**LAPORAN PRAKTIKUM**

**SISTEM OPERASI**



Modul 5

Asfal Fuad

240306031

Program Studi Teknologi Informasi

Fakultas Dakwah dan Ilmu Komunikasi

Universitas Islam Negeri Mataram

2025

|  |  |
| --- | --- |
| Pertemuan | 5 |
| Topik | Jaringan dan Keamanan Sistem Operasi Linux |
| Repository | - |
| Tanggal | - |

1. Tujuan

Tujuan praktikum Jaringan dan Keamanan Sistem Operasi Linux:

* 1. Memahami konfigurasi jaringan pada VirtualBox.
  2. Menganalisis konektivitas jaringan menggunakan perintah CLI.
  3. Mengakses sistem Linux melalui SSH dan mentransfer file.
  4. Menghubungkan PC dalam jaringan lokal menggunakan SSH.
  5. Mengelola firewall menggunakan UFW dan iptables.
  6. Mengelola user dan grup untuk keamanan sistem.

1. Requirement

1.      Sistem Operasi yang digunakan           : Ubuntu LTS 24.0.1

2.      Browser                                                : Google Version129.0.6668.10

3.      Tools yang digunakan                             : Virtualbox

1. Dasar Teori
2. Konfigurasi Jaringan VirtualBox

Dalam praktik jaringan menggunakan mesin virtual, VirtualBox menyediakan beberapa jenis konfigurasi jaringan yang penting untuk dipahami. Tiga jenis yang paling umum adalah NAT, Bridged Adapter, dan Host-Only Adapter. NAT (*Network Address Translation*) memungkinkan mesin virtual mengakses internet melalui IP dari host, namun tidak memungkinkan akses dari luar ke mesin virtual. Bridged Adapter membuat mesin virtual terhubung langsung ke jaringan fisik host, sehingga dapat menerima IP dari router yang sama dengan host dan berkomunikasi dengan perangkat lain dalam jaringan. Sementara itu, Host-Only Adapter menciptakan jaringan lokal antara host dan mesin virtual, tanpa akses ke jaringan eksternal, cocok untuk pengujian internal.

Perbedaan dari ketiga mode jaringan NAT, Bridged Adapter, dan Host-Only





1. Perintah CLI (*Commend Line Intraface*) untuk Menganalisis Konektivitas Jaringan

Linux menyediakan berbagai perintah baris (CLI) untuk mengecek dan menganalisis koneksi jaringan. Perintah `ping` digunakan untuk memeriksa apakah suatu alamat IP dapat dijangkau. `ip a` digunakan untuk melihat konfigurasi antarmuka jaringan. `ip route` menunjukkan rute lalu lintas jaringan yang digunakan sistem. `netstat` dan `ss` digunakan untuk melihat port yang sedang digunakan dan status koneksi. Penggunaan perintah-perintah ini sangat penting dalam diagnosis dan pemantauan jaringan.

1. Akses Sistem Linux melalui SSH dan Transfer File

SSH (*Secure Shell*) adalah protokol yang digunakan untuk mengakses sistem Linux secara jarak jauh dengan aman melalui jaringan. SSH mengenkripsi koneksi agar data yang ditransmisikan tidak mudah disadap. Perintah `ssh user@ip\_address` digunakan untuk masuk ke sistem remote. Selain itu, SSH juga memungkinkan transfer file menggunakan perintah `scp` dan `rsync`. `scp` digunakan untuk menyalin file antar komputer melalui SSH, sedangkan `rsync` memungkinkan sinkronisasi direktori antar sistem dengan efisiensi tinggi karena hanya bagian file yang berubah yang ditransfer.

1. Koneksi Antar-PC di Jaringan Lokal

Dalam jaringan lokal, dua atau lebih komputer dapat saling terhubung dan bertukar data selama berada dalam satu jaringan dan memiliki alamat IP yang sesuai dalam satu subnet. Untuk koneksi antar-PC, biasanya cukup mengatur alamat IP statis atau DHCP dan memastikan tidak ada firewall yang menghalangi. Pada simulasi dengan mesin virtual, koneksi ini dapat dilakukan dengan Host-Only atau Bridged Adapter agar mesin virtual dapat “melihat” dan berinteraksi satu sama lain.

1. Manajemen Firewall dengan UFW dan iptables

Linux memiliki sistem firewall untuk membatasi lalu lintas jaringan yang masuk dan keluar. `ufw` (*Uncomplicated Firewall*) merupakan antarmuka yang mempermudah pengguna dalam mengelola aturan firewall. Contohnya, `ufw allow 22` membuka akses ke port 22 untuk SSH. Untuk konfigurasi lebih kompleks, digunakan `iptables`, yang memungkinkan penyaringan paket berdasarkan berbagai parameter seperti alamat IP, port, dan protokol. Firewall penting digunakan untuk mencegah akses tidak sah dan serangan dari luar.

1. Manajemen User dan Grup dalam Keamanan Sistem

Keamanan sistem Linux juga melibatkan pengelolaan user dan grup. Setiap user memiliki ID unik dan hak akses terhadap file serta direktori tertentu. Administrator dapat menambahkan pengguna dengan `adduser`, menghapus dengan `deluser`, serta mengelola grup dengan `groupadd`. Hak akses dapat dibatasi dengan mengatur izin file atau direktori, sehingga hanya pengguna yang berwenang yang dapat mengakses atau memodifikasi data. Pengaturan ini merupakan bagian penting dari kebijakan keamanan sistem untuk mencegah pelanggaran akses dan kebocoran data.









































