

LAPORAN  
Praktikum Keamanan Informasi 1  
Pertemuan Kedua



Disusun Oleh :

Nama : Akbar Mertza Satya Putra  
NIM : 21/482067/SV/19895  
Kelas : RI4AA  
Dosen Pengampu : Anni Karimatul Fauziyyah,  
S.Kom., M.Eng.  
Hari, Tanggal : Selasa, 21 Februari 2023

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

## Unit 2 & 3

### Eksplorasi Nmap

&

Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark

#### A. Tujuan

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

#### B. Landasan Teori

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. Internet access

#### D.

## E. Tugas dan Penyelesaian

### 1. Eksplorasi Nmap

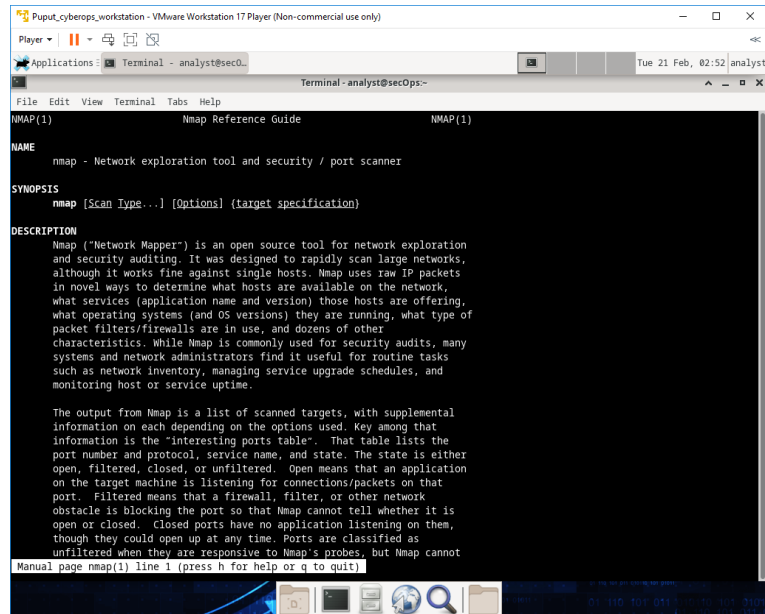
Start CyberOps Workstation

Buka terminal kemudian ketikkan

[analyst@secOps ~]\$ man nmap

Apa itu Nmap?

Apa fungsi dari Nmap?

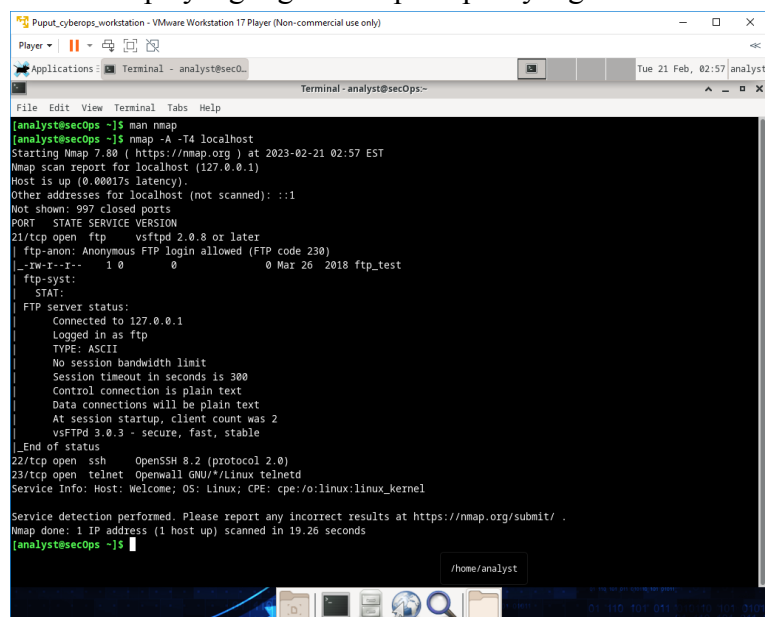


### 2. Localhost Scanning

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

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

Berapakah alamat IP dan subnet mask dari PC host?

```
CyberOps Workstation [Running] - Oracle VM VirtualBox
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 08:00:27:71:1a:82 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86254sec preferred_lft 86254sec
    inet6 fe80::a00:27ff:fe71:1a82/64 scope link
        valid_lft forever preferred_lft forever
[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 08:00:27:71:1a:82 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86254sec preferred_lft 86254sec
    inet6 fe80::a00:27ff:fe71:1a82/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Lakukanlah port scanning dengan menggunakan Nmap

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

Berapakah jumlah host yang terdeteksi?

