Modul 4: Information Gathering & Reconnaissance

Pelajari cara mengumpulkan informasi target secara **legal, sistematis, dan profesional** menggunakan teknik dan alat yang digunakan oleh para praktisi keamanan siber dunia.

C-SIX SECURITY

EDY SUSANTO — FOUNDER C-SIX SECURITY

Gambaran Umum

Tujuan Pembelajaran

Pada modul ini, peserta akan membangun kemampuan dasar dan lanjutan dalam proses pengumpulan informasi sebelum pengujian penetrasi. Setiap teknik yang dipelajari menggunakan pendekatan **etis dan legal**.

🔍 Memahami Teknik

Footprinting, OSINT, Whois, DNS Enumeration, dan Google Dorking.

🛠️ Menguasai Tools

Whois, Nslookup, Maltego CE, dan Shodan untuk pengumpulan data nyata.

🎯 Outcome Profesional

Mampu melakukan reconnaissance secara terstruktur dan dapat dipertanggungjawabkan.

Edy Susanto — Founder C-SIX Security

Bab 1

Apa Itu Footprinting?

Footprinting adalah tahap pertama dalam siklus hacking etis, di mana seorang penguji mengumpulkan sebanyak mungkin informasi tentang target **sebelum** melakukan serangan atau pengujian aktif. Tujuannya adalah memahami "jejak digital" yang ditinggalkan oleh suatu organisasi di internet.

Footprinting dibagi menjadi dua jenis utama:

- **Passive Footprinting** — mengumpulkan informasi tanpa berinteraksi langsung dengan target, misalnya melalui mesin pencari dan database publik.
- **Active Footprinting** — berinteraksi langsung dengan sistem target, seperti melakukan ping, traceroute, atau port scanning.

Edy Susanto — Founder C-SIX Security

Bab 2

Open Source Intelligence (OSINT)

OSINT adalah disiplin pengumpulan informasi yang memanfaatkan **sumber-sumber yang tersedia secara publik** — seperti website, media sosial, forum, repositori kode, dan dokumen pemerintah — untuk membangun gambaran lengkap tentang sebuah target.

Sumber Pasif

Mesin pencari, WHOIS database, arsip web, laporan tahunan perusahaan, dan publikasi pers.

Sumber Semi-Aktif

LinkedIn, GitHub, forum teknis, dan platform developer yang memuat informasi teknis internal.

Keunggulan OSINT

Tidak meninggalkan jejak pada sistem target, legal digunakan, dan memberikan konteks yang luas sebelum pengujian teknis dimulai.

Edy Susanto — Founder C-SIX Security

Bab 3

Whois Lookup

Whois adalah protokol yang memungkinkan siapapun untuk menanyakan informasi registrasi sebuah domain atau blok IP kepada database registrar. Data yang diperoleh sangat berguna dalam tahap awal reconnaissance.

Informasi yang Dapat Diperoleh

- Nama pemilik domain dan organisasi
- Tanggal registrasi dan kedaluwarsa
- Nama server (nameserver) yang digunakan
- Informasi kontak: email, telepon, alamat
- Registrar dan status domain

Cara Penggunaan

Gunakan terminal dengan perintah:

```
whois target.com
whois 8.8.8.8
```

Atau akses melalui layanan web seperti **who.is**, **whois.domaintools.com**, atau **ARIN/APNIC** untuk informasi blok IP regional Asia-Pasifik.

