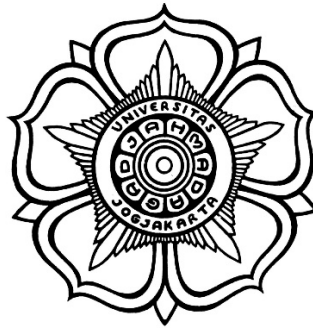


**LAPORAN PRAKTIKUM**  
**Praktikum Keamanan**  
**Informasi**

Virtual Machine



Surya Rahadi Pratama  
(21/479908/SV/19547)

**PROGRAM STUDI TEKNOLOGI REKAYASA**  
**INTERNETDEPARTEMEN TEKNIK ELEKTRO DAN**  
**INFORMATIKASEKOLAH VOKASI**  
**UNIVERSITAS GADJAH MADA**  
**2023**

## Latar Belakang

Nmap atau Network Mapper adalah sebuah tool yang digunakan untuk melakukan pemindaian jaringan atau port scanning. Tool yang dibuat oleh Gordon Lyon ini dapat digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan tool ini pun dapat digunakan untuk melihat host yang aktif, port yang terbuka, sistem operasi yang digunakan dan lainnya

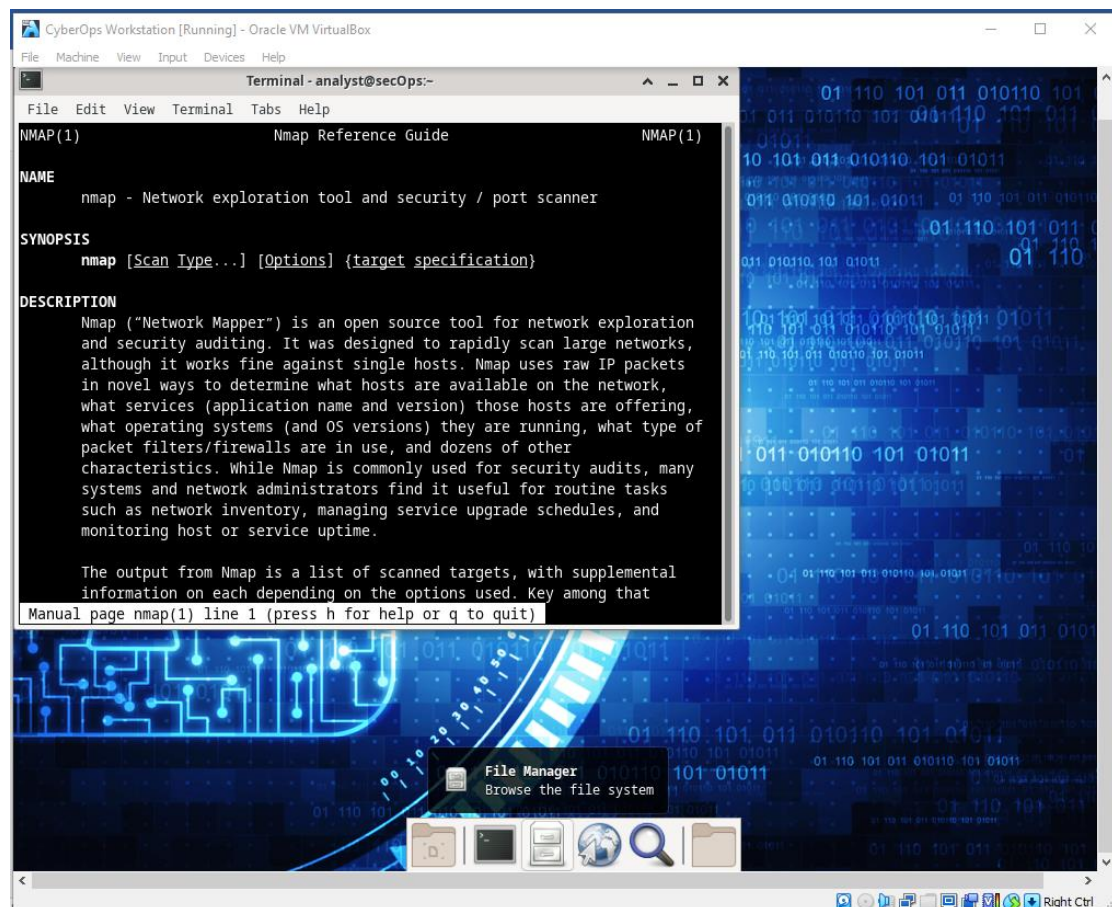
### 1. Eksplorasi Nmap

Start CyberOps Workstation

Buka terminal kemudian ketikkan

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

Apa itu Nmap? Apa fungsi dari Nmap?



#### 1. Digunakan untuk memeriksa jaringan

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.

