AST

Audit de Sécurité Technique

Chapter 2.1

Security Assessments, Frameworks and Preparation

Jean-Marc Bost

jean-marc.bost@heig-vd.ch

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Table of contents

- Security Assessments
- Frameworks and methodologies
- Preparing your security project

Table of Contents

- **Security Assessments**
- Frameworks and methodologies
- Preparing your security project

Types of Security Engagements

- Many people use the following terms interchangeably and without fixed meaning
  - Security assessment
  - Vulnerability assessment
  - Ethical hacking
  - Penetration testing or pentesting
  - Security Audit

- Leads to a lot of confusion

Hacking

- **Hacking** = playing with systems and making them do what they were never intended to do; hacking is also about freedom of speech and free access to information -- being able to find out anything
- **Ethic** = a set of moral principles, relating to a specified group, field, or form of conduct
- **Ethical hacking** = mastery of attack techniques needed to find security flaws in systems with the unique aim of improving their security, respectful of applying ethical rules
- **Hackers' hats** = colour of hacker's motivations
  - White hat = ethical hacker
  - Grey hat = in between, e.g. activist
  - Black hat = malicious hacker

Pentesting

- **Pentesting (Penetration testing)** = aimed at finding vulnerabilities, malicious content, flaws, and risks. This is an official procedure that can be deemed helpful and not a harmful attempt. It forms part of an ethical hacking process, specifically focusing on penetrating the information system.

“ethical hacking is like learning all the technical aspects of driving a vehicle, versus penetration testing, where you put all those acquired skills together to drive the car”

Why pentest ?

Find vulnerabilities before bad guys do and thus…

… allow the organisation to concretely realize the risk

- convincing evidences about the probability that a given vulnerability might be exploited
  - f (hacker's skills, time available)
- concrete discussions allowing to evaluate the impact on the systems and business

