Unit 3
Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark

A. Tujuan

- Merekam dan menganalisis trafik http
- Merekam dan menganalisis trafik https

B. Latar Belakang

HyperText Transfer Protocol (HTTP) adalah protokol lapisan aplikasi yang menyajikan data melalui browser web. Dengan HTTP, tidak ada perlindungan untuk pertukaran data antara dua perangkat yang berkomunikasi.

Dengan HTTPS, enkripsi digunakan melalui algoritma matematika. Algoritma ini menyembunyikan arti sebenarnya dari data yang sedang dipertukarkan. Hal ini dilakukan melalui penggunaan sertifikat yang dapat dilihat nanti di lab ini.

Terlepas dari HTTP atau HTTPS, hanya disarankan untuk bertukar data dengan situs web yang Anda percayai. Hanya karena sebuah situs menggunakan HTTPS tidak berarti itu adalah situs yang dapat dipercaya. Pelaku ancaman biasanya menggunakan HTTPS untuk menyembunyikan aktivitas mereka.

Di lab ini, Anda akan menjelajahi dan menangkap lalu lintas HTTP dan HTTPS menggunakan Wireshark

C. Alat dan Bahan

- CyberOps Workstation VM
- Koneksi Internet

D. Instruksi Kerja

1. Jalankan VM dan Login

   Username: **analyst**

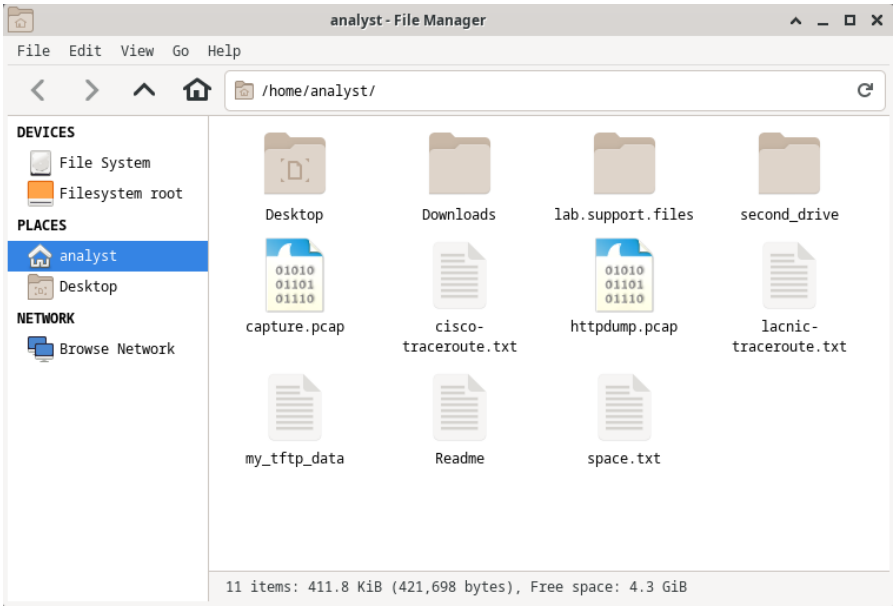
   Password: **cyberops**

2. Buka terminal dan menjalankan **tcpdump**
   Pengecekan alamat IP dengan menggunakan perintah:

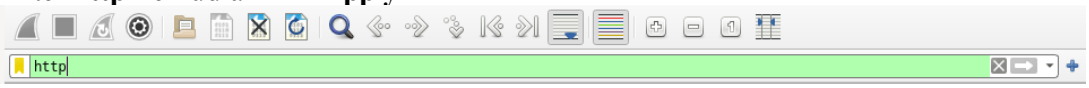
   [analyst@secOps ~]$ **ip address**
   [analyst@secOps ~]$ **sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap**
   [sudo] password for analyst:
   tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

3. Buka link http://www.altoromutual.com/login.jsp melalui browser di CyberOps Workstation VM.
   Username : **Admin**
   Password : **Admin**

