BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis keamanan jaringan wifi terhadap serangan sniffing pada YAMAHA, PT ALFA SCORPII Tembesi , dapat disimpulkan sebagai berikut;

1. Keamanan YAMAHA, PT ALFA SCORPII Tembesi memerlukan peningkatan, terutama terkait akses domain name *server* (DNS) dan informasi lainnya. Selain itu, masih banyak pengguna jaringan internet yang kurang familiar dengan istilah *sniffing* pada jaringan komputer.
2. Alamat *website* pada YAMAHA, PT ALFA SCORPII Tembesi tidak aman karena masalah keamanan kuki (*cookie*): Kuki adalah file kecil yang dikirim oleh server web dan disimpan di browser pengguna. Umumnya digunakan untuk menyimpan informasi otentikasi dan sesi. Ketika kuki dikirim melalui protokol HTTP, dapat mudah dicuri dan digunakan oleh pihak yang tidak berwenang untuk mengakses akun pengguna atau mencuri informasi sensitif.

5.2 Saran

Jika Anda hendak menganalisis hasil capture pada protokol *HTTP* dan *HTTPS*, berikut adalah beberapa saran yang dapat membantu:

1. Gunakan Alat *Capture*:Gunakan alat seperti Wireshark atau Fiddler untuk melakukan capture dan analisis lalu lintas jaringan. Alat ini mampu merekam dan menganalisis paket-paket data yang dikirim melalui koneksi *HTTP* dan *HTTPS.*
2. Perhatikan Keamanan:Saat menganalisis hasil capture, berfokus pada keamanan data yang terlibat. Apabila Anda sedang meninjau hasil capture pada koneksi *HTTPS*, pastikan untuk tidak mengungkapkan informasi sensitif, seperti kata sandi atau data pribadi pengguna.
3. Analisis *Header:* Amati header pada paket data yang tercatat. Header pada protokol *HTTP* dan *HTTPS* dapat memberikan informasi penting mengenai permintaan dan respons yang terjadi antara klien dan *server*.
4. Fokus pada *Payload:* Jika memungkinkan, berfokus pada payload (isi) dari paket data yang direkam. Pada protokol *HTTP*, payload dapat berisi data yang dikirim atau diterima oleh aplikasi. Meskipun payload pada protokol *HTTPS* umumnya terenkripsi, analisis header dan metode permintaan/respons dapat memberikan wawasan tambahan.
5. Perhatikan Perbedaan Keamanan:Saat membandingkan hasil capture antara protokol *HTTP* dan *HTTPS*, perhatikan perbedaan keamanan yang terkait. Pada koneksi *HTTP*, data dapat terlihat dan rentan terhadap serangan seperti

pemantauan lalu lintas atau serangan Man-in-the-Middle. Pada koneksi *HTTPS*, data terenkripsi dan lebih aman dari serangan-serangan tersebut.

6. Pelajari Spesifikasi Protokol: Untuk analisis yang lebih mendalam, pelajari spesifikasi protokol *HTTP* dan *HTTPS*. Pemahaman terhadap cara kerja protokol akan membantu Anda menginterpretasikan hasil capture dengan lebih baik.
7. Manfaatkan Sumber Daya dan Dokumentasi : Gunakan sumber daya online, forum, dan dokumentasi terkait untuk mendapatkan wawasan tambahan mengenai analisis hasil capture pada protokol *HTTP* dan *HTTPS*. Ada banyak sumber daya yang dapat membantu meningkatkan pemahaman Anda terkait topik ini.

Selalu ingat untuk menjaga privasi dan keamanan data saat melakukan analisis hasil capture, terutama jika data yang Anda peroleh mengandung informasi sensitif.