SKENARIO TUGAS BESAR

PASSIVE DAN ACTIVE RECONNAISSANCE

OLEH:

NAMA : **ANDINI FEBRIANTI**

KELAS : **5A JK**

NIM : **105841113223**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

Skenario Operasional

Di tengah dunia digital yang penuh risiko, Anda ditunjuk sebagai Konsultan Keamanan Siber dengan misi krusial: mengidentifikasi setiap potensi titik lemah pada sistem target sebelum serangan yang sesungguhnya terjadi. Misi ini dimulai dari fase *Reconnaissance*, tahap pengumpulan intelijen yang senyap dan metodis.

Misi dibagi menjadi dua operasi berbeda. Operasi pertama berfokus pada observasi eksternal (Pasif) terhadap target publik, yaitu Portal Web Resmi Pemerintah Kabupaten Maros (maroskab.go.id). Di sini, aturan etika sangat ketat: tidak ada interaksi langsung, hanya pengumpulan informasi dari sumber terbuka (OSINT) untuk memetakan wajah publik organisasi tersebut.

Operasi kedua bergeser ke lingkungan yang terkendali, sebuah Mesin Virtual Lab Rentan dengan IP 172.20.10.4. Di sinilah aktivitas pemindaian intensif (*Active Reconnaissance*) diizinkan. Dengan *platform* Kali Linux dan *tools* canggih seperti Nmap dan Wireshark, tujuan adalah mengungkap setiap *port* yang terbuka, mengidentifikasi layanan yang usang, hingga memastikan jenis sistem operasi target.

Hasil dari kedua operasi ini akan menjadi peta harta karun bagi *hacker*—peta yang menunjukkan jalur masuk paling mudah (*entry point*) dan menetapkan target mana yang akan dieksploitasi di fase berikutnya**.**

RANCANGAN KERJA

1. MANDAT DAN SASARAN UTAMAN

Elemen	Deskripsi
Peran	Konsultan Keamanan Siber
Misi utama	Mengumpulkan informasi kritis (*Reconnaissance*) untuk mengidentifikasi potensi titik masuk (*entry point*)

2. FOKUS DAN LINGKUP PENGUJIAN

Jenis Reconnaissance	Target Pengujian	Parameter Teknis	Status Target
Passive Reconnaissance	Portal Web Pemerintah Kab. Maros	maroskab.go.id	Target Publik (Non-Intrusif)
Active Reconnaissance	Mesin Virtual Lab Rentan	IP **172.20.10.4**	Target Lab (Intrusif Diizinkan)

Sasaran Teknis yang Harus Dicapai:

- Mengidentifikasi domain, subdomain, dan teknologi *website*.
- Menentukan *port*, layanan, versi, dan sistem operasi target.

3. METODOLOGI DAN INSTRUMEN KERJA

a. Instrumen pendukung (Tools)

Alat	Fungsi Kunci dalam Pengujia
Nmap & Netdiscover	Melakukan port scanning (TCP/UDP), deteksi host aktif, dan OS/Service detection.
Wireshark	Menganalisis pola protokol dan memvalidasi teknik scanning (misalnya Stealth Scan).
crt.sh & BuiltWith	Digunakan untuk *OSINT* pemetaan subdomain dan audit teknologi *website*.

b. Prosedur Operasi (*Work Flow*)

1. Fase Passive Reconnaissance

- **Audit Kebocoran**: Melakukan pencarian data sensitif di *repository* publik (GitHub Search).

- **Koleksi Data:** Mengumpulkan format email dan data staf dari publikasi resmi.

2. **Fase Active Reconnaissance**
    - **Verifikasi Host:** Memastikan target aktif menggunakan `Netdiscover`.
    - **Pemindaian Lengkap**: Melaksanakan TCP SYN scan dan UDP scan.
    - **Analisis Protokol:** Mengamati traffic menggunakan Wireshark.

4. KEBIJAKAN ETIKA DAN LEGALITAS

- **Prinsip Non-Intrusif:**

  Terhadap target publik, dipastikan tidak ada interaksi langsung atau pengiriman paket yang dapat dianggap sebagai gangguan.
- **Legalitas:**

  Pengujian ini dibatasi hanya pada *VM Lab Rentan* untuk tujuan akademik.