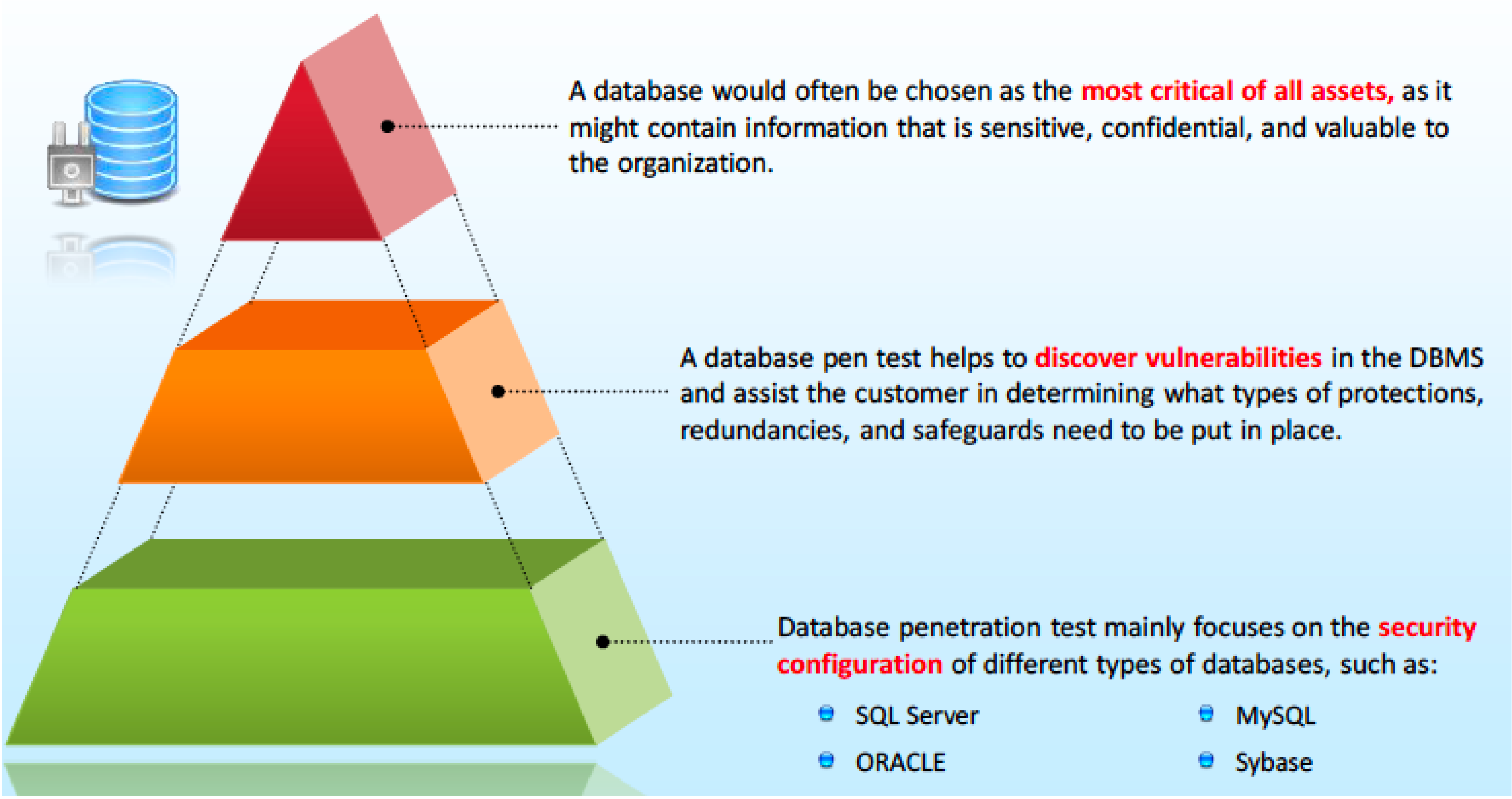
Activity: Database Penetration Testing



A database would often be chosen as the **most critical of all assets,** as it might contain information that is sensitive, confidential, and valuable to the organization.

A database pen test helps to **discover vulnerabilities** in the DBMS and assist the customer in determining what types of protections, redundancies, and safeguards need to be put in place.

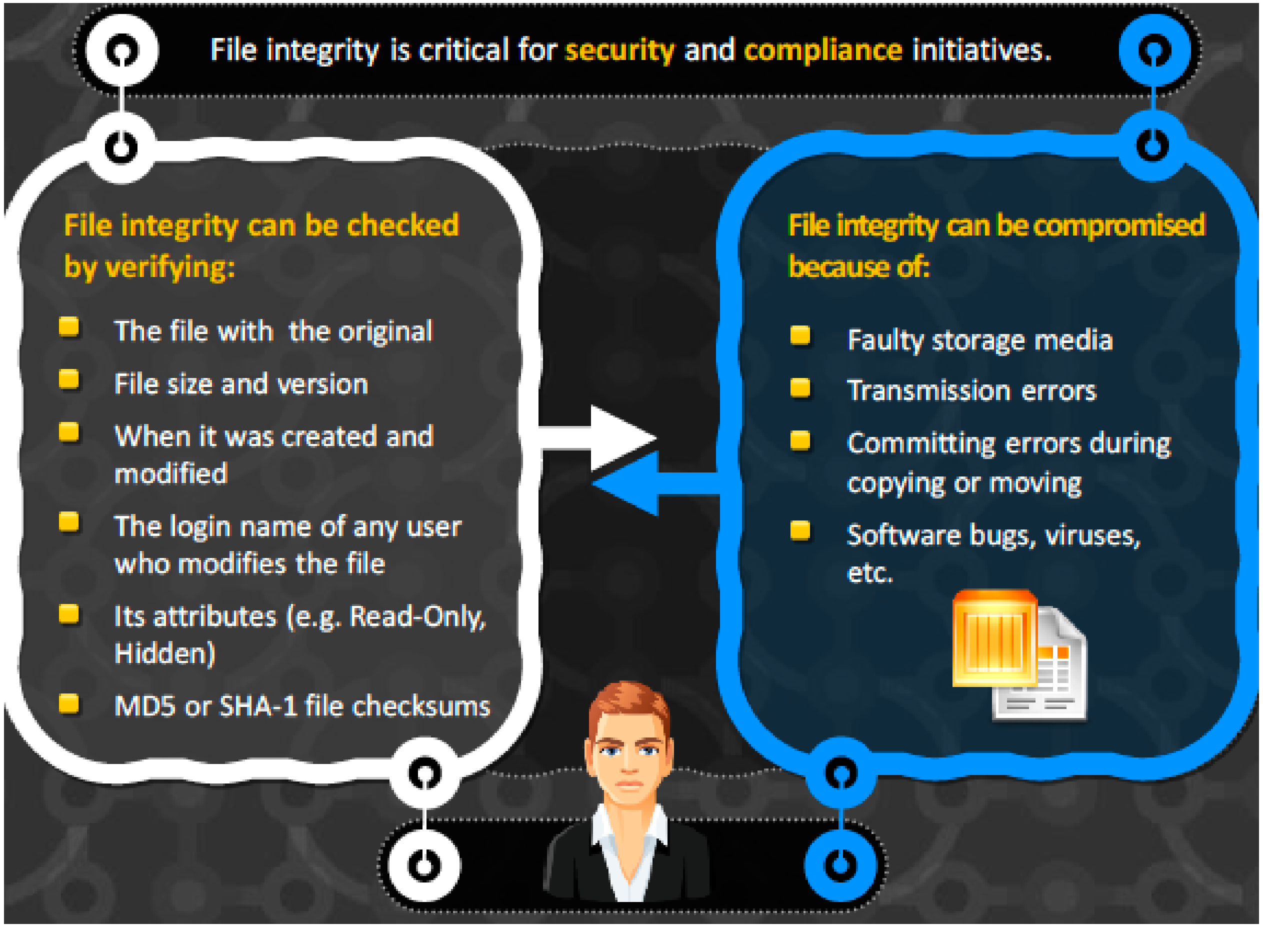
Database penetration test mainly focuses on the **security configuration** of different types of databases, such as:

- SQL Server
- ORACLE
- MySQL
- Sybase

Sumber: © Copyright by EC-Council

❖ Aktifitas berikut ini adalah pengujian terhadap database pada server, pengujian terhadap konfigurasi keamanan database tersebut.

Activity: File Integrity Checking



File integrity is critical for security and compliance initiatives.

File integrity can be checked by verifying:

- The file with the original
- File size and version
- When it was created and modified
- The login name of any user who modifies the file
- Its attributes (e.g. Read-Only, Hidden)
- MD5 or SHA-1 file checksums

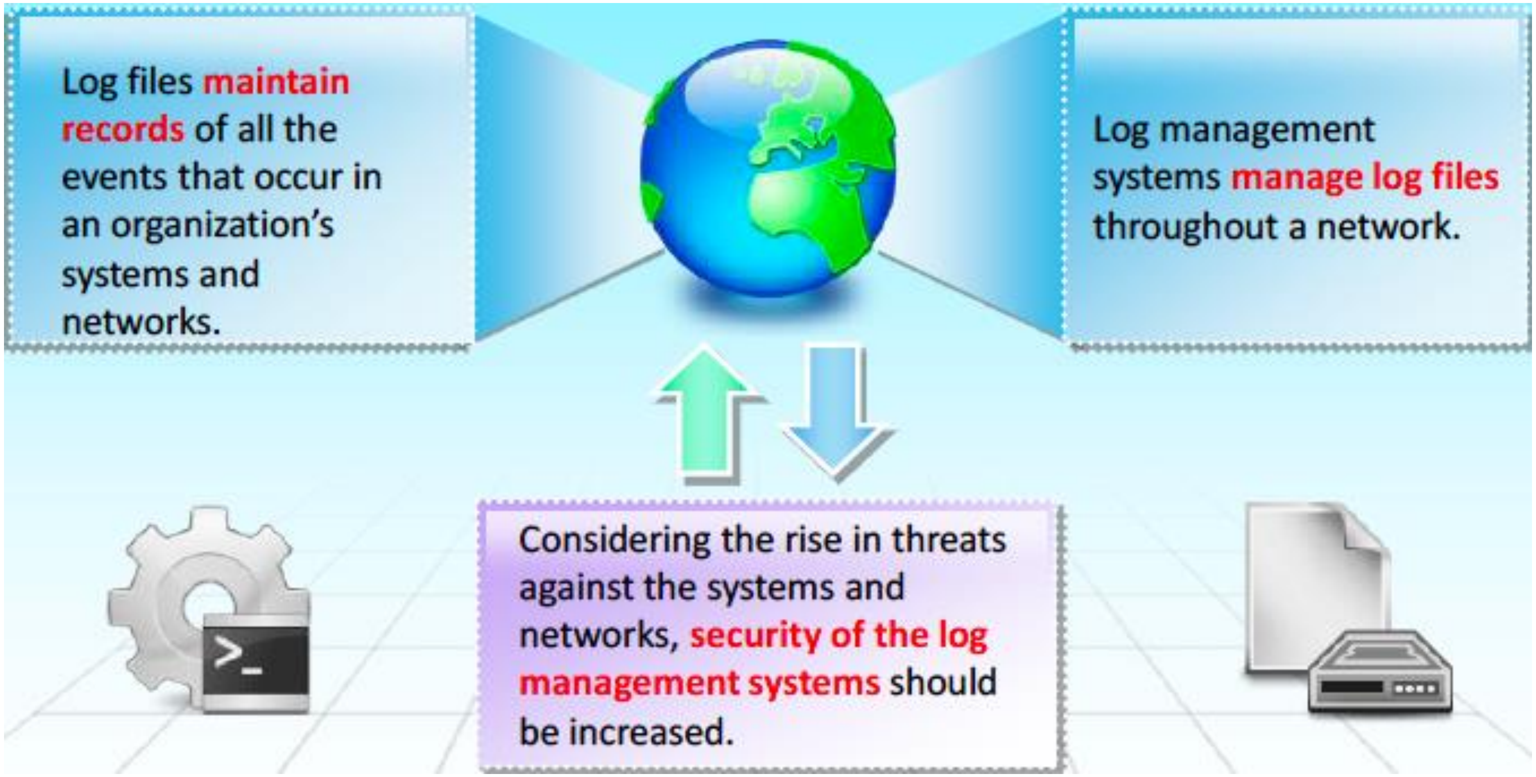
File integrity can be compromised because of:

- Faulty storage media
- Transmission errors
- Committing errors during copying or moving
- Software bugs, viruses, etc.

Sumber: © Copyright by EC-Council

❖ Aktifitas berikut ini adalah pengecekan terhadap integritas file atau keabsahan suatu file.

Activity: Log Management Penetration Testing



Log files **maintain records** of all the events that occur in an organization's systems and networks.

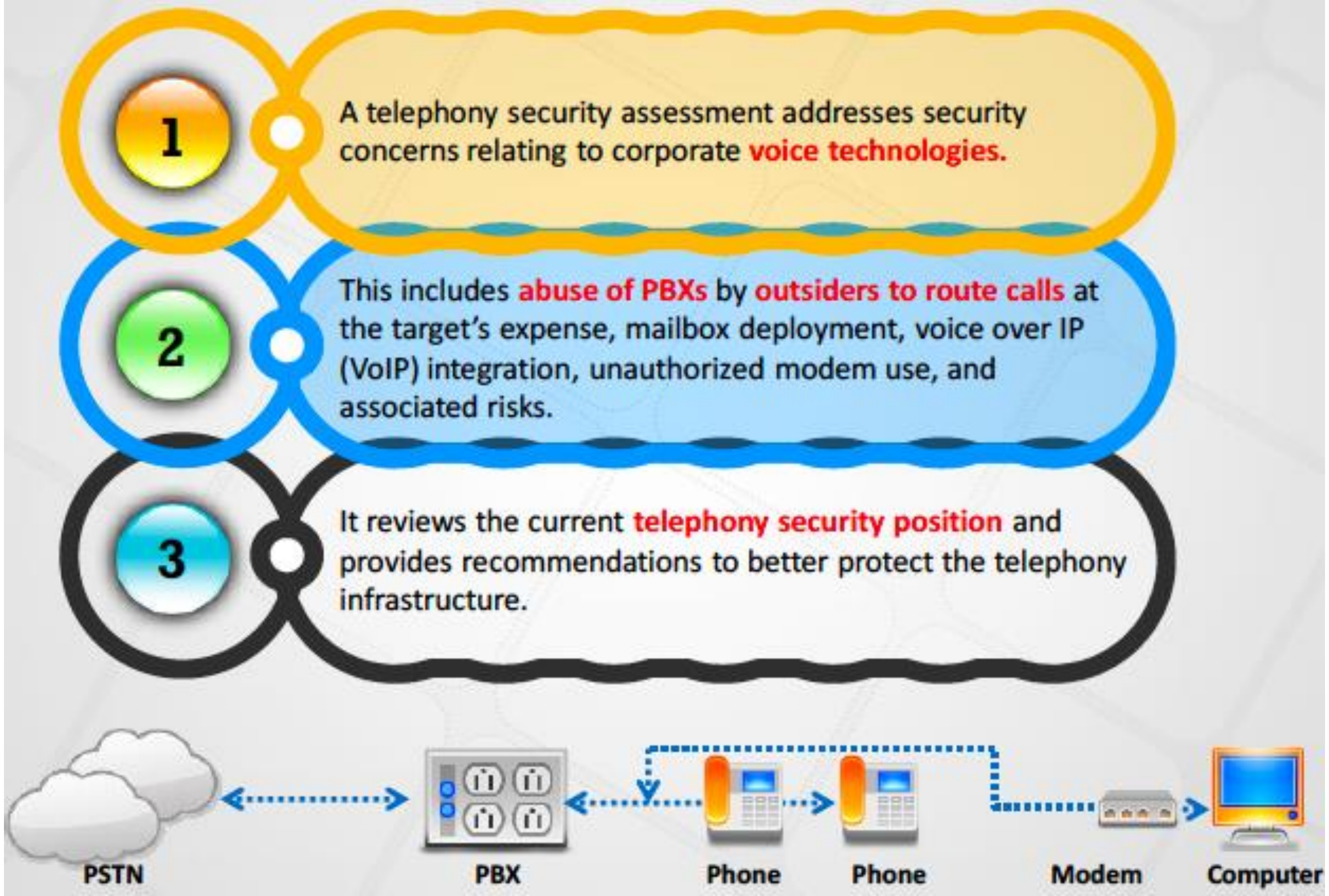
Log management systems **manage log files** throughout a network.

Considering the rise in threats against the systems and networks, **security of the log management systems** should be increased.

Sumber: © Copyright by EC-Council

- ❖ Aktifitas berikut ini adalah Pengujian terhadap semua file yang tercatat didalam sebuah sistem atau server.

Activity: Telephony Security Assessment



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

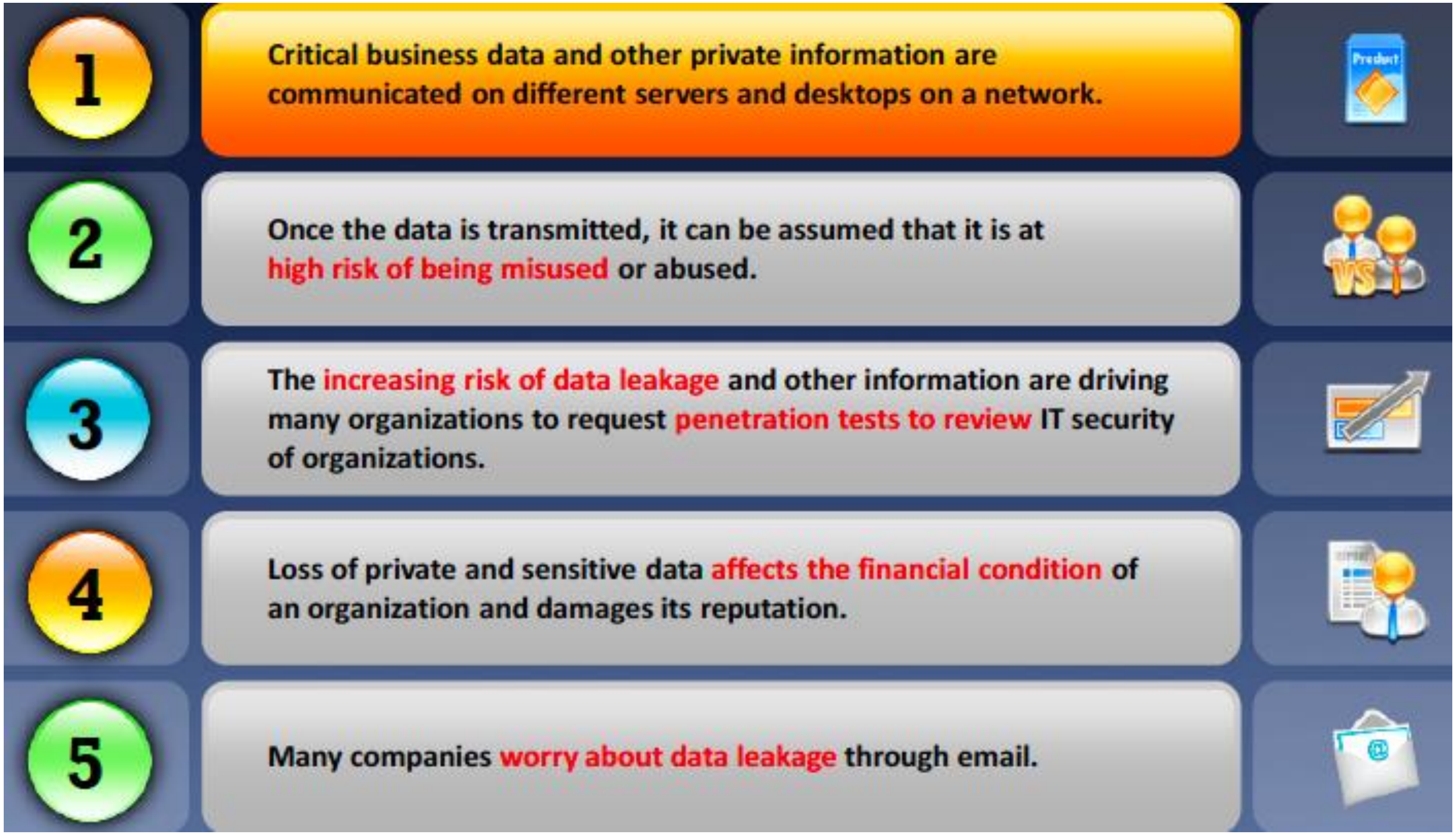
2 This includes abuse of PBXs by outsiders to route calls at the target's expense, mailbox deployment, voice over IP (VoIP) integration, unauthorized modem use, and associated risks.

