

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

UNIT 2 & 3

**Eksplorasi Nmap & Pemantauan Trafik HTTP dan HTTPS dengan
menggunakan Wireshark**



DISUSUN OLEH

Gabe Asriel Wolly Limbong

21/480067/SV/19566

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

Unit 2 & 3

Eksplorasi Nmap & Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark

A. Tujuan Percobaan

- Unit 2
 - Mengesplorasi Nmap
 - Melakukan Scan ke Port yang terbuka
- Unit 3
 - Merekam dan menganalisis trafik http
 - Merekam dan menganalisis trafik https

B. Teori Dasar

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.

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. Prosedur Percobaan

- Unit 2

1. Eksplorasi Nmap

Start CyberOps Workstation
Buka terminal kemudian ketikkan

```
[analyst@secOps ~]$ man nmap
```

Apa itu Nmap?
Apa fungsi dari Nmap?

2. *Localhost Scanning*

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

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:20 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000056s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 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 Apr 19 15:23 ftp_test
<some output omitted>
```

Port dan layanan apa yang terbuka?

Software apa yang digunakan pada port yang terbuka tersebut?

3. *Network Scanning*

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

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

<output omitted>

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UP group default qlen 1000
```

```
link/ether 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff
```

```
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
```

```
valid_lft 85777sec preferred_lft 85777sec
```

```
inet6 fe80::a00:27ff:feed:af2c/64 scope link
```

```
valid_lft forever preferred_lft forever
```

Berapakah alamat IP dan subnet mask dari PC host?

Lakukanlah port scanning dengan menggunakan Nmap

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
```

Starting Nmap 7.40 (<https://nmap.org>) at 2017-05-01 17:13 EDT
 <output omitted>
 Nmap scan report for 10.0.2.15
 Host is up (0.00019s 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 1
 | 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

 Post-scan script results:
 | clock-skew:
 | 0s:
 | 10.0.2.4
 | 10.0.2.3
 |_ 10.0.2.2
 Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
 Nmap done: 256 IP addresses (4 hosts up) scanned in 346.89 seconds

 Berapakah jumlah host yang terdeteksi?

4. Remote Server Scanning

Buka web browser dan kunjungi **scanme.nmap.org**

Ketikkan perintah berikut:

```
[analyst@secOps Desktop]$ nmap -A -T4 scanme.nmap.org
```

Starting Nmap 7.40 (<https://nmap.org>) at 2017-05-01 16:46 EDT

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.040s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 992 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

| ssh-hostkey:

| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)

| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)

| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)

25/tcp filtered smtp

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

|_ http-server-header: Apache/2.4.7 (Ubuntu)

|_ http-title: Go ahead and ScanMe!

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

593/tcp filtered http-rpc-epmap

4444/tcp filtered krb524

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

Service Info: 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 23.96 seconds

Port dan layanan apa yang terbuka?

Berapa alamat IP server?

Apa sistem operasi yang digunakan oleh server?

- Unit 3

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

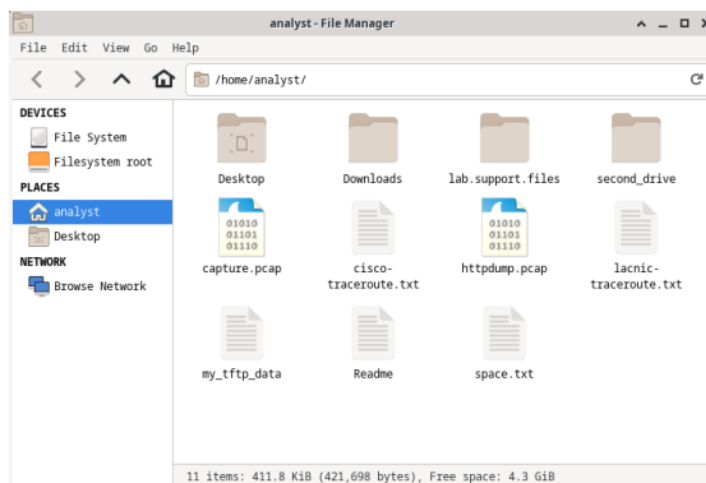
3. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM.

Username : **Admin**

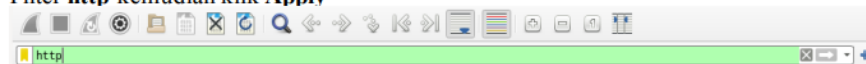
Password : **Admin**

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 **passw**

