



# **PENETRATION TESTING**

# WHAT IS PENETRATION TESTING

# HISTORY

The term **penetration test** and the methods used for testing were established in 1995 when the first Unix-based vulnerability scanner “SATAN” was introduced.

At that time the program was the first tool that was able to automatically scan computers to identify vulnerabilities.

# DEFINITION

*Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.*

– <https://searchsecurity.techtarget.com/>

# PENETRATION TESTING

- Involves manual and automated techniques to simulate an attack on an organisation's information security arrangements.
- Conducted by a qualified and independent penetration testing expert, sometimes referred to as an ethical security tester.
- Looks to exploit known vulnerabilities **and** use the expertise of the tester to identify specific weaknesses – unknown vulnerabilities

# PENETRATION TESTING PROCESS

- Involves an active analysis of the target system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures.
- This analysis is typically carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

# PENETRATION TESTING PROCESS

Process typically includes

1. Conducting research
2. Identifying vulnerabilities
3. Exploiting weaknesses
4. Reporting findings
5. Remediating issues.

# PEN TEST VS IT AUDIT

- Goal of IT audit: Generally examine the IT infrastructure in terms of its compliance, efficiency, effectiveness, etc.
  - Non necessarily to detect vulnerabilities
- Goal of pen test: Discover and document vulnerabilities
  - Does not involve verifying if backups can be retored, only if the data can be accessed



# ASSESSMENT

A Penetration Test is typically an assessment of IT infrastructure, networks and business applications to identify attack vectors, vulnerabilities and control weaknesses.

The two most common forms of penetration testing are:

- **Application penetration testing:** Typically web applications, which finds technical vulnerabilities
- **Infrastructure penetration testing:** Examines servers, firewalls and other hardware for security vulnerabilities.

# ASSESSMENT

Other forms of penetration testing are also popular, which include:

- Mobile application penetration testing
- Device penetration testing, (including workstations, laptops and consumer devices (eg. tablets and smartphones))
- Wireless penetration testing
- Telephony or VoIP penetration testing.

# **PENETRATION TESTING SKILLS**

Skills a Pentester Needs

# SYSTEM ADMINISTRATION/OPERATING SYSTEMS

- Knowledge of system administration/operating systems to be able to evaluate weaknesses in the operating system of the target system

# NETWORKS

- Knowledge of TCP/IP and, if applicable, other network protocols.
  - Data traffic on the internet is handled by TCP/IP, which has also become the standard in LANs, in-depth knowledge of this protocol is essential.

# PROGRAMMING LANGUAGES

- To be able to exploit vulnerabilities in applications and systems, knowledge of a programming language is advantageous.
  - Security gaps such as buffer overflows etc. can only be effectively exploited when the tester has the necessary programming knowledge.

# FIREWALLS AND IDS

- Knowledge of IT security products such as firewalls, intrusion detection systems
  - Security arrangements such as firewalls or intrusion detection systems are extremely common nowadays, the penetration tester should know how these security arrangements work and follow the latest reports on security gaps in IT security products.

# HACKER TOOLS AND VULNERABILITY SCANNERS

- Knowledge of how to handle hacker tools and vulnerability scanners
- In addition to some basic knowledge, experience in handling hacker tools and vulnerability scanners is necessary for performing penetration tests.
- Skills in the handling of these tools should be obtained through practical experience. Certain products have achieved a wide distribution (nmap for port scans, ...)
- The efficiency of the penetration test depends heavily on how experienced the penetration tester is in handling these tools.



# APPLICATION STRUCTURES AND USUAL ISSUES

- Many vulnerabilities are in the applications rather than the OS.
  - Span entire range of application systems, from insufficiently secured macro functions in word processing programs to vulnerabilities of browsers through scripting, to buffer overflow errors in large database systems, ...
  - Should be familiar with as many types of applications as possible.
  - Detailed knowledge of commonly used applications is important, since the risk of hackers and crackers here is generally particularly high.

# CREATIVITY

- In addition to the high professional requirements, creativity is an important quality in a penetration tester.
- A qualified penetration test can only follow a rigid pattern to a limited extent, the question of how to proceed at a particular point will undoubtedly arise during the course of a penetration test when it at first sight seems impossible to further compromise a system.
- A creative penetration tester should therefore be better positioned to perform a “successful” test than a penetration tester who merely relies on the results of his tools when performing the test.

# INTRUDER PROFILES

**Industrial espionage** - Serious problem for big enterprises.

- **Hackers:** Experimentally-minded programmers who target security loopholes in IT systems for technical reasons

# INTRUDER PROFILES

- **Crackers:** People with criminal energy who exploit weak points of IT systems to gain illegal advantages, social attention or respect.
  - **Insiders:** Crackers possessing privileged knowledge about the organization they are attacking. Often frustrated (former) employees of an organization
- **Script kiddies:** usually intruders lacking in-depth background knowledge and driven by curiosity who mainly direct attack tools downloaded from the internet against arbitrary or prominent targets.

# LEGAL ISSUES

# LEGAL ISSUES

1. Legal reason for penetration testing
2. Legal regulations and principles the tester should observe and clarify with client
3. Legal aspects which form the basis of the contract between client and tester

# LEGAL REASON FOR PENETRATION TESTING

There is usually no direct laws that require penetration testing, but indirectly, you must

- Secure handling and availability of data relevant to tax and commercial law
- Treatment of personal data (Fx GDPR)

# LEGAL FRAMEWORK FOR PENETRATION TESTING

During a penetration test, the tester carries out actions that, if performed without the client's consent may contravene present law.

