

Chapter 1

Hacking: The Next Generation

**Edited by:
Dr. Ahmed
Redha
PSU**

Learning Objective

- Explore the history and current state of hacking and penetration testing, including their ethical and legal implications.

Key Concepts

- Motives of hackers
- History of hacking
- Ethical hacking and penetration testing
- Laws and ethical standards for penetration testers and ethical hackers

Profiles and Motives of Different Types of Hackers

- **Good guys** are InfoSec professionals who use hacking skills to expose vulnerabilities and makes their systems more secure
- **Amateurs [Script Kiddies]** are entry-level hackers who use scripts and software from experienced hackers
- **Criminals** are hackers who conduct illegal activities for financial gain
- **Suicide Hackers:** aim for destruction without worrying about punishment
- **Ideologues [Hacktivists]** are hackers who conduct hacking activities for political or ideological goals

TAP Principle of Controls

Technical

- Software or hardware devices, such as firewalls and biometrics, and permissions

Administrative

- Policies and procedures

Physical

- Doors, locks, cameras, security guards, lighting, fences, gates, and similar devices

The Hacker Mindset

Victimless crime

They think that their actions are without victims

Robin Hood ideal

like taking money from the rich and give it to the poor

like a hacker who hacked into a big company and make it public to others

*ex: microsoft
subscribe*

افتخار
National pride and patriotism

وطني

i'm proud i can access this s.w

Educational value

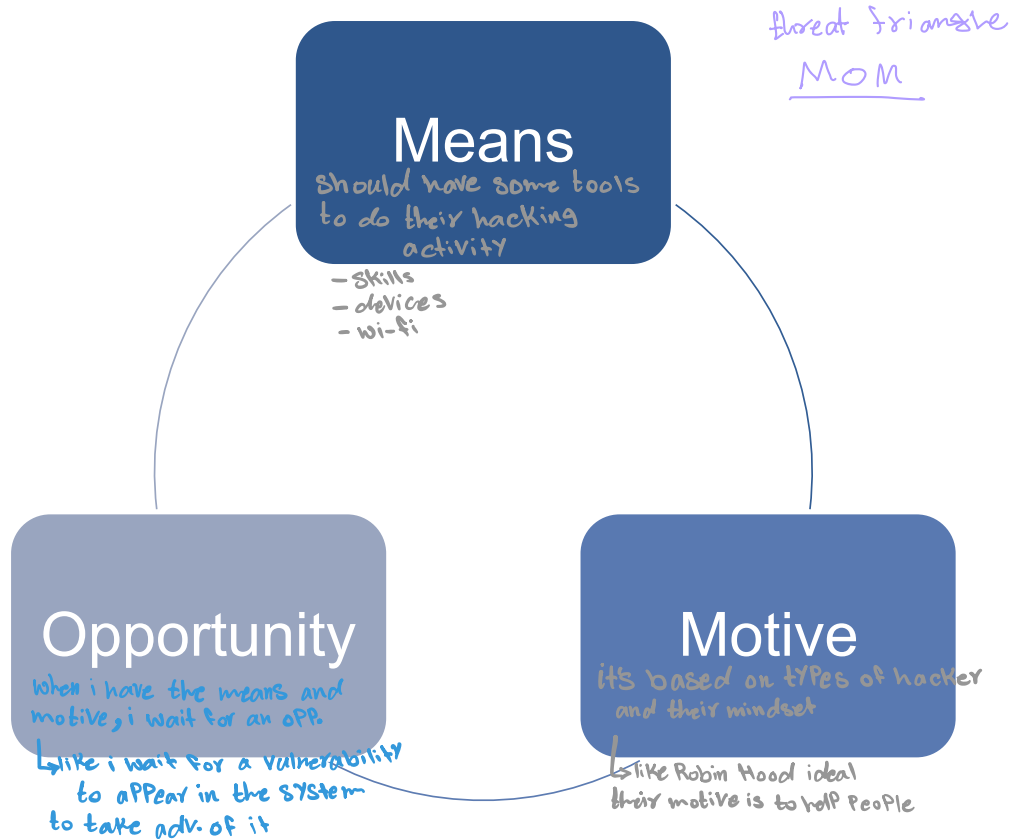
develop their hacking skills

Curiosity

like kids

they hack to check how strong is the security just out of curiosity

Motivations



Modern Hacking and Cybercriminals

- **New threats** in the form of worms, spam, spyware, adware, and rootkits *modern viruses*
- **Shift** from alone hacker to groups of hackers *that act as a group*
- **Crime rings**, organized crime, and nations with hostile interests use the Internet as an attack route -- cyberattacks
- **Hackers receive financing** from criminal organizations, terrorists, or even foreign governments *الناس الكبيرة تدفع لهم عشان يهكروا*

Ethical Hacking and Penetration Testing

- **Ethical hackers** require permission to engage in penetration testing without permission they are hackers not ethical hackers
- **Penetration testing** is the follow certain steps structured and methodical means of investigating, uncovering, attacking, and reporting on a target system's strengths and vulnerabilities
- Penetration tests are commonly part of **IT audits**

Ethical Hacking and Penetration Testing (Cont.)

Black-box Testing

- Used to simulate how attacker views system
- **No** knowledge of system provided to testing team

