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

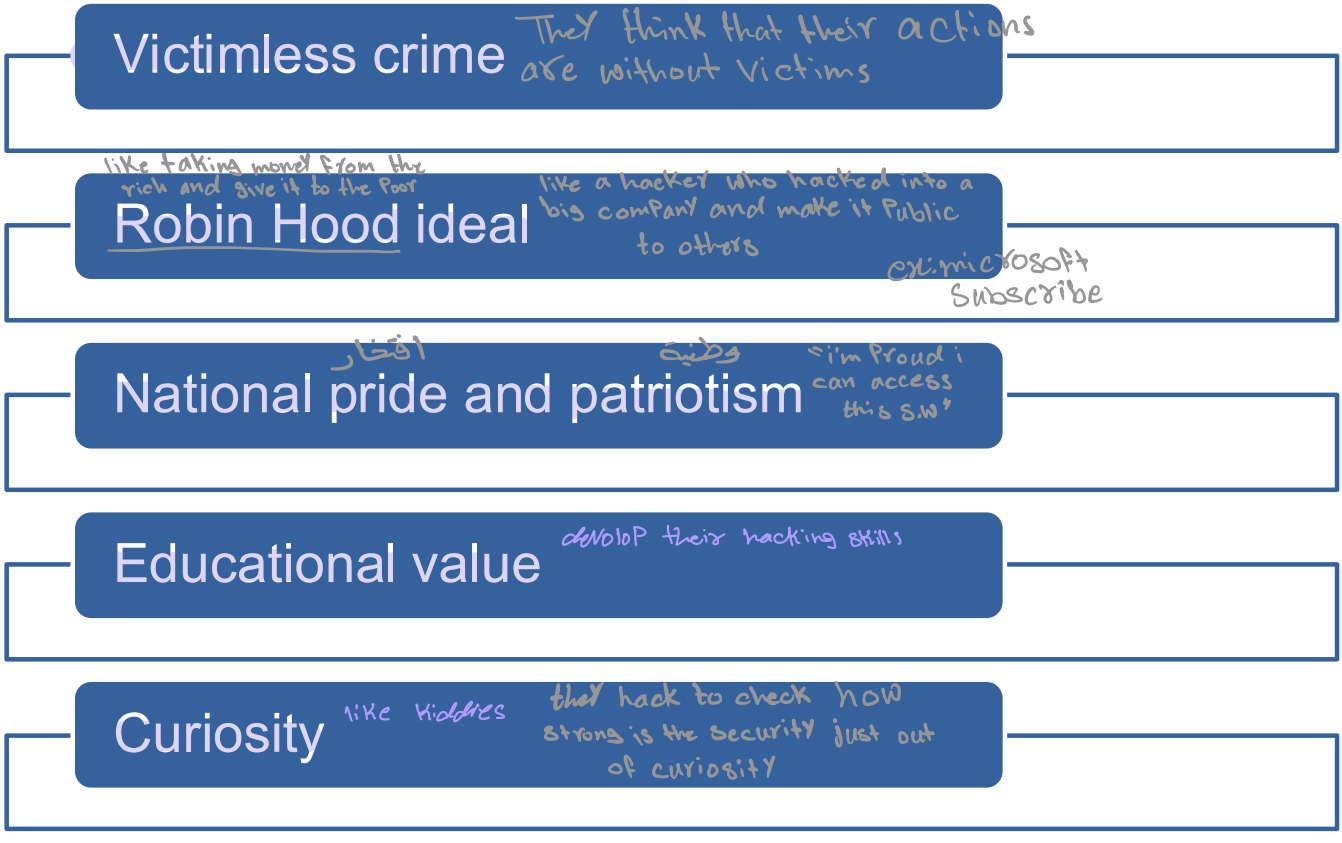
Profiles and Motives of Different Types of Hackers