- Intrusion is justified by the approval of the client
  - Must be agreed in the contract, including scope of the test



# LEGAL ISSUES

💡 Legislation is different from country to country. Some EU laws also come into play.

# ETHICAL ISSUES

# AFFECTING OTHERS

- What about 3rd parties (software integrated to)? Apart from the client, will others be directly or indirectly affected by the pentest?
  - 3rd party software, or network entities can easily be disrupted, if the scope is DoS tests.
  - AWS does not allow security scans/pentesting without prior approval

# LIABILITY RISKS

Have the liability risks received appropriate consideration?

The tester should have liability insurance with sufficient cover to insure himself against possible claims from 3rd parties.

Care should be taken to minimize risks against 3rd party before testing (but cannot completely be ruled out)

# AFFECTING EMPLOYEES AT CLIENT

Depending on scope and nature, some employees could be affected  
(extra work, slow work, etc.)

Should social engineering be used? And vulnerabilities discovered be  
exploited?

Should names be anonymized/can they? How many receptionists  
does a company have

Many testers reject the use of social engineering in security tests  
(the technique is very often successful)

# EXPLOITING VULNERABILITIES

Should you exploit found security vulnerabilities, to document whether it is feasible? Or just report them found?

# **PENETRATION TESTING OBJECTIVES**

# OBJECTIVES/CLIENT GOALS

One of four categories

1. Improving security of technical systems
2. Identifying vulnerabilities
3. Having IT security confirmed by an external third party
4. Improving security of organizational and personnel infrastructure



# IMPROVING SECURITY OF TECHNICAL SYSTEMS


- Tests confined to technical systems such as firewalls, routers, web servers, etc.
- Organizational and personnel infrastructure not being explicitly tested.
- Possible findings:
  - Unnecessary open firewall ports
  - Vulnerable versions of internet applications and operating systems.

# IDENTIFYING VULNERABILITIES

- Identification is the actual objective of the test.
- Example: before combining two LANs in the wake of a company merger, the new LAN can be tested to see whether it is possible to penetrate it from outside.
  - If this can be done in the penetration test, action has to be taken to secure the interface before the merger, or the two networks should not be combined at all.


# HAVING IT SECURITY CONFIRMED BY AN EXTERNAL THIRD PARTY

- Penetration test conducted to obtain confirmation from an independent external third party.
- Regular penetration testing may be suitable for demonstrating the increased security of customer data in a webshop or other internet application.

 Pen test only ever reflects the situation at a particular point in time and cannot therefore yield assertions about the level of security that are valid in the future.

# IMPROVING SECURITY OF ORGANIZATIONAL AND PERSONNEL INFRASTRUCTURE

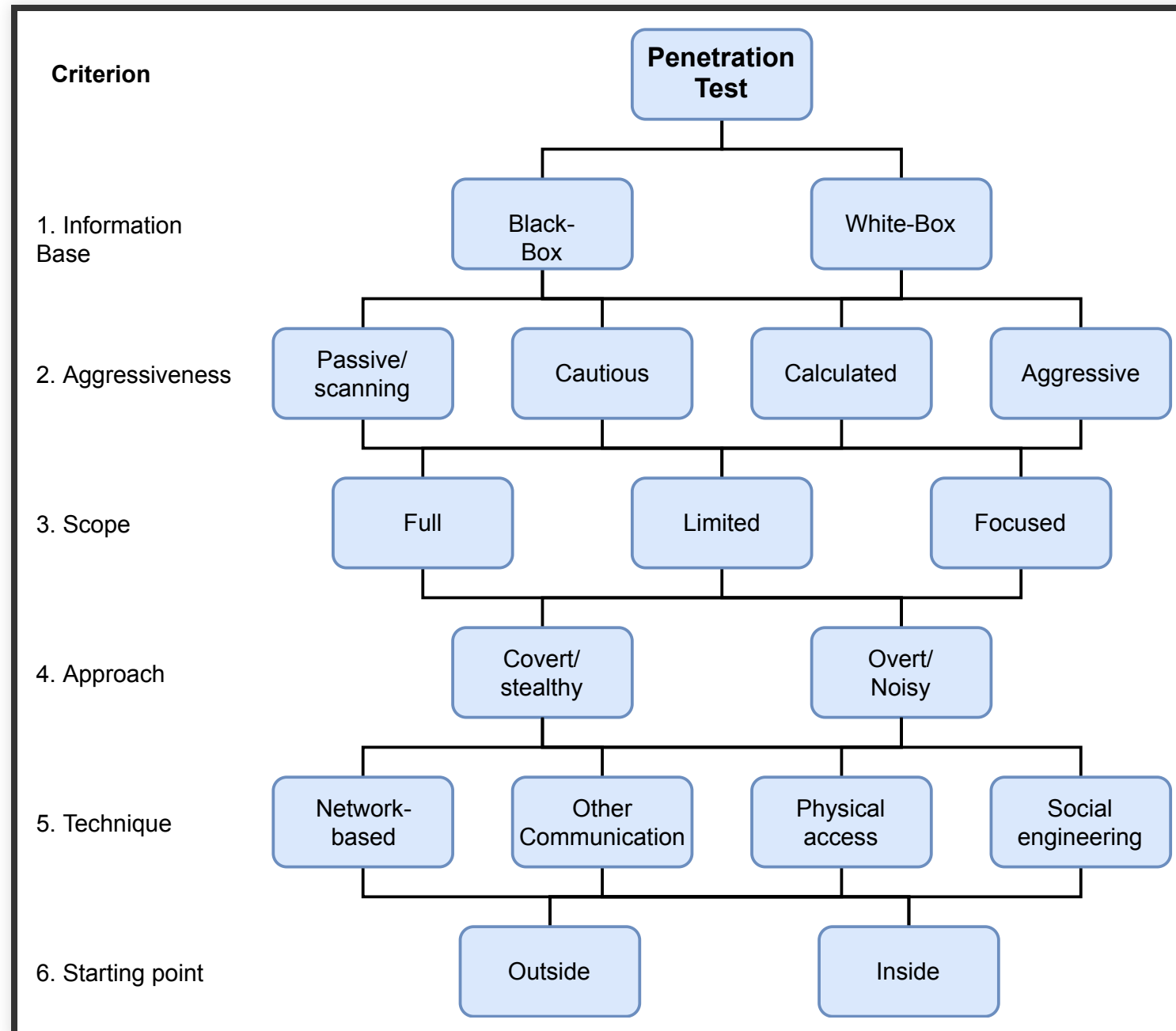
- Penetration test can also test the organizational and personnel infrastructure, to monitor escalation procedures
- Social engineering techniques, such as requesting passwords over the telephone, can be employed to assess the level of general security awareness and the effectiveness of security policies and user agreements.

