

LAPORAN PRAKTIKUM
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 2
EKSPLORASI NMAP & PEMANTAUAN TRAFIK HTTP DAN HTTPS
DENGAN MENGGUNAKAN WIRESHARK



DI SUSUN OLEH

Nama	:	Prama Yugas Nurhakim
NIM	:	21/474280/SV/18892
Hari, Tanggal	:	Selasa, 21 Februari 2023
Kelas	:	A

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA
2023

A. Tujuan

1. Mengesplorasi Nmap
2. Melakukan Scan ke Port yang terbuka
3. Merekam dan menganalisis trafik http
4. Merekam dan menganalisis trafik https

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.

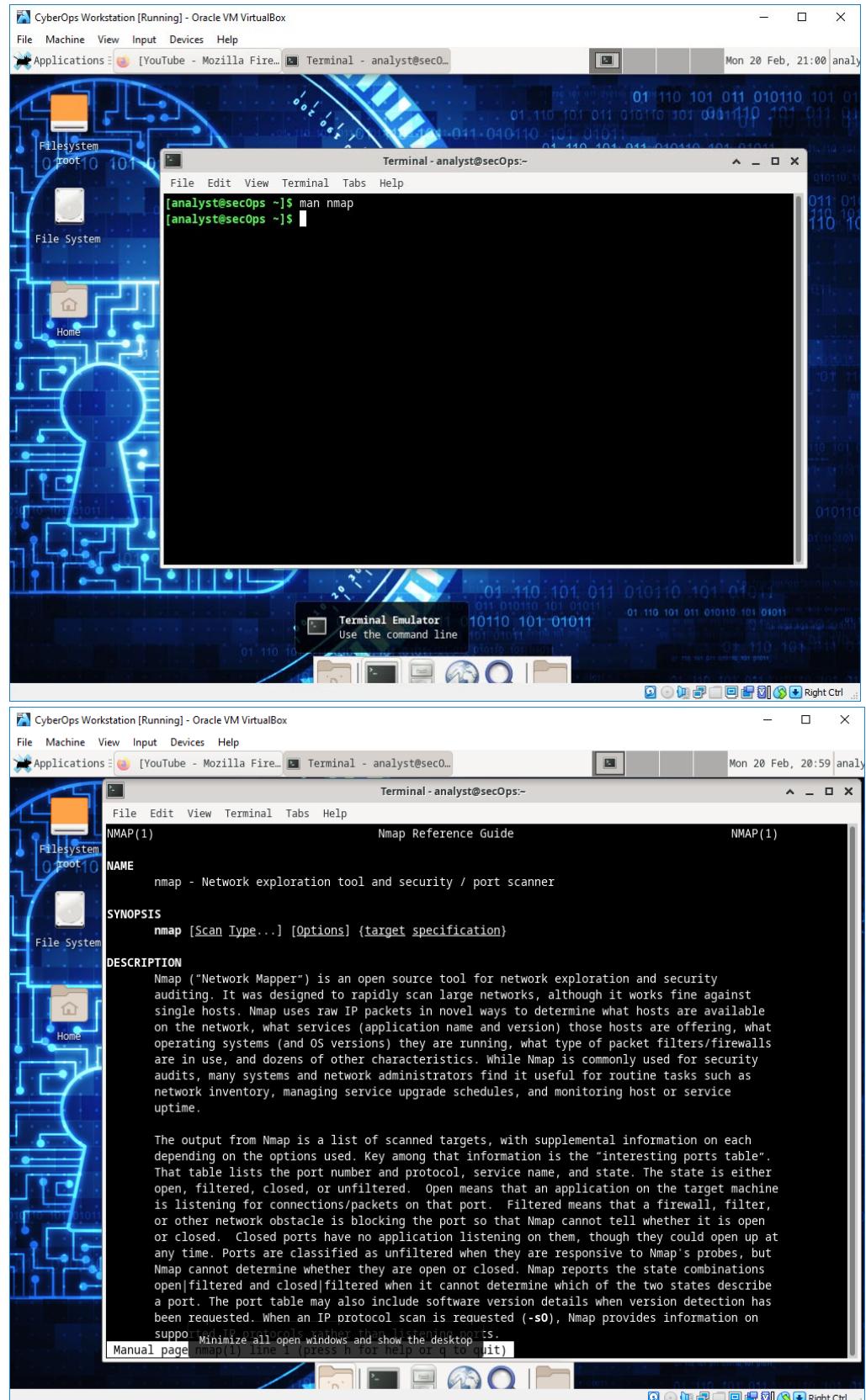
HyperText Transfer Protocol (HTTP) adalah protokol lapisan aplikasi yang menyajikan data melalui browser web. Dengan HTTP, tidak ada perlindungan untuk pertukaran data antara dua perangkat yang berkomunikasi. Dengan HTTPS, enkripsi digunakan melalui algoritma matematika. Algoritma ini menyembunyikan 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

- 1) CyberOps Workstation virtual machine
- 2) Koneksi Internet

D. Instruksi Kerja

1. Start VM Workstation dan buka terminal lalu lakukan eksplorasi Nmap dengan ketik man nmap di terminal



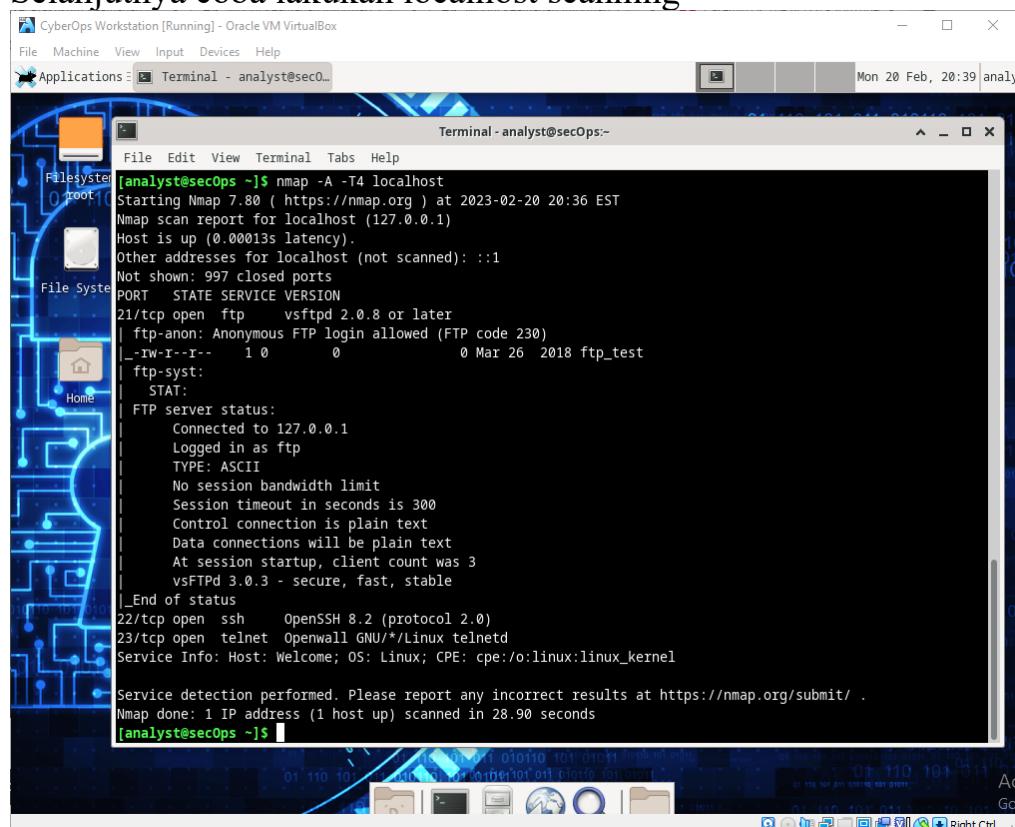
1) Apa itu Nmap?

