#linux/basics

KSL Dragon Learning Path: Dari Pengguna Biasa Menjadi Ahli Sistem Linux

Selamat datang di jalur pembelajaran yang dirancang khusus oleh untuk mengubah Anda dari seorang pemula menjadi seorang profesional yang mahir dalam ekosistem Linux. Learning path ini terdiri dari tiga kursus berjenjang yang akan membangun fondasi pengetahuan Anda secara sistematis dan praktis.

1. Linux Basics: Memulai perjalanan Anda dengan pengenalan fundamental.
2. System Administration with Linux: Mengaplikasikan pengetahuan dasar untuk mengelola sistem secara efektif.
3. Linux Security & Hardening: Membangun benteng pertahanan yang kuat pada sistem Linux.
4. Introduction to Ethical Hacking with Linux: Belajar bagaimana seorang penyerang melakukan penyerangan terhadap suatu sistem.

Linux Basics - Fondasi Menguasai Sistem Operasi Open-Source

Deskripsi Kursus

Kursus "Linux Basics" adalah gerbang utama Anda untuk memasuki dunia Linux. Dirancang untuk pemula absolut, kursus ini akan membongkar mitos bahwa Linux itu sulit dan hanya untuk para *geek*. Di sini, Anda akan mempelajari filosofi di balik Linux, memahami strukturnya, dan yang terpenting, menjadi terbiasa dengan antarmuka baris perintah (*Command Line Interface* - CLI) yang merupakan jantung dari sistem operasi ini. Setelah menyelesaikan kursus ini, Anda tidak hanya akan mampu menggunakan Linux untuk kegiatan sehari-hari, tetapi juga memiliki fondasi yang kokoh untuk melanjutkan ke topik yang lebih lanjut seperti administrasi sistem dan keamanan siber.

Target Audiens

- Mahasiswa atau individu yang belum pernah menggunakan Linux.
- Pengguna Windows atau macOS yang ingin beralih atau mempelajari sistem operasi baru.
- Calon sysadmin, developer, atau praktisi Cyber Security.

Outline Materi & Learning Path

- Section 1: Pengenalan Dunia Linux
  - Materi: Apa itu Linux? Sejarah, Filosofi Open-Source, dan Perbedaan antara Kernel dan Distribusi (Distro).
  - Tujuan: Memahami konsep dasar dan posisi Linux dalam dunia teknologi.
- Section 2: Instalasi dan Konfigurasi Awal
  - Materi: Memilih Distro yang Tepat, Instalasi via Virtual Machine vs. Dual Boot, dan Tour Antarmuka Desktop.
  - Tujuan: Mampu melakukan instalasi sistem operasi Linux secara mandiri di lingkungan yang aman.
- Section 3: Menguasai Terminal: Jantungnya Linux
  - Materi: Navigasi Sistem File (`ls`, `cd`, `pwd`), Manipulasi File dan Direktori (`mkdir`, `cp`, `mv`, `rm`), dan Membaca Konten File (`cat`, `less`, `nano`, `vim`).

    - Tujuan: Menjadi familiar dan efisien dalam menggunakan terminal untuk tugas-tugas dasar.
- Section 4: Manajemen Pengguna dan Hak Akses
    - Materi: Konsep *User* vs. *Root*, Perintah `sudo`, dan Memahami Hak Akses File (`chmod`, `chown`).
    - Tujuan: Memahami model keamanan fundamental di Linux dan cara mengelola izin akses.
- Section 5: Manajemen Software (Package Management)
    - Materi: Pengenalan `APT` (Advanced Package Tool), Mencari, Menginstal, dan Menghapus Aplikasi dari Terminal.
    - Tujuan: Mampu mengelola perangkat lunak pada sistem secara mandiri dan aman.
- Section 6: Proses dan Jaringan Dasar
    - Materi: Memonitor Proses yang Berjalan (`ps`, `htop`), dan Perintah Jaringan Dasar (`ip`, `ping`).
    - Tujuan: Mendapatkan pemahaman awal tentang apa yang terjadi "di balik layar" sistem.

