# Modul 3: Linux for Ethical Hackers

Kuasai sistem operasi yang menjadi fondasi dunia keamanan siber. Dari navigasi terminal hingga manajemen jaringan — semua dimulai dari sini.

C-SIX SECURITY

EDY SUSANTO · FOUNDER

# Tujuan Pembelajaran

Setelah menyelesaikan modul ini, peserta akan memiliki pemahaman dan kemampuan praktis menggunakan Linux sebagai sistem operasi utama dalam kegiatan keamanan siber profesional.

### 🎯 Kompetensi Utama

Mengoperasikan Linux dengan percaya diri untuk tugas-tugas hacking dan security assessment.

### 🛠️ Keterampilan Praktis

Mampu menginstall, mengkonfigurasi, dan menggunakan Kali Linux di lingkungan nyata.

### 🔐 Fondasi Keamanan

Memahami struktur sistem, izin akses, dan jaringan sebagai dasar ethical hacking.

# Mengapa Linux untuk Ethical Hacking?

## Linux Mendominasi Dunia Security

Lebih dari **90% tools keamanan siber** dibangun dan dioptimalkan untuk Linux. Sistem operasi ini memberikan kontrol penuh terhadap proses, jaringan, dan sistem file — sesuatu yang sangat krusial dalam penetration testing.

## Keunggulan Linux untuk Hacker

- Open-source dan dapat dikustomisasi sepenuhnya
- Akses root penuh ke seluruh sistem
- Ribuan tools keamanan tersedia secara native
- Komunitas aktif dan dokumentasi lengkap
- Ringan, cepat, dan stabil untuk operasi panjang

# Mengenal Kali Linux

Kali Linux adalah distribusi Linux berbasis Debian yang dirancang khusus untuk penetration testing, digital forensics, dan keamanan siber. Dikembangkan dan dikelola oleh **Offensive Security**, Kali hadir dengan lebih dari 600 tools pre-installed siap pakai.

### Versi Terkini

Kali Rolling — selalu update dengan tools dan patch terbaru secara berkala.

### Mode Instalasi

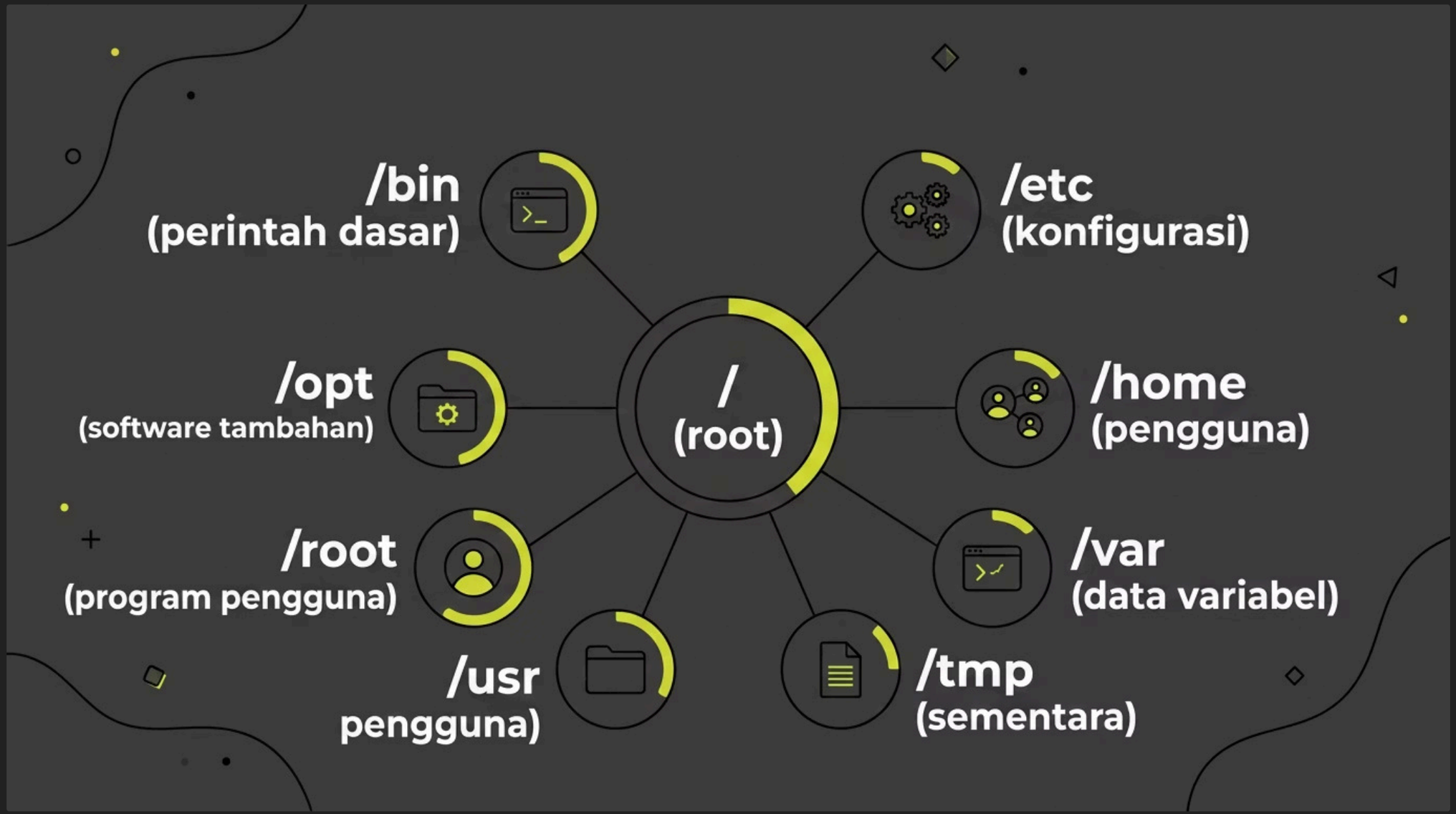
Live USB, Virtual Machine, WSL2 (Windows), atau instalasi langsung di bare metal.