NMAP adalah singkatan dari Network Mapper yang merupakan sebuah tool atau alat yang bersifat open source. Alat ini hanya digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan.

2) Apa fungsi dari Nmap?

Fungsi NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Meskipun begitu, NMAP juga mampu bekerja pada host tunggal. Cara kerjanya adalah dengan menggunakan IP raw yang berfungsi untuk menentukan mana host yang tersedia di dalam jaringan. Fungsi kedua dari adanya NMAP adalah untuk melakukan scanning terhadap suatu port jaringan komputer. Port adalah nomor yang berguna untuk membedakan antara aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer.

2. Selanjutnya coba lakukan localhost scanning

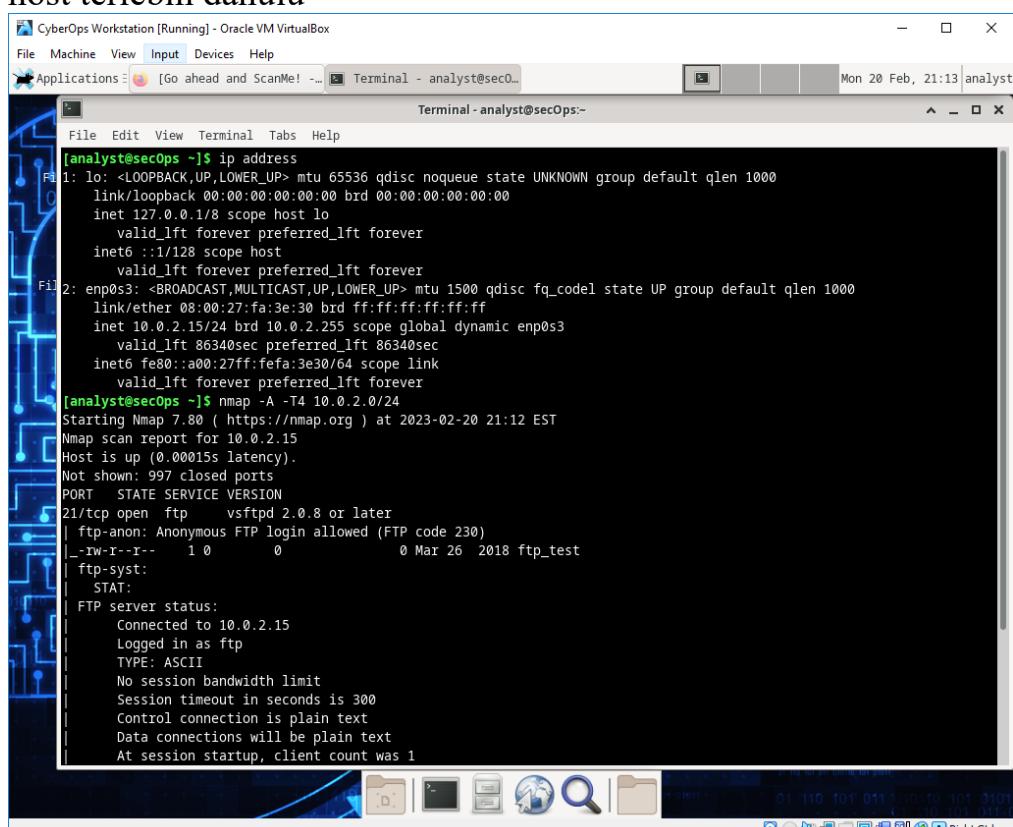


The screenshot shows a Linux desktop environment with a terminal window titled "Terminal - analyst@secOps:~". The terminal displays the output of the Nmap command "nmap -A -T4 localhost". The output shows that the host is up (0.00013s latency). It lists various ports and services: port 21/tcp is open (vsftpd 2.0.8 or later), port 22/tcp is open (OpenSSH 8.2), and port 23/tcp is open (Openwall GNU/*Linux telnetd). Service detection indicates the host is a Linux system. The terminal window is part of a desktop interface with icons for file system, root, and home.

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:36 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s 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 28.90 seconds
[analyst@secOps ~]$
```

- 1) Port dan layanan apa yang terbuka?
21/tcp: ftp, 22/tcp: ssh, 23/tcp: telnet.
 - 2) Software apa yang digunakan pada port yang terbuka tersebut?
ftp : vsftpd, ssh : OpenSSH, telnet : Openwall GNU/Linux telnetd.
3. Yang ketiga lakukan Network scanning dilakukan dengan cek ip host terlebih dahulu



```

CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications [Go ahead and ScanMe! -... Terminal - analyst@secOps...
Terminal - analyst@secOps... Mon 20 Feb, 21:13 analyst
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:fa:3e:30 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86340sec preferred_lft 86340sec
    inet6 fe80::a00:27ff:fea:3e30/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 21:12 EST
Nmap scan report for 10.0.2.15
Host is up (0.00015s 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 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
Nmap done at 2023-02-20 21:12 (0.00s)

