# Modul 2: Networking Fundamentals for Hackers

Memahami bagaimana komputer berkomunikasi dan bagaimana hacker memanfaatkan kelemahan jaringan — fondasi wajib bagi setiap praktisi keamanan siber.

EDY SUSANTO — FOUNDER C-SIX SECURITY

# Tujuan Pembelajaran

Di akhir modul ini, peserta akan memiliki pemahaman solid tentang cara kerja jaringan komputer dan bagaimana hacker mengeksploitasi celah-celah di dalamnya.

### 🧠 Konsep

Memahami arsitektur jaringan, protokol, dan infrastruktur internet secara menyeluruh.

### 🔧 Praktik

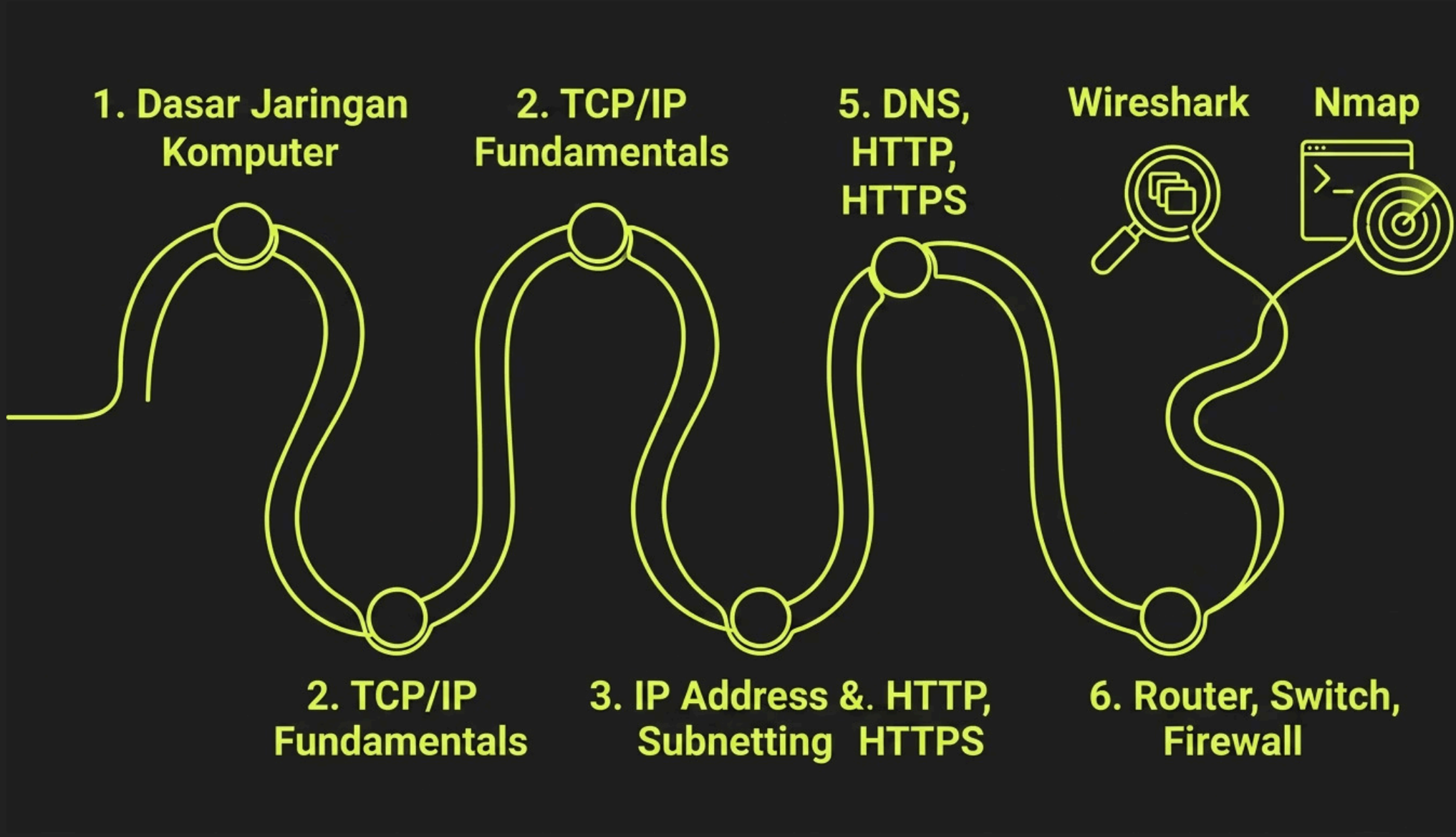
Menganalisis lalu lintas jaringan nyata menggunakan Wireshark dan Nmap.

