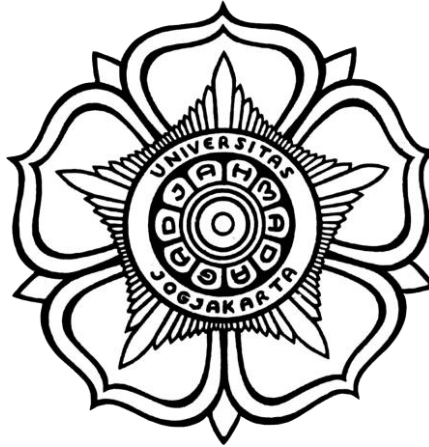


LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
“Eksplorasi HTTP & HTTPS Dengan Wireshark Dan eksplorasi NMAP”

Pertemuan 2



Disusun oleh :

Nama	:Nayaka Iman Wiraputra
NIM	: 21/482203/SV/19910
Kelas	: TRI A
Hari, Tanggal	: Selasa, 2022
Dosen Pengampu S.Kom., M.Eng.	: Anni Karimatul Fauziyyah,
Asisten Dosen	: Gabriella Alvera Chaterine

LABORATORIUM KEAMANAN INFORMASI
SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPATEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA

2022

A. TUJUAN

Tujuan dari eksplorasi HTTP dan HTTPS adalah untuk memahami perbedaan antara dua 2ensitiv tersebut dan bagaimana mereka beroperasi di web. Dengan memahami perbedaan antara HTTP dan HTTPS, pengguna dapat lebih memahami bagaimana informasi dipertukarkan antara server dan klien, serta mengapa keamanan informasi sangat penting dalam lingkungan web.

Beberapa tujuan eksplorasi HTTP dan HTTPS yang dapat dilakukan antara lain:

1. Memahami perbedaan antara HTTP dan HTTPS, termasuk bagaimana keduanya mengirimkan data dan bagaimana mereka berinteraksi dengan sisi server dan sisi klien.
2. Memahami bagaimana HTTP dan HTTPS digunakan dalam praktiknya, termasuk penggunaan HTTPS untuk meningkatkan keamanan koneksi web dan menghindari serangan yang dapat membahayakan keamanan data.
3. Mempelajari alat dan teknologi yang digunakan untuk mengimplementasikan 2ensitiv HTTP dan HTTPS, termasuk metode enkripsi yang digunakan untuk memastikan keamanan data yang dipertukarkan.
4. Memahami bagaimana 2ensitiv HTTP dan HTTPS beroperasi pada lapisan transportasi OSI (Open Systems Interconnection), dan bagaimana lapisan tersebut membantu memastikan keamanan data.

Dengan memahami HTTP dan HTTPS, pengguna dapat memahami bagaimana data dienkripsi, disimpan, dan ditransfer antara server dan klien dalam lingkungan web, dan dapat memilih 2ensitiv yang paling cocok untuk tujuan mereka.

B. ALAT DAN BAHAN

Alat dan bahan yang di butuhkan pada praktik kali ini adalah

1. Computer
2. Virtual box
3. Koneksi internet
4. CyberOps Workstation VM

C. DASAR TEORI

HTTP (Hypertext Transfer Protocol) dan HTTPS (Hypertext Transfer Protocol Secure) adalah 2ensitiv komunikasi yang digunakan untuk mempertukarkan data melalui internet.

HTTP adalah 2ensitiv yang digunakan untuk mentransfer data dalam bentuk dokumen hiperteks atau halaman web antara server web dan klien web. Ini adalah 2ensitiv yang paling umum digunakan di web dan beroperasi di atas TCP/IP. Namun, HTTP tidak aman karena data yang ditransfer antara server dan klien tidak dienkripsi, sehingga

informasi 3ensitive dapat mudah diretas atau disadap oleh pihak ketiga yang tidak berwenang.

HTTPS adalah varian dari HTTP yang menggunakan enkripsi untuk memastikan keamanan data yang ditransfer antara server dan klien. Dalam HTTPS, data yang dikirim antara server dan klien dienkripsi menggunakan 3ensitiv SSL (Secure Sockets Layer) atau TLS (Transport Layer Security). Hal ini membuatnya lebih sulit bagi pihak yang tidak berwenang untuk mengakses atau memanipulasi data yang ditransfer.