 The scope of such tests needs to be defined precisely in advance

# **PENETRATION TESTING CLASSIFICATION**

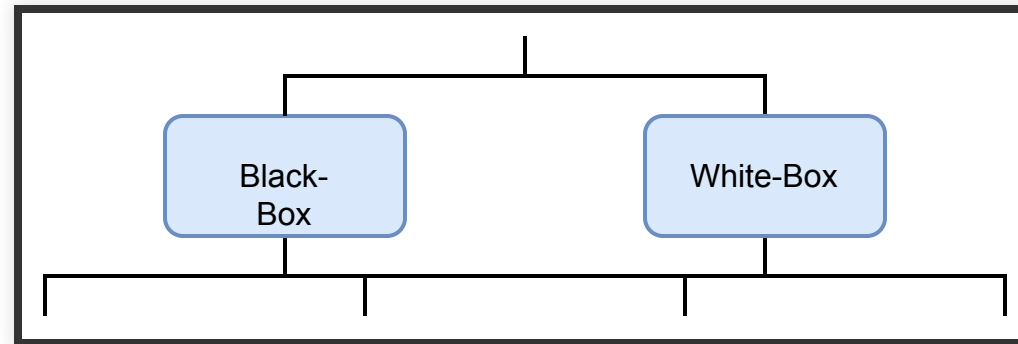
Knowing the scope makes it easier to classify the penetration test needed

# CLASSIFICATION





# INFORMATION BASE





# WHITE BOX PENETRATION TESTING

White Box Penetration Testing: Here, the tester has complete access and in-depth knowledge of the system to be tested. This is very helpful in carrying out extensive penetration testing.

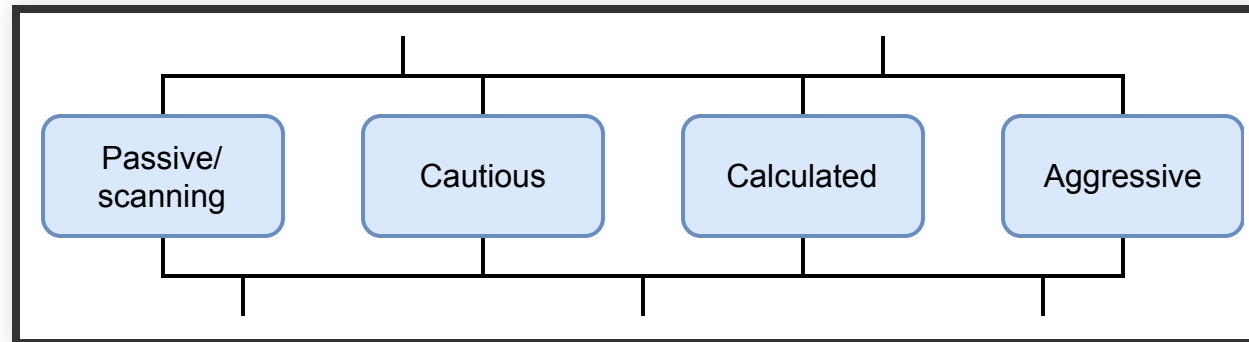
# BLACK BOX PENETRATION TESTING

Black Box Penetration Testing: In black box penetration testing approach, high-level of information is made available to the tester. The tester is totally unaware of the system/network. However, this approach might miss some areas while testing.

# GRAY BOX PENETRATION TESTING

Gray Box Penetration testing: Gray box penetration testing makes only limited information available to the tester to attack the system externally.

# AGGRESSIVENESS



# AGGRESSIVENESS

- **Passive/scanning:** Test objects are investigated passively only, i.e. any vulnerabilities that are detected are not exploited.
- **Cautious:** Identified vulnerabilities are only exploited when, to the best of the tester's knowledge, the system being tested will not suffer as a result, fx using known default passwords or trying to access directories on a web server.

