Ecole Supérieure d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

ETHICAL HACKING & DEFENSE

CEH Certified Ethical Hacker

PRÉPARÉ PAR:
SEBBAR ANASS

Année universitaire: 2024-2025

EC-COUNCIL | ACADEMIA PARTNER

Lecture: Introduction aux reseaux

Dr. Sebbar Anass

Email : anass.sebbar@uir.ac.ma
Bureau : B413 (Bat2, 4-ème étage)

When email me, please format the subject line as follows :
<ING4> – <CYB> - <FullName> - <Subject>

Coordinator de la filière Cybersecurity :

Cisco Networking Academy · Huawei ICT Academy · aws academy · FORTINET Network Security Academy · EC-COUNCIL | ACADEMIA PARTNER · Red Hat · Microsoft Azure

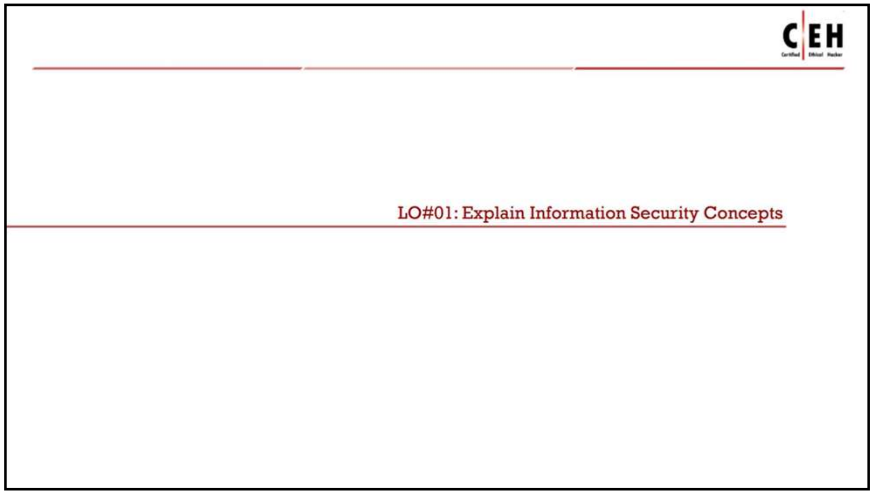
Evaluation

- CM - Quizzes : 10%
- Lab (CR + D) : 20%
- CC : 20%
- **Final Exam : 50%**

CEH

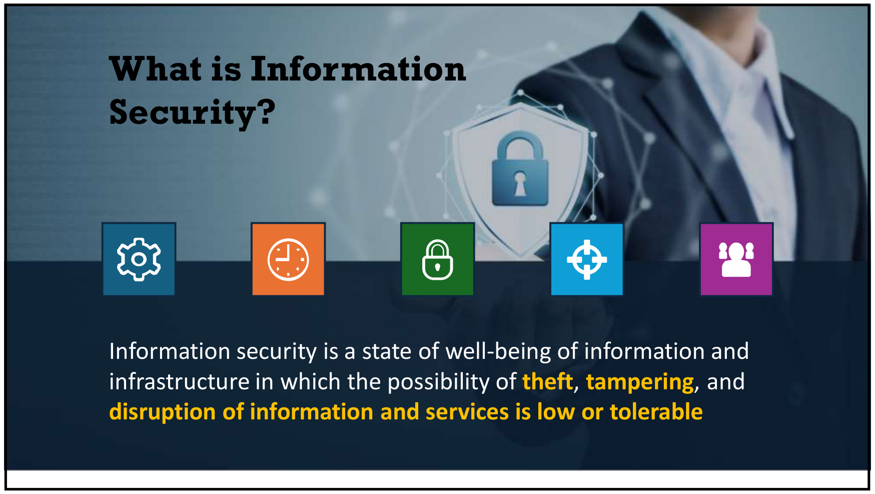
LEARNING OBJECTIVES

- LO#01: Explain Information Security Concepts
- LO#02: Explain Hacking Methodologies and Frameworks
- LO#03: Explain Hacking Concepts and Different Hacker Classes
- LO#04: Explain Ethical Hacking Concepts and Scope
- LO#05: Summarize the Techniques used in Information Security Controls
- LO#06: Explain the Importance of Applicable Security Laws and Standards



LO#01: Explain Information Security Concepts

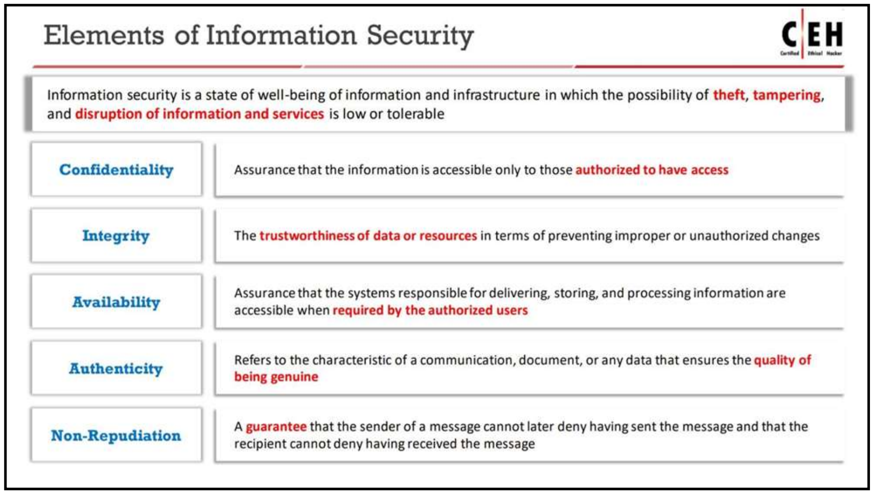
5



What is Information Security?

Information security is a state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services is low or tolerable**

6

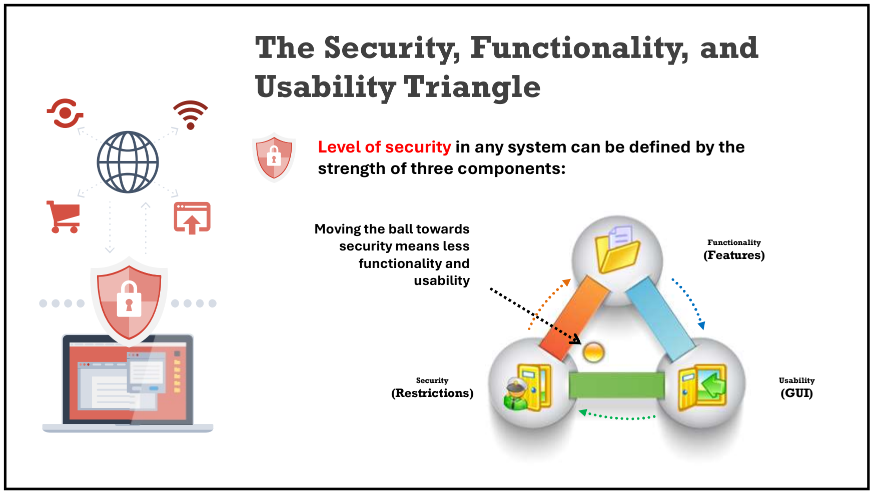


Elements of Information Security

Information security is a state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services** is low or tolerable

Confidentiality	Assurance that the information is accessible only to those **authorized to have access**
Integrity	The **trustworthiness of data or resources** in terms of preventing improper or unauthorized changes
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**
Authenticity	Refers to the characteristic of a communication, document, or any data that ensures the **quality of being genuine**
Non-Repudiation	A **guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

