

# 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

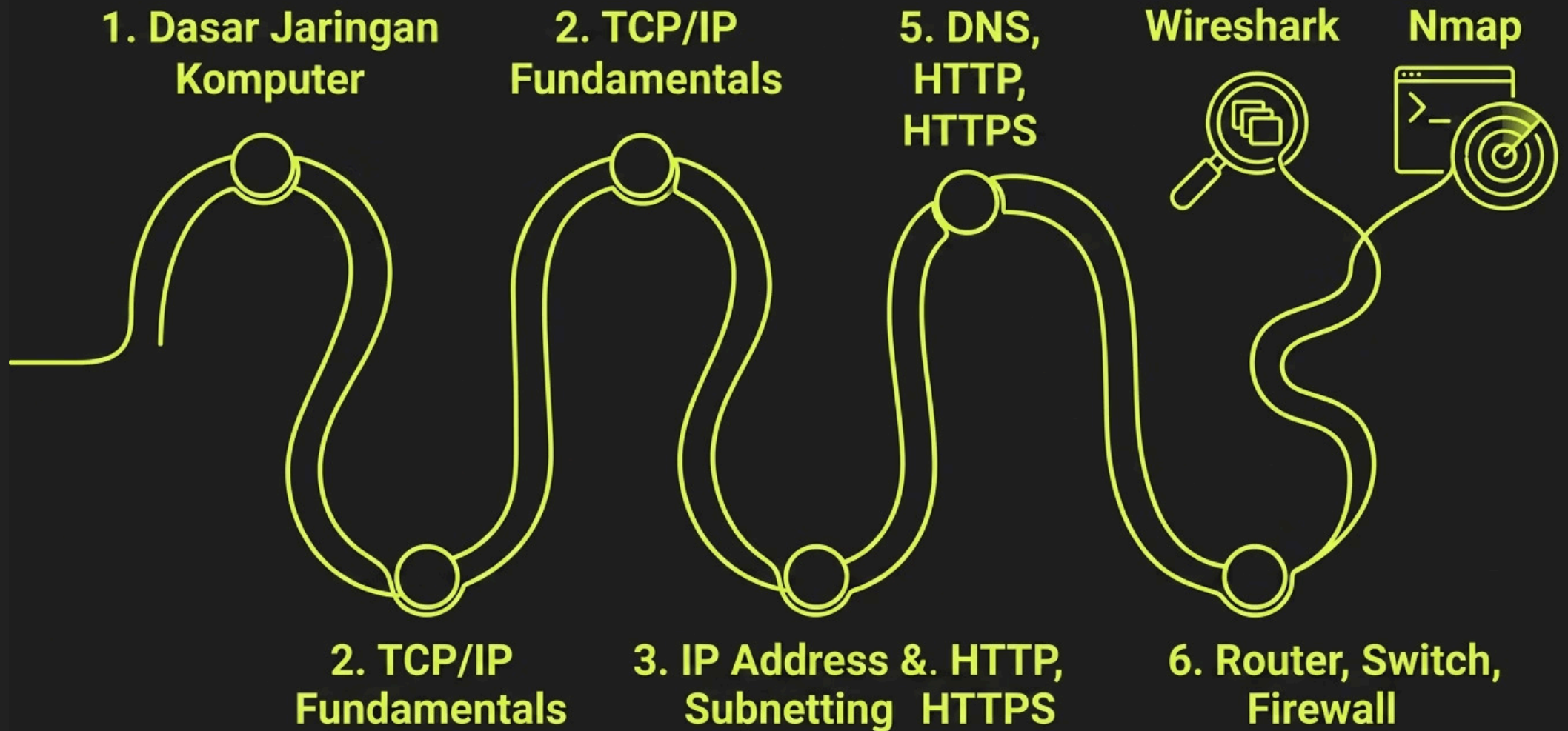
Menganalisis lalu lintas jaringan nyata menggunakan Wireshark dan Nmap.