- **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

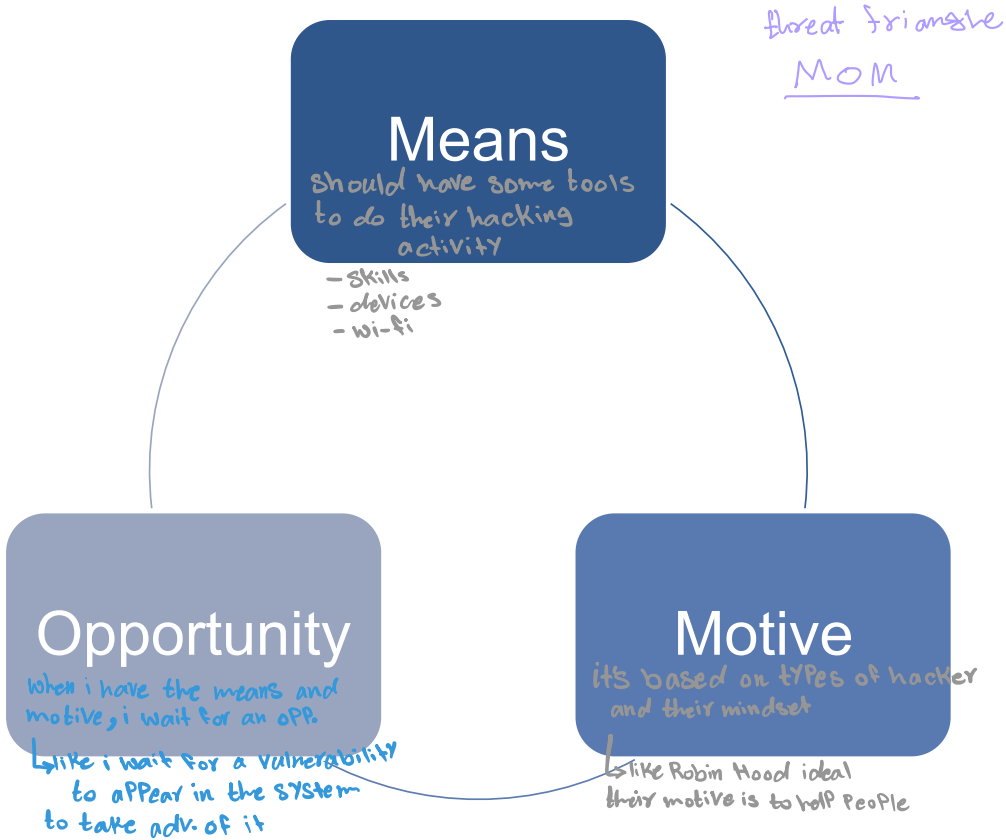
TAP Principle of Controls

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



Motivations



Modern Hacking and Cybercriminals

- New threats in the form of worms, spam, spyware, adware, and rootkits
- Shift from alone hacker to groups of hackers
- 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

Ethical Hacking and Penetration Testing

- **Ethical hackers** require permission to engage in penetration testing

Without Permission they hackers not ethical hackers

- **Penetration testing** is the structured and methodical means of investigating, uncovering, attacking, and reporting on a target system's strengths and vulnerabilities

follow certain steps

- 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
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

Security Audit

- A security audit just checks whether the organization is following a set of standard **security policies and procedures**

