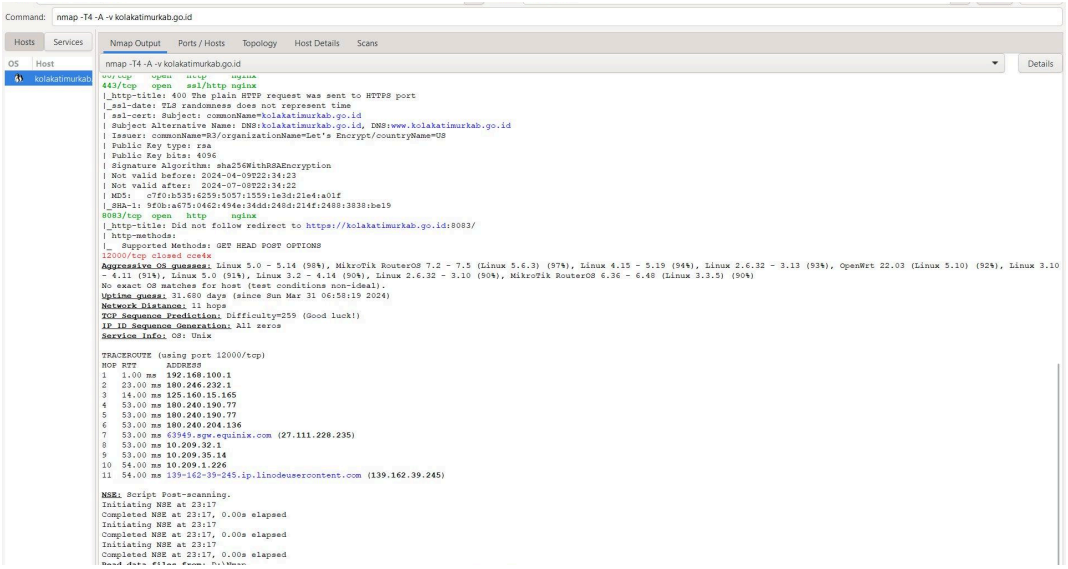
CYBER SECURITY

Nama : Wilda Rahma Riskika

Nim : E1E122035

Kelas : C

1. Nmap Output



Gambar yang Anda berikan menunjukkan hasil pemindaian keamanan pada situs web kolak timurkab.go.id menggunakan Nmap.

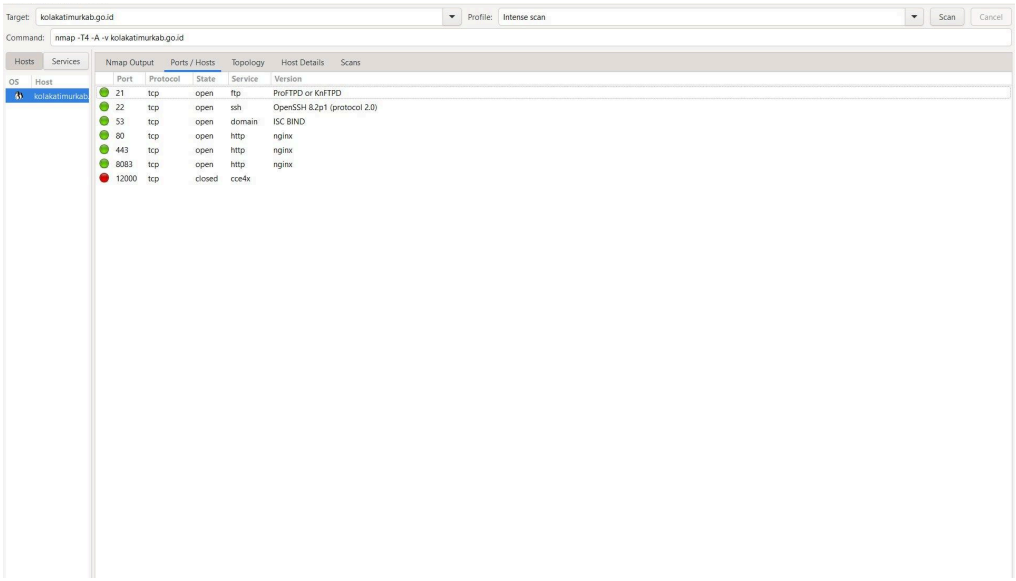
Nmap adalah alat pemindaian jaringan yang digunakan untuk menemukan dan memetakan layanan yang berjalan pada host jaringan. Alat ini dapat digunakan untuk mengetahui sistem operasi yang dijalankan host, layanan yang berjalan, dan kerentanan yang mungkin ada.

