Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts, Types, and Phases
4. Ethical Hacking Concepts and Scope
5. Information Security Controls
6. Information Security Laws and Standards

What is Hacking?

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system 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, pilfer, and redistribute intellectual property leading to business loss

Who is a Hacker?

C|EH Certified Ethical Hacker

01

Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware

02

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

03

Their intention can either be to gain knowledge or to poke around to do illegal things

Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

Hacker Classes

CEH Certified Ethical Hacker

1 Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

2 White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

3 Gray Hats

Individuals who work both offensively and defensively at various times

4 Suicide Hackers

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

5 Script Kiddies

An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

6 Cyber Terrorists

Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

7 State Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

8 Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites

Hacking Phases: 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

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

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

Port Scanner

Extract Information

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

Hacking Phases: Gaining Access

C|EH Certified Ethical Hacker

- Reconn-aissance
- Scanning
- **Gaining Access**
- Mainta-ining Access
- Clearing Tracks

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

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

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

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

Hacking Phases: Maintaining Access

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

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

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

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

Hacking Phases: Clearing Tracks

01

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

02

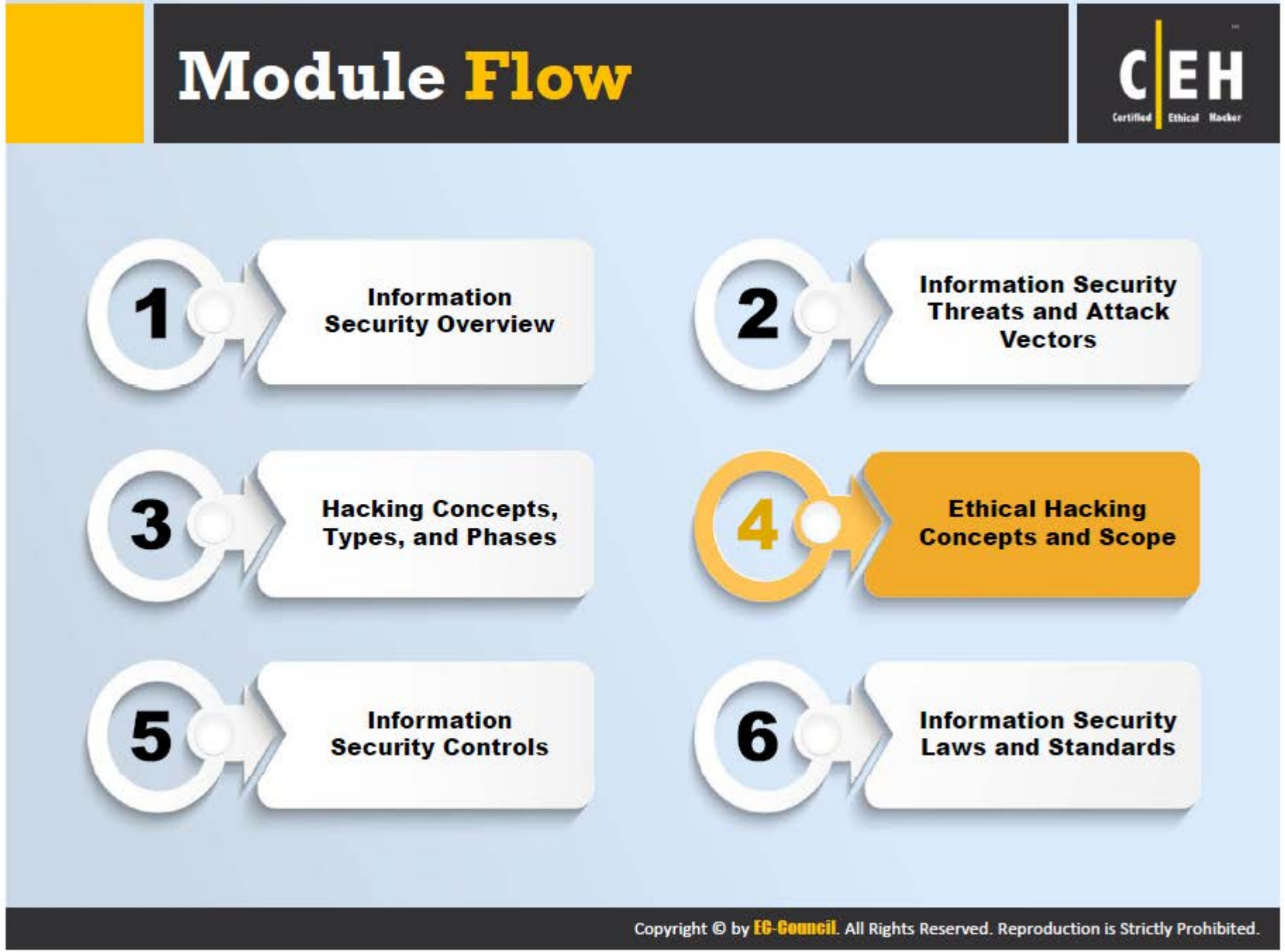
The attacker's intentions include: **Continuing access** to the victim's system, remaining **unnoticed and uncaught**, deleting evidence that might lead to his prosecution

03

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

Attackers always cover tracks to hide their identity

Module Flow



What is Ethical Hacking?

Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security

It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security

Ethical hackers performs security assessment of their organization **with the permission of concerned authorities**

Why Ethical Hacking is Necessary

C|EH Certified Ethical Hacker

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

Ethical hacking is necessary as it **allows to counter attacks from malicious hackers** by anticipating methods used by them to break into a system

Reasons why Organizations Recruit Ethical Hackers

To **prevent hackers** from gaining access to organization's information systems

To **uncover vulnerabilities** in systems and explore their potential as a risk

To analyze and **strengthen an organization's security posture** including policies, network protection infrastructure, and end-user practices

Why Ethical Hacking is Necessary (Cont'd)

C|EH Certified Ethical Hacker

Ethical Hackers Try to Answer the Following Questions

What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)

What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)

Does anyone at the target **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)

If all the **components of information system** are adequately protected, updated, and patched

How much effort, time, and money is required to obtain **adequate protection**?

Are the **information security measures** in compliance to industry and legal standards?

Skills of an Ethical Hacker

C|EH Certified 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**