

# Advanced security methodologies - Penetration testing

M2SSIC-Metz

Pascal Steichen

## 1 Hacking for money

- Motivations
- Limitations

## 2 IS and pentesting

- Classification (taxonomy)
- Contract
- Obligations
- Requirements
- Skills
- Techniques
- Ethical issues
- Report

## 3 Usual suspects

# Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.

# Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.
- **Tools:** Well the same as the bad guys: nmap, metasploit, dsniff ...

# Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.
- **Tools:** Well the same as the bad guys: nmap, metasploit, dsniff ...
- **Method:**

# Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.
- **Tools:** Well the same as the bad guys: nmap, metasploit, dsniff ...
- **Method:**
  - contract with "victim"

# Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.
- **Tools:** Well the same as the bad guys: nmap, metasploit, dsniff ...
- **Method:**
  - contract with "victim"
  - hack, but don't break anything

# Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.
- **Tools:** Well the same as the bad guys: nmap, metasploit, dsniff ...
- **Method:**
  - contract with "victim"
  - hack, but don't break anything
  - keep confidential information confidential

# Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.
- **Tools:** Well the same as the bad guys: nmap, metasploit, dsniff ...
- **Method:**
  - contract with "victim"
  - hack, but don't break anything
  - keep confidential information confidential
  - write a detailed report

## Motivations

- Evaluation of own security concepts

## Motivations

- Evaluation of own security concepts
- To convince management (for budget)

## Motivations

- Evaluation of own security concepts
- To convince management (for budget)
- To bypass "corporate blindness"

## Motivations

- Evaluation of own security concepts
- To convince management (for budget)
- To bypass "corporate blindness"
- Fear of industry espionage, real attacks, etc.

## Motivations

- Evaluation of own security concepts
- To convince management (for budget)
- To bypass "corporate blindness"
- Fear of industry espionage, real attacks, etc.
- Compliance with legal framework

## Motivations

- Evaluation of own security concepts
- To convince management (for budget)
- To bypass "corporate blindness"
- Fear of industry espionage, real attacks, etc.
- Compliance with legal framework
- Get independent advice

## Motivations

- Evaluation of own security concepts
- To convince management (for budget)
- To bypass "corporate blindness"
- Fear of industry espionage, real attacks, etc.
- Compliance with legal framework
- Get independent advice
- Image gain

## Limitations

- It's a "photographer's" approach

## Limitations

- It's a "photographer's" approach
- No guarantee that a successful attack will not occur

## Limitations

- It's a "photographer's" approach
- No guarantee that a successful attack will not occur
- It does not replace the general security policy nor the usual IT security tests (remember: security is a process)

# IS and pentesting

- Blackbox

# IS and pentesting

- Blackbox
  - little or no prior knowledge

# IS and pentesting

- Blackbox
  - little or no prior knowledge
  - all information needs to be researched

# IS and pentesting

- Blackbox
  - little or no prior knowledge
  - all information needs to be researched
  - simulate external attacker

# IS and pentesting

- Blackbox
  - little or no prior knowledge
  - all information needs to be researched
  - simulate external attacker
- Whitebox

# IS and pentesting

- Blackbox
  - little or no prior knowledge
  - all information needs to be researched
  - simulate external attacker
- Whitebox
  - nearly full-knowledge about organisation/systems

# IS and pentesting

- Blackbox
  - little or no prior knowledge
  - all information needs to be researched
  - simulate external attacker
- Whitebox
  - nearly full-knowledge about organisation/systems
  - simulate internal attacker

The methods of pentesting can vary depending on the way the target systems are being attacked:

- Network-based attacks

The methods of pentesting can vary depending on the way the target systems are being attacked:

- Network-based attacks
  - wireless/mobile (WiFi, bluetooth, Iphone, blackberry...)

