LAPORAN ANALISIS PASSIVE DAN ACTIVE RECONNAISSANCE

NAMA : MUH.REYHAN DWI WIJAYA
NIM : 105841112623
KELAS : 5JKA – ETHICAL HACKING

1. PENDAHULUAN

Laporan ini membahas kegiatan passive reconnaissance (pengintaian pasif) sebagai tahap awal dalam proses penetration testing terhadap sebuah organisasi. Tahap ini berfokus pada pengumpulan informasi dari sumber terbuka (Open-Source Intelligence/OSINT) tanpa melakukan interaksi langsung dengan sistem target, sehingga meminimalkan risiko terdeteksi dan tidak menimbulkan gangguan operasional. Melalui teknik OSINT, penelusuran DNS, mesin pencari, serta penelusuran jejak digital di platform publik, diperoleh berbagai informasi terkait domain, sub-domain, pola email, profil karyawan, teknologi yang digunakan, hingga potensi kebocoran data sensitif. Informasi tersebut kemudian dianalisis untuk memetakan permukaan serangan (attack surface) dan mengidentifikasi potensi titik masuk yang dapat dimanfaatkan pada tahap pengujian keamanan berikutnya.

2. RUANG LINGKUP & SKENARIO PENGUJIAN

a. Peran dan Tujuan

- **Peran** : Konsultan Keamanan Siber
- **Tujuan** : Mengidentifikasi sebanyak mungkin informasi publik yang berkaitan dengan infrastruktur, teknologi, dan identitas digital organisasi tanpa menimbulkan jejak teknis di sisi target.

b. Target Pengujian

Tabel 1.1 Ruang Lingkup dan Target Pengujian

Fase	**Target yang Diaudit**
Passive Reconnaissance	Website Pemerintah Kota makassar (makassar.go.id)
Active Reconnaissance	VM Lab Rentan – IP: **10.39.111.38**

c. Rules of Engagement

Seluruh aktivitas pemindaian aktif dibatasi hanya pada lingkungan laboratorium dan dilakukan secara eksklusif terhadap mesin dengan alamat IP 10.39.111.38 guna memastikan seluruh interaksi jaringan yang bersifat intrusif tetap berada dalam konteks pengujian terkontrol.

3. TOOLS & LINGKUNGAN PENGUJIAN

Tabel 1.2 Spesifikasi Alat (Tools) dan Fungsinya

Tools	**Fungsi**
Kali Linux	Sistem operasi pengujian keamanan
Netdiscover	Host discovery jaringan
Nmap	Port, service, dan OS scanning
Wireshark	Analisis protokol jaringan
crt.sh	Pemetaan domain & certificate transparency
BuiltWith	Identifikasi teknologi website
GitHub Search	Pencarian informasi sensitif dan kode publik

Lingkungan pengujian dilakukan pada jaringan lokal untuk memastikan legalitas.

4. METODOLOGI RECONNAISSANCE

Tahapan yang digunakan sebagai berikut:

a. Passive Reconnaissance
   - Mengumpulkan data melalui OSINT (Open Source Intelligence)
   - Tidak berinteraksi langsung dengan server

b. Active Reconnaissance
   - Memindai IP target untuk menemukan port dan service terbuka
   - Mengidentifikasi OS dan protokol jaringan

5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

Target: wakab.go.id

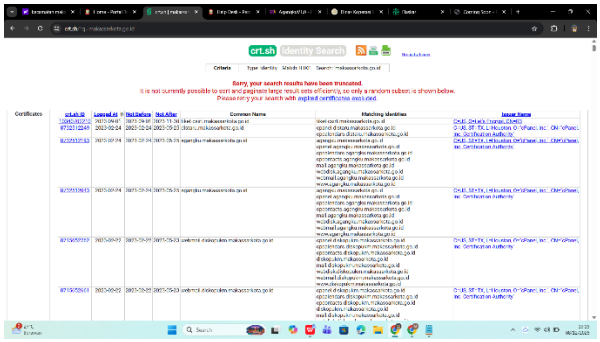
Tabel 1.3 Hasil Pengumpulan Informasi passive reconnaissance