3 It reviews the current telephony security position and provides recommendations to better protect the telephony infrastructure.

Sumber: © Copyright by EC-Council

- ❖ Aktivitas berikut ini adalah pengujian terhadap keamanan jaringan telepon yang terhubung dengan VoIP.

Activity: Data Leakage Penetration Testing

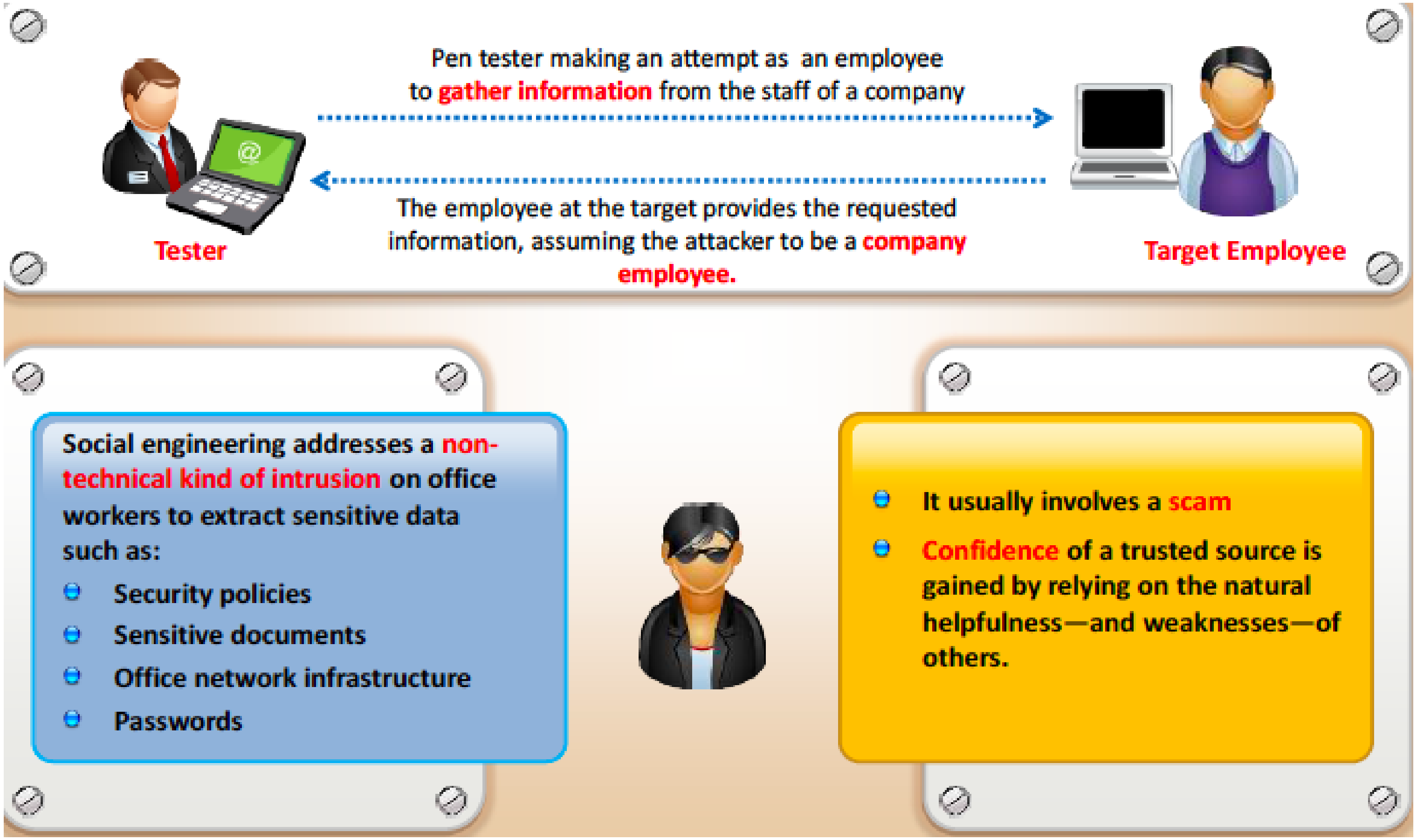


1. Critical business data and other private information are communicated on different servers and desktops on a network.
2. Once the data is transmitted, it can be assumed that it is at high risk of being misused or abused.
3. The increasing risk of data leakage and other information are driving many organizations to request penetration tests to review IT security of organizations.
4. Loss of private and sensitive data affects the financial condition of an organization and damages its reputation.
5. Many companies worry about data leakage through email.

Sumber: © Copyright by EC-Council

- Aktivitas berikut adalah melakukan tes pada jaringan apakah ada kebocoran data yang terjadi pada sebuah server maupun desktop.

Activity: Social Engineering



Pen tester making an attempt as an employee to **gather information** from the staff of a company

The employee at the target provides the requested information, assuming the attacker to be a **company employee.**

Social engineering addresses a **non-technical kind of intrusion** on office workers to extract sensitive data such as:

- Security policies
- Sensitive documents
- Office network infrastructure
- Passwords

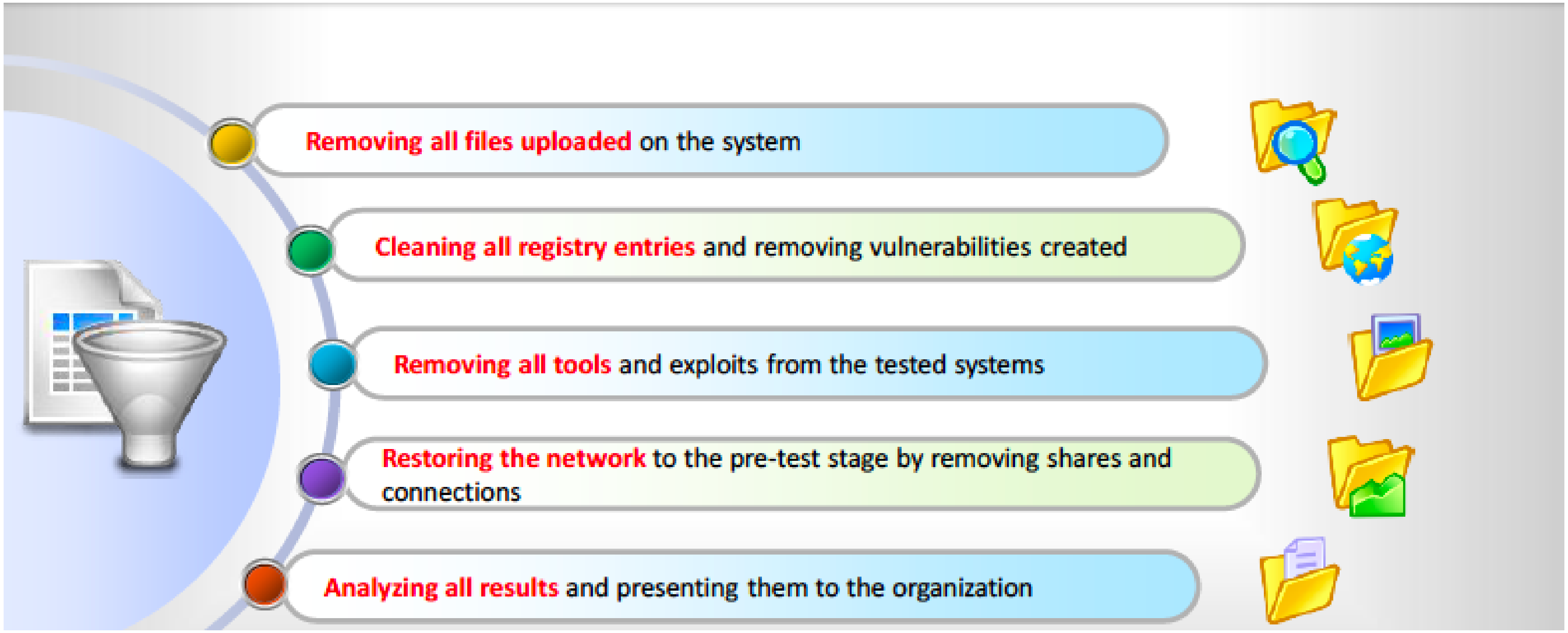
- It usually involves a **scam**
- **Confidence** of a trusted source is gained by relying on the natural helpfulness—and weaknesses—of others.

Sumber: © Copyright by EC-Council

- Aktivitas berikut ini adalah melakukan pengumpulan informasi dari salah satu staf pada perusahaan yang akan dilakukan pentes, biasanya social engineering bersifat tanya jawab yang berkaitan dengan kebijakan kemanan, sensifitas dokumen sampai password

Post-Attack Phase and Activities

This phase is critical to any penetration test, as it is the responsibility of the tester to restore systems to a pre-test state.

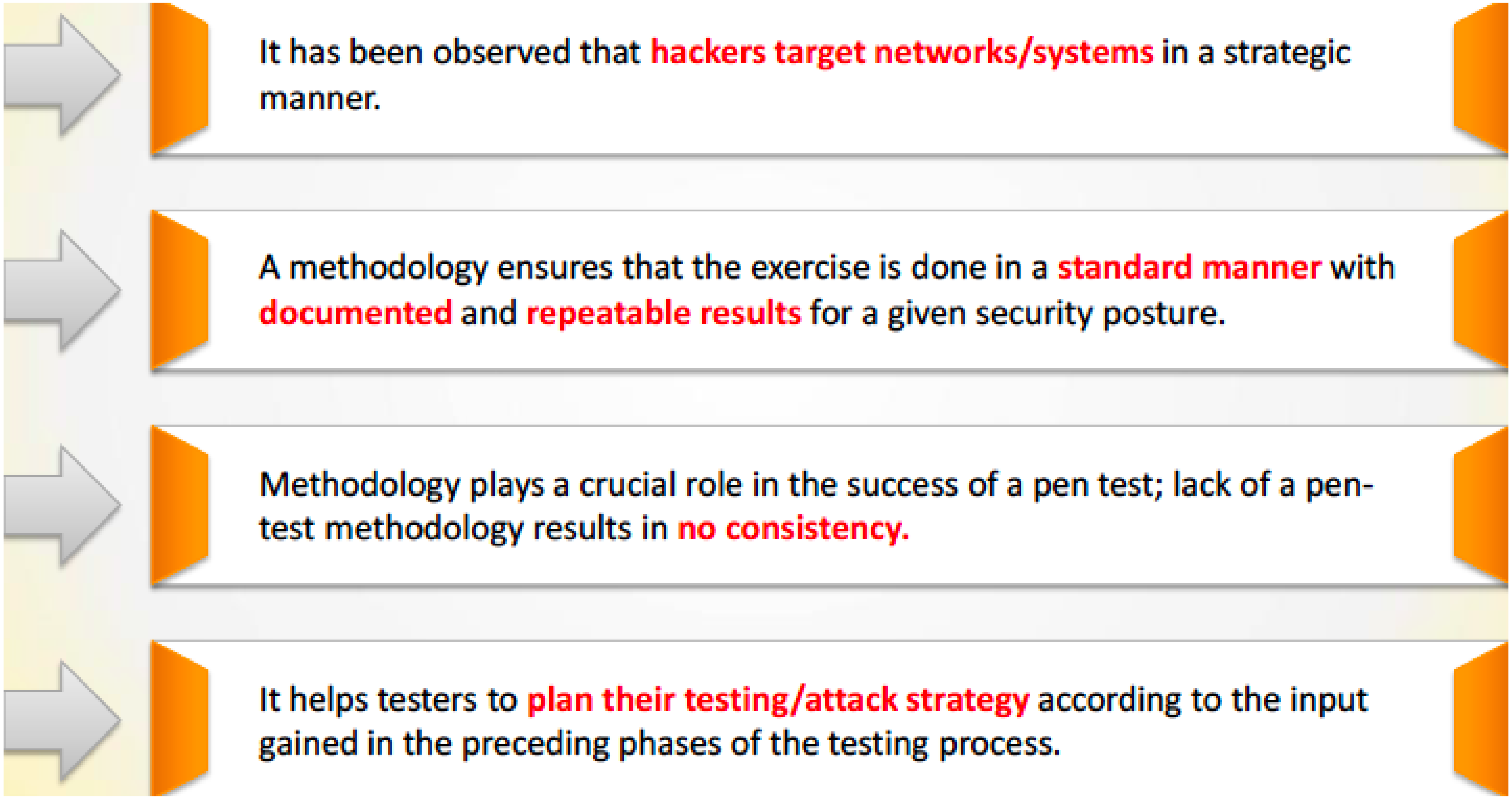


- Removing all files uploaded on the system
- Cleaning all registry entries and removing vulnerabilities created
- Removing all tools and exploits from the tested systems
- Restoring the network to the pre-test stage by removing shares and connections
- Analyzing all results and presenting them to the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

Sumber: © Copyright by EC-Council

❖ Tahap ini adalah tahap penting pada suatu penetration tes, karena pentester harus bertanggung jawab untuk melakukan pengembalian sistem seperti semula pada saat sebelum melakukan pengujian.

Need for a Methodology



It has been observed that **hackers target networks/systems** in a strategic manner.

A methodology ensures that the exercise is done in a **standard manner** with **documented** and **repeatable results** for a given security posture.

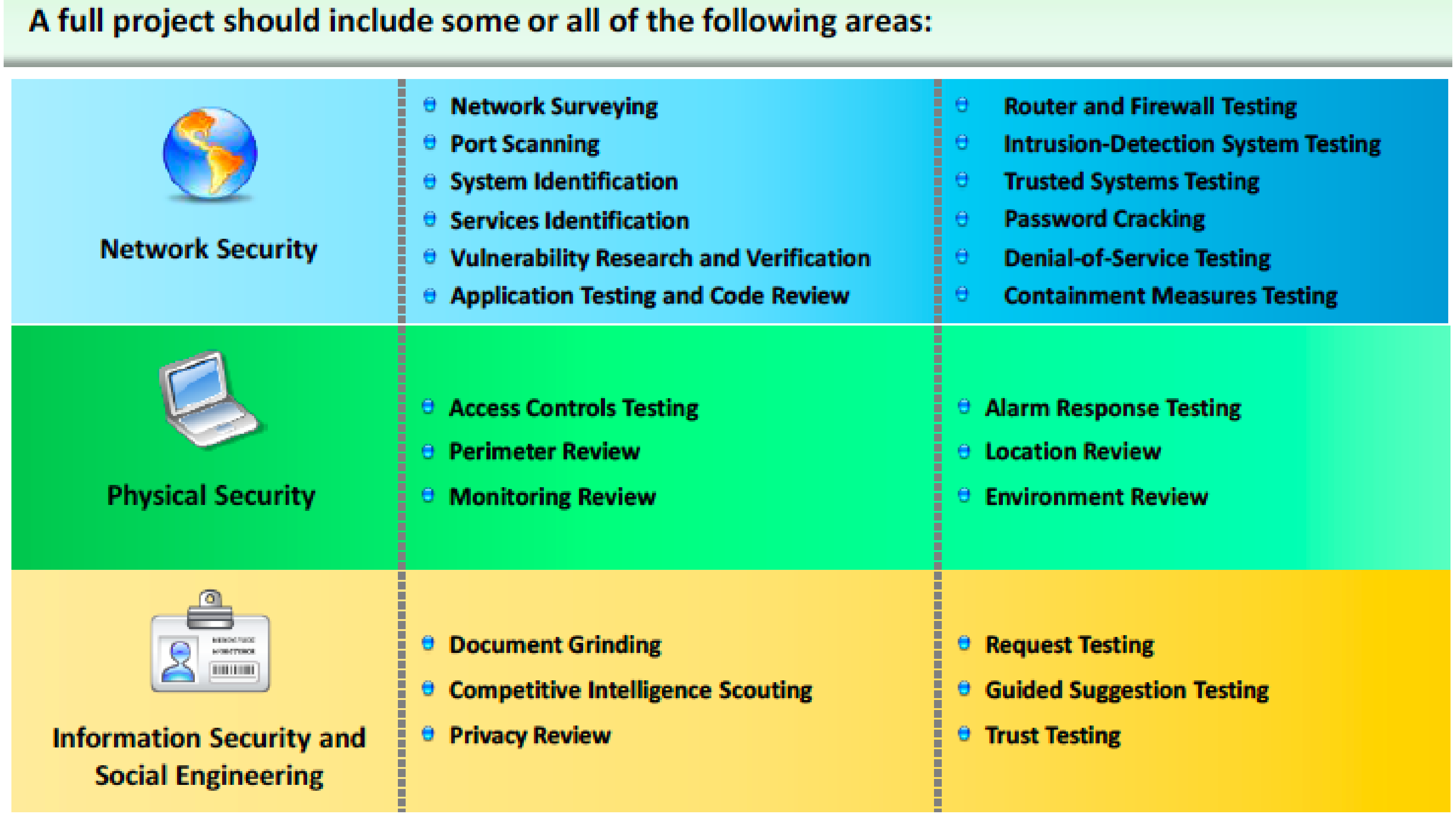
Methodology plays a crucial role in the success of a pen test; lack of a pen-test methodology results in **no consistency.**

It helps testers to **plan their testing/attack strategy** according to the input gained in the preceding phases of the testing process.

Sumber: © Copyright by EC-Council

- Perlunya suatu methodologi yaitu untuk memastikan semua pengujian dilakukan dengan baik dan memiliki cara standar dengan didokumentasikan dan hasil yang berulang untuk postur keamanan yang diberikan.

Penetration Testing Methodology



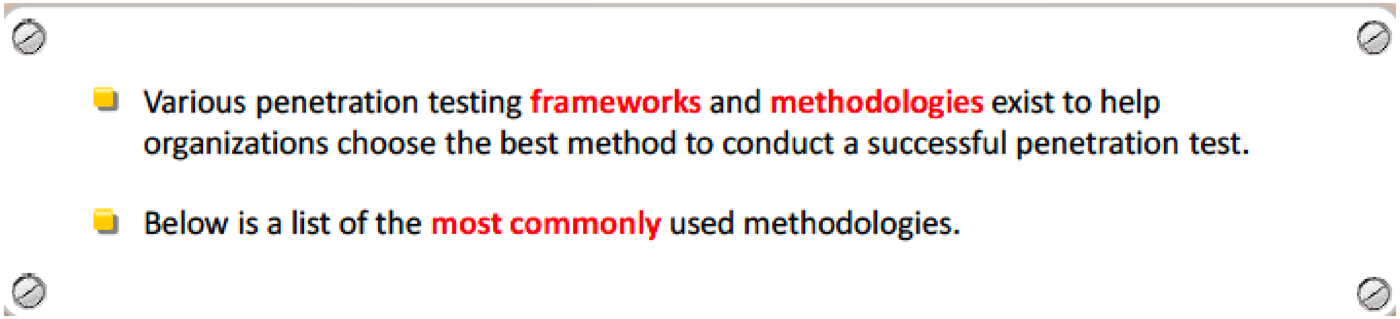
A full project should include some or all of the following areas:

Network Security	- Network Surveying - Port Scanning - System Identification - Services Identification - Vulnerability Research and Verification - Application Testing and Code Review	- Router and Firewall Testing - Intrusion-Detection System Testing - Trusted Systems Testing - Password Cracking - Denial-of-Service Testing - Containment Measures Testing
Physical Security	- Access Controls Testing - Perimeter Review - Monitoring Review	- Alarm Response Testing - Location Review - Environment Review
Information Security and Social Engineering	- Document Grinding - Competitive Intelligence Scouting - Privacy Review	- Request Testing - Guided Suggestion Testing - Trust Testing

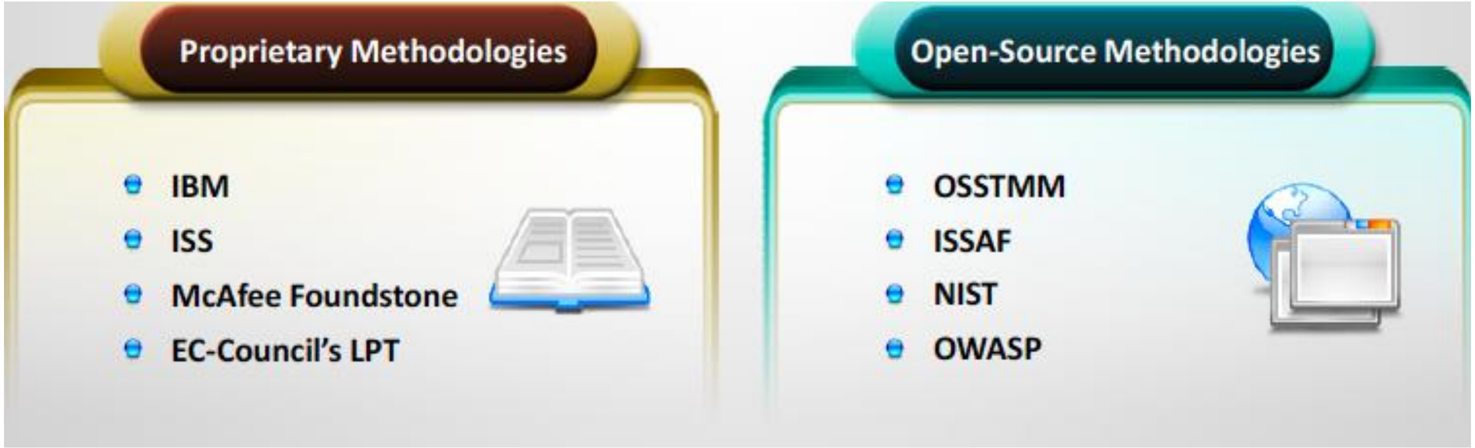
Sumber: © Copyright by EC-Council

❖ Metodologi Penetration Test meliputi; Network Security, Physical Security dan Information Security and Social Engineering.

