ANALISIS SERANGAN SNIFFING & MITIGASINYA DI WIRESHARK

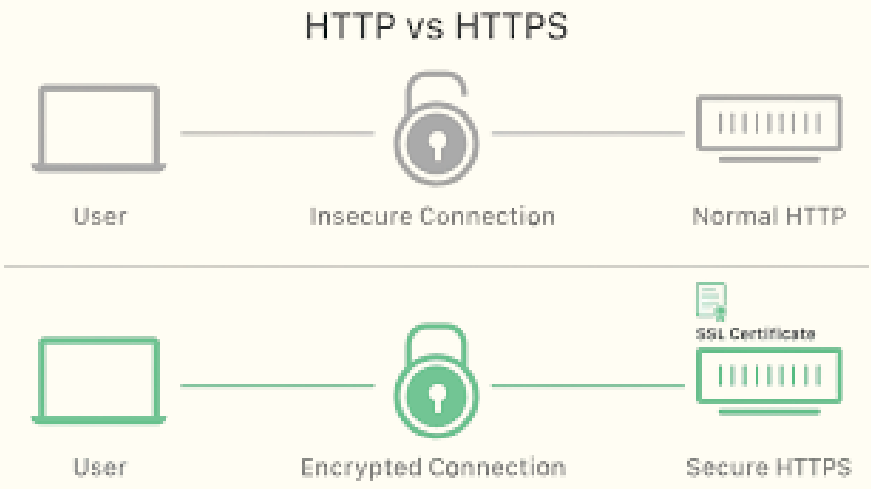
ANCAMAN KEAMANAN

- Penyadapan Data
- Metode Pencegahannya

TUJUAN PROYEK

- Memahami Paket Sniffing
- Metode Pencegahannya

Perbedaan HTTP DAN HTTPS



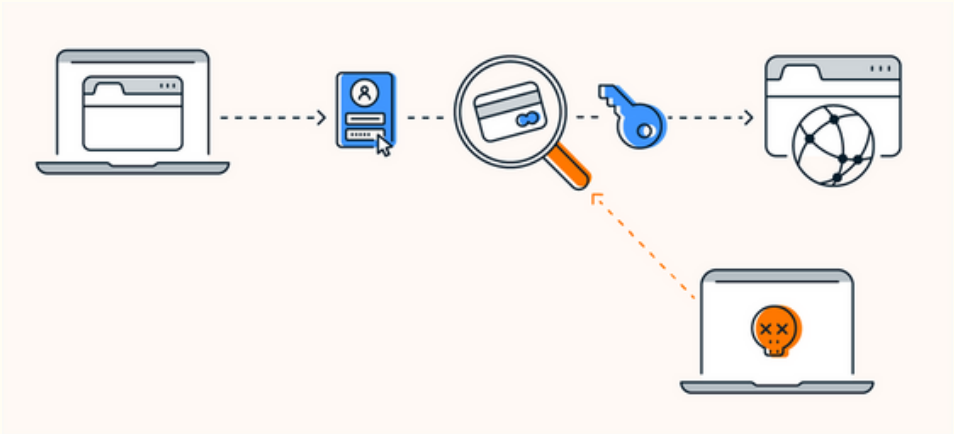
HTTP (HyperText Transfer Protocol)

- Data dikirim tanpa enkripsi
- Informasi dapat dibaca secara langsung
- Rentan terhadap serangan packet sniffing
- Tidak aman untuk pertukaran data sensitif

HTTPS (HyperText Transfer Protocol Secure)

- Data dikirim menggunakan enkripsi TLS/SSL
- Informasi tidak dapat dibaca oleh pihak ketiga
- Melindungi dari packet sniffing
- Aman untuk autentikasi dan pertukaran data

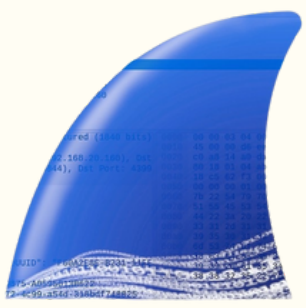
PAKET SNIFFING



Packet sniffing adalah teknik penyadapan lalu lintas jaringan dengan cara menangkap paket data yang dikirim antar perangkat. Serangan ini memanfaatkan jaringan yang tidak terenkripsi untuk membaca informasi yang dikirim, seperti username, password, atau data sensitif lainnya.

Packet sniffing dapat dilakukan secara pasif maupun aktif dan sering terjadi pada jaringan publik atau jaringan yang keamanannya lemah.

Wireshark



Wireshark adalah perangkat lunak network protocol analyzer yang digunakan untuk menangkap dan menganalisis paket data yang melewati suatu jaringan.

Pada proyek ini, Wireshark dimanfaatkan untuk mengamati lalu lintas HTTP dan HTTPS guna mengidentifikasi potensi serangan packet sniffing serta mengevaluasi efektivitas metode mitigasi keamanan.