Dalam sambungan HTTPS, server web dan klien web membentuk koneksi aman dengan mengatur kunci enkripsi yang digunakan untuk mengenkripsi dan mendekripsi data yang ditransfer. Hal ini membuat HTTPS lebih aman daripada HTTP dan lebih cocok untuk mentransfer informasi 3ensitive seperti informasi kartu kredit, kata sandi, atau informasi pribadi lainnya.

D. LANGKAH KERJA

UNIT 2

A. Tujuan

- Mengesplorasi Nmap
- Melakukan Scan ke Port yang terbuka

B. Latar Belakang

Port scanning biasanya merupakan bagian dari serangan pengintaian. Ada berbagai metode Port scanning yang dapat digunakan. Nmap adalah software jaringan yang digunakan untuk audit keamanan dengan menggunakan metode port scanning.

C. Alat dan Bahan

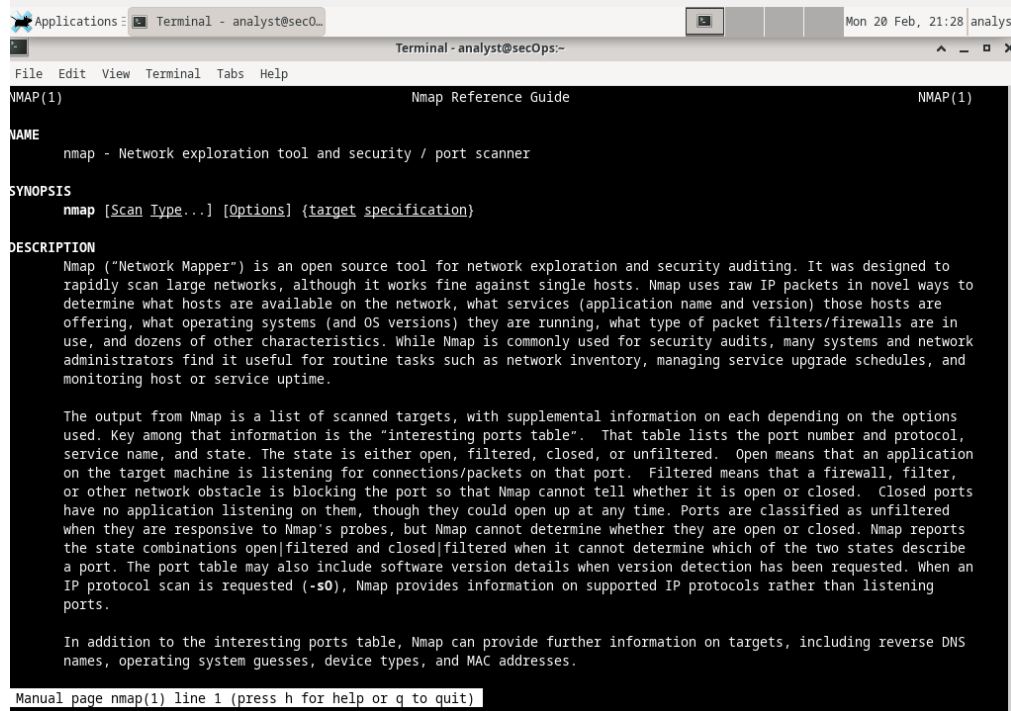
- CyberOps Workstation virtual machine
- Internet access

D. Instruksi Kerja

1. Eksplorasi Nmap

Start CyberOps Workstation

Buka terminal kemudian ketikkan `[analyst@secOps ~]$ man nmap`



```
Applications: Terminal - analyst@secOps~
Terminal - analyst@secOps~
File Edit View Terminal Tabs Help
NMAP(1) Nmap Reference Guide NMAP(1)

NAME
  nmap - Network exploration tool and security / port scanner

SYNOPSIS
  nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
  Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

  The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-s0), Nmap provides information on supported IP protocols rather than listening ports.

  In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

Manual page nmap(1) line 1 (press h for help or q to quit)
```

Apa itu Nmap?

Nmap (Network Mapper) adalah sebuah alat atau tool open source untuk melakukan pemindaian jaringan atau port scanning. Nmap digunakan untuk memeriksa jaringan komputer untuk mengetahui perangkat yang terhubung ke jaringan, port yang terbuka di perangkat tersebut, serta sistem operasi dan layanan yang dijalankan pada perangkat tersebut. Nmap dapat berjalan pada berbagai sistem operasi, termasuk Linux, Windows, dan macOS.