```
Frame 150: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface 0  
Ethernet II, Src: PcsCompu_82:75:df (08:00:27:82:75:df), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117  
Transmission Control Protocol, Src Port: 41156, Dst Port: 80, Seq: 1, Ack: 1, Len: 583  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded
```

8. Merekam Paket HTTPS

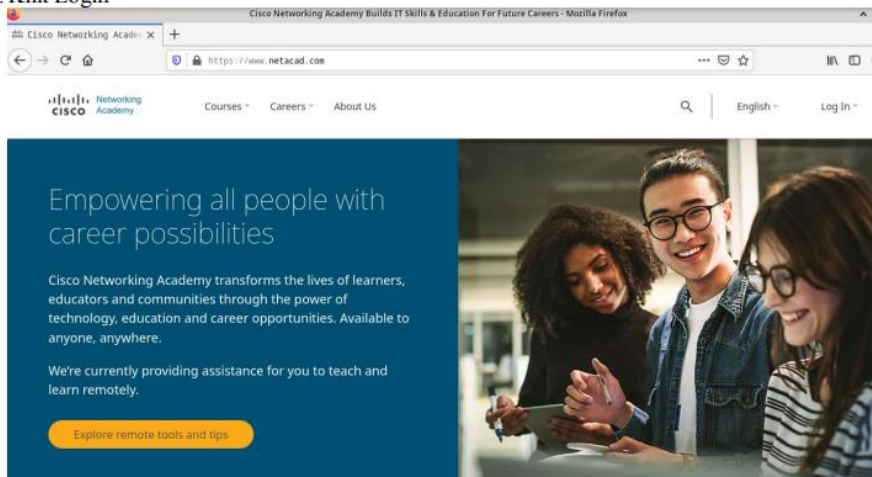
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
```

```
[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.

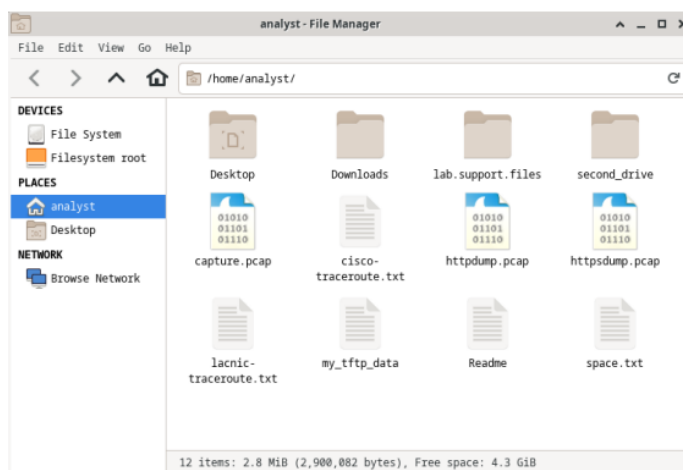
10. Klik Login



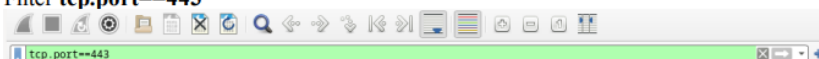
11. Masukkan *username* dan *password* anda

12. Melihat Rekaman Paket HTTPS

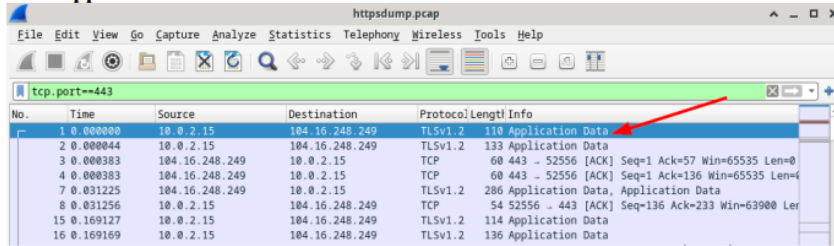
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama `httpsdump.pcap`. File ini terletak pada folder `/home/analyst/`.



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



14. Pilih Application Data



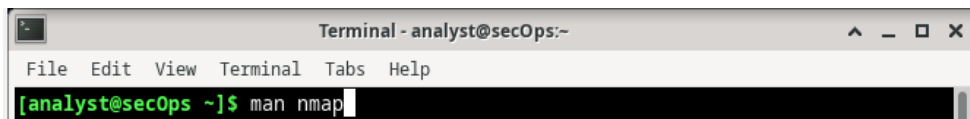
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	104.16.248.249	TLSv1.2	110	Application Data
2	0.000044	10.0.2.15	104.16.248.249	TLSv1.2	133	Application Data
3	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 -> 52556 [ACK] Seq=1 Ack=57 Win=65535 Len=0
4	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 -> 52556 [ACK] Seq=1 Ack=136 Win=65535 Len=0
7	0.031225	104.16.248.249	10.0.2.15	TLSv1.2	286	Application Data, Application Data
8	0.031256	10.0.2.15	104.16.248.249	TCP	54	52556 -> 443 [ACK] Seq=136 Ack=233 Win=63900 Len=0
15	0.169127	10.0.2.15	104.16.248.249	TLSv1.2	114	Application Data
16	0.169169	10.0.2.15	104.16.248.249	TLSv1.2	136	Application Data

15. Analisislah hasil yang didapatkan

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

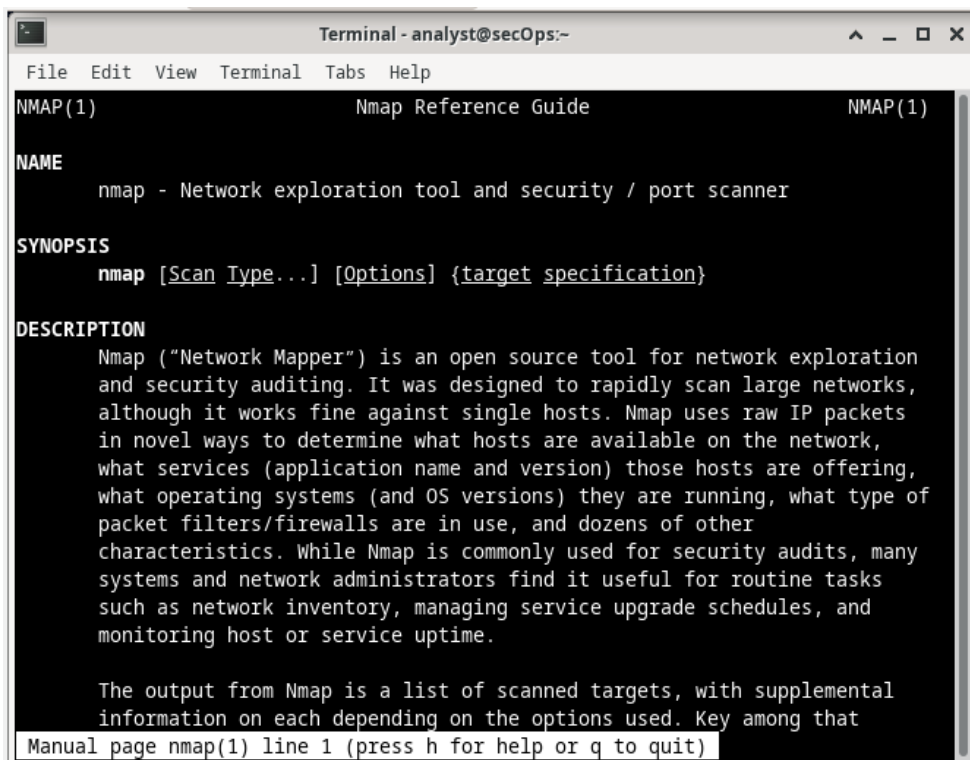
E. Hasil dan Pembahasan

- Unit 2
 - Masuk ke VM Workstation dan pergi ke terminal lalu ketik berikut



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ man nmap
```

