LAPORAN TUGAS MID: ANALISIS PASIVE DAN ACTIVE RECONNAISSANCE

NAMA : FATHYA SHABIRA A.T

KELAS : 5B / ETHICAL HECKING AND PENETRATION TESTING 1

NIM : 105841111923

---

1. PENDAHULUAN

Pada era digital saat ini, keamanan informasi menjadi aspek yang sangat penting dalam menjaga kelancaran layanan berbasis teknologi. Setiap organisasi perlu memastikan bahwa sistem yang digunakan tetap aman dari berbagai ancaman siber. Salah satu langkah awal dalam pengujian keamanan adalah melakukan reconnaissance, yaitu proses pengumpulan informasi untuk mengetahui struktur sistem dan potensi kerentanannya. Pada laporan ini digunakan dua pendekatan, yaitu Passive Reconnaissance dan Active Reconnaissance. Keduanya bertujuan untuk mengumpulkan data dari website Pemerintah Kabupaten Gowa sebagai target publik serta dari mesin rentan di lingkungan laboratorium sebagai target uji coba eksploitasi. Informasi yang diperoleh pada tahap ini akan menjadi dasar untuk proses eksploitasi pada tahapan selanjutnya.

2. RUANG LINGKUP DAN SKENARIO PENGUJIAN

a. Peran Dan Tujuan

- Peran: Analis Keamanan pada Dinas Komunikasi dan Informatika
- Tujuan: Mengumpulkan informasi terkait infrastruktur komunikasi dan sistem informasi target serta mengidentifikasi potensi risiko keamanan yang terkait.

b. Target Pengujian

Fase	Target Yang Di audit
Passive Reconnaissance	Website Pemerintahan Kota Surabaya (Surabaya.go.id)
Active Reconnaissance	VM Lab Rentan – IP: 192.168.132.2

Tabel 1.1 Ruang Lingkup dan Target Pengujian

c. Rules Of Engagement

Semua aktivitas pemindaian aktif dibatasi hanya pada mesin laboratorium dengan alamat IP 10.39.111.38. Pada seluruh website publik yang menggunakan domain surabaya.go.id, pengumpulan informasi dilakukan secara pasif melalui sumber terbuka tanpa melakukan tindakan yang bersifat intrusif atau berpotensi mengganggu layanan.

3. TOOLS & LINGKUNGAN PENGUJIAN

Tools	Fungsi
Kali Linux	Sistem operasi utama untuk aktivitas OSINT dan dokumentasi teknis.
Nmap	Port, service, dan OS scanning
crt.sh	Pemetaan domain dan subdomain melalui Certificate Transparency (CT log) untuk *.surabaya.go.id.
Netdiscover	Host discovery jaringan
BuiltWith / Wappalyzer	Identifikasi teknologi website (server, framework, CDN, WAF, analytics) yang digunakan oleh portal surabaya.go.id.
GitHub Search	Pencarian kemungkinan bocoran kode atau konfigurasi terkait surabaya.go.id di repositori publik.
Wireshark	Analisis protokol jaringan

Tabel 1.2 Spesifikasi Alat (Tools) dan Fungsinya

4. METODOLOGI RECONNAISSANCE

Tahapan yang digunakan sebagai berikut:

a. Passive Reconnaissance

- Mengumpulkan informasi menggunakan sumber terbuka (OSINT) dari internet dan dokumen publik.
- Tidak melakukan koneksi ataupun permintaan langsung yang bersifat aktif ke server target.

b. Active Reconnaissance

- Melakukan pemindaian terhadap IP target untuk mengidentifikasi port dan layanan yang sedang berjalan.
- Mencari tahu sistem operasi serta jenis protokol jaringan yang digunakan oleh host target.