Apa fungsi dari Nmap?

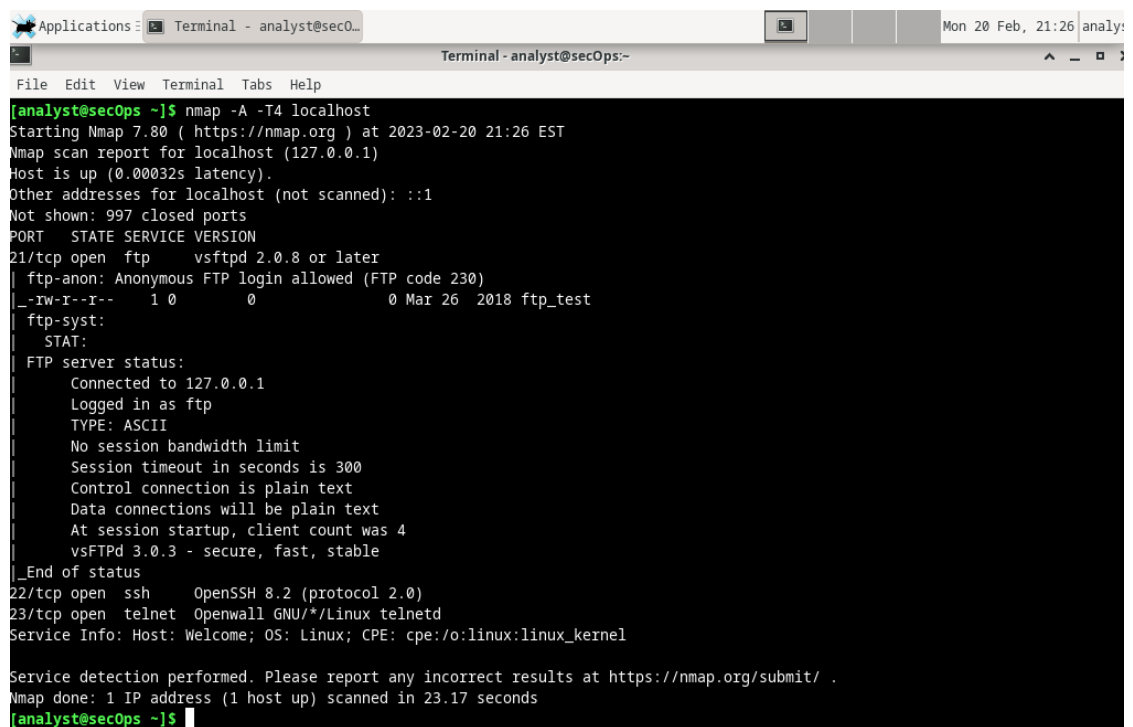
Nmap (Network Mapper) memiliki berbagai fungsi, antara lain:

1. Port scanning: Nmap dapat digunakan untuk memindai port pada suatu jaringan untuk menemukan port yang terbuka dan mengetahui layanan yang dijalankan pada port tersebut.
2. Pemindaian versi layanan: Nmap dapat memeriksa versi layanan yang dijalankan pada port yang terbuka untuk mengetahui informasi lebih detail tentang layanan tersebut.

3. Pemindaian sistem operasi: Nmap dapat mengidentifikasi sistem operasi yang dijalankan pada perangkat jaringan dengan menganalisis paket jaringan yang dikirimkan oleh perangkat tersebut.
4. Deteksi rentan: Nmap dapat digunakan untuk mendeteksi celah keamanan pada sistem dan layanan yang dijalankan pada perangkat jaringan.
5. Pemetaan topologi jaringan: Nmap dapat digunakan untuk memetakan topologi jaringan dengan mengetahui perangkat apa saja yang terhubung ke jaringan dan bagaimana hubungan antar perangkat tersebut.
6. Pemantauan jaringan: Nmap dapat digunakan untuk memantau kesehatan jaringan dengan memeriksa ketersediaan perangkat jaringan dan layanan yang dijalankan pada perangkat tersebut.
7. Audit keamanan: Nmap dapat digunakan untuk melakukan audit keamanan pada jaringan untuk menemukan celah keamanan dan memberikan saran untuk meningkatkan keamanan jaringan.
8. Administrasi jaringan: Nmap dapat digunakan untuk melakukan tugas administratif jaringan, seperti melakukan inventarisasi perangkat jaringan dan mengelola koneksi jaringan

2. Localhost Scanning

[analyst@secOps ~]\$ nmap -A -T4 localhost



```

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 21:26 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00032s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0      0          0 Mar 26 2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 127.0.0.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 8.2 (protocol 2.0)
23/tcp    open  telnet   Openwall GNU/*/Linux telnetd
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.17 seconds
[analyst@secOps ~]$

```

Output Nmap yang terlihat hanya ada 2 port yang terbuka, yaitu port 22 dengan layanan ssh dan port 23 dengan layanan telnet

3. Network Scanning

Sebelum melakukan scanning alangkah lebih baiknya untuk mengetahui alamat IP host terlebih dahulu.

