Modul 1 – Introduction to Online Pentesting

Pelajari metodologi dasar penetration testing, mulai dari konsep hingga praktik nyata. Modul ini dirancang untuk pemula dan praktisi keamanan siber yang ingin membangun fondasi kuat dalam dunia pengujian keamanan secara online.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Gambaran Modul

Tujuan Pembelajaran

Di akhir modul ini, peserta akan mampu memahami metodologi dasar penetration testing, mengenal tools yang digunakan secara online, serta menerapkan prinsip-prinsip etika dan legalitas dalam setiap tahapan pengujian keamanan.

🎯 Pemahaman Konsep

Menguasai definisi, tujuan, dan ruang lingkup penetration testing secara menyeluruh

⚙️ Penguasaan Alur

Memahami alur kerja pentest dari reconnaissance hingga pelaporan

⚖️ Etika & Legalitas

Menerapkan prinsip hukum dan etika dalam setiap aktivitas pengujian

🧪 Praktik Lab

Menentukan target sah dan menyusun checklist pentest dasar

Apa itu Penetration Testing?

Penetration Testing (atau "pentest") adalah proses simulasi serangan siber yang dilakukan secara resmi dan terstruktur terhadap sistem, jaringan, atau aplikasi untuk menemukan celah keamanan sebelum penyerang nyata memanfaatkannya.

Tujuan Utama

- Mengidentifikasi kelemahan sistem
- Menguji efektivitas kontrol keamanan
- Membantu organisasi memperbaiki postur keamanannya

Siapa yang Melakukannya?

- **Ethical Hacker** – profesional bersertifikat
- **Red Team** – tim internal/eksternal khusus
- **Security Researcher** – peneliti independen

EDY SUSANTO - FOUNDER C-SIX SECURITY

Konsep Dasar

Rules of Engagement

Rules of Engagement (RoE) adalah dokumen perjanjian resmi antara penguji keamanan dan klien yang mendefinisikan batasan, izin, dan prosedur selama proses pentest berlangsung. Tanpa RoE, setiap aktivitas pengujian berpotensi melanggar hukum.

📋 Ruang Lingkup

Mendefinisikan sistem, IP, atau aplikasi mana saja yang **boleh** dan **tidak boleh** diuji selama proses berlangsung.

🕐 Batasan Waktu

Menentukan jadwal pengujian — termasuk jam operasional yang diizinkan agar tidak mengganggu layanan produksi.

📞 Prosedur Darurat

Menetapkan kontak darurat jika ditemukan kerentanan kritis selama pengujian yang membutuhkan respons segera.