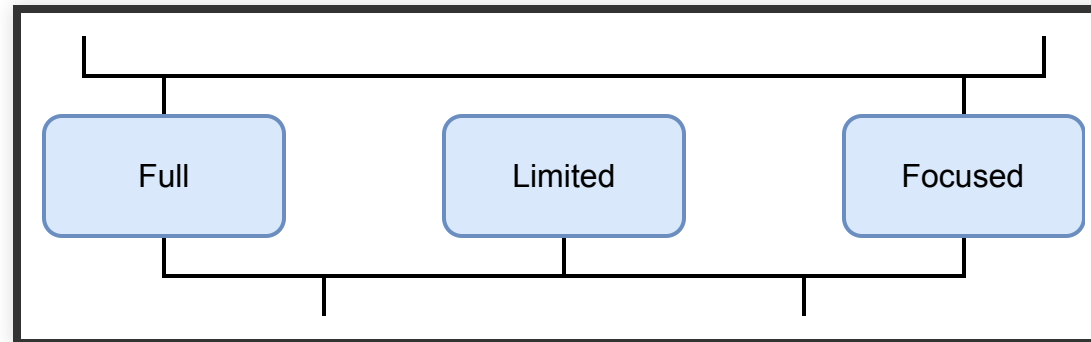
# AGGRESSIVENESS - CALCULATED

- **Calculated:** Tester also attempts to exploit vulnerabilities that might result in system disruptions.
  - This includes, for instance, automatically trying out passwords and exploiting known buffer overflows in precisely identified target systems.
  - Tester considers how likely they are to be successful and how serious the consequences would be.

# AGGRESSIVENESS - AGGRESSIVE

- **Aggressive:** Tester tries to exploit all potential vulnerabilities, e.g. buffer overflows are used even on target systems that are not clearly identified, or security systems are deactivated by deliberate overloading (denial of service (DoS)) attacks.
  - The tester has to be aware that, in addition to the systems being tested, neighboring systems or network components might also fail as a result of these tests.

# SCOPE





# SCOPE - FULL TEST

A **full test** covers all available systems. It should be noted that even in a complete test certain systems, e.g. outsourced and externally hosted systems, might not be able to be tested

When a penetration test is being carried out for the first time, a **full test** is advisable to ensure that no security loopholes are overlooked in systems that have not been tested.

# SCOPE - LIMITED

In a **limited** penetration test, a limited number of systems or services are examined.

For example, all systems in the DMZ, or systems comprising a functional unit can be tested.

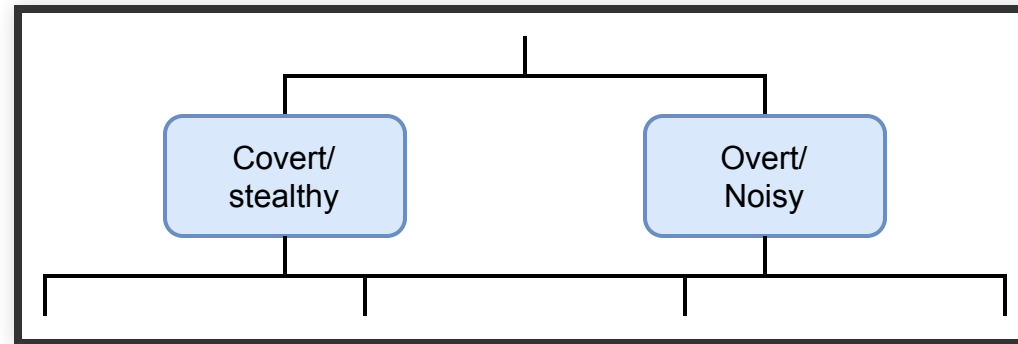
# SCOPE - FOCUSED

If only a specific sub-network, system or service is to be tested, for the purposes of this study the penetration test is termed **focused**.

This test scope is appropriate after a modification or extension of the system landscape, for instance.

**Cannot** provide general information about IT security.

# APPROACH



# APPROACH - COVERT

Penetration tests carried out on secondary security systems and existing escalation procedures should – at least in the beginning –  
**be covert**

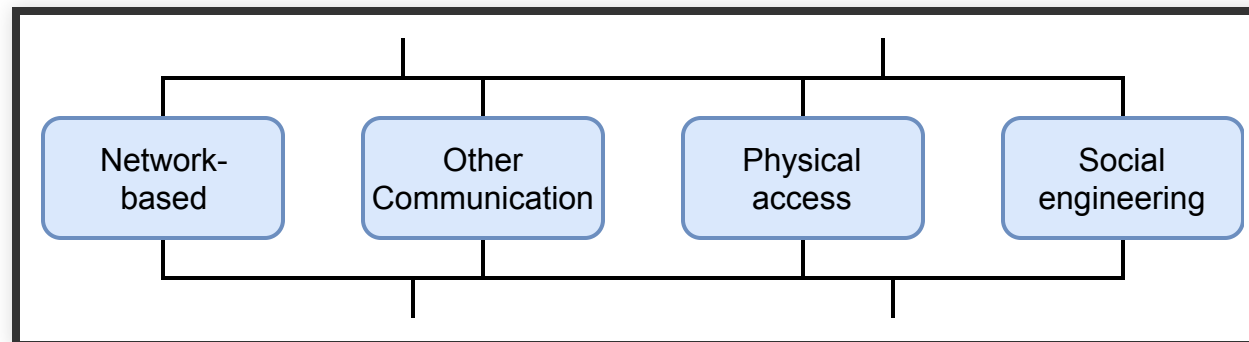
In the initial survey stage only methods that are not directly identifiable as attempts at attacking the system should be employed.

