Modul 2 – Reconnaissance Menggunakan Tools Online

Teknik pengumpulan informasi target dari sumber terbuka (OSINT) adalah langkah pertama dalam setiap penilaian keamanan siber. Modul ini membahas cara membangun profil target secara sistematis menggunakan tools online yang tersedia secara publik.

Edy Susanto – Founder C-SIX Security

Gambaran Modul

Tujuan Pembelajaran

Pada akhir modul ini, peserta akan mampu **mengumpulkan dan menganalisis informasi target menggunakan sumber terbuka** (Open Source Intelligence / OSINT) secara efektif dan terstruktur. Kemampuan ini adalah fondasi dari setiap pengujian penetrasi yang profesional.

🔍 Identifikasi

Menemukan aset digital dan infrastruktur target yang terekspos secara publik

🗺️ Pemetaan

Membangun peta lengkap domain, subdomain, dan teknologi yang digunakan

📋 Profiling

Menyusun profil target yang komprehensif dari informasi publik yang tersedia

Topik Utama

Apa yang Akan Dipelajari?

01

Domain Enumeration

Menemukan semua domain dan subdomain yang terkait dengan target

02

DNS Analysis

Menganalisis rekaman DNS untuk memetakan infrastruktur jaringan

03

Technology Fingerprinting

Mengidentifikasi teknologi, framework, dan versi software yang digunakan

04

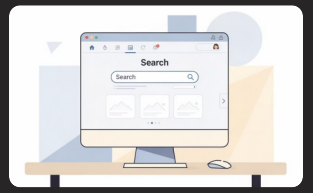
Asset Discovery & Internet Exposure Mapping

Menemukan aset tersembunyi dan memetakan eksposur layanan ke internet

Toolkit OSINT

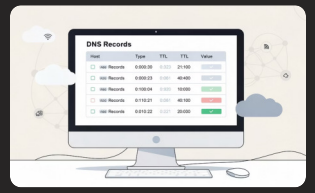
Tools yang Digunakan

Keempat tools berikut adalah standar industri dalam dunia reconnaissance. Semuanya dapat diakses secara gratis melalui browser tanpa instalasi tambahan.



Shodan

Mesin pencari perangkat yang terhubung ke internet. Menemukan server, kamera, router, dan layanan yang terekspos beserta versi software-nya.

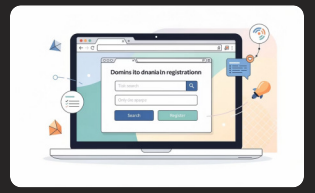


SecurityTrails

Platform intelijen DNS dan domain historis. Memberikan rekaman DNS lengkap, riwayat perubahan, dan data subdomain secara mendalam.

ViewDNS.info

Kumpulan tools DNS dan jaringan dalam satu platform. Mendukung reverse IP lookup, traceroute, WHOIS, dan berbagai query DNS lainnya.



WHOIS Lookup ICANN

Layanan resmi ICANN untuk mengakses data registrasi domain — termasuk informasi pendaftar, tanggal registrasi, dan nameserver.

Edy Susanto – Founder C-SIX Security

Materi 1

Domain Enumeration

Domain Enumeration adalah proses menemukan semua domain dan subdomain yang dimiliki atau dioperasikan oleh sebuah organisasi. Informasi ini membuka peta awal infrastruktur target.

Teknik yang umum digunakan meliputi:

- **Subdomain brute-forcing** – mencoba kombinasi nama subdomain yang umum
- **Certificate Transparency Logs** – memeriksa sertifikat SSL yang terdaftar publik
- **Pencarian riwayat DNS** – menggunakan SecurityTrails untuk melihat rekaman historis
- **Google Dorking** – menggunakan operator `site:` untuk menemukan subdomain yang terindeks

> ⓘ Subdomain yang terlupakan sering menjadi titik lemah yang paling mudah dieksploitasi.

Contoh Temuan Subdomain

Dari satu domain utama seperti `contoh.co.id`, enumeration dapat mengungkap:

- `mail.contoh.co.id`
- `dev.contoh.co.id`
- `staging.contoh.co.id`
- `api.contoh.co.id`
- `vpn.contoh.co.id`

Setiap subdomain = potensi vektor serangan baru yang perlu dievaluasi.

Materi 2

DNS Analysis & Technology Fingerprinting

🌐 DNS Analysis

Analisis DNS mengungkapkan bagaimana infrastruktur jaringan sebuah organisasi dibangun. Record DNS yang umum diperiksa:

- **A Record** – IP server utama
- **MX Record** – provider email yang digunakan
- **TXT Record** – konfigurasi SPF, DKIM, dan verifikasi layanan
- **NS Record** – nameserver pengelola domain
- **CNAME Record** – alias yang menunjuk ke layanan pihak ketiga

🖥️ Technology Fingerprinting

Proses mengidentifikasi teknologi di balik sebuah website atau layanan tanpa harus masuk ke dalam sistemnya.

- **HTTP Headers** – mengungkap server, framework, dan versi
- **HTML source code** – mendeteksi CMS, JavaScript library
- **Shodan banners** – informasi service dan versi dari port terbuka
- **SSL Certificate** – nama organisasi dan subdomain terdaftar

⚠ Versi software yang teridentifikasi dapat langsung dicocokkan dengan CVE database untuk menemukan kerentanan.

Edy Susanto – Founder C-SIX Security

Materi 3 & 4

Asset Discovery & Internet Exposure Mapping

Asset Discovery — Menemukan yang Tersembunyi

Banyak organisasi memiliki aset digital yang terlupakan — server lama, portal admin yang tidak terdaftar, atau bucket cloud yang salah konfigurasi. Asset discovery menggunakan kombinasi Shodan, SecurityTrails, dan pencarian Google untuk menemukan aset-aset ini sebelum penyerang menemukannya lebih dulu.