## 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.

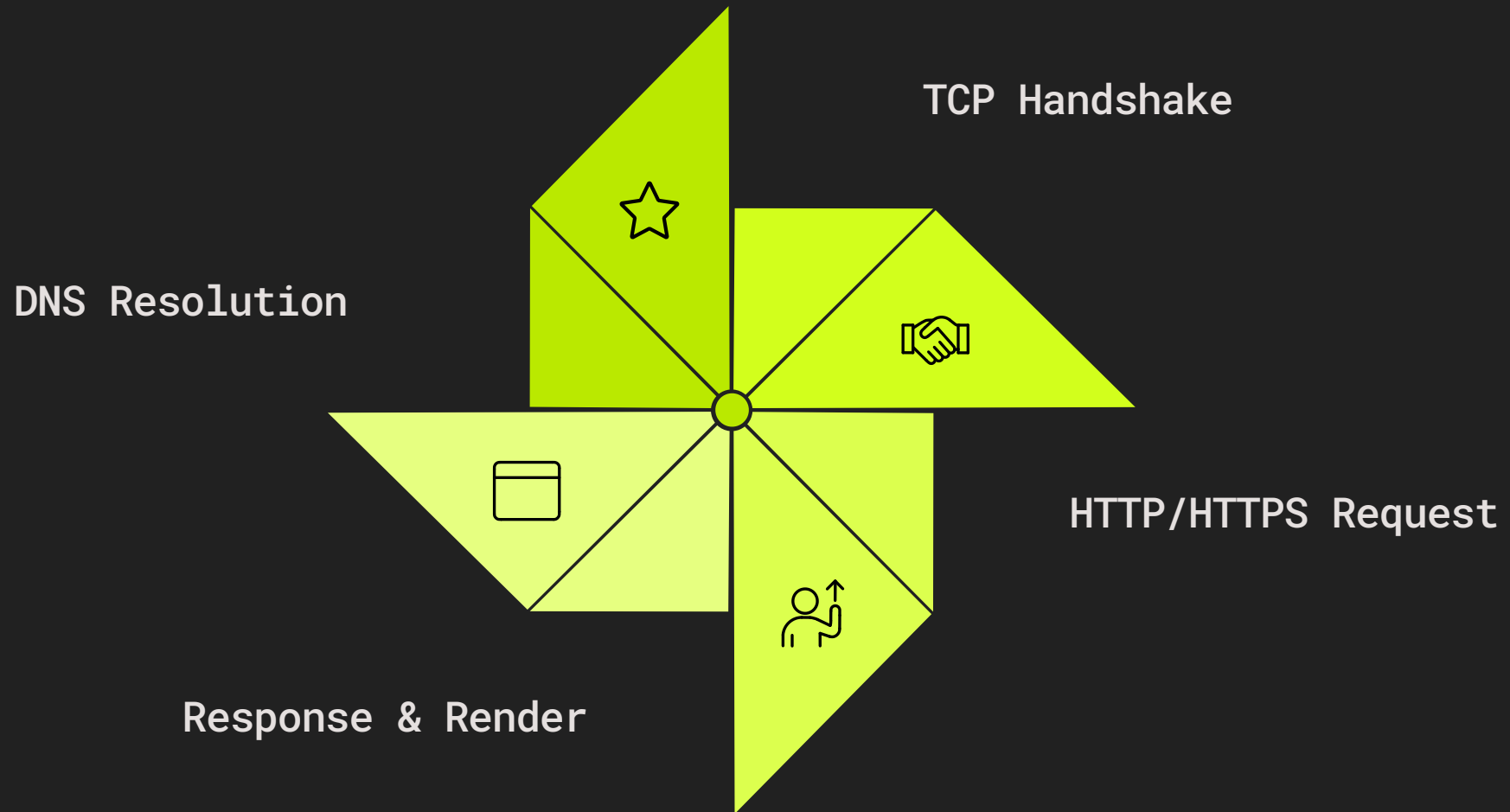


## Firewall

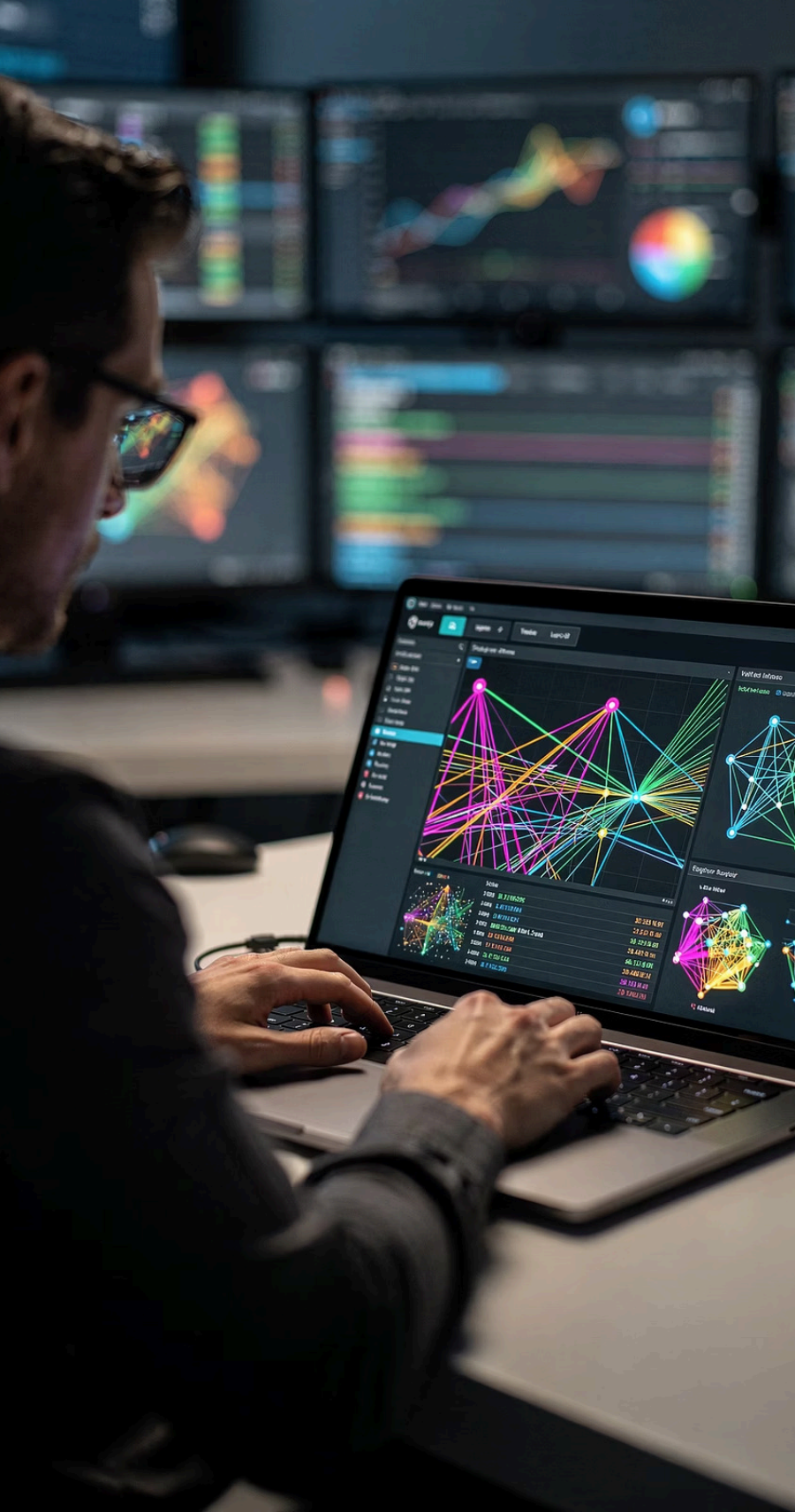
Memfilter lalu lintas berdasarkan aturan yang ditetapkan. Firewall yang salah konfigurasi justru menciptakan celah keamanan yang serius.

# 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](https://www.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.

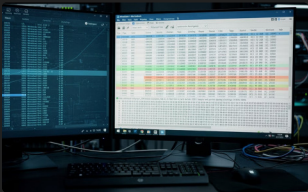
⚠ Hanya gunakan Nmap pada jaringan atau sistem yang kamu miliki izin untuk mengaksesnya. Scanning tanpa izin adalah tindakan ilegal.