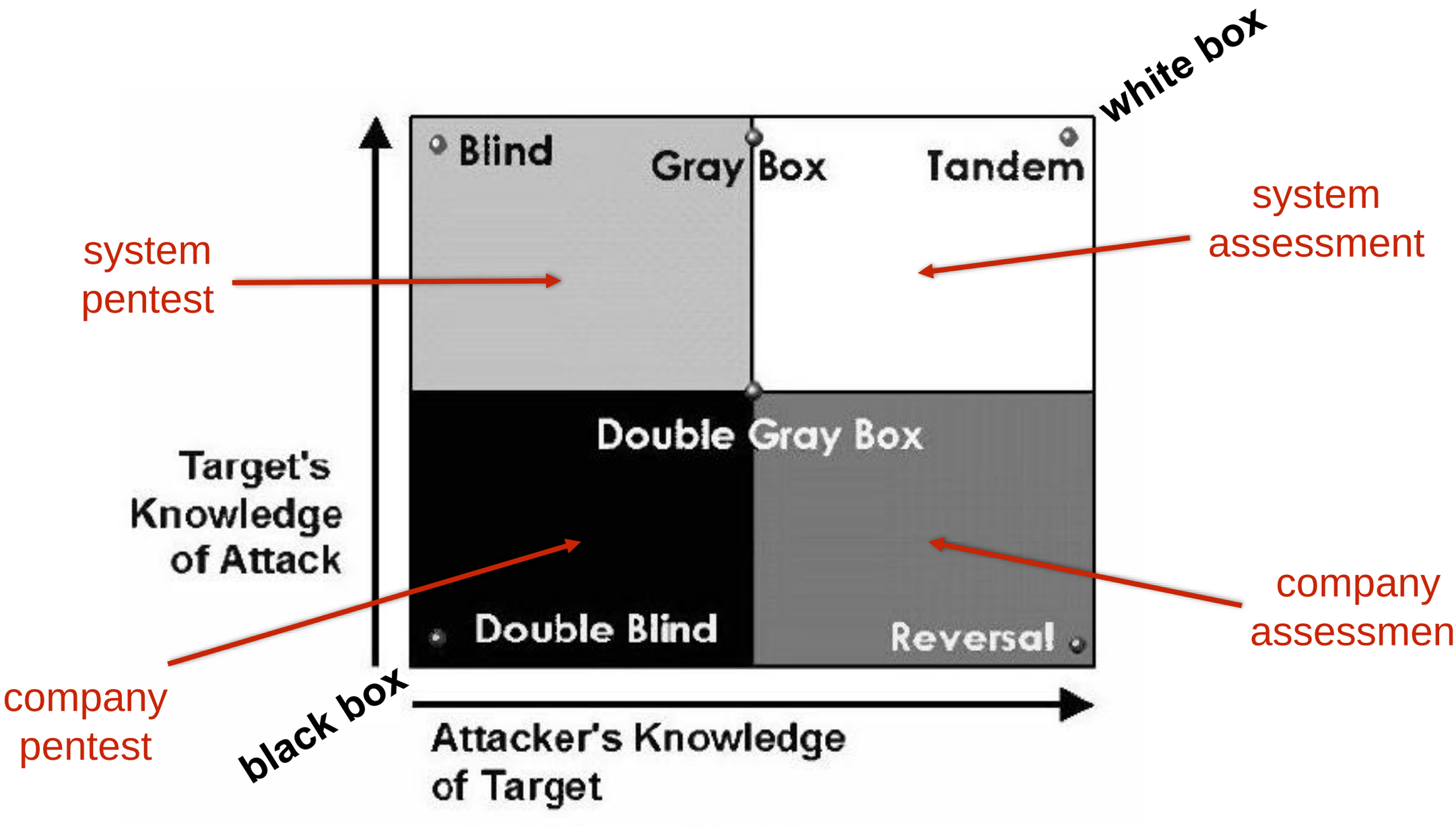
Other activities

- **Vulnerability assessment** = finding vulnerabilities without actually exploiting them and getting in
- **Security assessment** = analyzing the security of a system usually by performing a vulnerability assessment followed by the analysis of the impact and resulting risk
  - broader than pentesting
  - pentesting is intended to be more vertical (e.g. one specific application or business domain)
- **Security audit** = obtaining audit evidences and objectively evaluating them to determine the extent to which the audit criteria are fulfilled

Targets

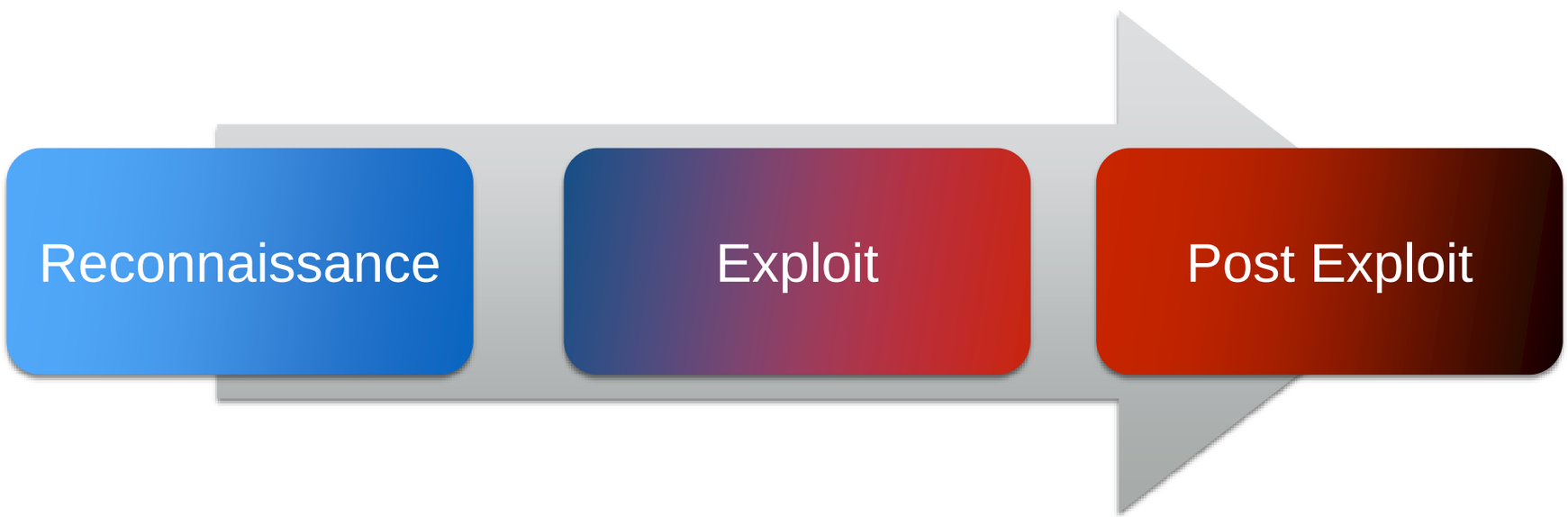
- **Network services** - looking for vulnerabilities on the target systems on the network and exploiting them. Systems can be publicly facing or located within the target's premises (internal network).
- **Client-side** - finding and exploiting vulnerabilities in the client-side software (browsers, media players, etc..)
- **Web application** - looking and exploiting vulnerabilities in web-based applications
- **Mobile application** - looking and exploiting vulnerabilities in mobile applications on iOS/Android platforms
- **Wireless security** - looking for unauthorised wireless AP or AP with security weaknesses
- **Social engineering** - forcing user to reveal sensitive information
- **Stolen equipment** - involves obtaining a piece of equipment from the target (e.g. corporate laptop computer) and trying to extract sensitive information from it
- **Cryptanalysis attack** - bypassing or breaking the encryption on a local system or across the network. Can also involve evaluation of digital rights management (DRM) solution.
- **Product security** - looking for security flaws in software products (exploitable buffer overflows, privilege escalation, exposure of unencrypted sensitive data)