Internet Exposure Mapping — Seberapa Luas Permukaan Serangan?

Setiap layanan yang terekspos ke internet adalah bagian dari *attack surface*. Pemetaan eksposur internet mencakup port terbuka, layanan tanpa autentikasi, panel admin publik, dan API endpoint yang tidak dilindungi. Shodan adalah tool utama untuk tahap ini — cukup dengan mencari nama organisasi atau blok IP untuk melihat gambaran lengkap eksposur mereka.

Mengapa Ini Penting bagi Defender?

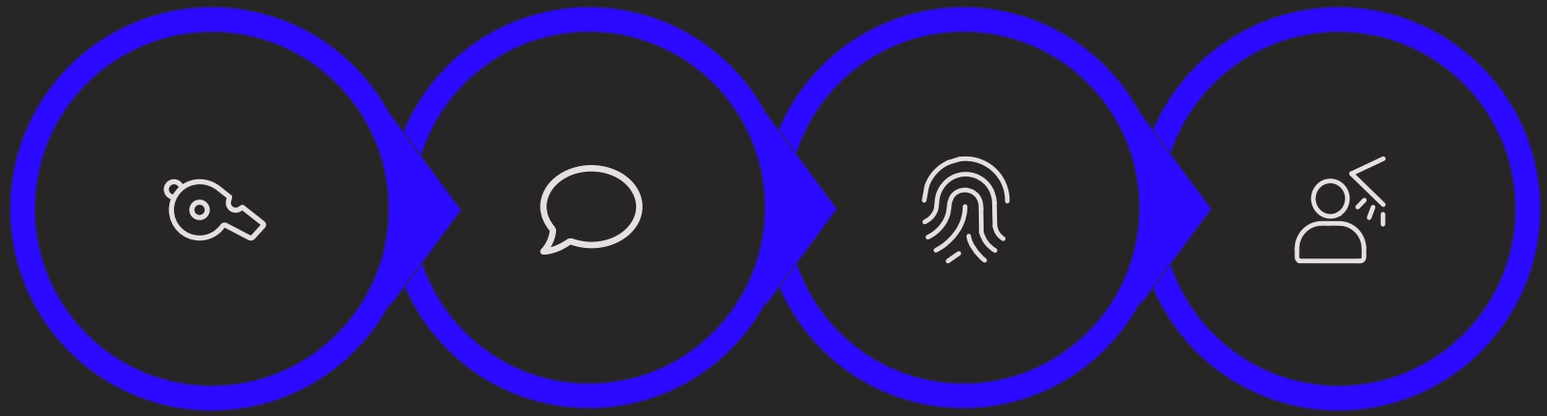
Sebagai administrator atau analis keamanan, memahami apa yang "terlihat" dari internet adalah langkah pertama dalam memperkuat pertahanan. Jika Anda belum pernah melakukan reconnaissance terhadap infrastruktur Anda sendiri, kemungkinan besar penyerang sudah melakukannya.

Edy Susanto – Founder C-SIX Security

Sesi Praktik

Lab: Memetakan Aset Digital Organisasi

Pada sesi praktik ini, peserta akan melakukan reconnaissance terhadap **organisasi contoh fiktif** menggunakan tools yang telah dipelajari. Ikuti langkah-langkah berikut secara berurutan:



Setiap peserta akan mendokumentasikan temuan dalam **lembar kerja reconnaissance** yang disediakan. Hasilnya akan dipresentasikan dan didiskusikan bersama di akhir sesi untuk membandingkan metodologi dan temuan.

> Seluruh praktik dilakukan hanya terhadap domain target yang telah disetujui. Penggunaan teknik ini terhadap sistem tanpa izin adalah **ilegal** dan melanggar etika profesi.

Edy Susanto – Founder C-SIX Security

Praktik Lanjutan

Mengidentifikasi Teknologi Website Target

Langkah-langkah Fingerprinting

1. Buka **Shodan.io** dan cari nama domain atau IP target
2. Perhatikan banner informasi: nama software, versi, port terbuka
3. Gunakan **ViewDNS.info** untuk reverse IP lookup — temukan domain lain yang berbagi IP yang sama
4. Periksa HTTP response headers menggunakan browser developer tools
5. Catat semua teknologi yang teridentifikasi dalam lembar kerja

Yang Perlu Didokumentasikan

Web Server

Apache, Nginx, IIS, dan versinya

CMS / Framework

WordPress, Laravel, React, dll.

CDN / Cloud

Cloudflare, AWS, GCP, Azure

Port Terbuka

22 (SSH), 80/443, 3306, 8080, dll.

Outcome Modul 2

Peserta Mampu Membangun Profil Target dari Sumber Publik

Setelah menyelesaikan Modul 2, peserta memiliki kemampuan nyata untuk melakukan **passive reconnaissance** secara profesional dan terstruktur.

Profil Target Lengkap

Mampu menyusun profil infrastruktur digital yang mencakup domain, IP, teknologi, dan eksposur layanan dari sumber publik

Penggunaan Tools OSINT

Terampil menggunakan Shodan, SecurityTrails, ViewDNS.info, dan WHOIS ICANN secara mandiri dan kombinasi

Perspektif Defender

Memahami apa yang terlihat oleh penyerang dari luar jaringan, sehingga dapat memprioritaskan langkah mitigasi yang tepat

Dokumentasi Profesional

Mampu mendokumentasikan temuan reconnaissance dalam laporan terstruktur yang siap digunakan dalam penugasan nyata

Edy Susanto – Founder C-SIX Security