7

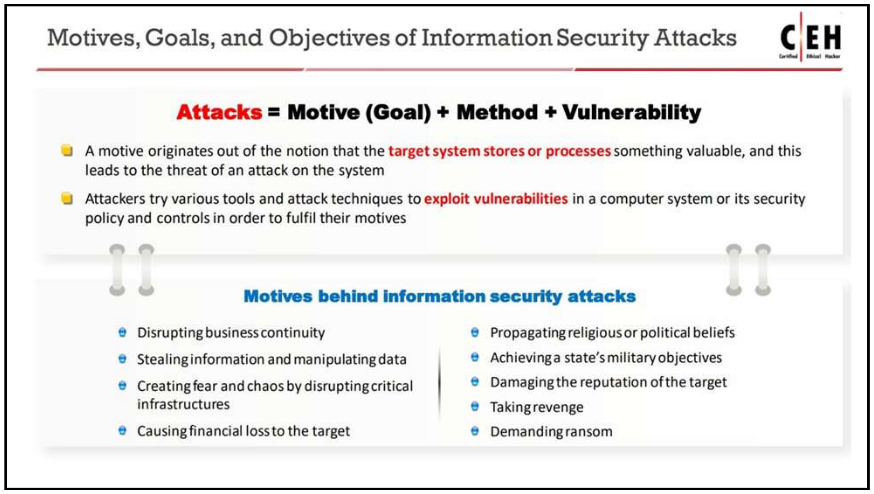


The Security, Functionality, and Usability Triangle

Level of security in any system can be defined by the strength of three components:

Moving the ball towards security means less functionality and usability
Functionality (Features)
Security (Restrictions)
Usability (GUI)

8



Motives, Goals, and Objectives of Information Security Attacks

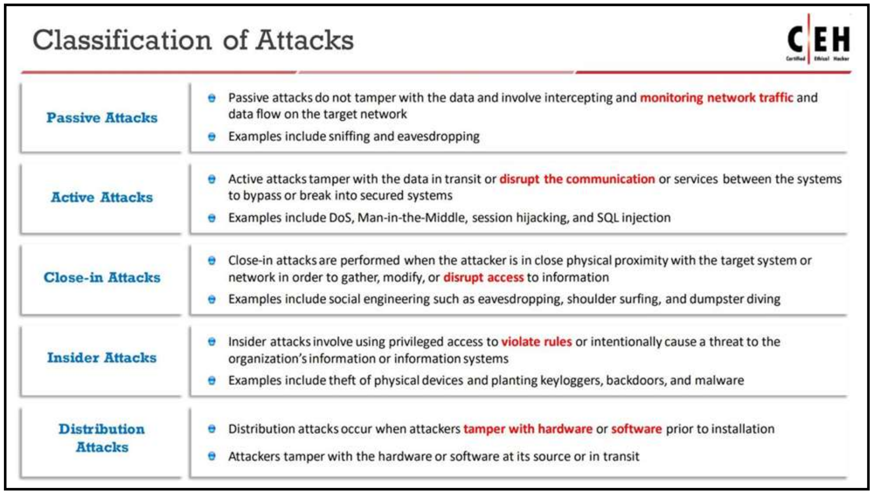
Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives

Motives behind information security attacks

- Disrupting business continuity
- Stealing information and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Causing financial loss to the target
- Propagating religious or political beliefs
- Achieving a state's military objectives
- Damaging the reputation of the target
- Taking revenge
- Demanding ransom

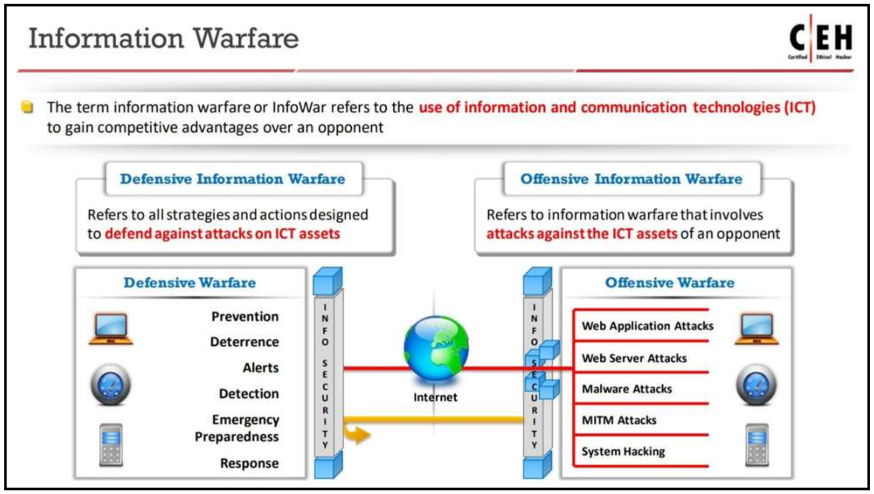
9



Classification of Attacks

Passive Attacks	Passive attacks do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network Examples include sniffing and eavesdropping
Active Attacks	Active attacks tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	Insider attacks involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	Distribution attacks occur when attackers **tamper with hardware** or **software** prior to installation Attackers tamper with the hardware or software at its source or in transit

10



Information Warfare

- The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to gain competitive advantages over an opponent

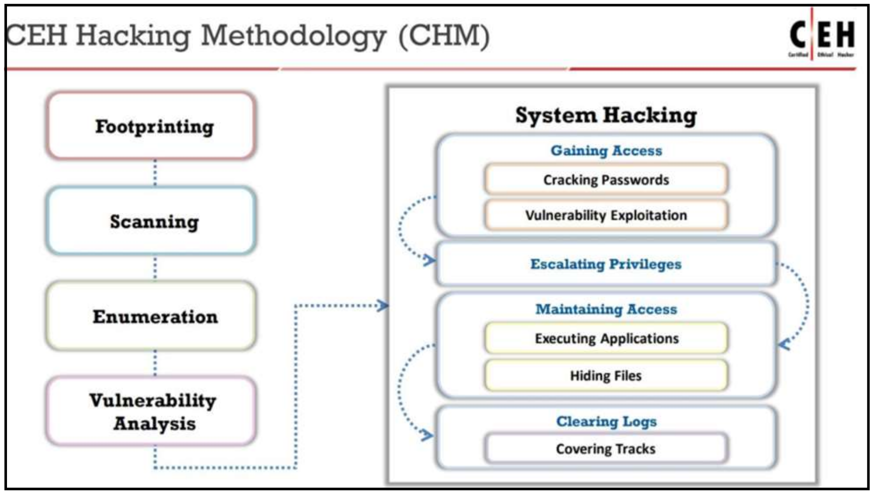
Defensive Information Warfare

Refers to all strategies and actions designed to **defend against attacks on ICT assets**

Offensive Information Warfare

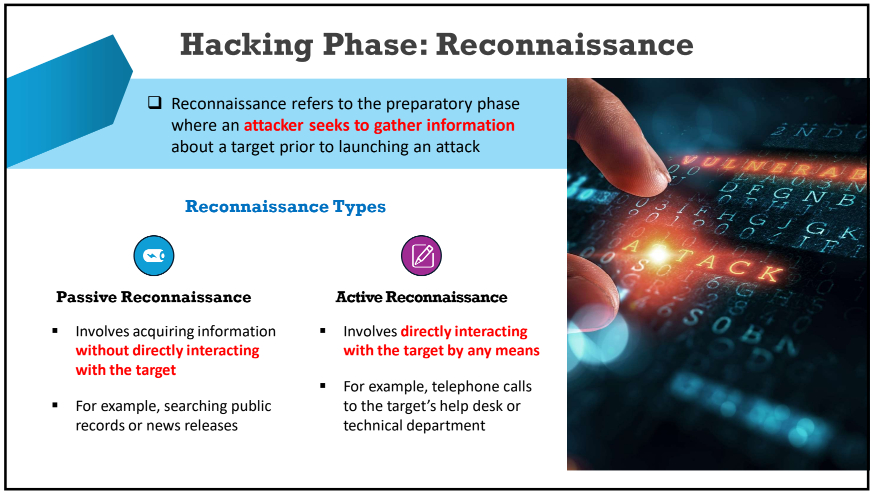
Refers to information warfare that involves **attacks against the ICT assets** of an opponent