Selain itu, adanya IP Raw juga untuk mengetahui layanan yang diberikan yang di dalamnya memuat nama dan juga versi aplikasi, sistem operasi lengkap dengan versinya, dan juga apa saja jenis firewall atau paket filter yang digunakan. Dengan menggunakan NMAP, maka pengguna bisa memperoleh informasi yang lengkap tentang seperti apa jaringan atau host tersebut.

## 2. Melakukan scanning pada port 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.

Contohnya, sekarang Anda tinggal di Malang yang memiliki kode pos 65141, sementara teman Anda sekarang berada di Bandung dengan kode pos 40111. Kode pos tersebut yang nantinya bisa digunakan untuk membedakan antar aplikasi. Setiap aplikasi yang terpasang pada komputer harus memiliki port dan masing-masing port tersebut harus berbeda. Port tersebut juga bisa dianalogikan sebagai sebuah IP Address yang berperan dalam membedakan antara perangkat atau komputer satu dengan komputer yang lainnya.

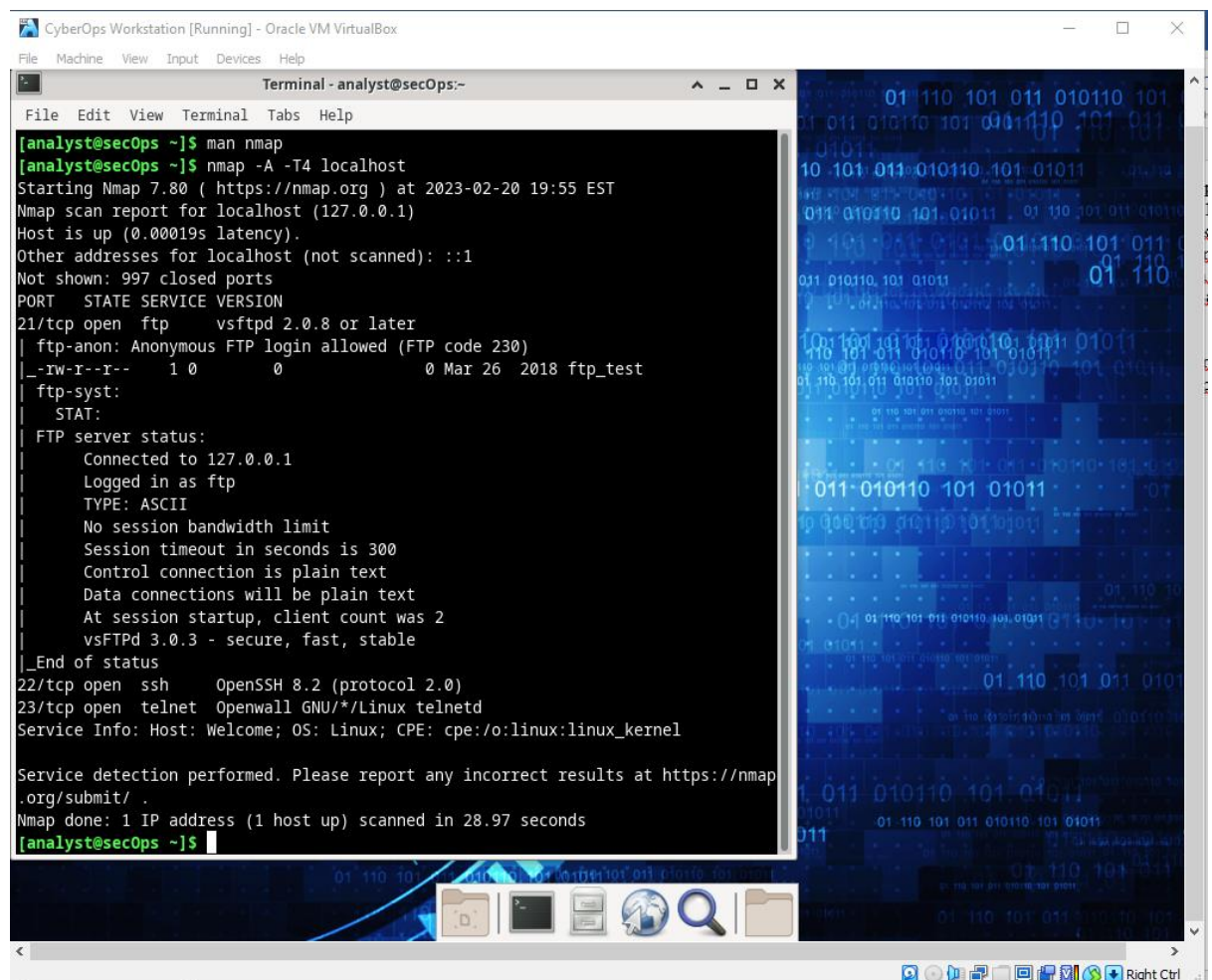
Dengan menggunakan NMAP, maka seseorang bisa melakukan scanning terhadap port-port tersebut. Maka seseorang bisa mengetahui aplikasi mana saja yang terpasang pada suatu perangkat.