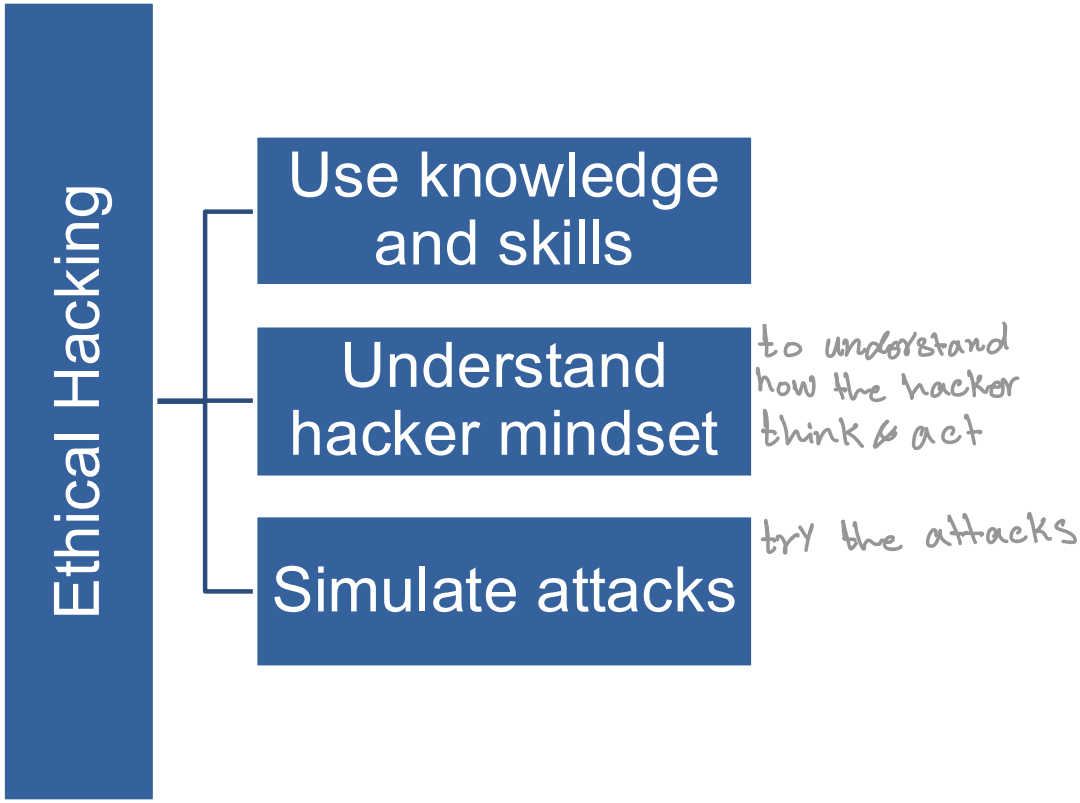
Vulnerability Assessment

- 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

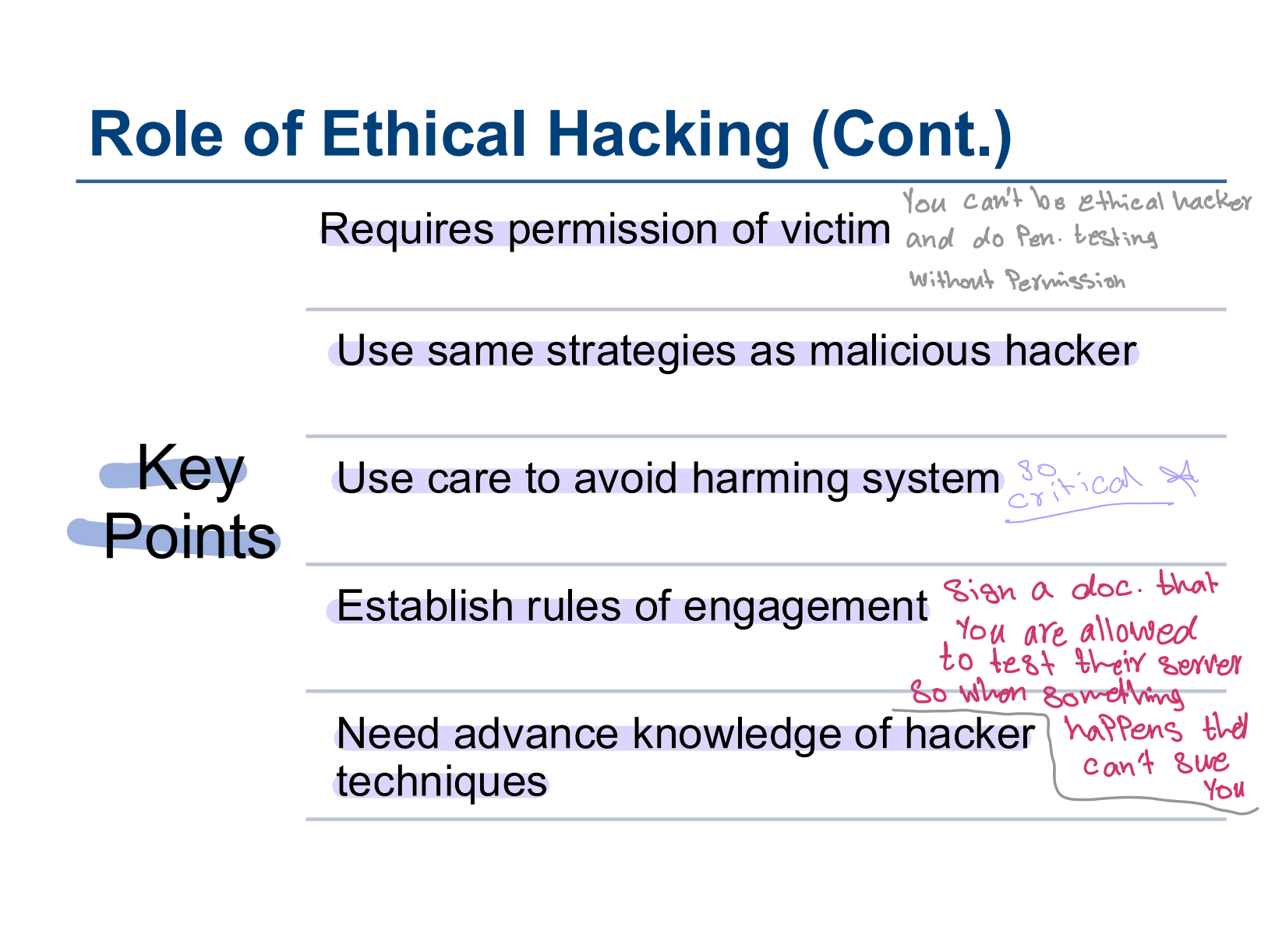
Role of Ethical Hacking



Role of Ethical Hacking (Cont.)

Key Points

- Requires permission of victim
- Use same strategies as malicious hacker
- Use care to avoid harming system