Working contexts



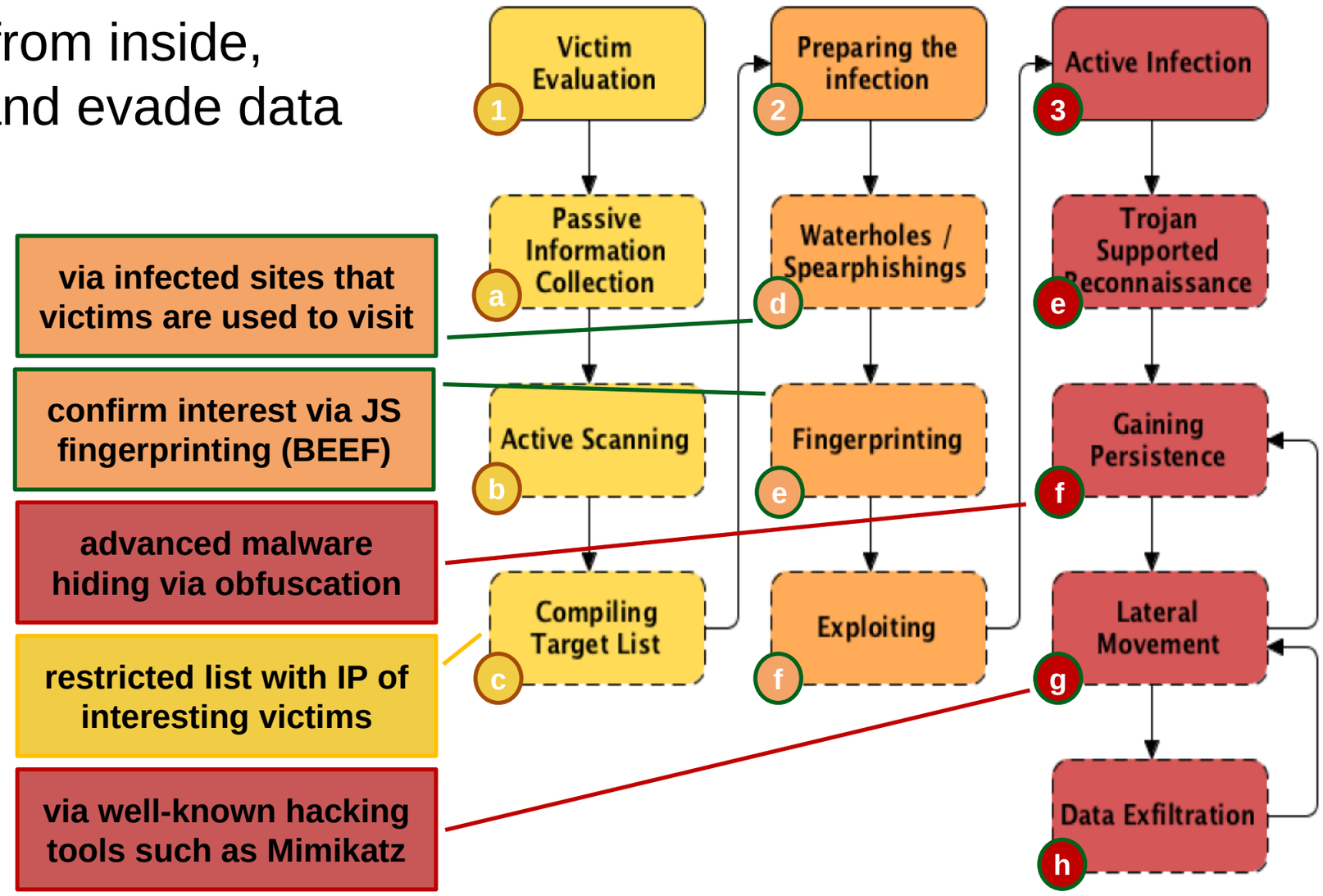
Attack Kill Chain

- Malicious and ethical hacker rely on same phases in their attacks
  - **Reconnaissance** - gathering information about target
    - Scanning - finding openings in the perimeter
  - **Exploitation** - exploit target systems to compromise them, possibly getting control of them or causing a denial of service
  - **Keeping control** and covering tracks (mostly black-hat and red teams)



Cyber-kill chain (RUAG case)

1. learn about victims, prepare traps
2. Incrementally trap the victims via waterholes or spearphishing
3. learn more from inside, propagate and evade data



GovCERT.ch

Limitations of Pentest

- Penetration testing cannot find all vulnerabilities in a target environment
- Constraints and limitations of a test
  - Project-oriented
    - Scope limit
    - Time limit
    - Access limit
    - Method limit
      - E.g. no Denial of Service to perform distraction
  - Other factors
    - Skills
    - Imagination
    - Known exploits
      - Majority don’t write their own exploits or do not have enough time to write an exploit for a specific flaw found in a specific environment

Table of Contents

- Security Assessments
- **Frameworks and methodologies**
- Preparing your security project

Testing methodology

- Approach to testing, so that the pentest is carried out systematically and professionally. Absence of methodology leads to:
  - Incomplete pentest
  - Time consuming pentest
  - Waste of effort
  - Ineffective pentest - results do not suit the requirements
- Methodology is your map to reach your end result and without it you will get lost.

