LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1 (SVRI214404)

Unit 3, Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark

DISUSUN OLEH:

Nama : Reyhan Gusnur Putra

NIM : 21/477927/SV/19223

Hari, Tanggal : Selasa, 21 Februari 2023

Kelas : A

PROGRAM STUDI TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

A. Tujuan

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

B. Dasar Teori

HTTP adalah singkatan dari Hypertext Transfer Protocol, yaitu protokol untuk komunikasi antarsistem serta mentransfer informasi dan data melalui jaringan. HTTPS adalah singkatan dari Hypertext Transfer Protocol Secure, yang mirip dengan HTTP tapi menggunakan SSL/TLS untuk mengamankan proses transfer data. HTTPS mengamankan koneksi dengan protokol keamanan digital menggunakan kunci kriptografik untuk mengenkripsi dan memvalidasi data. Untuk menggunakan HTTPS dan mengamankan domain, Anda memerlukan sertifikat SSL/TLS. Meskipun TLS kini secara umum sudah menjadi standar untuk HTTPS, sebagian besar sertifikat SSL mendukung baik protokol SSL maupun TLS.

HTTP adalah protokol lapisan aplikasi yang digunakan web browser dan web server untuk berkomunikasi melalui internet. Ketika Anda ingin membuka atau berinteraksi dengan halaman web, web browser akan mengirimkan permintaan HTTP ke server asal yang menghosting file website. Permintaan ini pada dasarnya adalah baris teks yang dikirim melalui internet. Kemudian, koneksi akan dibuat antara browser dan server, lalu server akan memproses permintaan dan mengirimkan kembali respons HTTP. Dengan demikian, halaman web pun bisa diakses oleh pengunjung website.

Wireshark adalah sebuah aplikasi capture paket data berbasis open-source yang berguna untuk memindai dan menangkap trafik data pada jaringan internet. Aplikasi ini umum digunakan sebagai alat troubleshoot pada jaringan yang bermasalah, selain itu juga biasa digunakan untuk pengujian software karena kemampuannya untuk membaca konten dari tiap paket trafik data. Aplikasi ini sebelumnya dikenal dengan nama Ethereal, namun karena permasalahan merek dagang lalu namanya diubah menjadi Wireshark.

Wireshark berguna untuk pekerjaan analisis jaringan. Cara kerjanya yaitu dengan ‘menangkap’ paket-paket data dari protokol-protokol yang berbeda dari berbagai tipe jaringan yang umum ditemukan di dalam trafik jaringan internet. Paket-paket data tersebut ‘ditangkap’ lalu ditampilkan di jendela hasil capture secara real-time.

C. Alat dan Bahan

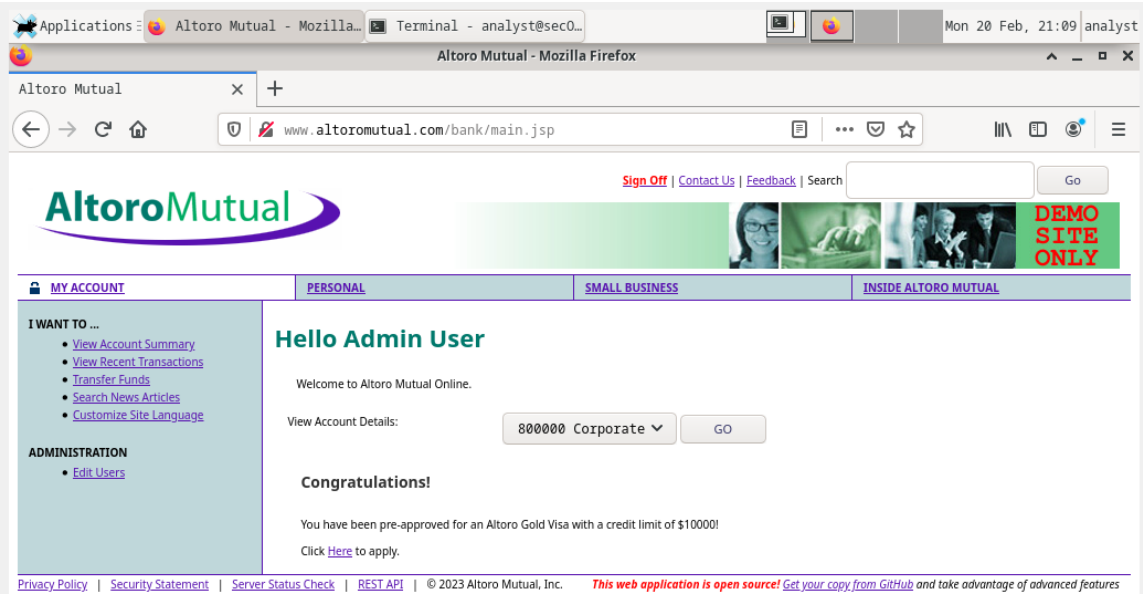
- CyberOps Workstation VM
- Koneksi Internet