- Maka akan muncul manual seperti berikut yang terdiri dari 3175 lines



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


- Apa itu Nmap?

Nmap (Network Mapper) adalah sebuah perangkat lunak untuk melakukan pemindaian jaringan dan pengenalan perangkat yang terhubung ke dalam jaringan tersebut. Nmap dapat digunakan untuk mengetahui informasi seperti host yang aktif, jenis sistem operasi yang digunakan, layanan yang aktif, dan port yang terbuka pada host tersebut.

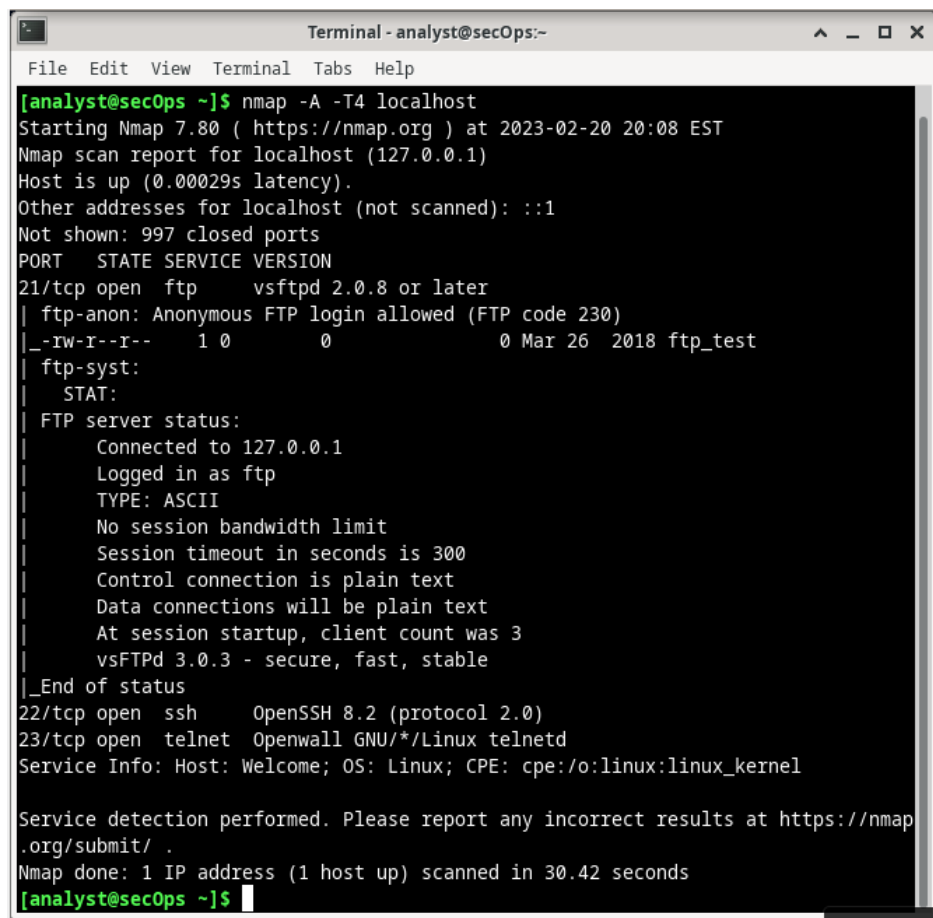
Nmap dapat dijalankan pada sistem operasi Windows, Linux, dan macOS. Selain itu, Nmap juga dapat digunakan untuk melakukan berbagai macam tugas seperti pemindaian port, enumerasi layanan, mengidentifikasi jenis sistem operasi, dan analisis keamanan jaringan.

Nmap sering digunakan oleh administrator jaringan dan profesional keamanan untuk membantu dalam pemantauan dan pengawasan jaringan, serta membantu dalam mengidentifikasi masalah keamanan dan mengambil tindakan yang diperlukan untuk mencegah serangan terhadap jaringan.