Public/Free Pentest methodologies

- Best methodologies include:
  - Penetration Testing Execution Standard (**PTES**) - http://www.pentest-standard.org/
  - Open Source Security Testing Methodology Manual (**OSSTMM**) - http://www.isecom.org/research/osstmm.html
  - Open Web Application Security Project (**OWASP**) Testing Guide - https://www.owasp.org/index.php/OWASP_Testing_Project
  - **NIST** Special Publication 800-115: Technical Guide to Information Security Testing and Assessment - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
  - Penetration Testing Framework - http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Penetration Testing Execution Standard (PTES)

- Aims at creating a standard so that organisations are able to understand what is involved in conducting a penetration test
- Includes information about:
  - Pre-engagement interactions (scoping and rules of engagement)
  - Intelligence gathering (Reconnaissance)
  - Threat modelling
  - Vulnerability analysis
  - Exploitation and Post exploitation
  - Reporting
- Great outline of an in-depth penetration test

Open Source Security Testing Methodology Manual

- Focus is on transparency and getting business value
- Aims at repeatability, consistency and high quality of results
- Broad description of categories of testing
  - Step-by-step process description without going too deep with particular tools and commands
- Covers scoping, metrics, human security testing, physical security, wireless security, telco security, data network security
- Includes information-gathering templates

NIST Guidelines on Network Security Testing

- Covers planning, process, analysis and validation methods
- Includes an appendix with Rules of Engagement template
- Another NIST document, The Guide for Assessing the Security Controls in Federal Information Systems, Special Publication 800-53A is more high-level, but provides some tips on how to plan security assessments.

National Institute of Standards and Technology
U.S. Department of Commerce

OWASP Testing Guide

- Focus is on Web Application Testing
  - Goes deep into techniques and tools
  - Information gathering
  - Business logic testing
  - Authentication testing
  - Session management testing
  - Data validation testing
  - DoS testing
  - Web services testing
  - Ajax testing
- Detailed description of determining the business risk posed by findings.
  - Rates risk based on the impact it could have on the business and likelihood of occurring

OWASP
Open Web Application Security Project

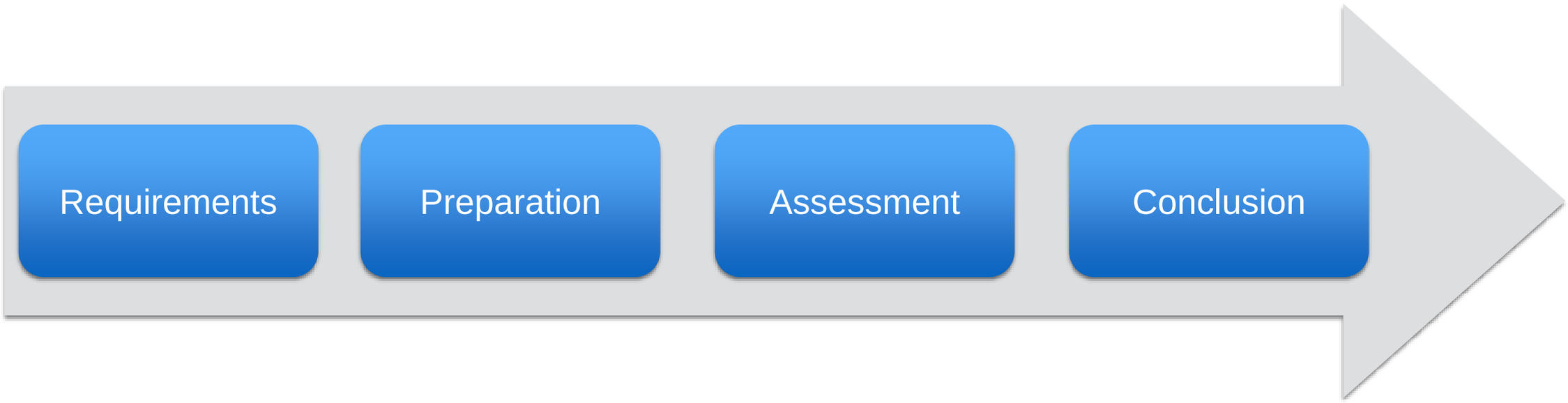
Penetration Testing Framework

- Focus on network penetration tests
- Very deep, with specific tools and commands
- Step-by-step, with links to tools
- Recon, Social Engineering, Scanning, Enumeration

