Studi Kasus: Investigasi Subdomain dalam Keamanan Jaringan

Latar Belakang

Salah satu langkah awal dalam proses pengujian keamanan adalah mengenali seluruh aset digital yang dimiliki oleh sebuah organisasi, termasuk subdomain. Subdomain enumeration dapat membantu dalam mengidentifikasi layanan atau sistem yang mungkin rentan terhadap serangan siber. Oleh karena itu, dalam studi kasus ini, Anda akan melakukan investigasi terhadap domain *ub.ac.id* untuk menemukan daftar subdomain yang ada beserta alamat IP-nya menggunakan berbagai teknik yang tersedia.

Permasalahan

Universitas Brawijaya memiliki banyak subdomain yang digunakan untuk berbagai layanan akademik dan administratif. Sebagai seorang profesional keamanan jaringan, Anda diminta untuk menyusun laporan terkait subdomain yang aktif di bawah domain utama *ub.ac.id* guna memahami potensi risiko keamanan yang mungkin timbul.

Tugas Anda

Sebagai bagian dari tim keamanan informasi, Anda ditugaskan untuk:

1. **Memahami Konsep Enumeration Subdomain**
    - Pelajari metode yang digunakan untuk mendapatkan daftar subdomain, seperti:
        - DNS Zone Transfer (jika memungkinkan)
        - Brute force dengan wordlist
        - OSINT (Open Source Intelligence)
        - Google Dorking
        - Penggunaan layanan publik seperti *crt.sh*, *SecurityTrails*, *Shodan*, dan *VirusTotal*
        - Penggunaan alat seperti `sublist3r`, `amass`, `theHarvester`, `findomain` dan `assetfinder`
2. **Menemukan Subdomain di Bawah Domain *ub.ac.id***
    - Terapkan metode yang telah dipelajari untuk menemukan subdomain di bawah domain *ub.ac.id*.
    - Gunakan minimal dua metode untuk membandingkan efektivitasnya.
3. **Menganalisis dan Mendokumentasikan Hasil**
    - Dokumentasikan langkah-langkah yang Anda lakukan dalam pencarian subdomain.
    - Susun daftar subdomain yang ditemukan beserta alamat IP-nya.
    - Analisis hasil dengan membandingkan jumlah subdomain yang ditemukan oleh masing-masing metode.
    - Identifikasi potensi risiko yang mungkin terjadi akibat subdomain yang ditemukan.

Konten Laporan

Laporan yang Anda buat harus mencakup:

- **Langkah-langkah:** Detail metode yang digunakan dan alasan pemilihannya.

- **Hasil pencarian:** Daftar subdomain yang ditemukan dan alamat IP-nya dalam format tabel.
- **Analisis:** Perbandingan efektivitas metode yang digunakan dan potensi risiko yang dapat muncul.

Batasan dan Etika

- Hanya gunakan teknik yang bersifat non-intrusif dan legal.
- Jangan mencoba mengeksploitasi atau merusak sistem target.
- Studi kasus ini bertujuan untuk pembelajaran keamanan siber, bukan untuk tindakan ilegal.

Format Pengumpulan

- **Mekanisme Pengumpulan:** Kumpulkan melalui Brone "Studi Kasus #2"
- **Format laporan:** PDF