### 🎯 Outcome

Menjadi fondasi kuat untuk teknik hacking dan penetration testing lebih lanjut.

# Peta Materi Modul 2

Modul ini dirancang secara bertahap — dari konsep dasar hingga praktik langsung dengan tools nyata.



# Dasar Jaringan Komputer

Jaringan komputer adalah infrastruktur yang memungkinkan perangkat saling bertukar data. Memahami strukturnya adalah langkah pertama memahami cara hacker bergerak di dalamnya.

## Jenis Jaringan

- **LAN** — Local Area Network, jaringan lokal (kantor, rumah)
- **WAN** — Wide Area Network, jaringan antar kota/negara
- **WLAN** — Wireless LAN, jaringan nirkabel

## Topologi Umum

- **Star** — semua perangkat terhubung ke satu switch pusat
- **Mesh** — setiap node terhubung ke banyak node lain
- **Bus** — semua perangkat berbagi satu kabel

# TCP/IP Fundamentals

TCP/IP adalah bahasa universal yang digunakan seluruh perangkat di internet untuk berkomunikasi. Hacker sangat memahami setiap lapisan model ini untuk mencari celah masuk.

1

### Application Layer

HTTP, HTTPS, DNS, FTP — tempat data diproduksi dan dikonsumsi aplikasi.

2

### Transport Layer

TCP (koneksi andal) dan UDP (cepat tanpa konfirmasi) — mengatur pengiriman data.

3

### Internet Layer

IP Address, routing — menentukan jalur data dari sumber ke tujuan.

4

### Network Access Layer

Ethernet, Wi-Fi — transmisi fisik data melalui media jaringan.

ⓘ Hacker perlu memahami setiap lapisan karena setiap lapisan menyimpan potensi kerentanan yang berbeda.

# IP Address dan Subnetting Dasar

## Apa Itu IP Address?

IP Address adalah identitas unik setiap perangkat dalam jaringan. Tersedia dua versi:

- **IPv4** — 32-bit, contoh: `192.168.1.1`
- **IPv6** — 128-bit, contoh: `2001:0db8::1`

Terdapat juga pembagian **IP Publik** (terlihat di internet) dan **IP Privat** (hanya di jaringan lokal).

## Subnetting Dasar

Subnetting memecah jaringan besar menjadi segmen lebih kecil menggunakan **subnet mask**.

- `/24` = 256 host (subnet mask `255.255.255.0`)
- `/16` = 65.536 host
- `/8` = 16 juta host

> Hacker menggunakan teknik **network scanning** untuk memetakan seluruh subnet target.

# Port dan Protokol

Port adalah "pintu" komunikasi di sebuah komputer. Setiap layanan berjalan di port tertentu — dan hacker selalu mencari port yang terbuka atau salah konfigurasi.

| Port | Protokol | Layanan |
|---|---|---|
| 21 | TCP | FTP — transfer file |
| 22 | TCP | SSH — remote shell terenkripsi |
| 80 | TCP | HTTP — web tidak terenkripsi |
| 443 | TCP | HTTPS — web terenkripsi |
| 3389 | TCP | RDP — Remote Desktop (Windows) |

⚠ Port terbuka yang tidak dimonitor adalah celah utama yang dieksploitasi penyerang.

# DNS, HTTP, dan HTTPS

Tiga protokol ini adalah tulang punggung web modern. Memahami cara kerjanya membantu mendeteksi serangan seperti DNS spoofing, man-in-the-middle, dan SSL stripping.

## DNS

Domain Name System menerjemahkan nama domain (seperti `google.com`) menjadi IP Address. Rentan terhadap **DNS Spoofing** dan **Cache Poisoning**.

## HTTP

HyperText Transfer Protocol — mengirim data web dalam teks biasa (*plain text*). Data bisa dicegat dan dibaca siapa saja di jaringan yang sama.

## HTTPS

Versi aman HTTP menggunakan enkripsi **TLS/SSL**. Data dienkripsi sehingga tidak bisa dibaca meski dicegat. Namun bukan berarti website tersebut sepenuhnya aman.

# Router, Switch, dan Firewall

Ketiga perangkat ini membentuk tulang punggung infrastruktur jaringan — dan masing-masing menjadi target potensial bagi seorang hacker.