11



CEH Hacking Methodology (CHM)

12



Hacking Phase: Reconnaissance

❑ Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack

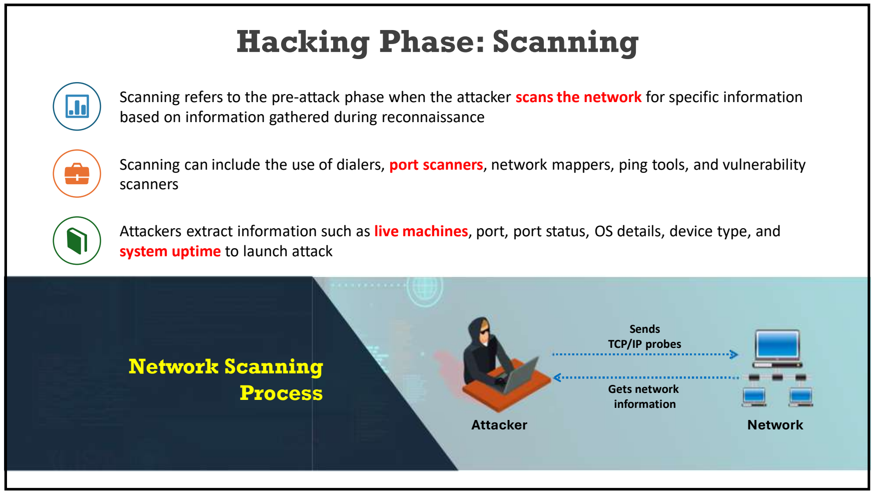
Reconnaissance Types

Passive Reconnaissance

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

Active Reconnaissance

- Involves **directly interacting with the target by any means**
- For example, telephone calls to the target's help desk or technical department



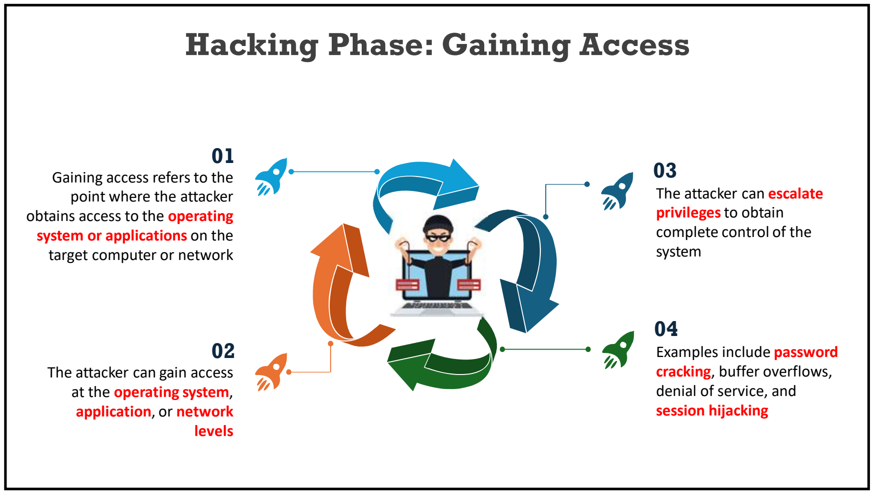
Hacking Phase: Scanning

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

Scanning can include the use of dialers, **port scanners**, network mappers, ping tools, and vulnerability scanners

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

Network Scanning Process



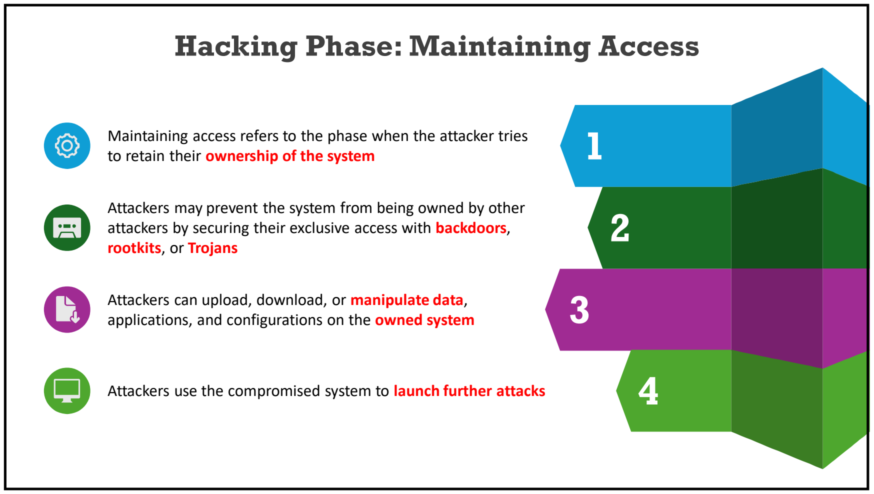
Hacking Phase: Gaining Access

01
Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the target computer or network

02
The attacker can gain access at the **operating system**, **application**, or **network levels**

03
The attacker can **escalate privileges** to obtain complete control of the system

04
Examples include **password cracking**, buffer overflows, denial of service, and **session hijacking**



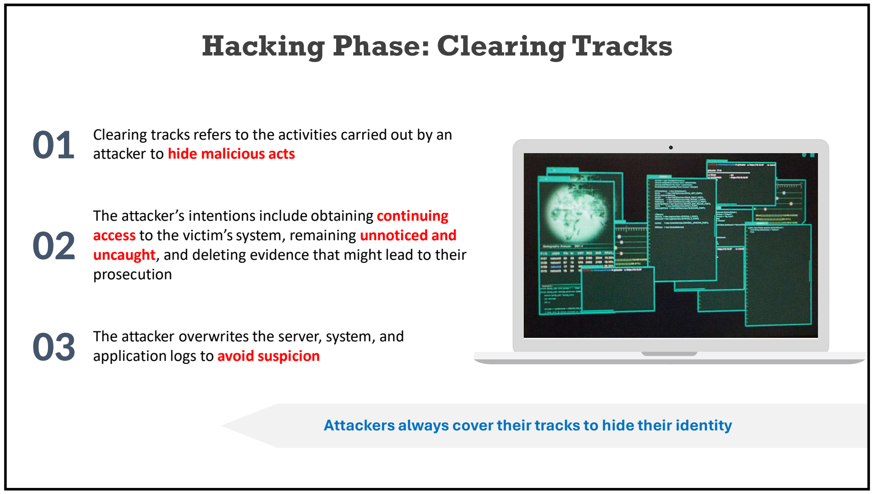
Hacking Phase: Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain their **ownership of the system**

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

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

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



Hacking Phase: Clearing Tracks

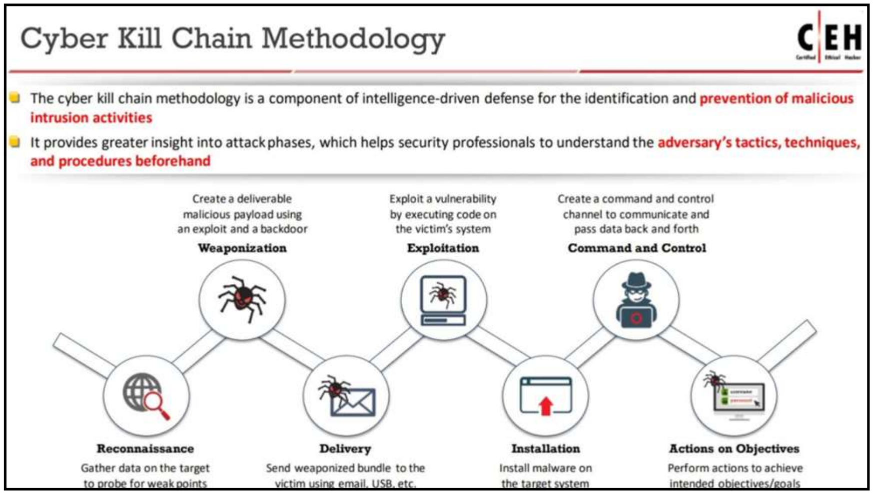
01 Clearing tracks refers to the activities carried out by an attacker to **hide malicious acts**