- Apa fungsi dari Nmap? Diantaranya adalah :

- Pemindaian port: Nmap dapat digunakan untuk memindai port pada host atau jaringan. Hal ini dapat membantu administrator jaringan untuk memastikan bahwa port yang diperlukan untuk layanan dan aplikasi tertentu telah terbuka dan dapat diakses.
- Identifikasi jenis sistem operasi: Nmap dapat mengidentifikasi jenis sistem operasi yang digunakan pada host atau jaringan. Informasi ini dapat membantu administrator jaringan dalam melakukan konfigurasi yang tepat dan memastikan bahwa sistem operasi yang digunakan aman.
- Analisis keamanan jaringan: Nmap dapat digunakan untuk melakukan analisis keamanan jaringan dengan memeriksa apakah ada celah keamanan atau port yang tidak terlindungi. Hal ini dapat membantu administrator jaringan untuk meningkatkan keamanan jaringan dan mencegah serangan dari pihak yang tidak bertanggung jawab.
- Pemantauan jaringan: Nmap dapat digunakan untuk memantau jaringan secara berkala untuk memastikan bahwa semua host dan layanan yang terhubung tetap aktif dan aman.

- Setelah membaca manual, coba port scanning menggunakan nmap



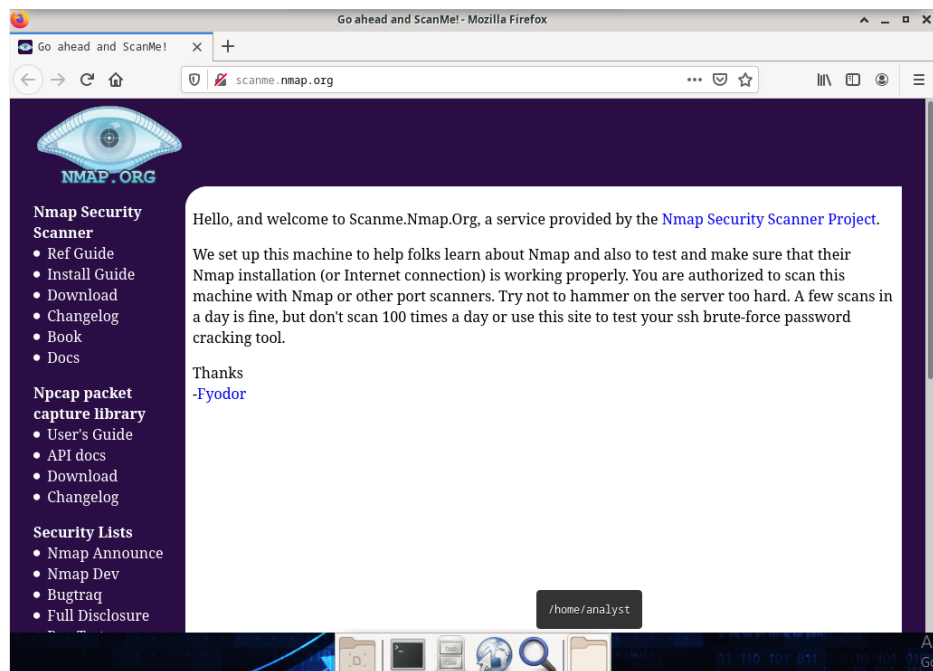
```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:08 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00029s 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 3
|   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

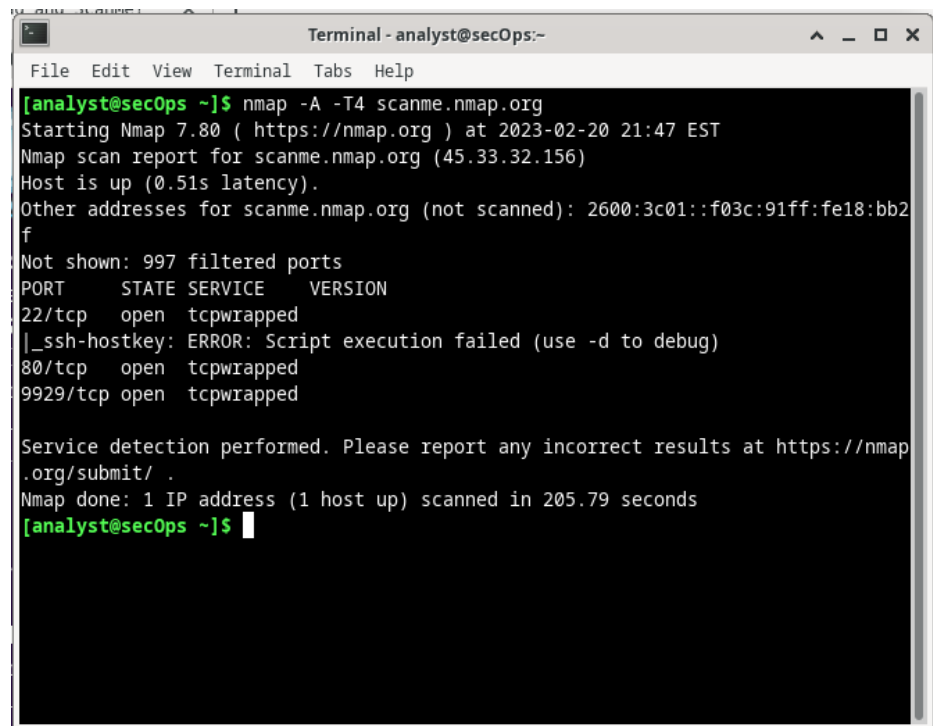
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.42 seconds
[analyst@secOps ~]$
```

- Port dan layanan apa yang terbuka?
Ada 3, yaitu port 21 ftp, 22 ssh, dan 23 telnet
- Software apa yang digunakan pada port yang terbuka tersebut?
Software yang digunakan ada 3, yaitu vsftpd 2.0.8, OpenSSH 8.2(protocol 2.0), Openwall GNU/*/Linux telnetd

- Lalu buka scanme.org pada browser di VM



- Saat scanme.org masih aktif, coba scanme lagi di terminal



- Port dan layanan apa yang terbuka?