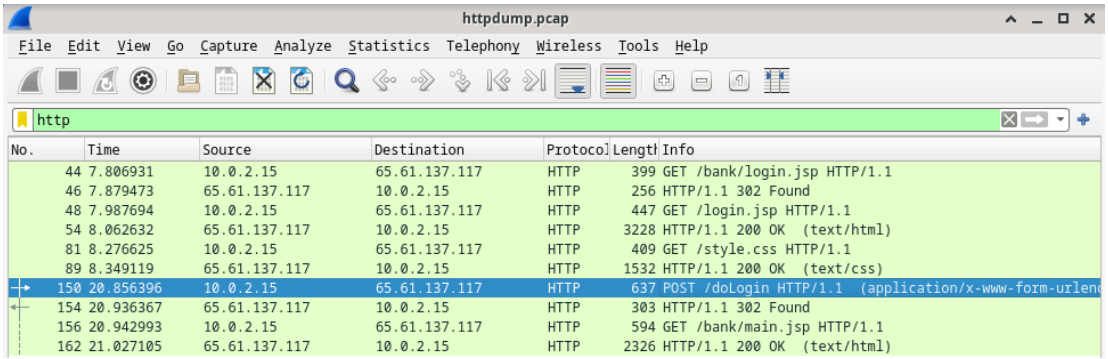
4. Merekam Paket HTTP
   Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /**home/analyst/**.



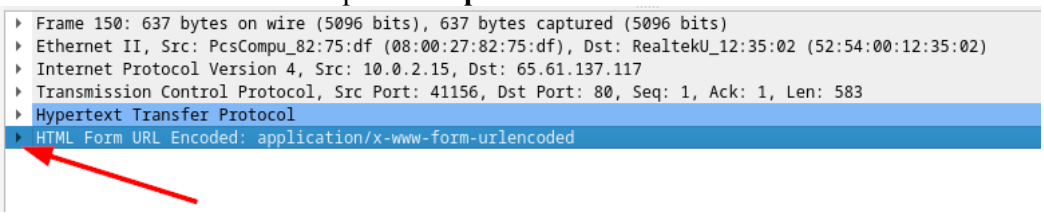
5. Filter **http** kemudian klik **Apply**



6. Pilih **POST**



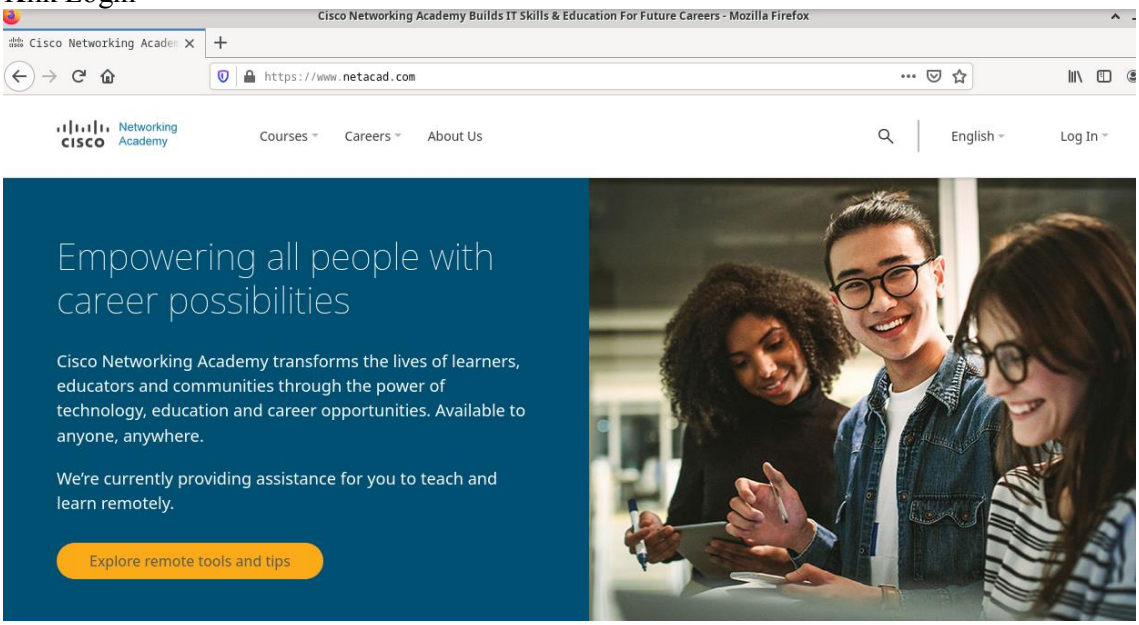
7. Lakukanlah analisis terhadap **uid** dan **passw**