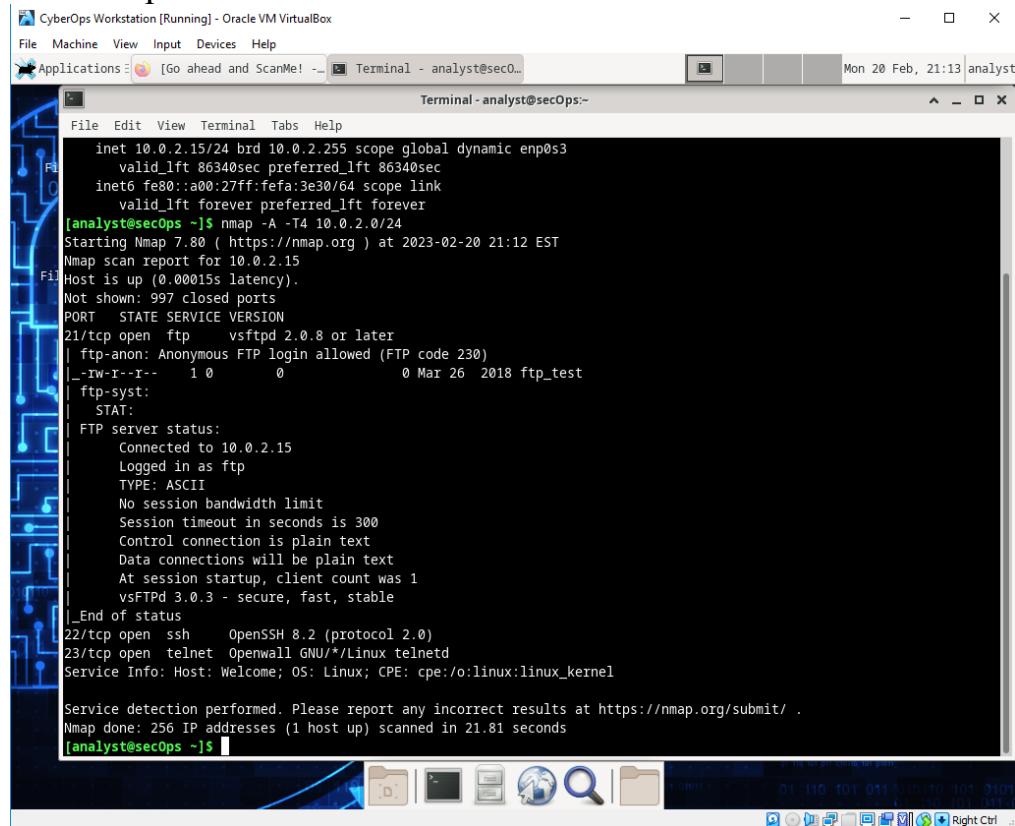
```

- 1) Berapakah alamat IP dan subnet mask dari PC host?

IP address = 10.0.2.15/24

subnet mask = 255.255.255.0

4. Lanjutkan dengan lakukan port scanning dengan Nmap dengan cara nmap -A -T4 10.0.2.0/24



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~". The window displays the results of an Nmap scan. The output includes network interface information, the command used (nmap -A -T4 10.0.2.0/24), and a detailed report of open ports, services, and versions. Key findings include an open FTP service (vsftpd 2.0.8 or later) and an open SSH service (OpenSSH 8.2). The terminal window is part of a desktop environment with a blue circuit board background.

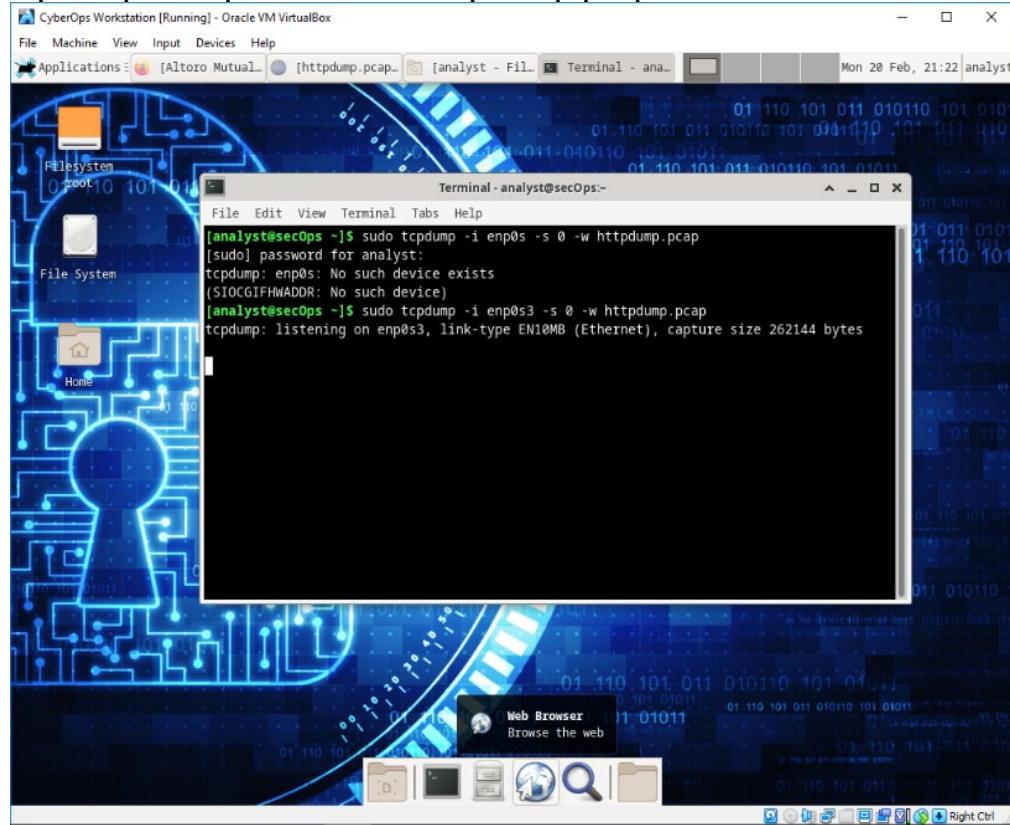
```
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
      valid_lft 86340sec preferred_lft 86340sec
inet6 fe80::a00:27ff:fe30:64 scope link