ما يعرف اي شيء عن النظام

White-box Testing

- **Advanced** knowledge provided to testing team

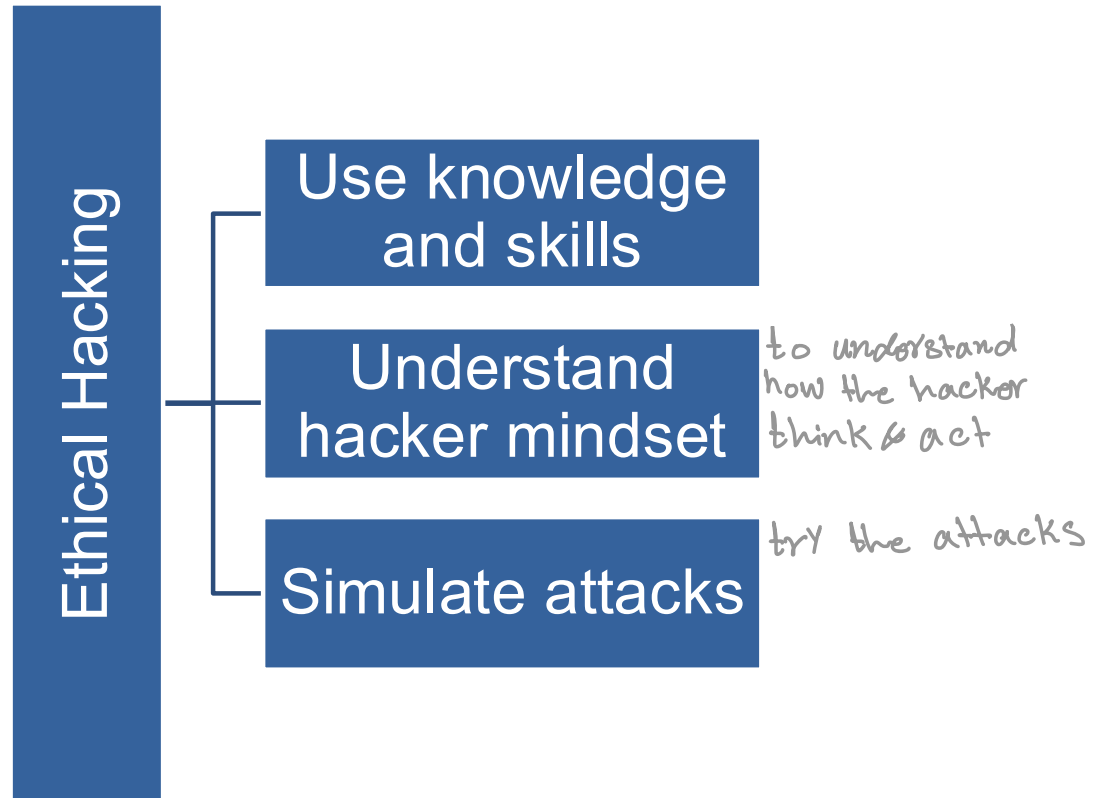
Gray-box Testing

- **Some** knowledge provided to testing team

Comparison among Audit, Vulnerability Assessment and Pen Testing

Introduction to Ethical Hacking Penetration Testing Concepts		Comparing Security Audit, Vulnerability Assessment, and Penetration Testing		CEH Certified Ethical Hacker	
		Security Audit A security audit just checks whether the organization is following a set of standard security policies and procedures			
		Vulnerability Assessment A vulnerability assessment focuses on discovering the vulnerabilities in the information system but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability			
		Penetration Testing Penetration testing is a methodological approach to security assessment that encompasses the security audit and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attackers			

Role of Ethical Hacking