```
CyberOps Workstation [Running] - Oracle VM VirtualBox
Terminal - analyst@secOps-
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:33 EST
Nmap scan report for 10.0.2.15
Host is up (0.00017s 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 2
|_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 44.96 seconds
[analyst@secOps ~]$
```

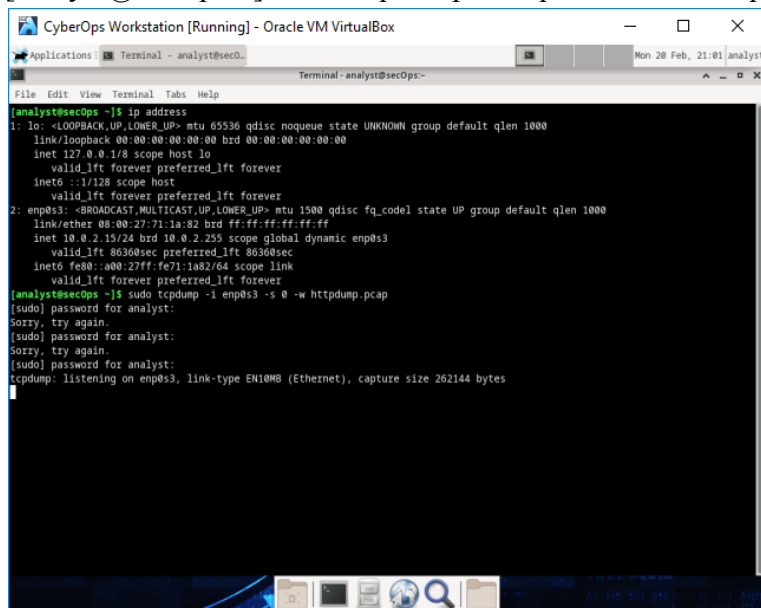
4. Remote Server Scanning Buka web browser dan kunjungi scanme.nmap.org  
Ketikkan perintah berikut:  
[analyst@secOps Desktop]\$ nmap -A -T4 scanme.nmap.org

Port dan layanan apa yang terbuka?

Berapa alamat IP server?

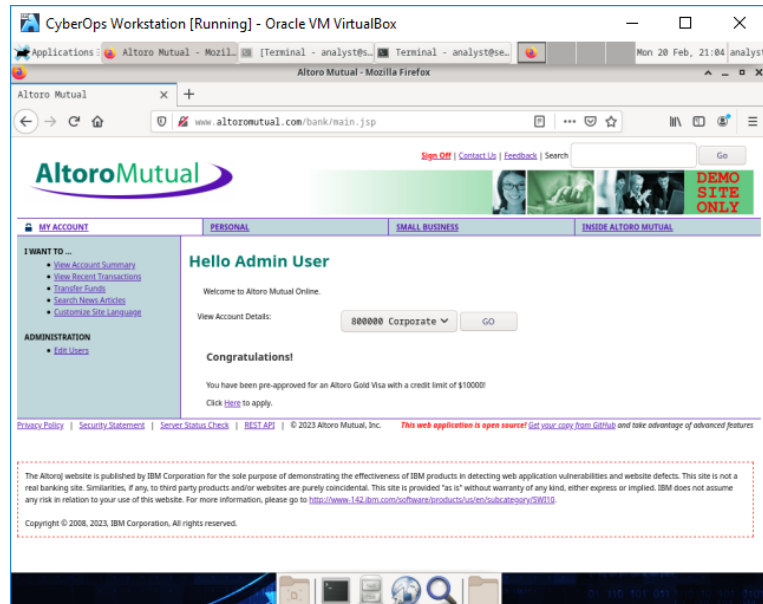
Apa sistem operasi yang digunakan oleh server?

5. 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

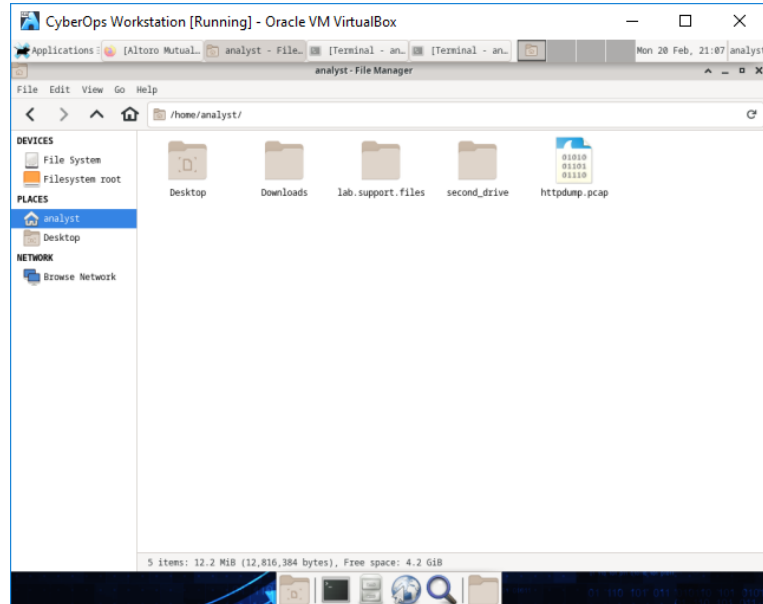