      valid_lft forever preferred_lft forever
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 21:12 EST
Nmap scan report for 10.0.2.15
Host is up (0.00015s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.0.8 or later
|_T2-I--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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 21.81 seconds
[analyst@secOps ~]$
```

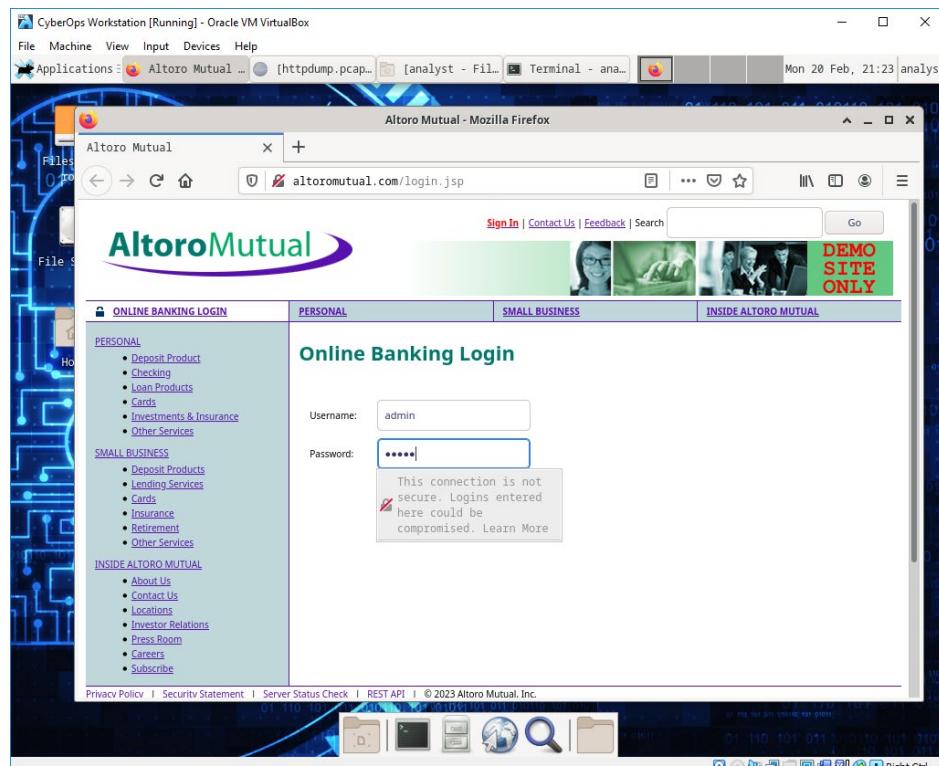
- 1) Berapakah jumlah host yang terdeteksi?
1 host

Unit 3

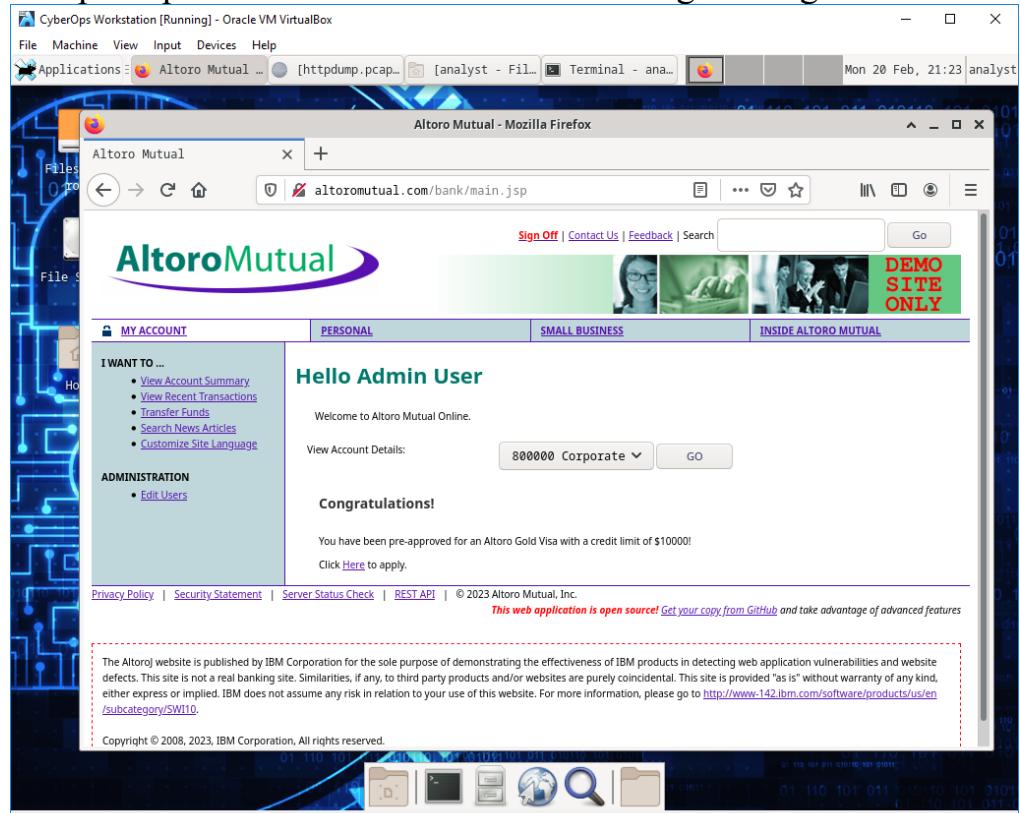
- Lakukan pengecekan alamat IP Setelah itu lanjutkan dengan sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap



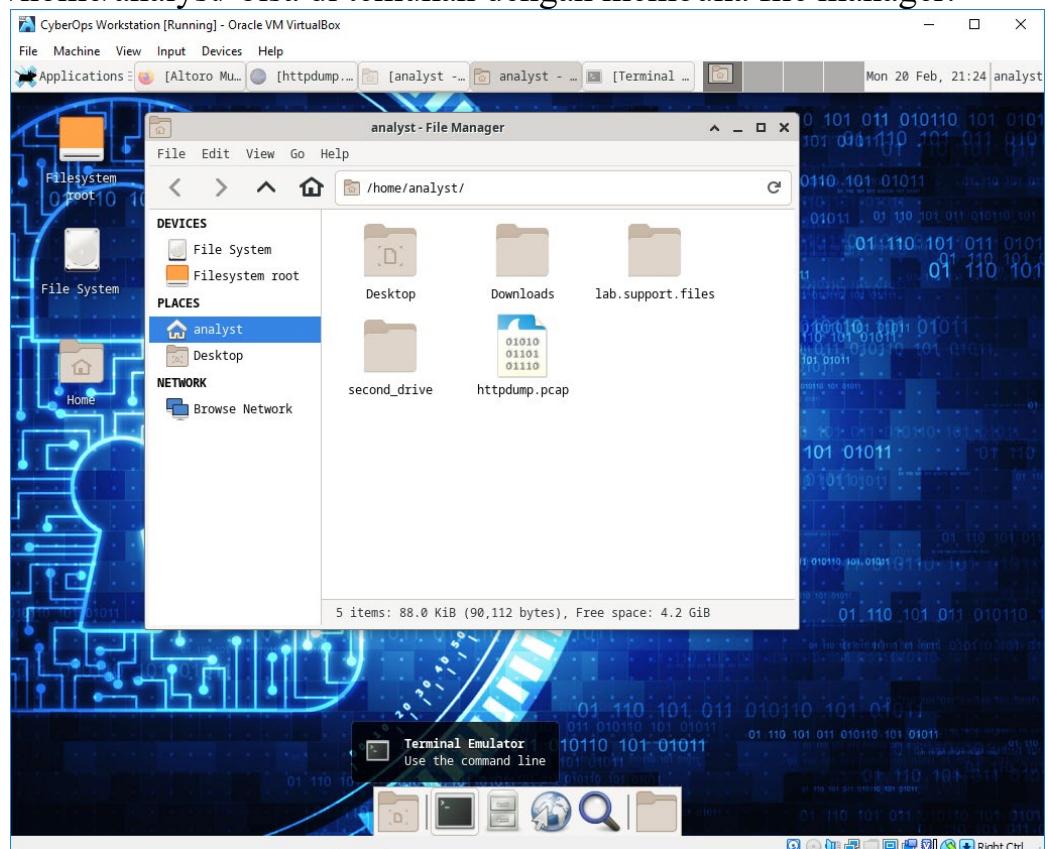
- Buka browser pada CyberOps Workstation VM lalu masuk ke web altoromutual Setelah itu login dengan isikan username dan password untuk admin



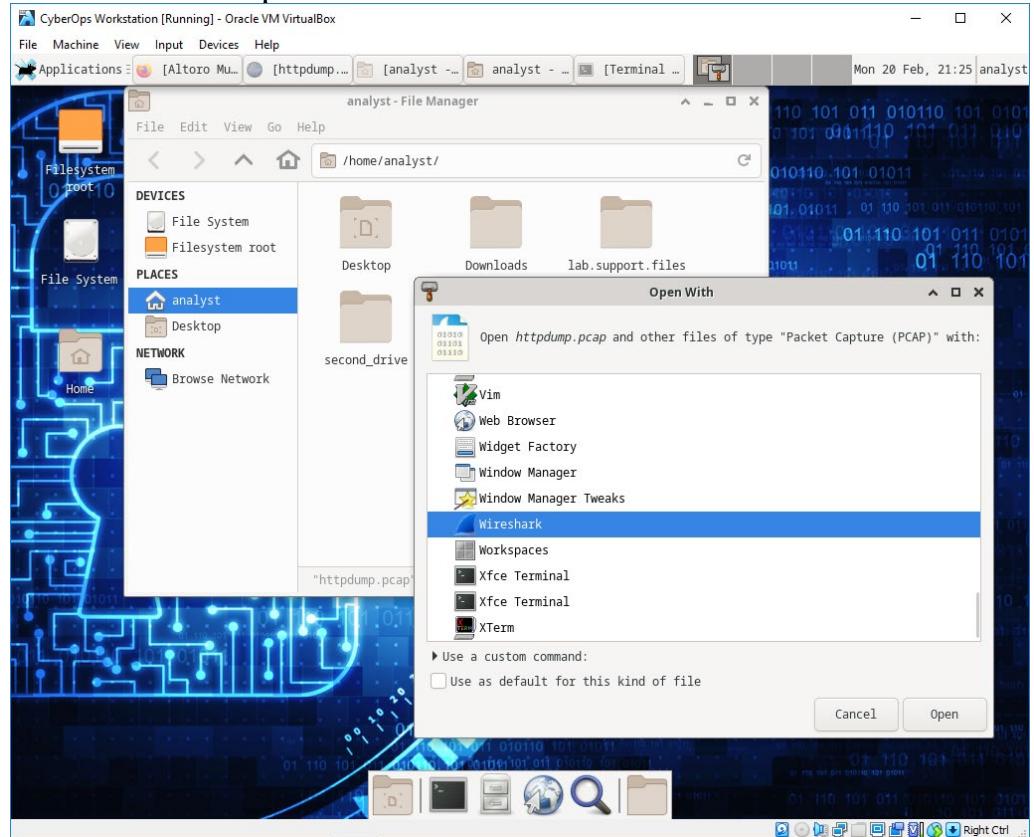
7. Tampilan pada web AltoroMutual Setelah login sebagai admin