02 The attacker's intentions include obtaining **continuing access** to the victim's system, remaining **unnoticed and uncaught**, and deleting evidence that might lead to their prosecution

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

Attackers always cover their tracks to hide their identity

17

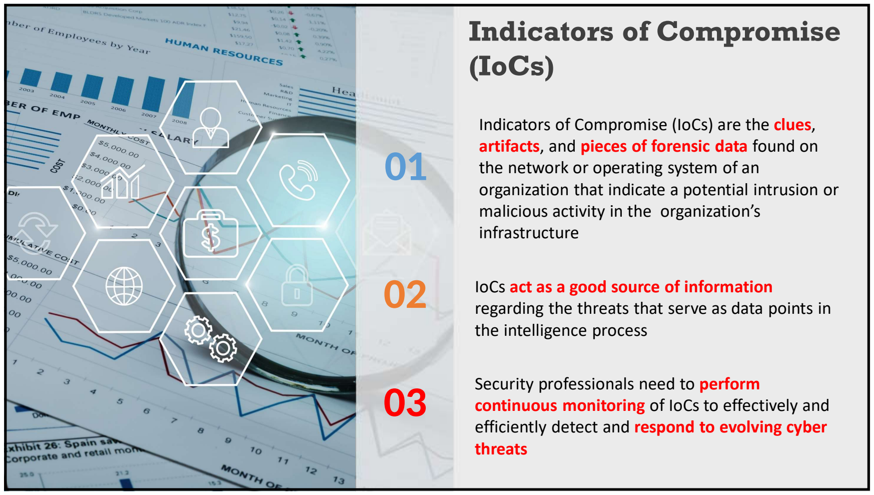


Cyber Kill Chain Methodology

- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and **prevention of malicious intrusion activities**
- It provides greater insight into attack phases, which helps security professionals to understand the **adversary's tactics, techniques, and procedures beforehand**

Create a deliverable malicious payload using an exploit and a backdoor
Weaponization
Exploit a vulnerability by executing code on the victim's system
Exploitation
Create a command and control channel to communicate and pass data back and forth
Command and Control
Reconnaissance
Gather data on the target to probe for weak points
Delivery
Send weaponized bundle to the victim using email, USB, etc.
Installation
Install malware on the target system
Actions on Objectives
Perform actions to achieve intended objectives/goals

18



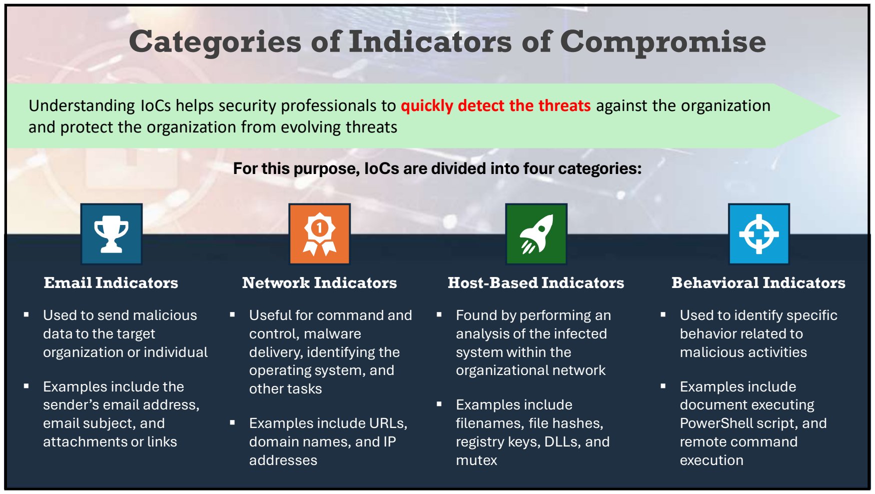
Indicators of Compromise (IoCs)

01 Indicators of Compromise (IoCs) are the **clues**, **artifacts**, and **pieces of forensic data** found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure

02 IoCs **act as a good source of information** regarding the threats that serve as data points in the intelligence process

03 Security professionals need to **perform continuous monitoring** of IoCs to effectively and efficiently detect and **respond to evolving cyber threats**

19



Categories of Indicators of Compromise

Understanding IoCs helps security professionals to **quickly detect the threats** against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:

Email Indicators

- Used to send malicious data to the target organization or individual
- Examples include the sender's email address, email subject, and attachments or links

Network Indicators

- Useful for command and control, malware delivery, identifying the operating system, and other tasks
- Examples include URLs, domain names, and IP addresses

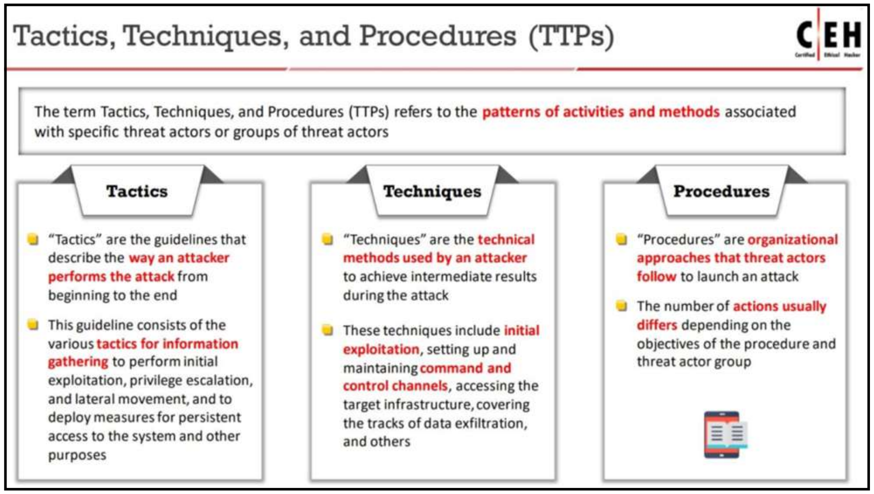
Host-Based Indicators

- Found by performing an analysis of the infected system within the organizational network
- Examples include filenames, file hashes, registry keys, DLLs, and mutex

Behavioral Indicators

- Used to identify specific behavior related to malicious activities
- Examples include document executing PowerShell script, and remote command execution

20



Tactics, Techniques, and Procedures (TTPs)

The term Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors

Tactics

- "Tactics" are the guidelines that describe the **way an attacker performs the attack** from beginning to the end
- This guideline consists of the various **tactics for information gathering** to perform initial exploitation, privilege escalation, and lateral movement, and to deploy measures for persistent access to the system and other purposes