5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

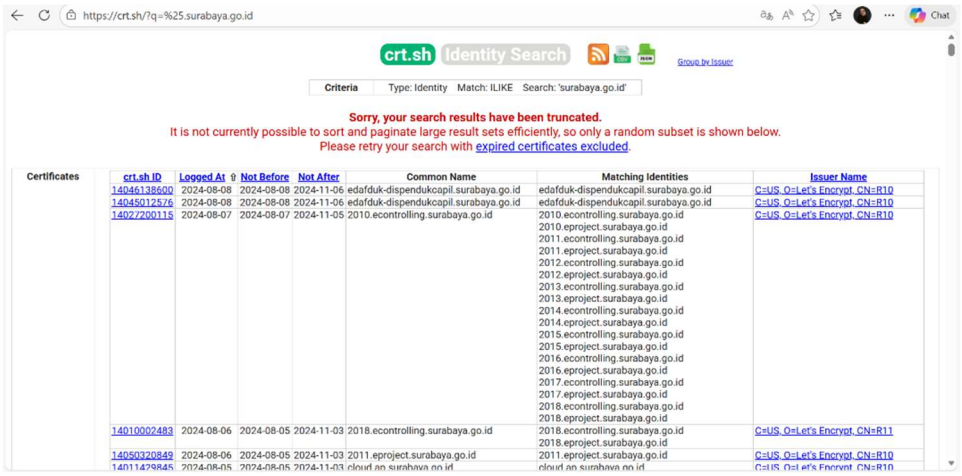
Target: Pemerintah Kota Surabaya

Kategori Informasi	Informasi yang Ditemukan	(Alat/Website)	Alasan Relevansi
Pencarian Sub-domain	• Pemerintah Kota Surabaya • Selamat Datang | Klampid New Generation • Simpora || Dinas Kepemudaan Dan Olahraga Kota Surabaya • E-Dafduk • Dprkpp Kota Surabaya Disperkim	crt.sh crt.sh | %.surabaya.go.id	Menggambarkan cakupan potensi titik serangan yang lebih besar.
Informasi Karyawan	• Indriatno Heryawan, S.Sos • Yudho Febriadi, Skom.,M.T • Yusuf Efendi, S.Kom	Website Resmi Pemkot Surabaya: Dinas Komunikasi Dan Informatika Kota Surabaya	Untuk memetakan susunan organisasi serta pihak-pihak yang berkaitan.
Format Email	disbudporapar@surabaya.go.id	Kontak Resmi Dinas Kebudayaan,	Digunakan untuk validasi pola email dalam

		Kepemudaan dan Olah Raga serta Pariwisata Pemerintah Kota Surabaya	simulasi keamanan.
Teknologi Website	Cloudflare React Cloudflare Web Analytics	BuiltWith: surabaya.go.id Technology Profile	Menunjukkan penggunaan WAF dan potensi analisis keamanan sisi klien.
Informasi Sensitif Terpapar	Repository GitHub:	GitHub Search (OSINT)	Potensi kebocoran source code atau kredensial.

Bukti Dokumentasi

a. Pencarian Domain dan Sub-domain



Gambar 1.1 Hasil Pencarian Subdomain menggunakan crt.sh

b. Informasi email dan karyawan

- **Informasi Email**

Gambar 1.2 Identifikasi Kontak Publik pada Footer Website

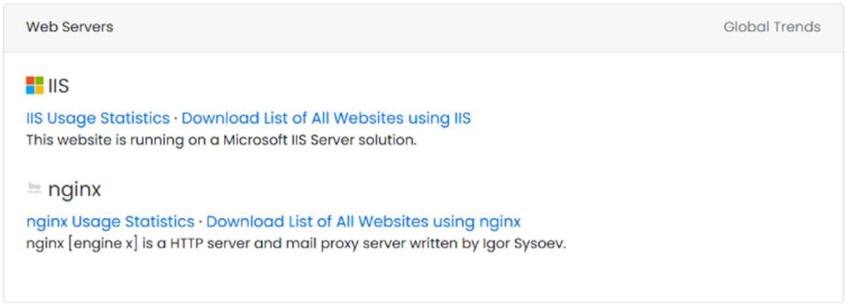
Penemuan alamat email generik (info @disbudporapar.surabaya.go.id) yang memvalidasi format domain email organisasi.