Role of Ethical Hacking (Cont.)

Requires permission of victim

*You can't be ethical hacker
and do Pen. testing
Without Permission*

Use same strategies as malicious hacker

Key Points

Use care to avoid harming system

*so critical **

Establish rules of engagement

*Sign a doc. that
You are allowed
to test their server
So when something*

Need advance knowledge of hacker
techniques

*happens that
can't sue
You*

Rules of Engagement Template

DATE: *[Date]*

TO: *[Name and Address of NASA Official]*

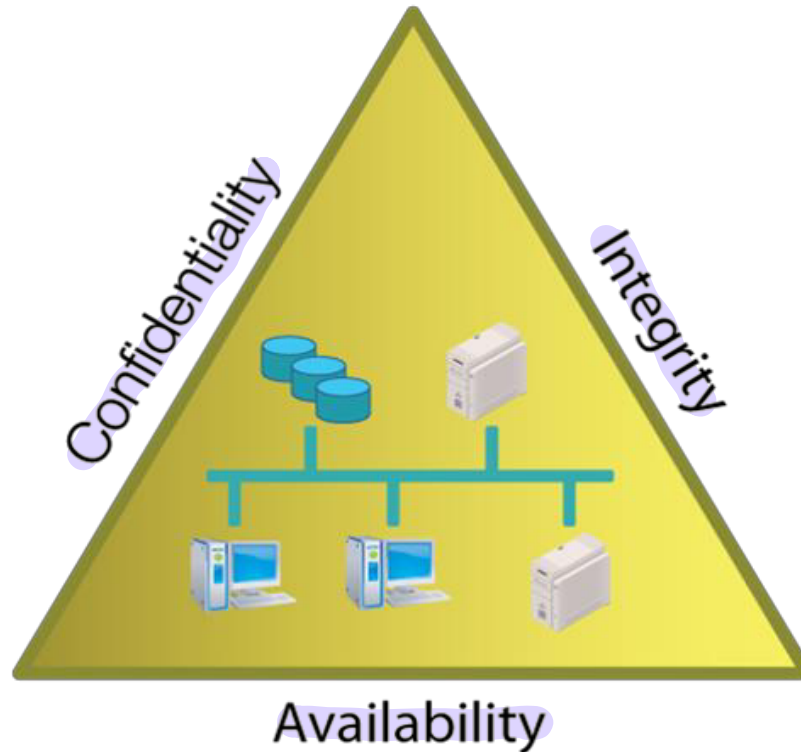
FROM: *[Name and Address of Third Party performing the Penetration Testing]*

CC: *[Name and Address of Interested NASA Officials]*

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of
[required activity]

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), *[Name of requesting organization]* to perform an audit of NASA's *[Name of risk assessment target]*. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

