# Modul 1: Introduction to Ethical Hacking

Memahami dunia keamanan siber dari sudut pandang yang benar — bukan sebagai ancaman, melainkan sebagai garda pertahanan digital.

EDY SUSANTO · FOUNDER C-SIX SECURITY

Gambaran Modul

# Apa yang Akan Kamu Pelajari?

Modul ini dirancang untuk membangun fondasi yang kuat sebelum kamu terjun ke dunia ethical hacking. Dari konsep dasar hingga etika profesi, semua akan dibahas secara menyeluruh.

01

## Konsep Dasar

Cyber Security, Ethical Hacker, dan tipe-tipe hacker

02

## Ancaman & Kerangka Kerja

CIA Triad, jenis ancaman siber modern, dan Cyber Kill Chain

03

## Hukum & Etika

Batas legal ethical hacking dan membangun mindset profesional

04

## Praktik & Outcome

Analisis kasus nyata dan menyusun roadmap belajar pribadi

# Apa Itu Cyber Security?

Cyber Security adalah praktik melindungi sistem, jaringan, dan program dari serangan digital yang bertujuan mengakses, mengubah, atau menghancurkan informasi sensitif — atau mengganggu proses bisnis normal.

### Kerahasiaan

Menjaga data hanya dapat diakses oleh pihak yang berwenang

### Integritas

Memastikan data tidak dimodifikasi oleh pihak yang tidak sah

### Ketersediaan

Memastikan sistem dan data selalu dapat diakses saat dibutuhkan

# Siapa Itu Ethical Hacker?

Ethical Hacker — juga dikenal sebagai **Penetration Tester** atau **White Hat Hacker** — adalah profesional keamanan yang diberi izin resmi untuk mencoba menembus sistem komputer, jaringan, atau aplikasi. Tujuannya bukan untuk merusak, melainkan untuk **menemukan celah keamanan sebelum penyerang jahat menemukannya**.

Ethical hacker bekerja dengan kontrak, izin tertulis, dan mengikuti metodologi yang terstruktur. Hasil temuan mereka dilaporkan kepada pemilik sistem untuk segera diperbaiki.

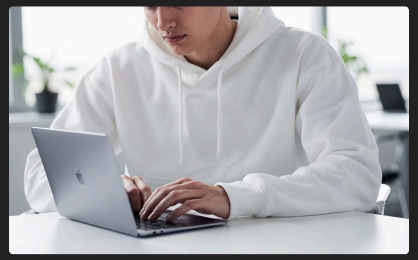
Ethical hacking adalah pekerjaan legal yang sangat dibutuhkan industri — dengan permintaan yang terus meningkat setiap tahunnya.

### Tugas Utama

- Melakukan penetration testing
- Mengidentifikasi kerentanan sistem
- Menulis laporan temuan
- Merekomendasikan solusi keamanan
- Membantu tim blue team memperkuat pertahanan

# White Hat, Gray Hat, dan Black Hat

Dalam dunia hacking, warna "topi" melambangkan motivasi dan legalitas tindakan seorang hacker. Memahami perbedaan ini sangat penting untuk menentukan posisi dan integritas kamu sebagai profesional.



## White Hat

Hacker etis yang bekerja secara legal dengan izin penuh. Membantu organisasi menemukan dan memperbaiki celah keamanan. Profesi resmi dan sangat dihargai.

## Gray Hat

Beroperasi di zona abu-abu — kadang tanpa izin resmi, namun tidak selalu bermotif jahat. Bisa melaporkan temuan atau meminta bayaran. Status hukumnya tidak jelas.

## Black Hat

Hacker berbahaya yang menyerang sistem tanpa izin untuk keuntungan pribadi, sabotase, atau pencurian data. Tindakan mereka ilegal dan dapat berujung hukuman berat.

# Jenis-Jenis Ancaman Siber Modern

Lanskap ancaman siber terus berkembang. Berikut adalah ancaman yang paling umum dan berbahaya yang wajib dipahami oleh setiap calon security professional.

### Malware

Perangkat lunak berbahaya seperti virus, trojan, ransomware yang dirancang untuk merusak atau mencuri data.

### Phishing

Serangan rekayasa sosial yang mengelabui korban untuk menyerahkan kredensial atau informasi sensitif.

### SQL Injection

Eksploitasi kerentanan database melalui input berbahaya untuk mengakses atau memanipulasi data.

### DDoS Attack

Membanjiri server dengan traffic palsu hingga sistem lumpuh dan tidak dapat melayani pengguna sah.

### Zero-Day Exploit

Serangan yang memanfaatkan kerentanan yang belum diketahui atau belum diperbaiki oleh vendor.