Kategori Informasi	Informasi yang Ditemukan	(Alat/Website)	Alasan Relevansi
Pencarian Sub-domain	makassarkota.go.id csirt.makassarkota.go.id diskopukm.makassarkota.go.id elaskar.bappeda.makassarkota.go.id agangku.makassarkota.go.id e-rota.makassarkota.go.id	crt.sh https://crt.sh/?q=makassarkota.go.id	Menunjukkan permukaan serangan (attack surface) yang lebih luas.
Informasi Karyawan	H. ABRAM LULULANGI,S.I.P(Kepala Bidang Persandian Sarjana) SUHENDRA,S.STP,M.Si(Kepala Bidang Pengolahan Data Elektronik Magister) ISMAWATY NUR,ST.,M.Sc.,Ph.D.(Sekretaris Dinas Komunikasi dan Informatika Magister)	Website Resmi Badan kepegawaian dan pengembangan sumber daya manusia daerah kota makassar https://bkpsdmd.makassarkota.go.id/profil-pegawai-pemerintah-kota-makassar/	Untuk memahami struktur organisasi dan pihak yang relevan.
Format Email	info@makassarkota.go.id	https://dev-portal.makassarkota.go.id/kontak	Digunakan untuk validasi pola email dalam simulasi keamanan.
Teknologi Website	Cloudflare React Cloudflare Web Analytics	BuiltWith https://builtwith.com/makassarkota.go.id	Menunjukkan penggunaan WAF dan potensi analisis keamanan sisi klien.

Informasi Sensitif Terpapar	Repository GitHub: dystianen/gowakab	GitHub Search (OSINT)	Potensi kebocoran source code atau kredensial.

a. Bukti Dokumentasi

1. Pencarian Domain dan Sub-domain



Gambar 1.1 Hasil Pencarian Subdomain menggunakan crt.sh

Menampilkan daftar subdomain yang terdaftar pada sertifikat SSL, memperluas attack surface.