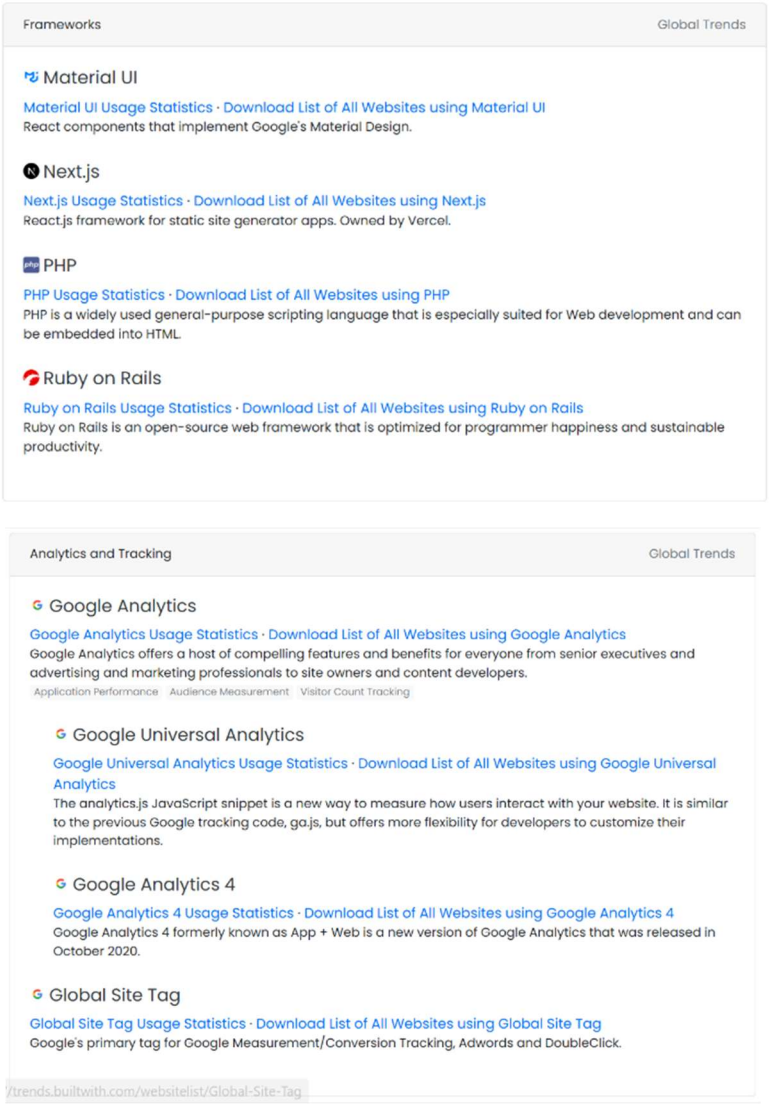
- **Informasi Karyawan Diskominfo**

Gambar 1.3 Identifikasi Profil Pejabat Struktural Diskominfo

Pengumpulan data personel kunci (High-Value Targets) melalui halaman profil publik untuk pemetaan struktur organisasi.