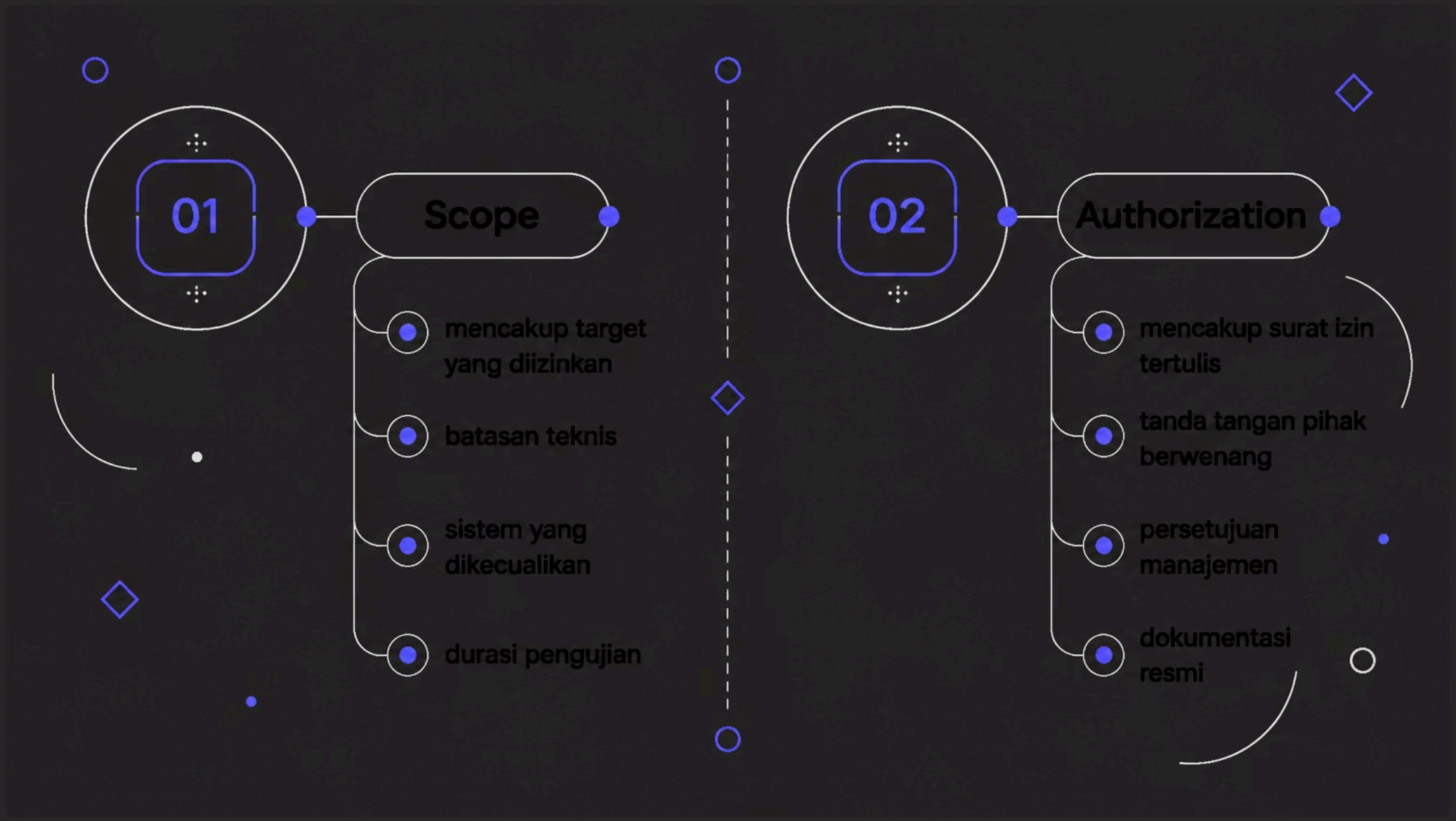
📄 Format Pelaporan

Menentukan bagaimana temuan dikomunikasikan — format laporan, tingkat kerahasiaan, dan kepada siapa hasilnya diserahkan.

Konsep Dasar

Scope & Authorization

Sebelum memulai pentest, **scope (ruang lingkup)** dan **authorization (otorisasi)** harus ditetapkan secara tertulis. Ini adalah fondasi legalitas seluruh kegiatan pengujian — tanpa keduanya, aktivitas pentest dapat dikategorikan sebagai tindak kejahatan siber.



⚠ ⚠️ Mengakses sistem tanpa otorisasi tertulis adalah **tindakan ilegal** di Indonesia berdasarkan UU ITE Pasal 30.

Alur Kerja

Pentest Workflow

Setiap pentest profesional mengikuti alur kerja yang terstruktur. Memahami tahapan ini memastikan pengujian dilakukan secara sistematis, dapat diulang, dan menghasilkan temuan yang dapat ditindaklanjuti.

Alur ini bersifat **iteratif** — penguji sering kembali ke tahap sebelumnya saat menemukan informasi baru yang mengubah strategi serangan.

Tahapan Kritis

Reconnaissance vs Exploitation

🔍 Reconnaissance

Fase pengumpulan informasi tentang target **sebelum** melakukan serangan aktif. Tujuannya adalah memetakan permukaan serangan seluas mungkin.

- **Passive Recon**: OSINT, Google Dorking, Whois
- **Active Recon**: Port scanning, banner grabbing
- Tidak memodifikasi atau menyentuh sistem target

💥 Exploitation

Fase aktif di mana penguji mencoba memanfaatkan kerentanan yang ditemukan untuk mendapatkan akses tidak sah ke sistem target.

- Menggunakan exploit atau payload yang sesuai
- Memanfaatkan misconfiguration dan kelemahan logika
- Mendokumentasikan setiap langkah serangan

ⓘ 💡 Recon yang baik adalah kunci sukses exploitation. Semakin detail informasi yang dikumpulkan, semakin terarah serangan yang dapat dilakukan.

Etika & Hukum

Legal & Ethical Considerations

Seorang penguji keamanan profesional tidak hanya wajib memiliki izin tertulis, tetapi juga harus menjunjung tinggi **etika profesi** dan memahami **kerangka hukum** yang berlaku di Indonesia.