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

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:81:ac:c4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86156sec preferred_lft 86156sec
    inet6 fe80::a00:27ff:fe81:acc4/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Alamat IP PC host adalah **10.0.2.15/24** dengan subnet mask **255.255.255.0**
(dinyatakan dalam notasi CIDR sebagai /24)

Lakukan lah port scanning degan menggunakan Nmap

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15/24
```

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 21:29 EST
Nmap scan report for 10.0.2.15
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0          0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 4
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 8.2 (protocol 2.0)
23/tcp    open  telnet   Openwall GNU/*/Linux telnetd
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 39.56 seconds
[analyst@secOps ~]$
```

Dari laporan scan Nmap tersebut hanya satu host yang terdeteksi dengan alamat IP 10.0.2.15. oleh karena itu, jumlah host yang terdeteksi adalah 1

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.

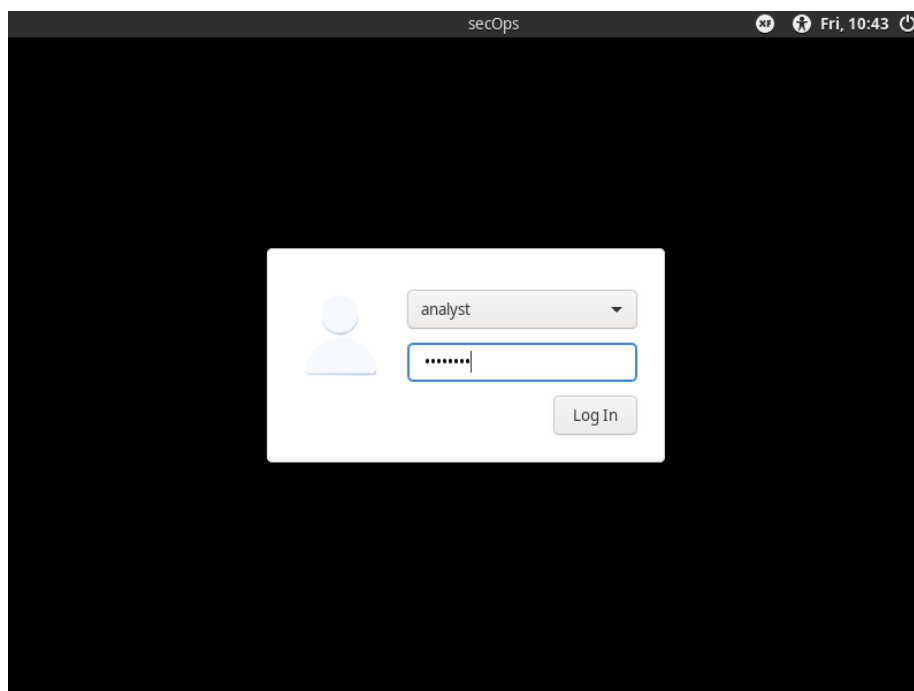
Di lab ini, Anda akan menjelajahi dan menangkap lalu lintas HTTP dan HTTPS menggunakan Wireshark

C. Alat dan Bahan

- CyberOps Workstation VM
- Koneksi Internet

D. intruksi kerja

1. Jalankan VM dan Login



2. Buka terminal dan menjalankan tcpdump

Pengecekan alamat IP dengan menggunakan perintah :