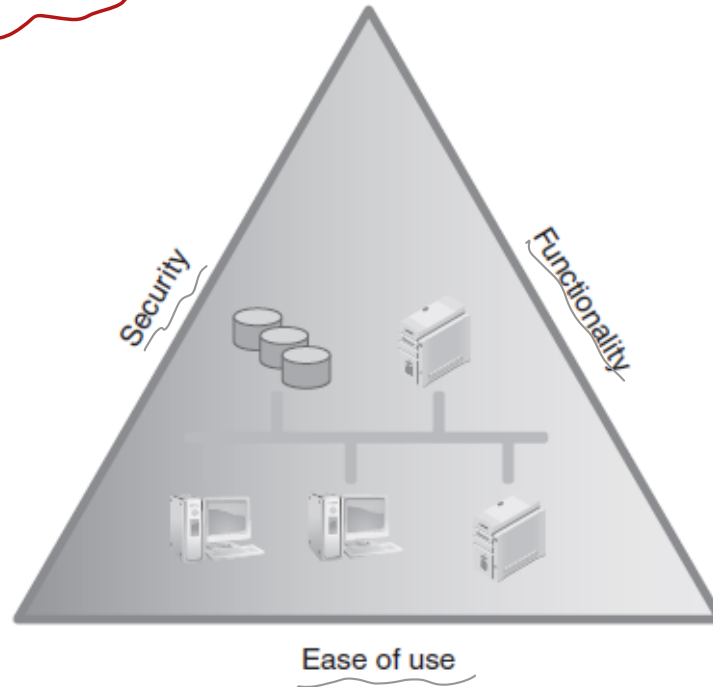
Ethical Hackers and the C-I-A Triad: The C-I-A Triad



Ethical Hackers and the C-I-A Triad: Usability vs. Security

* a Perfectly secure system is useless
if no one can use it *

- there should be
a balance
between these
3 things



Main Hacking Phases

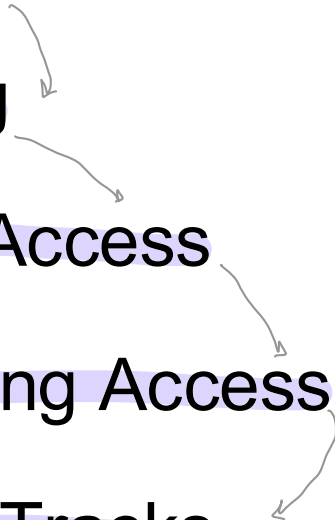
1. Reconnaissance *gather info. about the target*

2. Scanning

3. Gaining Access

4. Maintaining Access

5. Clearing Tracks



1- Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- Could be the future point of return, noted for ease of entry for an attack when more about the **target is known on a broad scale**
- Reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves **interacting with the target directly by any means**
- For example, telephone calls to the help desk or technical department

2- Scanning

Pre-Attack Phase

Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance



Port Scanner

Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.



Extract Information

Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc. to launch attack



3- Gaining Access

1

Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the computer or network

2

The attacker can gain access at the **operating system level, application level, or network level**



3

The attacker can **escalate privileges** to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

4

Examples include **password cracking**, buffer overflows, denial of service, **session hijacking**, etc.

4- Maintaining Access

بعد ما اكتسب (Gained) access
بهذه الخطوة بيعلن
كيف يا فظ (Maintain) عليه

Introduction to Ethical Hacking

Hacking Concepts

Hacking Phases: Maintaining Access

CEH

Certified Ethical Hacker

1

Maintaining access refers to the phase when the attacker tries to retain his or her **ownership of the system**

2

Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **Backdoors, RootKits, or Trojans**

3

Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**

4

Attackers use the compromised system to **launch further attacks**

5- Clearing Tracks

1

Covering tracks refers to the activities carried out by an attacker to **hide malicious acts**



2

The attacker's intentions include: **Continuing access** to the victim's system, remaining **unnoticed and uncaught**, deleting evidence that might lead to his prosecution