### Router

Menghubungkan jaringan berbeda dan menentukan jalur terbaik untuk paket data. Jika router dikompromikan, seluruh lalu lintas bisa disadap.

### Switch

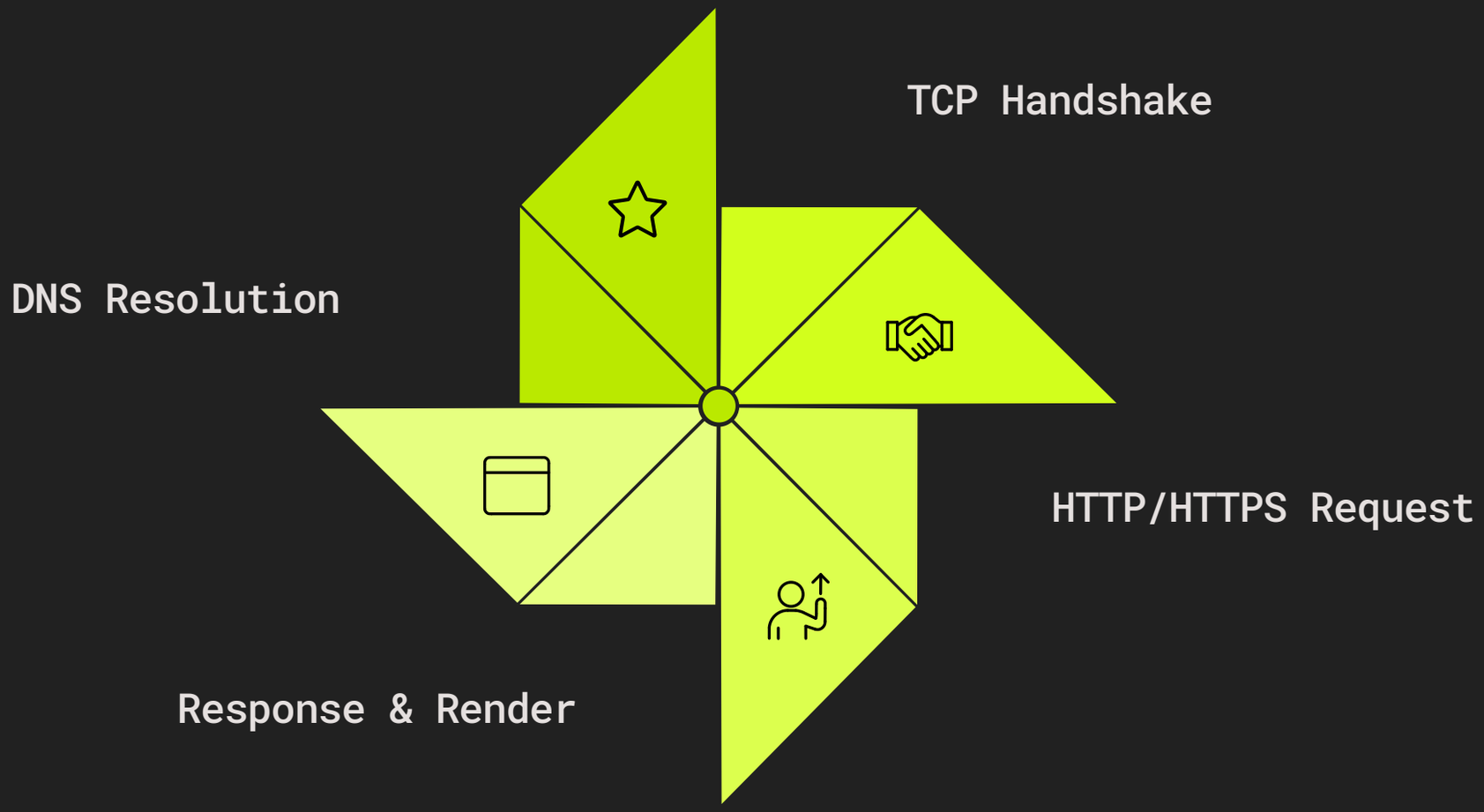
Menghubungkan perangkat dalam satu jaringan lokal (LAN). Serangan ARP Poisoning dapat membelokkan lalu lintas di level switch.