```
CyberOps Workstation [Running] - Oracle VM VirtualBox
Applications: Terminal - analyst@secOps
Terminal - analyst@secOps-
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 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 00:00:27:71:1a:a2 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86360sec preferred_lft 86360sec
    inet6 fe80::a00:27ff:fe71:1a82/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
Sorry, try again.
[sudo] password for analyst:
Sorry, try again.
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

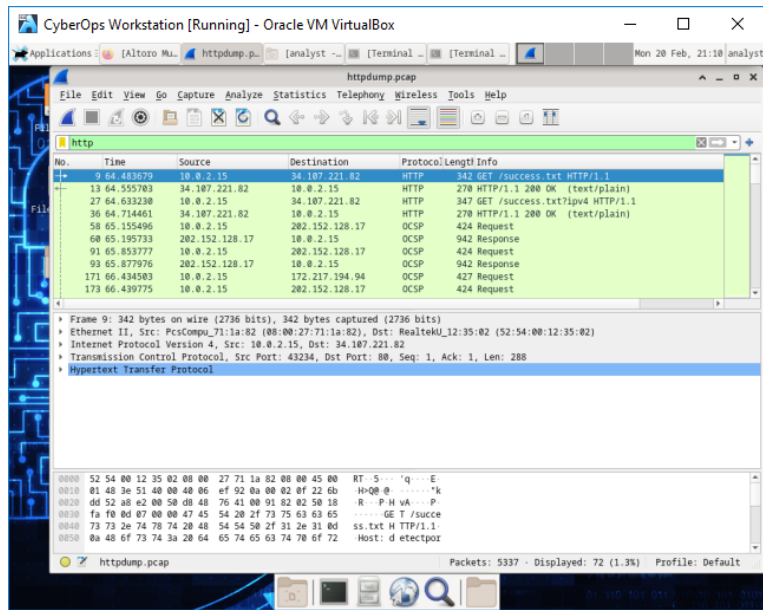
6. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation  
VM. Username : Admin  
Password : Admin



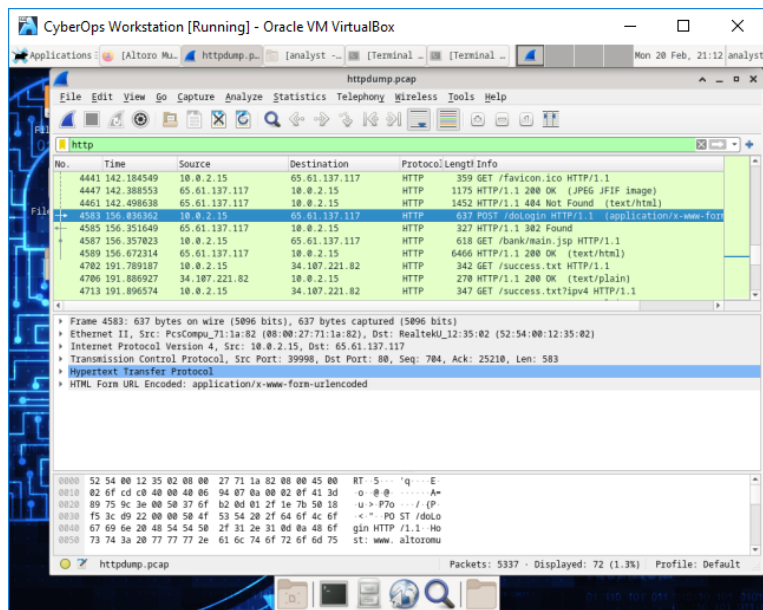
7. Merekam Paket HTTP Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/