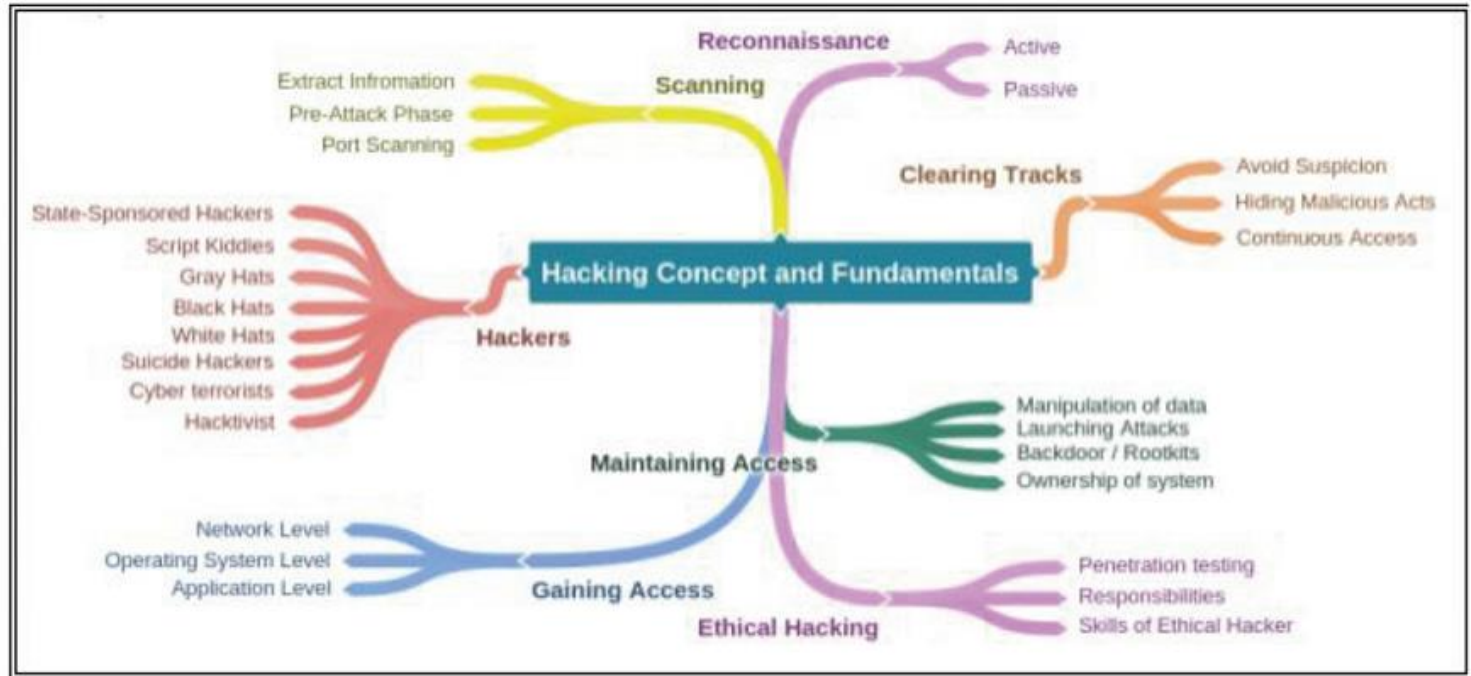
3

The attacker overwrites the server, system, and application logs to **avoid suspicion**



Attackers always cover their tracks to hide their identity

Mind Map



Skills of the Ethical Hacker

1

Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas** and related issues
- Has **"high technical" knowledge** to launch the sophisticated attacks

