Skenario

Anda adalah seorang konsultan keamanan siber yang ditugaskan untuk melakukan **penetration test** terhadap sebuah perusahaan fiksi, **PT. SecureCorp**. Tujuan Anda adalah mengumpulkan informasi sebanyak mungkin tentang infrastruktur *online* dan *offline* mereka untuk mengidentifikasi potensi titik masuk. Anda harus mendokumentasikan semua langkah, alat, dan hasil yang diperoleh.

Bagian 1: Passive Reconnaissance (Pengintaian Pasif)

Passive Recon adalah tahap pengumpulan informasi tanpa berinteraksi langsung dengan sistem target.

Tujuan

Mengidentifikasi informasi publik PT. SecureCorp tanpa meninggalkan jejak atau *log* di sistem mereka.

Tugas yang Harus Dilakukan

1. **Pencarian Domain dan Sub-domain:**
    - Identifikasi domain utama PT. SecureCorp (contoh: `securecorp.com`).
    - Gunakan teknik seperti **OSINT (Open-Source Intelligence)**, alat pencarian *DNS records* publik, dan mesin pencari untuk menemukan setidaknya **lima (5) sub-domain** yang aktif (contoh: `mail.securecorp.com`, `dev.securecorp.com`).
2. **Informasi Email dan Karyawan:**
    - Cari format alamat email standar yang digunakan perusahaan (contoh: `nama.belakang@securecorp.com`).
    - Identifikasi setidaknya **tiga (3) nama karyawan** di level teknis atau manajemen, serta peran/jabatan mereka, menggunakan platform seperti LinkedIn, Google, atau media sosial lainnya.
3. **Teknologi yang Digunakan:**
    - Gunakan alat OSINT (seperti BuiltWith atau Wappalyzer) untuk mengidentifikasi **tiga (3) teknologi utama** yang digunakan di *website* mereka (contoh: jenis *web server*, *framework* CMS, atau *analytics tool*).
4. **Informasi Sensitif yang Terpapar:**
    - Cari kemungkinan informasi sensitif yang bocor atau terekspos di layanan publik seperti GitHub (mencari *commit* atau *repository*), Pastebin, atau Google Dorks (contoh: file konfigurasi, *backup*, atau kredensial yang tidak sengaja terindeks).

Output yang Diharapkan (Pasif)

Buat tabel berisi: **Informasi yang Ditemukan**, **Sumber (Alat/Website)**, dan **Alasan Relevansi** (mengapa informasi ini penting untuk serangan).

Bagian 2: Active Reconnaissance (Pengintaian Aktif)

Active Recon adalah tahap pengumpulan informasi yang melibatkan interaksi langsung dengan sistem target.

Tujuan

Memetakan topologi jaringan dan mengidentifikasi layanan/port yang terbuka pada target secara terstruktur.

Peringatan Etis

- *Asumsi:* Anda telah mendapatkan **izin tertulis (Rules of Engagement)** untuk melakukan pemindaian pada alamat IP target spesifik (Asumsikan IP target adalah: `192.168.1.100`).
- *Anda hanya boleh melakukan pemindaian pada IP yang ditentukan dalam skenario ini.*

Tugas yang Harus Dilakukan

1. **Host Discovery dan Port Scanning:**
    - Gunakan alat *network scanner* (seperti **Nmap**) untuk memindai IP target (`192.168.1.100`).
    - Jalankan pemindaian **SYN Scan** (`-sS`) untuk mengidentifikasi semua **port TCP yang terbuka (open ports)**.
    - Jalankan pemindaian **UDP Scan** (`-sU`) untuk mencari setidaknya **satu (1) port UDP** yang terbuka atau tersaring (*filtered*).
2. **Service and Version Detection:**
    - Setelah mengidentifikasi port yang terbuka, jalankan pemindaian untuk mendeteksi **layanan (service)** dan **versi perangkat lunak** yang berjalan pada port-port tersebut (contoh: Apache HTTPD 2.4.41).
    - Gunakan *flag* Nmap yang sesuai untuk tugas ini.
3. **OS Fingerprinting:**
    - Cobalah untuk mengidentifikasi **sistem operasi (OS)** yang digunakan oleh target (contoh: Linux Kernel 4.x atau Windows Server 2016).
4. **Network Protocol Analysis (Bonus):**
    - *Jika memungkinkan secara teknis (tergantung pada lingkungan laboratorium Anda):* Ambil sampel *network traffic* kecil (menggunakan Wireshark) antara Anda dan target selama proses pemindaian aktif dan jelaskan protokol utama yang Anda lihat.

Output yang Diharapkan (Aktif)

Buat laporan terperinci berisi: **Command Nmap yang Digunakan**, **Hasil Output (Port, Layanan, Versi)**, dan **Potensi Kerentanan** (misalnya, jika layanan yang ditemukan sudah usang/rentan).