```
192.168.1.0/24
nmap -sV -Pn 192.168.1.0/24
```

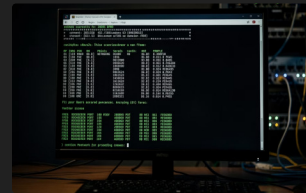
IP	PORT	STATE	SERVICE
192.168.1.1	22	tcp	ssh
192.168.1.1	80	tcp	open
192.168.1.1	443	tcp	open
192.168.1.1	8080	tcp	open http
192.168.1.1	8081	tcp	open
192.168.1.1	8082	tcp	open
192.168.1.1	8083	tcp	open
192.168.1.1	8084	tcp	open
192.168.1.1	8085	tcp	open
192.168.1.1	8086	tcp	open
192.168.1.1	8087	tcp	open
192.168.1.1	8088	tcp	open
192.168.1.1	8089	tcp	open
192.168.1.1	8090	tcp	open
192.168.1.1	8091	tcp	open
192.168.1.1	8092	tcp	open
192.168.1.1	8093	tcp	open
192.168.1.1	8094	tcp	open
192.168.1.1	8095	tcp	open
192.168.1.1	8096	tcp	open
192.168.1.1	8097	tcp	open
192.168.1.1	8098	tcp	open
192.168.1.1	8099	tcp	open
192.168.1.1	8100	tcp	open
192.168.1.1	8101	tcp	open
192.168.1.1	8102	tcp	open
192.168.1.1	8103	tcp	open
192.168.1.1	8104	tcp	open
192.168.1.1	8105	tcp	open
192.168.1.1	8106	tcp	open
192.168.1.1	8107	tcp	open
192.168.1.1	8108	tcp	open
192.168.1.1	8109	tcp	open
192.168.1.1	8110	tcp	open
192.168.1.1	8111	tcp	open
192.168.1.1	8112	tcp	open
192.168.1.1	8113	tcp	open
192.168.1.1	8114	tcp	open
192.168.1.1	8115	tcp	open
192.168.1.1	8116	tcp	open
192.168.1.1	8117	tcp	open
192.168.1.1	8118	tcp	open
192.168.1.1	8119	tcp	open
192.168.1.1	8120	tcp	open
192.168.1.1	8121	tcp	open
192.168.1.1	8122	tcp	open
192.168.1.1	8123	tcp	open
192.168.1.1	8124	tcp	open
192.168.1.1	8125	tcp	open
192.168.1.1	8126	tcp	open
192.168.1.1	8127	tcp	open
192.168.1.1	8128	tcp	open
192.168.1.1	8129	tcp	open
192.168.1.1	8130	tcp	open
192.168.1.1	8131	tcp	open
192.168.1.1	8132	tcp	open
192.168.1.1	8133	tcp	open
192.168.1.1	8134	tcp	open
192.168.1.1	8135	tcp	open
192.168.1.1	8136	tcp	open
192.168.1.1	8137	tcp	open
192.168.1.1	8138	tcp	open
192.168.1.1	8139	tcp	open
192.168.1.1	8140	tcp	open
192.168.1.1	8141	tcp	open
192.168.1.1	8142	tcp	open
192.168.1.1	8143	tcp	open
192.168.1.1	8144	tcp	open
192.168.1.1	8145	tcp	open
192.168.1.1	8146	tcp	open
192.168.1.1	8147	tcp	open
192.168.1.1	8148	tcp	open
192.168.1.1	8149	tcp	open
192.168.1.1	8150	tcp	open
192.168.1.1	8151	tcp	open
192.168.1.1	8152	tcp	open
192.168.1.1	8153	tcp	open
192.168.1.1	8154	tcp	open
192.168.1.1	8155	tcp	open
192.168.1.1	8156	tcp	open
192.168.1.1	8157	tcp	open
192.168.1.1	8158	tcp	open
192.168.1.1	8159	tcp	open
192.168.1.1	8160	tcp	open
192.168.1.1	8161	tcp	open
192.168.1.1	8162	tcp	open
192.168.1.1	8163	tcp	open
192.168.1.1	8164	tcp	open
192.168.1.1	8165	tcp	open
192.168.1.1	8166	tcp	open
192.168.1.1	8167	tcp	open
192.168.1.1	8168	tcp	open
192.168.1.1	8169	tcp	open