### Firewall

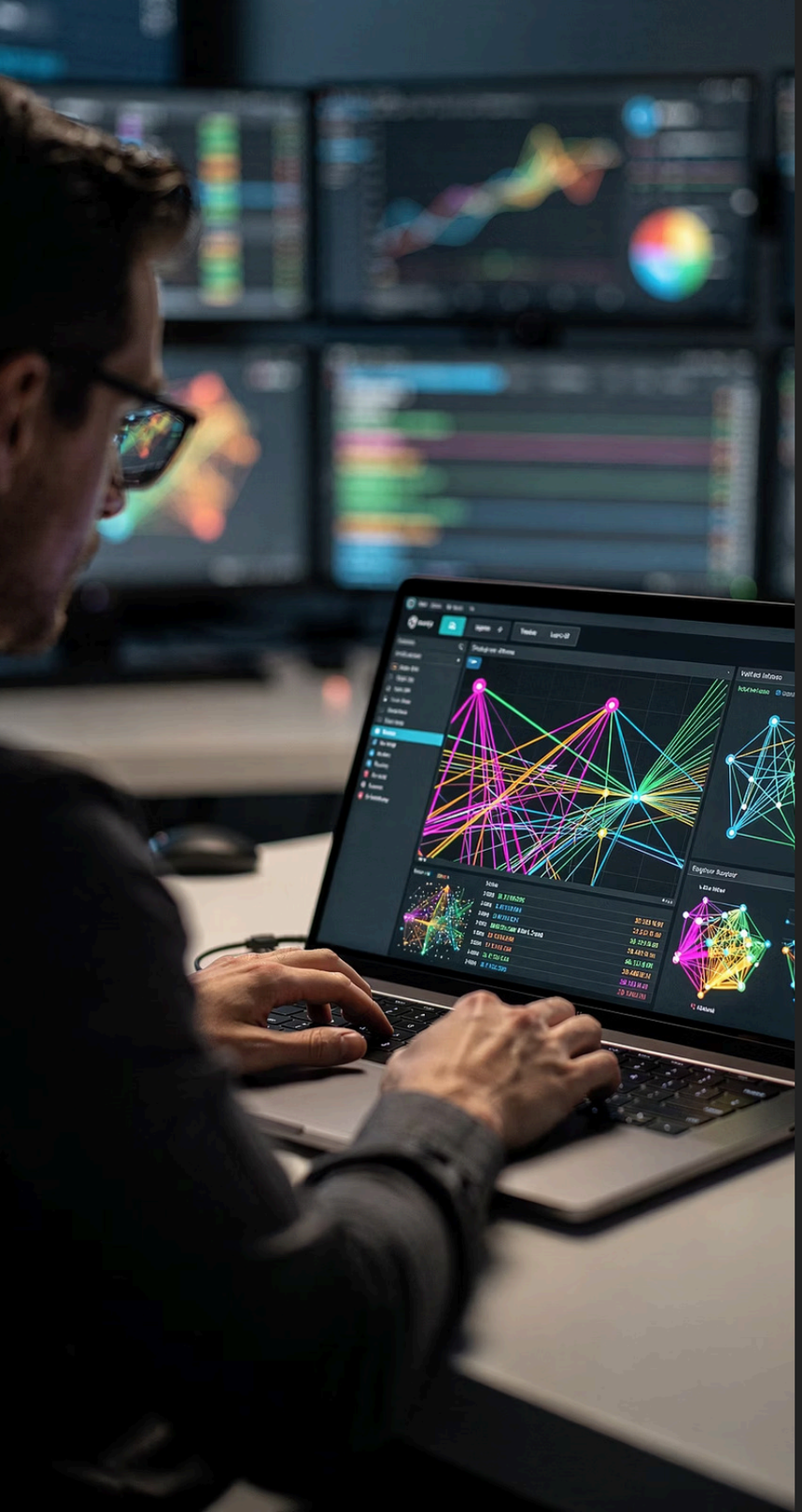
Memfilter lalu lintas berdasarkan aturan yang ditetapkan. Firewall yang salah konfigurasi justru menciptakan celah keamanan yang serius.

# Cara Kerja Internet

Saat kamu mengetik sebuah URL di browser, ada serangkaian proses kompleks yang terjadi dalam milidetik. Memahami alur ini sangat penting untuk memahami titik-titik kerentanan.




Setiap tahap dalam alur ini menyimpan potensi serangan — mulai dari DNS hijacking, TCP session hijacking, hingga man-in-the-middle attack pada level enkripsi.