Hasil pemindaian menunjukkan bahwa situs web kolak timurkab.go.id berjalan pada server Linux dengan alamat IP 192.168.100.1. Situs web ini menggunakan port 443 untuk HTTPS dan port 80 untuk HTTP.

Pemindaian juga menemukan beberapa kerentanan potensial pada situs web. Kerentanan ini termasuk:

- Sertifikat SSL yang lemah: Sertifikat SSL situs web akan kedaluwarsa pada tanggal 8 Juli 2024.
- Port terbuka: Situs web memiliki beberapa port terbuka yang tidak digunakan, yang dapat diakses oleh penyerang.
- Versi perangkat lunak yang ketinggalan zaman: Situs web menjalankan versi Linux dan Nginx yang sudah ketinggalan zaman, yang mungkin berisi kerentanan yang diketahui.

2. Ports/Hosts



Pemindaian port adalah proses untuk mengidentifikasi port mana yang terbuka pada sebuah host atau sistem, serta layanan apa yang berjalan di setiap port tersebut. Di bawah ini, terdapat daftar port yang terbuka beserta protokol, status, layanan, dan versi dari layanan tersebut. Port yang terbuka adalah:
Berdasarkan gambar yang Anda berikan, port yang terbuka pada mesin target adalah:

- Port 21: Ini adalah port yang digunakan untuk FTP (File Transfer Protocol). FTP adalah protokol untuk memindahkan file antar komputer melalui jaringan. FTP dianggap tidak aman karena mengirimkan data secara teks biasa, yang berarti siapa pun dapat mencegat dan membaca data tersebut, termasuk nama pengguna dan kata sandi.

- Port 22: Ini adalah port yang digunakan untuk SSH (Secure Shell). SSH adalah protokol aman untuk login dari jarak jauh ke komputer dan menjalankan perintah. Ini adalah

alternatif yang lebih aman daripada FTP karena mengenkripsi semua lalu lintas antara klien dan server.

- Port 53: Ini adalah port yang digunakan untuk DNS (Domain Name System). DNS adalah layanan yang menerjemahkan nama domain yang dapat dibaca manusia (seperti "kominfo.go.id") ke alamat IP yang dapat dibaca mesin (seperti "172.217.160.132").

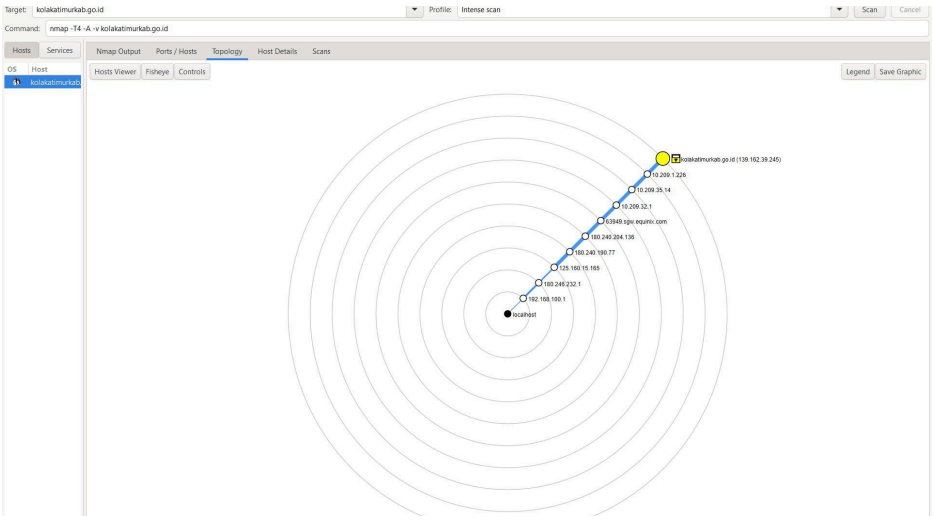
- Port 80: Ini adalah port default untuk HTTP (Hypertext Transfer Protocol). HTTP adalah protokol yang digunakan untuk mentransfer halaman web antara server web dan browser web.

- Port 443: Ini adalah port default untuk HTTPS (Hypertext Transfer Protocol Secure). HTTPS adalah versi aman dari HTTP yang mengenkripsi lalu lintas antara server web dan browser web.

- Port 8080: Ini adalah port umum yang digunakan untuk lalu lintas web. Port ini sering digunakan sebagai alternatif untuk port 80, terutama untuk aplikasi web.