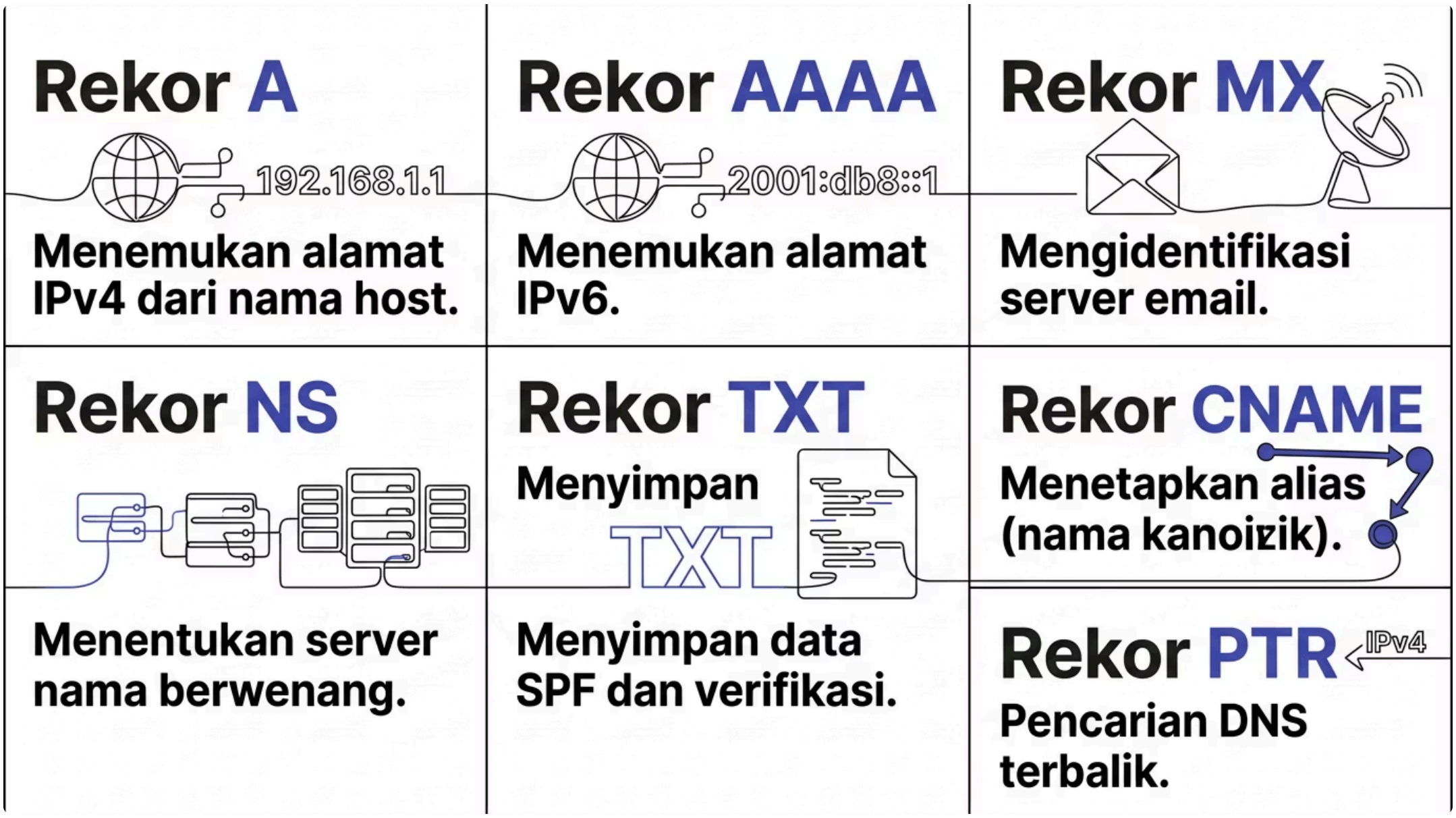
> ⓘ Privasi WHOIS kini banyak dilindungi oleh layanan privacy protection, namun data historis masih bisa diakses melalui tools tertentu.