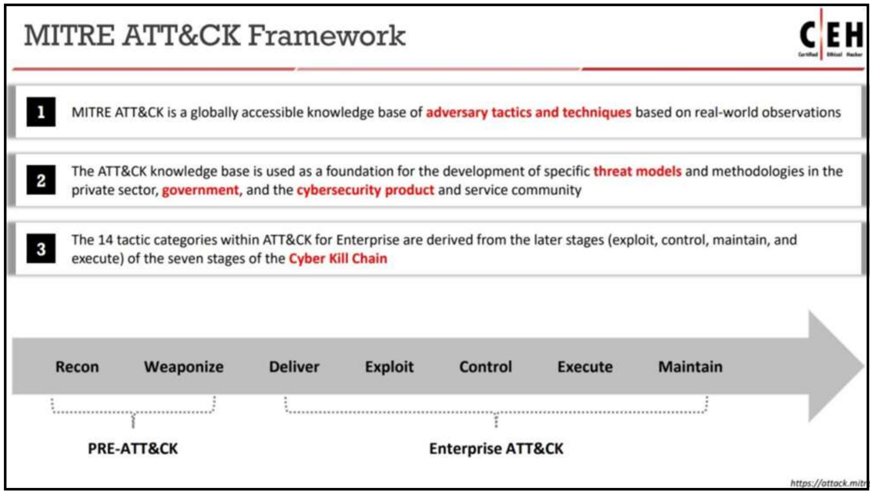
Techniques

- "Techniques" are the **technical methods used by an attacker** to achieve intermediate results during the attack
- These techniques include **initial exploitation**, setting up and maintaining **command and control channels**, accessing the target infrastructure, covering the tracks of data exfiltration, and others

Procedures

- "Procedures" are **organizational approaches that threat actors follow** to launch an attack
- The number of **actions usually differs** depending on the objectives of the procedure and threat actor group

21



MITRE ATT&CK Framework

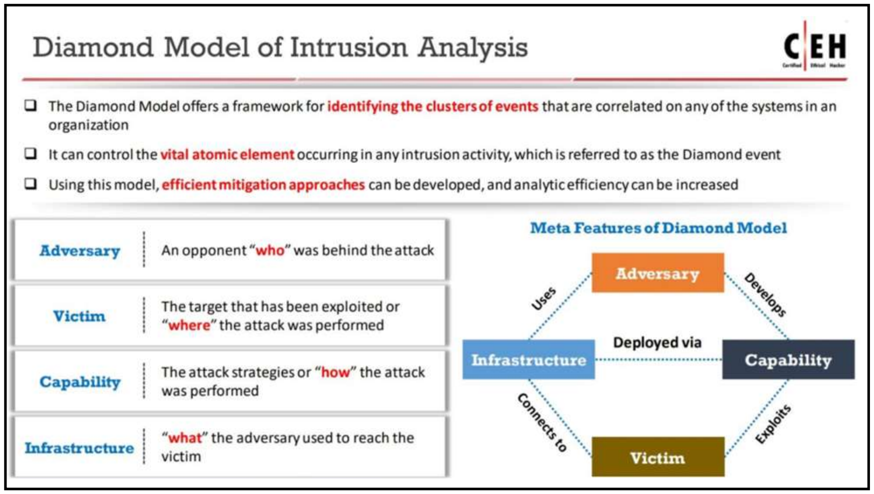
1 MITRE ATT&CK is a globally accessible knowledge base of **adversary tactics and techniques** based on real-world observations

2 The ATT&CK knowledge base is used as a foundation for the development of specific **threat models** and methodologies in the private sector, **government**, and the **cybersecurity product** and service community

3 The 14 tactic categories within ATT&CK for Enterprise are derived from the later stages (exploit, control, maintain, and execute) of the seven stages of the **Cyber Kill Chain**

https://attack.mitr

22

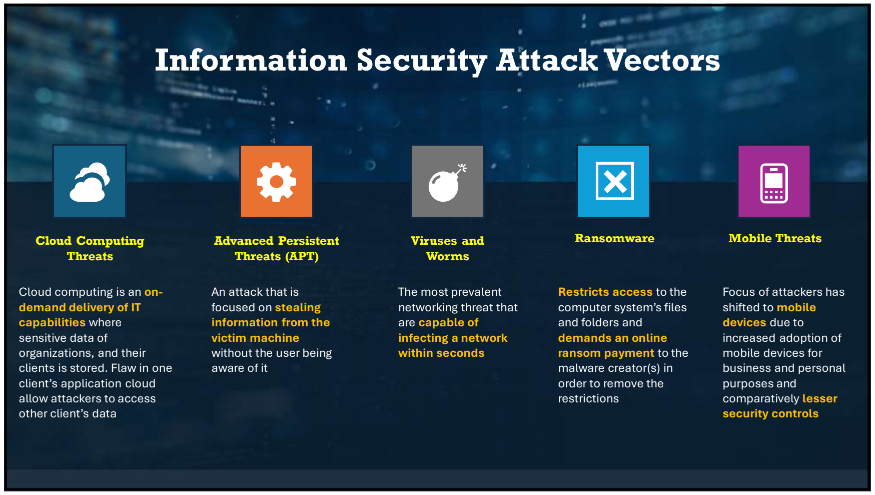


Diamond Model of Intrusion Analysis

- ❑ The Diamond Model offers a framework for **identifying the clusters of events** that are correlated on any of the systems in an organization
- ❑ It can control the **vital atomic element** occurring in any intrusion activity, which is referred to as the Diamond event
- ❑ Using this model, **efficient mitigation approaches** can be developed, and analytic efficiency can be increased

Adversary	An opponent "**who**" was behind the attack
Victim	The target that has been exploited or "**where**" the attack was performed
Capability	The attack strategies or "**how**" the attack was performed
Infrastructure	"**what**" the adversary used to reach the victim

23



Information Security Attack Vectors

Cloud Computing Threats

Cloud computing is an **on-demand delivery of IT capabilities** where sensitive data of organizations, and their clients is stored. Flaw in one client's application cloud allow attackers to access other client's data

Advanced Persistent Threats (APT)

An attack that is focused on **stealing information from the victim machine** without the user being aware of it

Viruses and Worms

The most prevalent networking threat that are **capable of infecting a network within seconds**

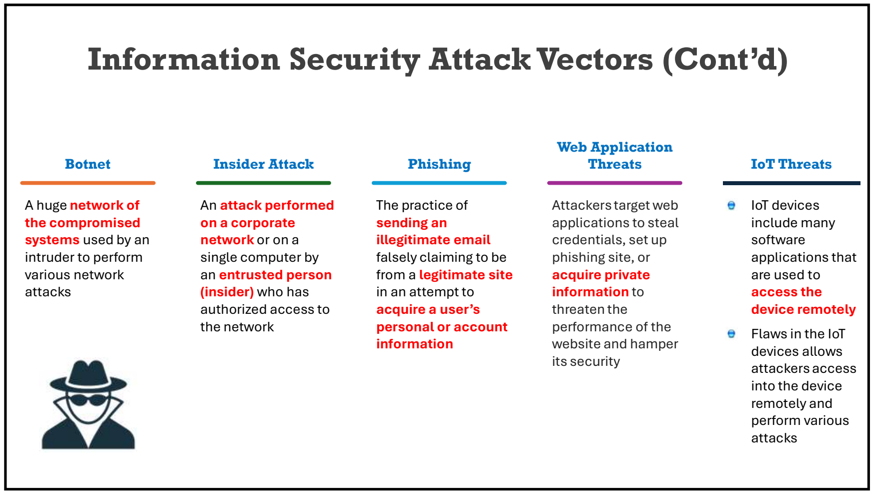
Ransomware

Restricts access to the computer system's files and folders and **demands an online ransom payment** to the malware creator(s) in order to remove the restrictions

Mobile Threats

Focus of attackers has shifted to **mobile devices** due to increased adoption of mobile devices for business and personal purposes and comparatively **lesser security controls**