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

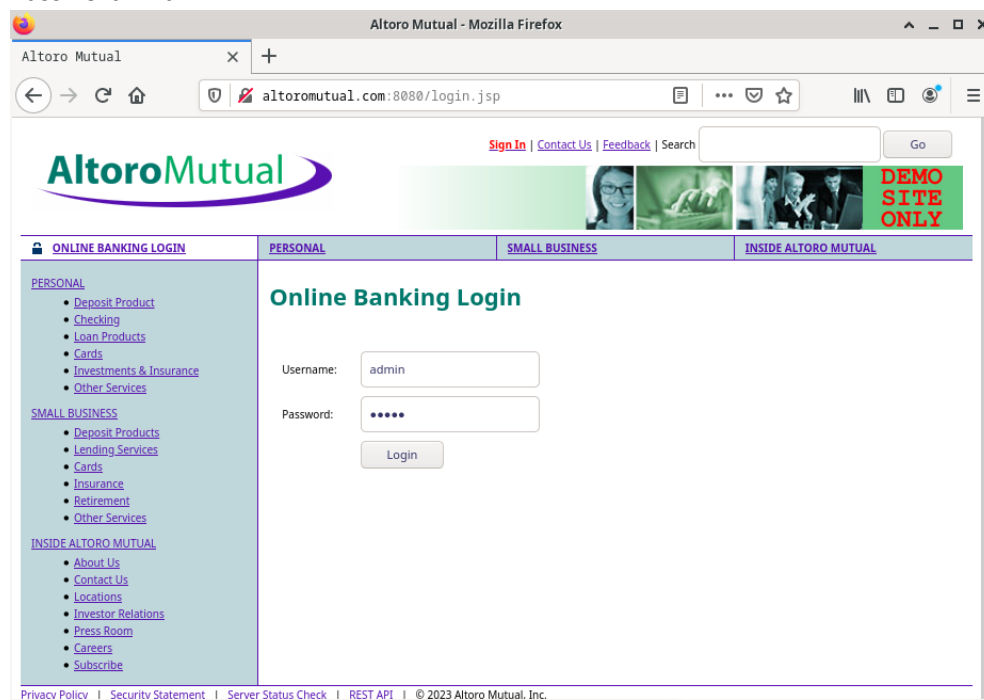
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

```
[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

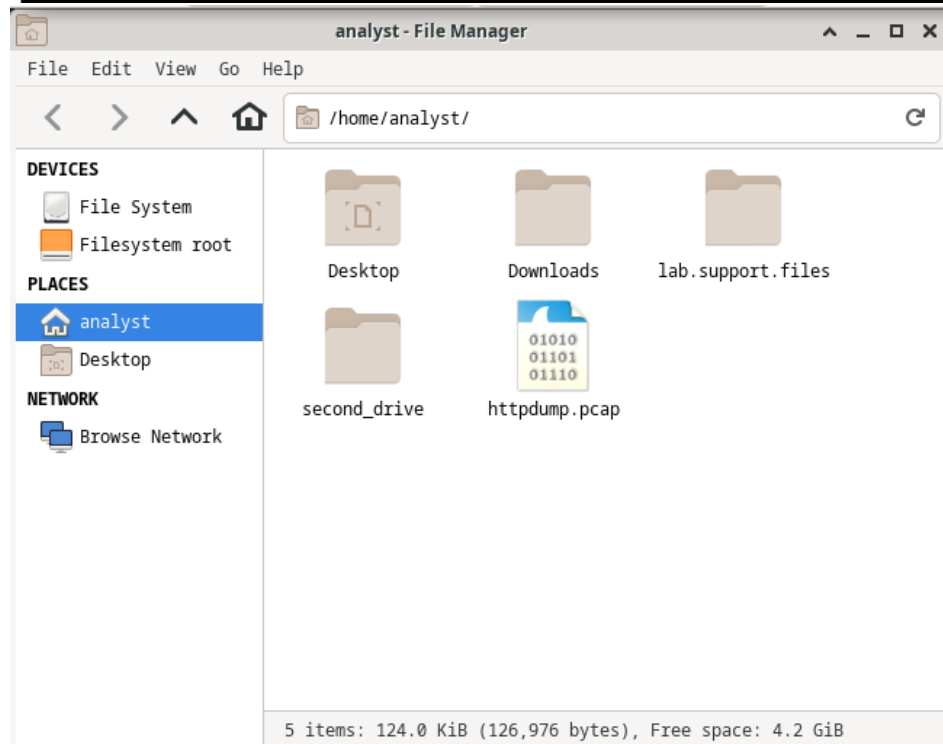
Password : Admin



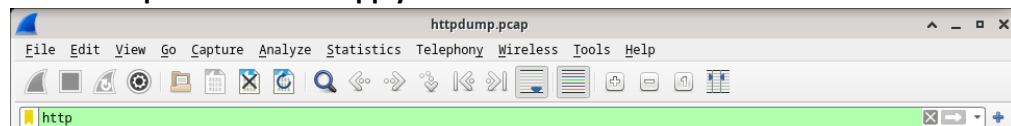