Penetration Testing Methodologies



- Various penetration testing frameworks and methodologies exist to help organizations choose the best method to conduct a successful penetration test.
- Below is a list of the most commonly used methodologies.



Proprietary Methodologies

- IBM
- ISS
- McAfee Foundstone
- EC-Council's LPT

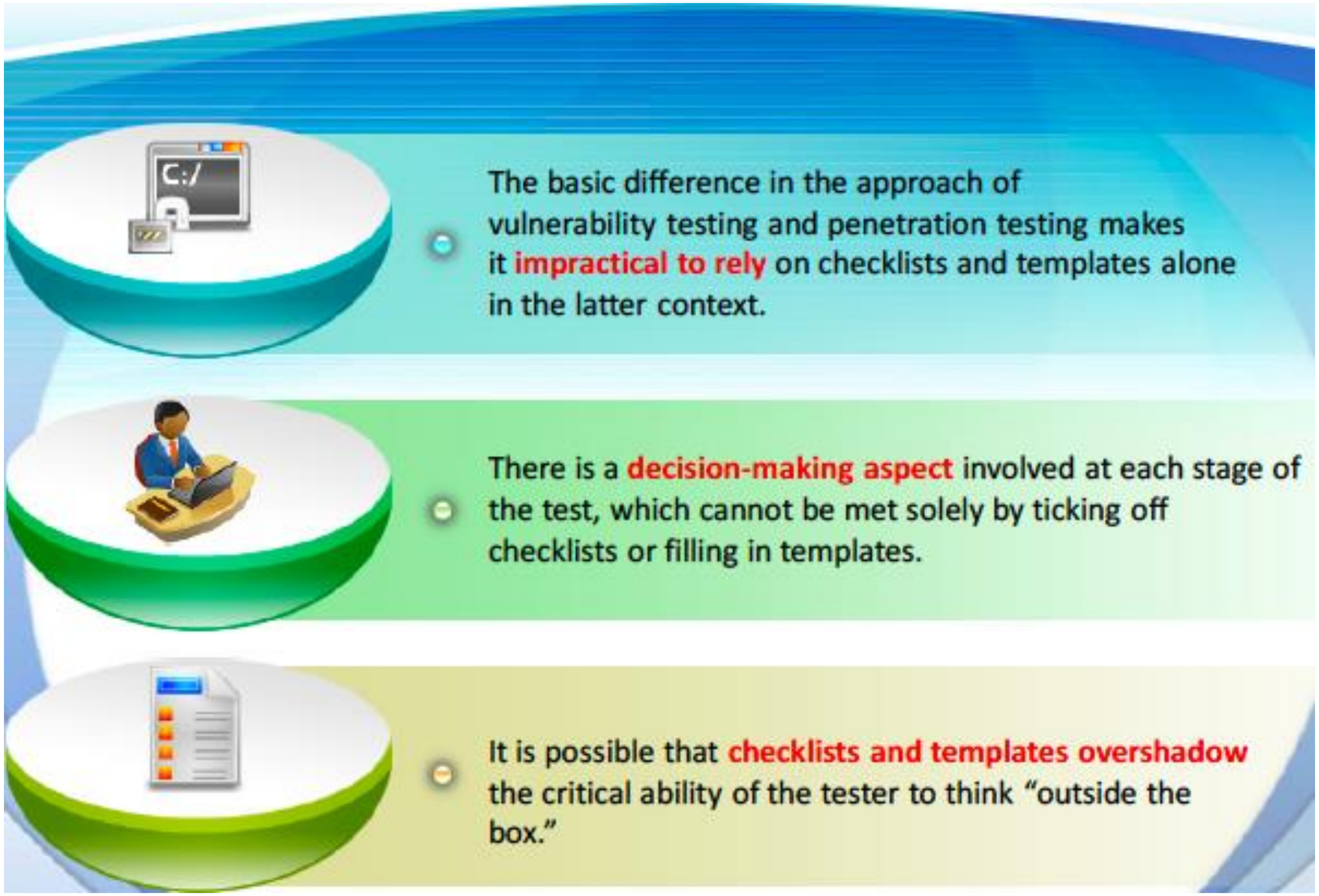
Open-Source Methodologies

- OSSTMM
- ISSAF
- NIST
- OWASP

Sumber: © Copyright by EC-Council

❖ Ada berbagai macam cara melakukan penetration test yaitu Proprietary Methodologies dan Open-Source Methodologies.

Reliance on Checklists and Template



The basic difference in the approach of vulnerability testing and penetration testing makes it impractical to rely on checklists and templates alone in the latter context.

There is a decision-making aspect involved at each stage of the test, which cannot be met solely by ticking off checklists or filling in templates.

It is possible that checklists and templates overshadow the critical ability of the tester to think "outside the box."

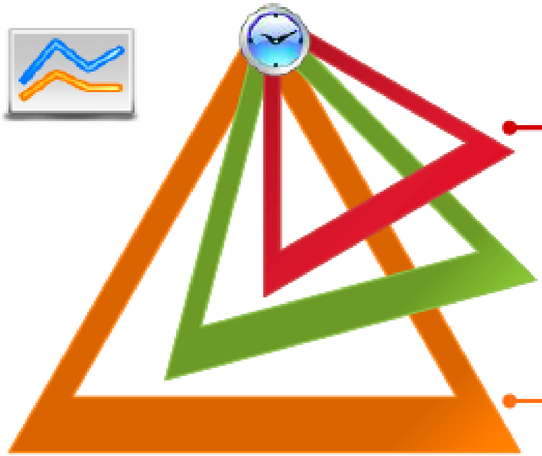
Sumber: © Copyright by EC-Council

- ❖ Perbedaan mendasar pada pendekatan vulnerability analysis dan penetration test yaitu praktis nya sangat mengandalkan daftar dan template.

Penetration Testing Strategies

Operational Strategies for Security Testing

- The object of performing a security test is to **maximize** the benefit to the organization.
- The decisions of what to test during the **implementation phase** depend on the system.
- The **prioritization process** should be considered for the interconnectivity of the systems.
- The types and **frequency of penetration testing** during the operational and maintenance phases involve a prioritization process based on:



Security category of the information system

Cost of conducting tests for each test type

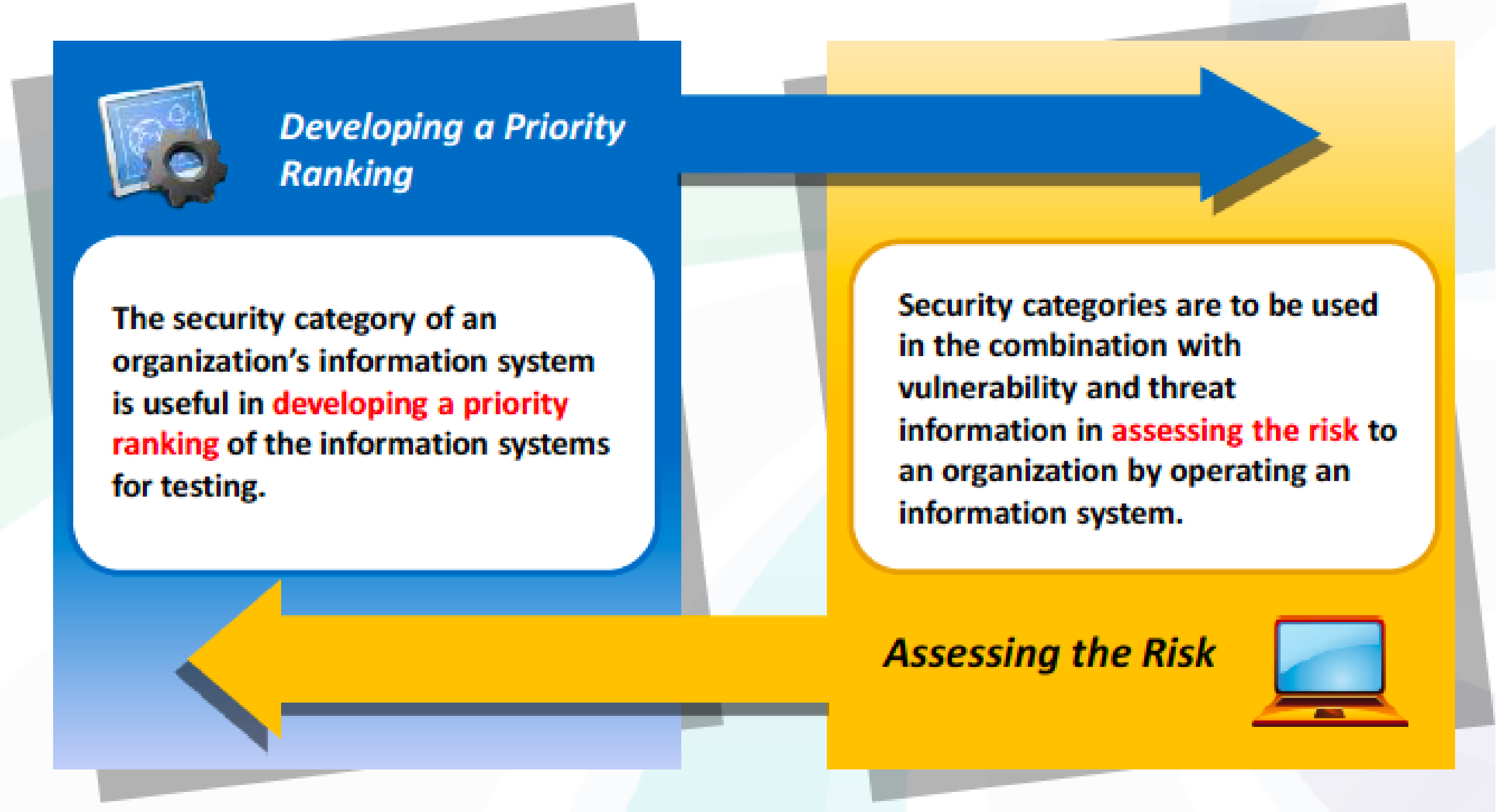
Identifying benefits to the organization's system

Sumber: © Copyright by EC-Council

❖ Strategi operasional untuk pengujian keamanan memprioritaskan proses berdasarkan, Katagori Keamanan pada sistem informasi, Biaya test untuk melakukan semua jenis test, dan mengidentifikasi manfaat bagi sistem.

Cyber Computer Security

Identifying Benefits of Each Test Type



Developing a Priority Ranking

The security category of an organization's information system is useful in developing a priority ranking of the information systems for testing.

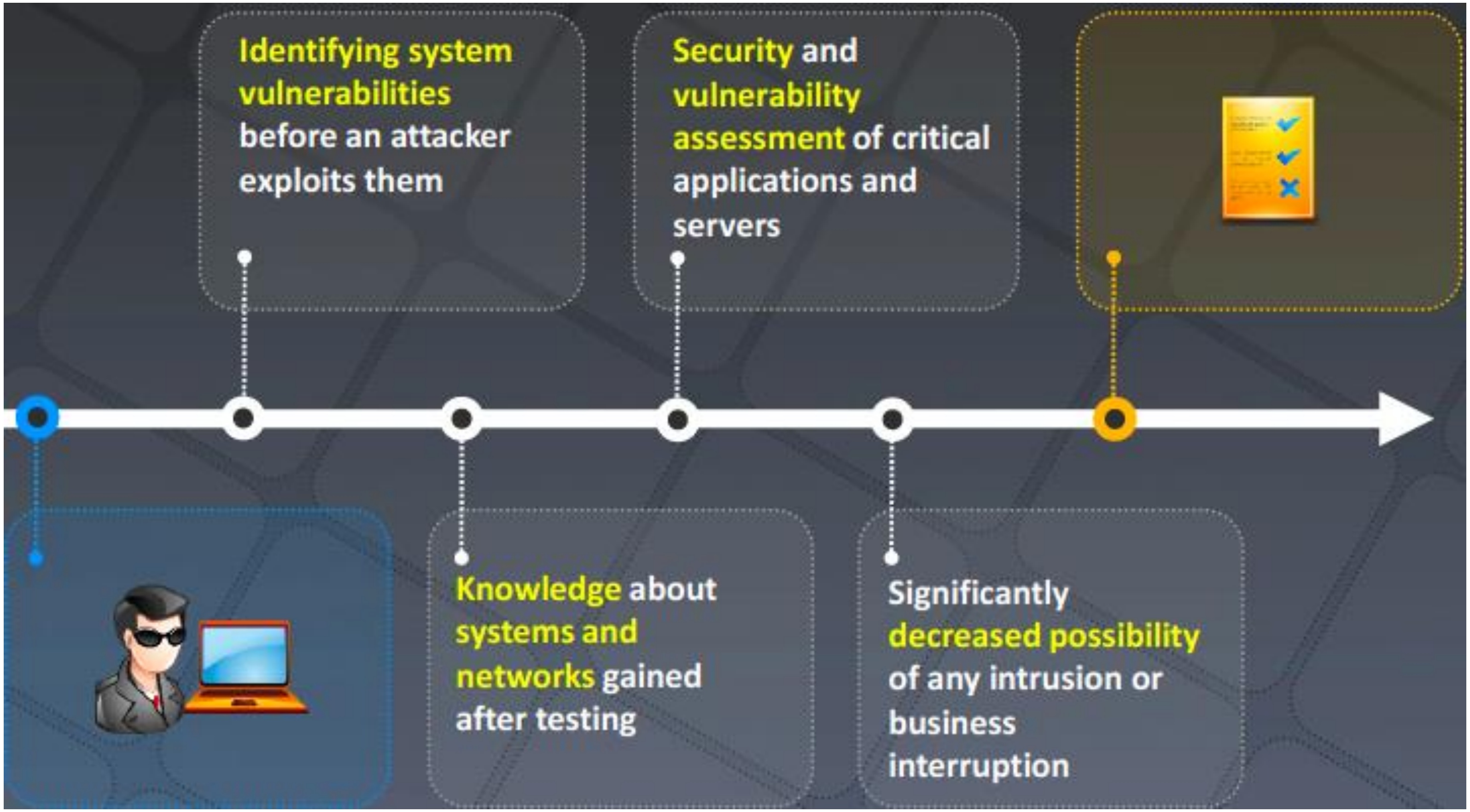
Security categories are to be used in the combination with vulnerability and threat information in assessing the risk to an organization by operating an information system.

Assessing the Risk

Sumber: © Copyright by EC-Council

- ❖ Mengidentifikasi manfaat dari tipe pengujian yang lain yaitu Developing a priority rangking dan Assessing the Risk.

Prioritizing Systems for Testing



Identifying system vulnerabilities before an attacker exploits them

Security and vulnerability assessment of critical applications and servers

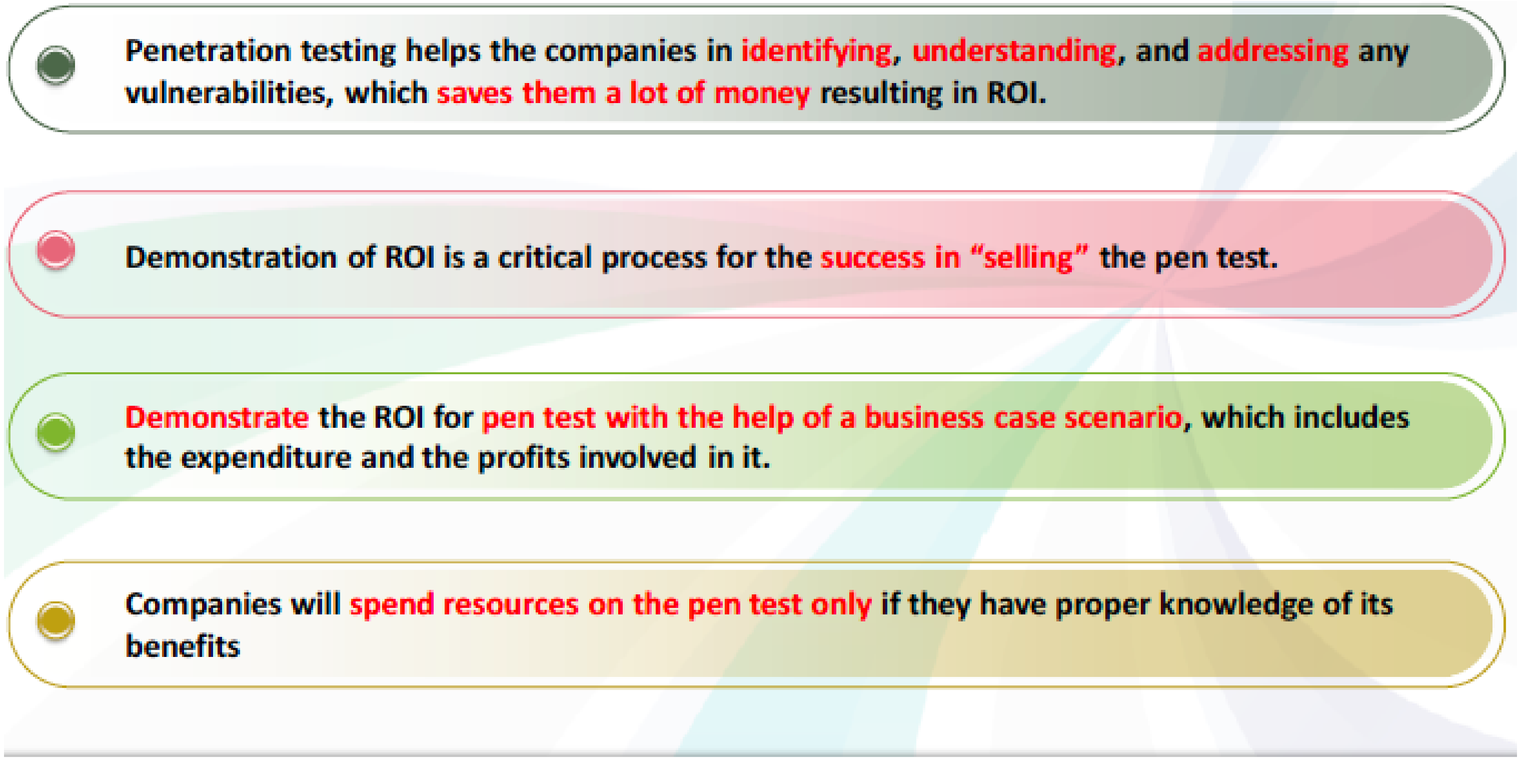
Knowledge about systems and networks gained after testing

Significantly decreased possibility of any intrusion or business interruption

Sumber: © Copyright by EC-Council

❖ Memprioritaskan sistem yang akan diuji; mengidentifikasi kerentanan sistem sebelum di serang, pengetahuan tentang sistem dan jaringan yang diperoleh dari pengujian.