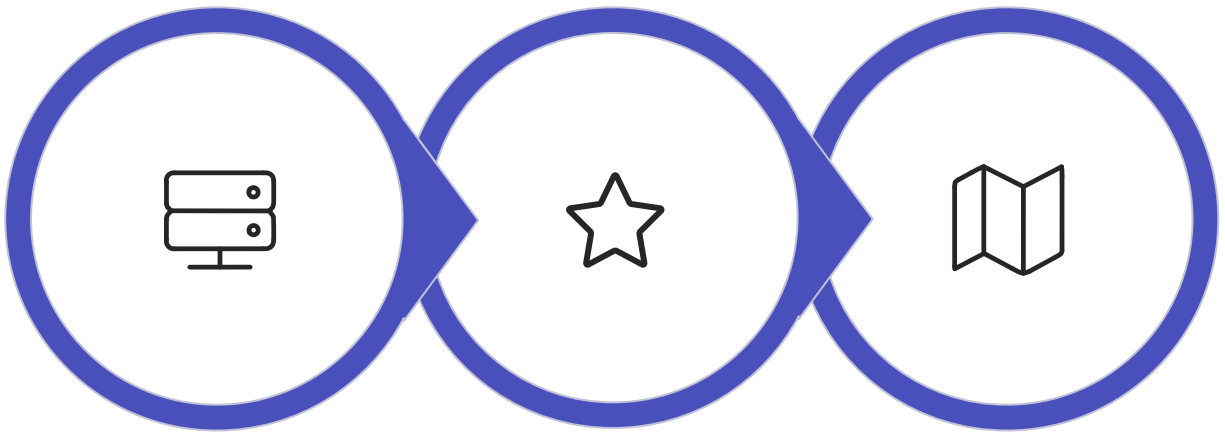
Edy Susanto — Founder C-SIX Security

Bab 4

DNS Enumeration

DNS Enumeration adalah proses mengidentifikasi semua record DNS yang terkait dengan sebuah domain. Informasi ini dapat mengungkap infrastruktur jaringan target, server yang digunakan, dan potensi titik masuk.