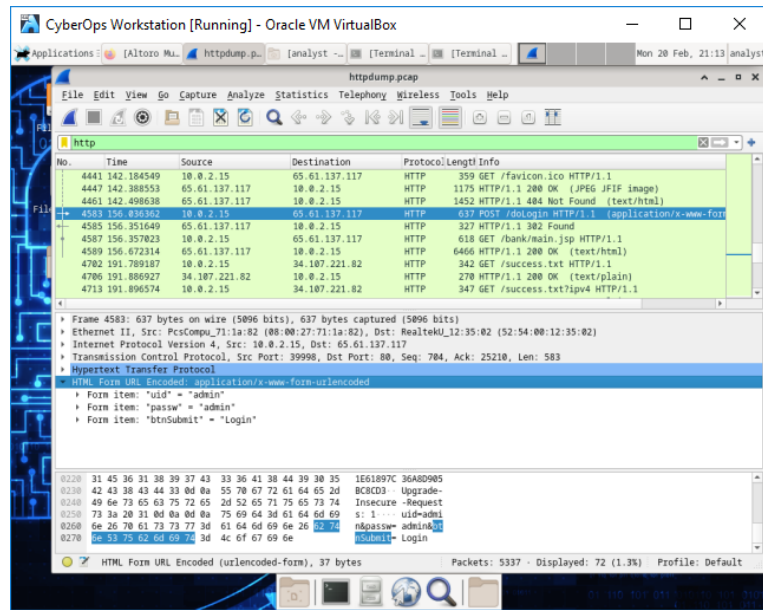
## 8. Filter http kemudian klik Apply



## 9. Pilih POST

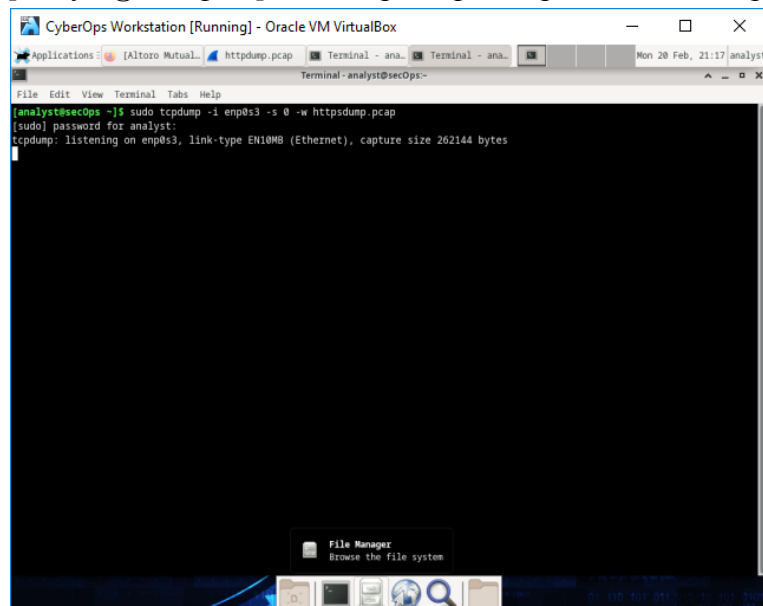


## 10. Lakukanlah analisis terhadap uid dan passw



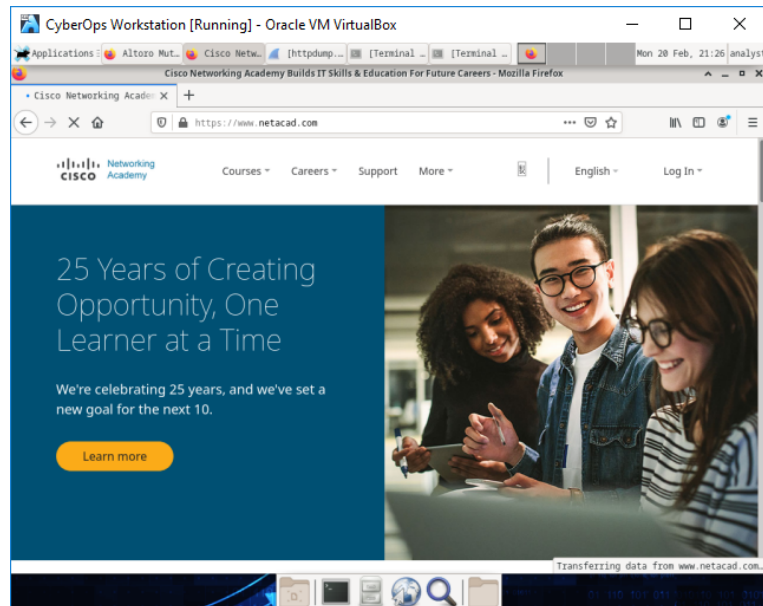
