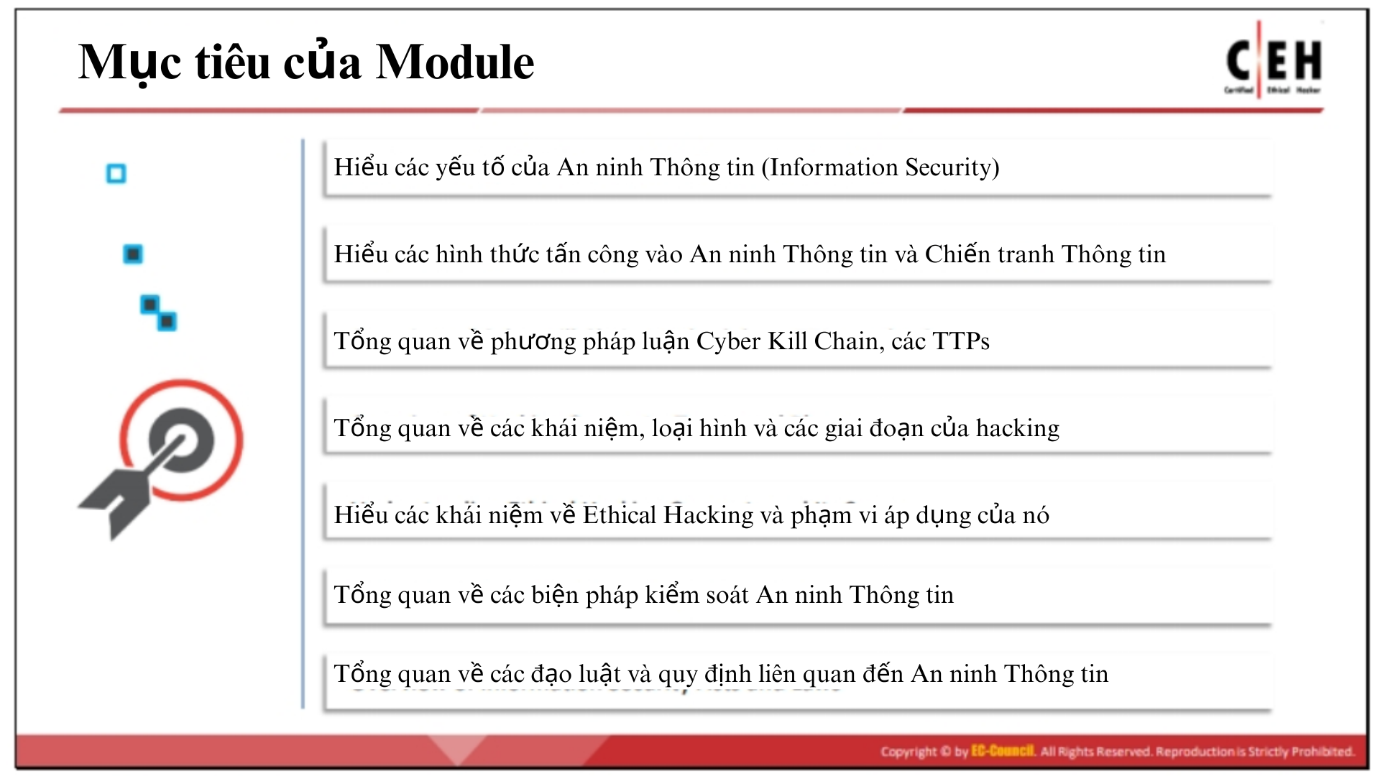
**Module 01: Giới thiệu về Ethical Hacking**