Ada 3, yaitu 22/tcp, 88/tcp, 9929/tcp dengan layanan yang sama yaitu tcpwrapped

- Berapa alamat IP server?

Tidak ada

- Apa sistem operasi yang digunakan oleh server?

Tidak terlihat

- Unit 3

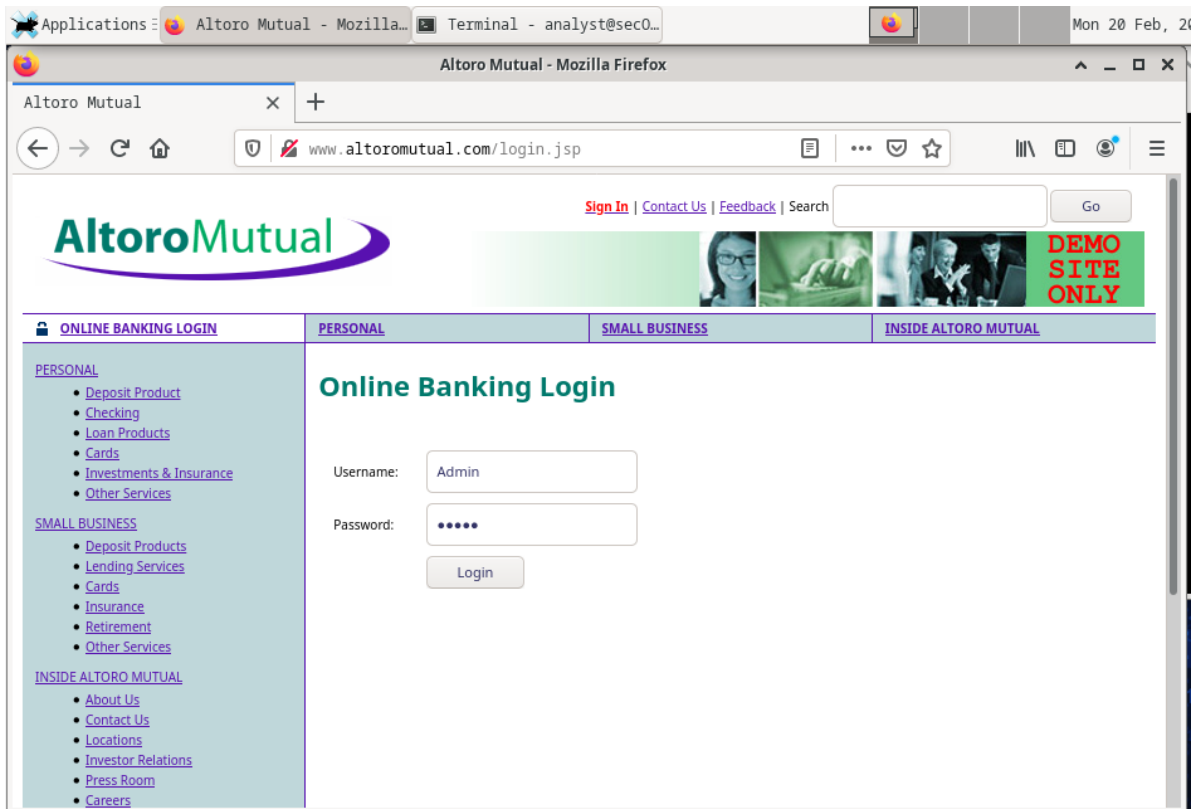
- Sama seperti unit 2, masuk ke VM dan klik terminal lalu lakukan TCP dump seperti dibawah

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[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:f9:2b:ff brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86376sec preferred_lft 86376sec
    inet6 fe80::a00:27ff:f92b:64 scope link
        valid_lft forever preferred_lft forever
[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
^C441 packets captured
527 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```