# APPROACH - OVERT

**Overt** methods, such as extensive port scans with a direct connection, may be employed.

The client's staff may be included in the team conducting an overt white-box test. This is particularly advisable with highly critical systems because it means that the testers are able to react faster to unexpected problems.

# TECHNIQUE



# TECHNIQUE - NETWORK-BASED

Network-based penetration test is the normal procedure, and simulates a typical hacker attack.

Most IT networks currently use the TCP/IP protocol, which is why such tests are also called IP-based penetration tests.



# TECHNIQUE - COMMUNICATION NETWORKS

Apart from TCP/IP networks there are other communication networks that can also be used for staging an attack.

These include telephone and fax networks, wireless networks for mobile communication, incl bluetooth

# TECHNIQUE - PHYSICAL

Firewalls etc., are widespread, and the configurations of such systems usually afford a high level of security. It is often easier and quicker to obtain the desired or necessary data by circumventing these systems in a direct **physical attack**.

A physical attack can, for example, involve directly accessing data at a non-password protected workstation after gaining unauthorized access to the building and/or server rooms.

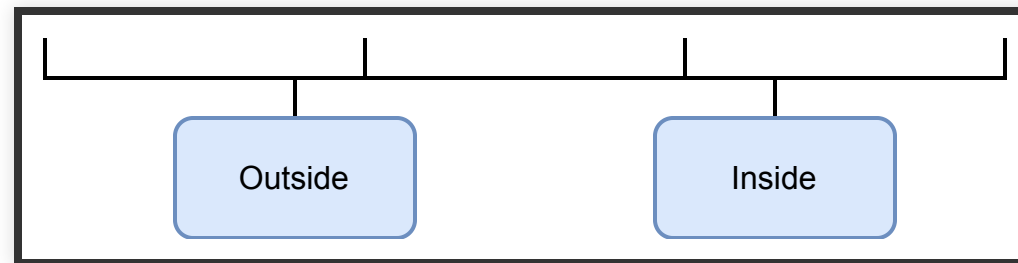
# TECHNIQUE - SOCIAL ENGINEERING

People are frequently the weakest link in the security chain

Social engineering techniques that exploit inadequate security skills or insufficient security awareness are often successful.

Such tests are appropriate after the introduction of a general security policy, for example, to assess the extent of its implementation and/or acceptance.

# STARTING POINT



# STARTING POINT

The starting point of the penetration test, i.e. the point where the penetration tester connects his computer to the network or where his attacking attempts originate can be either inside or outside the client's network or building.

# STARTING POINT - OUTSIDE

A penetration test from the outside is able to detect and evaluate the potential risk of a real hacker attack.

Typically, the firewall, systems in the DMZ and RAS connections are investigated in such tests.

# STARTING POINT - INSIDE

In a penetration test from the inside, the tester does not normally have to overcome firewalls or entry controls to access internal networks.

Therefore a test from the inside can assess the effects of an error in the firewall configuration, a successful attack on the firewall, or of an attack by persons with access to the internal network.

# MULTISTAGE APPROACH

Combination of the different penetration tests shown in the classification is often advisable