ROI for Penetration Testing



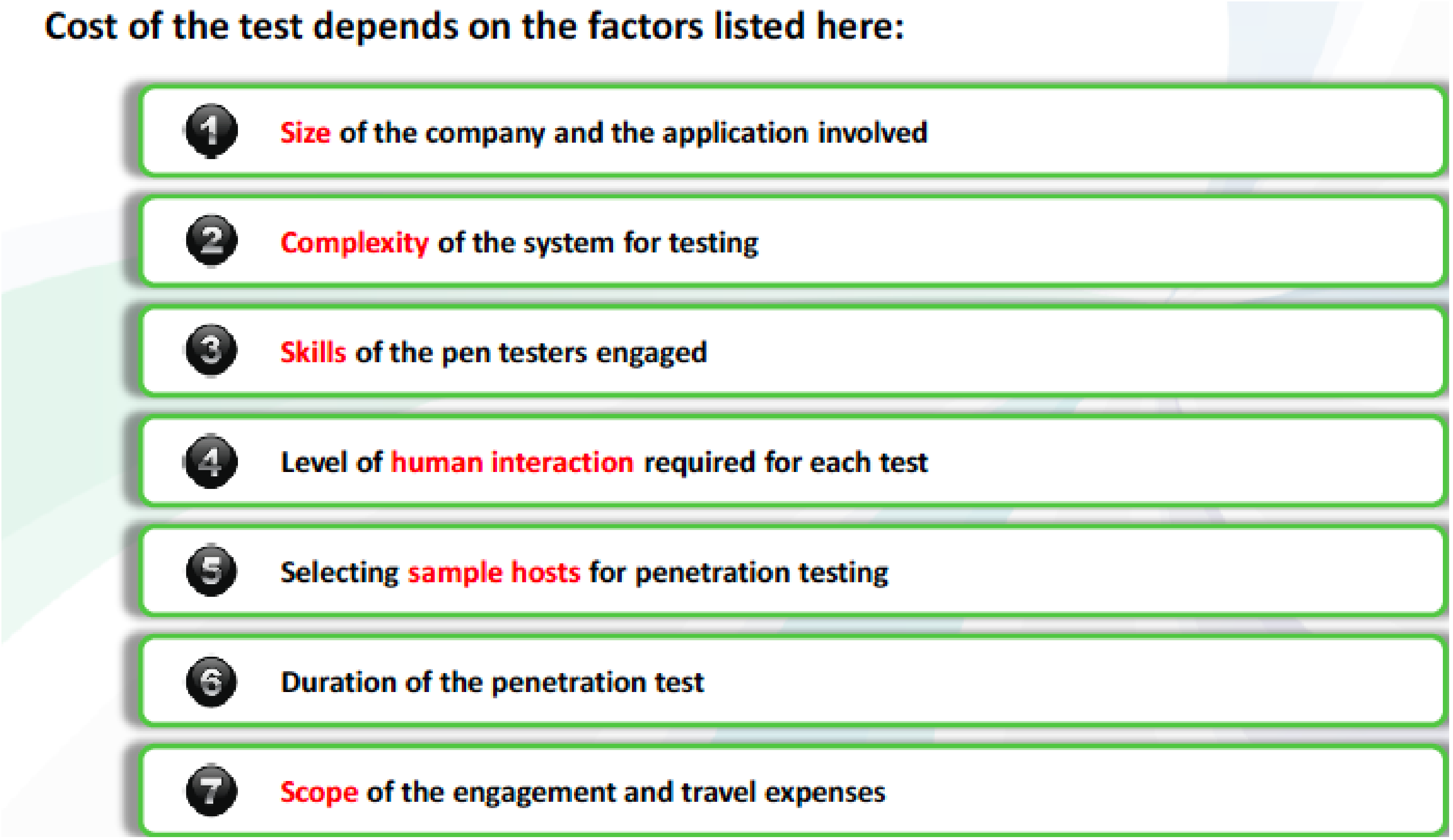
- Penetration testing helps the companies in identifying, understanding, and addressing any vulnerabilities, which saves them a lot of money resulting in ROI.
- Demonstration of ROI is a critical process for the success in “selling” the pen test.
- Demonstrate the ROI for pen test with the help of a business case scenario, which includes the expenditure and the profits involved in it.
- Companies will spend resources on the pen test only if they have proper knowledge of its benefits

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

Sumber: © Copyright by EC-Council

❖ Penetration testing membantu organisasi perusahaan untuk mengidentifikasi, memahami dan menemukan kelemahan, yang dapat menghemat pengeluaran dari hasil ROI.

Determining Cost of Each Test Type



Cost of the test depends on the factors listed here:

1. Size of the company and the application involved
2. Complexity of the system for testing
3. Skills of the pen testers engaged
4. Level of human interaction required for each test
5. Selecting sample hosts for penetration testing
6. Duration of the penetration test
7. Scope of the engagement and travel expenses

Sumber: © Copyright by EC-Council

- Menentukan biaya dari setiap jenis pengujian dengan beberapa faktor; ukuran, kesulitan, kemampuan, intaraksi manusia, dan jangkauan.

Penetration Testing Best Practices

It is vital to **maintain a log of all the activities carried out** and the results obtained.

Ensure that all **work is time-stamped** and **communicated** to the proper person in the organization, as per the rules of engagement.

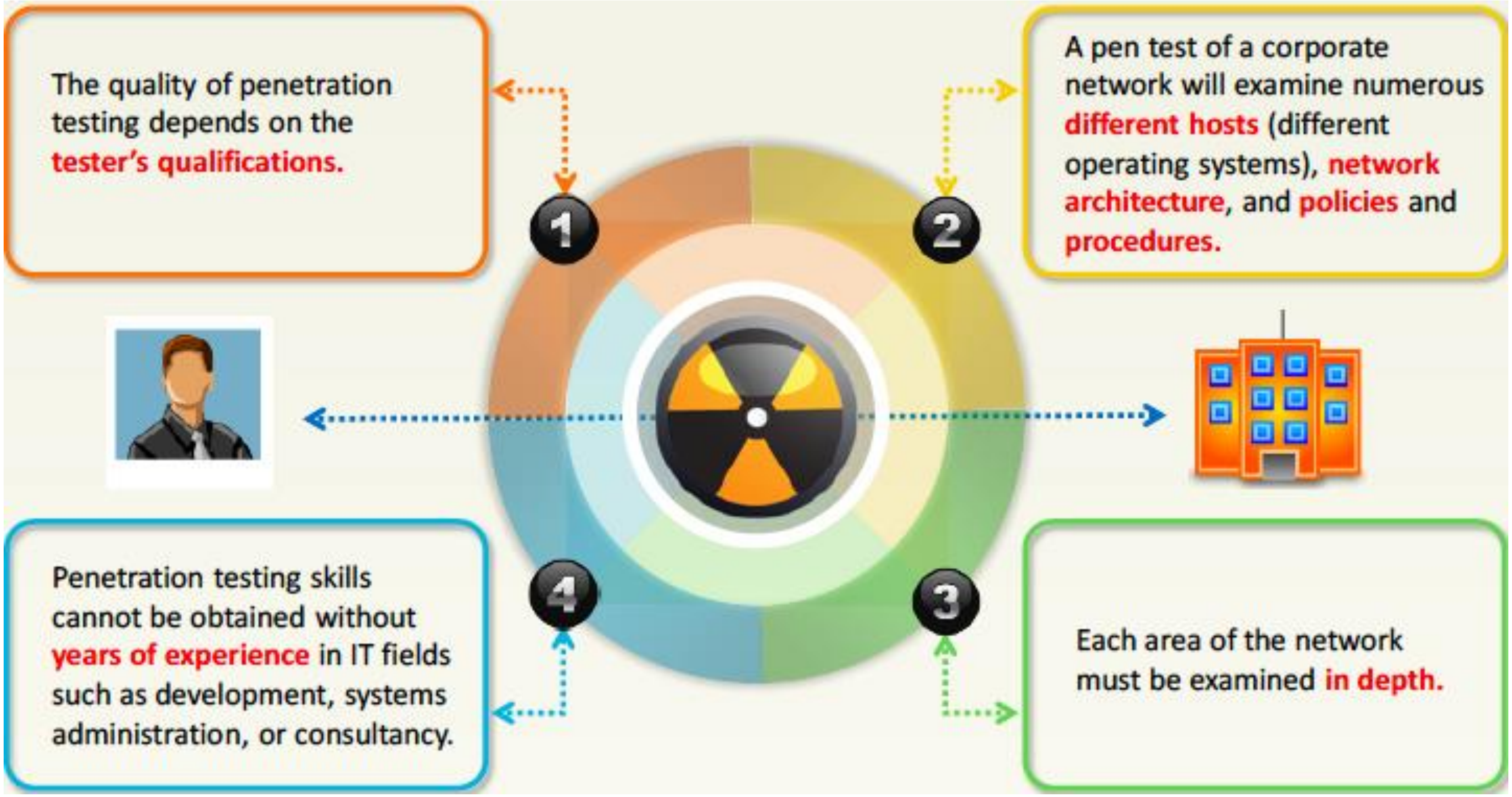
While planning an attack strategy, make sure that you are able to **reason out your strategic choices** to the input or output obtained from the pre-attack phase.

Look at your log and **start** either developing the tools you need or acquiring them according to need, to **help reduce the attack area** that might be inadvertently passed over.

Sumber: © Copyright by EC-Council

- ❖ Penetration Testing best practice

Penetration Testing Consultants



The quality of penetration testing depends on the tester's qualifications.

A pen test of a corporate network will examine numerous different hosts (different operating systems), network architecture, and policies and procedures.

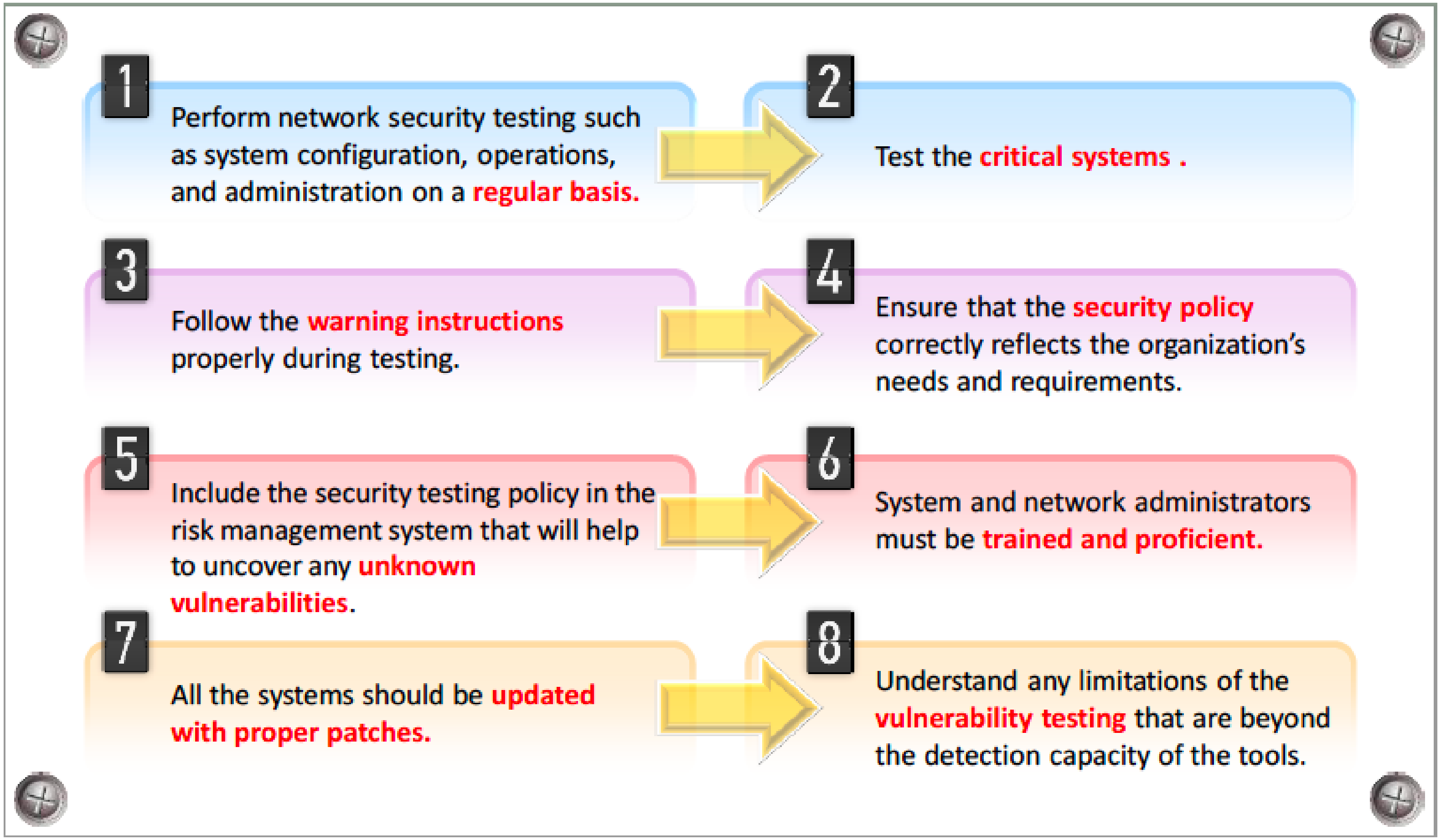
Each area of the network must be examined in depth.

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

Sumber: © Copyright by EC-Council

- Kualitas dari Penetration Testing tergantung pada keahlian penguji/tester.

Guidelines for Security Checking



1. Perform network security testing such as system configuration, operations, and administration on a regular basis.

2. Test the critical systems .

3. Follow the warning instructions properly during testing.

4. Ensure that the security policy correctly reflects the organization's needs and requirements.

5. Include the security testing policy in the risk management system that will help to uncover any unknown vulnerabilities.

6. System and network administrators must be trained and proficient.

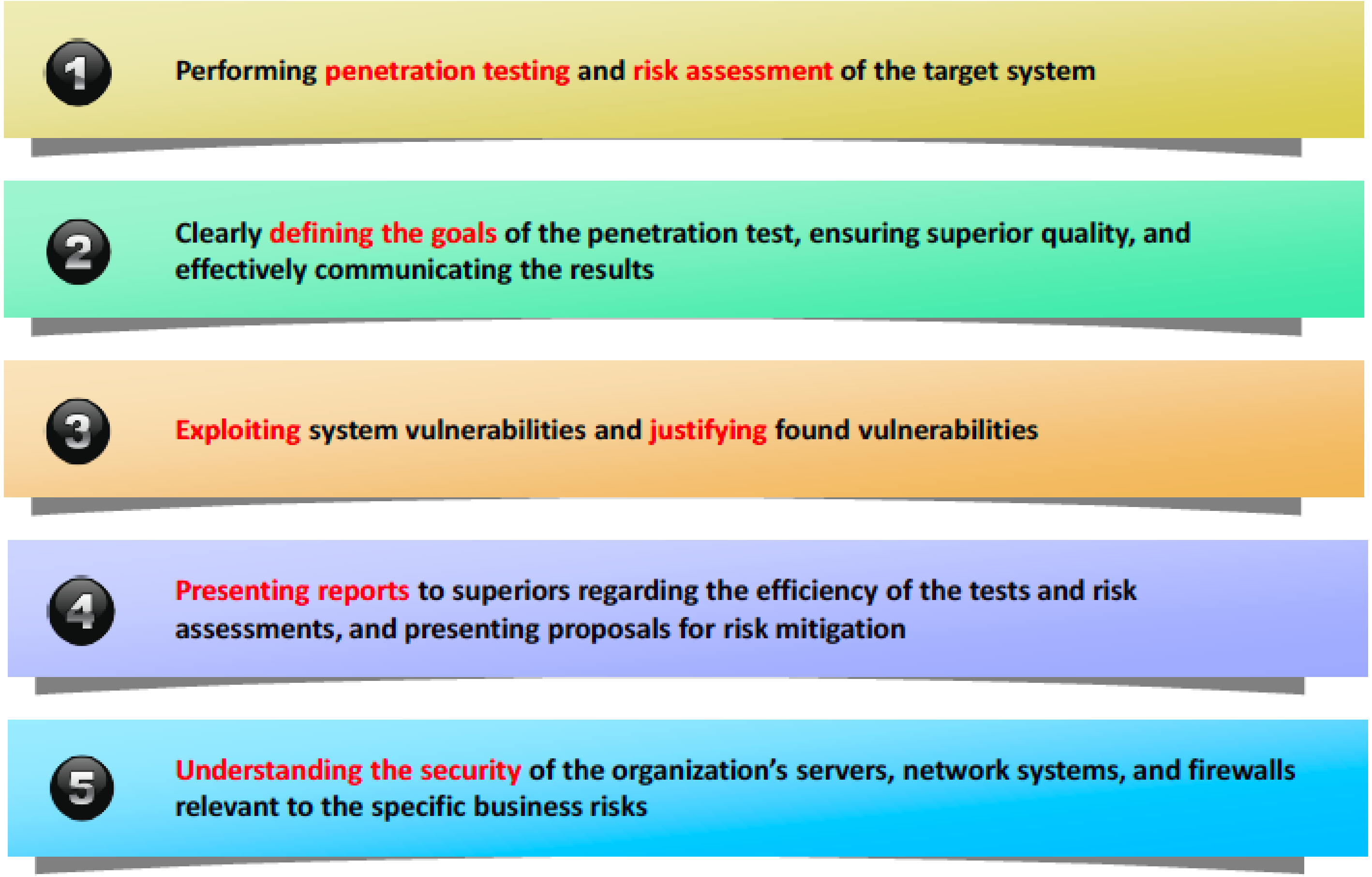
7. All the systems should be updated with proper patches.

8. Understand any limitations of the vulnerability testing that are beyond the detection capacity of the tools.

Sumber: © Copyright by EC-Council

❖ Pedoman untuk Pemeriksaan Keamanan; secara teratur, sistem kritis, instruksi peringatan, kebijakan keamanan, kelemahan yang tidak diketahui, terlatih dan mahir, memperbarui dengan patch baru, pengujian pada kelemahan.

Responsibilities of the Penetration Test

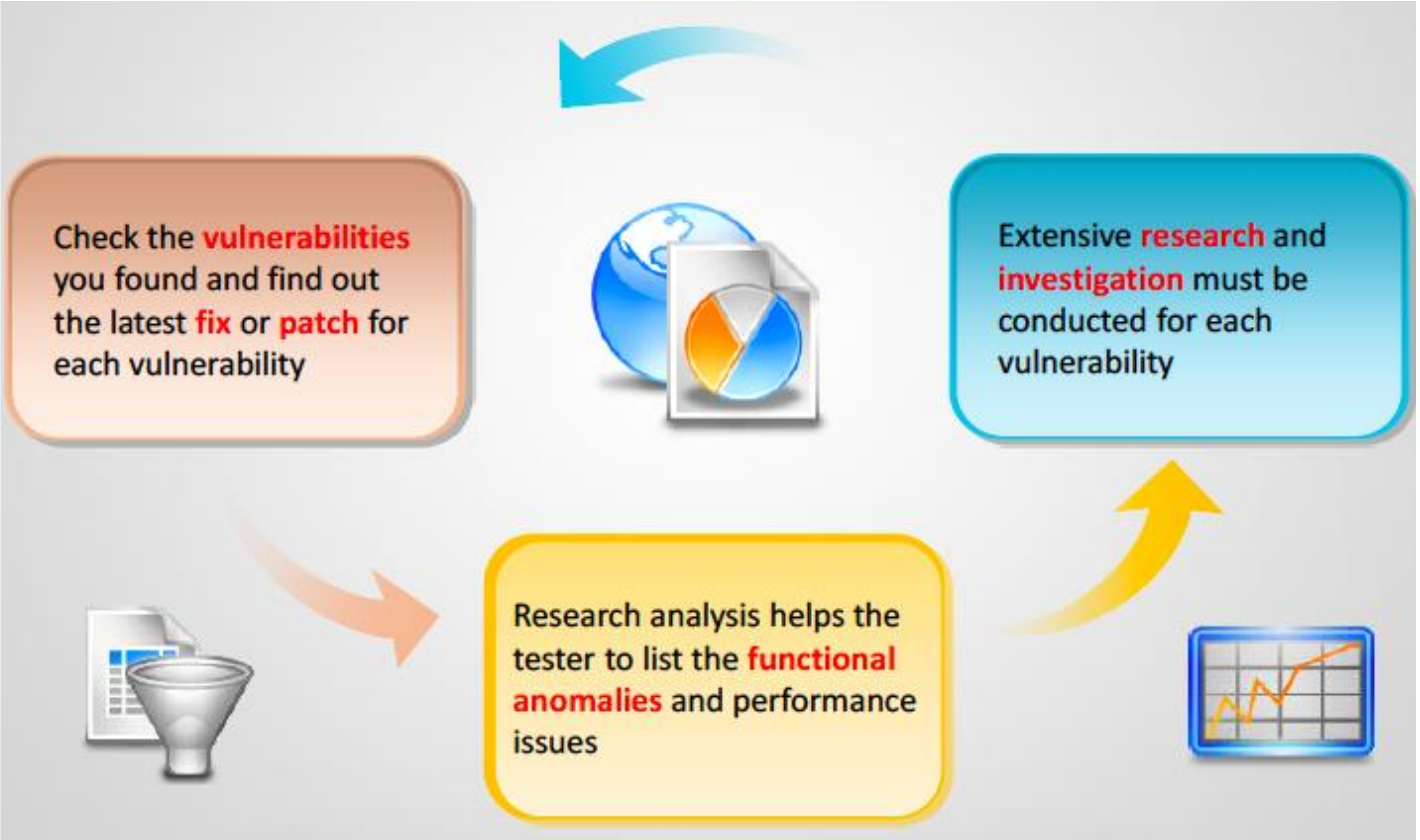


1. Performing penetration testing and risk assessment of the target system
2. Clearly defining the goals of the penetration test, ensuring superior quality, and effectively communicating the results
3. Exploiting system vulnerabilities and justifying found vulnerabilities
4. Presenting reports to superiors regarding the efficiency of the tests and risk assessments, and presenting proposals for risk mitigation
5. Understanding the security of the organization's servers, network systems, and firewalls relevant to the specific business risks

Sumber: © Copyright by EC-Council

❖ Pertanggungjawaban dari penetration test; memahami keamanan dari manajemen organisasi server, sistem jaringan dan firewall yang memiliki hubugan penting dengan resiko bisnis perusahaan tersebut.