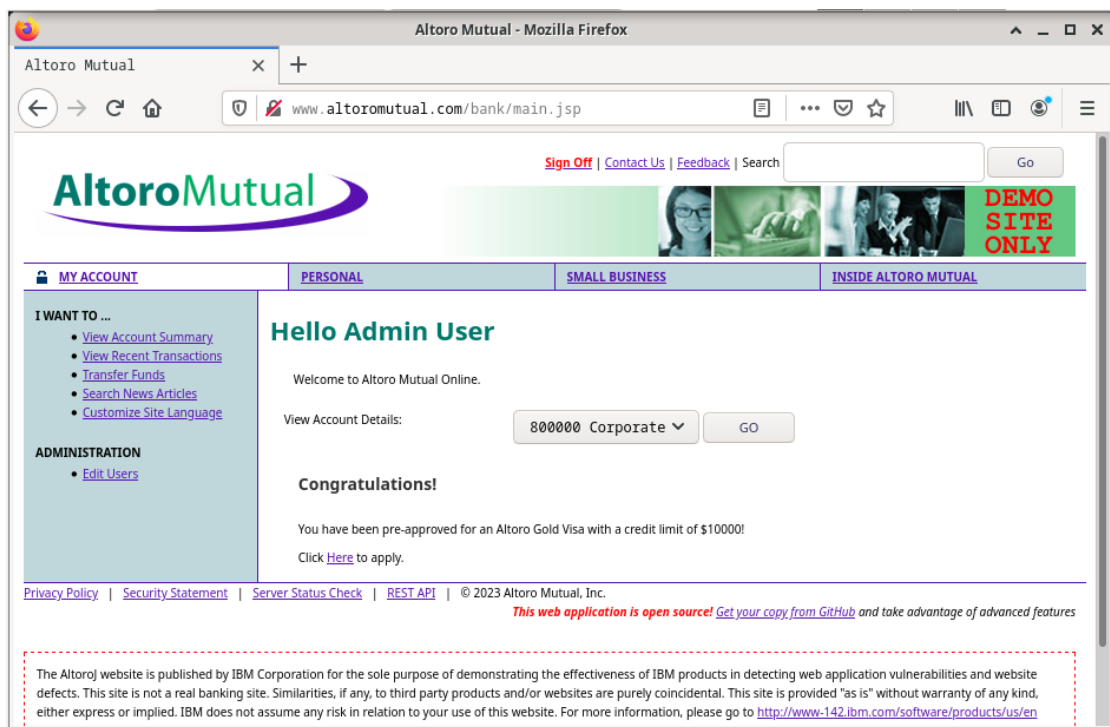
- Koneksikan komputer ke internet (dalam kasus ini Wifi UGM memblokir koneksi VM)

```
[analyst@secOps ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=80.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=71.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=55 time=74.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=55 time=67.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=55 time=64.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=55 time=65.1 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 64.362/70.588/80.730/5.741 ms
[analyst@secOps ~]$
```

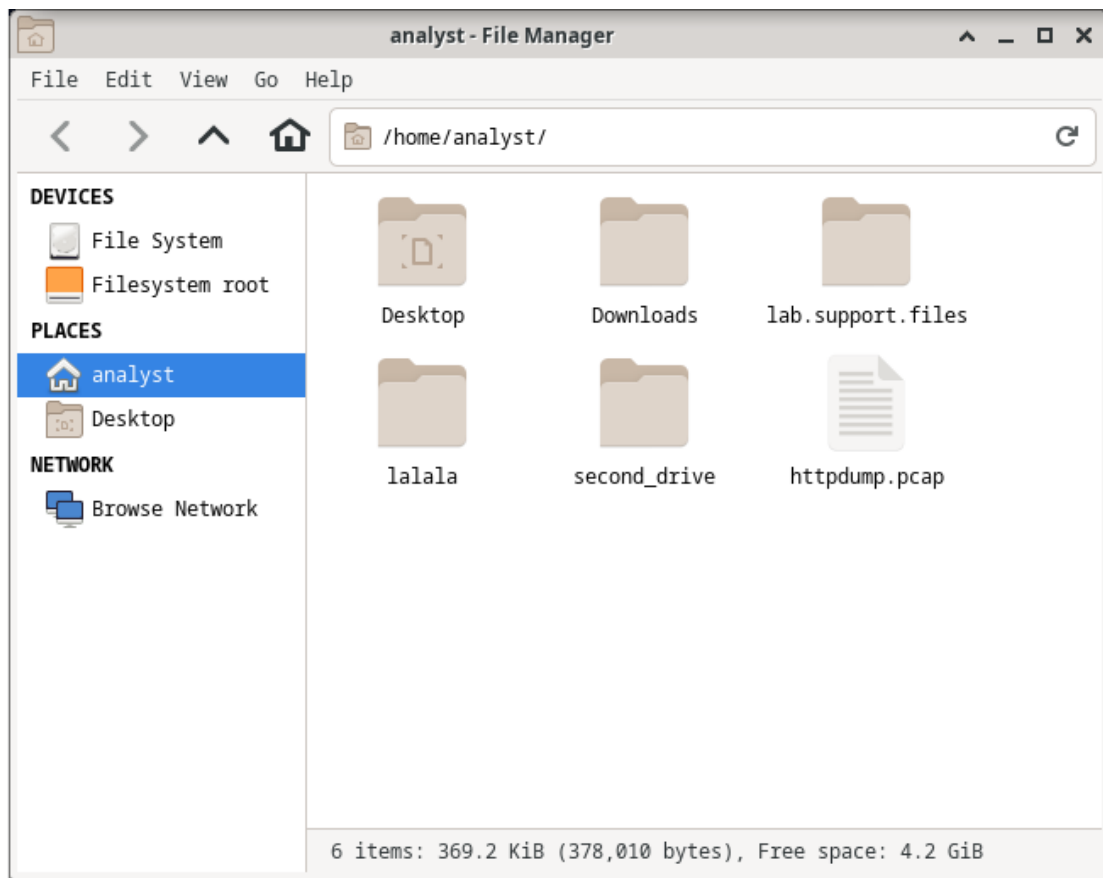
- Buka website <http://www.altoromutual.com/login.jsp> dan login