For instance

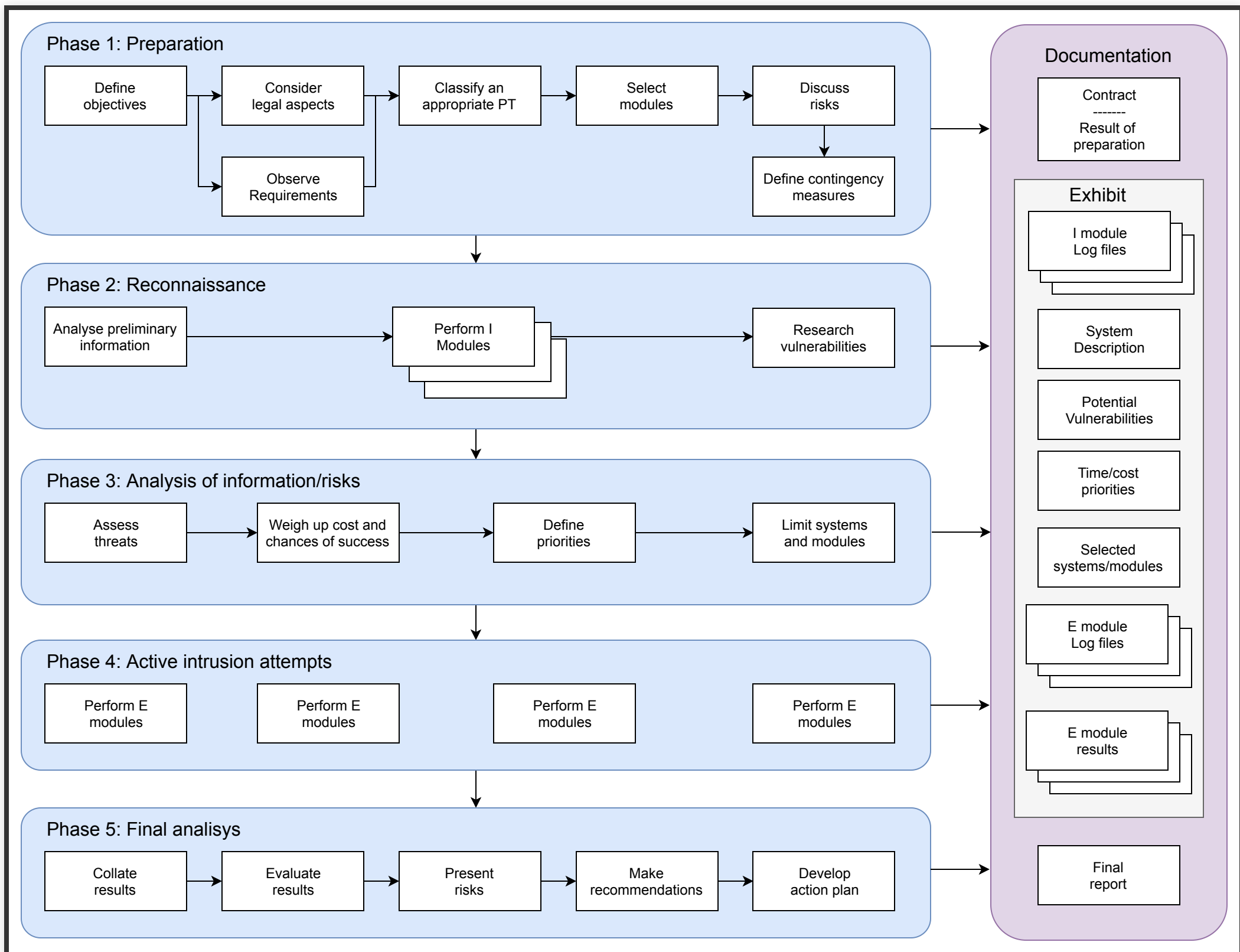
1. Cautious, covert black-box test can be carried out from the outside in a first step
2. Followed by an aggressive, overt white-box test from the inside.

Combines the advantages of a black-box test - a realistic simulation of a genuine attack - with the benefits of a white-box test in terms of efficiency and damage limitation.



# **METHODOLOGY AND EXECUTION**

Phases in Planning and Executing a Penetration Test



# PHASES OVERVIEW

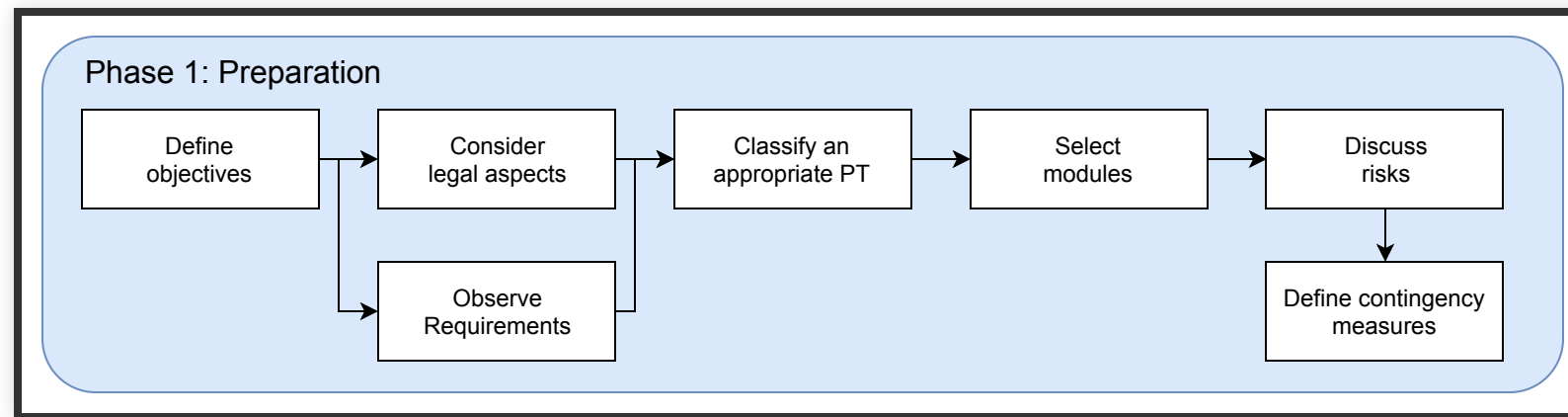
Different testing procedures which can be carried out in a penetration test have been grouped together in modules.