4. Merekam Paket HTTP Tcpcap yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap.

File ini terletak pada folder /home/analyst/.

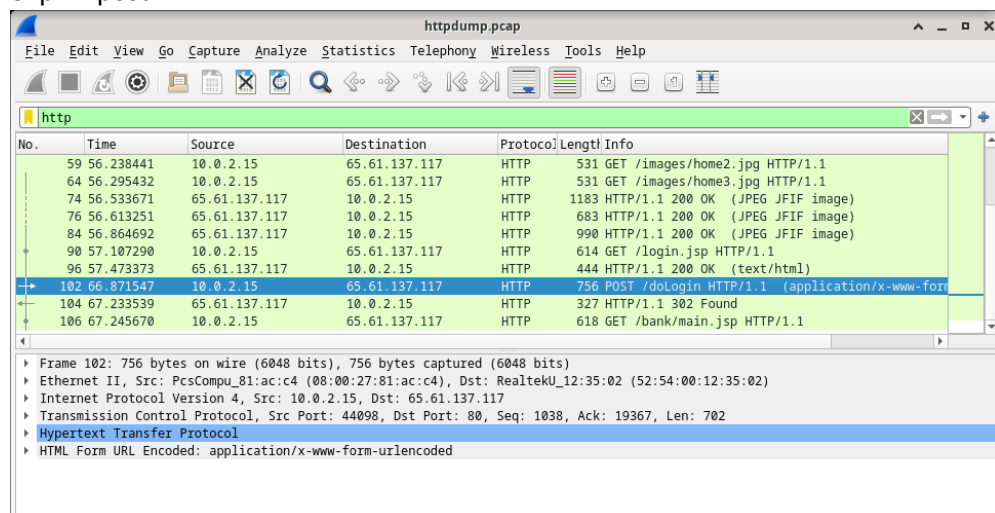
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```



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



6. pilih post



7. Lakukan analisis terhadap uid dan password