Research Analysis



Check the vulnerabilities you found and find out the latest fix or patch for each vulnerability

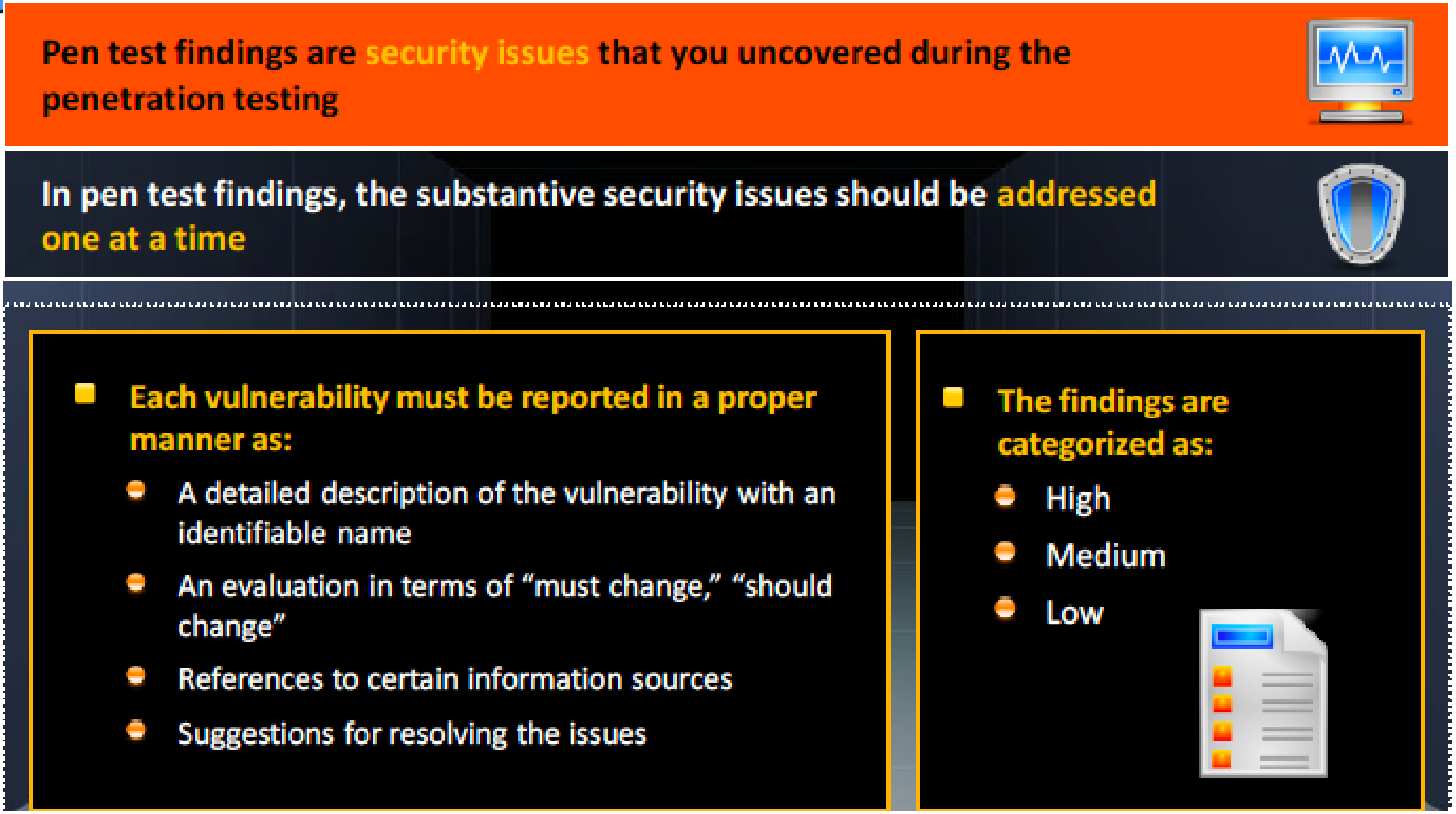
Extensive research and investigation must be conducted for each vulnerability

Research analysis helps the tester to list the functional anomalies and performance issues

Sumber: © Copyright by EC-Council

- ❖ Research analysis membantuk penguji untuk membuat daftar anomali fungsi dan

Pen Test Findings



Pen test findings are security issues that you uncovered during the penetration testing

In pen test findings, the substantive security issues should be addressed one at a time

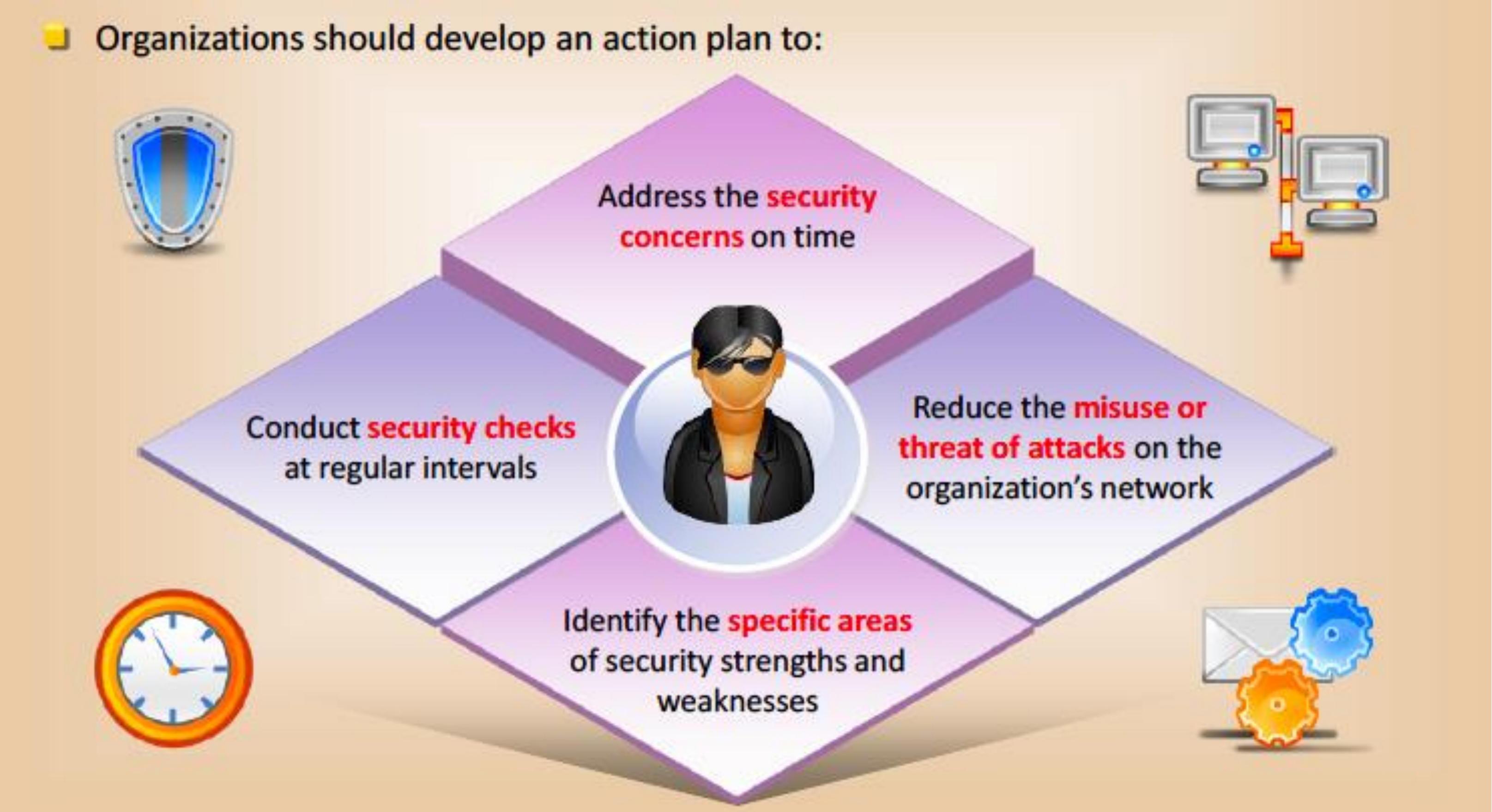
- Each vulnerability must be reported in a proper manner as:
  - A detailed description of the vulnerability with an identifiable name
  - An evaluation in terms of “must change,” “should change”
  - References to certain information sources
  - Suggestions for resolving the issues

- The findings are categorized as:
  - High
  - Medium
  - Low

Sumber: © Copyright by EC-Council

❖ Hasil temuan dari pen test dapat dikatagorikan high, medium dan low.

Develop Action Plan



- Organizations should develop an action plan to:

Address the security concerns on time

Conduct security checks at regular intervals

Reduce the misuse or threat of attacks on the organization's network

Identify the specific areas of security strengths and weaknesses

Sumber: © Copyright by EC-Council

❖ Merencanakan pengembangan pada area yang telah dilakukan pengujian.

Points to Check in Action Plan

Does the current security situation support the complete **business strategy**; what other technologies might give the firm a competitive edge?

Does the **current Information Technology** environment reach e-business requirements?

Are the **company's security-related expenses** included in the overall budget?

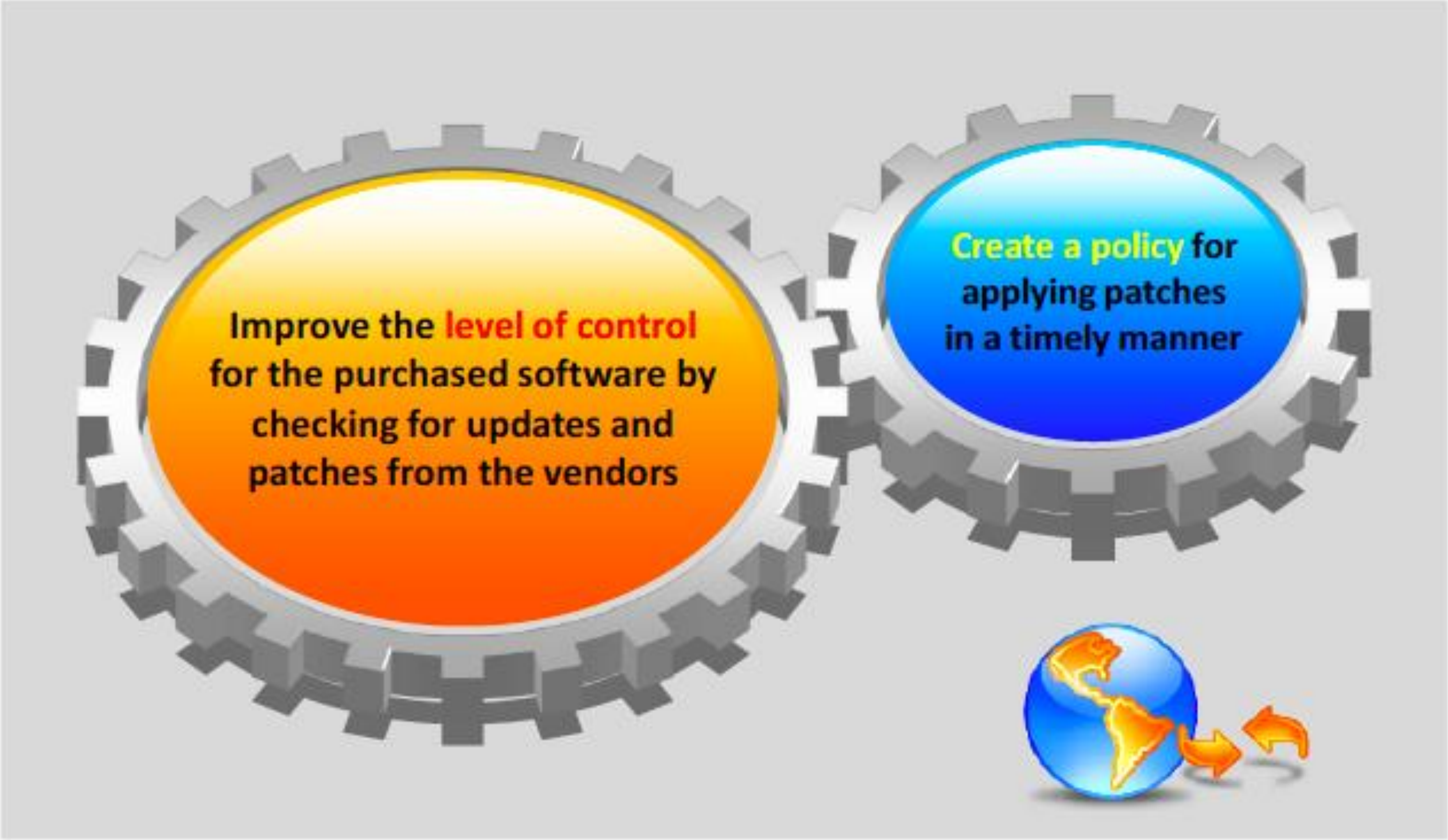
In what ways does the **company manage its risks**, and do other tests need to be performed?

Are **security**, **reliability**, and **privacy issues** ensured for the customer's data?

Are sufficient **resources** allocated to reduce the **business risks** or not?

Sumber: © Copyright by EC-Council

Updates and Patches



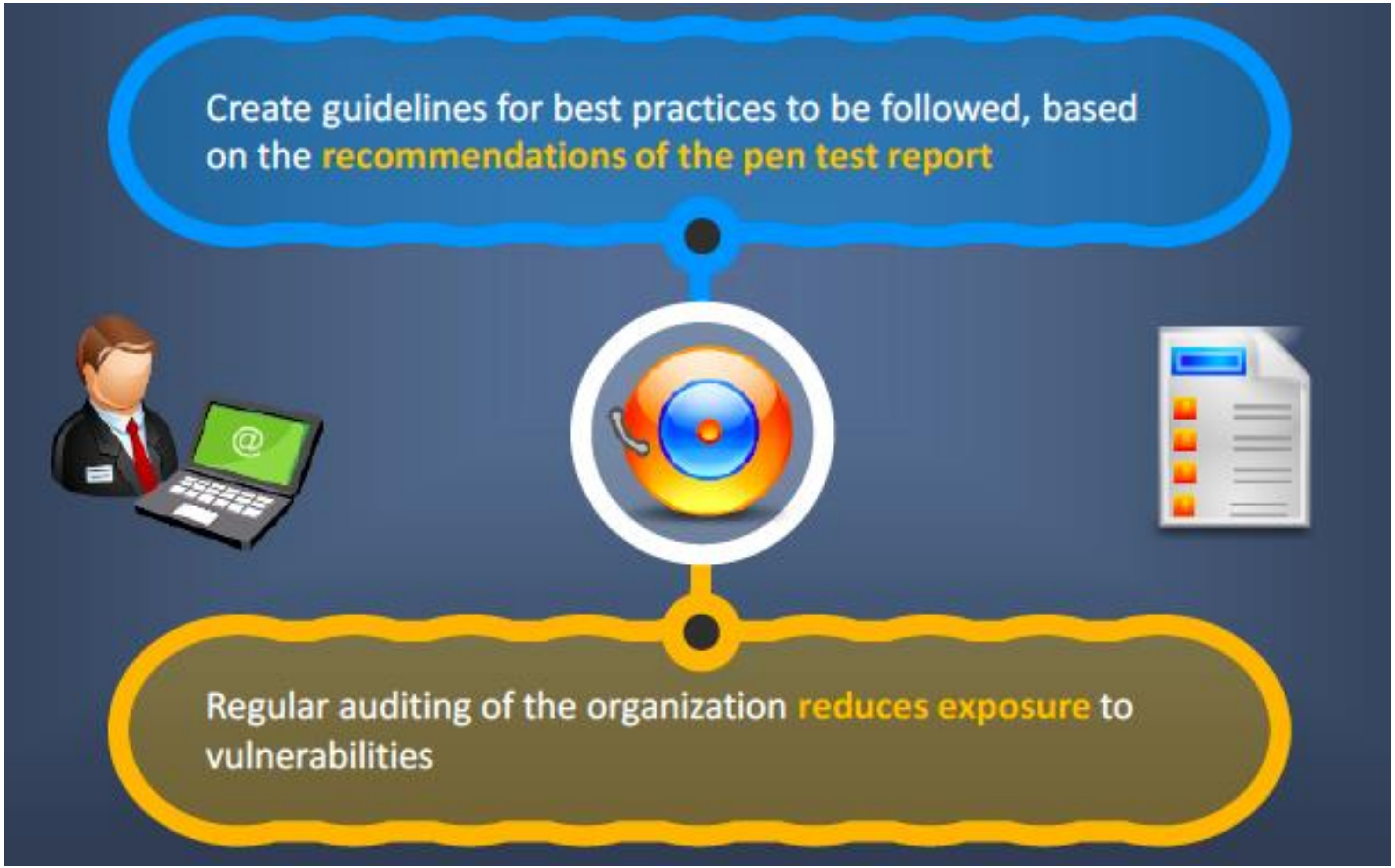
Improve the level of control for the purchased software by checking for updates and patches from the vendors

Create a policy for applying patches in a timely manner

Sumber: © Copyright by EC-Council

- ❖ Membuat kebijakan untuk melakukan update dan patch setiap software.

Capture Lessons Learned and Best Practices



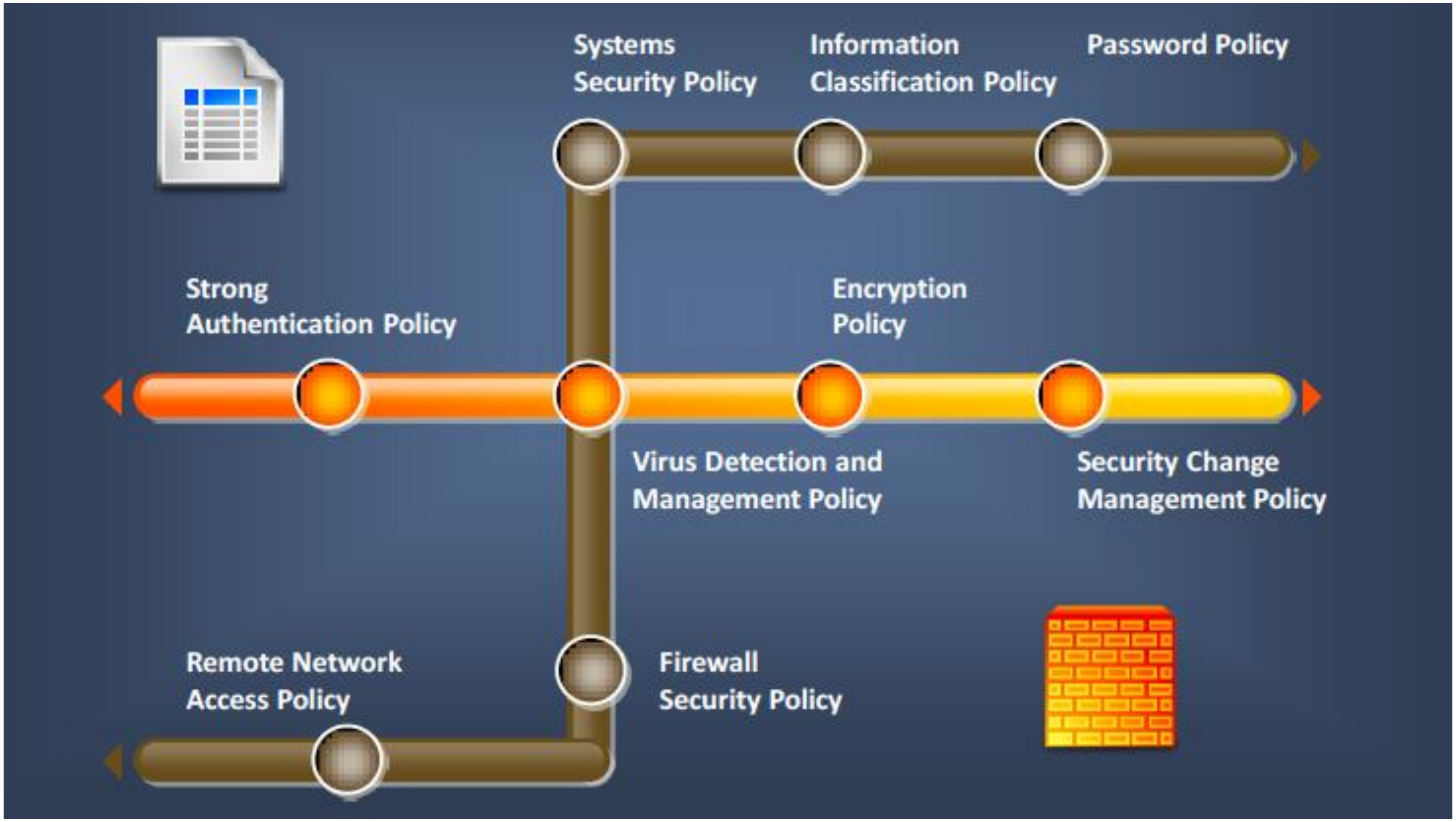
Create guidelines for best practices to be followed, based on the recommendations of the pen test report

Regular auditing of the organization reduces exposure to vulnerabilities

Sumber: © Copyright by EC-Council

- ❖ Membuat panduan untuk best practice.