2. Informasi email dan karyawan

- Informasi email

Gambar 1.2 Identifikasi Kontak Publik pada Footer Website

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

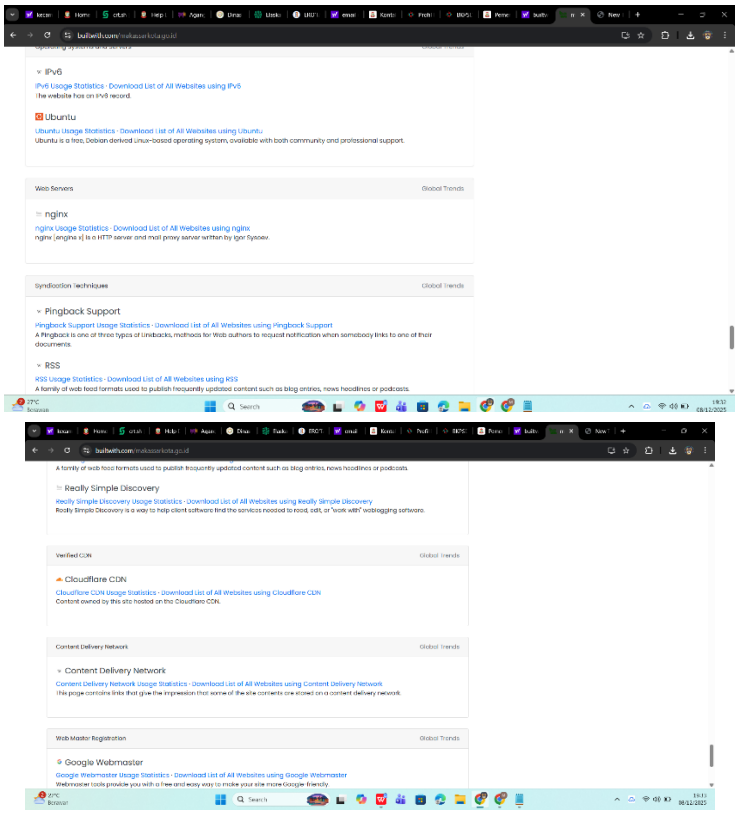
- Karyawan diskominfo

117	H. ABRAM LULULANGI,S.I.P	197107211991011001	IV/a	Kepala Bidang Persandian	Sarjana
118	SUHENDRA,S.STP,M.Si	197909301997111001	IV/a	Kepala Bidang Pengolahan Data Elektronik	Magister
119	ISMAWATY NUR,ST.,M.Sc.,Ph.D.	197406072004112001	IV/a	Sekretaris Dinas Komunikasi dan Informatika	Magister

Gambar 1.3 Identifikasi Profil Pejabat pegawai makassar kota

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

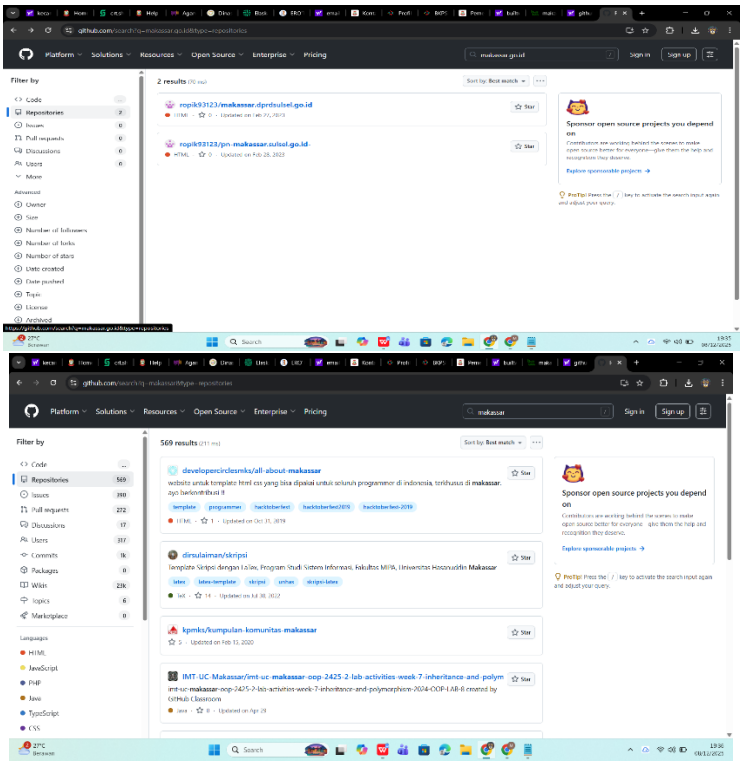
3. Teknologi yang digunakan



Gambar 1.4 Identifikasi Teknologi Website dan Struktur Organisasi

Penggunaan Cloudflare menunjukkan bahwa server asli (Origin IP) mungkin tersembunyi di balik WAF (Web Application Firewall). Serangan langsung ke domain utama mungkin akan diblokir, sehingga penyerang kemungkinan akan mengalihkan fokus ke subdomain yang tidak terlindungi Cloudflare (seperti yang ditemukan di crt.sh)