System Administration with Linux

Deskripsi Kursus

Kursus "System Administration with Linux" akan membawa pengetahuan dasar Anda dan mengaplikasikannya dalam skenario dunia nyata untuk mengelola, meng-konfigurasi, dan memelihara server atau sistem Linux. Anda akan belajar praktik terbaik dalam administrasi sistem, mulai dari skrip otomatisasi, manajemen layanan, hingga pemantauan kinerja. Kursus ini bersifat sangat praktis dan akan membekali Anda dengan keterampilan yang dibutuhkan untuk menjadi seorang *System Administrator* (SysAdmin) yang handal.

Target Audiens

- Lulusan kursus "Linux Basics" atau individu dengan pemahaman dasar Linux.
- Mahasiswa yang tertarik pada infrastruktur IT dan manajemen server.

- Pengembang yang ingin mengelola lingkungan *deployment* mereka sendiri.

Outline Materi & Learning Path

- Section 1: Automasi Tugas dengan Bash Scripting
  - Materi: Pengenalan Shell Scripting (*bash*), Variabel, *Conditional Statements* (`if-else`), dan *Loops* (`for`, `while`).
  - Tujuan: Mampu mengotomatisasi tugas-tugas repetitif untuk meningkatkan efisiensi.
- Section 2: Manajemen Layanan dan Proses Tingkat Lanjut
  - Materi: Pengenalan `systemd`, Mengelola *Services* dengan `systemctl` (`start`, `stop`, `enable`), dan penjadwalan tugas dengan `cron`.
  - Tujuan: Mampu mengontrol layanan yang berjalan di sistem dan menjadwalkan eksekusi tugas secara otomatis.
- Section 3: Manajemen Penyimpanan (Storage)
  - Materi: Memahami Partisi Disk, *Logical Volume Management* (LVM), dan melakukan *backup* dan *restore* data.
  - Tujuan: Mampu mengelola ruang penyimpanan pada sistem secara efektif dan aman.
- Section 4: Konfigurasi Jaringan Tingkat Lanjut
  - Materi: Konfigurasi Alamat IP Statis, Pengenalan *Firewall* dengan `UFW`, dan Konfigurasi Dasar SSH.
  - Tujuan: Mampu mengamankan dan mengonfigurasi konektivitas jaringan pada server.
- Section 5: Pemantauan dan Analisis Kinerja
  - Materi: Menganalisis Penggunaan CPU, Memori, dan Disk, serta Membaca dan Memahami *Log* Sistem.
  - Tujuan: Mampu mendiagnosis masalah kinerja dan melakukan *troubleshooting* dasar.

Linux Security & Hardening

Deskripsi Kursus

Kursus "Linux Security & Hardening" akan mengubah cara pandang Anda dari seorang administrator sistem menjadi seorang penjaga benteng digital. Di sini, kita tidak hanya akan belajar

mengelola sistem, tetapi juga memperkuat, mengamankan, dan memantau sistem Linux dari berbagai potensi ancaman. Anda akan mempelajari praktik-praktik terbaik untuk mengurangi celah keamanan (*attack surface*), mengonfigurasi pertahanan berlapis, dan mendeteksi aktivitas mencurigakan. Kursus ini adalah fondasi esensial bagi siapa pun yang serius ingin melindungi infrastruktur digital.

Target Audiens

- Lulusan kursus "System Administration with Linux".
- Calon *System Administrator*, *DevOps Engineer*, atau *Cyber Security Analyst* (Blue Team).
- Siapa saja yang bertanggung jawab atas server atau sistem Linux yang terhubung ke jaringan.