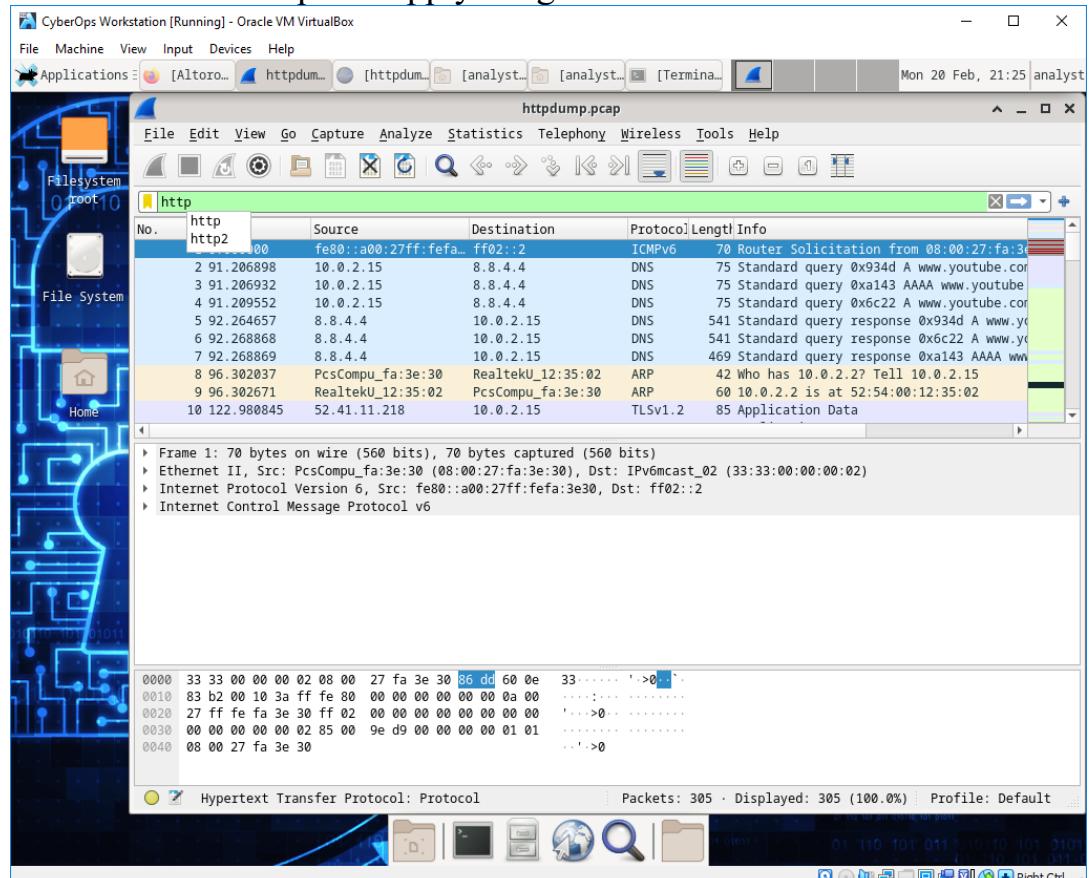
8. Langkah selanjutnya adalah merekam paket HTTP. Tcpdump tersimpan kedalam file bernama httpdump.pcap. terletak pada folder /home/analyst/ bisa di temukan dengan membuka file manager.



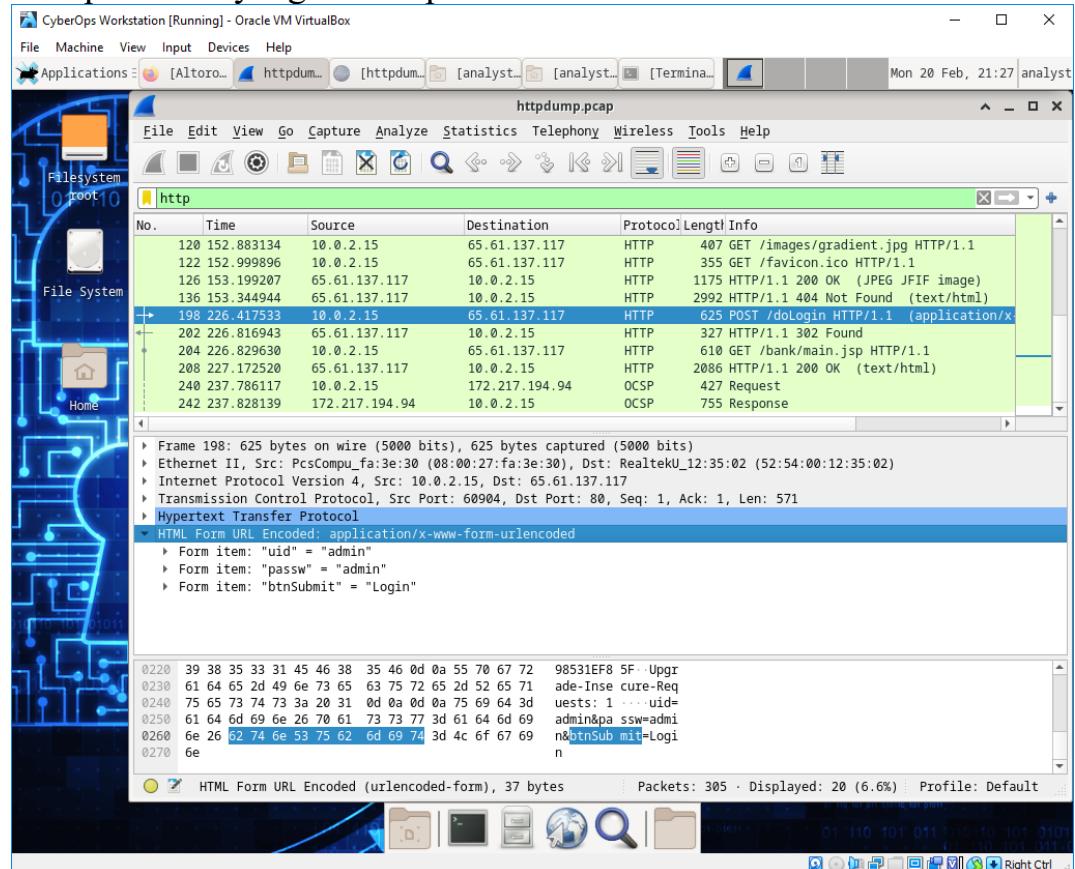
9. Lalu pada httpdump.pcap lakukan perintah open with dan pilih wirershark dan open



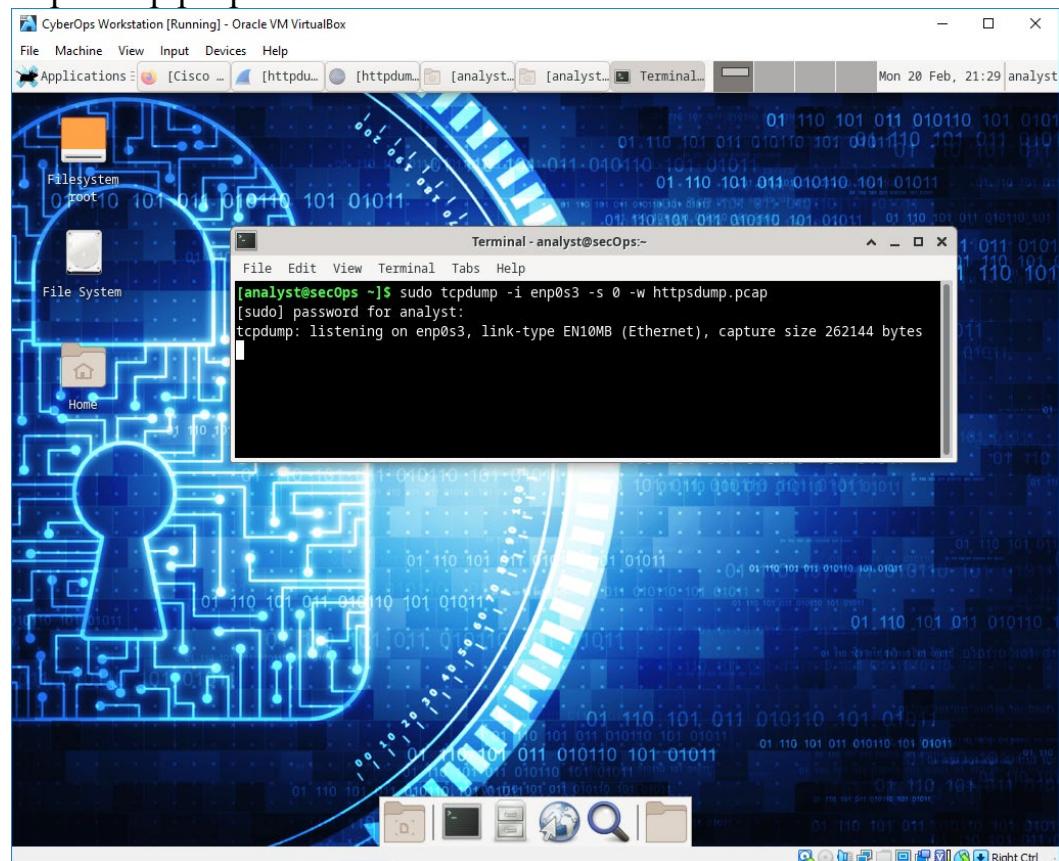
10. Pada filter ketik http lalu apply dengan cara enter



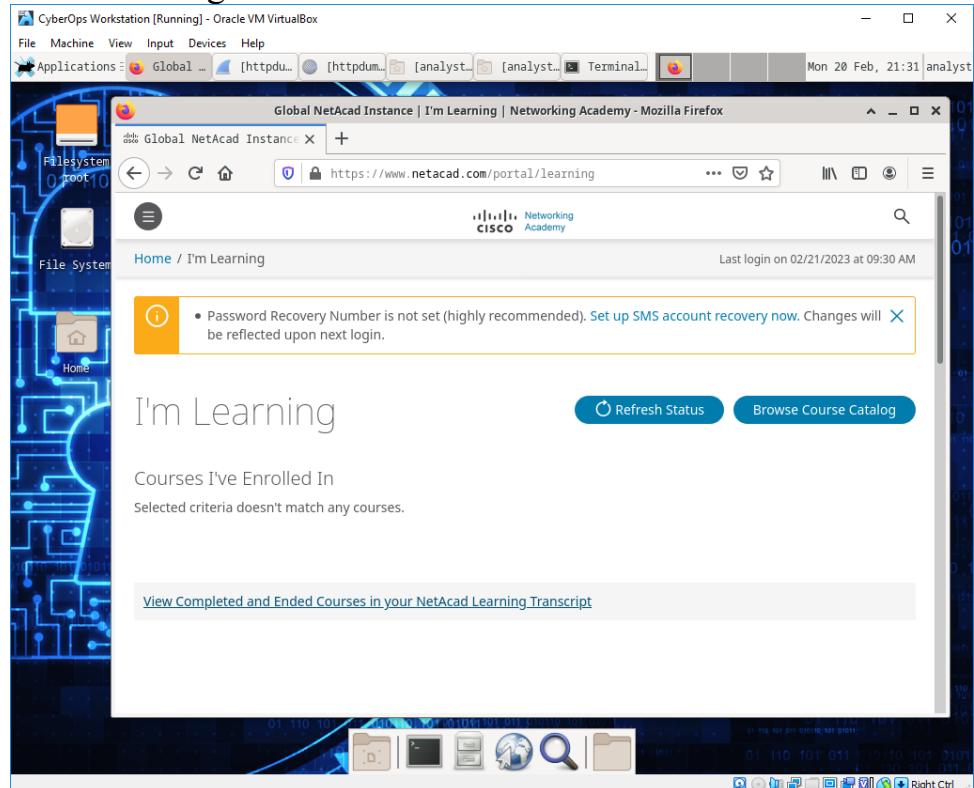
11. Cari pada info yang menampilkan POST



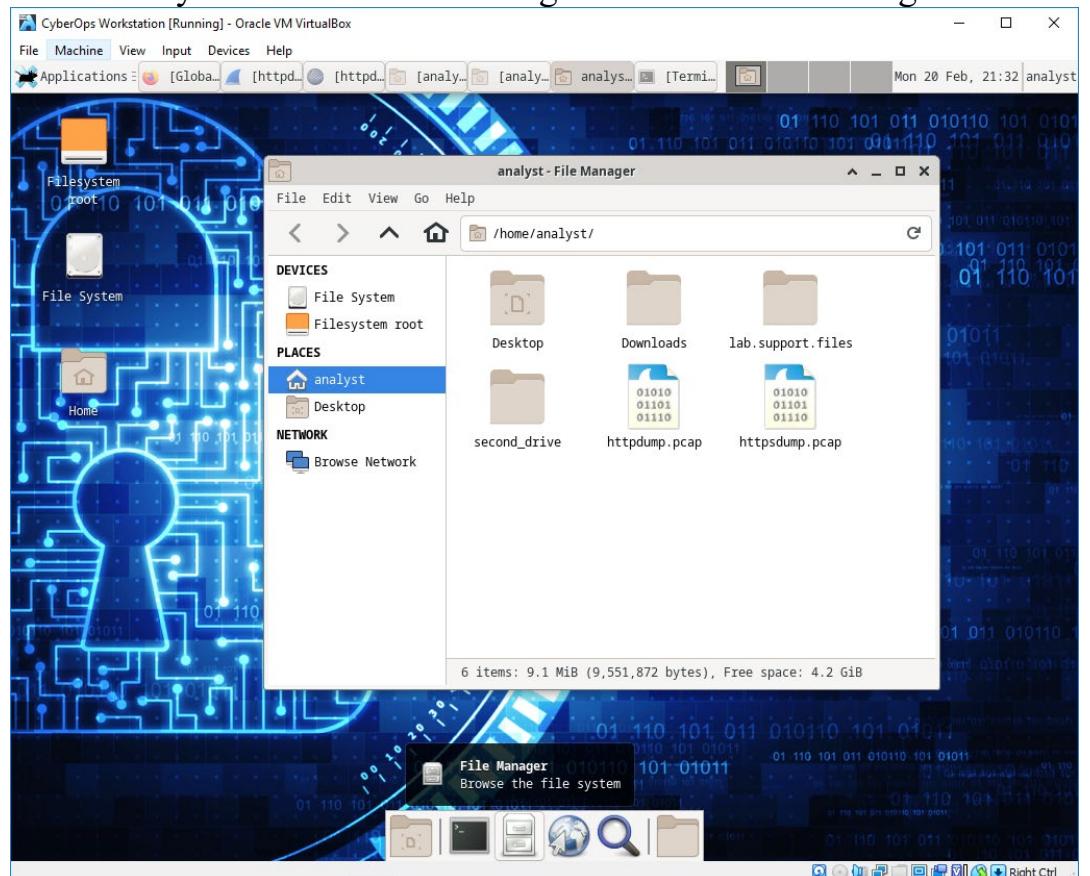
12. Lanjutkan dengan HTTPS dengan sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap



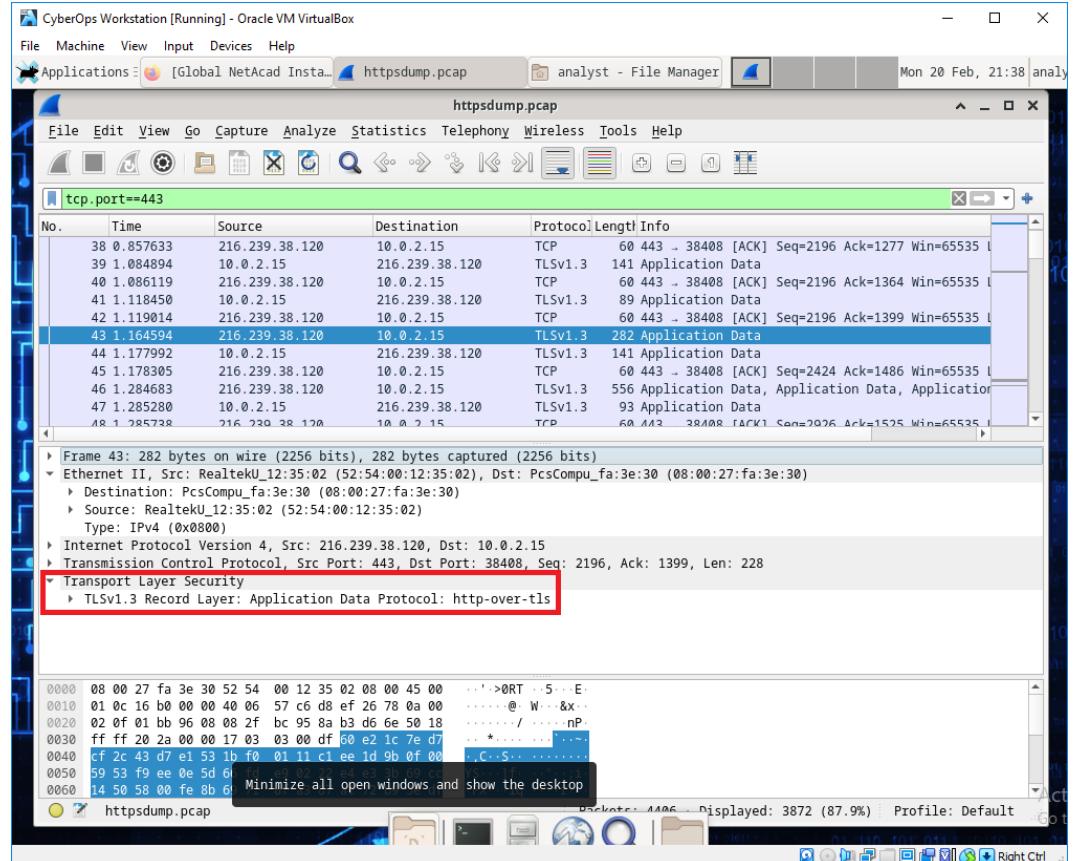
13. Setelah itu login ke Netacad



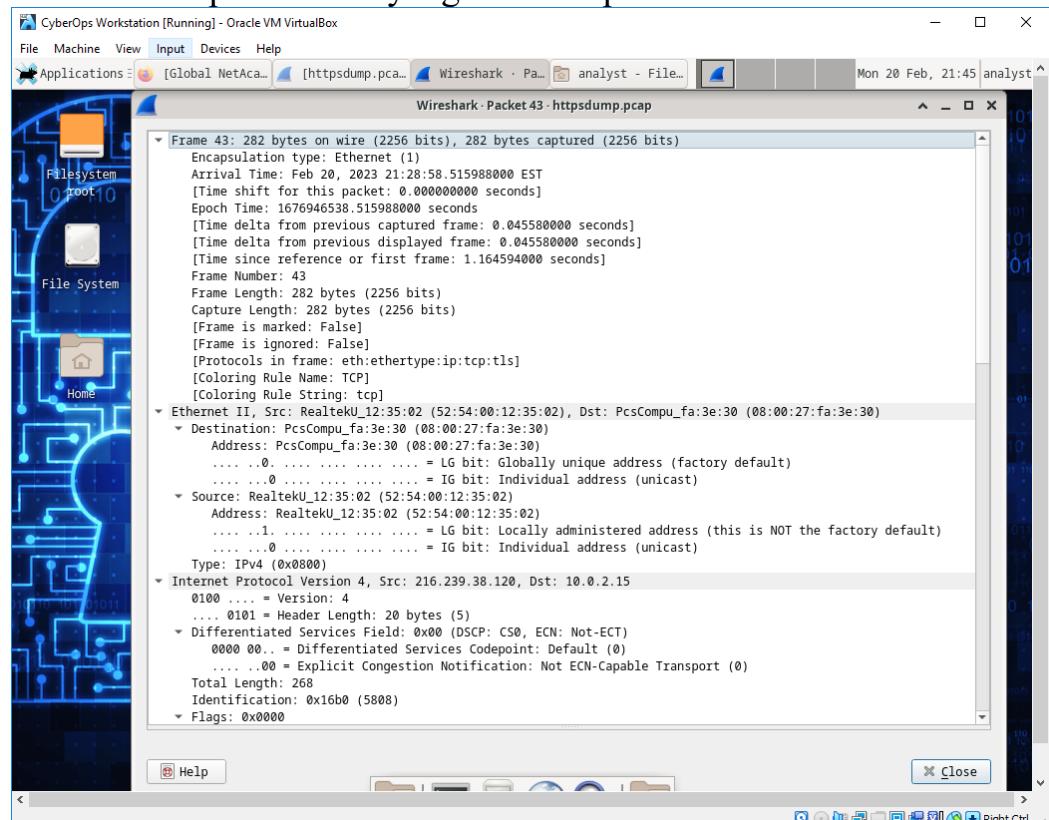
14. Selanjutnya adalah merekam paket HTTPS. Tcpdump tersimpan kedalam file bernama httpSdump.pcap. terletak pada folder /home/analyst/ bisa di temukan dengan membuka file manager