c. Teknologi yang digunakan



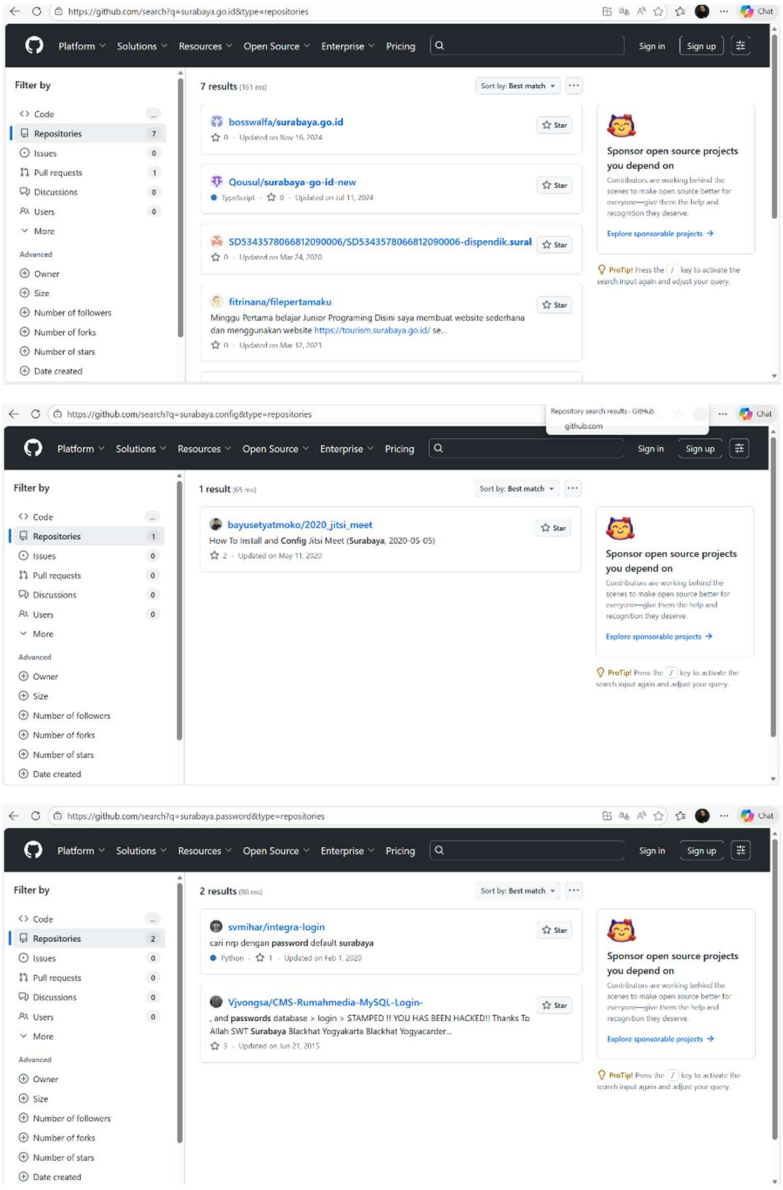


Gambar 1.4 Identifikasi Teknologi Website dan Struktur Organisasi

Deteksi penggunaan Cloudflare dan daftar pejabat terkait yang rentan terhadap serangan Social Engineering.

Gambar ini berisi hasil deteksi teknologi menggunakan tools seperti BuiltWith/Wappalyzer yang menampilkan komponen yang dipakai situs surabaya.go.id, misalnya framework, server, dan layanan pendukung. Dengan informasi ini, dapat diketahui adanya penggunaan teknologi tertentu (seperti WAF, CDN, atau framework frontend) yang berpengaruh terhadap jenis kerentanan dan pendekatan pengujian yang relevan.

d. Informasi sensitive yang terpapar

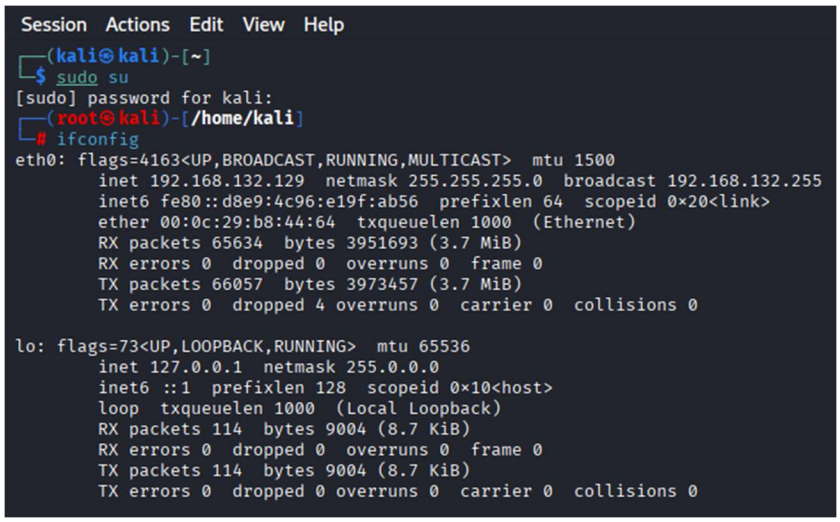


Gambar 1.5 Temuan Repository GitHub (OSINT) Potensi kebocoran source code atau kredensial pada repository publik.