8. Merekam Paket HTTPS
   [analyst@secOps ~]$ sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap
   [sudo] password for analyst:
   tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

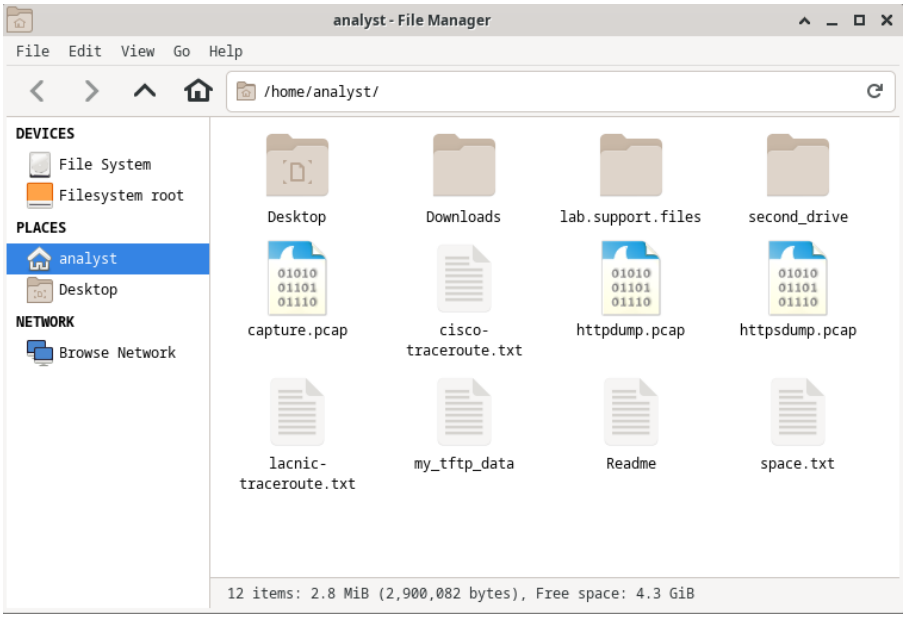
9. Buka link **https://www.netacad.com/** melalui browser di CyberOps Workstation VM.

10. Klik Login

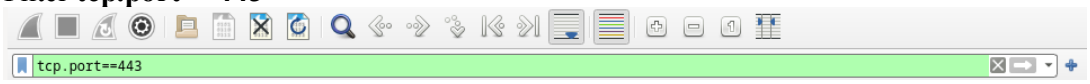


11. Masukkan *username* dan *password* anda

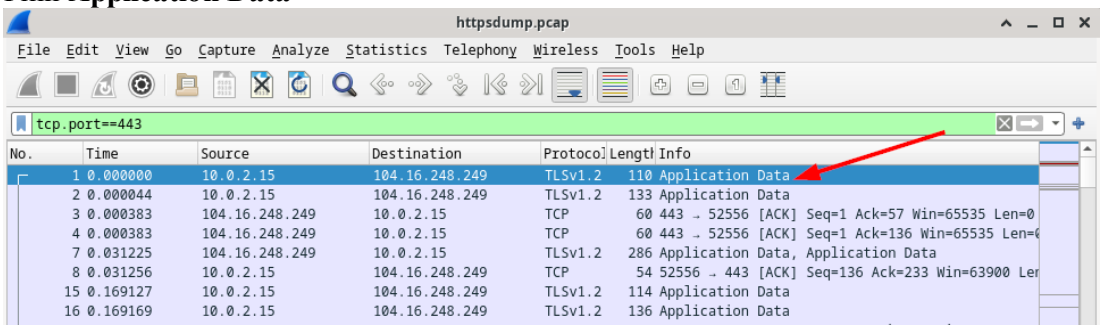
12. Melihat Rekaman Paket HTTPS
    Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpsdump.pcap. File ini terletak pada folder /**home/analyst/**.



13. Filter **tcp.port==443**



14. Pilih **Application Data**



15. Analisislah hasil yang didapatkan

16. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.