

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:

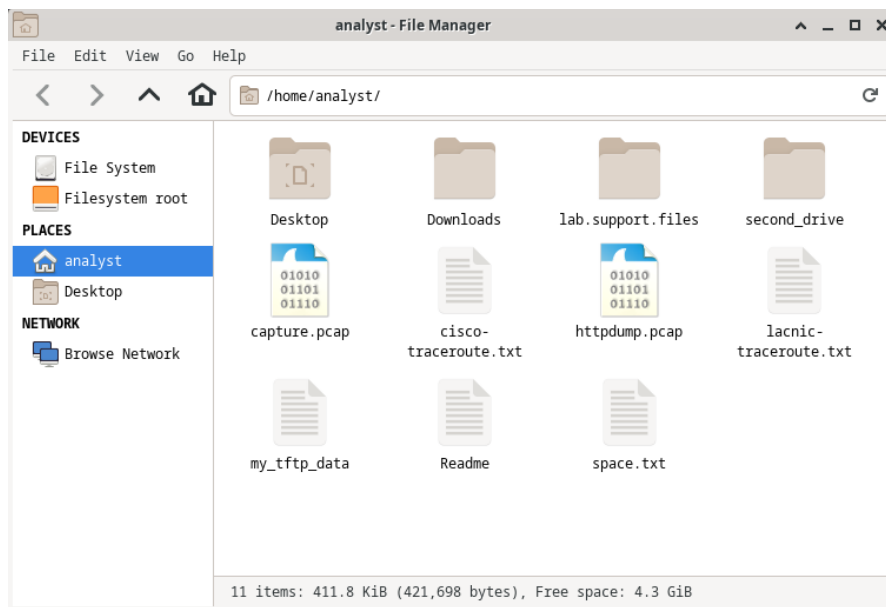
```
[analyst@secOps ~]$ ip address
```

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

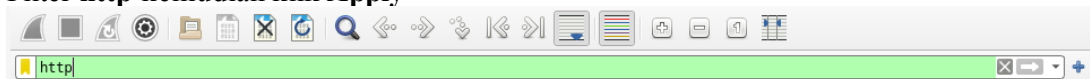
```
[sudo] password for analyst:
```

```
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/**.



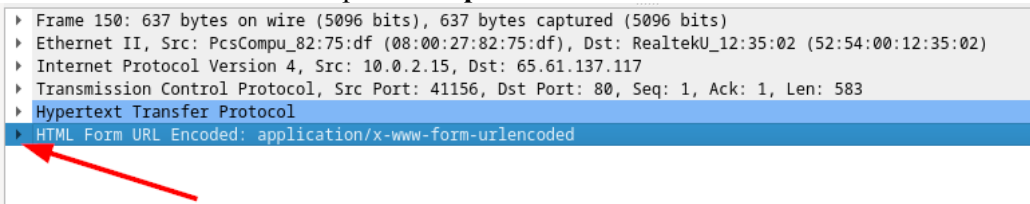
5. Filter **http** kemudian klik **Apply**



6. Pilih **POST**

No.	Time	Source	Destination	Protocol	Length	Info
44	7.806931	10.0.2.15	65.61.137.117	HTTP	399	GET /bank/login.jsp HTTP/1.1
46	7.879473	65.61.137.117	10.0.2.15	HTTP	256	HTTP/1.1 302 Found
48	7.987694	10.0.2.15	65.61.137.117	HTTP	447	GET /login.jsp HTTP/1.1
54	8.062632	65.61.137.117	10.0.2.15	HTTP	3228	HTTP/1.1 200 OK (text/html)
81	8.276625	10.0.2.15	65.61.137.117	HTTP	409	GET /style.css HTTP/1.1
89	8.349119	65.61.137.117	10.0.2.15	HTTP	1532	HTTP/1.1 200 OK (text/css)