## 11. Merekam Paket HTTPS

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

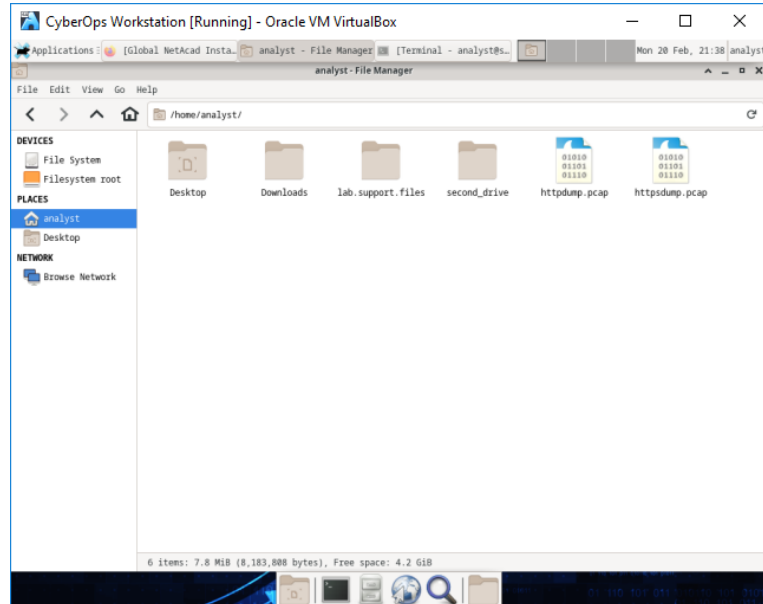




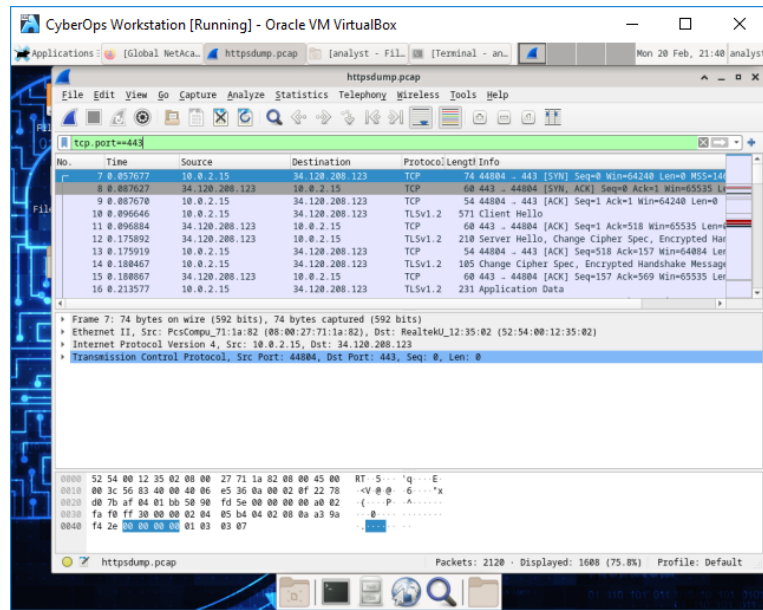
12. Buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM.