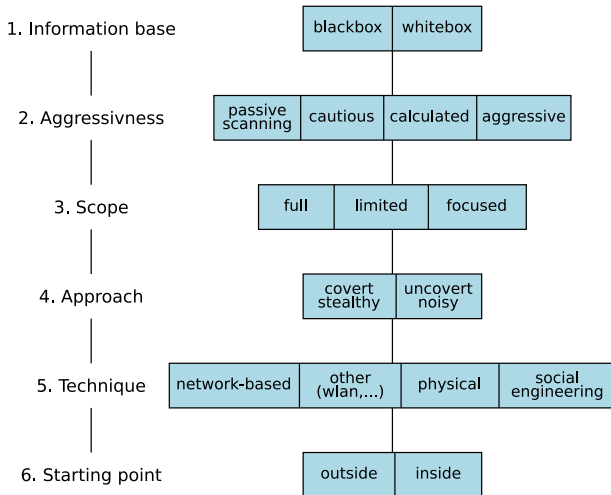
The methods of pentesting can vary depending on the way the target systems are being attacked:

- Network-based attacks
  - wireless/mobile (WiFi, bluetooth, Iphone, blackberry...)
- Social engineering

The methods of pentesting can vary depending on the way the target systems are being attacked:

- Network-based attacks
  - wireless/mobile (WiFi, bluetooth, Iphone, blackberry...)
- Social engineering
- Circumvention of physical security measures

## Classification (taxonomy)



## Contract

- Objective(s) of the penetration test

## Contract

- Objective(s) of the penetration test
  - Increasing the security of the technical systems,

## Contract

- Objective(s) of the penetration test
  - Increasing the security of the technical systems,
  - Identifying vulnerability as a criterion for making decisions (e.g. for investments or the suitability of products),

## Contract

- Objective(s) of the penetration test
  - Increasing the security of the technical systems,
  - Identifying vulnerability as a criterion for making decisions (e.g. for investments or the suitability of products),
  - Obtaining certification/confirmation from an external third party,

## Contract

- Objective(s) of the penetration test
  - Increasing the security of the technical systems,
  - Identifying vulnerability as a criterion for making decisions (e.g. for investments or the suitability of products),
  - Obtaining certification/confirmation from an external third party,
  - Increasing the security of the organizational/personnel infrastructure.

## Contract

- Objective(s) of the penetration test
  - Increasing the security of the technical systems,
  - Identifying vulnerability as a criterion for making decisions (e.g. for investments or the suitability of products),
  - Obtaining certification/confirmation from an external third party,
  - Increasing the security of the organizational/personnel infrastructure.
- Nature of the penetration test

## Contract

- Objective(s) of the penetration test
  - Increasing the security of the technical systems,
  - Identifying vulnerability as a criterion for making decisions (e.g. for investments or the suitability of products),
  - Obtaining certification/confirmation from an external third party,
  - Increasing the security of the organizational/personnel infrastructure.
- Nature of the penetration test
- Techniques to be used and excluded

## Contract

- Objective(s) of the penetration test
  - Increasing the security of the technical systems,
  - Identifying vulnerability as a criterion for making decisions (e.g. for investments or the suitability of products),
  - Obtaining certification/confirmation from an external third party,
  - Increasing the security of the organizational/personnel infrastructure.
- Nature of the penetration test
- Techniques to be used and excluded
- Joker

## Obligations

- The Client

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test
  - Information from potentially affected third persons

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test
  - Information from potentially affected third persons
  - Protective measures for unforeseeable system failure

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test
  - Information from potentially affected third persons
  - Protective measures for unforeseeable system failure
- The Testers

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test
  - Information from potentially affected third persons
  - Protective measures for unforeseeable system failure
- The Testers
  - Secrecy

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test
  - Information from potentially affected third persons
  - Protective measures for unforeseeable system failure
- The Testers
  - Secrecy
  - Compliance with licensing regulations

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test
  - Information from potentially affected third persons
  - Protective measures for unforeseeable system failure
- The Testers
  - Secrecy
  - Compliance with licensing regulations
  - Documenting the testing procedures and results

## Obligations

- The Client
  - Provision of information depending on the nature of the penetration test
  - Information from potentially affected third persons
  - Protective measures for unforeseeable system failure
- The Testers
  - Secrecy
  - Compliance with licensing regulations
  - Documenting the testing procedures and results
  - General duty of due care

## Requirements

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?

## Requirements

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?
- Have the liability risks received appropriate consideration?

## Requirements

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?
- Have the liability risks received appropriate consideration?
- What needs to be considered in respect of the time of testing?

## Requirements

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?
- Have the liability risks received appropriate consideration?
- What needs to be considered in respect of the time of testing?
- What needs be done in the event of system failure or other emergency?

## Requirements

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?
- Have the liability risks received appropriate consideration?
- What needs to be considered in respect of the time of testing?
- What needs be done in the event of system failure or other emergency?
- Which of the client's employees are affected by the penetration test?