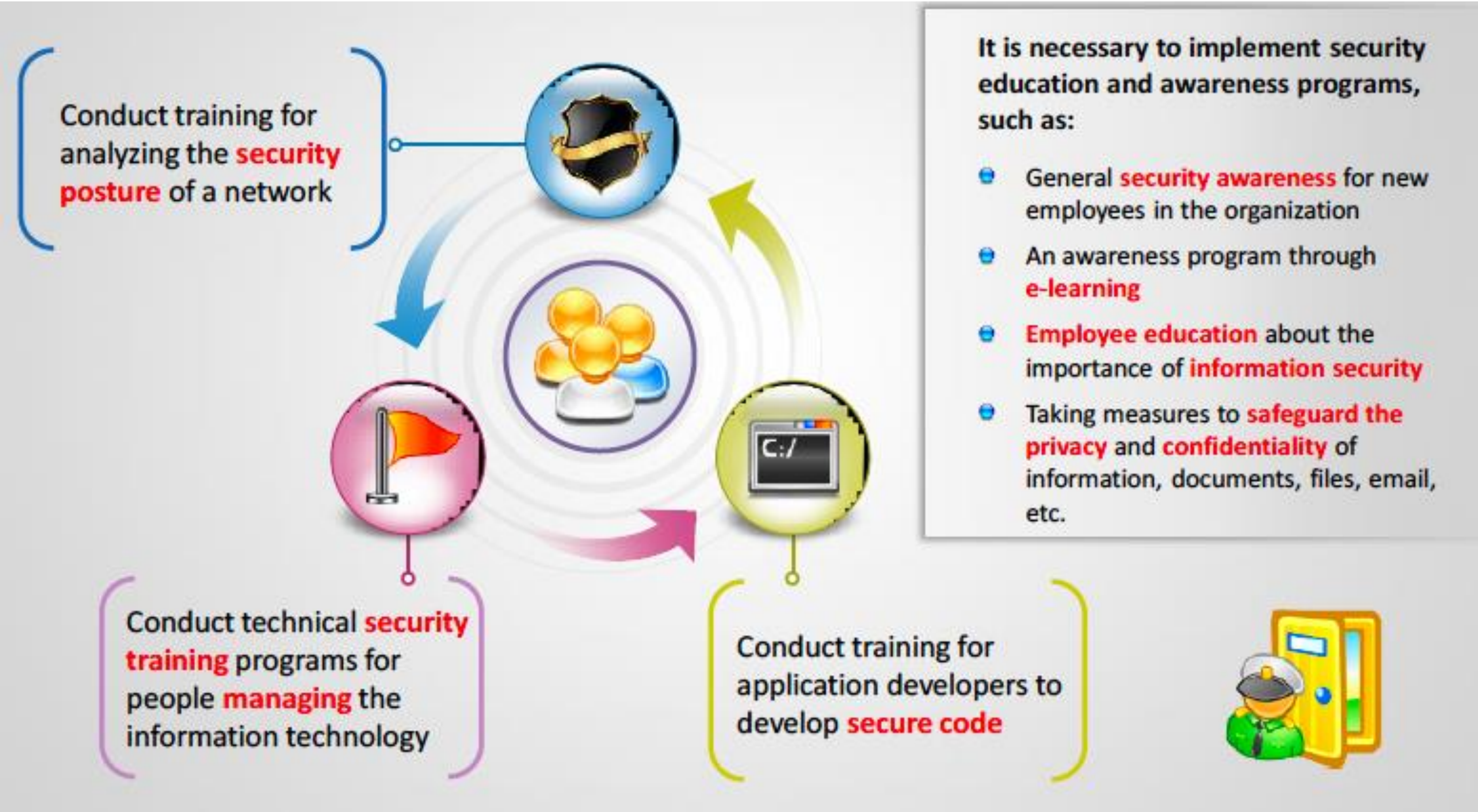
Create Security Policies


Systems Security Policy
Information Classification Policy
Password Policy
Strong Authentication Policy
Encryption Policy
Virus Detection and Management Policy
Security Change Management Policy
Remote Network Access Policy
Firewall Security Policy

Sumber: © Copyright by EC-Council

- ❖ Membuat kebijakan kemananan.

Conduct Training



Conduct training for analyzing the **security posture** of a network

Conduct technical **security training** programs for people **managing** the information technology

Conduct training for application developers to develop **secure code**

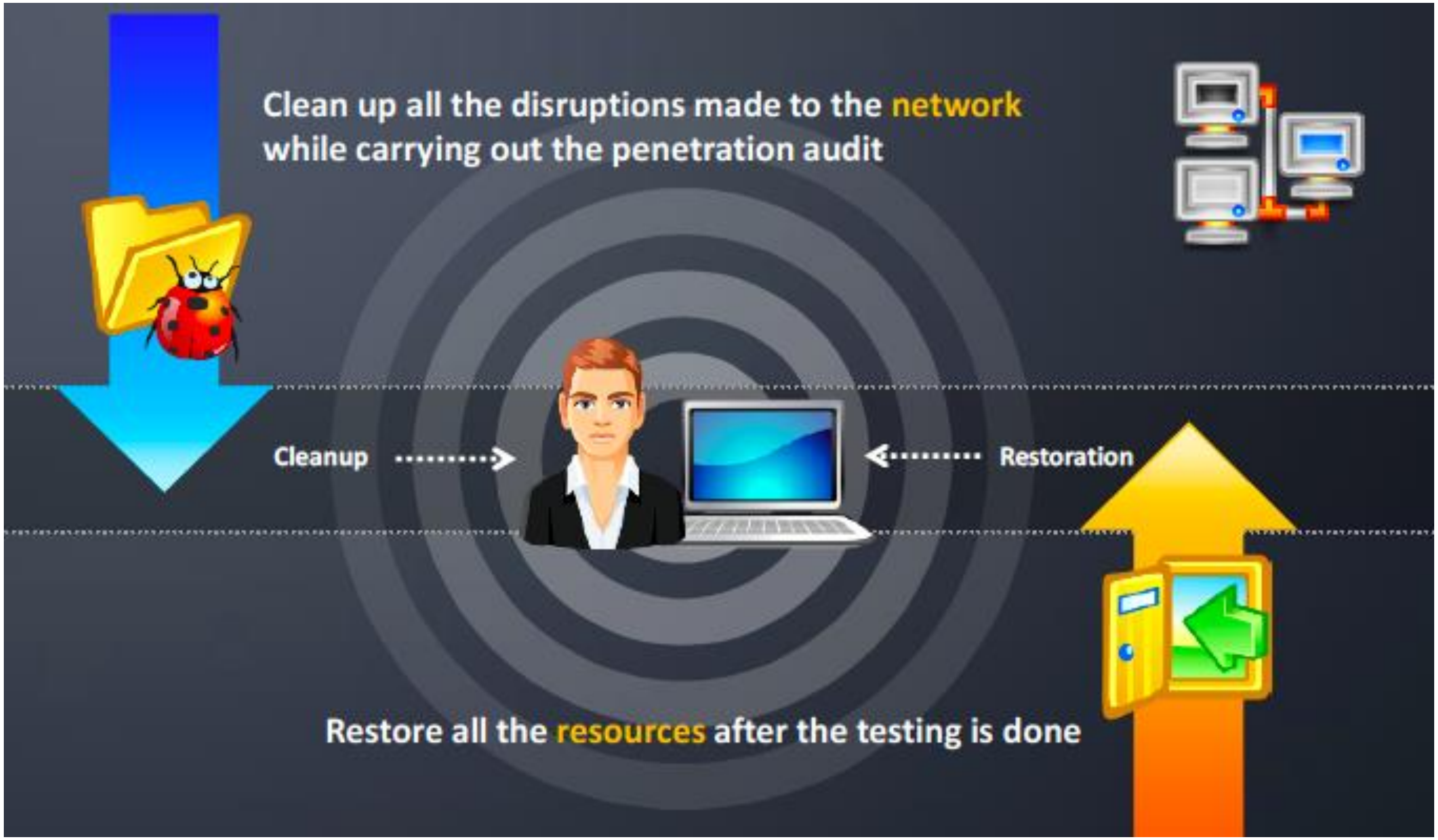
It is necessary to implement security education and awareness programs, such as:

- General **security awareness** for new employees in the organization
- An awareness program through **e-learning**
- **Employee education** about the importance of **information security**
- Taking measures to **safeguard the privacy** and **confidentiality** of information, documents, files, email, etc.

Sumber: © Copyright by EC-Council

❖ Mengadakan Training kepada staff IT yang ada di perusahaan tersebut.

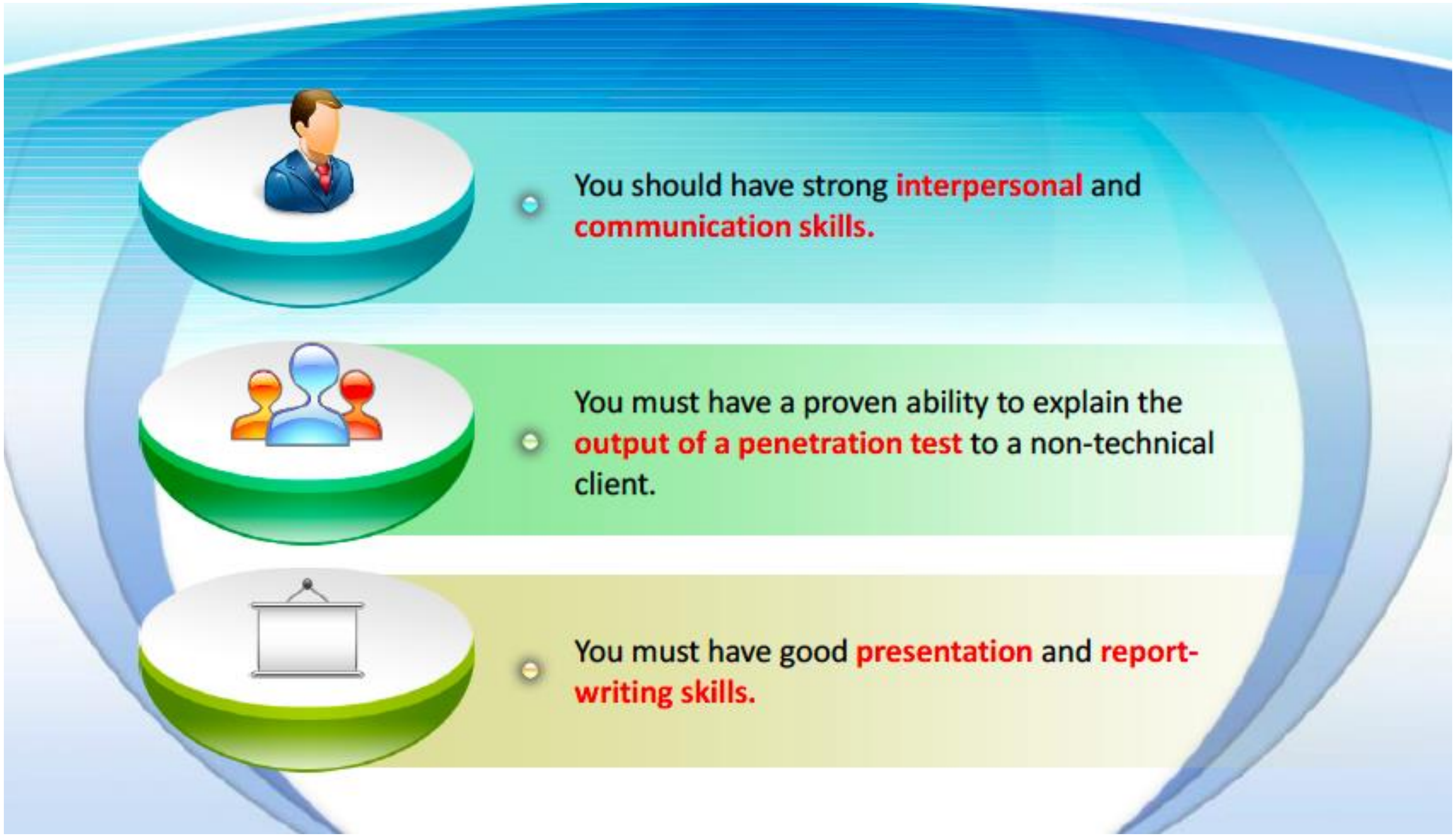
Cleanup and Restoration


Clean up all the disruptions made to the network while carrying out the penetration audit
Cleanup
Restoration
Restore all the resources after the testing is done

Sumber: © Copyright by EC-Council

- ❖ Membersihkan dan mengembalikan sistem dan jaringan yang telah dilakukan Penetration Test.

Communication Skills of a Penetration Tester

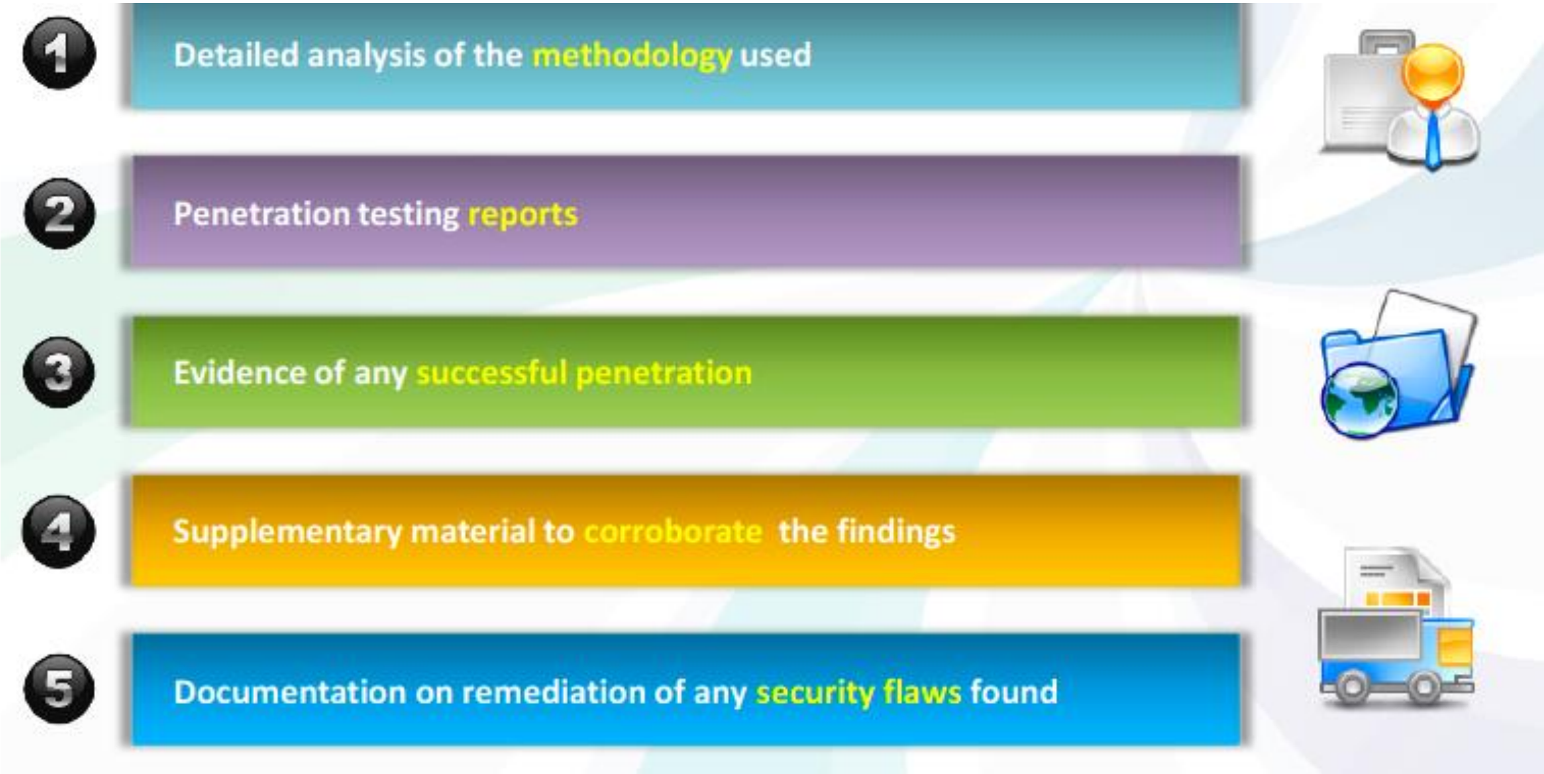


- You should have strong **interpersonal** and **communication skills.**
- You must have a proven ability to explain the **output of a penetration test** to a non-technical client.
- You must have good **presentation** and **report-writing skills.**

Sumber: © Copyright by EC-Council

❖ Sebagai seorang penetration tester harus memiliki ketrampilan dalam berkomunikasi karena pada saat penyampaian laporan hasil pengujian, penguji/pentester harus menyajikan dan mempresentasikan laporan kepada client/atasan perusahaan tersebut.

Penetration Testing Deliverables

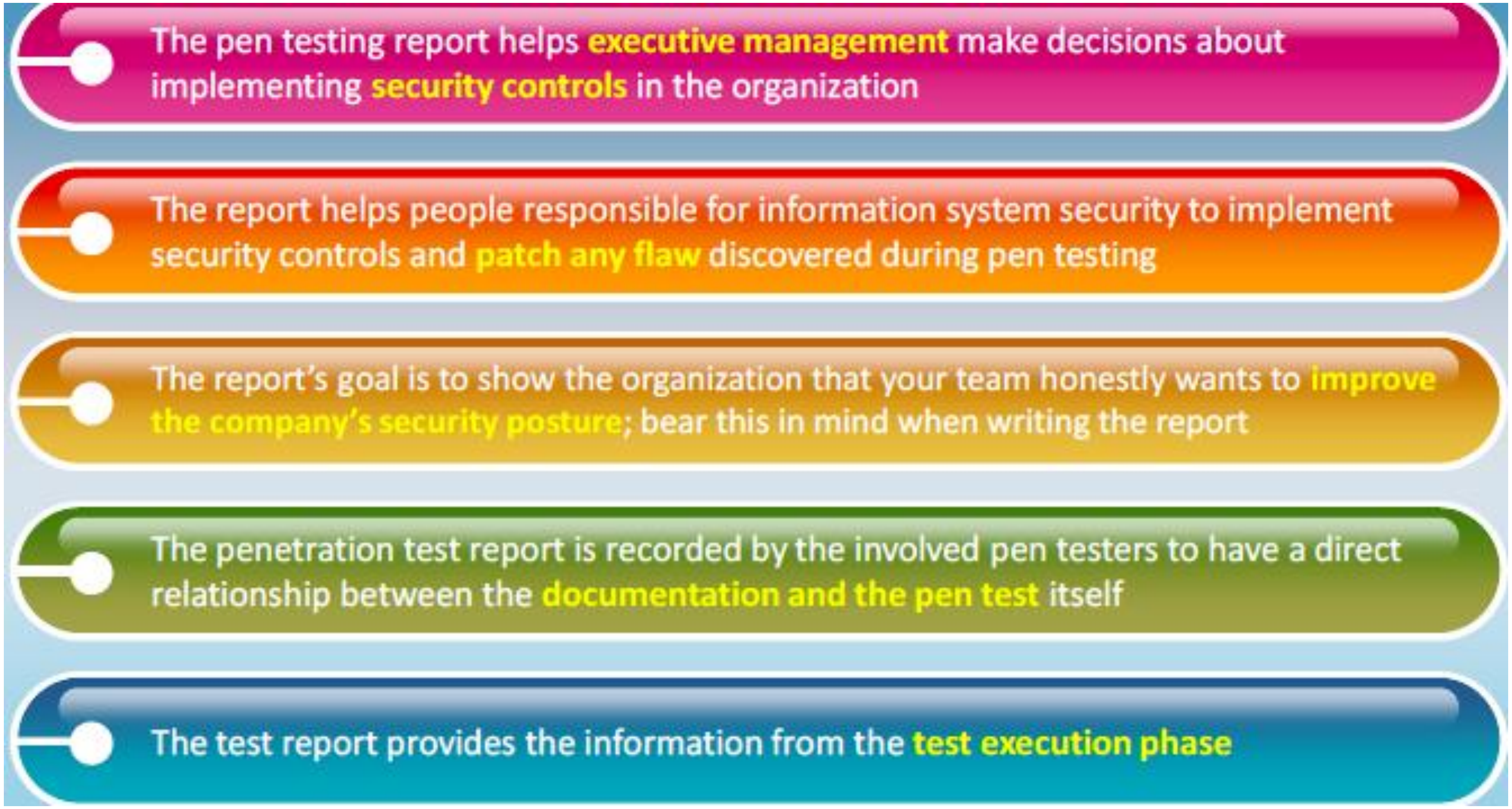


1. Detailed analysis of the methodology used
2. Penetration testing reports
3. Evidence of any successful penetration
4. Supplementary material to corroborate the findings
5. Documentation on remediation of any security flaws found

Sumber: © Copyright by EC-Council

- Pada saat penyampaian hasil penetration test harus jelas dan jujur dengan hasil yang sudah ada yaitu dengan menyampaikan metodologi yang digunakan, bukti dari setiap keberhasilan pengujian dan dokumentasi dari remediasi kelemahan keamanan yang ditemukan.