4. Informasi sensitive yang terpapar

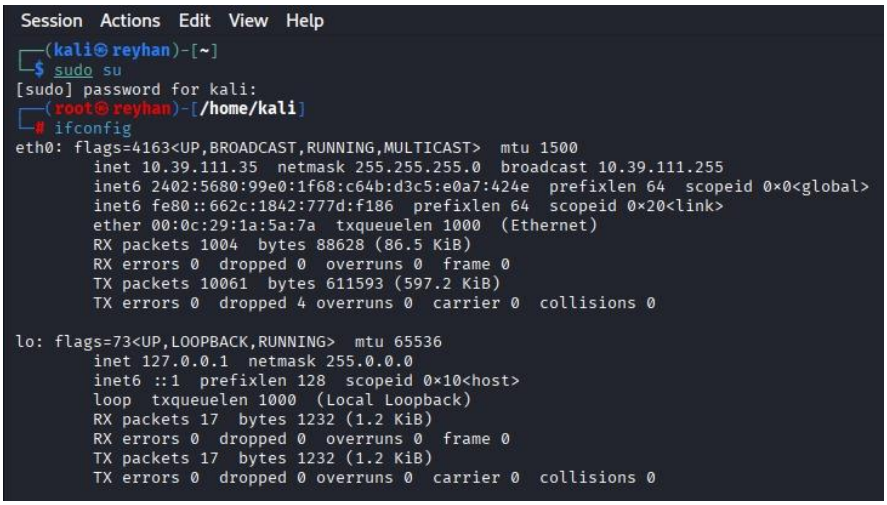


Gambar 1.5 Temuan Repository GitHub (OSINT)

Potensi kebocoran source code atau kredensial pada repository publik. Temuan repository pada GitHub (makassar) sangat kritis. Jika pengembang lupa menghapus file konfigurasi (seperti .env atau config.php), penyerang dapat menemukan *hardcoded credentials* (username/password database) yang memungkinkan pengambilalihan sistem tanpa perlu mengeksploitasi celah software

4. ACTIVE RECONNAISSANCE (HASIL & ANALISIS)

ifconfig



Gambar 1.6 Konfigurasi IP Attacker (Kali Linux)

Sebelum melakukan pemindaian aktif, terlebih dahulu dilakukan verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) menggunakan perintah ifconfig untuk memastikan parameter antarmuka jaringan telah sesuai dengan skenario pengujian. Hasil keluaran ifconfig pada antarmuka eth0 menunjukkan bahwa mesin penyerang memperoleh alamat IP 10.39.111.35 dengan netmask 255.255.255.0 dan gateway yang mengarah ke jaringan 10.39.111.0/24, sehingga dapat dipastikan bahwa host penyerang berada pada segmen jaringan yang sama dengan target 10.39.111.38 dan memiliki konektivitas yang diperlukan untuk pelaksanaan teknik pemindaian selanjutnya.

a. Host Discovery dan Port Scanning

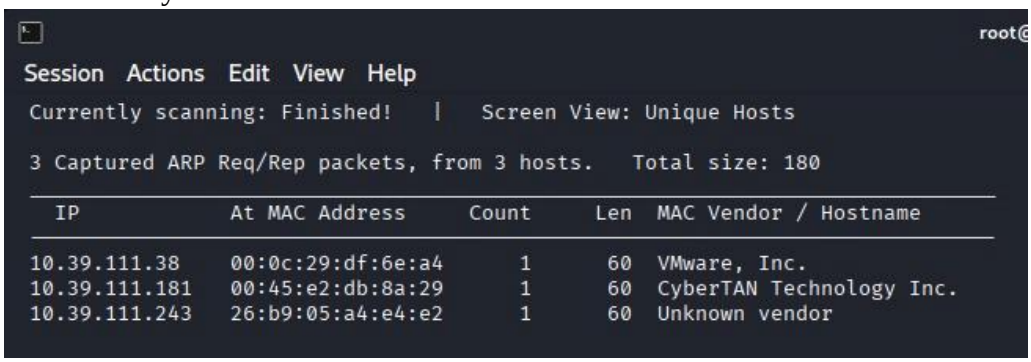
Tabel 1.4 Hasil Pemindaian Host dan Port (Active Reconnaissance

Tugas	Command	Hasil	Potensi Dampak
Host Discovery	sudo netdiscover -r 10.39.111.0/24	Target ditemukan: 10.39.111.38	Memastikan host 10.39.111.38 aktif di jaringan. Dan dapat dijadikan objek pemindai lanjutan
TCP SYN Scan	sudo nmap -sS -p- 10.39.111.38	Port terbuka: 22, 80, 6667	Permukaan serangan pada layanan SSH, HTTP, dan IRC yang dapat dieksploitasi jika terdapat kerentanan