- Establish rules of engagement
- Need advance knowledge of hacker techniques



Rules of Engagement Template

DATE: *[Date]*

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

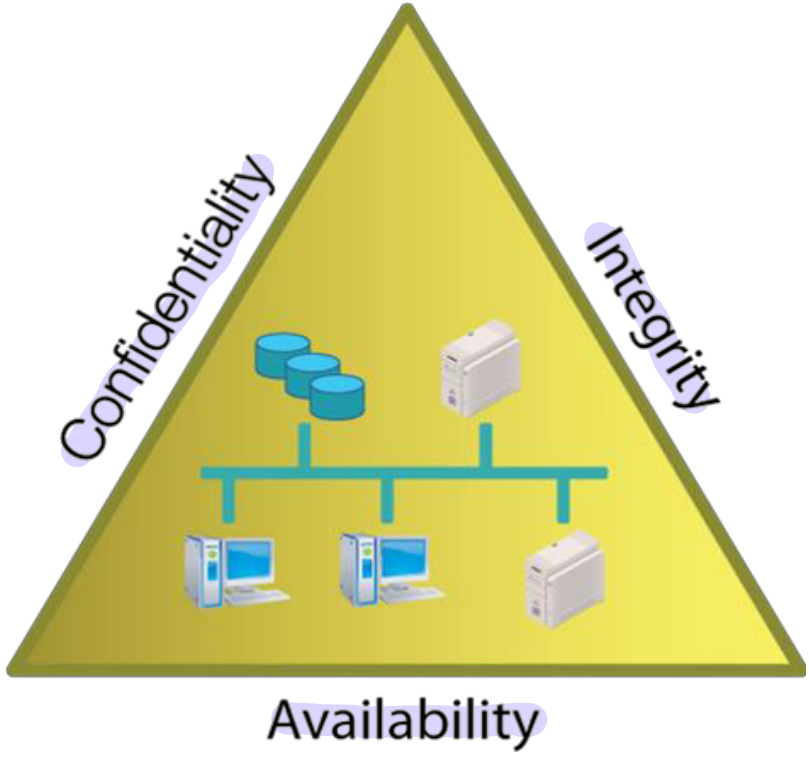
FROM: *[Name and Address of Third Party performing the Penetration Testing]*

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.