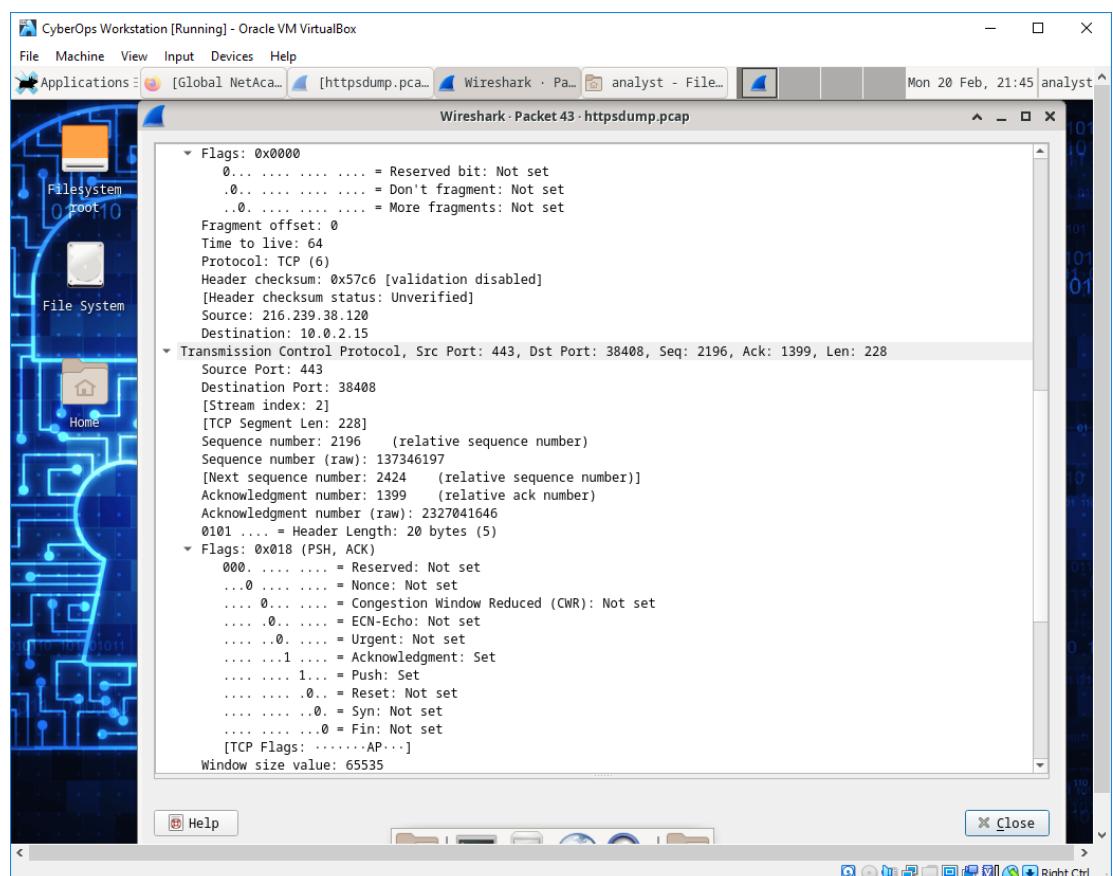
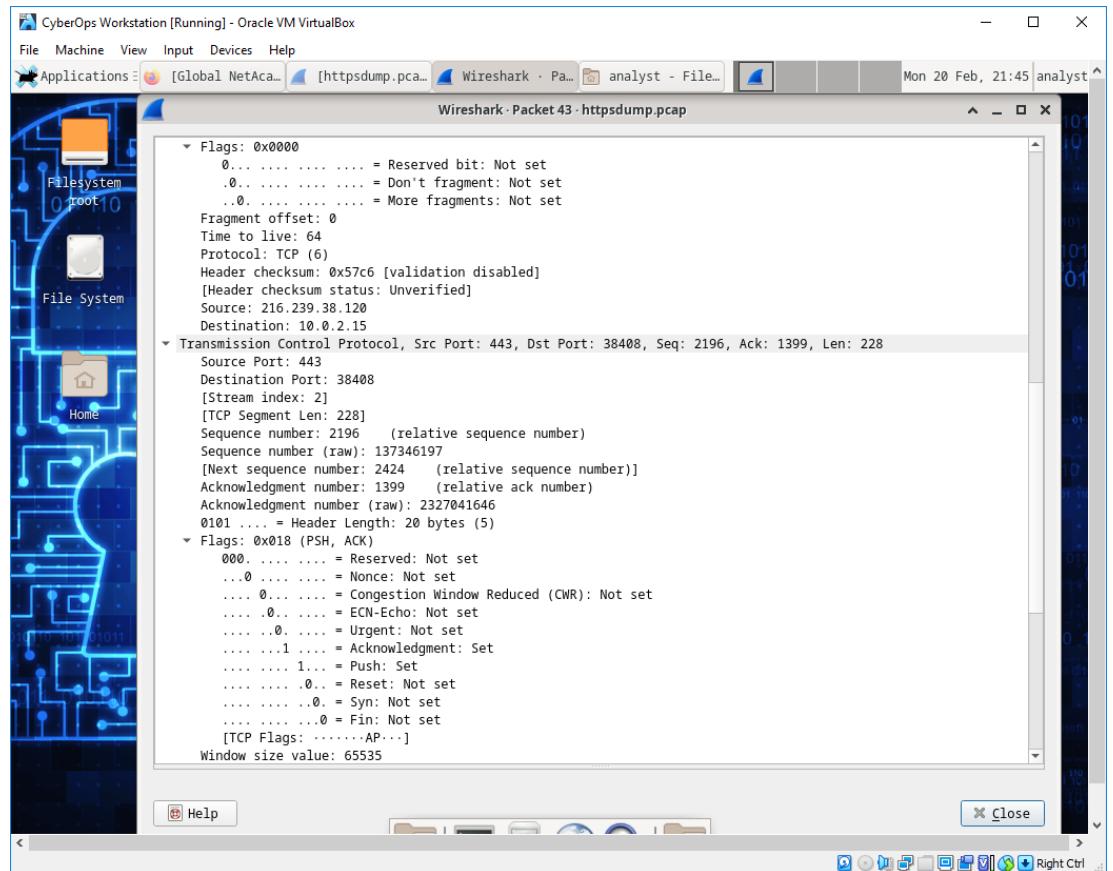


15. Jika sudah dibuka menggunakan wireshark pada filter cari `tcp.port==443` setelah itu pilih info yang menampilkan application data.



16. Berikut merupakan hasil yang bisa didapatkan.





E. Analisis

Network Mapper atau biasa disebut dengan nmap adalah tool open source yang digunakan untuk membantu mengaudit serta mengeksplorasi keamanan suatu jaringan. Beberapa fungsi NMAP yang berperan dalam keamanan jaringan. Port discovery, Nmap mampu melakukan scanning dan mendeteksi port-port mana saja yang terbuka pada sebuah jaringan. Network mapping, Menguraikan dan memberikan gambaran sebuah jaringan serta setiap perangkat, port, atau service yang terhubung dengannya. Vulnerability scanning, Menemukan celah-celah keamanan yang kemungkinan dapat dieksloitasi di sebuah jaringan.

