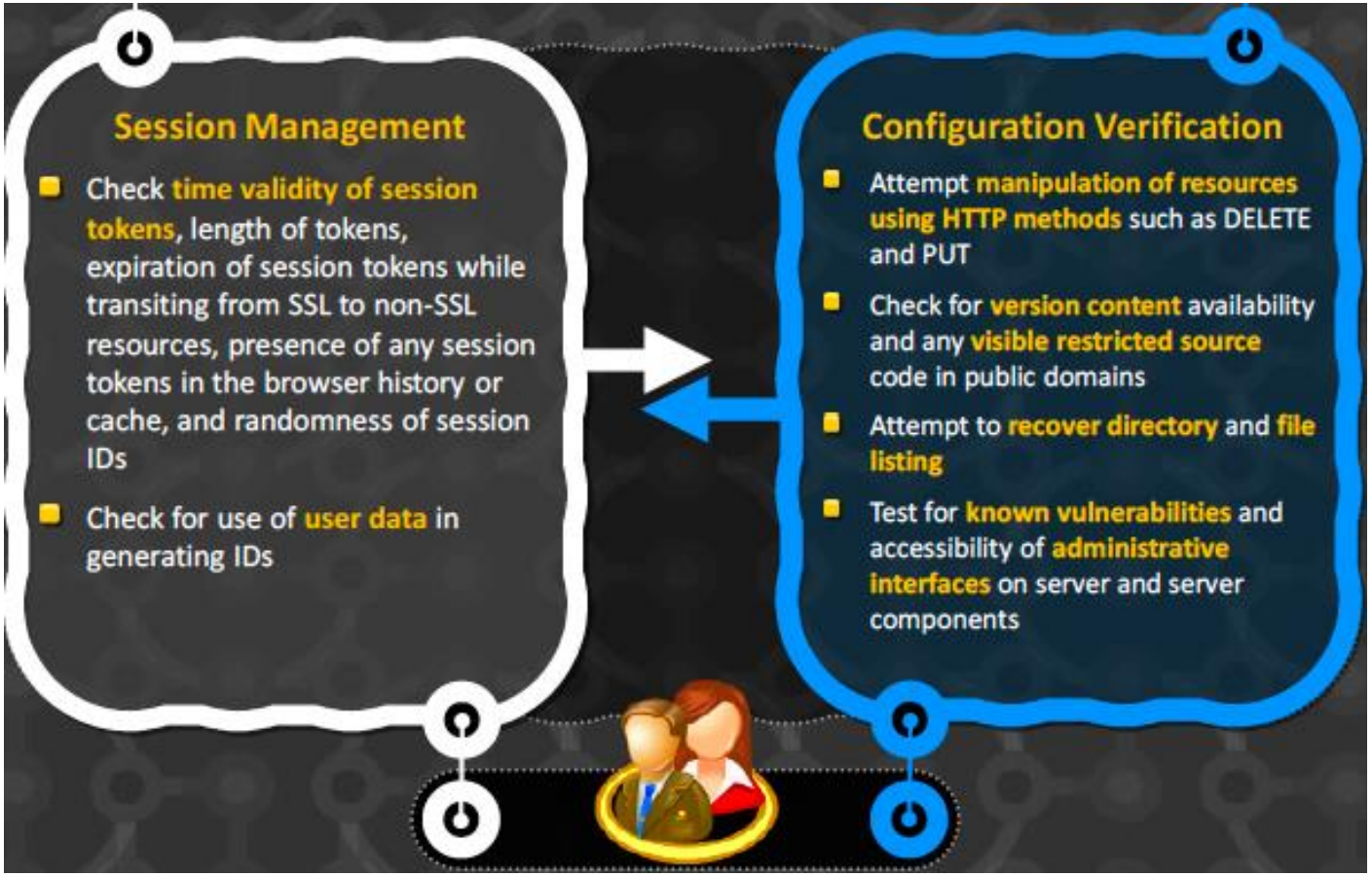
- Aktifitas berikut adalah Pentester melakukan pengujian pada semua web aplikasi

Activity: Web Application Testing - II



- Aktifitas berikut adalah Pentester melakukan pengujian pada semua web aplikasi yang meliputi, Security control, Security Lapses, Secure protocol.

Activity: Web Application Testing - III



- Setelah melakukan pengujian I dan II pentester akan melanjutkan pengujian Iii yaiutu Session Management dan Configuration Verification

Activity: Wireless Testing

Check if the access point's default **Service Set Identifier** (SSID) is easily available. Test for "**broadcast SSID**" and access to the LAN through this. Tests can include brute forcing the SSID character string using tools such as 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 there. Check if **layer 2 switched networks are being used** instead of hubs, for access-point connectivity.

