SKENARIO

PASSIVE DAN ACTIVE RECONNAISANCE

NAMA : FATHYA SHABIRA A.T

KELAS : 5B

NIM : 105841111923

---

1. **Latar Belakang**

   Pada awal semester, kamu sebagai konsultan keamanan siber di lingkungan pemerintah kota diminta melakukan pengujian awal terhadap dua target berbeda: sebuah website publik milik Pemerintah Kota Surabaya dan sebuah mesin virtual rentan di laboratorium internal kampus. Tahap yang dikerjakan masih berada pada fase reconnaissance, sehingga fokus utamanya adalah mengumpulkan informasi sebanyak mungkin tanpa langsung melakukan eksploitasi.

   Fase ini penting karena hasilnya akan menjadi dasar untuk memahami bagaimana arsitektur layanan dibangun, teknologi apa saja yang digunakan, serta titik lemah mana yang paling mungkin dimanfaatkan penyerang. Dengan pemetaan permukaan serangan yang jelas, tahapan eksploitasi berikutnya dapat direncanakan secara lebih terarah dan tetap berada dalam batas etika pengujian.

2. **Tujuan Pengujian**

   Pengujian ini memiliki beberapa tujuan utama:

   a. Mengumpulkan informasi publik terkait domain dan subdomain yang digunakan Pemerintah Kota Surabaya.
   b. Mengidentifikasi teknologi web (server, framework, CDN, WAF, dan komponen pendukung lain) yang terpasang pada portal surabaya.go.id.
   c. Mengetahui pola penamaan email serta struktur organisasi yang terekspos untuk mendukung analisis risiko social engineering.
   d. Mengidentifikasi host, port, dan layanan yang terbuka pada mesin lab rentan di jaringan internal.

e. Menentukan sistem operasi dan karakteristik jaringan target melalui teknik OS fingerprinting dan analisis protokol.

3. Ruang Lingkup Pengujian

Jenis Pengujian	Target
Passive Reconnaissance	Website Pemerintah Kota Surabaya (surabaya.go.id)
Active Reconnaissance	VM lab rentan – IP: 192.168.132.2

Seluruh aktivitas active reconnaissance dibatasi hanya pada mesin virtual laboratorium yang sudah disediakan pengajar. Untuk domain publik surabaya.go.id, hanya dilakukan teknik passive reconnaissance berbasis OSINT tanpa mengirimkan request yang bersifat intrusif ataupun mengganggu ketersediaan layanan.

4. Tools Yang Digunakan

Tools	Fungsi utama dalam skenario
Kali Linux	Sistem operasi utama untuk menjalankan seluruh tools pengujian.
Nmap	Pemindaian port, deteksi service & version, serta OS fingerprinting.
Netdiscover	Menemukan host aktif di segmen jaringan internal menggunakan ARP scan.
Wireshark	Menganalisis paket dan protokol jaringan (terutama saat menjalankan Nmap).
crt.sh	Pencarian domain dan subdomain surabaya.go.id berbasis Certificate Transparency.
BuiltWith/Wappalyzer	Identifikasi teknologi web (server, framework, WAF, CDN, analytics).
GitHub Search	Menelusuri kemungkinan repository publik yang terkait dengan surabaya.go.id.
VMware + VM rentan	Menyediakan lingkungan lab dan mesin target untuk active reconnaissance.

5. Metodologi Penelitian

Passive Reconnaissance (surabaya.go.id)

a. Langkah yang direncanakan:
   - Menggunakan crt.sh untuk memetakan domain dan subdomain yang masih aktif di bawah *.surabaya.go.id.

- Mengumpulkan informasi kontak, format email, dan data pejabat/pegawai dari situs resmi serta halaman organisasi terkait.
- Mengidentifikasi teknologi web (web server, framework, CDN, WAF, analytics) menggunakan BuiltWith atau Wappalyzer.
- Melakukan pencarian repository publik di GitHub yang mengandung kata kunci terkait surabaya.go.id untuk mendeteksi potensi kebocoran konfigurasi atau kode.

b. Active Reconnaissance (VM lab rentan 192.168.132.2)

Langkah yang direncanakan pada jaringan internal:

- Menjalankan Netdiscover untuk memastikan IP target aktif dan berada pada segmen jaringan yang sama dengan attacker.
- Melakukan TCP SYN scan menggunakan Nmap untuk menemukan port TCP terbuka beserta service yang berjalan.
- Menjalankan UDP scan terbatas (misalnya top 20 ports) untuk mengidentifikasi layanan UDP penting seperti DNS dan DHCP.
- Mengaktifkan opsi service & version detection (-sV) untuk mendapatkan versi layanan yang lebih rinci.
- Melakukan OS fingerprinting (-O) guna mengidentifikasi sistem operasi atau tipe perangkat (misalnya VMware NAT device).
- Menangkap trafik selama proses pemindaian dengan Wireshark untuk melihat pola paket (SYN, SYN-ACK, RST) dan mengonfirmasi teknik scanning yang digunakan.

6. Output Yang Diharapkan

Dari skenario ini diharapkan beberapa keluaran utama:

a. Laporan tertulis berisi hasil passive dan active reconnaissance beserta analisis risiko awal.

b. Kumpulan screenshot yang terdokumentasi rapi untuk setiap tahapan penting (OSINT, scanning, Wireshark).

c. Video dokumentasi proses pengujian mulai dari persiapan, eksekusi tools, sampai interpretasi hasil.

7. Etika Dan Legalitas

Seluruh aktivitas dilakukan untuk tujuan akademik dengan izin pengajar, dan hanya pada target yang telah disetujui. Untuk website publik surabaya.go.id, aktivitas dibatasi pada pengumpulan informasi pasif yang tidak mengubah, merusak, atau mengganggu layanan, sedangkan semua tindakan aktif hanya diarahkan ke mesin virtual laboratorium.