## Requirements

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?
- Have the liability risks received appropriate consideration?
- What needs to be considered in respect of the time of testing?
- What needs be done in the event of system failure or other emergency?
- Which of the client's employees are affected by the penetration test?
- How much time and cost will the penetration test involve for the client?

## Requirements

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?
- Have the liability risks received appropriate consideration?
- What needs to be considered in respect of the time of testing?
- What needs be done in the event of system failure or other emergency?
- Which of the client's employees are affected by the penetration test?
- How much time and cost will the penetration test involve for the client?
- How much time and effort will the penetration test require of the tester?

## Skills

- Knowledge of system administration/operating systems

## Skills

- Knowledge of system administration/operating systems
- Knowledge of TCP/IP and, if applicable, other network protocols

## Skills

- Knowledge of system administration/operating systems
- Knowledge of TCP/IP and, if applicable, other network protocols
- Knowledge of programming languages

## Skills

- Knowledge of system administration/operating systems
- Knowledge of TCP/IP and, if applicable, other network protocols
- Knowledge of programming languages
- Knowledge of IT security products such as firewalls, intrusion detection systems

## Skills

- Knowledge of system administration/operating systems
- Knowledge of TCP/IP and, if applicable, other network protocols
- Knowledge of programming languages
- Knowledge of IT security products such as firewalls, intrusion detection systems
- Knowledge of how to handle hacker tools and vulnerability scanners

## Skills

- Knowledge of system administration/operating systems
- Knowledge of TCP/IP and, if applicable, other network protocols
- Knowledge of programming languages
- Knowledge of IT security products such as firewalls, intrusion detection systems
- Knowledge of how to handle hacker tools and vulnerability scanners
- Knowledge of applications/application systems

## Skills

- Knowledge of system administration/operating systems
- Knowledge of TCP/IP and, if applicable, other network protocols
- Knowledge of programming languages
- Knowledge of IT security products such as firewalls, intrusion detection systems
- Knowledge of how to handle hacker tools and vulnerability scanners
- Knowledge of applications/application systems
- Creativity

# Techniques

## 1 Preparation

## Techniques

- 1 Preparation
- 2 Reconnaissance

## Techniques

- 1 Preparation
- 2 Reconnaissance
- 3 Enumeration

## Techniques

- 1 Preparation
- 2 Reconnaissance
- 3 Enumeration
- 4 Exploitation

## Techniques

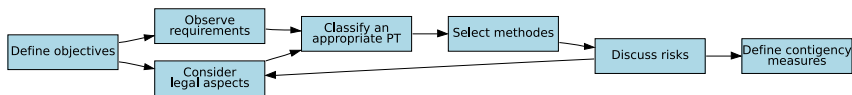
- 1 Preparation
- 2 Reconnaissance
- 3 Enumeration
- 4 Exploitation
- 5 Reporting

## Techniques

- 1 Preparation
  - 2 Reconnaissance
  - 3 Enumeration
  - 4 Exploitation
  - 5 Reporting
- Documentation (throughout the process)

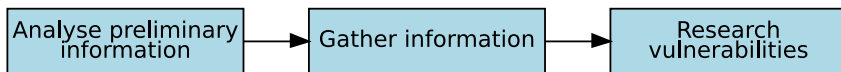
## Techniques

# 1. Preparation



## Techniques

### 2. Reconnaissance



## Techniques

### 3. Enumeration (analysing information and risks)

- Scan target systems for services.

## Techniques

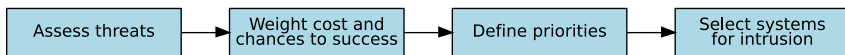
### 3. Enumeration (analysing information and risks)

- Scan target systems for services.
- Identify systems and applications.

## Techniques

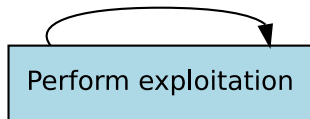
### 3. Enumeration (analysing information and risks)

- Scan target systems for services.
- Identify systems and applications.
- Researching Vulnerabilities.