Gambar ini menunjukkan hasil pencarian di GitHub yang menemukan repository publik yang berkaitan dengan surabaya.go.id atau unit di bawahnya. Temuan tersebut menunjukkan adanya potensi kebocoran informasi, seperti potongan source code, konfigurasi, atau referensi kredensial, sehingga perlu ditinjau dan diamankan melalui pengaturan private repo atau penghapusan data sensitif.

6. ACTIVE RECONNAISSANCE (HASIL & ANALISIS)

IFCONFIG



Gambar 1.6 Konfigurasi IP Attacker (Kali Linux)

Sebelum melakukan pemindaian aktif, verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) dilakukan menggunakan perintah ifconfig, di mana interface eth0 teridentifikasi memiliki alamat IP 192.168.132.129 dengan netmask 255.255.255.0 (Gambar [Nomor]). Konfigurasi ini mengonfirmasi bahwa penyerang berada dalam satu segmen jaringan (subnet) yang sama dengan target 172.20.10.3, memvalidasi skenario Internal Network Attack melalui konektivitas Layer 2 (Data Link) yang memungkinkan efektivitas teknik ARP Scanning serta memastikan paket probe Nmap dapat mencapai target tanpa terhalang oleh Network Firewall atau router eksternal.

a. Host Discovery dan Port Scanning

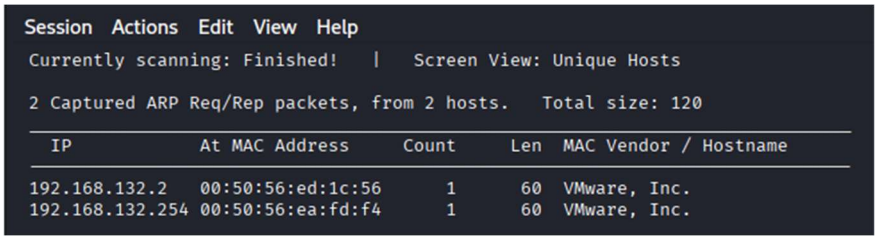
Tabel 1.4 Hasil Pemindaian Host dan Port (Active Reconnaissance)

Tugas	Command	Hasil	Potensi
Host Discovery	sudo netdiscover -r 192.168.132.0/24	Target ditemukan: 192.168.132.2	Memastikan host aktif di jaringan.
TCP SYN Scan	sudo nmap -sS 192.168.132.2	Port terbuka:	Permukaan serangan layanan aktif.
UDP Scan	sudo nmap -sU --top ports 20 192.168.132.2	Open/Filtered:	DNS dan DHCP berpotensi

			menjadi target analisis.

Dokumentasi

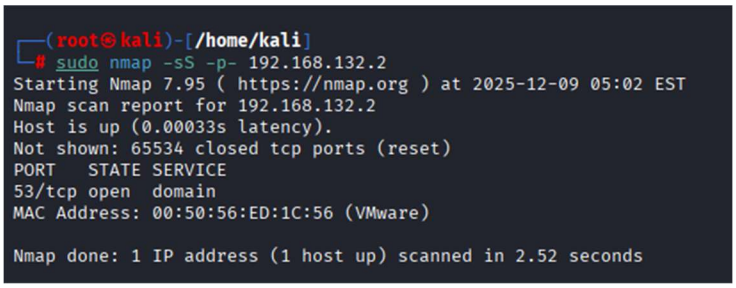
- Host discovery



Gambar 1.7 Hasil Host Discovery dengan Netdiscover

Mengidentifikasi host yang aktif. Target 192.168.132.2 teridentifikasi menggunakan vendor VMware (volunsOS)