```
▶ Transmission Control Protocol, Src Po
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x
  ▼ Form item: "uid" = "Admin"
    Key: uid
    Value: Admin
  ▼ Form item: "passw" = "Admin"
    Key: passw
    Value: Admin
  ▼ Form item: "btnSubmit" = "Login"
    Key: btnSubmit
    Value: Login
```

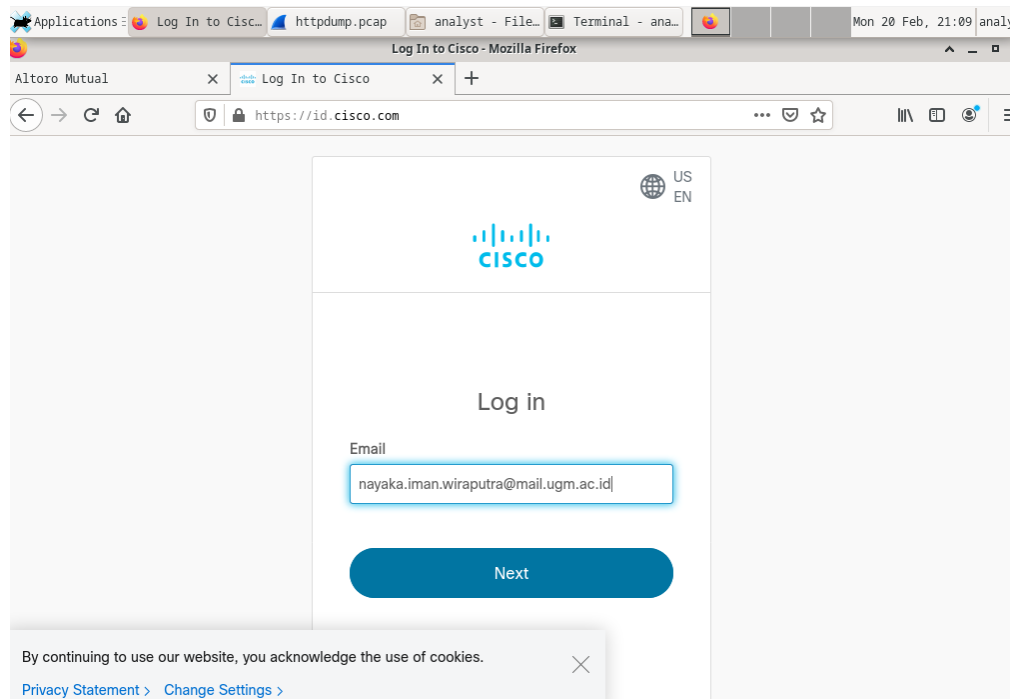
8. Merekam Paket HTTPS

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

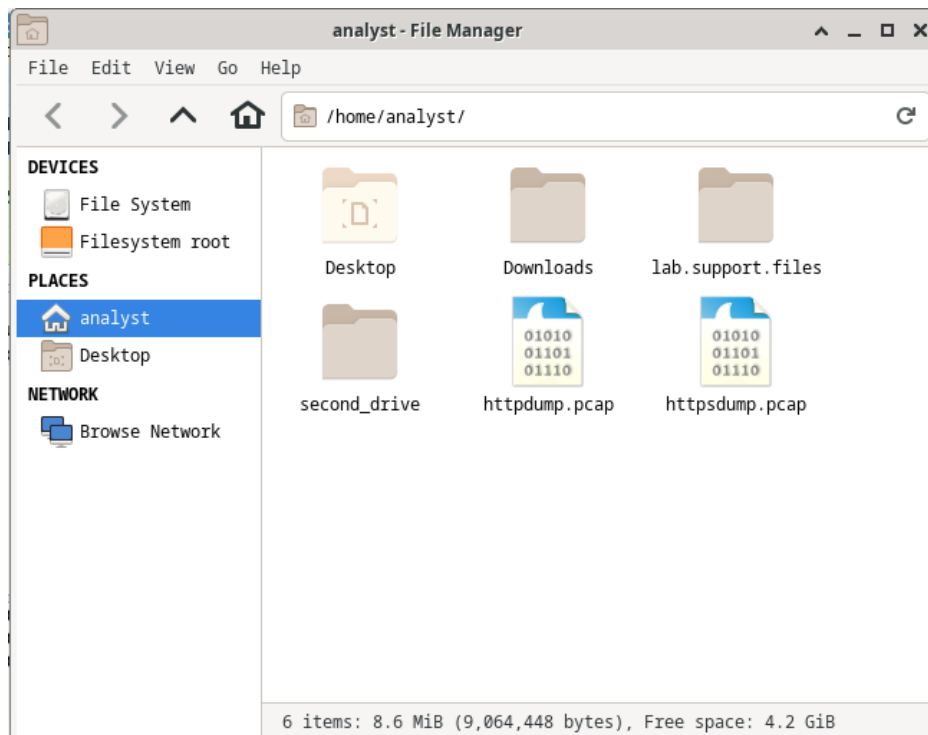
[sudo] password for analyst:

tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

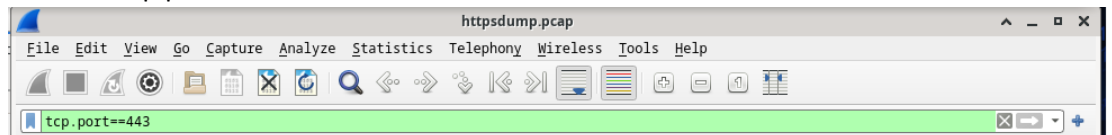
9. Buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM



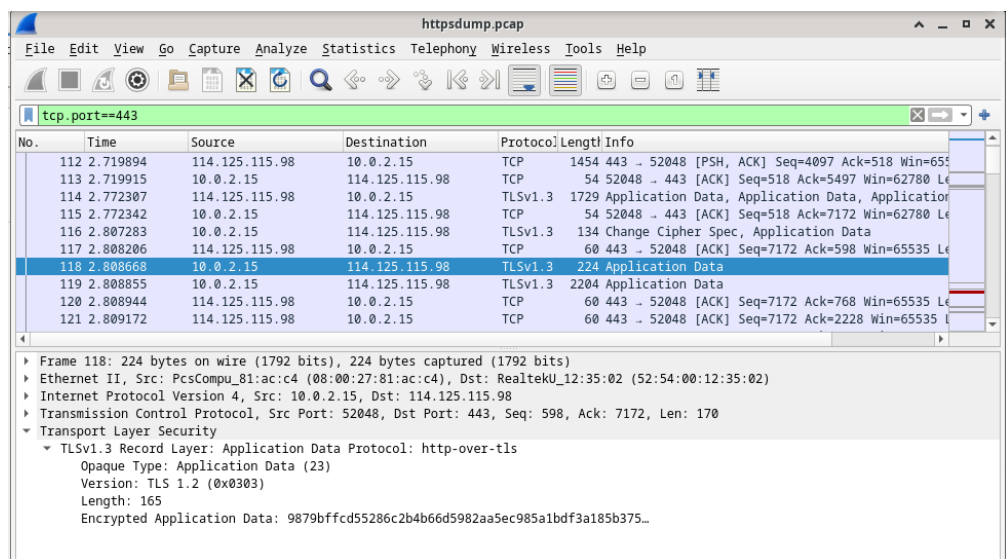
12. Melihat Rekaman Paket HTTPS Tcpcap yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpsdump.pcap. File ini terletak pada folder /home/analyst/.



13. Filter tcp.port==443



14. Pilih Application Data



E. PEMBAHASAN

Pada pertemuan ke 2 ini, praktikan melakukan pengujian dengan materi **Eksplorasi HTTP & HTTPS Dengan Menggunakan Wireshark**. HTTP (Hypertext Transfer Protocol) dan HTTPS (Hypertext Transfer Protocol Secure) adalah protokol komunikasi yang digunakan untuk mengirimkan data melalui jaringan internet. Kedua protokol ini digunakan untuk mengakses situs web dan mentransfer informasi antara server web dan browser klien.

Namun, ada perbedaan penting antara HTTP dan HTTPS. HTTP mengirimkan data dalam bentuk teks biasa (plaintext), yang dapat dengan mudah dicuri atau dimanipulasi oleh penjahat siber. Sebaliknya, HTTPS menggunakan enkripsi SSL/TLS untuk mengamankan data yang ditransmisikan melalui jaringan. Ini berarti bahwa ketika data dikirimkan melalui HTTPS, itu dienkripsi dan tidak dapat dibaca oleh pihak ketiga yang mencoba mengintip.