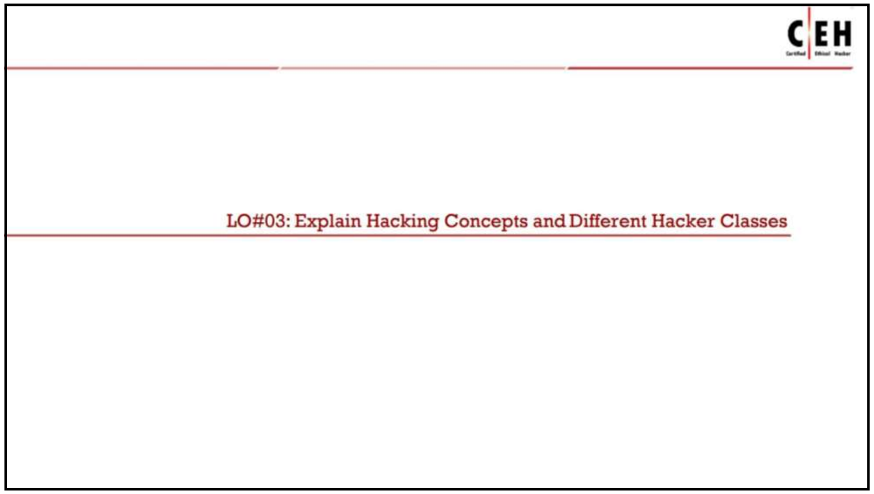
24



Information Security Attack Vectors (Cont'd)

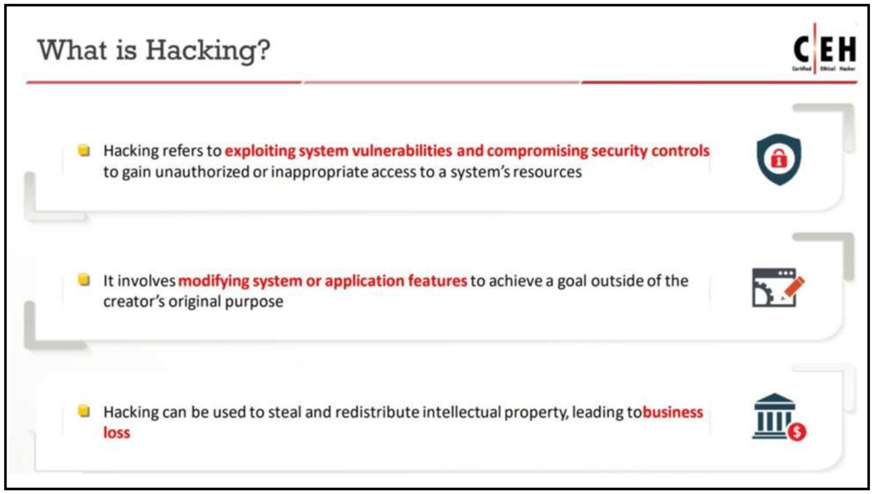
Botnet	Insider Attack	Phishing	Web Application Threats	IoT Threats
A huge **network of the compromised systems** used by an intruder to perform various network attacks	An **attack performed on a corporate network** or on a single computer by an **entrusted person (insider)** who has authorized access to the network	The practice of **sending an illegitimate email** falsely claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**	Attackers target web applications to steal credentials, set up phishing site, or **acquire private information** to threaten the performance of the website and hamper its security	- IoT devices include many software applications that are used to **access the device remotely** - Flaws in the IoT devices allows attackers access into the device remotely and perform various attacks

25



LO#03: Explain Hacking Concepts and Different Hacker Classes

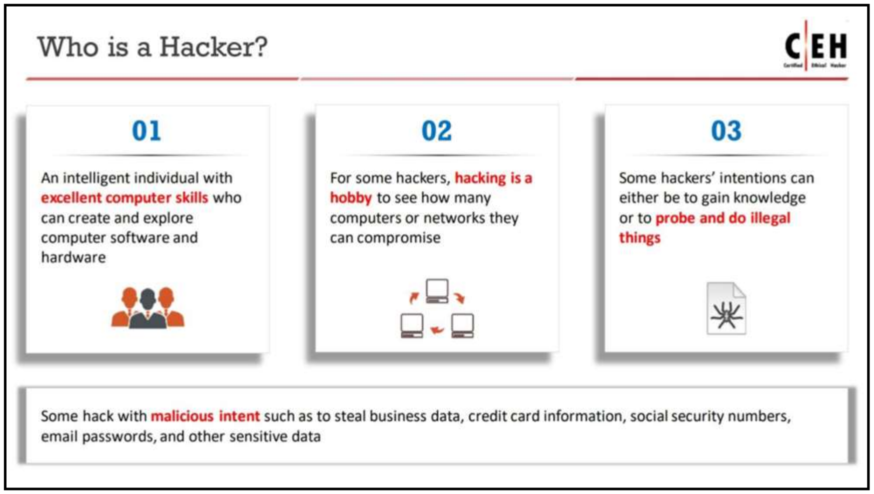
26



What is Hacking?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources
- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose
- Hacking can be used to steal and redistribute intellectual property, leading to**business loss**

27



Who is a Hacker?

01

An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware

02

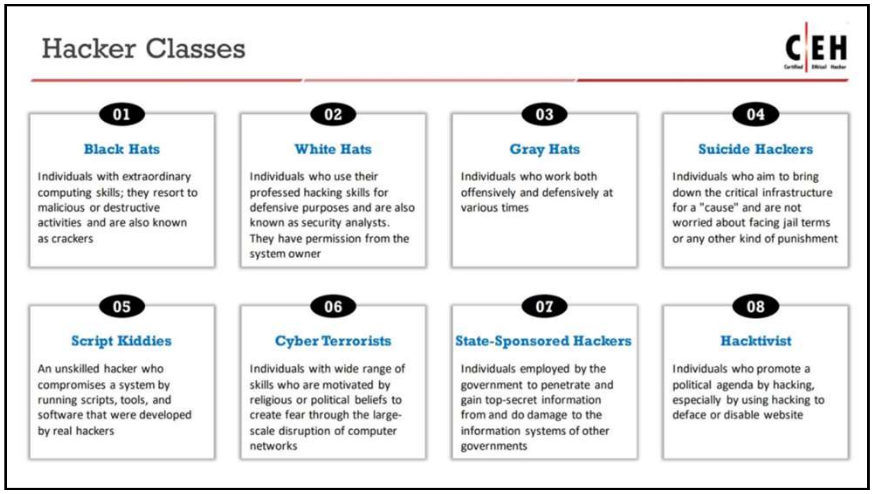
For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise

03

Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**

Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data

28



Hacker Classes

C|EH

01 Black Hats
Individuals with extraordinary computing skills; they resort to malicious or destructive activities and are also known as crackers

02 White Hats
Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner

03 Gray Hats
Individuals who work both offensively and defensively at various times

04 Suicide Hackers
Individuals who aim to bring down the critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

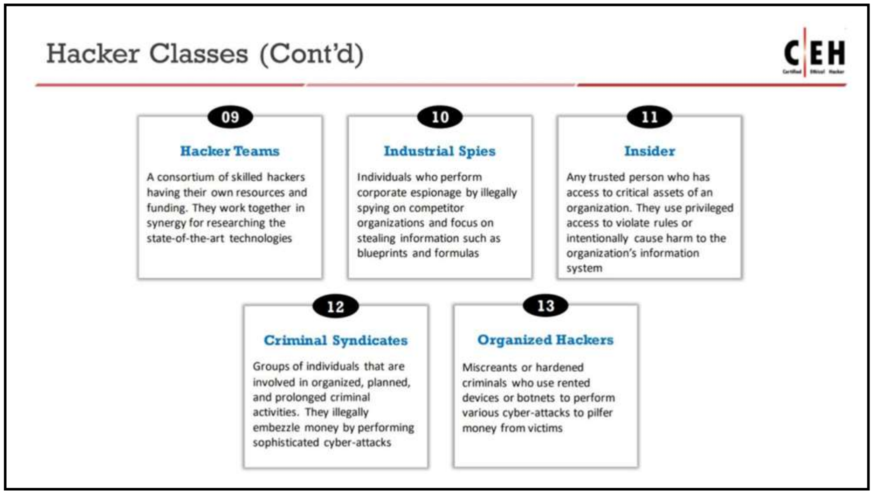
05 Script Kiddies
An unskilled hacker who compromises a system by running scripts, tools, and software that were developed by real hackers