Table of Contents

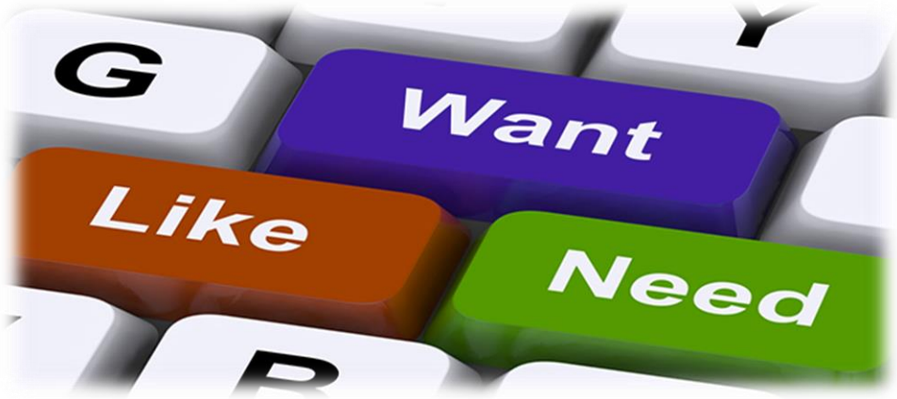
- Security Assessments
- Frameworks and methodologies
- **Preparing your security project**

Security project high-level view



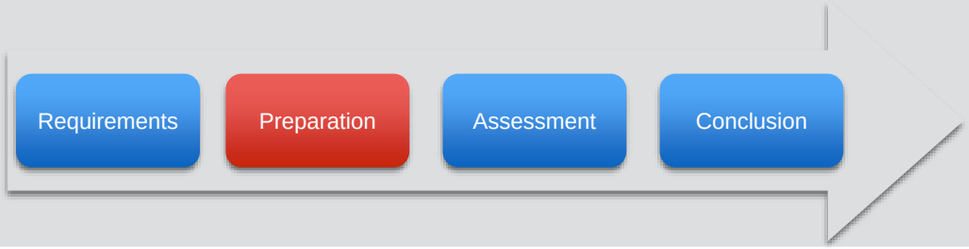
Requirements

Usually based on a Request of Proposal or a business discussion with a prospective customer



- You should get an idea of
  - Context of the organisation
  - High-level project description
  - Requirements (« cahier des charges »)
    - Main deliverables - what the customer expects from the work
      - Depending on the project and customer (e.g. non-expert), the customer might have a very vague idea
      - It is up to you, as a security expert, to frame the deliverable up to a certain point
    - Timeframe - start, finish, how long the customer expects the project to last
- Always keep in mind the high-level goals - Risks, assets and impact on business

Preparation



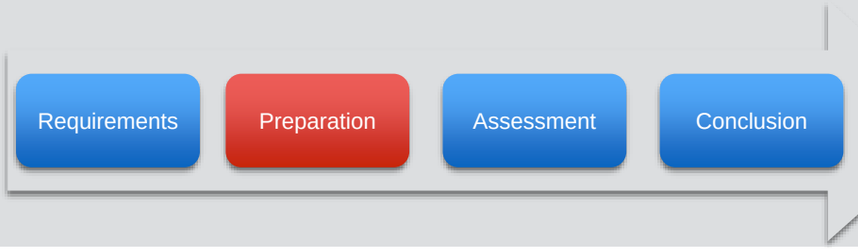
Preparation is THE critical step in your security project

- If neglected, high risk to miss the objectives

- Taking as input information from the Requirement step, you perform the scoping and planning of the project
  - Non-disclosure Agreement (NDA), if applicable
  - Biggest business risks and concerns
  - Rules of Engagement
  - Scope of work
  - Permission to test document
  - Assign the team

- Preparation is performed along discussions with your customer

Permission to test



As a third-party penetration tester, get a signed memo giving you the permission to perform offensive testing!

- E.g. http://www.counterhack.net/permission_memo.html

Memorandum for File

Subject: Vulnerability Assessment and Penetration Testing Authorization

Date: MMDDYY

To properly secure this organization's information technology assets, the information security team is required to assess our security stance periodically by conducting vulnerability assessments and penetration testing. These activities involve scanning our desktops, laptops, servers, network elements, and other computer systems owned by this organization on a regular, periodic basis to discover vulnerabilities present on these systems. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment.

The purpose of this memo is to grant authorization to specific members of our information security team to conduct vulnerability assessments and penetration tests against this organization's assets. To that end, the undersigned attests to the following:

1) [Insert name of tester], [Insert name of tester], and [Insert name of tester] have permission to scan the organization's computer equipment to find vulnerabilities. This permission is granted for from [insert start date] until [insert end date].

2) [Insert name of approver] has the authority to grant this permission for testing the organization's Information Technology assets.

[Insert additional permissions and/or restrictions if appropriate.]

Signature: _____ Signature: _____

[Name of Approver] [Name of Test Team Lead]

[Title of Approver] [Title of Test Team Lead]

Date: _____ Date: _____

Permission to test

Memorandum for File

Subject: Vulnerability Assessment and Penetration Testing Authorization

Date: MMDDYY

To properly secure this organization's information technology assets, the information security team is required to assess our security stance periodically by conducting vulnerability assessments and penetration testing. These activities involve scanning our desktops, laptops, servers, network elements, and other computer systems owned by this organization on a regular, periodic basis to discover vulnerabilities present on these systems. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment.

The purpose of this memo is to grant authorization to specific members of our information security team to conduct vulnerability assessments and penetration tests against this organization's assets. To that end, the undersigned attests to the following:

1) [Insert name of tester], [Insert name of tester], and [Insert name of tester] have permission to scan the organization's computer equipment to find vulnerabilities. This permission is granted for from [insert start date] until [insert end date].