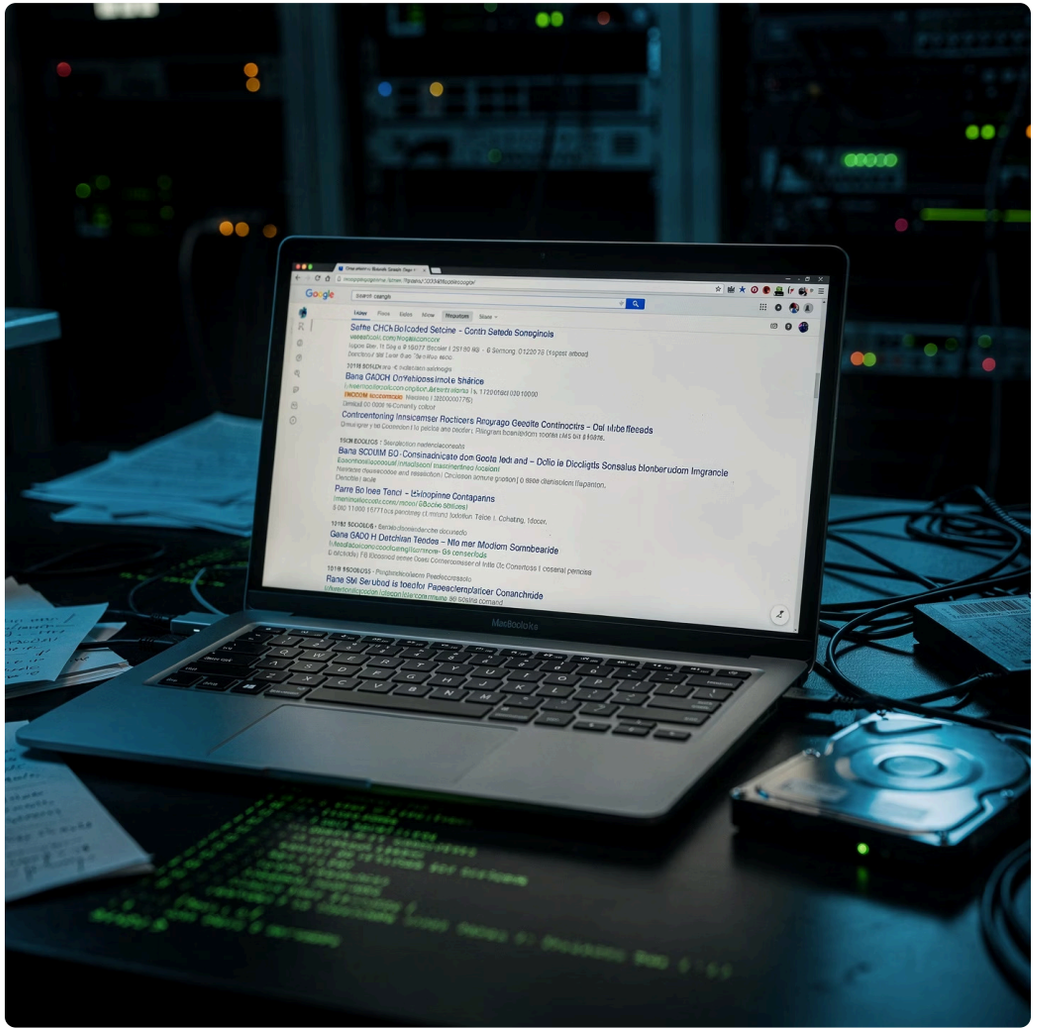




Edy Susanto — Founder C-SIX Security

Bab 5

Google Dorking



Google Dorking (atau Google Hacking) adalah teknik menggunakan **operator pencarian lanjutan** Google untuk menemukan informasi sensitif yang tidak sengaja terekspos di internet oleh target.

Operator-operator penting yang wajib dikuasai:

- `site:target.com` — membatasi pencarian hanya pada domain tertentu
- `filetype:pdf` — mencari file dengan ekstensi spesifik
- `intitle:"index of"` — menemukan direktori terbuka
- `inurl:admin` — mencari halaman administrasi
- `intext:"password"` — mencari konten berisi kata kunci sensitif

> ⚠ Gunakan teknik ini hanya pada sistem yang Anda miliki izin resmi untuk mengujinya. Penyalahgunaan dapat melanggar hukum ITE Indonesia.

Edy Susanto — Founder C-SIX Security

Bab 6

Social Media Intelligence (SOCMINT)

SOCMINT adalah cabang OSINT yang berfokus pada penggalian informasi dari platform media sosial. Profil LinkedIn, Twitter/X, Instagram, dan Facebook sering mengandung data berharga yang dapat dieksploitasi dalam tahap awal serangan siber.

LinkedIn

Mengungkap struktur organisasi, nama karyawan, jabatan, teknologi yang digunakan, dan proses rekrutmen yang menyebut stack teknologi internal.

Platform Umum

Facebook, Instagram, dan Twitter dapat mengungkap lokasi fisik, kebiasaan, jadwal, dan koneksi personal yang rentan terhadap serangan social engineering.