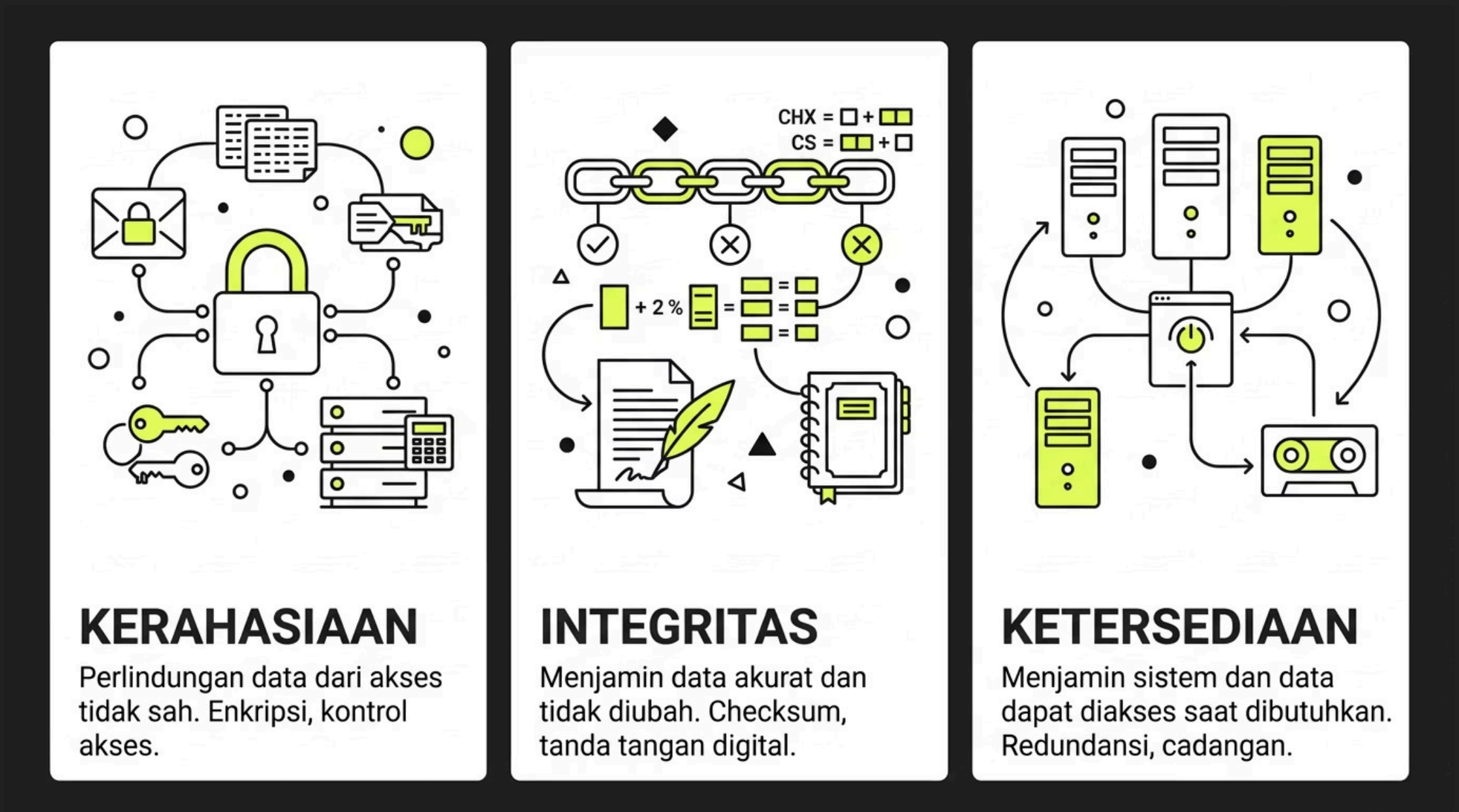
### Man-in-the-Middle

Penyerang menyadap komunikasi antara dua pihak tanpa sepengetahuan mereka untuk mencuri data.