2

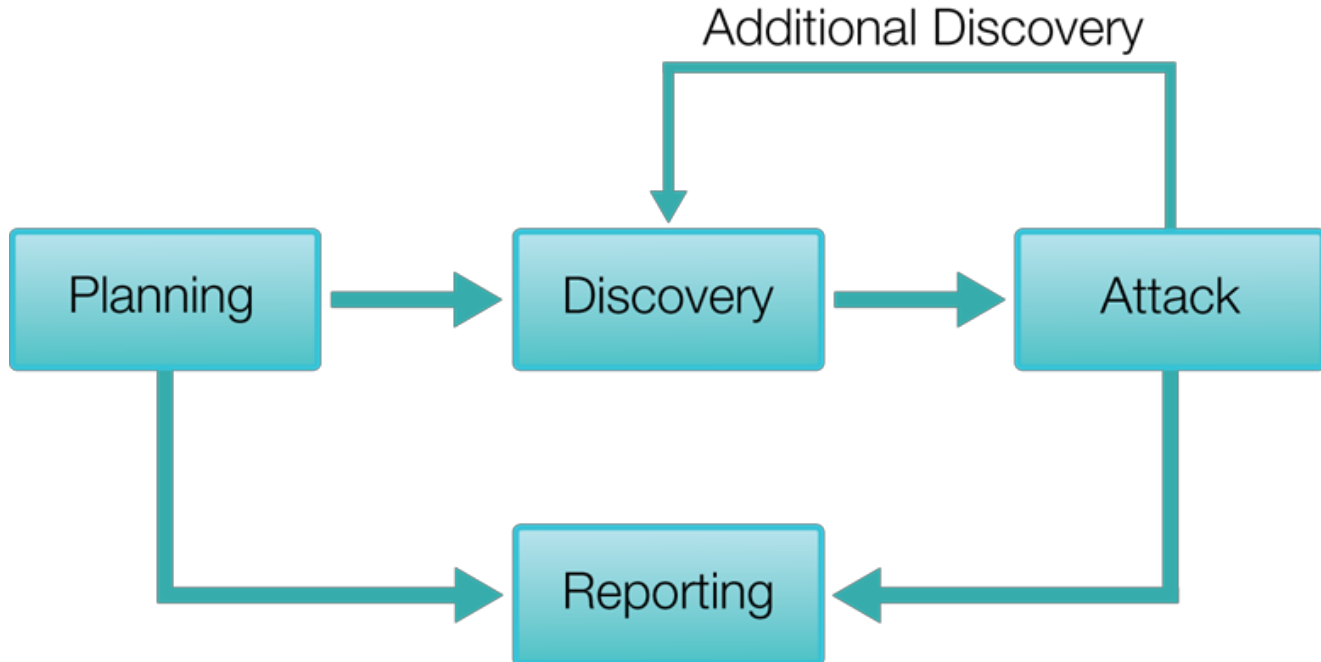
Non-Technical Skills

Some of the non-technical characteristics of an ethical hacker include:

- Ability to learn** and adapt new technologies quickly
- Strong work ethics**, and good problem solving and communication skills
- Committed to **organization's security policies**
- Awareness of **local standards and laws**



Performing a Penetration Test: Ethical Hacking Steps



Performing a Penetration Test (Cont.)

Types of Penetration Test Attacks

Technical

Administrative

Physical

Laws and Ethical Standards

Trust

- Client places trust in ethical hacker to use proper discretion when performing tests
- If ethical hacker breaks trust, can degrade trust in other project aspects, such as the reported results of tests

Legal implications

- Violating limits defined by the permitted scope of testing may be sufficient cause for client to take legal action against ethical hacker
- If violating test scope results in damages, client may be compelled to take legal action

Laws and Ethical Standards (Cont.)

Examples of laws and ethical standards:

- Computer Fraud and Abuse Act
- US Electronic Communications Privacy Act
- Sarbanes-Oxley Act (SOX)
- Federal Information Security Modernization Act (FISMA 2014)

Certifications

- **CEH:** Certified Ethical Hacker from EC-Council
<https://www.eccouncil.org>
- **GPEN:** GIAC (Global Information Assurance Certification) Penetration Tester from SANS
<https://www.giac.org/certification/penetration-tester-gpen>
- **OSCP:** Offensive Security Certified Professional from offensive security
<https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/>
- **Mile2:** are less well known <https://mile2.com/>
- **CISSP:** Certified Information Systems Security Professional: not a penetration testing certificate. It is a general information security certification.

Summary

- Motives of hackers
- History of hacking
- Ethical hacking and penetration testing
- Laws and ethical standards for penetration testers and ethical hackers
- Certifications

in ch.2
-define OSINT