# Praktik: Menggunakan Wireshark

Wireshark adalah tool analisis jaringan paling populer di dunia. Dengan Wireshark, kamu bisa "melihat" semua paket data yang melintas di jaringanmu secara real-time.

01

## Install dan Buka Wireshark

Download dari wireshark.org, jalankan sebagai administrator, pilih interface jaringan aktif (Wi-Fi atau Ethernet).

02

## Mulai Capture

Klik tombol capture, lalu buka browser dan kunjungi sebuah website. Amati paket yang muncul secara real-time.

03

## Filter Paket

Gunakan display filter seperti `http`, `dns`, atau `tcp.port==443` untuk menyaring lalu lintas yang relevan.

04

## Analisis Paket

Klik satu paket untuk melihat detail: source IP, destination IP, protokol yang digunakan, dan isi data (payload).

# Analisis Lalu Lintas Jaringan

Setelah mampu menangkap paket, langkah selanjutnya adalah memahami apa yang kamu lihat. Analisis lalu lintas membantu mengidentifikasi aktivitas normal vs. mencurigakan.

### Yang Dicari dalam Analisis

- IP Address yang paling sering mengirim data
- Port dan protokol yang digunakan
- Pola request yang tidak wajar
- Data sensitif yang dikirim tanpa enkripsi

### Filter Wireshark yang Berguna

- `http.request` — semua HTTP request
- `dns` — query DNS
- `ip.src == 192.168.1.1` — paket dari IP tertentu
- `tcp.flags.syn == 1` — deteksi port scanning

ⓘ Coba buka website HTTP (bukan HTTPS) dan lihat apakah kamu bisa membaca isi halamannya di Wireshark!

# Praktik: Nmap untuk Identifikasi Service

Nmap (Network Mapper) adalah tool open-source standar industri untuk network discovery dan security auditing. Dengan Nmap, kamu bisa memetakan perangkat dan service yang aktif dalam sebuah jaringan.

### Scan Host Aktif

`nmap -sn 192.168.1.0/24`

Menemukan semua perangkat yang aktif dalam subnet tanpa melakukan port scanning.

### Scan Port Terbuka

`nmap -sV 192.168.1.1`

Menampilkan port yang terbuka beserta versi service yang berjalan di setiap port.

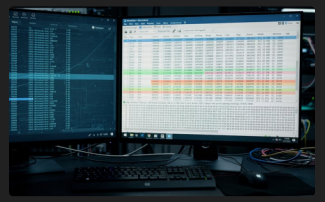
### Scan Agresif

`nmap -A 192.168.1.1`

Mendeteksi OS, versi service, script scanning, dan traceroute secara bersamaan.

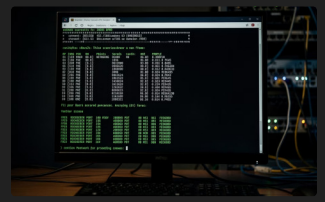
⚠ Hanya gunakan Nmap pada jaringan atau sistem yang kamu miliki izin untuk mengaksesnya. Scanning tanpa izin adalah tindakan ilegal.

# Tools yang Digunakan



## Wireshark

Packet analyzer gratis dan open-source. Tersedia untuk Windows, macOS, dan Linux. Digunakan oleh profesional keamanan siber di seluruh dunia untuk analisis forensik jaringan dan troubleshooting.



## Nmap

Network scanner paling andal untuk memetakan jaringan, menemukan host aktif, mengidentifikasi port terbuka, dan mendeteksi versi service. Tersedia gratis di nmap.org dan sudah terintegrasi di banyak distro Linux keamanan seperti Kali Linux.

# Ringkasan & Outcome Modul 2

Setelah menyelesaikan modul ini, kamu telah membangun fondasi yang kuat untuk perjalananmu di dunia keamanan siber.

### ✅ Jaringan Komputer

Memahami topologi, jenis jaringan, dan cara perangkat saling terhubung.

### ✅ TCP/IP & Protokol

Mengenal lapisan model TCP/IP, port, DNS, HTTP, dan HTTPS secara mendalam.

### ✅ Infrastruktur

Memahami peran router, switch, dan firewall dalam ekosistem jaringan.

### ✅ Praktik Langsung

Mampu menggunakan Wireshark dan Nmap untuk analisis dan identifikasi jaringan.

Fondasi jaringan yang kuat adalah kunci untuk memahami teknik hacking, penetration testing, dan pertahanan keamanan siber di modul-modul berikutnya.

EDY SUSANTO — FOUNDER C-SIX SECURITY