2) [Insert name of approver] has the authority to grant this permission for testing the organization's Information Technology assets.

[Insert additional permissions and/or restrictions if appropriate.]

Signature: _____ Signature: _____

[Name of Approver] [Name of Test Team Lead]

[Title of Approver] [Title of Test Team Lead]

Date: _____ Date: _____

Liability limitation

By itself, the permission to test is not enough

- Limitations of liability agreement in contractual language is required
- Should be written by a lawyer
- Usually the liability is limited to the value of the project
- Most information security companies carry liability insurance and errors and omissions insurance

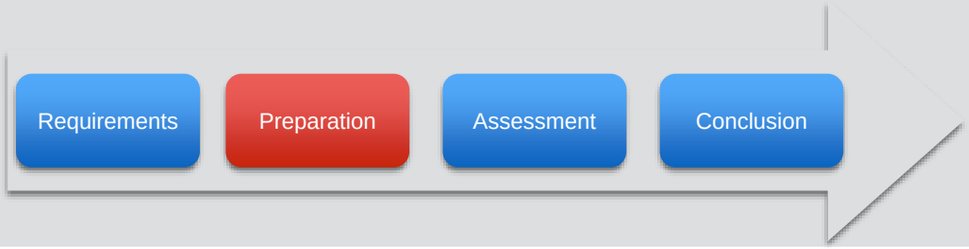
Scoping

The scope document defines **WHAT** will be tested

- Often one of the most overlooked part of preparation

- The key matter of the exercise is to determine where you should spend your energy and effort
- Customer might have no clue about what to test
  - The usual reply is everything
- At kick-off, determine with the customer what are its biggest security concerns:
  - Disclosure of sensitive information
  - Interruption of production processing
  - Embarrassment due to defacement of a website
  - Hijacking of valuable online transactions
  - Rebound attack on customers partners
  - ...

Scoping - Scope creep

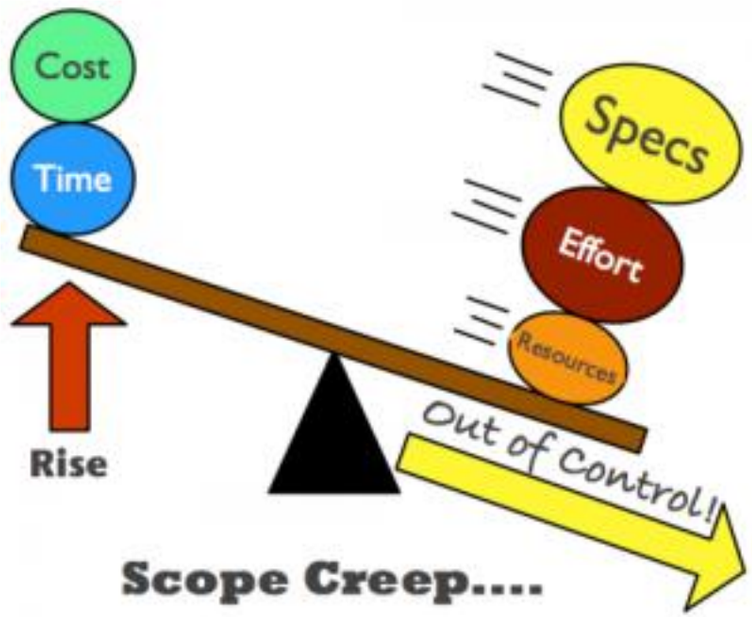


Scope creep: misunderstand what is included and what is not

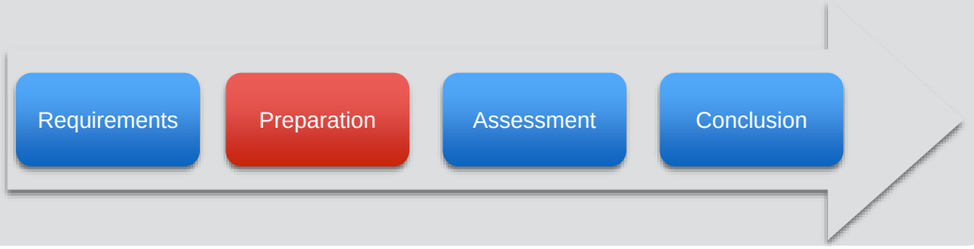
- The customer later adds more systems, networks, types of testing

⇒ kill your project and your relationship with your customer

- Keep focused
  - Set priority on known vulnerabilities, likely threats and perceived risks
  - Suggest to include low-hanging fruit first
- Specify start and end dates