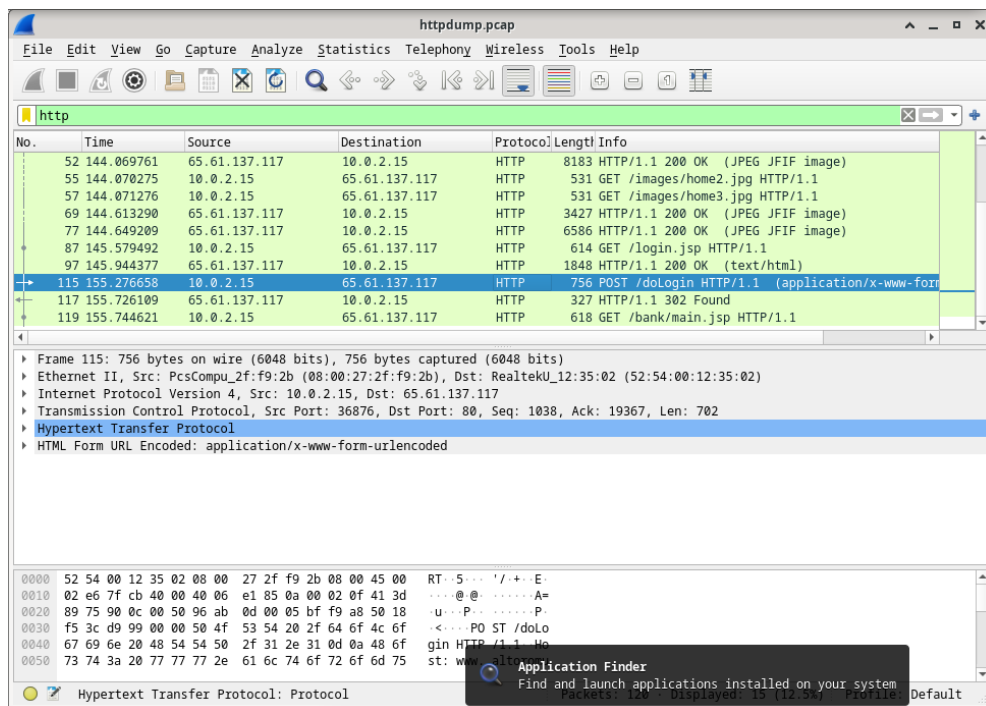
- Berikut tampilan ketika sudah login



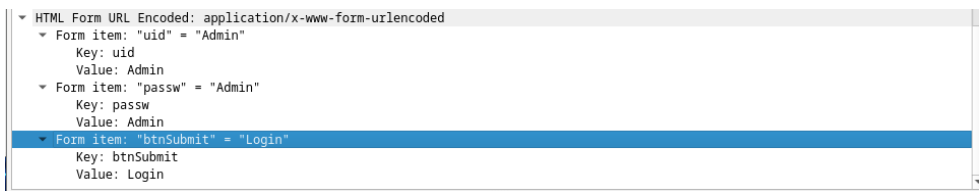
- Cari TCPdump di Home/Analyst atau File Manager



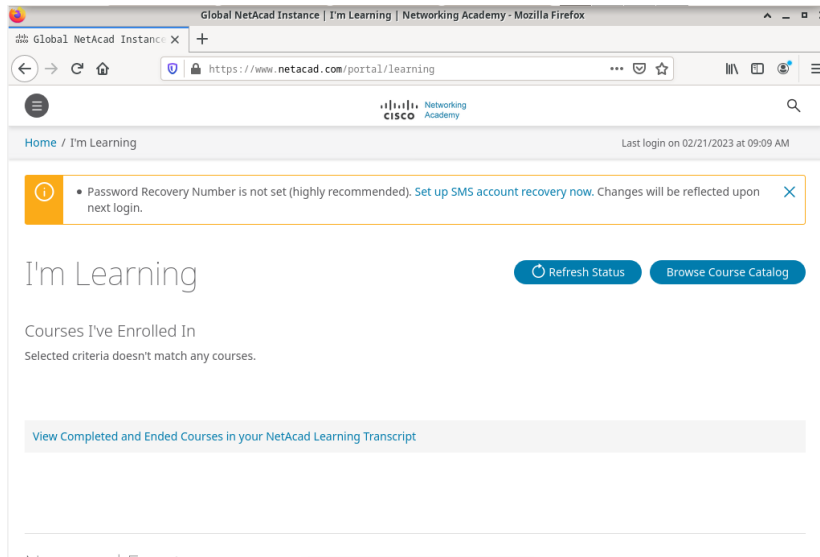
- Klik httpdump.pcap, lalu filter http dan pilih POST



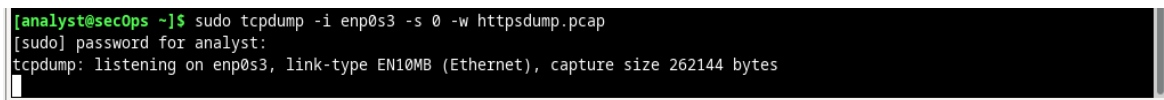
- Lakukan analisis terhadap UID dan Password