06 Cyber Terrorists
Individuals with wide range of skills who are motivated by religious or political beliefs to create fear through the large-scale disruption of computer networks

07 State-Sponsored Hackers
Individuals employed by the government to penetrate and gain top-secret information from and do damage to the information systems of other governments

08 Hacktivist
Individuals who promote a political agenda by hacking, especially by using hacking to deface or disable website

29



Hacker Classes (Cont'd)

C|EH

09 Hacker Teams
A consortium of skilled hackers having their own resources and funding. They work together in synergy for researching the state-of-the-art technologies

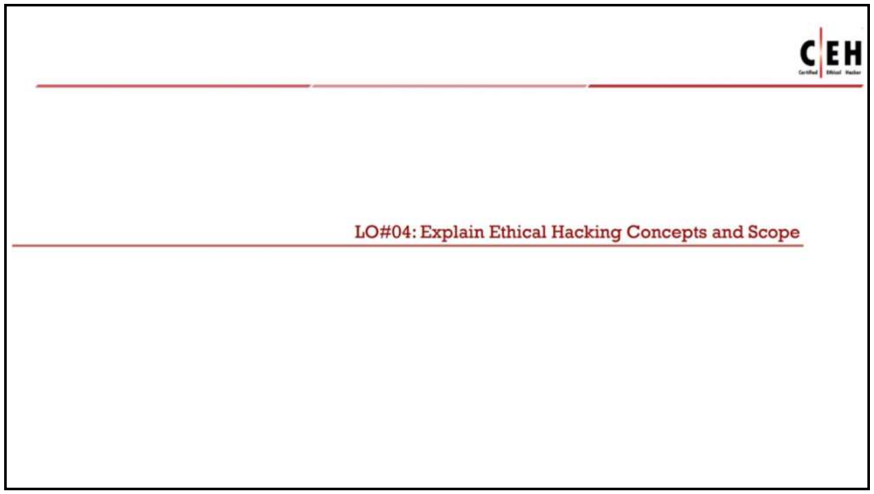
10 Industrial Spies
Individuals who perform corporate espionage by illegally spying on competitor organizations and focus on stealing information such as blueprints and formulas

11 Insider
Any trusted person who has access to critical assets of an organization. They use privileged access to violate rules or intentionally cause harm to the organization's information system

12 Criminal Syndicates
Groups of individuals that are involved in organized, planned, and prolonged criminal activities. They illegally embezzle money by performing sophisticated cyber-attacks

13 Organized Hackers
Miscreants or hardened criminals who use rented devices or botnets to perform various cyber-attacks to pilfer money from victims

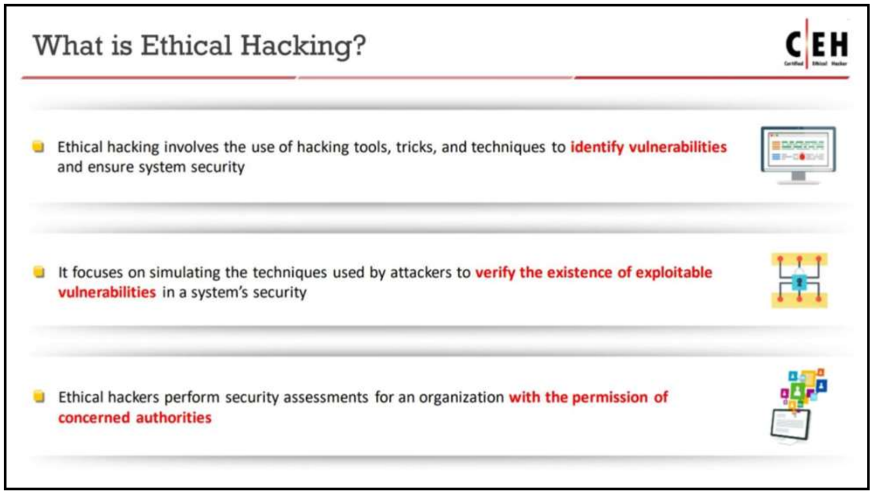
30



C|EH

LO#04: Explain Ethical Hacking Concepts and Scope

31

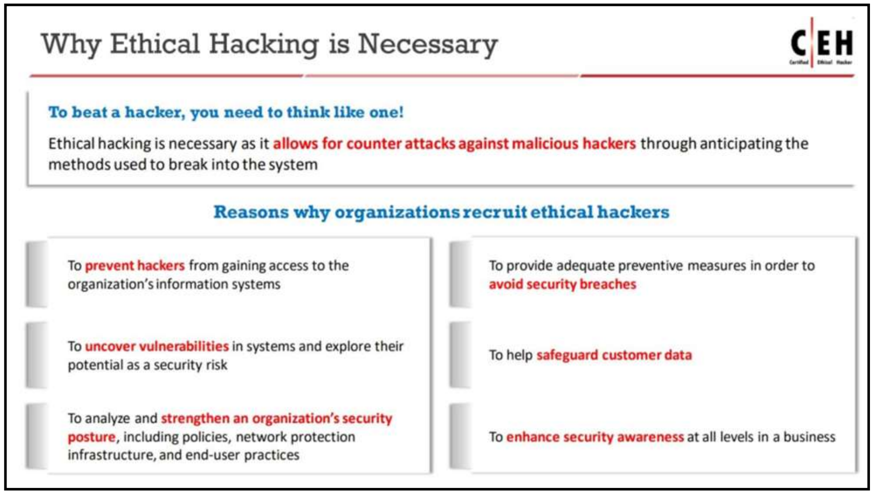


What is Ethical Hacking?

C|EH

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** and ensure system security
- It focuses on simulating the techniques used by attackers to **verify the existence of exploitable vulnerabilities** in a system's security
- Ethical hackers perform security assessments for an organization **with the permission of concerned authorities**

32



Why Ethical Hacking is Necessary

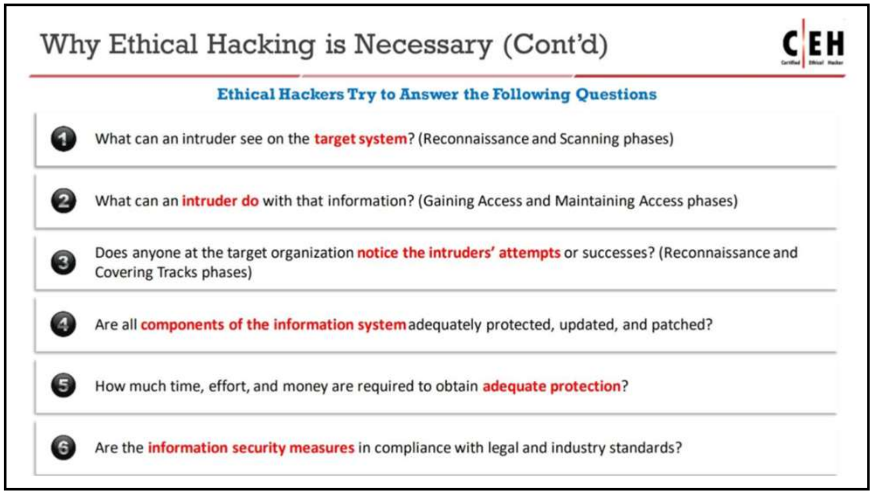
To beat a hacker, you need to think like one!