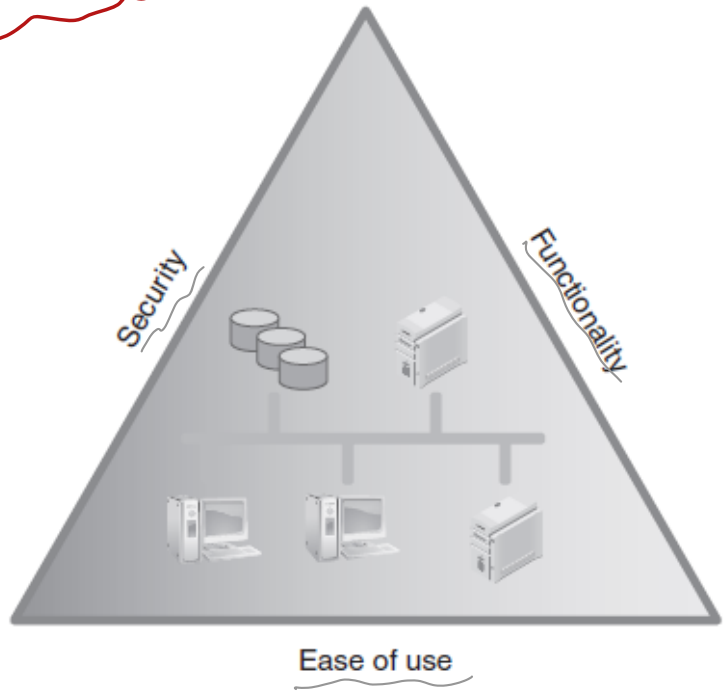
Ethical Hackers and the C-I-A Triad: The C-I-A Triad



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

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

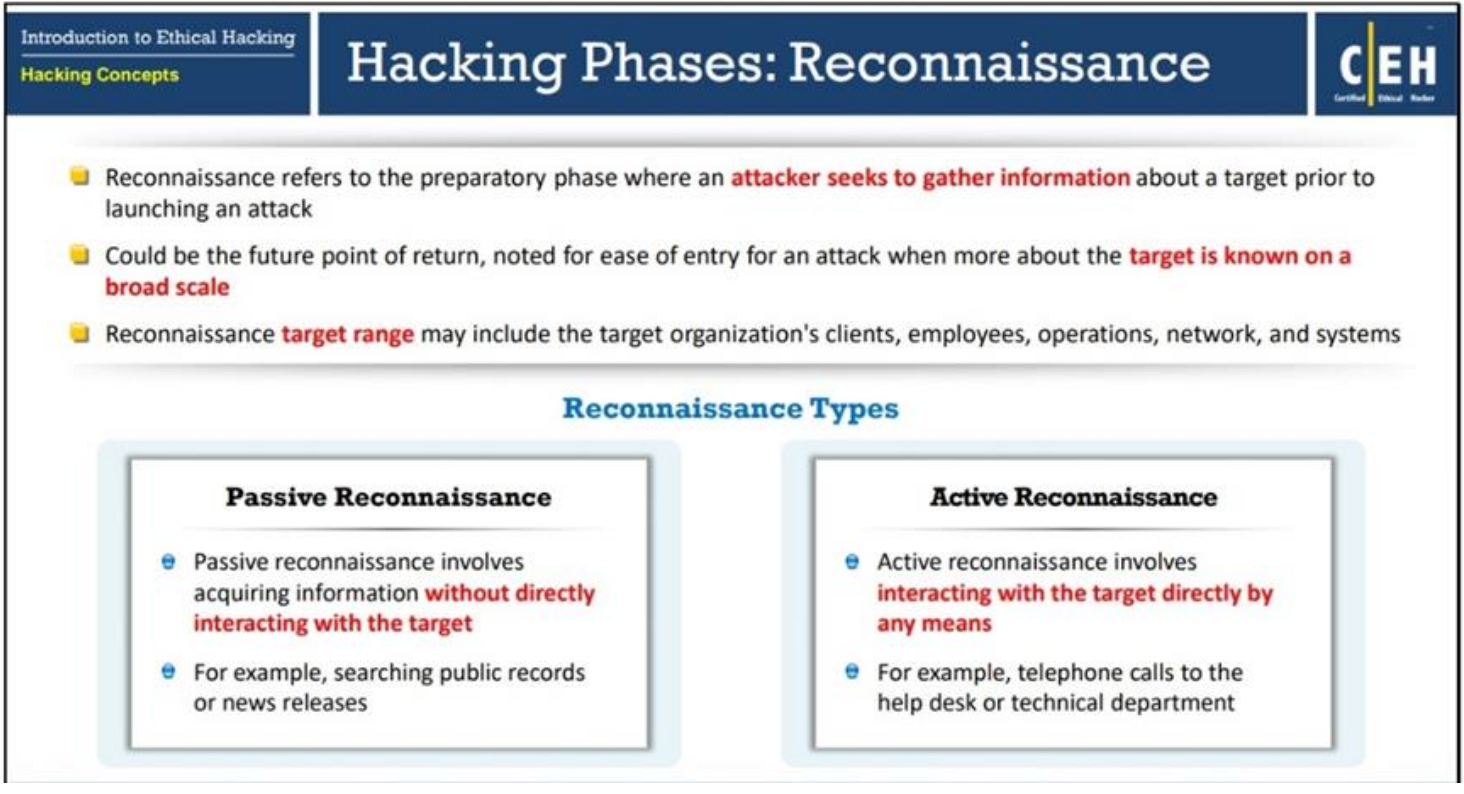
- there should be a balance between these 3 things