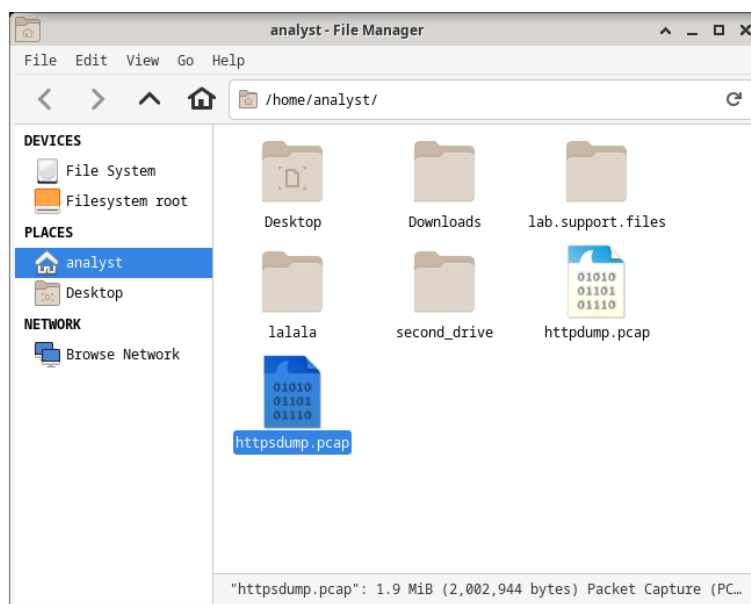
- Setelah itu buka website yang bertipe https dalam kasus ini netacad



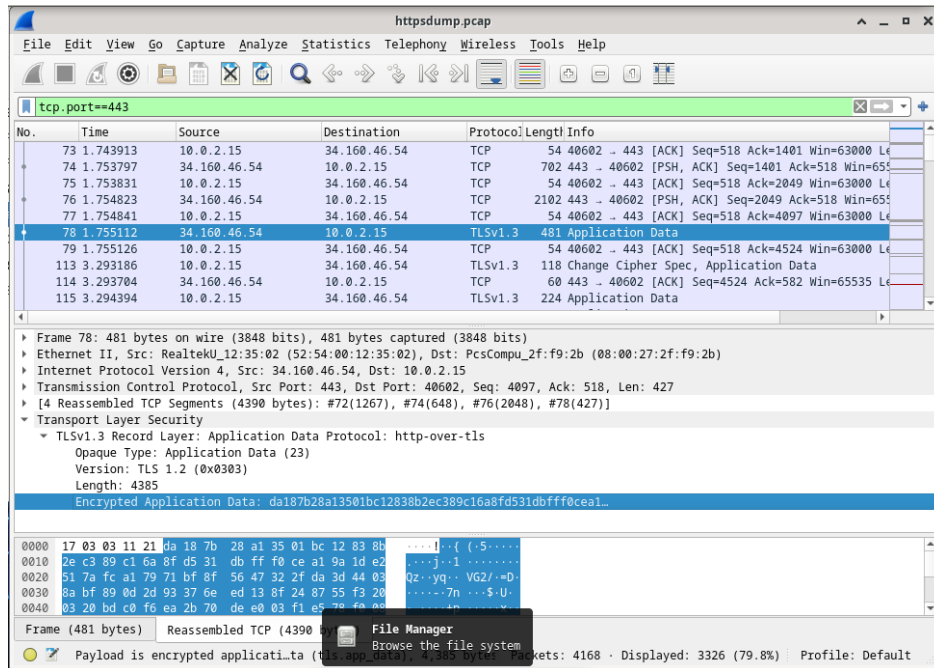
- Ganti command TCPdump menjadi https sebagai berikut :



- Buka file httpsdump.pcap di Home/Analyst juga



- Filter tcp port==443 dan pilih hasil filter dengan info application data dan analisis hasil



Pembahasan :

- Unit 2

Pada unit 2, hal yang pertama kali dilakukan adalah mengetahui apa itu Nmap dan bagaimana cara kerjanya melalui manual, setelah itu port scanning atau eksplorasi Nmap dilakukan kepada localhost dengan menggunakan command “nmap -A -T4 localhost” lalu akan muncul port dan layanan yang terbuka serta software yang digunakan. Begitu juga pada Langkah-langkah berikutnya, yaitu mengubah localhost menjadi scanme.org sehingga eksplorasi Nmap dilakukan pada scanme.org server dan bukan localhost

- Unit 3

Pada unit 3, praktik yang dilakukan adalah membandingkan traffic packet HTTP dan HTTPS menggunakan software wireshark. Dari hasil yang didapatkan, website bertipe HTTPS jauh lebih aman dibandingkan dengan website yang menggunakan HTTP dikarenakan website yang menggunakan HTTPS sudah mengenkripsi data pengguna sehingga tidak menampilkan Username dan Password pengguna, berbeda dengan HTTP yang tidak mengenkripsi datanya sehingga data pengguna langsung terlihat begitu saja

F. Kesimpulan

Hal-hal yang dapat disimpulkan ialah :

- Nmap dan Wireshark merupakan 2 contoh utilities yang dapat digunakan untuk mencari celah keamanan
- HTTPS jauh lebih aman dibandingkan dengan HTTP

G. Daftar Pustaka

- Zakaria Muchammad. (2022). Pengertian NMAP Beserta Fungsi dan Cara Kerjanya yang Perlu Diketahui. <https://www.nesabamedia.com/pengertian-nmap/>
- Saputro Nur. (2022). Kenali Pengertian Wireshark Beserta Fungsi dan Cara kerjanya, Lengkap!. <https://www.nesabamedia.com/pengertian-wireshark/#:~:text=Funksi%20Wireshark&text=Cara%20kerjanya%20yaitu%20dengan%20'menangkap,hasil%20capture%20secara%20real%2Dtime.>