GitHub & Forum Dev

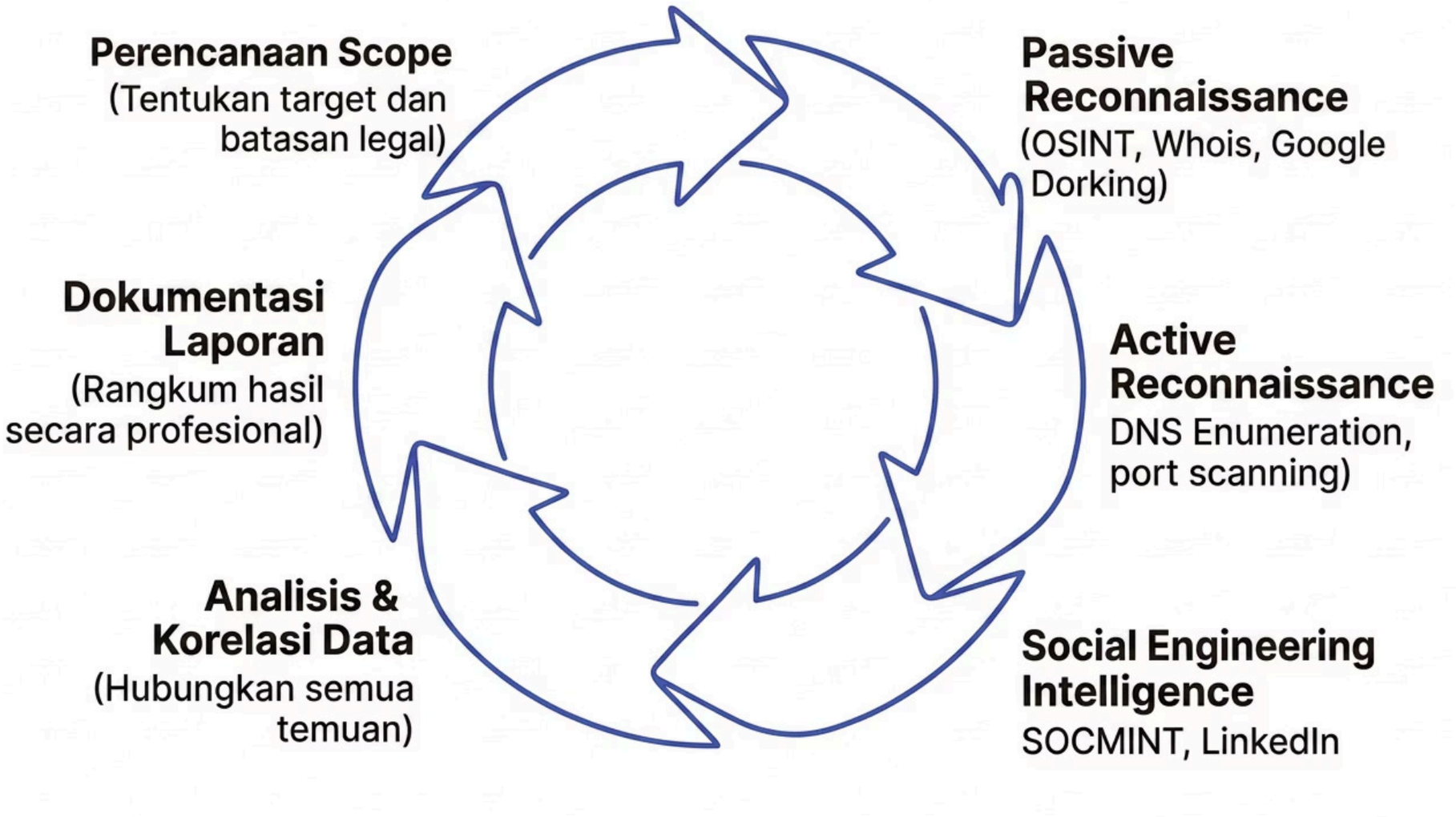
Developer sering mengunggah kode yang mengandung API key, kredensial database, atau konfigurasi server secara tidak sengaja ke repositori publik.

Edy Susanto — Founder C-SIX Security

Metodologi

Reconnaissance Methodology

Proses reconnaissance yang profesional tidak dilakukan secara acak. Ada metodologi terstruktur yang memastikan informasi dikumpulkan secara komprehensif, efisien, dan dapat didokumentasikan dengan baik.



Edy Susanto — Founder C-SIX Security

Tools

Perangkat Utama Reconnaissance

Whois

Tool baris perintah standar untuk mengambil data registrasi domain dan IP. Tersedia di Linux/macOS secara native. Gunakan `whois domain.com` untuk memulai.

Nslookup & Dig

Alat DNS query untuk mengekstraksi record A, MX, NS, dan TXT dari sebuah domain. `nslookup -type=MX domain.com` mengungkap server email target.