Main Hacking Phases

1. Reconnaissance — gather info. about the target
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

1- Reconnaissance

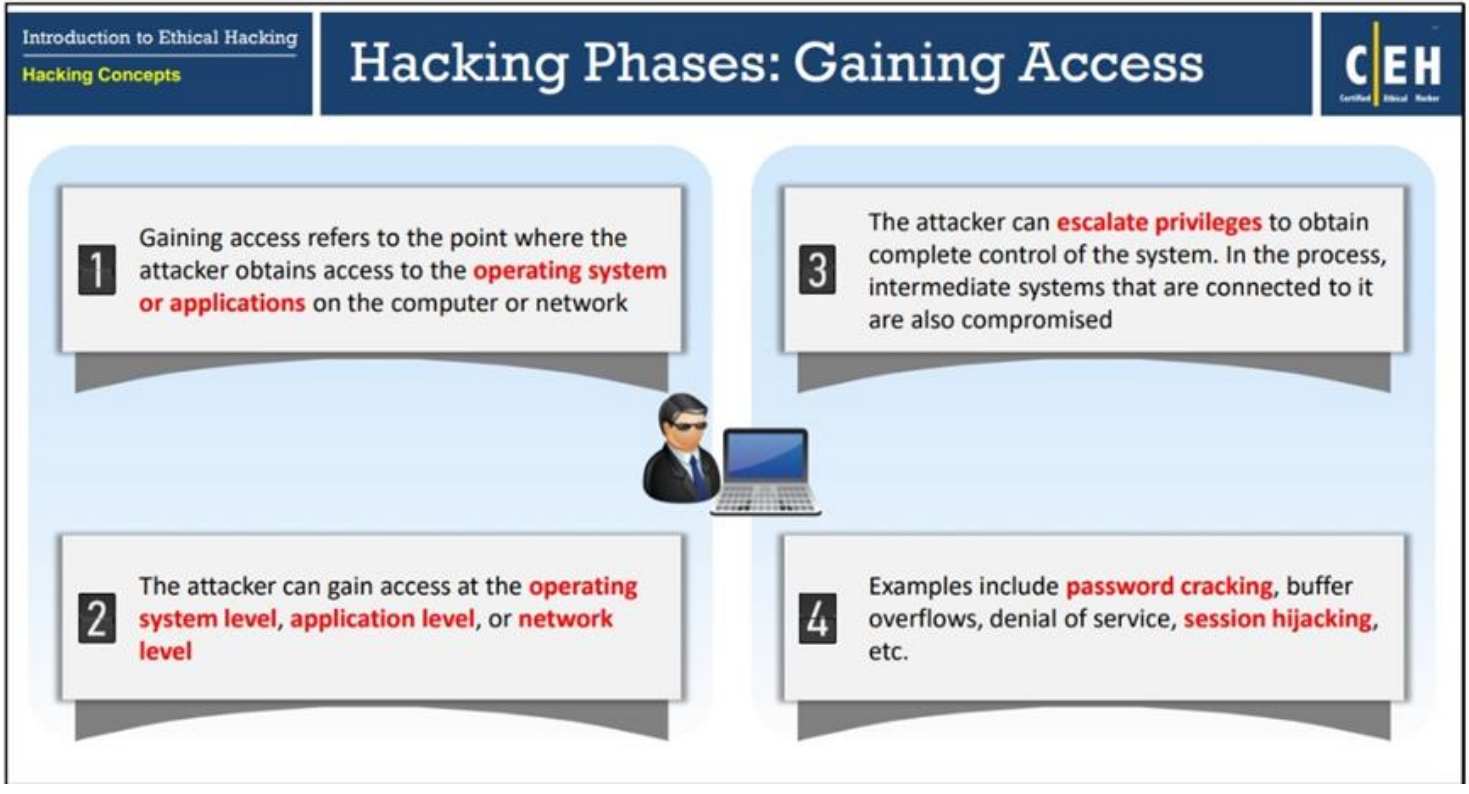


2- Scanning

Hacking Phases: Scanning

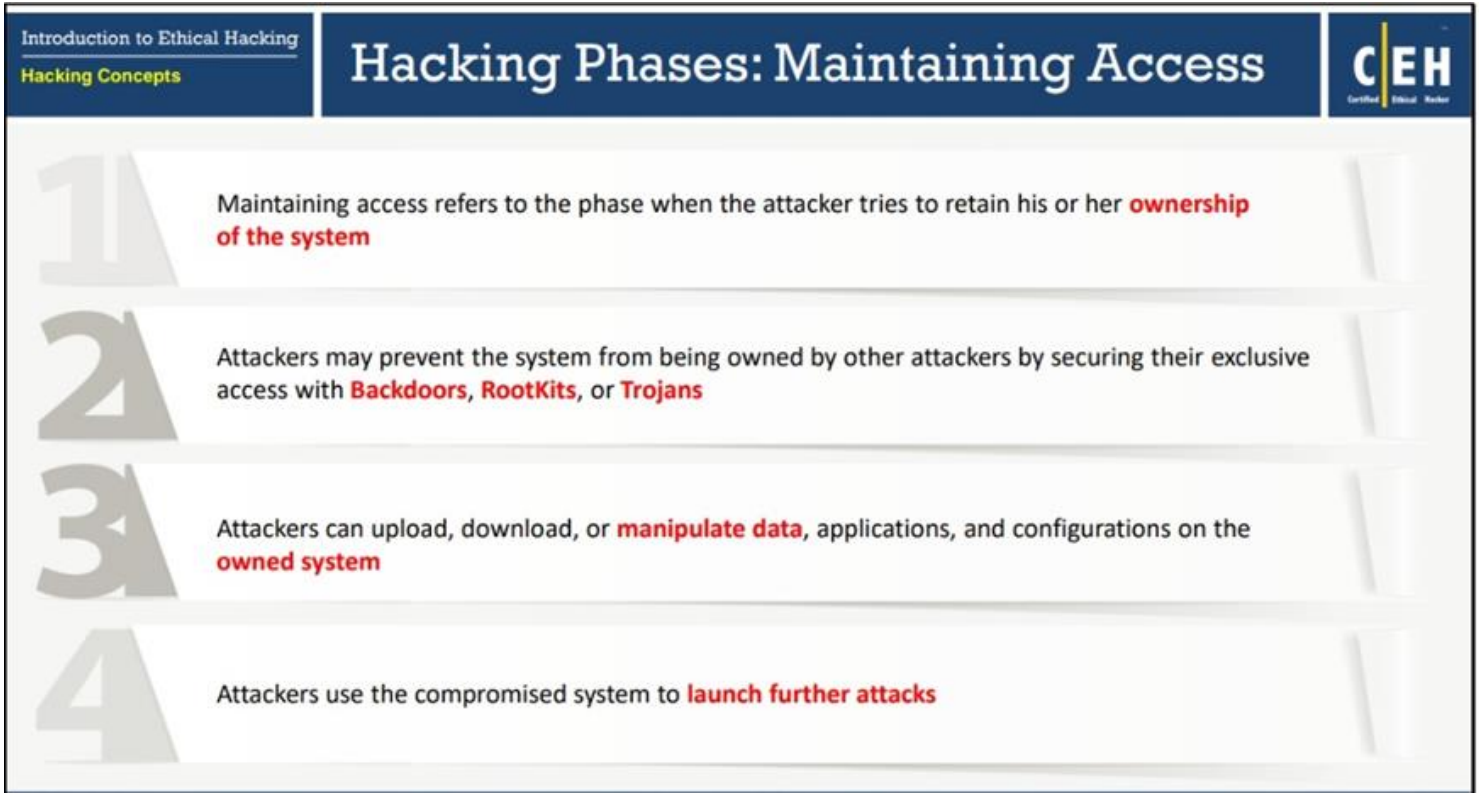
Pre-Attack Phase	Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance
Port Scanner	Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, 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