Outline Materi & Learning Path

- Section 1: Prinsip Keamanan & Model Ancaman
  - Materi: CIA Triad (*Confidentiality, Integrity, Availability*), Prinsip *Least Privilege*, dan Konsep *Defense in Depth*.
  - Tujuan: Membangun kerangka berpikir (*mindset*) keamanan yang solid.
- Section 2: System Hardening Tingkat Lanjut
  - Materi: Mengamankan Layanan SSH (*Key-based authentication, disable root login*), Konfigurasi Firewall dengan `UFW` / `firewalld`, Manajemen *Patch* Keamanan, dan Audit Konfigurasi Dasar.
  - Tujuan: Mampu "mengunci" titik-titik masuk paling umum pada sistem Linux.
- Section 3: Audit & Pemantauan Sistem
  - Materi: Menganalisis *Log* Sistem (`/var/log`), Pengenalan *tools* seperti `fail2ban` untuk proteksi otomatis, dan Memonitor koneksi jaringan aktif dengan `ss` atau `netstat`.
  - Tujuan: Mampu mendeteksi dan merespons anomali atau upaya serangan secara proaktif.
- Section 4: Manajemen Izin Akses Tingkat Lanjut
  - Materi: Memahami *Special Permissions* (SUID, GUID, Sticky Bit), dan Pengenalan *Access Control Lists* (ACL).
  - Tujuan: Mampu menerapkan kontrol akses yang lebih granular dan kompleks pada file dan direktori.

- Section 5: Pengintaian Defensif
  - Materi: Menggunakan `nmap` pada sistem sendiri untuk melihat "apa yang terlihat oleh penyerang", dan memahami *output* dari *tools* pemindaian keamanan.
  - Tujuan: Mampu melihat sistem dari perspektif penyerang untuk menemukan dan memperbaiki kelemahan.

Introduction to Ethical Hacking with Linux

Deskripsi Kursus

Untuk mengalahkan seorang penyerang, Anda harus berpikir seperti mereka. Kursus "Introduction to Ethical Hacking with Linux" adalah langkah pertama Anda memasuki dunia *offensive security*. Di sini, Anda akan belajar metodologi dan menggunakan *tools* standar industri yang dijalankan di atas Linux untuk mengidentifikasi dan mengeksploitasi kerentanan secara etis dan bertanggung jawab. Dari pengumpulan informasi hingga eksploitasi dasar, kursus ini akan membekali Anda dengan pola pikir seorang *pentester*, di mana setiap sistem adalah teka-teki yang menunggu untuk dipecahkan.

Target Audiens

- Lulusan kursus "Linux Security & Hardening".
- Mahasiswa yang tertarik pada karir *Penetration Testing* atau *Red Teaming*.
- Administrator sistem yang ingin memahami metode serangan secara praktis.

Outline Materi & Learning Path

- Section 1: Etika Hacking & Metodologi
  - Materi: Aturan hukum dan etika dalam *pentesting*, perbedaan *White/Gray/Black Hat*, dan pengenalan fase-fase *penetration testing* (*Reconnaissance, Scanning, Exploitation, Post-Exploitation, Reporting*).

    - Tujuan: Memahami batasan legal dan etis serta alur kerja standar seorang *pentester*.
- Section 2: Pengumpulan Informasi (*Reconnaissance*)
    - Materi: Teknik *Passive Reconnaissance* (`whois`, `nslookup`) dan *Active Reconnaissance* menggunakan `nmap` untuk pemindaian port dan identifikasi layanan.
    - Tujuan: Mampu mengumpulkan informasi awal sebanyak mungkin tentang sistem target.
- Section 3: Pemindaian Kerentanan (*Vulnerability Scanning*)
    - Materi: Menggunakan *script* pada `nmap` (*Nmap Scripting Engine* - NSE) untuk mencari kerentanan umum dan pengenalan *tools* pemindaian otomatis seperti `Nikto` untuk web server.
    - Tujuan: Mampu menemukan potensi celah keamanan berdasarkan layanan dan versi perangkat lunak yang berjalan.
- Section 4: Eksploitasi Dasar
    - Materi: Pengenalan konsep *exploit* dan *payload*. Praktik eksploitasi pada lingkungan lab yang aman, menargetkan miskonfigurasi umum atau kerentanan yang sudah diketahui (misalnya, pada aplikasi web sederhana).
    - Tujuan: Memahami mekanisme dasar bagaimana sebuah kerentanan dapat dieksploitasi untuk mendapatkan akses.
- Section 5: Post-Exploitation & Reporting
    - Materi: Pengenalan konsep *privilege escalation* (dari *user* biasa menjadi *root*), navigasi sistem target, dan yang terpenting: cara membuat laporan temuan yang jelas dan profesional.
    - Tujuan: Memahami apa yang harus dilakukan setelah berhasil mendapatkan akses dan bagaimana cara melaporkan temuan secara efektif.