Scoping - what to test



Establish a clear and explicit scope for the project

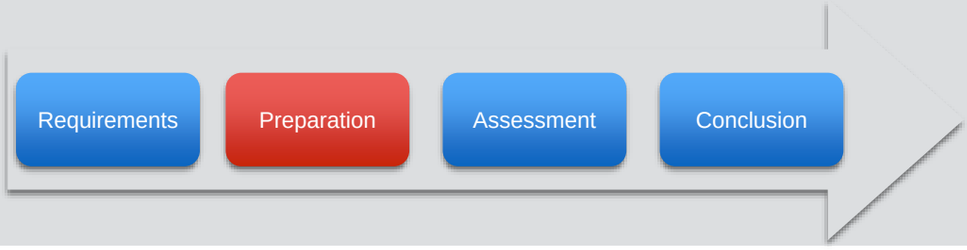
- for a pentest, explicitly state what is to be tested
  - Domain names
  - Network IP ranges
  - Individual hosts
  - Particular applications

Furthermore, explicitly state what will be excluded

- E.g. social engineering, wireless network test, exploitation of targets

- in a pentest
  - important to determine whether any network equipement - Firewalls, IDS/IPS, load balancers are present between you and your targets
  - Any third-party equipment (e.g. cloud environment)

Scoping - 3rd parties



Before you start, validate that your targets are owned by the customer

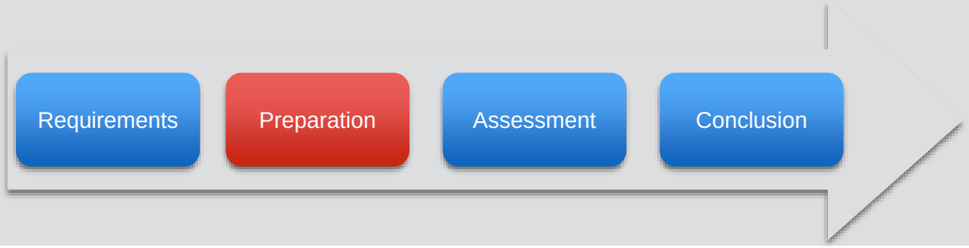
- Make sure to get a written permission to test the equipment/data of any third parties (e.g. routers, mail servers, DNS)
- Web hosting companies
  - Single web server housing several companies web sites
- Cloud providers
  - Public vs private cloud
  - Many cloud providers have explicit procedures for penetration testing
  - May forbid the testing and send you their last pentest report
  - Some may allow application-level testing and forbid the network testing

Scoping – target env

Do you conduct your security assessments on test or production environment?

- for a pentest, beware of impact to operations!
  - Ideally run it against a test or pre-production environment
  - Otherwise…
    - … test during off-hours, weekends, …
    - … ask for backups, restore procedures, restart support, …

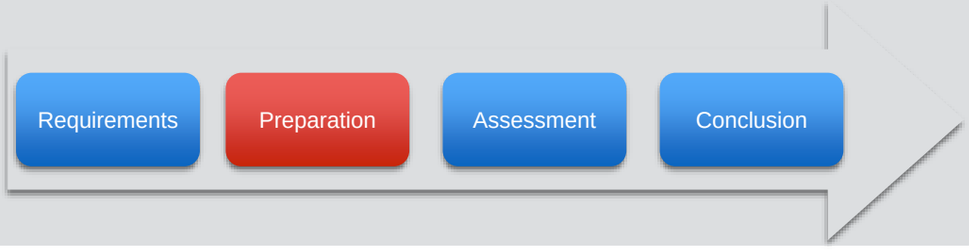
Scoping - activities



State in the scope what will be done

- for a pentest
  - Ping sweep of network ranges (host discovery)
  - Port scan of alive hosts
  - Vulnerability scan of alive hosts
  - Exploitation of vulnerabilities discovered on services
  - Exploitation of client-side software
  - Application-level exploitation
  - Social engineering
- for ISO 27001 recommendations
  - Look into specific clauses and controls
  - Assess if the related part of the ISMS has been implemented

Rules of Engagement



The RoE document defines **HOW** the project will occur

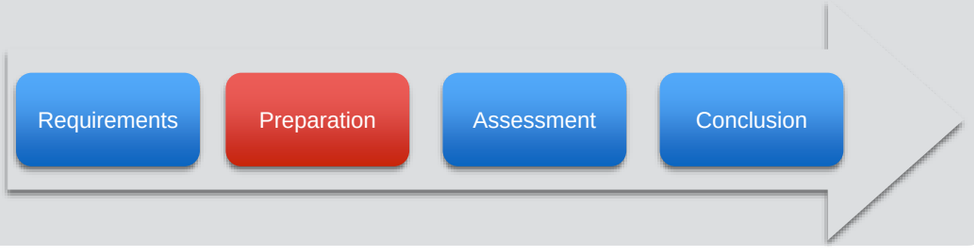
- Separate document from Scope

- Without RoE some value is lost - wasted effort
- Potential conflicts with customer might arise
- Sometimes the RoE is defined before defining the scope, and sometimes RoE is defined around the scope
- For Scope and RoE the process may be iterative

RoE - communication?