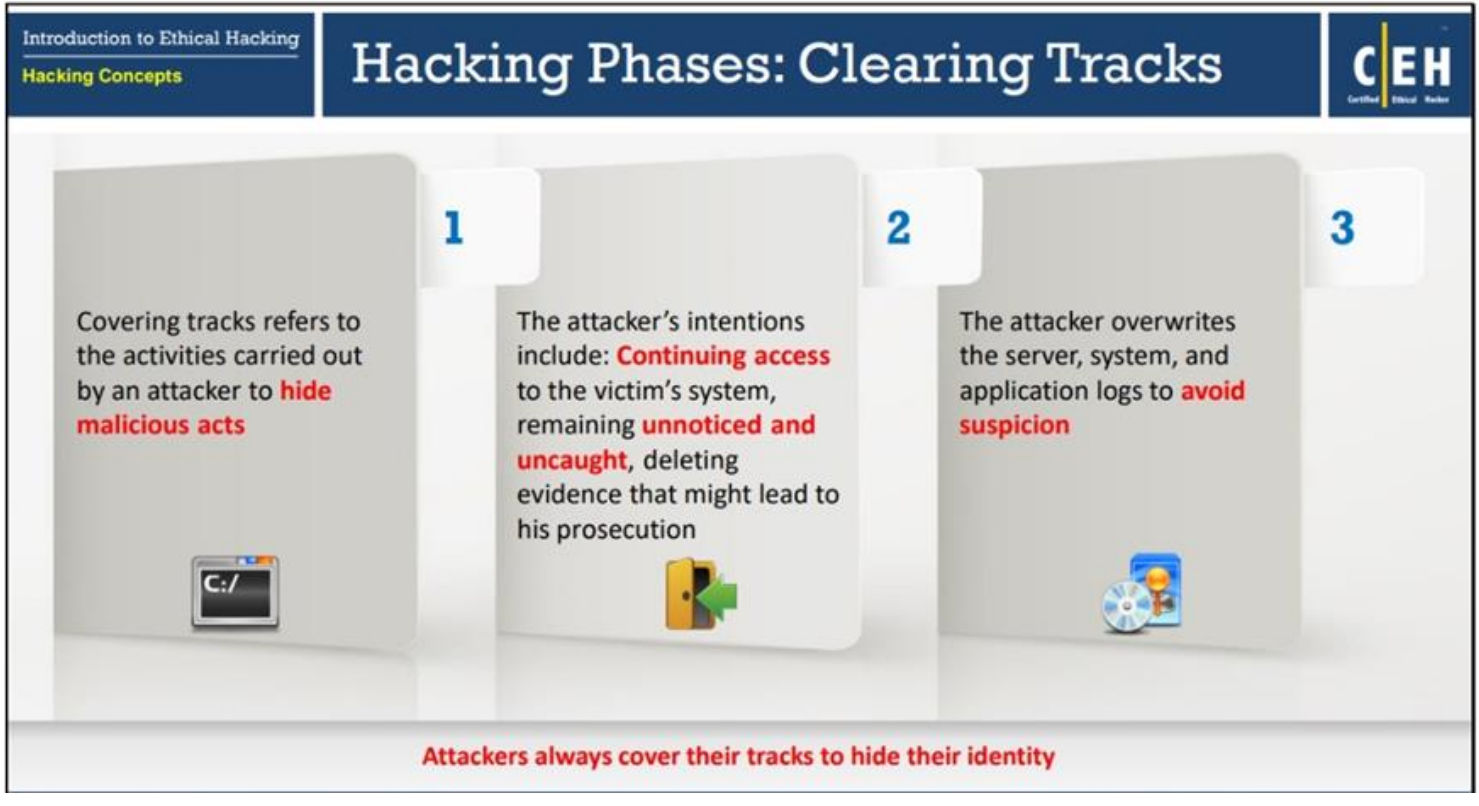


بعد ما اكتسب access (Gained)
بهذي الخطوة بيعلم
كيف يحافظ (Maintain) عليه

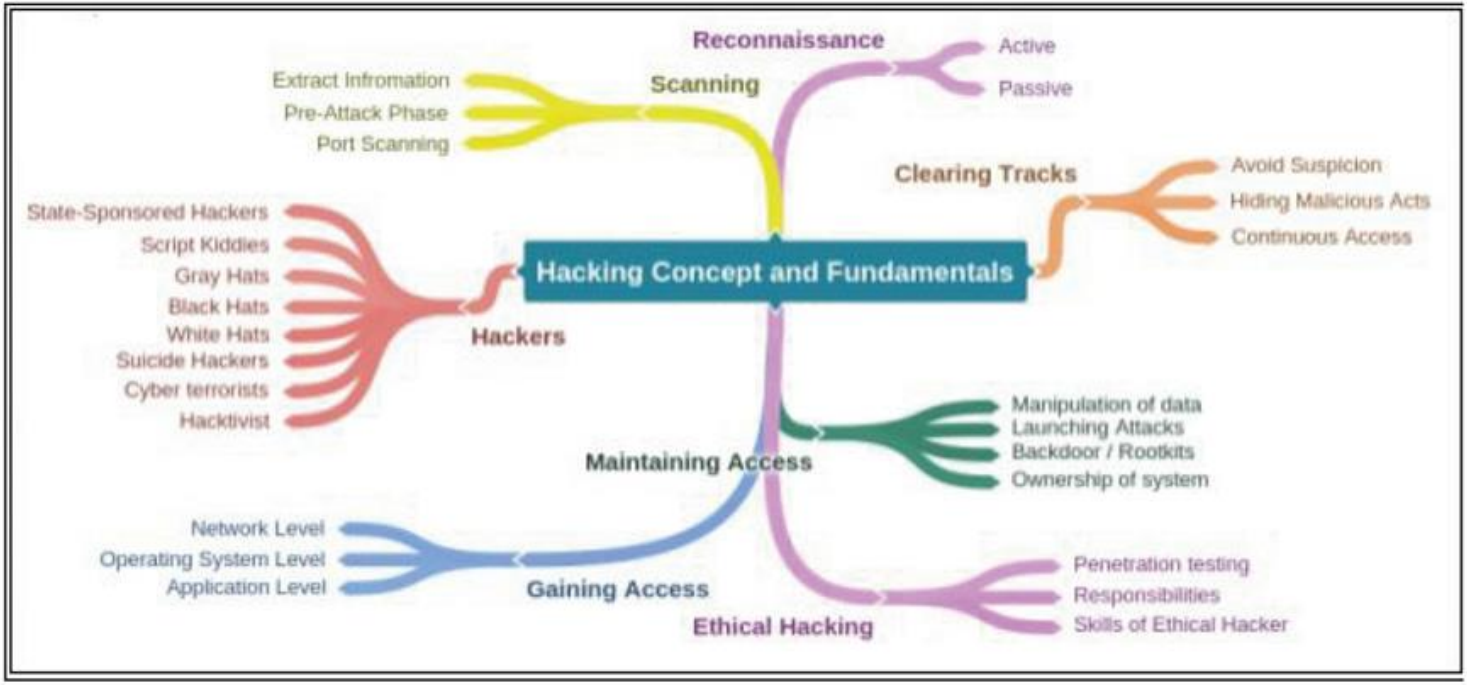
4- Maintaining Access



5- Clearing Tracks



Mind Map


Hacking Concept and Fundamentals
Reconnaissance
Active
Passive
Scanning
Extract Infromation
Pre-Attack Phase
Port Scanning
Clearing Tracks
Avoid Suspicion
Hiding Malicious Acts
Continuous Access
Hackers
State-Sponsored Hackers
Script Kiddies
Gray Hats
Black Hats
White Hats
Suicide Hackers
Cyber terrorists
Hacktivist
Maintaining Access
Manipulation of data
Launching Attacks
Backdoor / Rootkits
Ownership of system
Gaining Access
Network Level
Operating System Level
Application Level
Ethical Hacking
Penetration testing
Responsibilities
Skills of Ethical Hacker