192.168.1.1	8170	tcp	open
192.168.1.1	8171	tcp	open
192.168.1.1	8172	tcp	open
192.168.1.1	8173	tcp	open
192.168.1.1	8174	tcp	open
192.168.1.1	8175	tcp	open
192.168.1.1	8176	tcp	open
192.168.1.1	8177	tcp	open
192.168.1.1	8178	tcp	open
192.168.1.1	8179	tcp	open
192.168.1.1	8180	tcp	open
192.168.1.1	8181	tcp	open
192.168.1.1	8182	tcp	open
192.168.1.1	8183	tcp	open
192.168.1.1	8184	tcp	open
192.168.1.1	8185	tcp	open
192.168.1.1	8186	tcp	open
192.168.1.1	8187	tcp	open
192.168.1.1	8188	tcp	open
192.168.1.1	8189	tcp	open
192.168.1.1	8190	tcp	open
192.168.1.1	8191	tcp	open
192.168.1.1	8192	tcp	open
192.168.1.1	8193	tcp	open
192.168.1.1	8194	tcp	open
192.168.1.1	8195	tcp	open
192.168.1.1	8196	tcp	open
192.168.1.1	8197	tcp	open
192.168.1.1	8198	tcp	open
192.168.1.1	8199	tcp	open
192.168.1.1	8200	tcp	open
192.168.1.1	8201	tcp	open
192.168.1.1	8202	tcp	open
192.168.1.1	8203	tcp	open
192.168.1.1	8204	tcp	open
192.168.1.1	8205	tcp	open
192.168.1.1	8206	tcp	open
192.168.1.1	8207	tcp	open
192.168.1.1	8208	tcp	open
192.168.1.1	8209	tcp	open
192.168.1.1	8210	tcp	open
192.168.1.1	8211	tcp	open
192.168.1.1	8212	tcp	open
192.168.1.1	8213	tcp	open
192.168.1.1	8214	tcp	open
192.168.1.1	8215	tcp	open
192.168.1.1	8216	tcp	open
192.168.1.1	8217	tcp	open
192.168.1.1	8218	tcp	open
192.168.1.1	8219	tcp	open
192.168.1.1	8220	tcp	open
192.168.1.1	8221	tcp	open
192.168.1.1	8222	tcp	open
192.168.1.1	8223	tcp	open
192.168.1.1	8224	tcp	open
192.168.1.1	8225	tcp	open
192.168.1.1	8226	tcp	open
192.168.1.1	8227	tcp	open
192.168.1.1	8228	tcp	open
192.168.1.1	8229	tcp	open
192.168.1.1	8230	tcp	open
192.168.1.1	8231	tcp	open
192.168.1.1	8232	tcp	open
192.168.1.1	8233	tcp	open
192.168.1.1	8234	tcp	open
192.168.1.1	8235	tcp	open
192.168.1.1	8236	tcp	open
192.168.1.1	8237	tcp	open
192.168.1.1	8238	tcp	open
192.168.1.1	8239	tcp	open
192.168.1.1	8240	tcp	open
192.168.1.1	8241	tcp	open
192.168.1.1	8242	tcp	open
192.168.1.1	8243	tcp	open
192.168.1.1	8244	tcp	open
192.168.1.1	8245	tcp	open
192.168.1.1	8246	tcp	open
192.168.1.1	8247	tcp	open
192.168.1.1	8248	tcp	open
192.168.1.1	8249	tcp	open
192.168.1.1	8250	tcp	open
192.168.1.1	8251	tcp	open
192.168.1.1	8252	tcp	open
192.168.1.1	8253	tcp	open
192.168.1.1	8254	tcp	open
192.168.1.1	8255	tcp	open
192.168.1.1	8256	tcp	open
192.168.1.1	8257	tcp	open
192.168.1.1	8258	tcp	open
192.168.1.1	8259	tcp	open
192.168.1.1	8260	tcp	open
192.168.1.1	8261	tcp	open
192.168.1.1	8262	tcp	open
192.168.1.1	8263	tcp	open
192.168.1.1	8264	tcp	open
192.168.1.1	8265	tcp	open
192.168.1.1	8266	tcp	open