D. Hasil

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

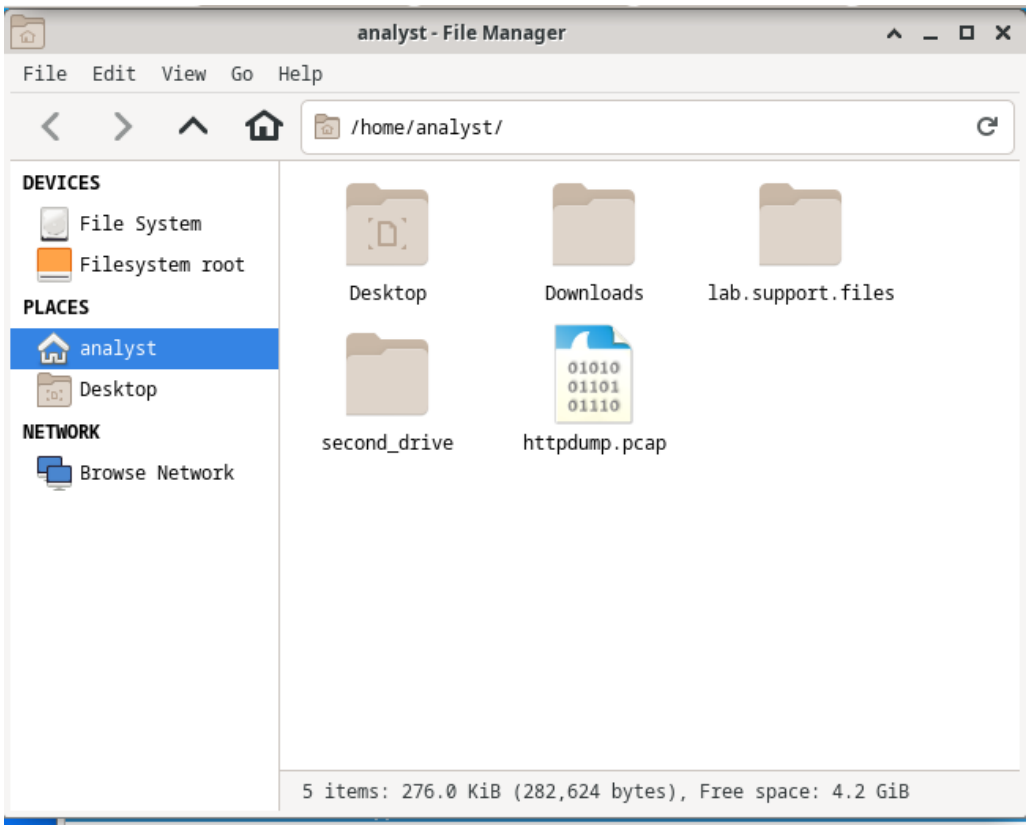
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
```

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

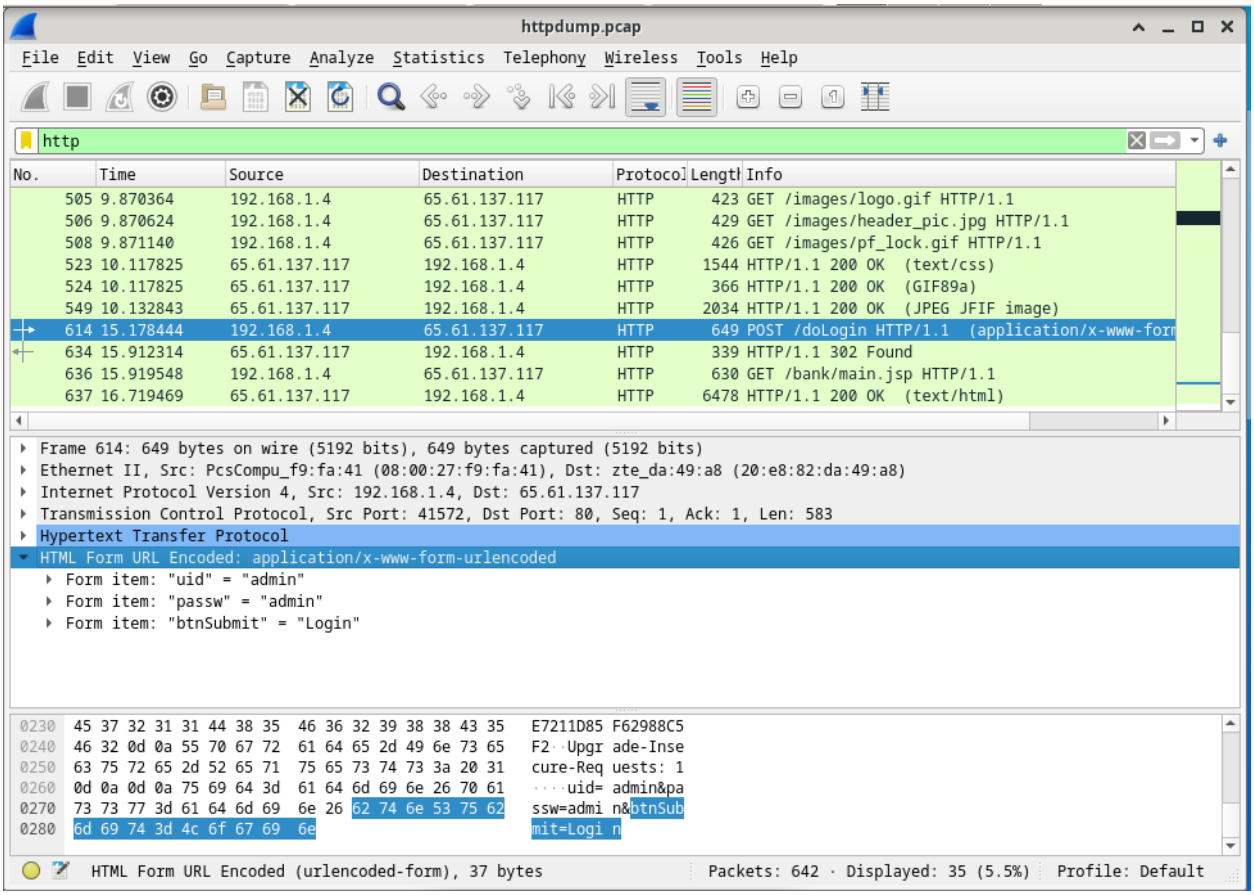


4. Merekam paket HTTP

   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**

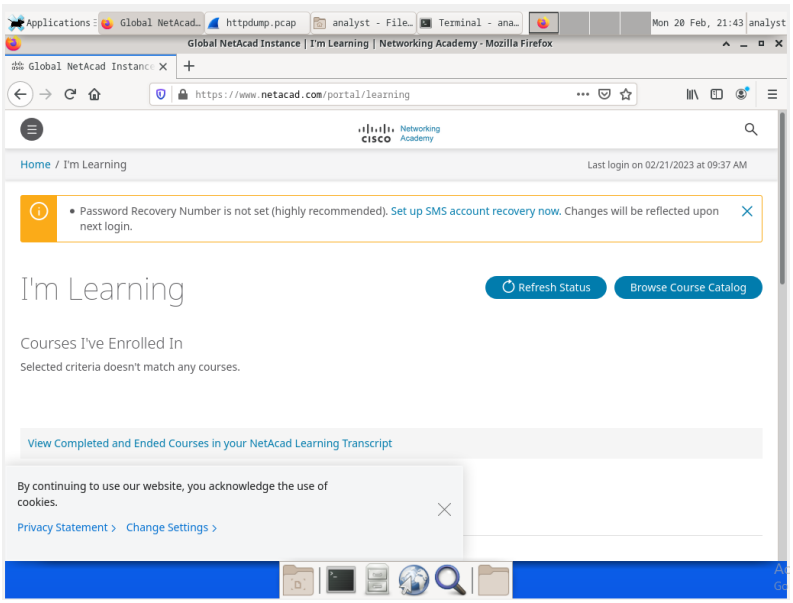


8. Merekam Paket HTTPS

   [analyst@secOps ~]$ sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap

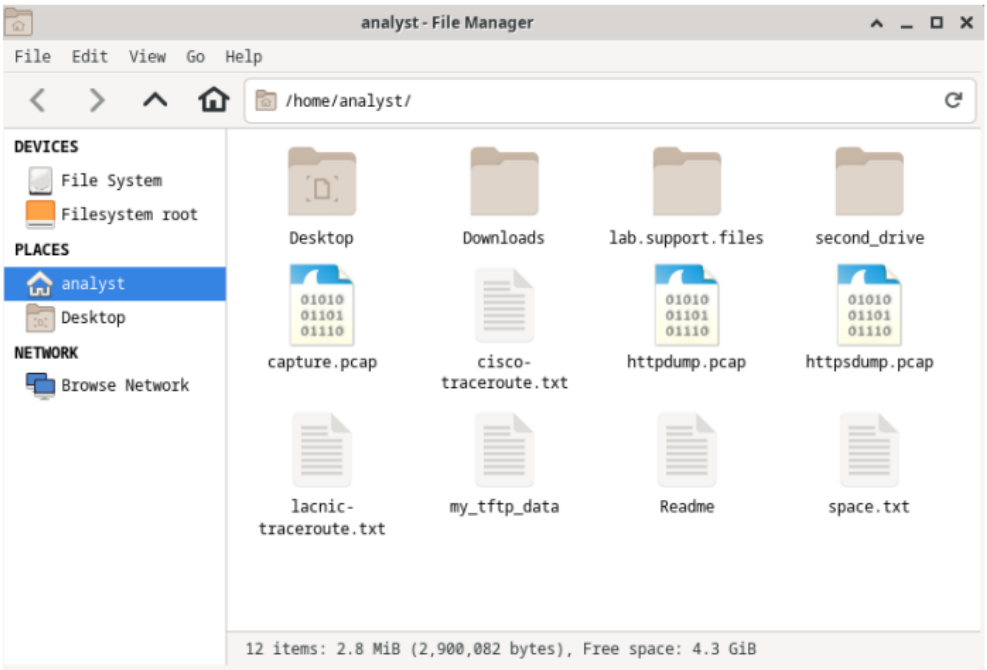
   [sudo] password for analyst:

   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



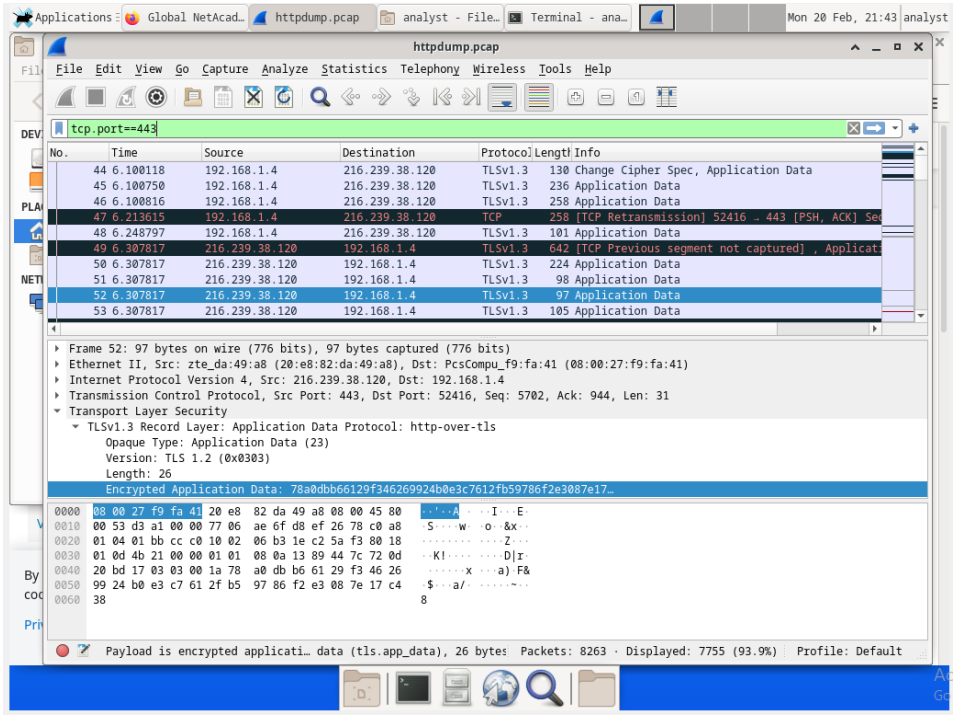
12. Melihat Rekaman Paket HTTPS

    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

E. Analisis

Tcmdump adalah perintah yang digunakan untuk mengumpulkan paket TCP/IP yang melewati adapter jaringan. tcpdump tidak hanya dapat menganalisis lalu