Maltego Community Edition

Platform visual OSINT yang menghubungkan entitas seperti domain, IP, email, dan nama orang dalam graf interaktif. Versi Community Edition gratis untuk keperluan edukasi.

Shodan

Disebut sebagai "mesin pencari untuk perangkat IoT dan server," Shodan mengindeks perangkat yang terhubung ke internet beserta informasi port, banner, dan layanannya.

Edy Susanto — Founder C-SIX Security

Praktik 1

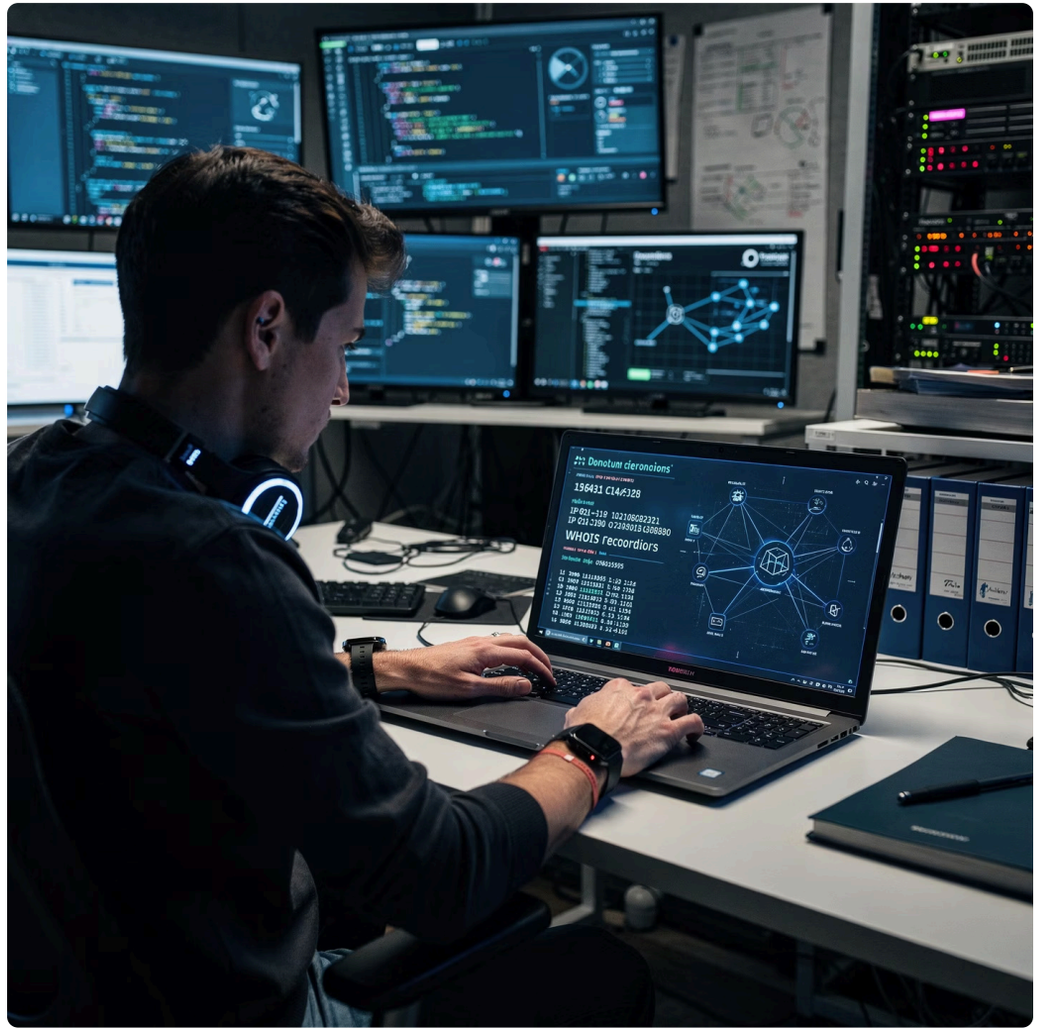
Analisis Domain Publik

Dalam sesi praktik pertama, peserta akan melakukan analisis menyeluruh terhadap sebuah domain publik yang telah ditentukan instruktur. Latihan ini mensimulasikan langkah awal penugasan penetration testing nyata.