UDP Scan	sudo nmap -sU --topports 10.39.111.38	Seluruh port UDP pada daftar top 20 terdeteksi dalam keadaan closed	Layanan UDP pada daftar top ports,sehingga risiko eksploitasi melalui UDP relative rendah pada scenario ini.

a. Dokumentasi

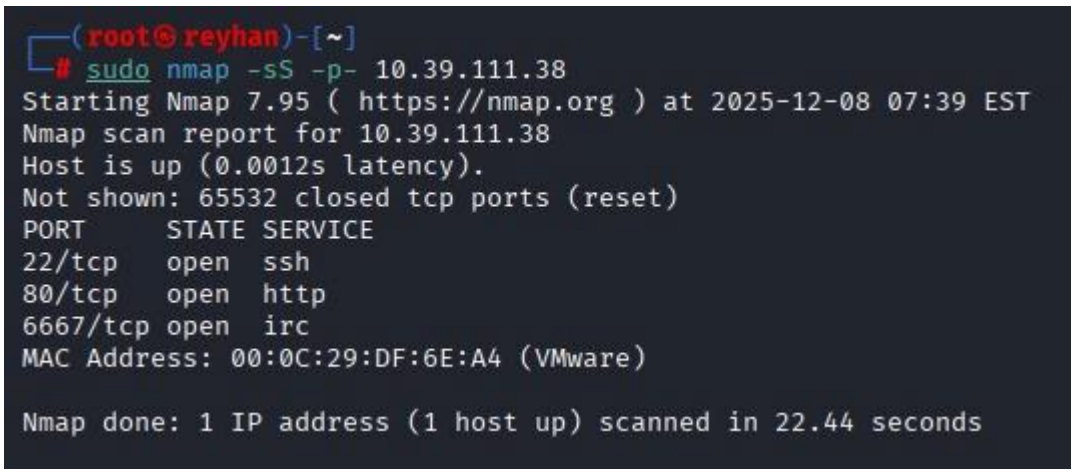
- Host discovery



Gambar 1.7 Hasil Host Discovery dengan Netdiscover

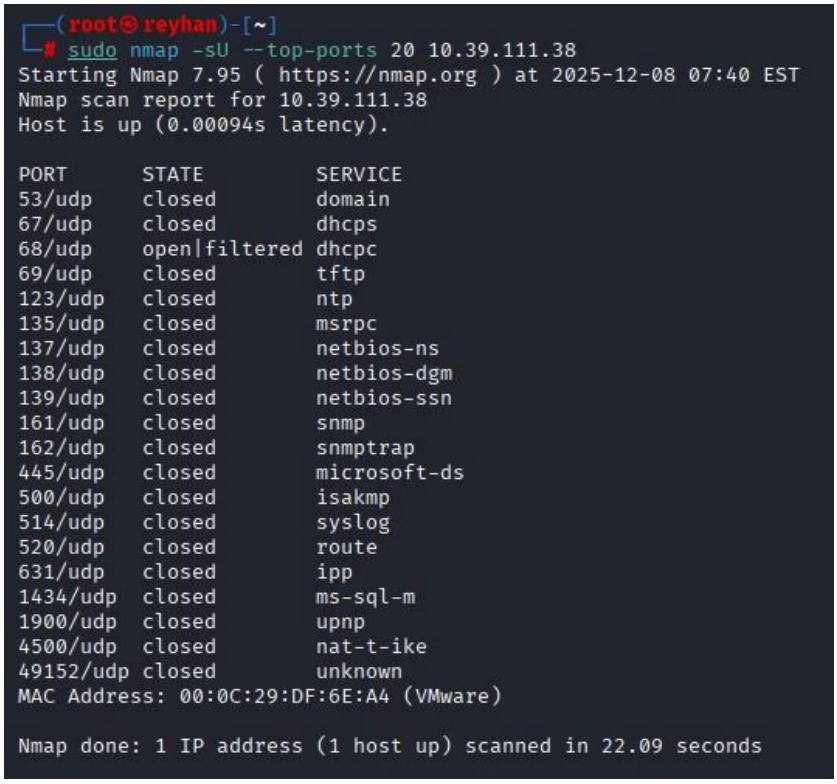
Mengidentifikasi host yang aktif. 10.39.111.38 teridentifikasi menggunakan vendor VMware (volunsOS)