Goal of the Penetration Testing Report

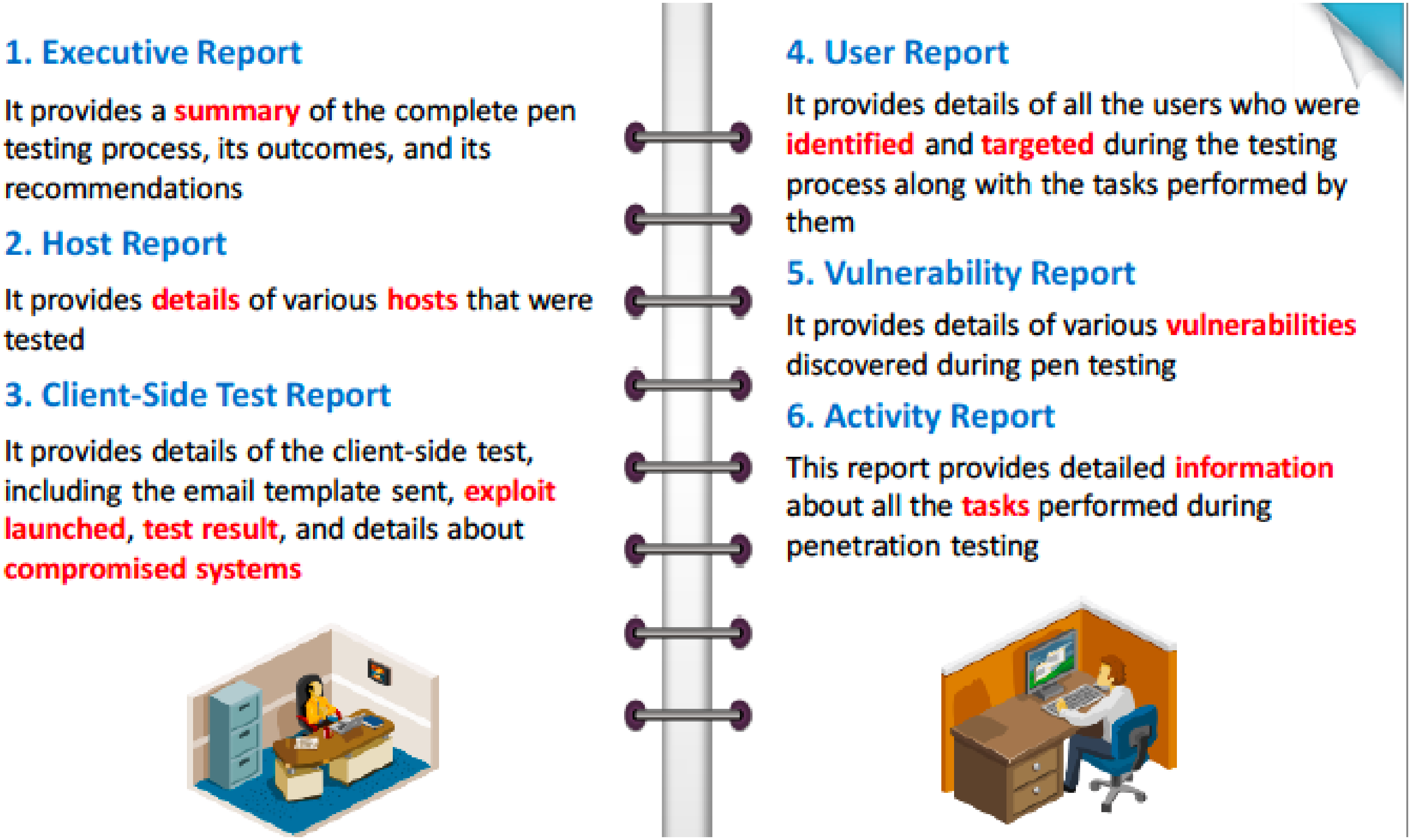


- The pen testing report helps **executive management** make decisions about implementing **security controls** in the organization
- The report helps people responsible for information system security to implement security controls and **patch any flaw** discovered during pen testing
- The report's goal is to show the organization that your team honestly wants to **improve the company's security posture**; bear this in mind when writing the report
- The penetration test report is recorded by the involved pen testers to have a direct relationship between the **documentation and the pen test** itself
- The test report provides the information from the **test execution phase**

Sumber: © Copyright by EC-Council

❖ Tujuan dari Laporan hasil Penetration Test yaitu dapat membantu eksekutif manajer untuk membuat keputusan terhadap kontrol keamanan dari organisasi perusahaan tersebut.

Types of Pen Test Reports



1. Executive Report

It provides a **summary** of the complete pen testing process, its outcomes, and its recommendations

2. Host Report

It provides **details** of various **hosts** that were tested

3. Client-Side Test Report

It provides details of the client-side test, including the email template sent, **exploit launched**, **test result**, and details about **compromised systems**

4. User Report

It provides details of all the users who were **identified** and **targeted** during the testing process along with the tasks performed by them

5. Vulnerability Report

It provides details of various **vulnerabilities** discovered during pen testing

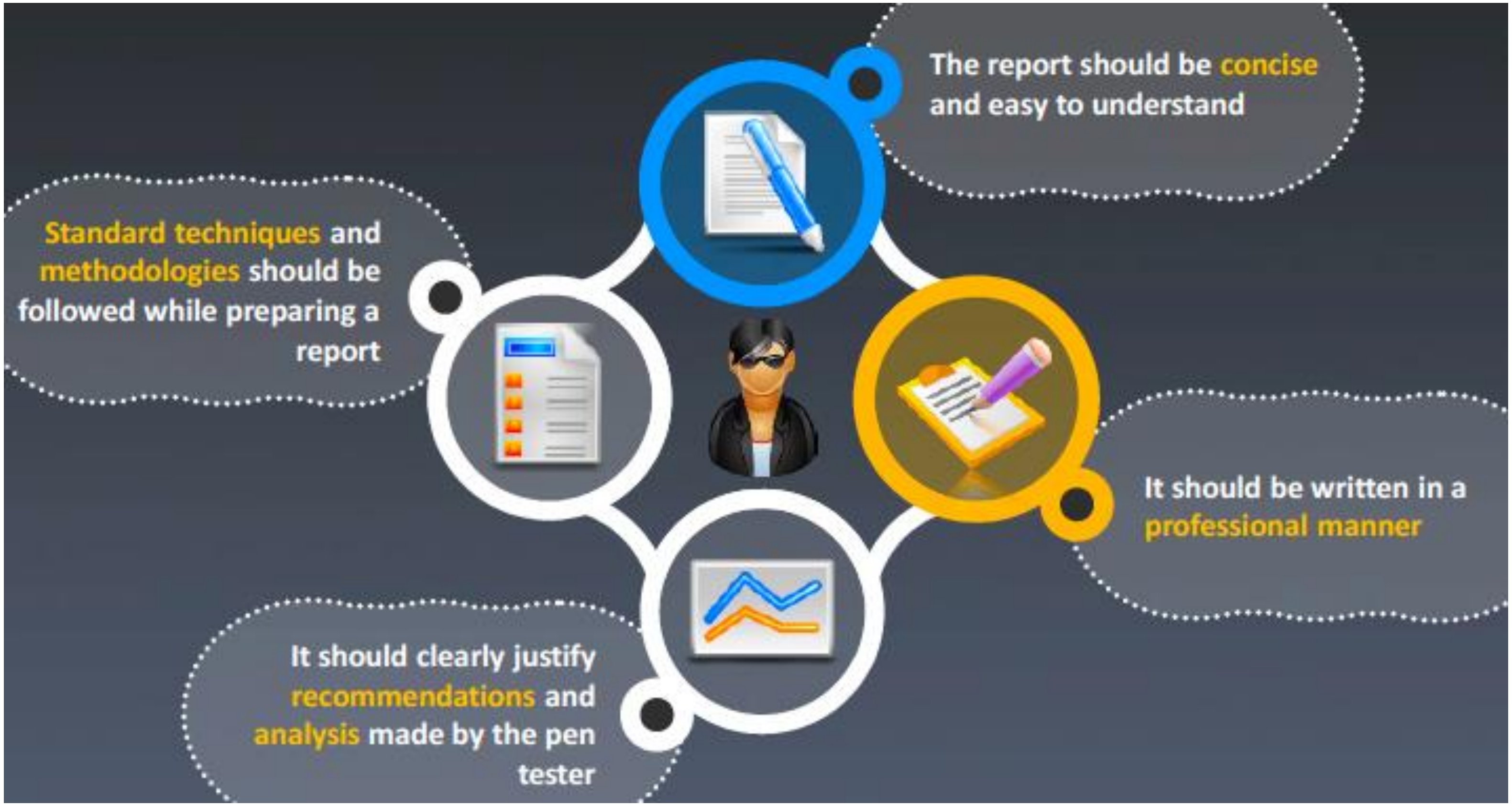
6. Activity Report

This report provides detailed **information** about all the **tasks** performed during penetration testing

Sumber: © Copyright by EC-Council

❖ Tipe-tipe dari Laporan Pen Test yaitu Executive Report, Host Report, Client-Side Test Report, User Report, Vulnerability Report dan Activity Report.

Characteristics of a Good Pen Testing Report



The report should be concise and easy to understand

Standard techniques and methodologies should be followed while preparing a report

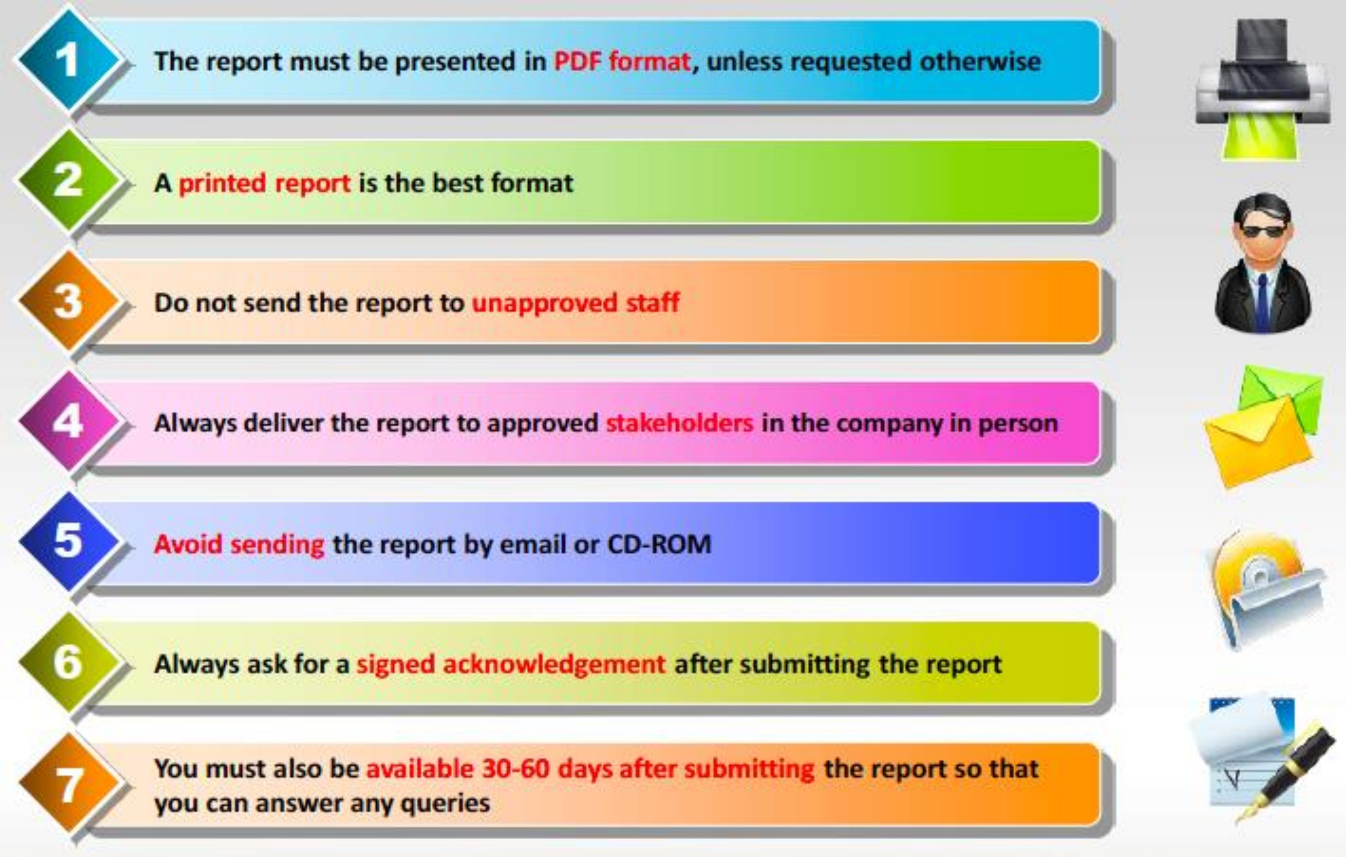
It should be written in a professional manner

It should clearly justify recommendations and analysis made by the pen tester

Sumber: © Copyright by EC-Council

❖ Karakteristik dari laporan Penetration Test

Delivering Penetration Testing Report

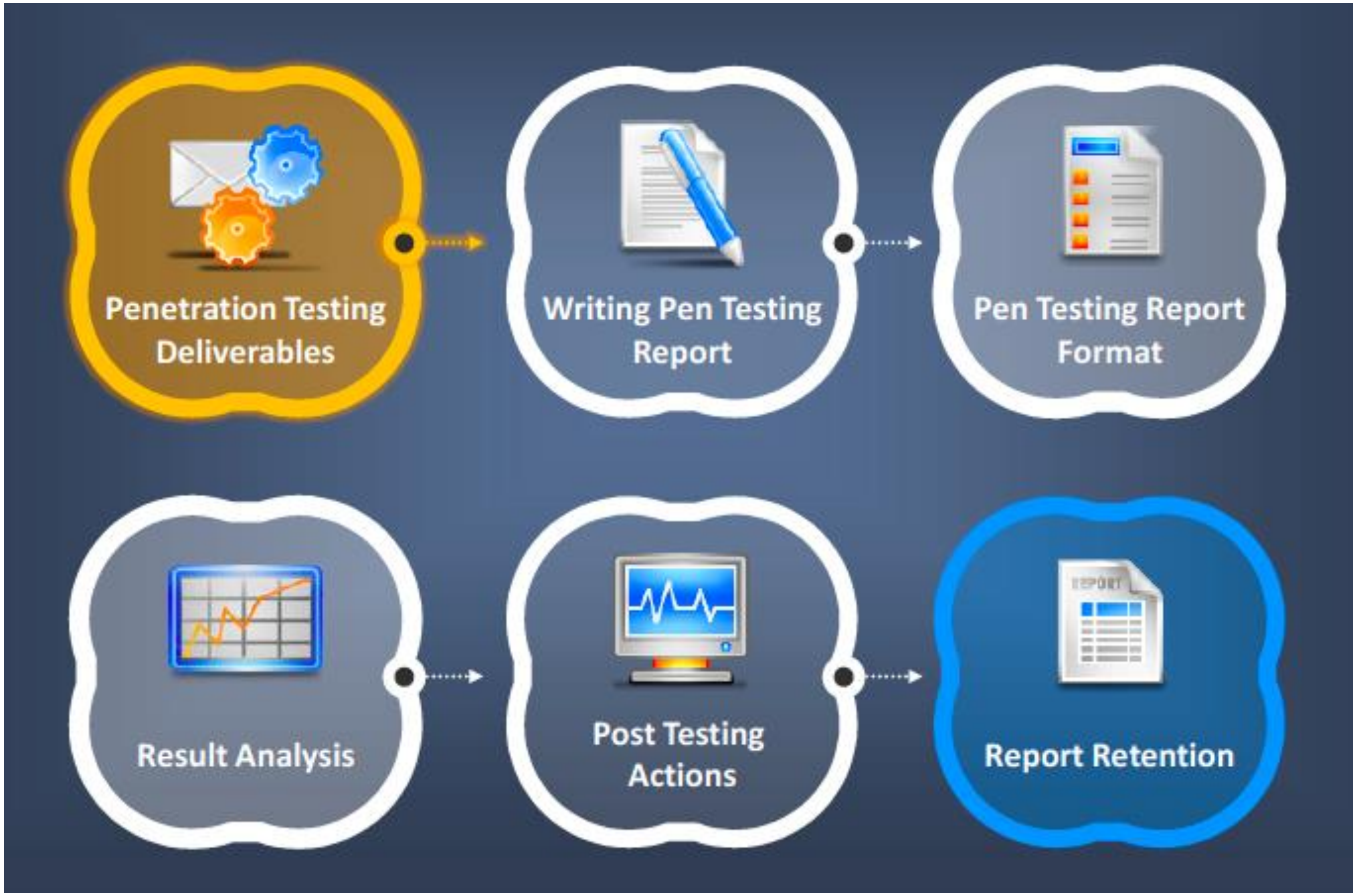


1. The report must be presented in PDF format, unless requested otherwise
2. A printed report is the best format
3. Do not send the report to unapproved staff
4. Always deliver the report to approved stakeholders in the company in person
5. Avoid sending the report by email or CD-ROM
6. Always ask for a signed acknowledgement after submitting the report
7. You must also be available 30-60 days after submitting the report so that you can answer any queries

Sumber: © Copyright by EC-Council

- Penyampaian Hasil Laporan dapat berupa dokumen presentasi format PDF, dokument yang sudah dicetak.