192.168.1.1	8267	tcp	open
192.168.1.1	8268	tcp	open
192.168.1.1	8269	tcp	open
192.168.1.1	8270	tcp	open
192.168.1.1	8271	tcp	open
192.168.1.1	8272	tcp	open
192.168.1.1	8273	tcp	open
192.168.1.1	8274	tcp	open
192.168.1.1	8275	tcp	open
192.168.1.1	8276	tcp	open
192.168.1.1	8277	tcp	open
192.168.1.1	8278	tcp	open
192.168.1.1	8279	tcp	open
192.168.1.1	8280	tcp	open
192.168.1.1	8281	tcp	open
192.168.1.1	8282	tcp	open
192.168.1.1	8283	tcp	open
192.168.1.1	8284	tcp	open
192.168.1.1	8285	tcp	open
192.168.1.1	8286	tcp	open
192.168.1.1	8287	tcp	open
192.168.1.1	8288	tcp	open
192.168.1.1	8289	tcp	open
192.168.1.1	8290	tcp	open
192.168.1.1	8291	tcp	open
192.168.1.1	8292	tcp	open
192.168.1.1	8293	tcp	open
192.168.1.1	8294	tcp	open
192.168.1.1	8295	tcp	open
192.168.1.1	8296	tcp	open
192.168.1.1	8297	tcp	open
192.168.1.1	8298	tcp	open
192.168.1.1	8299	tcp	open
192.168.1.1	8300	tcp	open
192.168.1.1	8301	tcp	open
192.168.1.1	8302	tcp	open
192.168.1.1	8303	tcp	open
192.168.1.1	8304	tcp	open
192.168.1.1	8305	tcp	open
192.168.1.1	8306	tcp	open
192.168.1.1	8307	tcp	open
192.168.1.1	8308	tcp	open
192.168.1.1	8309	tcp	open
192.168.1.1	8310	tcp	open
192.168.1.1	8311	tcp	open
192.168.1.1	8312	tcp	open
192.168.1.1	8313	tcp	open
192.168.1.1	8314	tcp	open
192.168.1.1	8315	tcp	open
192.168.1.1	8316	tcp	open
192.168.1.1	8317	tcp	open
192.168.1.1	8318	tcp	open
192.168.1.1	8319	tcp	open
192.168.1.1	8320	tcp	open
192.168.1.1	8321	tcp	open
192.168.1.1	8322	tcp	open
192.168.1.1	8323	tcp	open
192.168.1.1	8324	tcp	open
192.168.1.1	8325	tcp	open
192.168.1.1	8326	tcp	open
192.168.1.1	8327	tcp	open
192.168.1.1	8328	tcp	open
192.168.1.1	8329	tcp	open
192.168.1.1	8330	tcp	open
192.168.1.1	8331	tcp	open
192.168.1.1	8332	tcp	open
192.168.1.1	8333	tcp	open
192.168.1.1	8334	tcp	open
192.168.1.1	8335	tcp	open
192.168.1.1	8336	tcp	open
192.168.1.1	8337	tcp	open
192.168.1.1	8338	tcp	open
192.168.1.1	8339	tcp	open
192.168.1.1	8340	tcp	open
192.168.1.1	8341	tcp	open
192.168.1.1	8342	tcp	open
192.168.1.1	8343	tcp	open
192.168.1.1	8344	tcp	open
192.168.1.1	8345	tcp	open
192.168.1.1	8346	tcp	open
192.168.1.1	8347	tcp	open
192.168.1.1	8348	tcp	open
192.168.1.1	8349	tcp	open
192.168.1.1	8350	tcp	open
192.168.1.1	8351	tcp	open
192.168.1.1	8352	tcp	open
192.168.1.1	8353	tcp	open
192.168.1.1	8354	tcp	open
192.168.1.1	8355	tcp	open
192.168.1.1	8356	tcp	open
192.168.1.1	8357	tcp	open
192.168.1.1	8358	tcp	open
192.168			

# 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](http://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.