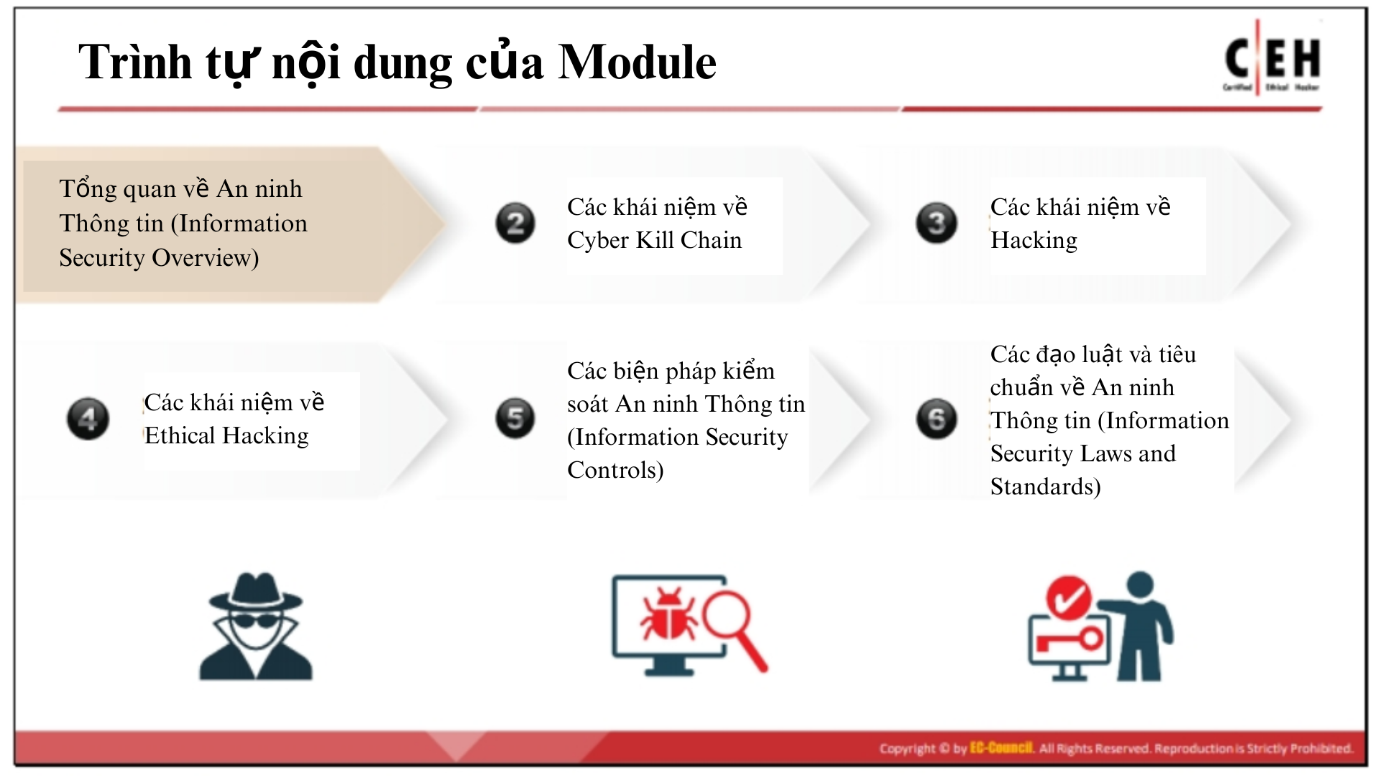
**Mục tiêu của Module**

Kẻ tấn công (attacker) xâm nhập vào hệ thống vì nhiều lý do và mục đích khác nhau. Do đó, điều quan trọng là phải hiểu cách mà các hacker độc hại (malicious hackers) tấn công và khai thác hệ thống, cũng như những động cơ có thể đứng sau các cuộc tấn công đó. Như Tôn Tử đã viết trong *Binh pháp*:  
**“Biết người biết ta, trăm trận trăm thắng. Biết mình mà không biết người, đánh một thắng một bại.”**  
Các quản trị viên hệ thống và chuyên gia an ninh cần bảo vệ hạ tầng của mình khỏi các lỗ hổng bị khai thác bằng cách **hiểu rõ kẻ thù**—tức là các hacker độc hại—những kẻ tìm cách sử dụng chính hạ tầng đó cho các hoạt động phi pháp.

Module này bắt đầu bằng cái nhìn tổng quan về bối cảnh an ninh hiện tại và các hướng tấn công (threat vectors) mới nổi. Nội dung cung cấp cái nhìn chuyên sâu về các yếu tố khác nhau của **An ninh Thông tin (Information Security)**. Tiếp theo, module thảo luận về các khái niệm liên quan đến **hacking** và **ethical hacking**, và kết thúc bằng phần trình bày ngắn gọn về các biện pháp kiểm soát an ninh thông tin cũng như các đạo luật và quy định liên quan.

**Sau khi hoàn thành module này, bạn sẽ có thể:**

* Mô tả các yếu tố cấu thành của An ninh Thông tin (Information Security)
* Giải thích các hình thức tấn công An ninh Thông tin và Chiến tranh Thông tin (Information Security Attacks và Information Warfare)
* Mô tả phương pháp luận **Cyber Kill Chain**, các **TTPs** (Tactics, Techniques, and Procedures – Chiến thuật, Kỹ thuật và Quy trình) và các **IoCs** (Indicators of Compromise – Chỉ báo bị xâm phạm)
* Trình bày các khái niệm, loại hình và các giai đoạn của **hacking**
* Giải thích các khái niệm về **Ethical Hacking** và phạm vi áp dụng
* Hiểu các biện pháp kiểm soát An ninh Thông tin (chẳng hạn như: phòng thủ nhiều lớp – *defense-in-depth*, quản lý rủi ro – *risk management*, tình báo mối đe dọa mạng – *cyber threat intelligence*, mô hình hóa mối đe dọa – *threat modeling*, quy trình xử lý sự cố – *incident management process*, và ứng dụng AI/ML trong bảo mật)
* Nắm được các đạo luật và quy định về An ninh Thông tin (Information Security Acts and Laws)



