SKENARIO

Penetration Testing – Reconnaissance Phase

NAMA : IRYAN TEGAR

NIM : 105841113023

KELAS : 5JKA ETHICAL HACKING

---

1. **Latar Belakang**

   Dalam tugas besar mata kuliah Ethical Hacking, saya berperan sebagai konsultan keamanan siber yang bertugas melakukan tahapan Reconnaissance (pengumpulan informasi) untuk mengidentifikasi potensi titik masuk suatu sistem.
   Pengujian dilakukan pada dua target berbeda:

   - Passive Reconnaissance: Website Pemerintah Kabupaten Gowa (gowakab.go.id)
   - Active Reconnaissance: Mesin virtual lab rentan (IP: 172.20.10.3)

2. **Tujuan Pengujian**

   Tujuan pengujian ini adalah:

   - Mengumpulkan informasi publik terkait target
   - Mengidentifikasi domain dan subdomain aktif
   - Mengetahui teknologi yang digunakan oleh website
   - Mengidentifikasi port dan layanan yang terbuka
   - Mengidentifikasi kemungkinan sistem operasi target

3. **Ruang Lingkup Pengujian**

Jenis Pengujian	Target
Passive Reconnaissance	gowakab.go.id
Active Reconnaissance	172.20.10.3 (VulnOSv2)

   Seluruh pengujian aktif dilakukan hanya pada mesin virtual yang telah diizinkan.

4. Tools yang Digunakan

Tools	Fungsi
crt.sh	Pencarian subdomain melalui data Certificate Transparency
BuiltWith	Identifikasi teknologi yang digunakan website
Google Search	OSINT dasar untuk pengumpulan informasi publik
GitHub Search	Pencarian potensi kebocoran data dan repository publik
Nmap	Port scanning dan deteksi service serta versi
Netdiscover	Mendeteksi host aktif di jaringan (ARP scan)
Wireshark	Analisis trafik jaringan dan protokol
Kali Linux	Sistem operasi utama untuk melakukan pengujian keamanan
VulnOS	Mesin target rentan untuk simulasi serangan
VMware Workstation	Menjalankan mesin virtual dan membuat lingkungan lab

5. Metodologi Pengujian

A. Passive Reconnaissance

Tahapan yang akan dilakukan:

- Melakukan pencarian domain dan subdomain menggunakan crt.sh
- Mengumpulkan format email dan data staf dari website resmi
- Mengidentifikasi teknologi website menggunakan BuiltWith
- Melakukan pencarian potensi data sensitif di GitHub

B. Active Reconnaissance

Tahapan yang akan dilakukan:

- Pencarian host aktif menggunakan Netdiscover
- Melakukan TCP SYN scan menggunakan Nmap
- Melakukan UDP scan untuk identifikasi port UDP
- Melakukan service & version detection
- Melakukan OS fingerprinting
- Mengamati traffic menggunakan Wireshark

6. **Output yang Diharapkan**

   Dokumen yang diharapkan dari skenario ini:

   - Laporan lengkap hasil pengujian
   - Screenshot dokumentasi setiap tahapan
   - Video dokumentasi proses pengujian

7. **Etika dan Legalitas**

   Pengujian ini dilakukan hanya untuk tujuan akademik dan hanya pada target yang memiliki izin.