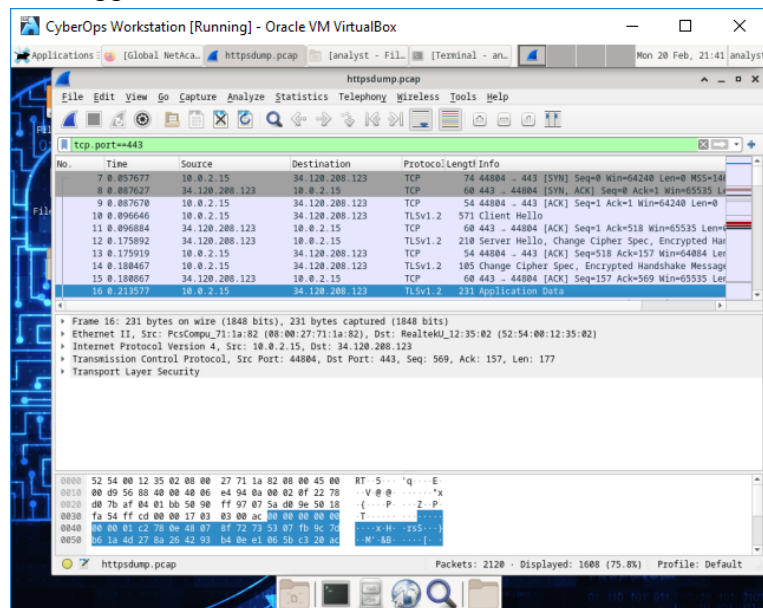
13. Klik Login
14. Masukkan username dan password anda
15. Melihat Rekaman Paket HTTPS Tcpcdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpsdump.pcap. File ini terletak pada folder /home/analyst/.



## 16. Filter tcp.port==443



## 17. Pilih Application Data



#### F. Pembahasan

Nmap ("Network Mapper") adalah alat *open source* untuk menjelajahi dan mengaudit keamanan jaringan. Ini dirancang untuk memindai jaringan besar dengan cepat, meskipun juga dapat bekerja melawan satu host. Nmap menggunakan paket IP mentah dengan cara yang canggih untuk menentukan host mana yang tersedia di jaringan, layanan apa (nama dan versi aplikasi) yang disediakan, sistem operasi (dan versi) apa yang digunakan, jenis firewall/filter paket apa yang digunakan, dan sejumlah karakteristik lainnya. Sementara Nmap terutama digunakan untuk audit keamanan, banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas-tugas rutin seperti inventaris jaringan, mengelola jadwal peningkatan layanan, dan memantau host atau uptime layanan.

Keluaran Nmap adalah daftar target yang diperiksa, dengan informasi tambahan tergantung pada opsi yang digunakan. Hal utama di antara informasi itu adalah "tabel port menarik". Tabel mencantumkan nomor port dan protokol, nama layanan, dan status.

Argumen yang digunakan dalam conadalah -A, untuk pemeriksaan sistem operasi dan versi, pemeriksaan skrip, dan traceroute; -T4 untuk eksekusi lebih cepat

Wireshark adalah aplikasi penangkap paket data open-source yang berguna untuk memindai dan menangkap lalu lintas data di jaringan internet. Aplikasi ini biasa digunakan sebagai troubleshooting tool pada jaringan yang bermasalah, selain itu juga biasa digunakan untuk software testing karena kemampuannya dalam membaca isi setiap paket lalu lintas data. Aplikasi ini sebelumnya dikenal sebagai Ethernet, namun karena masalah merek dagang namanya diubah menjadi Wireshark.

Secara positif, Wireshark berguna untuk pekerjaan analisis jaringan. Cara kerjanya adalah dengan 'menangkap' paket data dari berbagai protokol dari berbagai jenis jaringan yang banyak terdapat pada lalu lintas jaringan internet. Paket data 'ditangkap' dan kemudian ditampilkan di jendela hasil tangkapan secara real-time.

#### G. Kesimpulan

Nmap ("Network Mapper") adalah alat *open source* untuk menjelajahi dan mengaudit keamanan jaringan. Wireshark berguna untuk pekerjaan analisis jaringan. Cara kerjanya adalah dengan 'menangkap' paket data dari berbagai protokol dari berbagai jenis jaringan yang banyak terdapat pada lalu lintas jaringan internet. Paket data 'ditangkap' dan kemudian ditampilkan di jendela hasil tangkapan secara real-time.

#### H. Daftar Pustaka

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

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

Saputro, N. (2022, June 11). *Pengertian Wireshark : Fungsi dan Cara kerjanya*

(*Lengkap*). Nesabamedia. Retrieved February 27, 2023, dari

<https://www.nesabamedia.com/pengertian-wireshark/>