Subject authentication to playback of previous authentications to check for privilege escalation and unauthorized access.

Verify **that access is granted only to client machines** with registered MAC addresses.

- Pada aktivitas ini, pengujian terhadap koneksi wireless,, apakah ada celah atau tidak pada konfigurasi wireless tersebut.

Activity: Application Security Assessment

- Aktivitas ini, pentester akan mencoba mengeksploitasi aplikasi keamanan

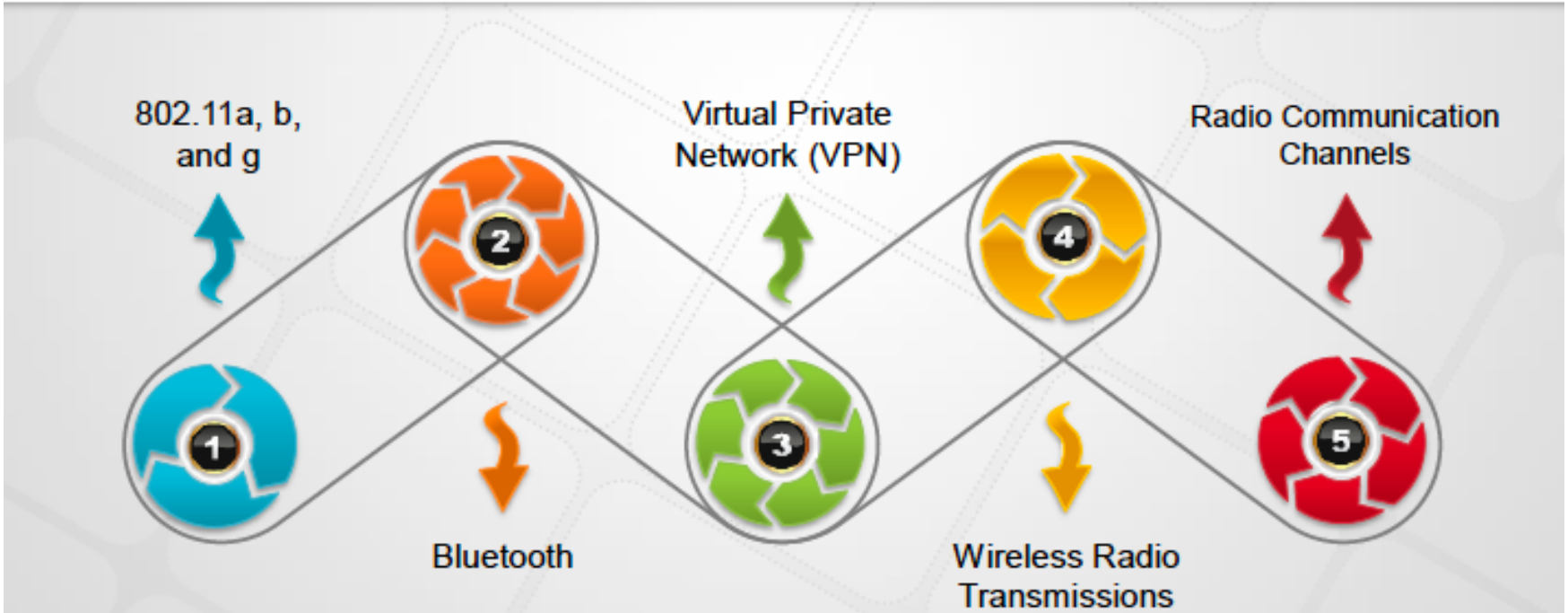
Activity: Network Security Assessment

I	It **scans the network environment** for **identifying vulnerabilities** and helps to improve the enterprise's security policy.
II	It **uncovers network security faults** that can lead to data or equipment being damaged or destroyed by Trojans, denial-of-Service attacks, and other intrusions.
III	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.
IV	It is performed by a team attempting to **break into the network** or servers.

- Aktivitas berikut ini adalah pengujian terhadap keamanan jaringan.

Activity: Wireless/Remote Access Assessment

- Wireless/Remote Access Assessment addresses the **security risks** associated with an increasingly mobile workforce.
- It involves testing following wireless/remote access networks:



❖ Aktifitas berikut ini adalah pengujian terhadap Wireless atau Remote Akses pada jaringan internet, seperti VPN, Wirelesss Radio Transmissions bahkan bluetooth