Skills of the Ethical Hacker

Skills of an Ethical Hacker

1 Technical Skills

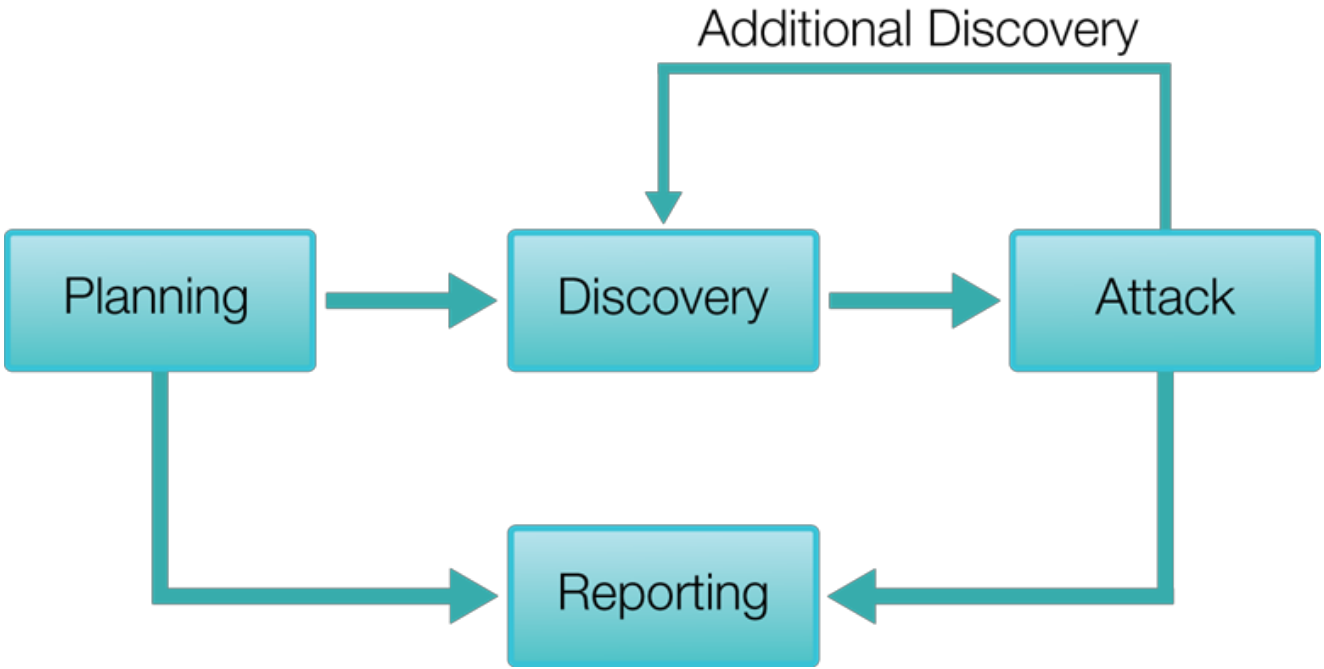
- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas**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

2 Non-Technical Skills

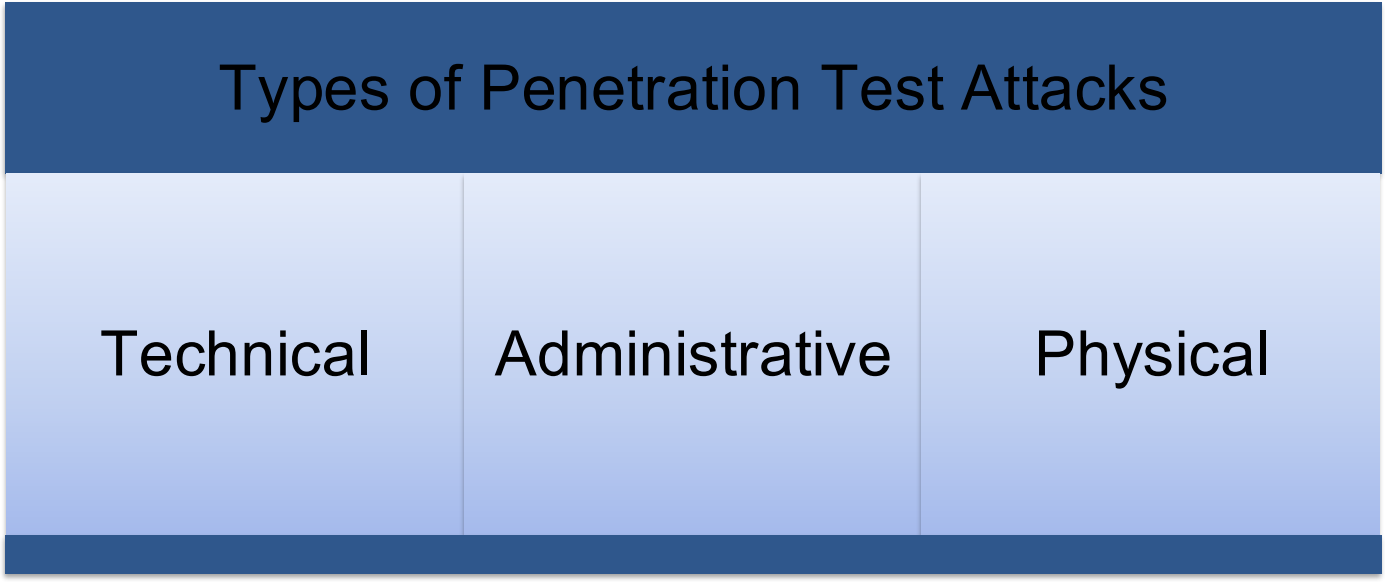
Some of the non-technical characteristics of an ethical hacker include:

- **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.)



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