**Tổng quan về An ninh Thông tin (Information Security Overview)**

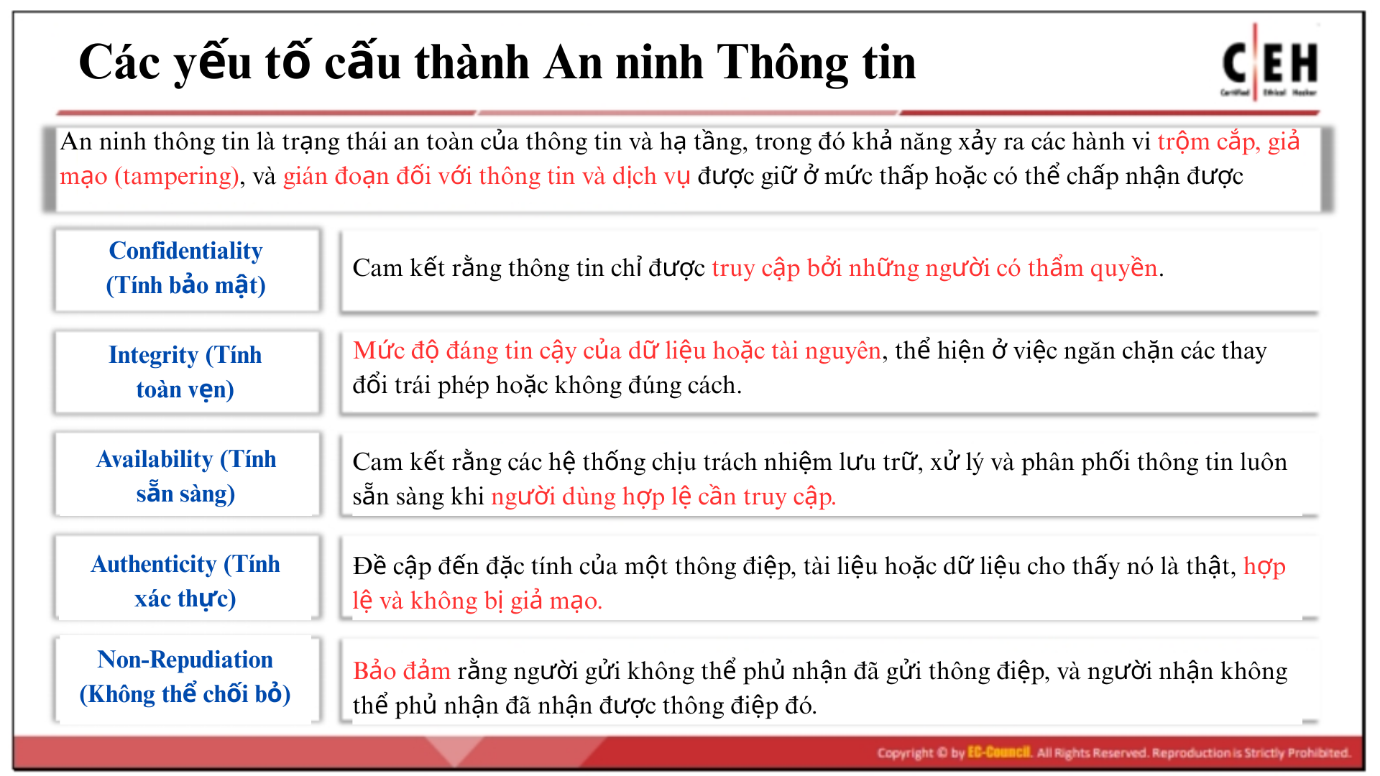
**An ninh Thông tin (Information Security)** là việc bảo vệ hoặc gìn giữ thông tin và các hệ thống thông tin—những hệ thống sử dụng, lưu trữ và truyền tải thông tin khỏi các hành vi truy cập trái phép, tiết lộ, thay đổi hoặc phá hủy thông tin.

Thông tin là một tài sản quan trọng (critical asset) mà mọi tổ chức đều phải bảo vệ. Nếu thông tin nhạy cảm rơi vào tay kẻ xấu, tổ chức đó có thể phải gánh chịu những tổn thất nghiêm trọng như thiệt hại tài chính, ảnh hưởng đến uy tín thương hiệu, mất khách hàng hoặc những hậu quả khác.

Để giúp người học hiểu được cách bảo vệ các tài nguyên thông tin quan trọng như vậy, module này mở đầu bằng phần tổng quan về **an ninh thông tin**.