150	20.856396	10.0.2.15	65.61.137.117	HTTP	637	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
154	20.936367	65.61.137.117	10.0.2.15	HTTP	303	HTTP/1.1 302 Found
156	20.942993	10.0.2.15	65.61.137.117	HTTP	594	GET /bank/main.jsp HTTP/1.1
162	21.027105	65.61.137.117	10.0.2.15	HTTP	2326	HTTP/1.1 200 OK (text/html)

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



8. Merekam Paket HTTPS

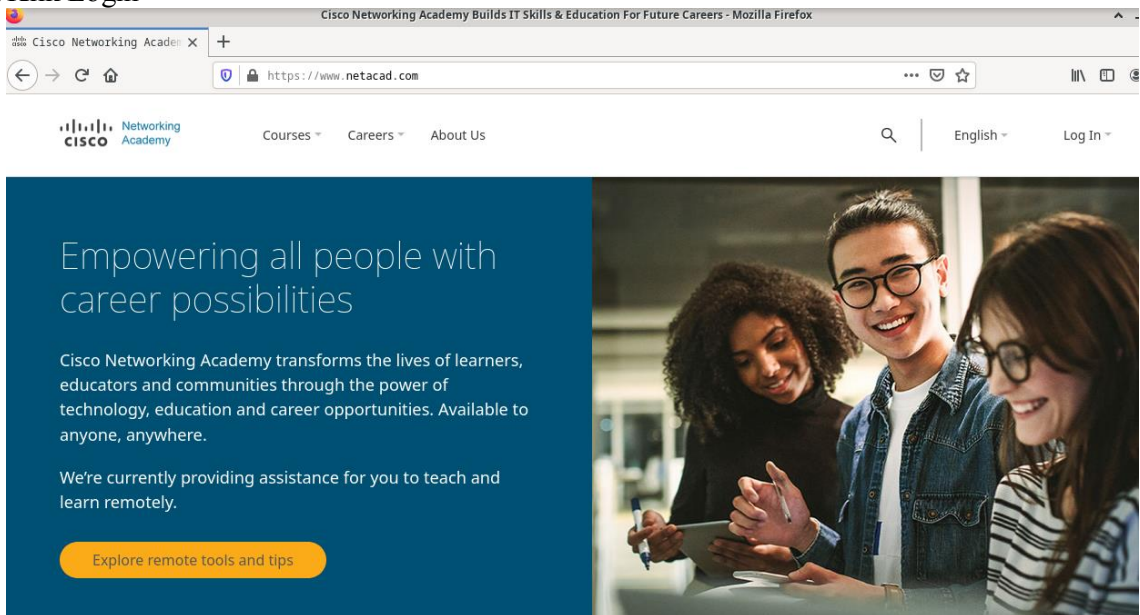
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
```

```
[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.

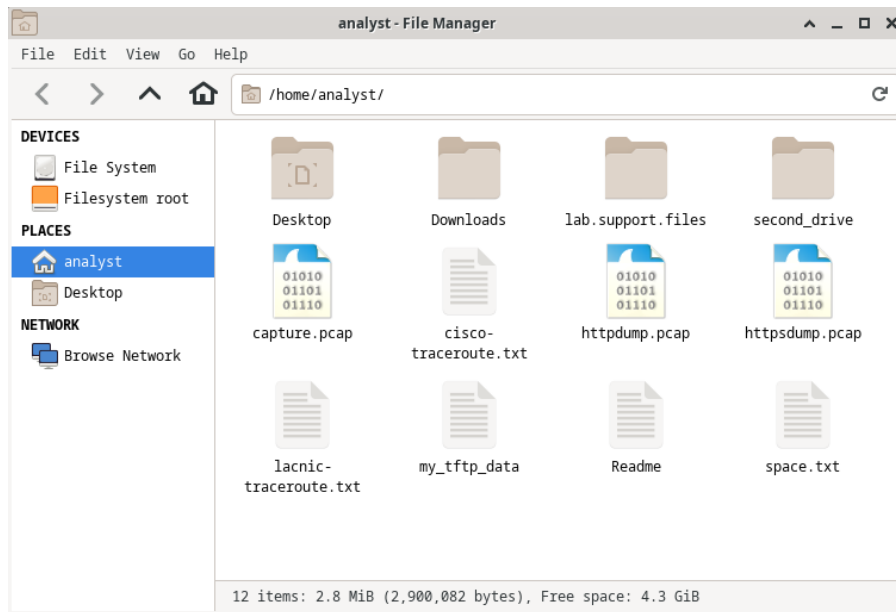
10. Klik Login



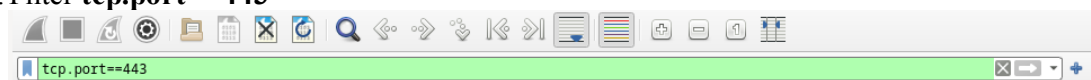
11. Masukkan *username* dan *password* anda

12. Melihat Rekaman Paket HTTPS

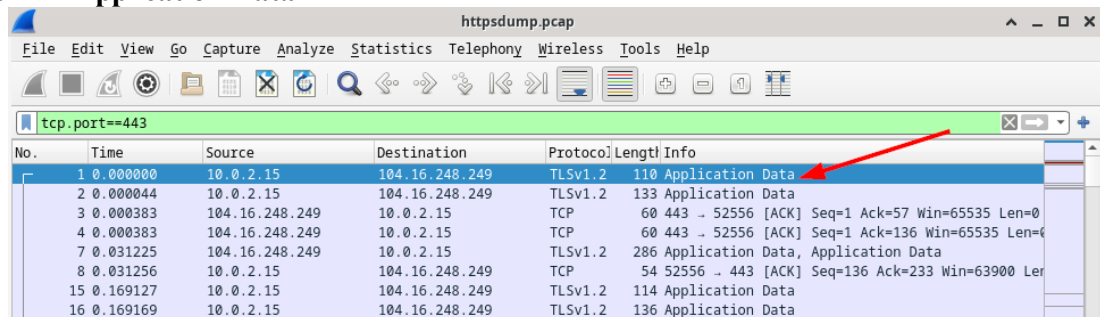
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama `httpsdump.pcap`. File ini terletak pada folder `/home/analyst/`.



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.