- **Phase 2:** "Reconnaissance" → I modules
- **Phase 4:** "Active intrusion" → E modules



We will discuss the phases with examples

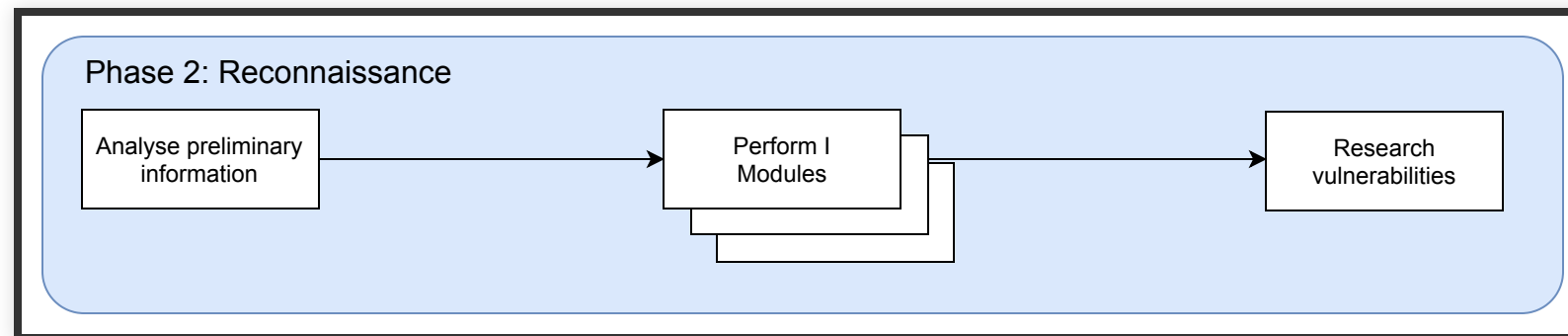
# PHASE 1: PREPARATION



# PHASE 1: PREPARATION

- Agree on scope and expectations (including economy)
- Based on classification: Define the modules to be used.
- Secure contract and legal matters are resolved
- Discuss risks
- **All details agreed to should be put in writing in the contract**

# PHASE 2: RECONNAISSANCE



💡 This phase is the passive penetration test.

# PRELIMINARY INFORMATION

**Goal:** Obtain a complete and detailed overview of the systems installed, including areas open to attack or known security shortcomings.

Can be timeconsuming if many IP's behind firewall

Highly dependent on type: Black-box vs. whitebox.

# I MODULES (EXAMPLES)

No.	Module
I1	Analysis of Published Data
I2	Covert Queries of Basic Network Information
I3	Overt Queries of Basic Network Information
I4	Stealthy Port Scans
I5	Noisy Port Scans



# 15 MODULE: NOISY PORT SCANS

A port scan is run on all identified devices in order to identify which services each device offers, and with which operating system.

- **Expected results:**
  - Information on the services offered by the device
  - Identification of the operating system
- **Requirements:**
  - Knowledge of basic network information
- **Test Steps → Effort**
  - Perform a normal port scan → Medium
- **Risks: None**

# EXAMPLE TOOL: NMAP

## Scan selected ports - ignore discovery

```
sudo nmap -sV -p 1-65535 62.198.248.41
```

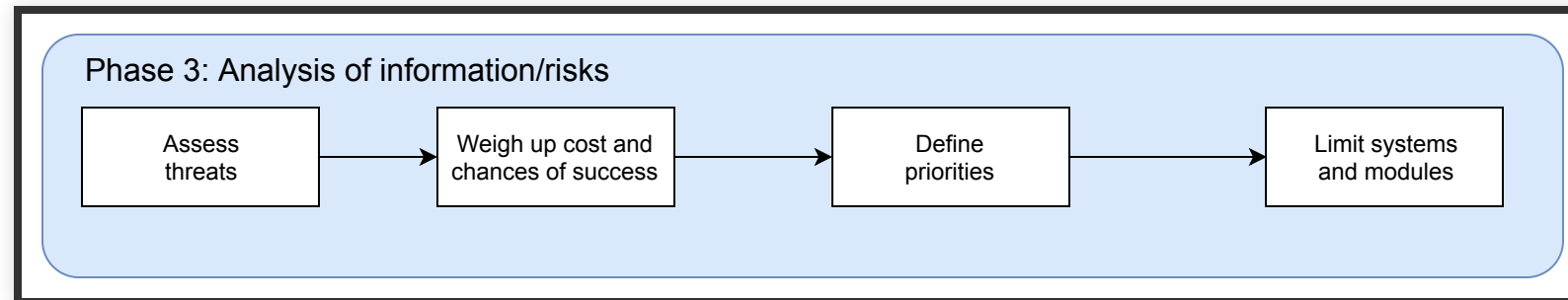
```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-11-24 14:04 CET
WARNING: Service 62.198.248.41:39763 had already soft-matched rtsp, but now soft-r
Nmap scan report for 0x3ec6f829.static.customer.dk.telia.net (62.198.248.41)
Host is up (0.0040s latency).
Not shown: 65524 closed ports
PORT      STATE      SERVICE      VERSION
53/tcp    open      domain
80/tcp    open      http         nginx
139/tcp   open      netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open      ssl/http     nginx
445/tcp   open      netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8080/tcp   filtered  http-proxy
9999/tcp   filtered  abyss
39763/tcp open      rtsp
41952/tcp open      upnp
44842/tcp open      unknown
60022/tcp open      ssh          Dropbear sshd (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.c
Nmap done: 1 IP address (1 host up) scanned in 6914.00 seconds
```

# RECONNAISSANCE TOOLS

Needed for Blackbox

- whois
- websiteinformer - <https://website.informer.com/>
- nmap
- spokeo.com
- osint (Open Source INteligence Tools) - Examples:
  - Shodan: <https://www.shodan.io/>
  - Spiderfoot: <https://www.spiderfoot.net/>
  - TheHarvester: <https://github.com/laramies/theHarvester>