- TCP SYN scan



Gambar 1.8 Hasil TCP SYN Scan (Stealth Scan) Menemukan port TCP terbuka (22, 80, 6667) 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

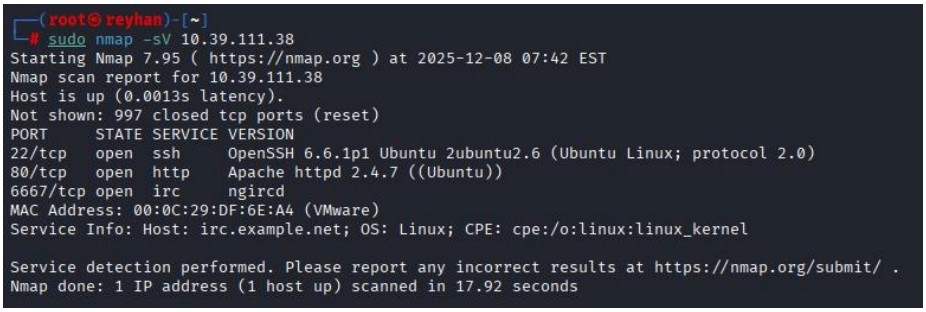
sudo nmap -sV 172.20.10.3

Tabel 1.5 Deteksi Versi Layanan dan Analisis Kerentanan

Port	Service	Version	Analisis Risiko
22	SSH	OpenSSH 6.6.1p1	Versi lama → potensi brute force & enumeration kredensial jika tidak di lindungi mekanisme hardening dan pembatasan akses yang memadai
80	HTTP	Apache 2.4.7	Versi apache yang sudah using dan memiliki banyak kerentanan web server jika patch keamanan tidak diterapkan

6667	IRC	(terdeteksi sebagai layanan IRC standar)	Ditemukannya Port 6667 (IRC) dengan service ngircd adalah anomali besar untuk server pemerintah atau perusahaan. Port ini sering dikaitkan dengan *backdoor* (seperti kerentanan pada UnrealIRCd) atau digunakan oleh botnet untuk Command & Control (C2). Ini adalah prioritas utama untuk tahap eksploitasi selanjutnya

• Bukti service detection



Gambar 1.10 Deteksi Versi Layanan dan Sistem Operasi

Target teridentifikasi menggunakan Ubuntu Linux lawas dengan layanan OpenSSH 6.6.1p1 dan Apache 2.4.7.

c. OS Fingerprinting

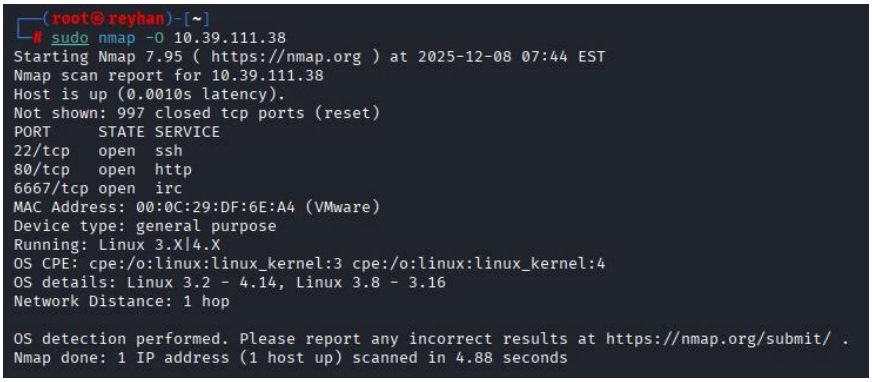
sudo nmap -O 172.20.10.3

Tabel 1.6 Hasil Identifikasi Sistem Operasi Target

Hasil	Detail OS	Analisis

OS Terdeteksi	Linux Kernel 3.x – 4.x	Berdasarkan fingerprinting Nmap, sistem operasi target teridentifikasi menggunakan kernel Linux generasi 3.x hingga 4.x, yang umumnya ditemukan pada distribusi Linux versi lama. Sistem operasi dengan kernel lama berpotensi tidak lagi menerima pembaruan keamanan penuh, sehingga lebih rentan terhadap eksploitasi kerentanan lokal maupun remote jika patch dan hardening tidak diterapkan secara konsisten.