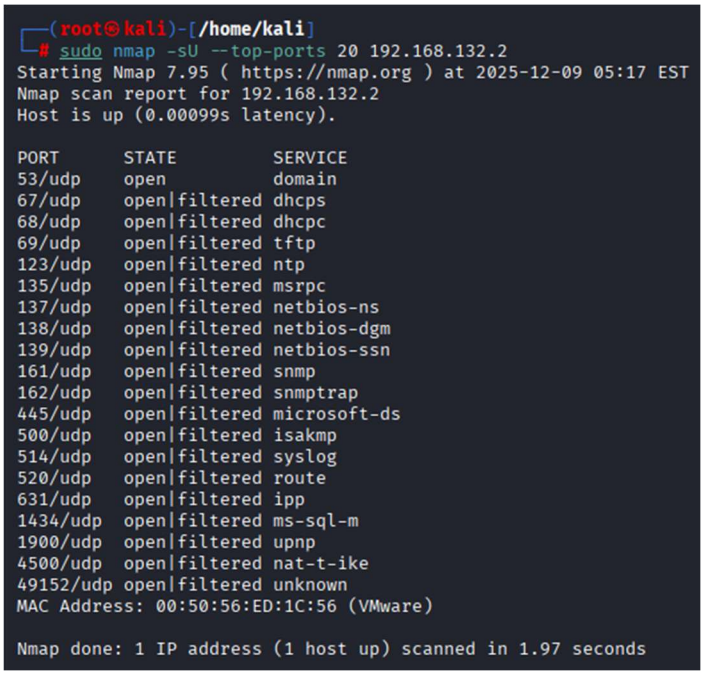
- TCP SYN scan



Gambar 1.8 Hasil TCP SYN Scan (Stealth Scan)

Menemukan port TCP terbuka (53) tanpa menyelesaikan 3-way handshake

- UDP scn



Gambar 1.9 Hasil UDP Scan

Identifikasi layanan berbasis UDP seperti DNS (53) dan DHCP (67) yang berstatus open/filtered

b. Service and Version Detection

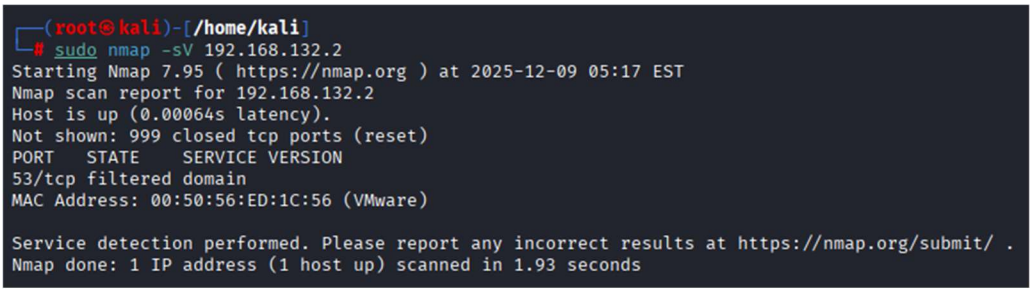
sudo nmap -sV 10.39.111.38

Port	Service	Version	Analisis resiko
53	domain	-	Port 53 (DNS) terbuka/terfilter, berisiko dimanfaatkan untuk serangan DNS (DNS amplification, spoofing, misconfiguration) jika tidak dikonfigurasi dengan baik; perlu pembatasan query,

			hardening DNS, dan monitoring akses.

Tabel 1.5 Deteksi Versi Layanan dan Analisis Kerentanan

Bukti service detection



Gambar 1.10 Deteksi Versi Layanan dan Sistem Operasi

c. OS Fingerprinting

sudo nmap -O 10.39.111.38

Hasil	Detail OS	Analisis
OS terdeteksi	Vmware Player Virtual	Host teridentifikasi sebagai mesin virtual VMware Player; mengindikasikan lingkungan lab/guest OS, namun tetap berisiko jika jaringan tidak diisolasi dengan baik karena kerentanan pada guest atau VMware dapat dimanfaatkan untuk menyerang host atau jaringan lain. Disarankan mengaktifkan isolasi

		jaringan (host-only/NAT terkontrol), patch VMware dan guest OS, serta membatasi layanan yang diekspos.