Ethical hacking is necessary as it **allows for counter attacks against malicious hackers** through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers

- To **prevent hackers** from gaining access to the organization's information systems
- To **uncover vulnerabilities** in systems and explore their potential as a security risk
- To analyze and **strengthen an organization's security posture**, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to **avoid security breaches**
- To help **safeguard customer data**
- To **enhance security awareness** at all levels in a business

33

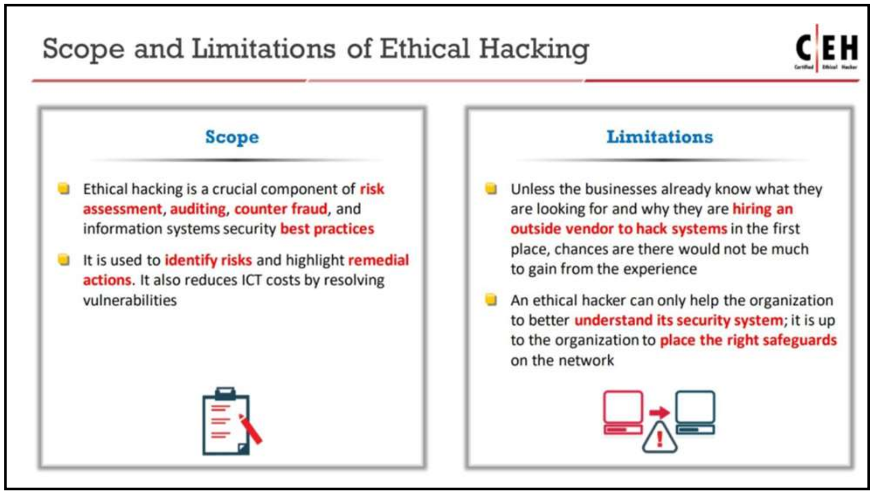


Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1. What can an intruder see on the **target system**? (Reconnaissance and Scanning phases)
2. What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
3. Does anyone at the target organization **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)
4. Are all **components of the information system** adequately protected, updated, and patched?
5. How much time, effort, and money are required to obtain **adequate protection**?
6. Are the **information security measures** in compliance with legal and industry standards?

34



Scope and Limitations of Ethical Hacking

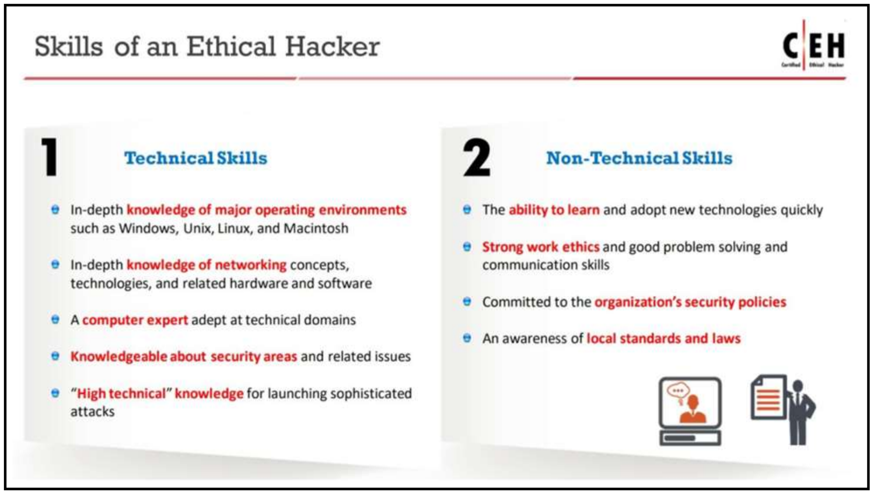
Scope

- Ethical hacking is a crucial component of **risk assessment**, **auditing**, **counter fraud**, and information systems security **best practices**
- It is used to **identify risks** and highlight **remedial actions**. It also reduces ICT costs by resolving vulnerabilities

Limitations

- Unless the businesses already know what they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience
- An ethical hacker can only help the organization to better **understand its security system**; it is up to the organization to **place the right safeguards** on the network

35



Skills of an Ethical Hacker

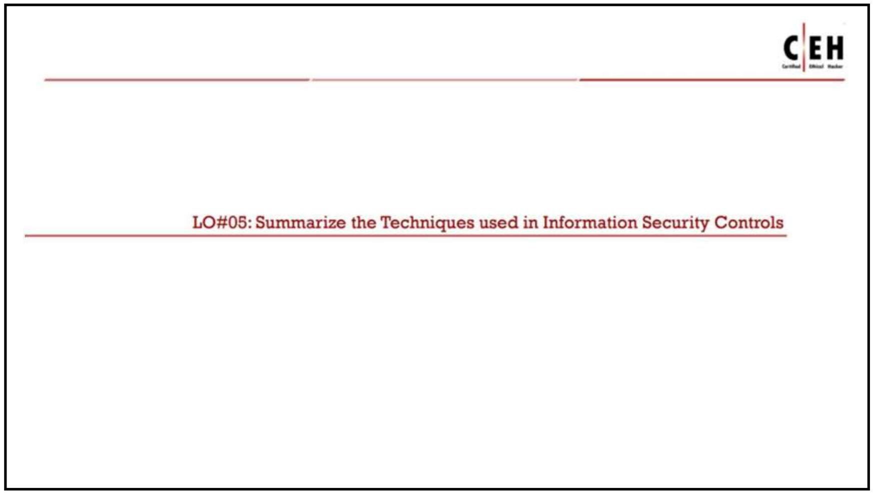
1 Technical Skills

- In-depth **knowledge of major operating environments** such as Windows, Unix, Linux, and Macintosh
- In-depth **knowledge of networking** concepts, technologies, and related hardware and software
- A **computer expert** adept at technical domains
- **Knowledgeable about security areas** and related issues
- **"High technical" knowledge** for launching sophisticated attacks

2 Non-Technical Skills

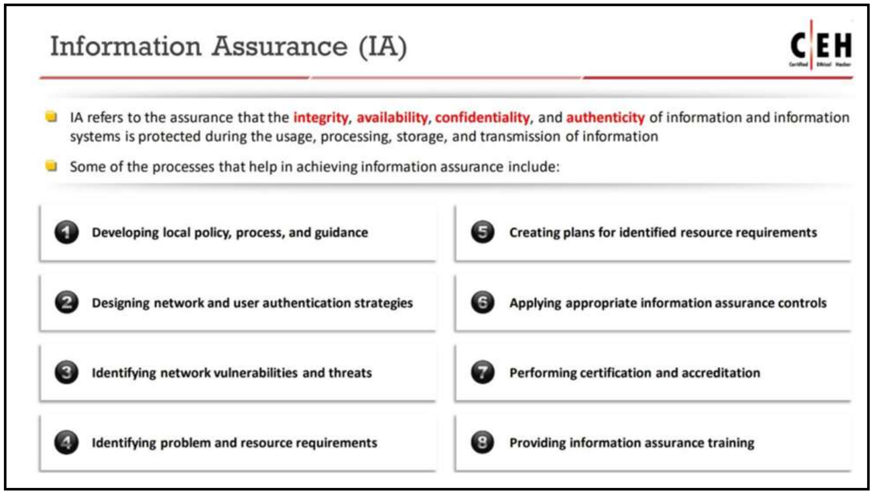
- The **ability to learn** and adopt new technologies quickly
- **Strong work ethics** and good problem solving and communication skills
- Committed to the **organization's security policies**
- An awareness of **local standards and laws**

36



LO#05: Summarize the Techniques used in Information Security Controls

37



Information Assurance (IA)

- IA refers to the assurance that the **integrity**, **availability**, **confidentiality**, and **authenticity** of information and information systems is protected during the usage, processing, storage, and transmission of information
- Some of the processes that help in achieving information assurance include:

1. **Developing local policy, process, and guidance**
2. **Designing network and user authentication strategies**
3. **Identifying network vulnerabilities and threats**
4. **Identifying problem and resource requirements**
5. **Creating plans for identified resource requirements**
6. **Applying appropriate information assurance controls**
7. **Performing certification and accreditation**
8. **Providing information assurance training**

38