MODUL 9

MONITORING JARINGAN MENGGUNAKAN *WIRESHARK*

9.1 Tujuan Praktikum

1. Dapat mengenal dan memahami penggunaan *Wireshark* dalam menganalisis Jaringan.
2. Mengetahui model OSI dan masing-masing lapisan dalam komunikasi jaringan.
3. Mempelajari konsep *packet sniffing* dan cara kerjanya.
4. Menjelaskan manfaat dari monitoring jaringan bagi administrator jaringan.

9.2 Alat dan Bahan

1. Laptop
2. *Wireshark*

9.3 Dasar Teori

9.3.1 Wireshark

Wireshark adalah aplikasi *open-source* yang digunakan untuk menangkap dan menghasilkan paket data dalam jaringan komputer. Dengan *Wireshark*, pengguna dapat melihat isi setiap paket berdasarkan *protocol* jaringan yang digunakan. Program ini berguna dalam *troubleshooting* jaringan, analisis keamanan, dan pembelajaran protokol.

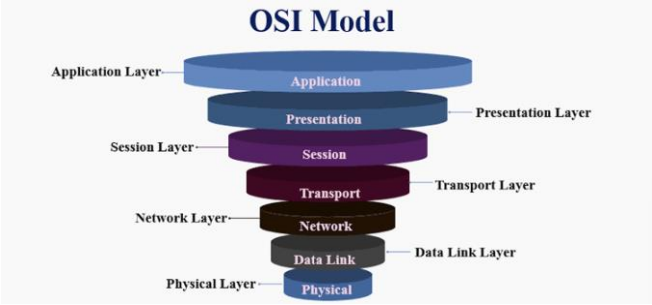
Tujuan dan manfaat *Wireshark* dari penggunaan aplikasi *Wireshark* ini yaitu sebagai berikut:

a) Menangkap informasi atau data paket yang dikirim dan diterima dalam jaringan komputer.
b) Mengetahui aktifitas yang terjadi dalam jaringan komputer.

c) Mengetahui dan menganalisa kinerja jaringan komputer yang dimiliki seperti kecepatan akses/*share* data dan koneksi jaringan ke internet.

d) Mengamati keamanan dari jaringan komputer. Kegunaan *Wireshark*, beberapa kegunaan *Wireshark* diantaranya, *Wireshark* digunakan oleh seorang *network* administrator untuk menganalisis lalu lintas dalam jaringannya. *Wireshark* dapat mengambil paket data ataupun informasi yang sedang terjadi di dalam sebuah jaringan dan semua jenis informasi yang diperoleh ini bisa dengan mudah untuk dianalisis, dalah satu caranya menggunakan *sniffing*, dengan menggunakan *sniffing* maka memungkinkan untuk memperoleh informasi prnting seperti *username* dan *password* yang ada di dalam jaringan.

9.3.2 Model OSI dan Pengertian Masing-masing Lapisan



Model OSI *(Open Systems Interconnection)* adalah kerangka konseptual yang menggambarkan fungsi komunikasi jaringan komputer dalam tujuh lapisan:

1. *Physical Layer:* Media transmisi fisik (kabel, sinyal).
2. *Data Link Layer:* Pengalamatan fisik dan deteksi kesalahan (MAC).
3. *Network Layer:* Pengalamatan logis dan *routing* (IP).
4. *Transport Layer:* Komunikasi *end-to-end* dan keandalan data (TCP/UDP).
5. *Session Layer:* Mengelola sesi komunikasi.
6. *Presentation Layer:* Penerjemah format data dan enkripsi.
7. *Application Layer:* Antarmuka langsung ke aplikasi pengguna (HTTP. FTP, DNS).

9.3.3 *Packet Sniffing*

Packet Snifiing adalah metode untuk menangkap dan merekam paket data yang sedang dikirimkan dalam suatu jaringan. Aktivitas ini dilakukan menggunakan perangkat lunak seperti *Wireshark* untuk memantau lalu lintas dan mengidentifikasi masalah atau proteksi ancaman. Dampak negatif dari *sniffing* adalah seseorang bisa melihat informasi rahasia milik orang lain yang terhubung ke jaaringan contohnya adalah *username* dan *password.* Dampak baik dari *sniffing* jaringan adalah untuk menganalisa paket data yang melewati jaringan sehingga jaringan dapat lebih optimal, menganalisa data apaakah mempengaruhi performa jaringan atau tidak, dan dapat mengetahui bila ada pihak asing yang menyusup kedalam jaringan.

9.3.4 Manfaat Monitoring Jaringan

Monitoring jaringan sangat penting dalam manajemen jaringan modern, di antaranya:

1. Mendeteksi gangguan dan potensi serangan.
2. Meningkatkan efisiensi jaringan.
3. Menyediakan data historis untuk *troubleshooting.*
4. Mendeteksi *bottleneck* dan penggunaan *bandwidth* tidak wajar.
5. Memastikan kepatuhan terhadap kebijakan kemanan performa.