Tabel 1.6 Hasil Identifikasi Sistem Operasi Target

Bukti OS fingerprinting

Gambar 1.11 Hasil Identifikasi Sistem Operasi (OS Fingerprinting)

Deteksi Vmware Player Virtual NAT device menggunakan opsi -O pada Nmap, mengindikasikan target menggunakan sistem operasi yang sudah usang (End-of-Life).

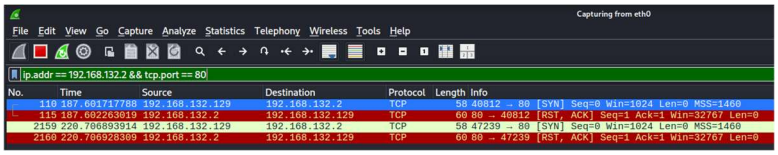
d. Network Protocol Analysis

Tools: Wireshark

- Berdasarkan hasil tangkapan trafik pada Gambar 1.12, terlihat pola komunikasi yang konsisten dengan aktivitas pemindaian port menggunakan Nmap terhadap host target di jaringan lokal. Dalam beberapa paket TCP, mesin penyerang mengirimkan segment SYN ke port 53 milik target untuk menginisiasi koneksi, dan kemudian diikuti dengan paket RST yang dikirim kembali oleh attacker setelah menerima respons dari target.
- Secara konseptual, alur ini berbeda dengan Three-Way Handshake TCP normal yang seharusnya mengikuti urutan SYN → SYN-ACK → ACK hingga koneksi benar-benar terbentuk. Pada trafik yang ditangkap, koneksi tidak pernah diselesaikan dengan ACK, melainkan segera di-reset melalui pengiriman paket RST oleh penyerang sehingga sesi hanya "setengah terbuka". Pola ini mengindikasikan penggunaan teknik TCP SYN Scan (Stealth Scan) yang umum

dilakukan dengan opsi $-sS$ pada Nmap untuk mengidentifikasi port terbuka tanpa membangun koneksi penuh ke layanan aplikasi.

- Implikasi keamanannya adalah adanya jejak percobaan enumerasi port yang mencoba memetakan layanan aktif (dalam kasus ini DNS pada port 53) dengan tingkat deteksi log aplikasi yang lebih rendah dibandingkan koneksi TCP normal. Serangkaian paket SYN dan RST dalam interval singkat dapat diklasifikasikan sebagai pola scanning yang seharusnya terdeteksi oleh mekanisme IDS/IPS atau firewall, sehingga administrator jaringan perlu menerapkan aturan deteksi dan pembatasan terhadap anomali handshake seperti ini.
- Bukti network protocol analysis



Gambar 1.12 Analisis Paket Jaringan dengan Wireshark

Menangkap pola scanning Nmap, terlihat adanya paket RST yang dikirimkan kembali oleh attacker.

7. KESIMPULAN DAN SARAN

Berdasarkan temuan di atas, berikut adalah rekomendasi perbaikan (remediasi) yang disarankan:

a. Manajemen aset digital (digital footprint)
   - Menyesuaikan pengaturan repositori GitHub yang berkaitan agar bersifat privat, atau menghapus informasi sensitif dari riwayat commit.
   - Menyelenggarakan pelatihan Security Awareness bagi pegawai, khususnya pejabat struktural yang teridentifikasi, terkait risiko phishing dan rekayasa sosial.

b. Patch management dan hardening sistem
   - Melakukan pembaruan sistem operasi dan layanan (seperti Apache dan OpenSSH) ke rilis stabil terbaru untuk menutup kerentanan yang sudah diketahui.
   - Menonaktifkan service yang tidak dibutuhkan, terutama port 6667 (IRC) jika tidak ada fungsi operasional yang memerlukannya.

c. Peningkatan keamanan jaringan

- Menerapkan aturan firewall untuk membatasi akses hanya ke port-port penting, misalnya port 80/443 untuk web dan port 22 hanya dari alamat IP tertentu.
- Memanfaatkan IDS/IPS guna memantau dan mengenali pola pemindaian jaringan atau aktivitas mencurigakan lainnya secara langsung.