lintas jaringan tetapi juga menyimpannya ke file. Tcpdump mencetak header paket pada antarmuka jaringan yang sesuai dengan Boolean ekspresi . Ini juga bisa dijalankan dengan-w flag, yang menyebabkannya untuk menyimpan data paket ke file untuk analisis nanti, dan / atau dengan-r flag, yang menyebabkannya membaca dari file paket yang disimpan daripada membaca paket dari antarmuka jaringan. Dalam semua kasus, hanya paket yang cocok ekspresi akan diproses oleh tcpdump.

Kemudian menggunakan wireshark pada file tcpdump yang sudah dikumpulkan untuk menganalisis jaringan, pada percobaan pertama atau percobaan wireshark pada tcpdump dari link http://www.altoromutual.com/login.jsp, kita diminta untuk memfilter http dan menganalisis hasilnya, pada bagian HTML Form URL Encoded: application/x-

www-form-urlencoded kita mendapatkan username (uid) dan password (passw) yang dimasukkan pada bagian login.

Percobaan selanjutnya kita login pada web netacad dan melakukan tcpdump pada web tersebut. Filter yang digunakan dalam wireshark adalah tcp.port==443. Port 443 adalah port default dari koneksi dengan protokol HTTPS, yaitu sebuah protokol komunikasi data yang aman karena dilindungi oleh sertifikat SSL . SSL adalah metode yang memastikan setiap informasi data akan dienkripsi sehingga tidak mudah dibaca oleh pihak lain, seperti hacker. Hasil yang didapat pada Transport Layer Security adalah Encrypted Application Data atau enkripsi data, Enkripsi data adalah proses pengamanan data informasi. Enkripsi data mengamankan data informasi dengan cara membuat data informasi tersebut tidak bisa dibaca tanpa bantuan khusus.

F. Kesimpulan

Kesimpulan yang didapat dari praktikum ini adalah:

1. Tcmdump adalah perintah yang digunakan untuk mengumpulkan paket TCP/IP yang melewati adapter jaringan.
2. Wireshark adalah sebuah aplikasi capture paket data berbasis open-source yang berguna untuk memindai dan menangkap trafik data pada jaringan internet.
3. Cara wireshark yaitu dengan ‘menangkap’ paket-paket data dari protokol-protokol yang berbeda dari berbagai tipe jaringan yang umum ditemukan di dalam trafik jaringan internet.

G. Daftar Pustaka

JAGOAN HOSTING. 2022. *Ap aitu Enkripsi Data? Begini Manfaat dan Cara Kerjanya.* Diakses pada 27 Februari 2023. https://www.jagoanhosting.com/blog/apa-itu-enkripsi-data/

Faradilla A. 2023. *Perbedaan HTTP dan HTTPS serta Pengertiannya*. Diakses pada 27 Februari 2023. https://www.hostinger.co.id/tutorial/perbedaan-http-dan-https#:~:text=HTTP%20adalah%20singkatan%20dari%20Hypertext,untuk%20mengamankan%20proses%20transfer%20data.

Saputro, Nur. 2022. *Kenali Pengertian Wireshark Beserta Fungsi dan Cara kerjanya, Lengkap!*. Diakses pada 27 Februari 2023. https://www.nesabamedia.com/pengertian-wireshark/