Karena keamanan yang ditawarkan oleh HTTPS, protokol ini menjadi pilihan yang lebih baik untuk situs web yang memerlukan pengiriman informasi yang sensitif seperti nomor kartu kredit, informasi login, dan lain sebagainya. Banyak situs web e-commerce, bank, dan organisasi lain yang membutuhkan keamanan tinggi menggunakan HTTPS untuk melindungi informasi pribadi pengguna mereka.

Namun, HTTPS juga membutuhkan biaya dan waktu untuk mengkonfigurasi sertifikat SSL/TLS yang diperlukan untuk menggunakan enkripsi tersebut. Karena itu, beberapa situs web yang tidak memerlukan keamanan tinggi mungkin masih menggunakan HTTP.

F. KESIMPULAN

HTTPS adalah pilihan yang lebih aman untuk situs web yang memerlukan keamanan tinggi, sementara HTTP cocok untuk situs web yang tidak memerlukan enkripsi data yang kuat. Namun, dalam era di mana keamanan data menjadi semakin penting, semakin banyak situs web yang beralih dari HTTP ke HTTPS untuk meningkatkan perlindungan data mereka.

DAFTAR PUSTAKA

- Anni Karimatul Fauziyyah, S. M. (2023, February 21). *ELOK*. Retrieved from https://elok.ugm.ac.id/pluginfile.php/2302264/mod_resource/content/1/Pertemuan%20%20Keamanan%20Informasi%201.pdf
- monitor teknologi*. (2021, February 8). Retrieved from Cybersecurity: <https://www.monitorteknologi.com/cara-menggunakan-nmap/>
- musk, E. (2023, February 23). *Open AI*. Retrieved from <https://chat.openai.com/chat>
- Wibowo, P. (2013, February 4). *ilmukomputer*. Retrieved from <https://ilmukomputer.org/2013/02/04/keamanan-dan-eksplorasi-jaringan-dengan-nmap/>
- Wijayanti, N. N. (2022, February 14). Retrieved from Niagahoster: <https://www.niagahoster.co.id/blog/perbedaan-http-dan-https/#:~:text=HTTP%20adalah%20sebuah%20protokol%20pada%20suatu%20jaringan%20yang,memiliki%20standar%20keamanan%20yang%20lebih%20tinggi%20dari%20HTTP.>