### Default User

Sejak versi 2020, default user bukan lagi root — menerapkan prinsip least privilege.

# Struktur File Linux

Linux menggunakan sistem hierarki direktori tunggal yang dimulai dari root `/`. Memahami struktur ini adalah kunci navigasi dan operasi yang efektif di terminal.




Direktori seperti `/etc` menyimpan konfigurasi kritis, sementara `/var/log` menjadi target penting dalam analisis forensik dan log review.

# Perintah Dasar Linux

Menguasai perintah dasar adalah fondasi mutlak. Berikut adalah perintah-perintah esensial yang wajib dikuasai setiap ethical hacker sebelum melangkah ke tools yang lebih kompleks.

## 📁 Navigasi & File

```
ls -la       # daftar file lengkap
cd /path     # pindah direktori
pwd          # lokasi saat ini
cp src dst   # salin file
mv src dst   # pindah/rename
rm -rf dir   # hapus direktori
find / -name  # cari file
```

## 🔍 Proses & Sistem

```
ps aux # lihat proses
top / htop # monitor sistem
kill -9 PID # hentikan proses
whoami # identitas user
uname -a # info kernel
history # riwayat perintah
man [cmd] # manual perintah
```

# User dan Permission di Linux

Sistem permission Linux adalah lapisan keamanan yang sangat penting. Ethical hacker harus memahami bagaimana hak akses bekerja — baik untuk mengeksploitasi celah privilege escalation maupun mengamankan sistem.

### Format Permission: rwxrwxrwx

**r (read)** = 4, **w (write)** = 2, **x (execute)** = 1. Dibagi menjadi tiga grup: Owner | Group | Others. Contoh: `chmod 755 file.sh`

### Manajemen User

`adduser`, `passwd`, `usermod`, dan `deluser` untuk mengelola akun. File `/etc/passwd` dan `/etc/shadow` menyimpan data user dan hash password.

### Privilege Escalation

Perintah `sudo` memberikan akses root sementara. Konfigurasi `/etc/sudoers` menentukan siapa yang boleh menggunakan sudo — target umum dalam privilege escalation assessment.

# Networking di Linux

Linux menyediakan toolkit jaringan yang sangat powerful — menjadikannya platform ideal untuk network reconnaissance, traffic analysis, dan uji penetrasi jaringan.

## Konfigurasi Interface

`ip addr`, `ip link`, `ifconfig` — melihat dan mengatur interface jaringan aktif.

## Konektivitas & Routing

`ping`, `traceroute`, `netstat -tulnp`, `ss` — memetakan jalur dan koneksi aktif.

## DNS & Transfer Data

`nslookup`, `dig`, `curl`, `wget` — resolusi nama domain dan transfer data dari command line.

## Network Capture

`tcpdump` dan `Wireshark` untuk menangkap dan menganalisis paket jaringan secara real-time.

# Package Management

Kali Linux menggunakan sistem paket APT (Advanced Package Tool) berbasis Debian. Menguasai manajemen paket memungkinkan ethical hacker menginstall, memperbarui, dan mengelola tools dengan cepat dan efisien.

01

## Update Repository

`sudo apt update` — memperbarui daftar paket dari semua repository yang dikonfigurasi di `/etc/apt/sources.list`.

02

## Upgrade Sistem

`sudo apt upgrade` atau `apt full-upgrade` — memperbarui semua paket yang terinstall ke versi terbaru.

03

## Instalasi Tools

`sudo apt install [nama-paket]` — menginstall tools baru. Contoh: `apt install nmap metasploit-framework`.

04

## Pencarian Paket

`apt search [keyword]` dan `apt-cache show [paket]` — menemukan dan membaca detail paket sebelum diinstall.