UU ITE Indonesia

UU No. 11/2008 jo UU No. 19/2016 mengatur tentang akses ilegal terhadap sistem elektronik. Pelanggaran dapat dikenai pidana penjara hingga **8 tahun**.

Responsible Disclosure

Temuan kerentanan wajib dilaporkan kepada pemilik sistem sesuai prosedur. Tidak diperbolehkan mempublikasikan atau menjual informasi kerentanan.

Kerahasiaan Data

Semua data yang diperoleh selama pentest bersifat rahasia dan hanya digunakan untuk tujuan pengujian. Non-disclosure agreement (NDA) wajib ditandatangani.

Batasan Teknis

Penguji tidak boleh melampaui scope yang telah disepakati, merusak data, atau mengganggu ketersediaan layanan tanpa izin eksplisit.

Etika Profesional

Hacker Hitam vs Putih vs Abu-Abu

Dalam dunia keamanan siber, istilah "warna topi" digunakan untuk membedakan motivasi dan legalitas aktivitas hacking. Sebagai peserta kursus ini, Anda berlatih untuk menjadi **White Hat** — penguji keamanan yang bekerja secara legal dan etis.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Sesi Praktik

Menentukan Target Lab yang Sah

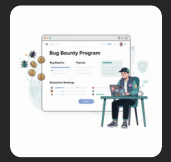
Praktik pentest harus dilakukan di lingkungan yang **aman, legal, dan terkontrol**. Berikut adalah platform dan environment yang direkomendasikan untuk berlatih tanpa risiko hukum:

Platform CTF Online

Hack The Box, TryHackMe, dan PicoCTF menyediakan mesin virtual yang dirancang khusus untuk dieksploitasi. Semua aktivitas sepenuhnya legal dan ada sistem poin serta panduan belajar terstruktur.

Lab Virtual Lokal

Bangun lab sendiri menggunakan VirtualBox atau VMware dengan OS seperti Metasploitable, DVWA, atau VulnHub. Anda memiliki kontrol penuh atas lingkungan pengujian tanpa terkoneksi ke internet.



Program Bug Bounty

Platform seperti HackerOne dan Bugcrowd menyediakan program resmi di mana perusahaan mengizinkan peneliti menemukan bug dengan imbalan finansial. Setiap target memiliki scope yang jelas dan legal.

Sesi Praktik

Menyusun Checklist Pentest Dasar

Checklist adalah alat bantu penting yang memastikan tidak ada tahapan yang terlewat selama proses pengujian. Berikut adalah checklist pentest dasar yang wajib dikuasai peserta modul ini:

📌 Pre-Engagement

- [x] ~~Dapatkan otorisasi tertulis dari klien~~
- [x] ~~Tentukan scope dan batasan target~~
- [x] ~~Tandatangani NDA dan RoE~~
- [x] ~~Siapkan environment pengujian~~
- [ ] Dokumentasikan baseline sistem target

📌 Selama Pengujian

- [ ] Lakukan reconnaissance pasif terlebih dahulu
- [ ] Catat semua temuan secara real-time
- [ ] Screenshot bukti setiap temuan
- [ ] Jangan melampaui scope yang disepakati
- [ ] Laporkan temuan kritis segera ke klien

✅ Checklist yang baik adalah pembeda antara penguji amatir dan profesional. Biasakan menggunakannya di setiap penugasan.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Outcome Modul 1

Apa yang Telah Anda Kuasai?

Selamat! Dengan menyelesaikan Modul 1 ini, Anda telah membangun fondasi yang kuat untuk perjalanan Anda sebagai seorang **Ethical Hacker profesional**. Berikut adalah kompetensi yang telah Anda capai:

Memahami Konsep Penetration Testing

Definisi, tujuan, jenis pentest, dan perbedaan antara black box, white box, dan grey box testing.

Menguasai Rules of Engagement & Scope

Menyusun dan memahami dokumen legal yang melindungi penguji dan klien selama proses berlangsung.

Mengikuti Pentest Workflow

Memahami alur kerja dari perencanaan, reconnaissance, eksploitasi, hingga pelaporan secara sistematis.

Menerapkan Prinsip Legal & Etika

Memahami UU ITE, responsible disclosure, dan batas-batas profesional dalam kegiatan pengujian keamanan.

> *"Ethical hacking bukan tentang melanggar aturan — ini tentang memahami aturan lebih baik dari siapa pun, lalu menggunakannya untuk melindungi."*
>
> — Edy Susanto, Founder C-SIX Security

EDY SUSANTO - FOUNDER C-SIX SECURITY