# PHASE 3: ANALYZING INFORMATION AND RISKS

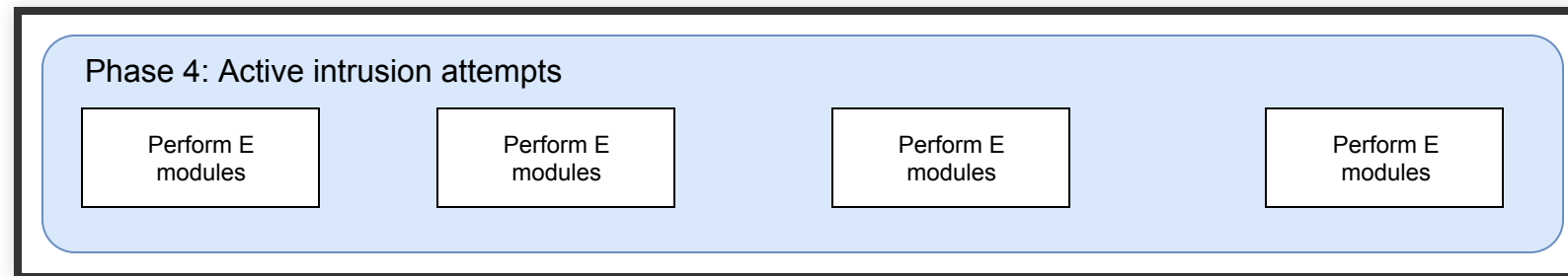


# PHASE 3: ANALYZING INFORMATION AND RISKS

- Evaluate the finding from phase 2
- Analysis must include
  - Defined goals of the penetration test
  - Potential risks to the system
  - Estimated time required for evaluating the potential security flaws for the subsequent active penetration attempts.

**Result:** Selected targets for phase 4

# PHASE 4: ACTIVE INTRUSION ATTEMPT



**Selected systems are actively assailed**

# PHASE 4: ACTIVE INTRUSION ATTEMPT

- This phase must be performed if a verification of potential vulnerabilities is required.
- Only this phase reveals the extent to which the supposed vulnerabilities identified in the reconnaissance phase present actual risks.
  - Just because there is a vulnerability in a used product, does not mean that component is actually used.
- Important to consider risks for systems with very high availability or integrity requirements

# E MODULES (EXAMPLES)

## Modules for Active Intrusion Attempts

No.	Module
E1	Covert Verification of Actual Vulnerabilities
E2	Overt Verification of Actual Vulnerabilities
E3	Overt Queries of Basic Network Information
E10	IDS System Testing
E11	Intercepting Passwords
E12	Password Cracking



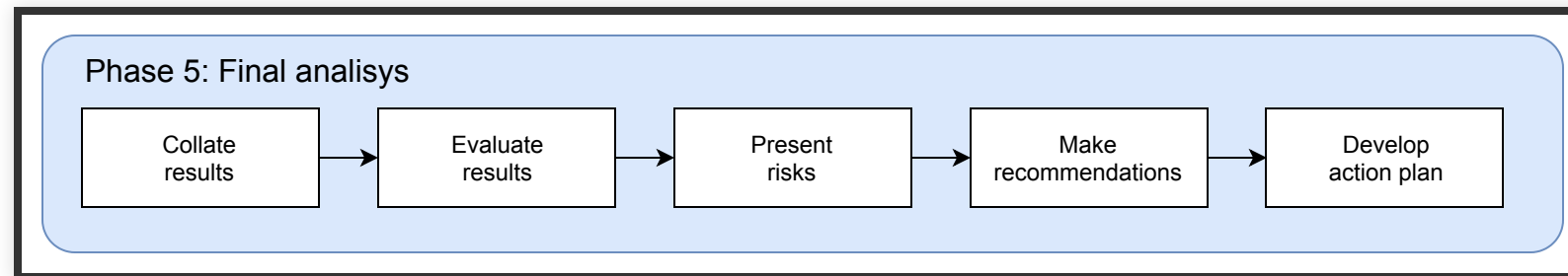
# SELECTING MODULES

Depending on the classification, some of the modules will be excluded.

Fx. if approach is covert  $\Rightarrow$  All overt modules are excluded.

This is both for I and E modules.

# PHASE 5: FINAL ANALYSIS



# PHASE 5: FINAL ANALYSIS

- Final report should contain an evaluation of the vulnerabilities located in the form of potential risks and recommendations for eliminating the vulnerabilities and risks.
- The report must guarantee the transparency of the tests and the vulnerabilities it disclosed.

# ELEMENTS IN THE REPORT

- Contract, including the results and agreements negotiated
- Documentation of the test steps completed for reconnaissance (I Modules) the log files of the tools used, including the list of vulnerabilities tested
  - System descriptions derived from these
- List of potential vulnerabilities, broken down according to system with a brief description

# ELEMENTS IN THE REPORT

- Results of the risk analysis (time/cost and priorities) and the systems or E modules selected on this basis for phase 4 (active intrusion attempts)
- Documentation of the modules completed for active intrusion attempts and the log files of the tools used
- Individual results of the E modules including the list of verified vulnerabilities

# SUMMARY

- Contract up front to handle scope, legal and ethical issues
- Classification of pen test important for content
- Documentation needed in all 5 phases
- Reconnaissance and active intrusion are separate phases with planning in between

# QUESTIONS

# RESOURCES

- <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publication>
- <https://hackertarget.com/nmap-tutorial/>
- <https://www.crest-approved.org/wp-content/uploads/CREST-Penetra>