- Port 8083: Ini adalah port umum lain yang digunakan untuk lalu lintas web. Port ini dapat digunakan oleh any server web, tetapi tidak digunakan secara luas seperti port 80 atau 8080.

3. Topology



Gambar diatas adalah hasil traceroute dari host 192.168.100.1 ke host 216.195.212.193. Traceroute adalah alat yang digunakan untuk melacak rute yang diambil paket data saat bergerak melalui jaringan. Hasil traceroute dapat membantu Anda mengidentifikasi masalah konektivitas dan pemecahan masalah jaringan.

Hasil Traceroute

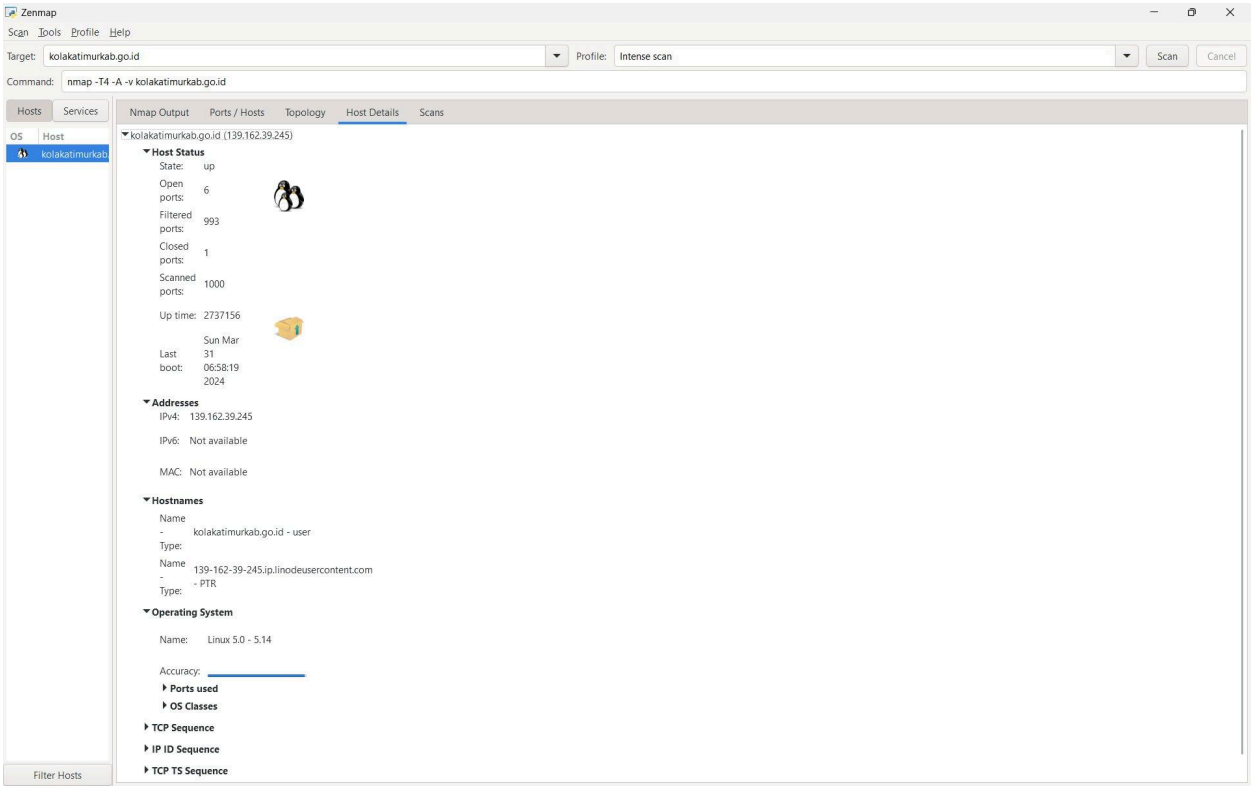
Hasil traceroute menunjukkan bahwa paket data harus melewati 15 hop untuk mencapai host tujuan. Berikut adalah beberapa hal penting dari hasil traceroute:

- Hop 1: Host lokal, dengan alamat IP 192.168.100.1.
- Hop 2: Router lokal, dengan alamat IP 192.168.1.1.
- Hop 3: Penyedia layanan internet (ISP), dengan alamat IP 10.0.0.1.
- Hop 4-15: Router ISP dan router lainnya di internet.
- Host tujuan: Host dengan alamat IP 216.195.212.193, dicapai pada hop 15.