# Bash Scripting Basics

Bash scripting mengotomatisasi tugas berulang dalam keamanan siber — mulai dari scanning otomatis, log parsing, hingga pembuatan report. Ini adalah keterampilan yang membedakan ethical hacker biasa dengan yang profesional.

## Struktur Dasar Script

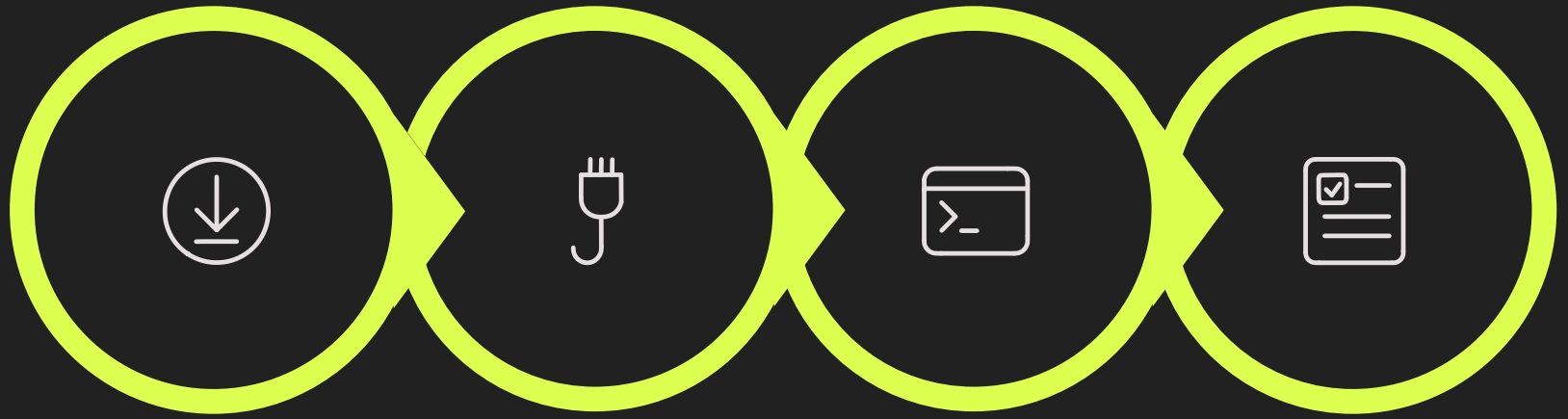
```
#!/bin/bash
# Komentar script
NAME="Kali"
echo "Hello, $NAME!"
if [ "$NAME" == "Kali" ]; then
  echo "Sistem siap!"
fi
for i in {1..5}; do
  echo "Loop ke-$i"
done
```

## Konsep Penting Bash

- **Shebang** `#!/bin/bash` — mendefinisikan interpreter
- **Variabel** — menyimpan dan memanipulasi data
- **Kondisional** if/else — logika pengambilan keputusan
- **Loop** for/while — iterasi dan automasi
- **Pipe** `|` dan **redirect** `>` — alur data antar perintah
- **Chmod +x** — memberikan izin eksekusi pada script

# Praktik: Instalasi & Navigasi Kali Linux

Praktik langsung adalah cara terbaik untuk menguasai Linux. Berikut adalah alur praktik yang harus diselesaikan dalam sesi ini.




Pastikan setiap langkah berhasil sebelum melanjutkan ke tahap berikutnya. Dokumentasikan setiap perintah yang digunakan sebagai catatan belajar.

# Praktik Lanjutan: Network Troubleshooting

1

## Identifikasi Interface

Jalankan `ip addr show` dan catat nama interface aktif (eth0, wlan0). Cek status UP/DOWN dan alamat IP yang terdapat pada setiap interface.

2

## Test Konektivitas

Gunakan `ping 8.8.8.8` untuk test koneksi internet dan `ping [gateway]` untuk test koneksi lokal. Analisis packet loss dan response time.

3

## Analisis Port & Layanan

Jalankan `netstat -tulnp` atau `ss -tulnp` untuk melihat port yang terbuka dan layanan yang berjalan di sistem target lokal.

# Rangkuman & Outcome Modul 3

Selamat! Dengan menyelesaikan Modul 3, Anda telah membangun fondasi Linux yang kuat sebagai ethical hacker. Kemampuan ini akan menjadi tulang punggung seluruh aktivitas keamanan siber Anda ke depan.

## Terminal Proficient

Navigasi dan operasi file via command line dengan percaya diri dan efisien.

## Security Mindset

Memahami permission, user management, dan implikasinya terhadap keamanan sistem.

## Network Ready

Mampu mengkonfigurasi, menganalisis, dan melakukan troubleshooting jaringan dari terminal.

## Automation Capable

Menulis Bash script dasar untuk mengotomatisasi tugas keamanan yang berulang.

EDY SUSANTO · FOUNDER C-SIX SECURITY