• Bukti OS fingerprinting



Gambar 1.11 Hasil Identifikasi Sistem perasi (OS Fingerprinting)

Berdasarkan fingerprinting Nmap, sistem operasi target teridentifikasi menggunakan kernel Linux generasi 3.x hingga 4.x, yang umumnya ditemukan pada distribusi Linux versi lama. Sistem operasi dengan kernel lama berpotensi tidak lagi menerima pembaruan keamanan penuh, sehingga lebih rentan terhadap eksploitasi kerentanan lokal maupun remote jika patch dan hardening tidak diterapkan secara konsisten.

d. Network Protocol Analysis

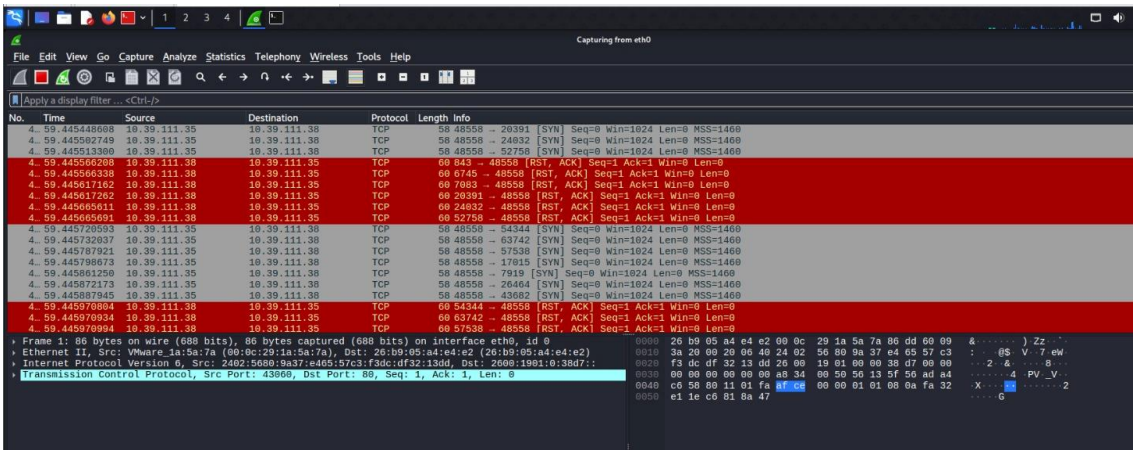
Tools:Wireshark

Berdasarkan hasil tangkapan trafik pada Gambar …, terlihat rangkaian paket TCP antara host penyerang 10.39.111.35 dan target 10.39.111.38 yang merepresentasikan proses pemindaian TCP SYN Scan. Pertama, penyerang mengirimkan segmen TCP dengan flag SYN ke port layanan target untuk meminta inisiasi koneksi.

Target kemudian merespons dengan paket SYN-ACK pada port yang berstatus open, yang menandakan bahwa port tersebut siap menerima koneksi.

Alih-alih menyelesaikan three-way handshake dengan mengirim ACK, host penyerang justru mengirim paket RST sehingga koneksi tidak pernah benar-benar terbentuk secara penuh.

Pola pertukaran SYN → SYN-ACK → RST yang berulang pada beberapa port ini mengonfirmasi penggunaan teknik TCP SYN Scan (stealth scan), di mana koneksi hanya dibuka secara parsial. Pendekatan ini membantu mengidentifikasi port terbuka sekaligus meminimalkan jejak koneksi yang tercatat pada aplikasi layanan di sisi target.