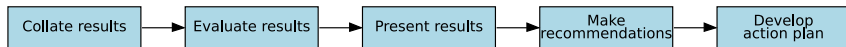
## Techniques

#### 4. Exploitation (active intrusion attempts)



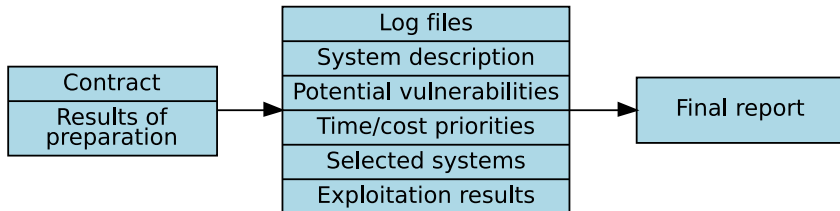
## Techniques

## 5. Reporting (final analysis)



## Techniques

## Documentation



## Ethical issues

- Usage of *social engineering* techniques should be clarified and justified.

## Ethical issues

- Usage of *social engineering* techniques should be clarified and justified.
- *Exploitation of vulnerabilities* (to what extent) should be discussed.

## Ethical issues

- Usage of *social engineering* techniques should be clarified and justified.
- *Exploitation of vulnerabilities* (to what extent) should be discussed.
- A penetration test is ever only a commissioned activity (any proactive behaviour is unacceptable, i.e. launching an attack attempt without a mandate should always be considered a punishable attack).

## Ethical issues

- **Social engineering**

## Ethical issues

- **Social engineering**
  - It works because, humans are

## Ethical issues

- **Social engineering**
  - It works because, humans are
    - amiable,

## Ethical issues

- **Social engineering**
  - It works because, humans are
    - amiable,
    - have a feeling of moral obligation,

## Ethical issues

- **Social engineering**
  - It works because, humans are
    - amiable,
    - have a feeling of moral obligation,
    - are helpful,

## Ethical issues

- **Social engineering**
  - It works because, humans are
    - amiable,
    - have a feeling of moral obligation,
    - are helpful,
    - opportunistic,

## Ethical issues

- **Social engineering**

- It works because, humans are
  - amiable,
  - have a feeling of moral obligation,
  - are helpful,
  - opportunistic,
  - and often unwilling to assume responsibilities.

## Ethical issues

- **Social engineering**

- It works because, humans are
  - amiable,
  - have a feeling of moral obligation,
  - are helpful,
  - opportunistic,
  - and often unwilling to assume responsibilities.
- But

## Ethical issues

- **Social engineering**

- It works because, humans are
  - amiable,
  - have a feeling of moral obligation,
  - are helpful,
  - opportunistic,
  - and often unwilling to assume responsibilities.
- But
  - social engineering techniques have a direct influence on the client's employees,

## Ethical issues

### • **Social engineering**

- It works because, humans are
  - amiable,
  - have a feeling of moral obligation,
  - are helpful,
  - opportunistic,
  - and often unwilling to assume responsibilities.
- But
  - social engineering techniques have a direct influence on the client's employees,
  - even if the report is anonymous, these techniques can make employees feel insecure.

## Ethical issues

- **Vulnerabilities exploitation**

## Ethical issues

- **Vulnerabilities exploitation**
  - Best practice approach:

## Ethical issues

- **Vulnerabilities exploitation**

- Best practice approach:
  - identify vulnerability (in the enumeration phase)

## Ethical issues

- **Vulnerabilities exploitation**

- Best practice approach:
  - identify vulnerability (in the enumeration phase)
  - **only if it is wanted and/or not harmful to production operations:**  
exploit vulnerability

## Report

- Management summary

The report itself is of course essential for the client, but there's something more important, that is most often not recognized:

## Report

- Management summary
- Detailed technical analysis

The report itself is of course essential for the client, but there's something more important, that is most often not recognized:

## Report

- Management summary
- Detailed technical analysis

The report itself is of course essential for the client, but there's something more important, that is most often not recognized:

- Meeting

# Usual suspects

## or where to begin

- Reconnaissance:

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs
  - unused or forgotten services

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs
  - unused or forgotten services
  - client-side software (flash, ...)

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs
  - unused or forgotten services
  - client-side software (flash, ...)
  - open shares

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs
  - unused or forgotten services
  - client-side software (flash, ...)
  - open shares
  - WLAN

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs
  - unused or forgotten services
  - client-side software (flash, ...)
  - open shares
  - WLAN
  - backups

# Usual suspects

## or where to begin

- Reconnaissance:
  - website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs
  - unused or forgotten services
  - client-side software (flash, ...)
  - open shares
  - WLAN
  - backups