## 2. Localhost Scanning

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

Port dan layanan apa yang terbuka?

Software apa yang digunakan pada port yang terbuka tersebut?



```
CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ man nmap
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:55 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00019s 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 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: 1 IP address (1 host up) scanned in 28.97 seconds
[analyst@secOps ~]$
```

21/tcp	ftp
22/tcp	ssh
23/tcp	telnet

### 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

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: 1 IP address (1 host up) scanned in 28.97 seconds
[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:aa:ea:17 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 83778sec preferred_lft 83778sec
    inet6 fe80::a00:27ff:feaa:ea17/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

IP Address :10.0.2.15/24

Subnet Mask :10.0.2.255

Lakukanlah port scanning dengan menggunakan Nmap

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



```
inet6 fe80::a00:27ff:feaa:ea17/64 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 20:17 EST
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 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 44.80 seconds
[analyst@secOps ~]$
```

Berapakah jumlah host yang terdeteksi?

1 host

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

CyberOps Workstation [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications: Go ahead and ScanMe! [analyst - File Manag... Terminal - analyst@se... Mon 20 Feb, 21:46 analyst

Terminal - analyst@secOps-

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 21:45 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ac:00:a0:1a:02:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered smtp
53/tcp    open  domain   ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
|_ dns-nsid:
|_ bind.version: 9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.4
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel, cpe:/o:redhat:enterprise_linux:6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.12 seconds
[analyst@secOps ~]$
```

Activate Windows  
Go to Settings to activate Windows.

9:46  
21/02/2023

Port dan layanan apa yang terbuka? Berapa alamat IP server? Apa sistem operasi yang digunakan oleh server?

## Unit 3

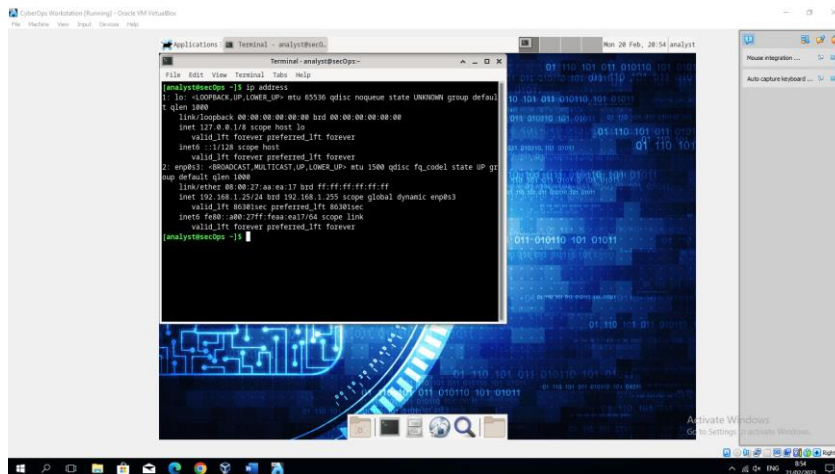
### Latar Belakang

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

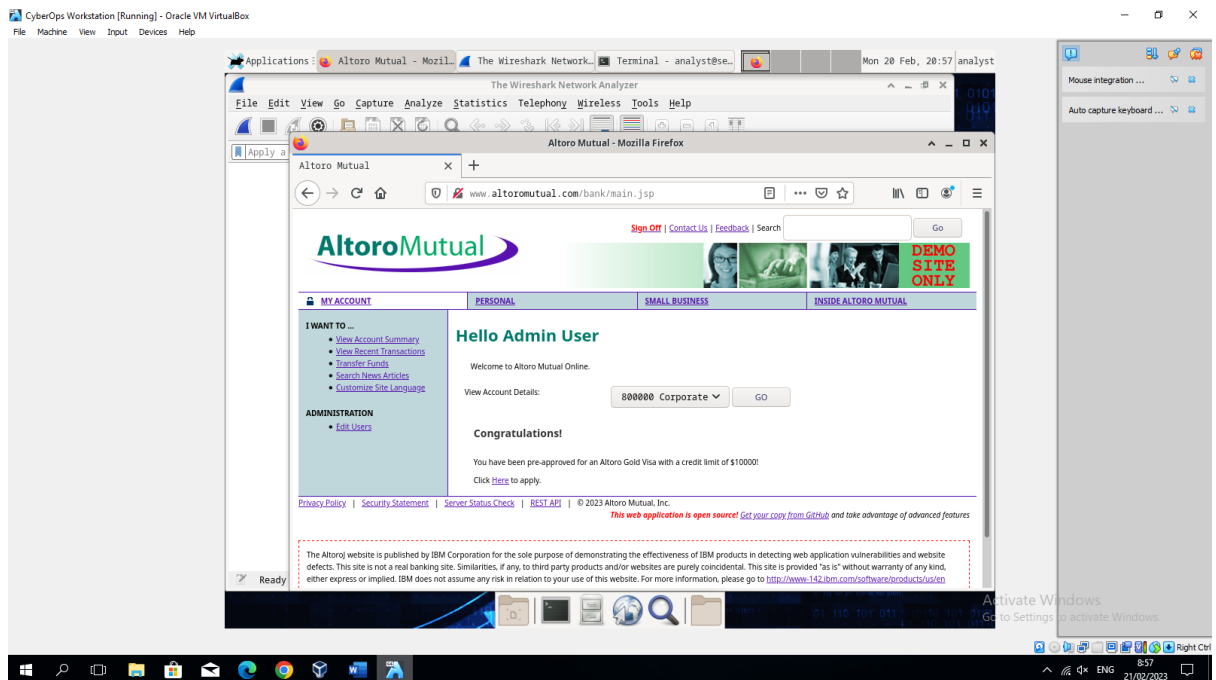
### Wireshark

Wireshark merupakan alat networking administrator yang bekerja sebagai analisis lalu lintas jaringan termasuk protokol yang ada di dalam jaringan tersebut, baik