Gambar 1.12 Analisis Paket Jaringan dengan Wireshark

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

5. KESIMPULAN DAN SARAN a. Kesimpulan

Berdasarkan serangkaian aktivitas *Passive* dan *Active Reconnaissance* yang telah dilakukan, dapat ditarik beberapa kesimpulan penting terkait postur keamanan target:

1. Dari sisi passive reconnaissance, pemanfaatan layanan publik seperti GitHub, BuiltWith, crt.sh, portal resmi pemerintah, dan dokumen profil pegawai telah mengungkap informasi teknologi, struktur organisasi, dan jejak domain/subdomain tanpa melakukan interaksi langsung berisiko dengan sistem target.
2. Informasi teknis yang diperoleh secara pasif (misalnya CMS WordPress, server Ubuntu dengan Nginx/Cloudflare, serta keberadaan berbagai subdomain layanan) memberikan gambaran arsitektur layanan dan potensi permukaan serangan, namun tetap berada dalam batas pengamatan OSINT yang legal dan minim dampak.
3. Melalui active reconnaissance di lingkungan lab tertutup terhadap host 10.39.111.38, pemindaian Nmap (host discovery, TCP SYN scan, UDP scan, OS fingerprinting, dan

service/version detection) berhasil mengidentifikasi port 22, 80, dan 6667 yang terbuka, versi OpenSSH dan Apache yang usang, serta sistem operasi Linux kernel 3.x–4.x yang berpotensi sudah mendekati atau melewati EOL.

4. Analisis paket menggunakan Wireshark mengonfirmasi pola TCP SYN Scan (SYN → SYN-ACK → RST) sebagai teknik half-open scanning yang efektif untuk memetakan port terbuka sekaligus mengurangi jejak koneksi penuh pada sisi layanan target.
5. Kombinasi passive dan active reconnaissance tersebut menyediakan basis yang kuat untuk penilaian awal risiko keamanan, di mana hasil OSINT publik menuntun fokus pengujian, sementara eksperimen aktif di lab memberikan bukti teknis detail mengenai konfigurasi layanan dan kelemahan potensial tanpa menyentuh langsung infrastruktur produksi.

b. Saran dan Rekomendasi

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

1. Manajemen Aset Digital (Digital Footprint)
    - Segera ubah pengaturan repository GitHub terkait sistem/aplikasi pemerintah menjadi private atau batasi hanya untuk internal, serta hapus informasi sensitif yang tidak perlu dipublikasikan agar mengurangi risiko information disclosure yang dapat dimanfaatkan untuk social engineering.
    - Laksanakan pelatihan security awareness bagi pegawai, khususnya yang alamat emailnya dipublikasikan pada portal resmi, untuk meningkatkan kewaspadaan terhadap phishing, spear-phishing, dan rekayasa sosial lainnya.
2. Patch Management & Hardening
    - Lakukan pembaruan (upgrade) sistem operasi dan layanan pada server uji yang menggunakan Linux kernel 3.x–4.x, OpenSSH 6.6.1p1, dan Apache 2.4.7 ke versi yang masih mendapatkan dukungan keamanan, sehingga kerentanan dengan CVE publik dapat diminimalkan.
    - Nonaktifkan atau batasi akses ke layanan pada port 6667/tcp (IRC) apabila tidak digunakan untuk kebutuhan operasional yang sah, karena port tersebut sering diasosiasikan dengan kanal Command & Control (C2) botnet maupun backdoor.
3. Implementasi Keamanan Jaringan

- Terapkan aturan firewall berbasis host maupun perimeter (misalnya dengan iptables atau solusi firewall lain) untuk membatasi akses hanya dari alamat IP yang terotorisasi ke port layanan esensial seperti 22/tcp, 80/tcp, dan 443/tcp.
- Gunakan IDS/IPS jaringan untuk memantau pola pemindaian aktif, termasuk deteksi signature TCP SYN Scan, sehingga aktivitas reconnaissance yang mirip dengan uji lab dapat terpantau dan direspons secara real-time