Analisis File PCAP unntuk Menemukan Username dan Password Menggunakan Wireshark

- Tujuan analisis ini adalah untuk mencari dan mengidentifikasi *username* dan *password* yang terkirim melalui jaringan dalam file PCAP menggunakan Wireshark.
- Alat dan Bahan :
  - Aplikasi Wireshark
  - File PCAP dari LMS
  - Laptop
- Langkah – langkah Analisis
  - Membuka File PCAP di wireshark
  - Menyaring traffic yang berpotensi membawa username/password menggunakan filter (http.request.method ==”POST”)
  - Pilih pake POST yang mencurigakan
  - Scroll ke bagian Hypertext Transfer Protocol
  - Buka bagian HTML From URL Encoded
  - Pada paket Nomor 102 ditemukan
    Username = “admin”
    Password = “password”
    Login = “Login”
    User token ="50133d1123f960bb58f29afad28fc463"
  - Pada paket Nomor 256 ditemukan
    Username = “gordonb”
    Password = “abc123”
    Login = “Login”
    User token = "c3019b9aa6e1d5d2e185782f128f4e7c"
  - Pada paket Nomor 499 ditemukan
    Username = “pablo”
    Password = “letmein”
    Login = “Login”
    User token = "3b529b1d260fa34ee1d9ac15cddf7a92"
- Username dan password dapat terlihat dengan jelas pada paket HTTP POST karena proses pengiriman data dilakukan melalui protokol **HTTP**, yang merupakan protokol *unencrypted* atau tidak terenkripsi. Pada protokol ini, seluruh data yang dikirimkan, termasuk informasi sensitif seperti kredensial login, ditransmisikan dalam bentuk teks biasa (*plain text*). Akibatnya, data tersebut dapat dengan mudah ditangkap dan dibaca menggunakan tools seperti Wireshark. Berbeda dengan HTTPS yang menggunakan enkripsi SSL/TLS untuk melindungi data selama proses transmisi, HTTP tidak menyediakan perlindungan terhadap penyadapan (*sniffing*). Hal inilah yang menyebabkan username dan password pada file PCAP dapat ditemukan dengan jelas pada bagian *HTML Form URL Encoded*.