Pertemuan kali ini untuk unit 2 berfokus pada eksplorasi Nmap seperti localhost scanning dan juga network scanning, menggunakan nmap -A -T4

- 1) -T4 untuk eksekusi lebih cepat dengan melarang penundaan pemindaian dinamis melebihi 10 ms untuk port TCP
- 2) -A untuk megaktifkan deteksi OS, deteksi versi, pemindaian skrip, dan traceroute

Lanjut pada unit 3 yaitu 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, memerlukan sertifikat SSL/TLS. Terlihat pada hasil praktikum pada HTTP langsung menampilkan uid dan juga password sedangkan pada HTTPS tidak tertampil uid dan juga password.

F. Kesimpulan

Pada praktikum kali ini memiliki kesimpulan :

1. Nmap mampu melakukan scanning dan mendeteksi port-port mana saja yang terbuka pada sebuah jaringan
2. HTTP langsung menampilkan uid dan juga password
3. HTTPS tidak tertampil uid dan juga password.

DAFTAR PUSTAKA

Pengertian NMAP Adalah : Fungsi, Cara Kerja & Penggunaannya. (n.d.).

Www.nesabamedia.com. <https://www.nesabamedia.com/pengertian-nmap/>

Anendya, A. (2023, January 12). *Mencegah Serangan Jaringan Komputer Ilegal dengan Nmap*. Blog Dewaweb.

<https://www.dewaweb.com/blog/nmap-mencegah-jaringan-illegal/>

Valencia, V. N. G. A. P. (2022, February 26). *Pengertian NMAP, Fungsi dan Cara Kerjanya*. DosenIT.com. <https://dosenit.com/software/network-mapper>

Bermain dengan NMAP. (n.d.). Cyber. Retrieved February 27, 2023, from <https://student-activity.binus.ac.id/csc/2021/06/bermain-dengan-nmap/>

Panduan Refensi Nmap (Man Page, bahasa Indonesia). (n.d.). Nmap.org.

Retrieved February 27, 2023, from <https://nmap.org/man/id/index.html>

A, F. (2022, May 11). *Perbedaan HTTP dan HTTPS serta Pengertiannya*. Hostinger Tutorial. <https://www.hostinger.co.id/tutorial/perbedaan-http-dan-https>