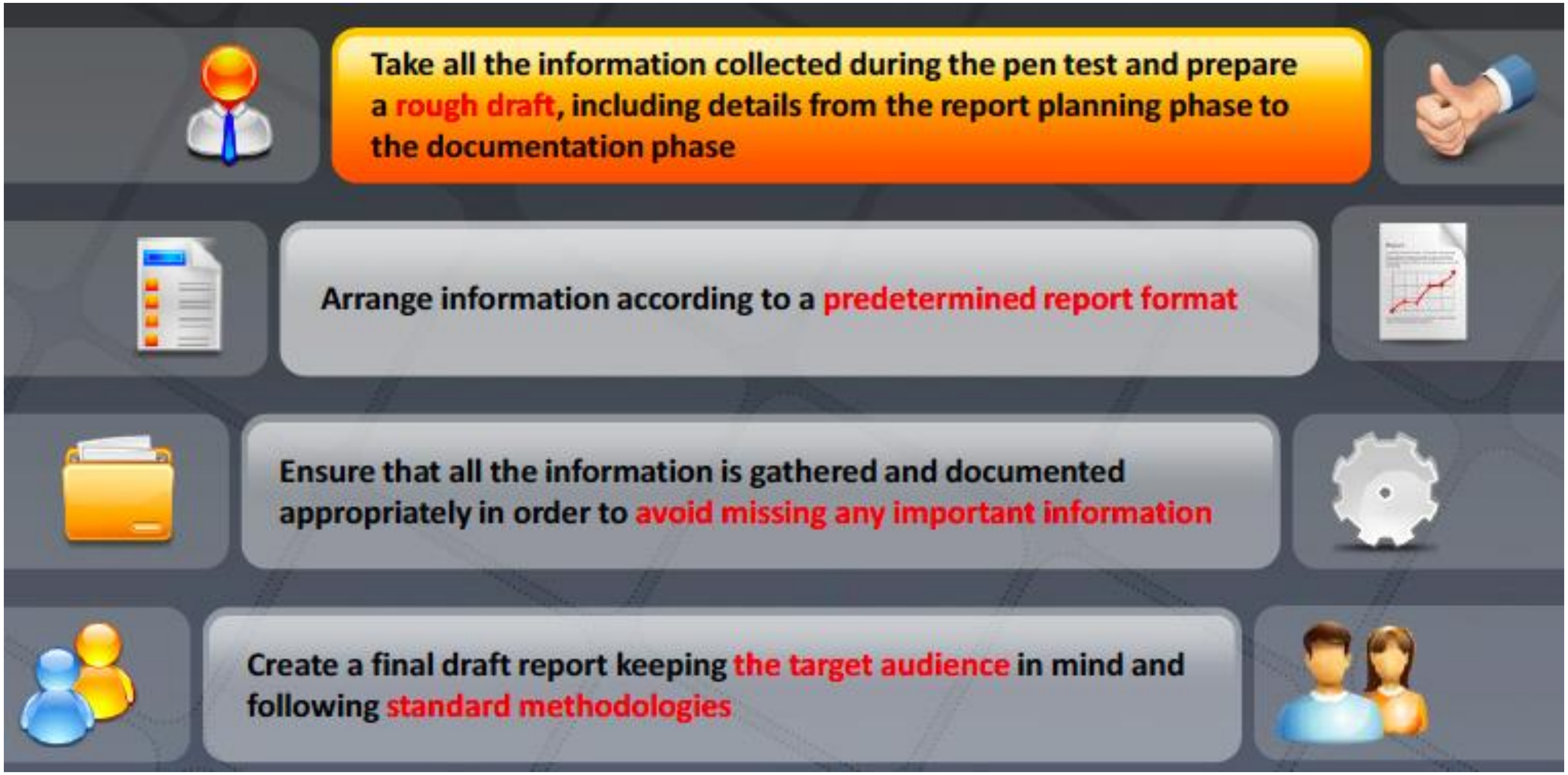
Reporting Flow


Penetration Testing Deliverables
Writing Pen Testing Report
Pen Testing Report Format
Result Analysis
Post Testing Actions
Report Retention

Sumber: © Copyright by EC-Council

- ❖ Alur dari pembuatan laporan.

Write a Draft Report



Take all the information collected during the pen test and prepare a rough draft, including details from the report planning phase to the documentation phase

Arrange information according to a predetermined report format

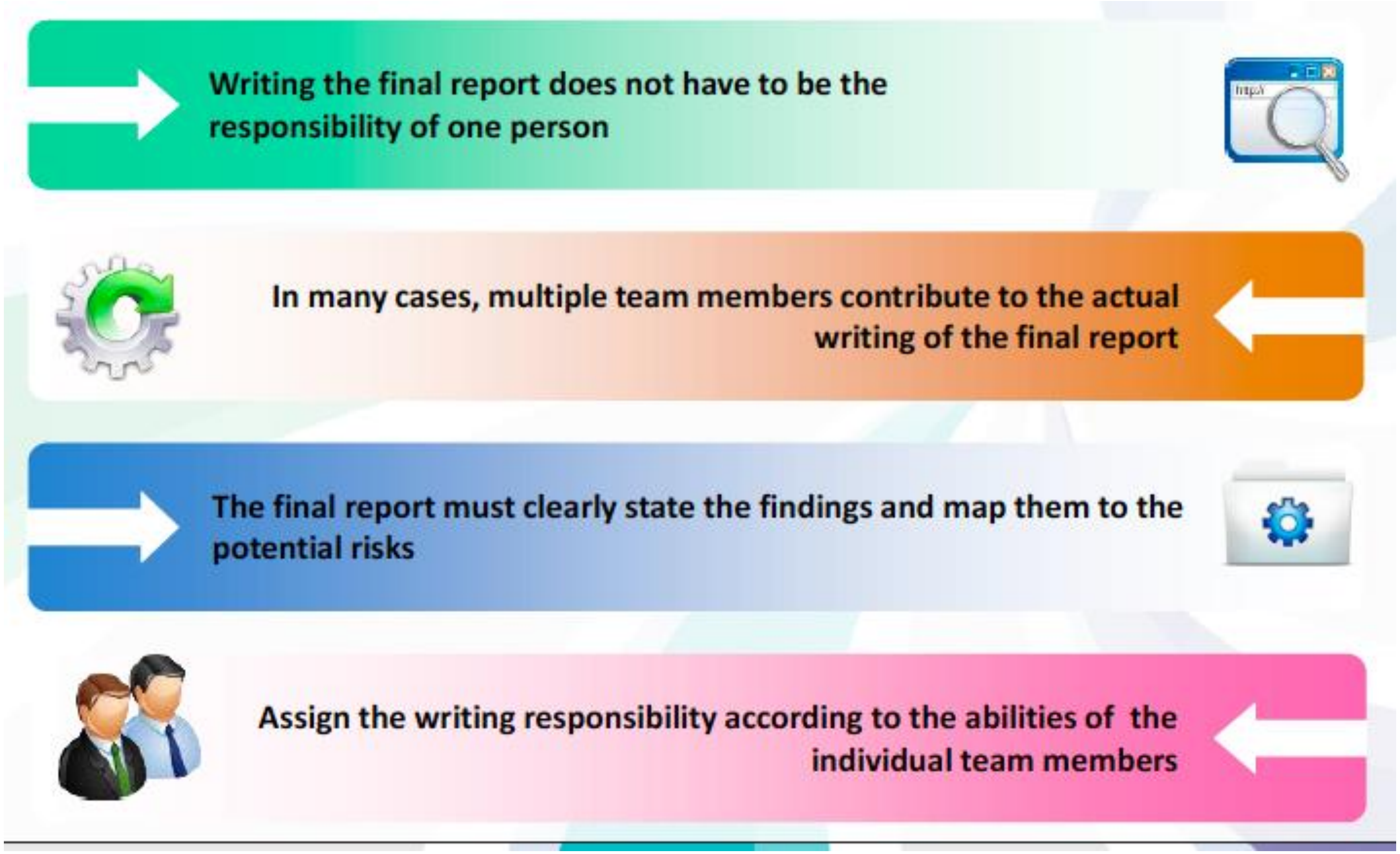
Ensure that all the information is gathered and documented appropriately in order to avoid missing any important information

Create a final draft report keeping the target audience in mind and following standard methodologies

Sumber: © Copyright by EC-Council

❖ Membuat draft laporan berguna pada saat kita akan membuat laporan akhir, karena jika kita sudah mempunyai draft laporan maka kita hanya mengumpulkan draft yang sudah ada.

Writing the Final Report



Writing the final report does not have to be the responsibility of one person

In many cases, multiple team members contribute to the actual writing of the final report

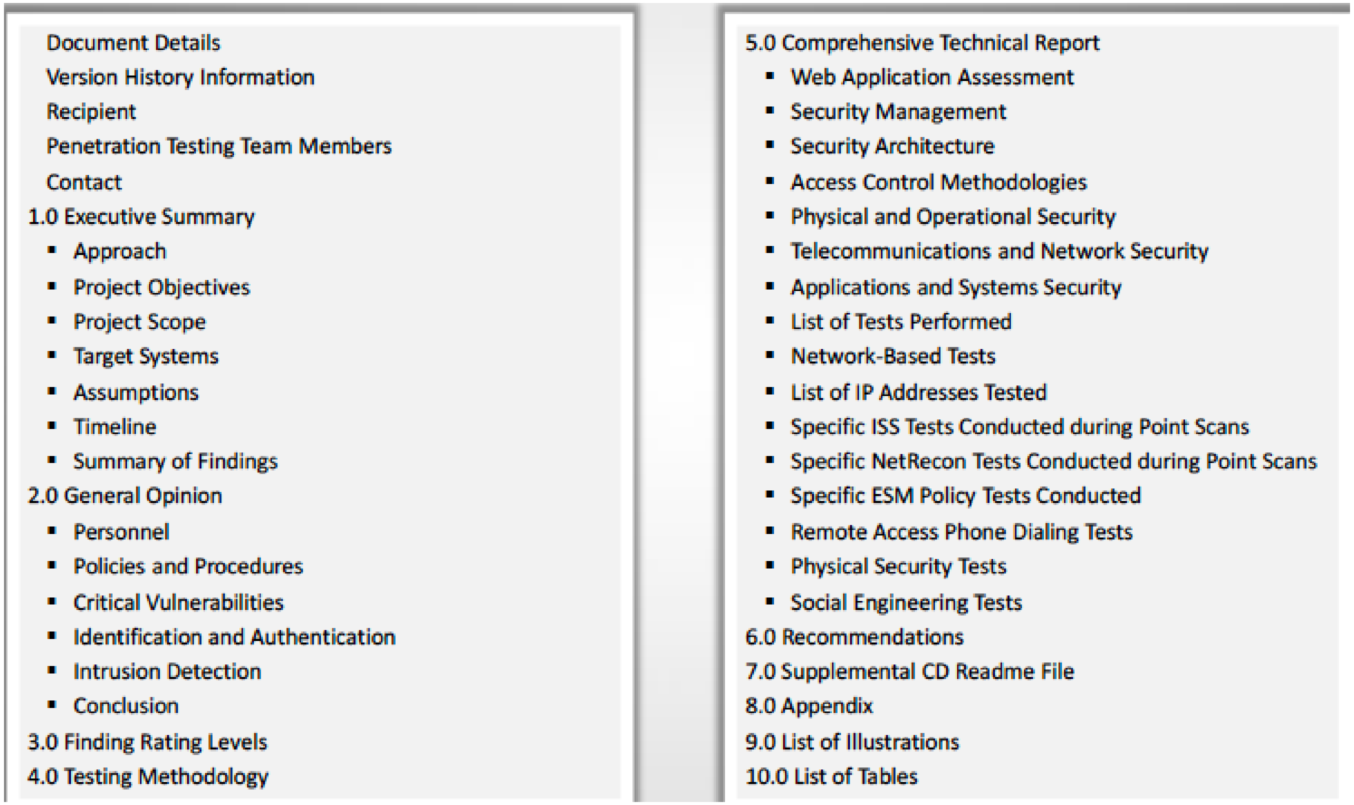
The final report must clearly state the findings and map them to the potential risks

Assign the writing responsibility according to the abilities of the individual team members

Sumber: © Copyright by EC-Council

- Pada saat penulisan laporan akhir jangan mengandalkan satu orang saja, lebih baik membuat laporan dengan seluruh tim yang terlibat.

Sample Pen Testing Report Format



Document Details
Version History Information
Recipient
Penetration Testing Team Members
Contact

1.0 Executive Summary

- Approach
- Project Objectives
- Project Scope
- Target Systems
- Assumptions
- Timeline
- Summary of Findings

2.0 General Opinion

- Personnel
- Policies and Procedures
- Critical Vulnerabilities
- Identification and Authentication
- Intrusion Detection
- Conclusion

3.0 Finding Rating Levels

4.0 Testing Methodology

5.0 Comprehensive Technical Report

- Web Application Assessment
- Security Management
- Security Architecture
- Access Control Methodologies
- Physical and Operational Security
- Telecommunications and Network Security
- Applications and Systems Security
- List of Tests Performed
- Network-Based Tests
- List of IP Addresses Tested
- Specific ISS Tests Conducted during Point Scans
- Specific NetRecon Tests Conducted during Point Scans
- Specific ESM Policy Tests Conducted
- Remote Access Phone Dialing Tests
- Physical Security Tests
- Social Engineering Tests

6.0 Recommendations

7.0 Supplemental CD Readme File

8.0 Appendix

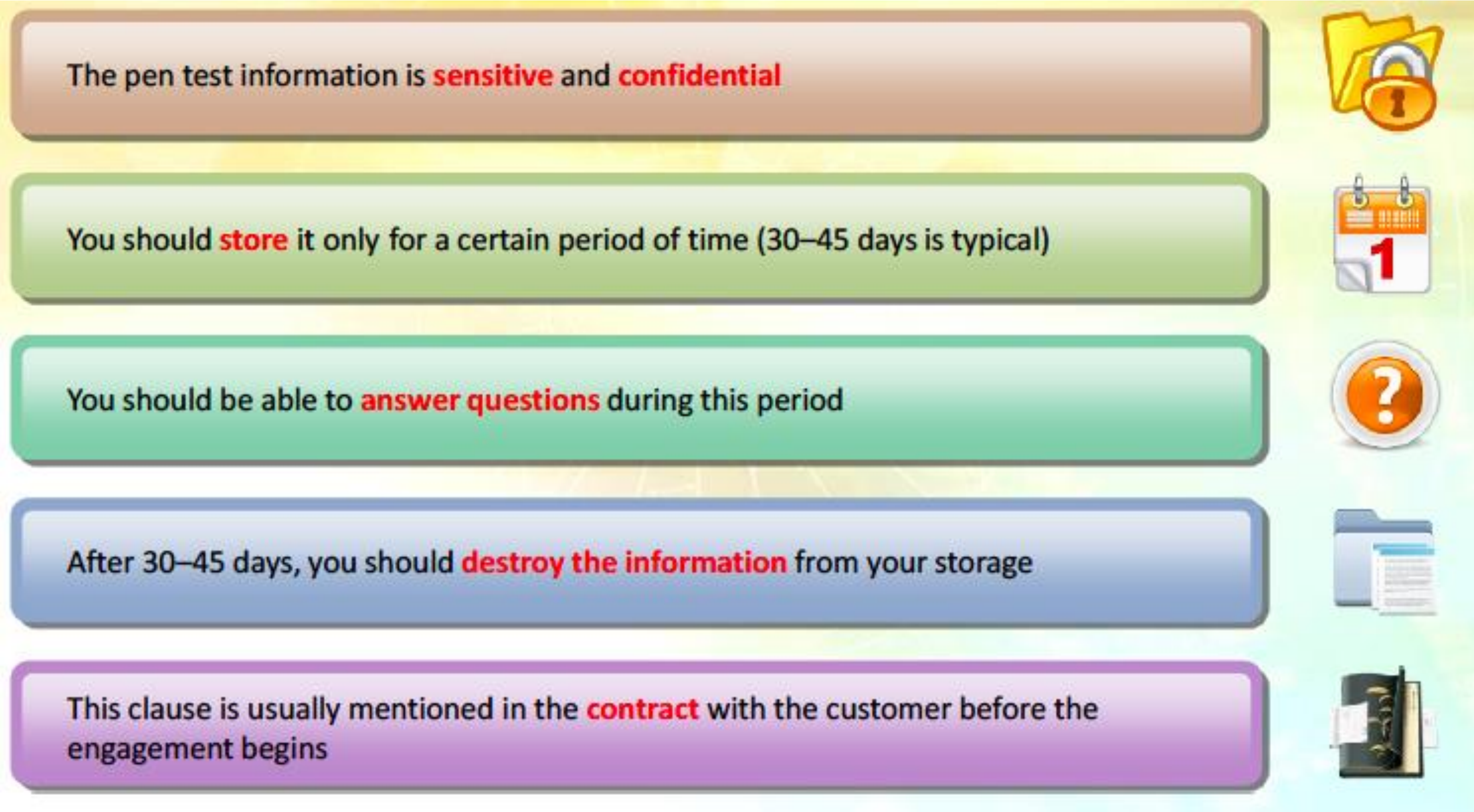
9.0 List of Illustrations

10.0 List of Tables

Sumber: © Copyright by EC-Council

- Contoh dari Laporan Penetration Test

Report Rentation



The pen test information is **sensitive** and **confidential**

You should **store** it only for a certain period of time (30–45 days is typical)

You should be able to **answer questions** during this period

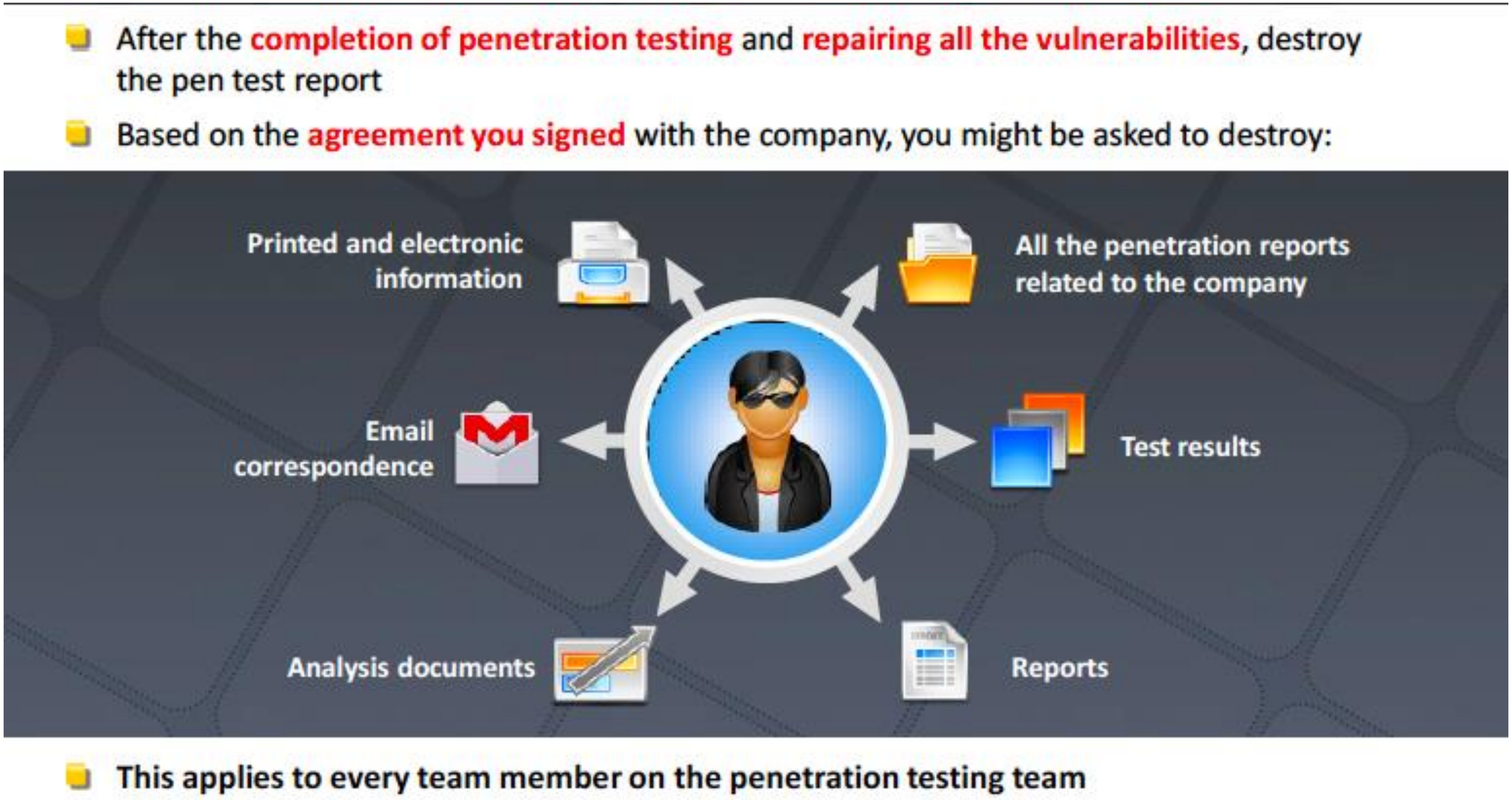
After 30–45 days, you should **destroy the information** from your storage

This clause is usually mentioned in the **contract** with the customer before the engagement begins

Sumber: © Copyright by EC-Council

- ❖ Retensi Laporan, Informasi pen test sangat sensitif dan rahasia, file harus disimpan sampai periode yang sudah ditentukan (30-45 hari), pen tester harus dapat menjawab semua pertanyaan selama periode tersebut. Setelah 30-45 hari file tersebut harus di musnahkan.

Destroy the Report



- After the **completion of penetration testing** and **repairing all the vulnerabilities**, destroy the pen test report
- Based on the **agreement you signed** with the company, you might be asked to destroy:

Printed and electronic information
All the penetration reports related to the company
Email correspondence
Test results
Analysis documents
Reports

- This applies to every team member on the penetration testing team

Sumber: © Copyright by EC-Council

❖ Setelah menyelesaikan semua kegiatan pen test, memperbaiki semua kerentanan sistem, membuat dokumen laporan maka tahap terakhir adalah memusnahkan dokumen tersebut.