Phần này sẽ giới thiệu:

* **Các yếu tố cấu thành An ninh Thông tin (Elements of Information Security)**
* **Phân loại các hình thức tấn công (Classification of Attacks)**
* **Chiến tranh thông tin (Information Warfare)**



**Các yếu tố của An ninh Thông tin (Elements of Information Security)**

**An ninh thông tin** được định nghĩa là *“trạng thái an toàn của thông tin và hạ tầng, trong đó khả năng xảy ra các hành vi trộm cắp, giả mạo hoặc gián đoạn thông tin và dịch vụ được giữ ở mức thấp hoặc trong phạm vi chấp nhận được.”*  
An ninh thông tin dựa trên 5 yếu tố cốt lõi: **Confidentiality (bảo mật), Integrity (toàn vẹn), Availability (sẵn sàng), Authenticity (xác thực)** và **Non-repudiation (không thể chối bỏ)**.

**1. Confidentiality (Tính bảo mật)**

Tính bảo mật là sự đảm bảo rằng thông tin **chỉ có thể được truy cập bởi các đối tượng được ủy quyền**.  
Sự cố vi phạm bảo mật có thể xảy ra do xử lý dữ liệu không đúng cách hoặc do bị tấn công (ví dụ: hacking).

**Các biện pháp kiểm soát bảo mật thông tin bao gồm**:

* Phân loại dữ liệu (data classification)
* Mã hóa dữ liệu (data encryption)
* Tiêu hủy đúng cách các thiết bị lưu trữ (chẳng hạn như đĩa DVD, USB, Blu-ray…)

**2. Integrity (Tính toàn vẹn)**

Tính toàn vẹn là **mức độ đáng tin cậy của dữ liệu hoặc tài nguyên**, đảm bảo rằng dữ liệu không bị thay đổi một cách **trái phép hoặc không phù hợp**, và **đủ chính xác** cho mục đích sử dụng của nó.

**Các biện pháp duy trì toàn vẹn dữ liệu có thể bao gồm**:

* **Checksum**: số kiểm tra được tạo bởi một hàm toán học để xác minh dữ liệu không bị thay đổi
* **Kiểm soát truy cập (access control)**: chỉ cho phép người dùng được ủy quyền thực hiện cập nhật, thêm hoặc xóa dữ liệu

*Checksum*: Còn gọi là mã kiểm, thường dùng trong truyền tải hoặc lưu trữ dữ liệu để phát hiện lỗi hoặc can thiệp trái phép.

**3. Availability (Tính sẵn sàng)**

Tính sẵn sàng là sự đảm bảo rằng **các hệ thống chịu trách nhiệm phân phối, lưu trữ và xử lý thông tin** luôn có thể truy cập được **bởi những người dùng hợp lệ khi cần thiết**.

**Các biện pháp bảo đảm tính sẵn sàng có thể bao gồm**:

* Hệ thống lưu trữ dự phòng (disk arrays), máy chủ được cụm hóa (clustered machines)
* Phần mềm chống mã độc (antivirus software)
* Hệ thống ngăn chặn tấn công từ chối dịch vụ phân tán (**DDoS prevention**)

*DDoS (Distributed Denial of Service)*: hình thức tấn công làm quá tải tài nguyên của hệ thống khiến dịch vụ không thể truy cập được bởi người dùng hợp pháp.

**4. Authenticity (Tính xác thực)**

Tính xác thực liên quan đến đặc tính của một thông điệp, tài liệu hoặc dữ liệu bảo đảm rằng nó **là thật, không bị giả mạo hoặc thay đổi**.  
Vai trò chính của xác thực là **xác minh tính hợp lệ của người dùng hoặc thông tin**.

**Các phương pháp kiểm soát xác thực bao gồm**:

* Sinh trắc học (biometrics)
* Thẻ thông minh (smart cards)
* Chứng thư số (digital certificates)

*Digital certificate*: Chứng nhận điện tử do một bên thứ ba (CA) phát hành, xác nhận danh tính và khóa công khai của người dùng.

**5. Non-Repudiation (Không thể chối bỏ)**

Không thể chối bỏ là cơ chế đảm bảo rằng **người gửi không thể phủ nhận việc đã gửi thông điệp**, và **người nhận không thể phủ nhận việc đã nhận**.  
Điều này rất quan trọng trong các giao dịch pháp lý, tài chính và thương mại điện tử.

**Cách thức thực hiện:**

* Sử dụng chữ ký số (digital signatures) để xác nhận hành động gửi/nhận một cách rõ ràng và có thể kiểm chứng.

*Digital signature*: Cơ chế mã hóa không thể giả mạo, được dùng để xác minh danh tính và nội dung một cách không thể phủ nhận.