Langkah-langkah yang dilakukan:

1. Lakukan `whois` lookup pada domain target
2. Identifikasi nameserver dan record DNS utama menggunakan `nslookup`
3. Cari informasi tambahan menggunakan Google Dorking dengan operator `site:`
4. Periksa keberadaan subdomain menggunakan tools seperti Sublist3r atau crt.sh
5. Dokumentasikan semua temuan dalam format laporan singkat

> Gunakan domain latihan yang disediakan instruktur atau domain milik Anda sendiri. Jangan pernah melakukan analisis ini tanpa izin tertulis.



Edy Susanto — Founder C-SIX Security

Praktik 2

Pemetaan Informasi Organisasi

Pada sesi ini, peserta belajar memetakan struktur sebuah organisasi fiktif menggunakan informasi yang tersedia secara publik, kemudian memvisualisasikannya menggunakan Maltego Community Edition.

01

Tentukan Entitas Awal

Mulai dengan nama domain atau nama organisasi sebagai titik awal graf di Maltego.

02

Jalankan Transform

Gunakan fitur "Run Transform" di Maltego untuk memperluas graf — menemukan IP, email, dan subdomain terkait secara otomatis.

03

Integrasikan Data OSINT

Tambahkan data dari LinkedIn (nama karyawan, jabatan) dan GitHub (repositori publik) ke dalam peta informasi.

04

Visualisasi & Analisis

Atur layout graf dan identifikasi hubungan antar entitas. Temukan aset yang paling berisiko berdasarkan keterpaparan informasi.

05

Ekspor Laporan

Ekspor hasil graf sebagai gambar atau laporan PDF untuk dokumentasi temuan reconnaissance.

Edy Susanto — Founder C-SIX Security

Praktik 3

Pengumpulan Informasi dengan Sumber Terbuka

Skenario Latihan

Peserta diberikan nama sebuah perusahaan fiktif dan diminta mengumpulkan sebanyak mungkin informasi hanya dari sumber publik dalam waktu 30 menit. Hasilnya dibandingkan antar kelompok untuk mengevaluasi efektivitas teknik masing-masing.

- Cari profil perusahaan di LinkedIn dan website resmi
- Identifikasi email format menggunakan Hunter.io
- Temukan dokumen publik dengan Google Dorking

Target Capaian

Di akhir sesi, peserta mampu menghasilkan **profil intelijen** yang mencakup:

- Struktur jaringan dan domain yang digunakan
- Nama dan kontak karyawan kunci
- Teknologi dan platform yang digunakan organisasi
- Potensi vektor serangan berdasarkan informasi terbuka

> Semua data yang dikumpulkan bersifat fiktif dan hanya digunakan untuk tujuan edukasi dalam lingkungan pelatihan C-SIX Security.

Edy Susanto — Founder C-SIX Security

Penutup Modul

Outcome & Kompetensi yang Dicapai

Setelah menyelesaikan Modul 4, peserta telah membangun fondasi yang kuat untuk melaksanakan fase reconnaissance dalam sebuah penugasan keamanan siber secara profesional dan bertanggung jawab.

Reconnaissance Pasif

Mampu menggunakan OSINT, Whois, dan Google Dorking untuk mengumpulkan data tanpa menyentuh sistem target.

DNS Enumeration

Mampu mengekstraksi dan menganalisis record DNS menggunakan Nslookup dan dig secara mandiri.

Maltego & Shodan

Mampu membangun peta informasi visual menggunakan Maltego CE dan memahami data dari Shodan.

Dokumentasi Profesional

Mampu mendokumentasikan temuan reconnaissance dalam format laporan yang terstruktur dan dapat dipresentasikan.