Kerangka Keamanan

# Memahami CIA Triad

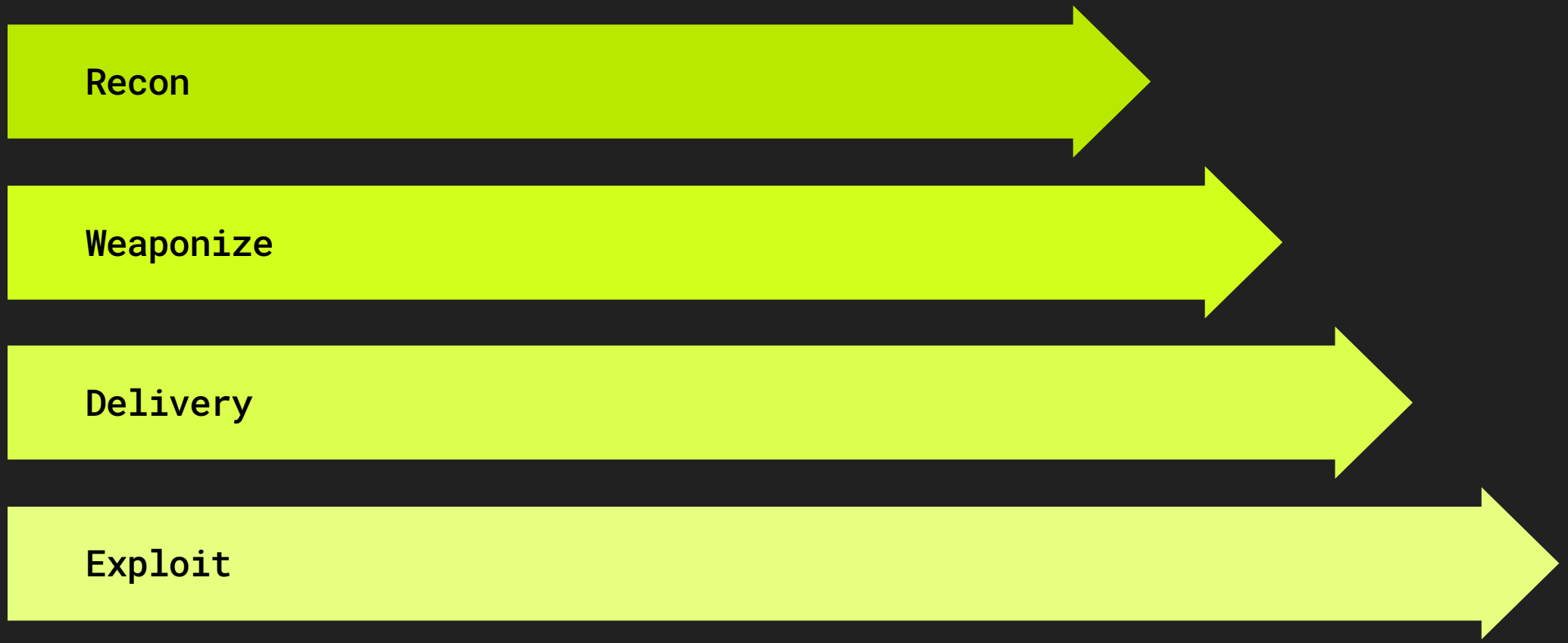
CIA Triad adalah fondasi dari seluruh konsep keamanan informasi. Ketiga pilar ini menjadi acuan dalam merancang, mengevaluasi, dan merespons setiap aspek keamanan sistem.




Setiap keputusan keamanan — dari memilih enkripsi hingga merancang infrastruktur — harus mempertimbangkan ketiga elemen ini secara seimbang. Pelanggaran terhadap salah satunya dapat berdampak serius pada bisnis dan kepercayaan pengguna.

# Cyber Kill Chain

Dikembangkan oleh Lockheed Martin, Cyber Kill Chain adalah model yang menggambarkan tahapan serangan siber dari awal hingga akhir. Memahami model ini membantu defender memutus rantai serangan di tahap sedini mungkin.




Semakin awal rantai ini diputus, semakin kecil dampak serangan yang terjadi. Ethical hacker menggunakan kerangka ini untuk mensimulasikan serangan nyata dan mengidentifikasi titik lemah pertahanan pada setiap tahap.

Aspek Legal

# Hukum dan Etika Ethical Hacking

## Dasar Hukum di Indonesia

- **UU ITE No. 11/2008** — mengatur akses ilegal ke sistem elektronik
- **PP No. 82/2012** — penyelenggaraan sistem elektronik
- **UU PDP No. 27/2022** — perlindungan data pribadi

## Prinsip Etika Wajib

- Selalu dapatkan izin tertulis sebelum pengujian
- Jaga kerahasiaan temuan dan data klien
- Laporkan semua temuan secara transparan
- Jangan melebihi scope yang disepakati
- Tidak menyimpan atau menyalahgunakan data yang ditemukan

⊗ Melakukan akses tanpa izin ke sistem orang lain — meskipun dengan niat baik — tetap merupakan tindakan ilegal dan dapat dikenai sanksi hukum yang berat.

# Membangun Mindset Security Professional

Menjadi ethical hacker bukan hanya soal menguasai tools — ini tentang cara berpikir. Seorang security professional sejati memiliki pola pikir yang membedakan mereka dari sekadar "script kiddie".