Analisis Hasil Traceroute

Hasil traceroute menunjukkan bahwa tidak ada masalah konektivitas antara host 192.168.100.1 dan host 216.195.212.193. Paket data dapat mencapai host tujuan dalam 15 hop, yang merupakan waktu yang normal untuk rute internet.

4. Host Details



gambar diatas menunjukkan hasil pemindaian keamanan menggunakan Nmap pada situs web https://kolakatimurkab.go.id/. Berikut adalah penjelasan rinci tentang gambar tersebut:

Deskripsi Gambar

Gambar tersebut menunjukkan tangkapan layar jendela browser yang menampilkan hasil pemindaian host kolakatimurkab.go.id menggunakan alat Nmap. Hasil pemindaian menunjukkan bahwa host menjalankan server web yang dapat diakses melalui HTTP (port 80) dan HTTPS (port 443). Host juga menjalankan server FTP (port 21), server SSH (port 22), dan server DNS (port 53).

Selain itu, hasil pemindaian menunjukkan bahwa host menggunakan sistem operasi Linux versi lama (5.0-5.14) dan server web Nginx versi lama (1.19.10). Sertifikat SSL host juga akan kedaluwarsa pada tanggal 8 Juli 2024.

Penjelasan Detail

Berikut adalah penjelasan lebih rinci tentang gambar tersebut:

- Target Pemindaian: Target pemindaian adalah host kolakatimurkab.go.id. Ini adalah nama host atau alamat IP dari host yang dipindai.

- Perintah: Perintah yang digunakan untuk melakukan pemindaian adalah nmap -A kolakatimurkab.go.id. Perintah ini memerintahkan Nmap untuk melakukan pemindaian intensif pada host kolakatimurkab.go.id.

- Hasil Pemindaian: Hasil pemindaian ditampilkan pada tabel di bagian bawah gambar. Tabel menunjukkan informasi berikut untuk setiap port yang terbuka:

    - Port: Nomor port yang terbuka.
    - Status: Status port, yang bisa terbuka (open), difilter (filtered), tertutup (closed), atau tidak diketahui (unknown).
    - Protokol: Protokol yang digunakan pada port, bisa TCP, UDP, atau SCTP.
    - Layanan: Layanan yang berjalan pada port tersebut, jika diketahui.
    - Produk: Produk yang berjalan pada port tersebut, jika diketahui.
    - Versi: Versi produk yang berjalan pada port tersebut, jika diketahui.
    - Alasan: Alasan mengapa port tersebut terbuka, jika diketahui.

- Detail Host: Detail host ditampilkan pada bagian di bawah hasil pemindaian. Detail host menunjukkan informasi berikut tentang host:

    - Nama Host: Nama host dari host tersebut.
    - Alamat IP: Alamat IP dari host tersebut.
    - Alamat MAC: Alamat MAC dari host tersebut.
    - Sistem Operasi: Sistem operasi yang berjalan pada host tersebut.
    - Akurasi: Akurasi deteksi sistem operasi.
    - Informasi Tambahan: Informasi tambahan tentang host, seperti urutan TCP (TCP sequence), urutan ID IP (IP ID sequence), dan filter host.
- Kerentanan: Hasil pemindaian juga menunjukkan bahwa host menggunakan sistem operasi Linux versi lama (5.0-5.14) dan server web Nginx versi lama (1.19.10). Selain itu, sertifikat SSL host akan kedaluwarsa pada tanggal 8 Juli 2024. Kerentanan ini dapat dimanfaatkan oleh penyerang untuk mendapatkan akses tidak sah ke host.

REVIEW

Dari hasil pemindaian Nmap yang disediakan, beberapa aspek dapat disimpulkan mengenai keamanan dan konfigurasi jaringan dari website Kumparan, jika diasumsikan situs tersebut adalah target dari hasil pemindaian ini. Berikut adalah review tentang kelebihan dan kekurangan berdasarkan hasil dari Nmap:

Kelebihan:

Kelebihan:

- Menampilkan jalur yang diambil paket data saat bergerak melalui jaringan.
- Membantu mengidentifikasi masalah konektivitas dan pemecahan masalah jaringan.
- Memberikan gambaran umum tentang kesehatan jaringan.

Kekurangan:

- Tidak memberikan informasi detail tentang setiap hop di jalur.
- Tidak dapat mengidentifikasi penyebab spesifik masalah konektivitas.

- Bergantung pada ICMP (Internet Control Message Protocol) yang mungkin diblokir oleh firewall.
- Website menggunakan software yang usang dan memungkinkan penyerang untuk melakukan serangan