- Emergency contact information for customer and service provider
  - Name, mobile phone number
- Method for exchanging data
  - Encryption for sensitive data such as vulnerability details and final report
  - GnuPG and PGP
  - Encrypted ZIP files are less secure but better than…
- Debriefing meetings
  - Frequency (e.g. daily or twice per week)
  - Can be just half-hour long
  - Ensures that everyone is on the same page and to avoid surprises
  - What the team has done during a given period, any issues and plan for next days

RoE - when and where?

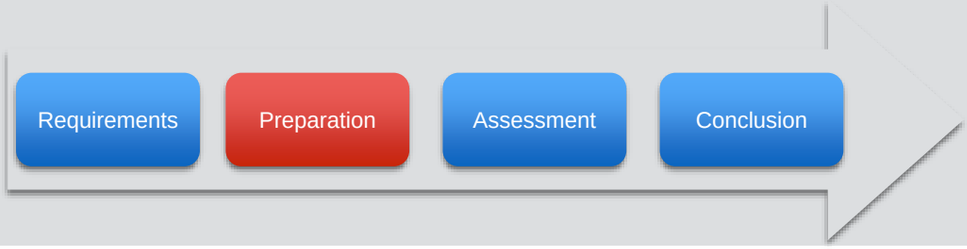


- Agreement on an explicit start date and finish date

Start	End	Month	Year	Phases
12th May 2013	18th	May	2013	Scope Definition
19th May 2013	27th	May	2013	Reconnaisance
28th May 2013	2th	June	2013	Scanning
3rd june 2013	16th	june	2013	Exploitation
17th June 2013	21th	June	2013	POST Exploitation
21st June 2013	28th	June	2013	Reporting

- Clear timeline for the project
  - GANTT charts or Work Breakdown Structures
  - Helps to get an idea where resources need to be applied and identify possible roadblocks
- Agreement on acceptable times for specific tasks
  - Production environments
  - Evening/WE-only tasks
- Locations
  - On-premises vs remotely
  - Number of locations with an exact address
  - Necessary access to locations: clearing, VPN, 2FA, …

RoE - blind? how far?



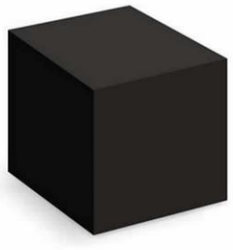
Are we measuring the ability of the security to respond to an attack?

- Who is aware of the project?
  - system administrators?
  - security Operations team?
- for a pentest,
  - security staff/tools might detect the attacks/scans and block traffic
    - then, be ready to congratulate staff and ask for whitelisting for the next steps
  - report your findings on security: reaction time, efficiency

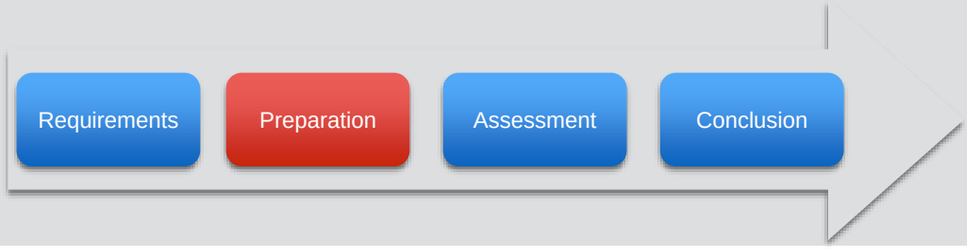
RoE - black- or white-box?

Act as a blind attacker or assume recon steps already done?

- for penetration testing,
  - Black-box = only use the information you collect yourself.
    - Much more time consuming and expensive
    - … but close to reality
  - White-box = agree to disclose information about targets
    - Not to loose time and money
    - E.g. architecture documents, configuration, network topology, …
    - Still reality, in a scenario where the attacker has already this information
- Grey-box = hybrid approaches = disclose some information



RoE - privacy!



Agree in the RoE on how to proceed when you have successfully compromised a system

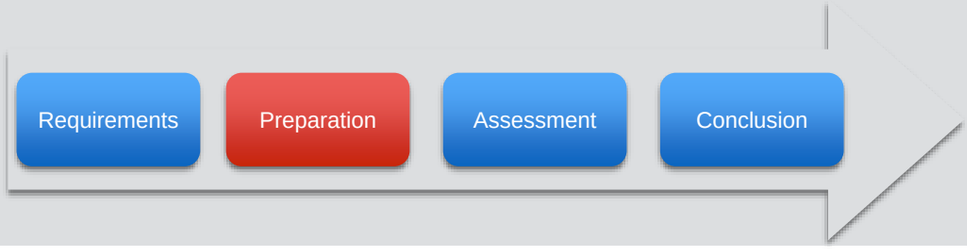
- Usually, you must agree on the rights to

  (during a debrief meeting)

  - use the system as a pivot
  - review the system’s configuration

- … but include a clause that you will not look at, nor report about sensitive data
  - Especially on production environments
  - … but also on pre-prod and test env carrying samples of sensitive data
  - Otherwise, risk of violating privacy regulations and directives!

More



- Make sure to take a look at the pre-engagement description of penetration testing standard at:

  http://www.pentest-standard.org/index.php/Pre-engagement