## Berpikir Seperti Penyerang

Selalu bertanya: "Bagaimana saya bisa menembus ini?" sebelum bertanya "Bagaimana saya melindunginya?"

## Belajar Tanpa Henti

Ancaman siber terus berkembang. Security professional harus selalu mengikuti perkembangan terbaru.

## Integritas Tinggi

Kepercayaan adalah aset terbesar. Selalu bertindak dalam batas etika dan hukum, bahkan ketika tidak ada yang mengawasi.

## Problem Solver

Setiap sistem unik. Kemampuan berpikir kreatif dan analitis adalah kunci keberhasilan dalam setiap engagement.

Studi Kasus

# Serangan Siber Nyata yang Mengubah Dunia

Mempelajari kasus nyata adalah cara terbaik untuk memahami dampak serangan siber dan pentingnya pertahanan yang solid.

### WannaCry Ransomware (2017)

Menyerang lebih dari **200.000 komputer** di 150 negara dalam 4 hari. Mengeksploitasi kerentanan Windows yang belum dipatch. Kerugian diperkirakan mencapai **$4 miliar**.

### SolarWinds Supply Chain Attack (2020)

Penyerang menyusup ke software update resmi SolarWinds, menginfeksi **18.000+ organisasi** termasuk lembaga pemerintah AS. Salah satu serangan paling canggih dalam sejarah.

### Bjorka – Indonesia (2022)

Hacker anonim membocorkan data **105 juta warga Indonesia** dari KPU, serta data pelanggan Indihome dan Telkomsel. Menjadi alarm keras bagi keamanan data nasional.

# Praktik: Mengenali Kasus Serangan Siber

## Tujuan Praktik

Melatih kemampuan analisis untuk mengidentifikasi jenis serangan, tahap kill chain, dan vektor yang digunakan dalam kasus nyata.

## Yang Akan Dilakukan

- Membaca laporan insiden keamanan
- Mengidentifikasi jenis ancaman
- Memetakan ke Cyber Kill Chain
- Diskusi solusi pencegahan

## Pertanyaan Analisis

1. Apa vektor awal serangan masuk ke sistem?
2. Di tahap mana Kill Chain seharusnya dapat diputus?
3. Pilar CIA Triad mana yang dilanggar?
4. Apa kontrol keamanan yang seharusnya sudah ada?
5. Apa pelajaran terpenting dari kasus ini?

Gunakan template analisis yang disediakan dan presentasikan temuan kamu di depan kelas.


# Praktik: Membuat Roadmap Belajar Cyber Security Pribadi

Setiap perjalanan belajar itu unik. Pada sesi ini, kamu akan menyusun roadmap yang realistis dan personal berdasarkan tujuan karier, kekuatan, dan waktu belajar yang kamu miliki.

1

## Kenali Dirimu

Tentukan tujuan karier, skill saat ini, dan berapa jam per minggu yang bisa kamu dedikasikan

2

## Pilih Jalur Spesialisasi

Penetration Testing, Blue Team, Digital Forensics, Cloud Security, atau Bug Bounty Hunter

3

## Tentukan Milestone

Sertifikasi target (CEH, OSCP, CompTIA), platform belajar, dan proyek praktik yang akan dikerjakan

# Jalur Karier Ethical Hacker

Dunia cyber security menawarkan berbagai jalur karier yang menjanjikan. Temukan posisi yang paling sesuai dengan minat dan kekuatanmu.

## Penetration Tester

Menguji keamanan sistem secara profesional dengan simulasi serangan nyata. Gaji rata-rata: $70K–$130K/tahun.

## SOC Analyst

Memantau dan merespons insiden keamanan secara real-time dari Security Operations Center.

## Digital Forensics

Menyelidiki insiden siber, mengumpulkan bukti digital, dan mendukung proses hukum jika diperlukan.

## Bug Bounty Hunter

Mencari celah keamanan di platform perusahaan besar dan mendapatkan hadiah atas setiap temuan valid.

Ringkasan Modul 1

# Outcome & Langkah Selanjutnya

## Yang Sudah Kamu Kuasai

- Definisi Cyber Security dan peran Ethical Hacker
- Perbedaan White, Gray, dan Black Hat Hacker
- Jenis-jenis ancaman siber modern
- CIA Triad sebagai fondasi keamanan informasi
- Model Cyber Kill Chain
- Batas hukum dan etika dalam ethical hacking

## Langkah Selanjutnya

- Selesaikan analisis kasus serangan siber
- Finalisasi roadmap belajar pribadimu
- Bergabung dengan komunitas: Hack The Box, TryHackMe
- Ikuti Modul 2: Networking & Reconnaissance Fundamentals

Kamu sudah selangkah lebih dekat menjadi Security Professional!

*Edy Susanto · Founder C-SIX Security*