secara TCP, UDP maupun HTTP. Wireshark mampu menangkap paket-paket informasi dalam berbagai format protokol secara lengkap dan mudah untuk dianalisis. Wireshark sangat mirip dengan tcpdump, tetapi Wireshark memiliki antarmuka grafis serta mampu melakukan pencarian sortir serta 2 filtering tergantung pengguna. Terlepas dari kekurangan yang ada, Wireshark tetaplah sebuah aplikasi yang telah membantu banyak pengguna.

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:

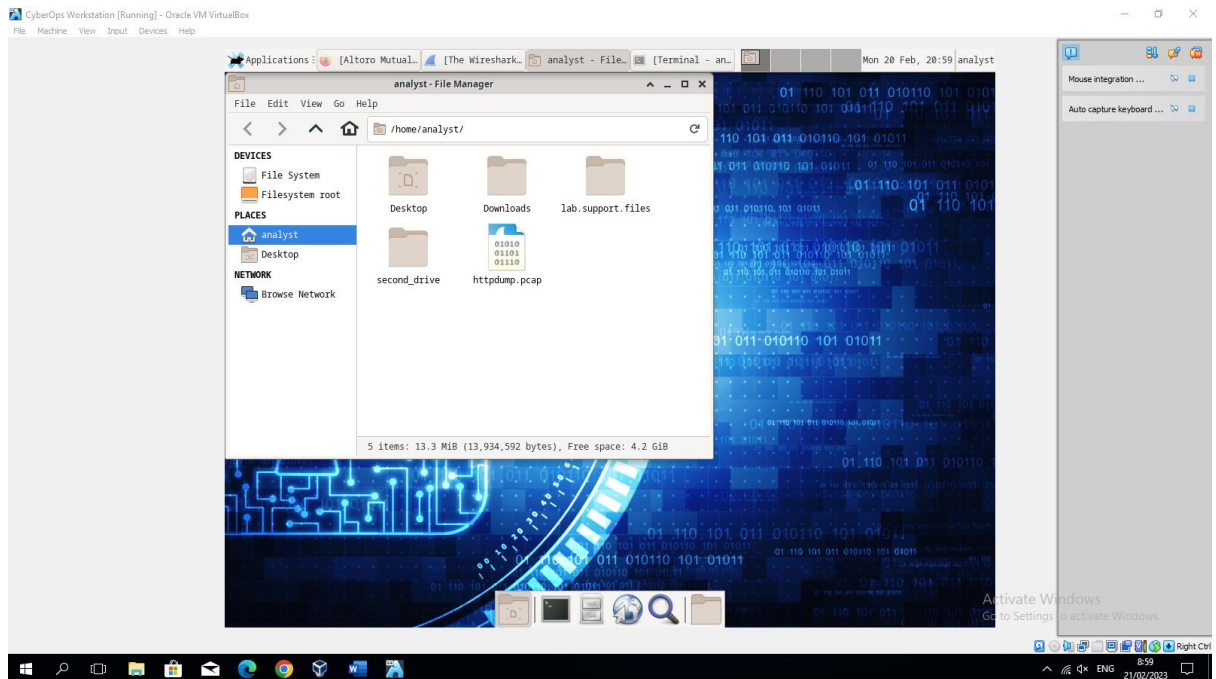


3. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM.  
Username : Admin  
Password : Admin

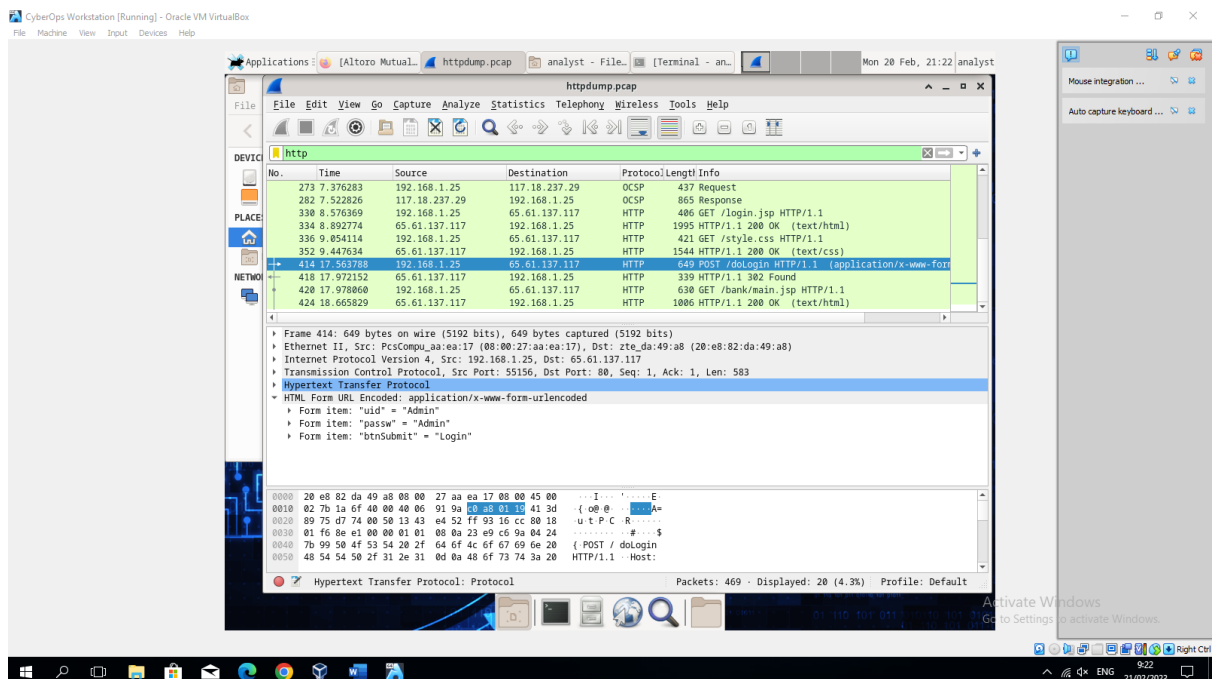




4. Merekam Paket HTTP Tcpcdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/.

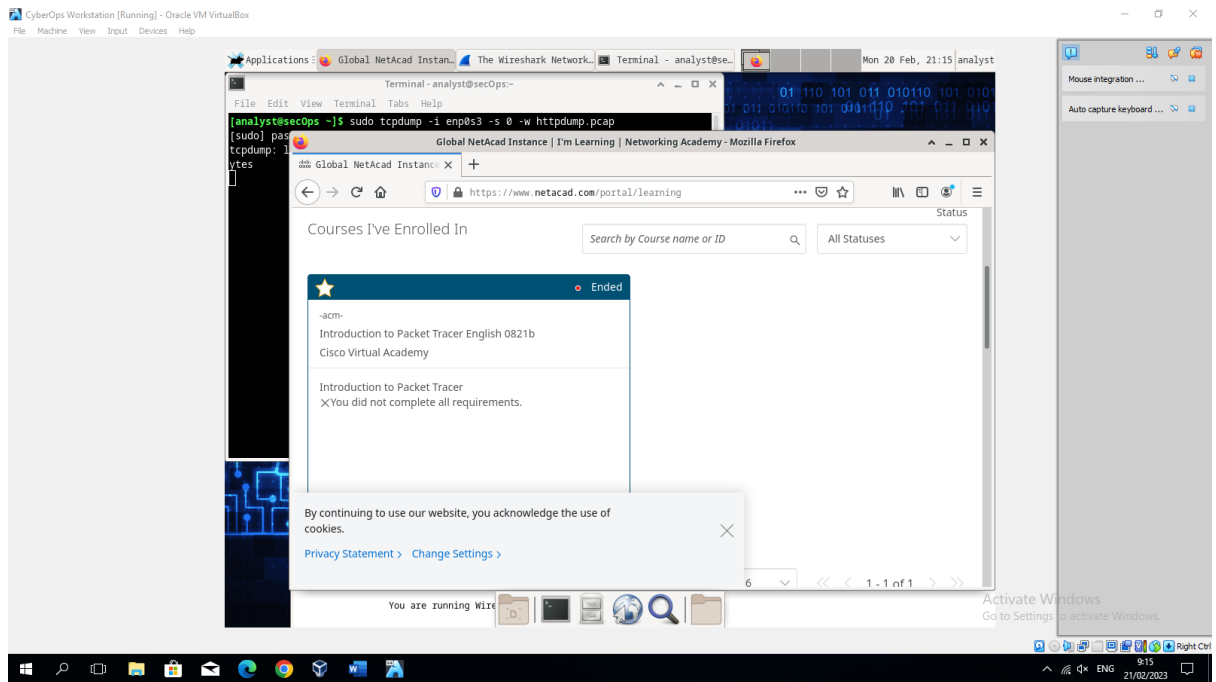


5. Filter http kemudian klik Apply
6. Pilih POST
7. Lakukanlah analisis terhadap uid dan passw

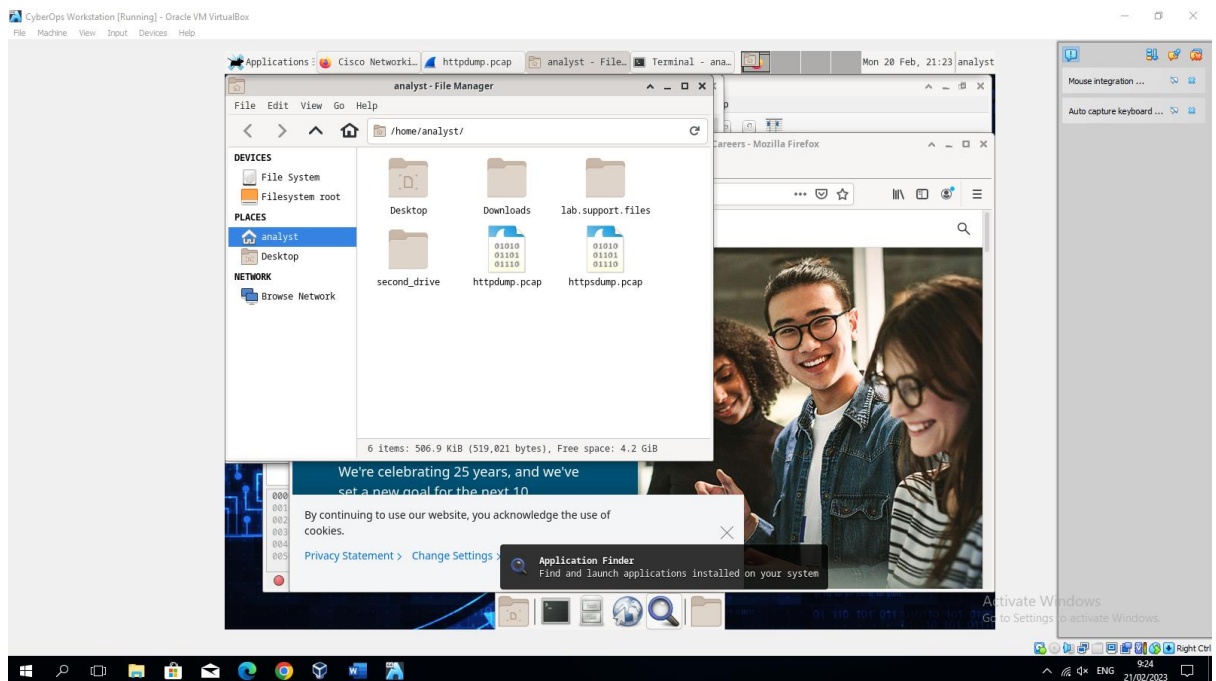


8. Merekam Paket HTTPS  
[analyst@secOps ~]\$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap  
[sudo] password for analyst:

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

The screenshot shows the Wireshark interface with the filter 'tcp.port == 443' applied. The packet list shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
75	6.583989	192.168.1.25	192.168.1.25	TCP	74	52918 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
91	7.512429	192.168.1.25	192.168.1.25	TCP	74	[TCP Retransmission] 52918 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
128	7.763962	192.168.1.25	192.168.1.25	TCP	74	49878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
149	7.986847	216.239.38.120	192.168.1.25	TCP	74	443 → 49878 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
151	7.986182	192.168.1.25	216.239.38.120	TCP	66	49878 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
153	7.918425	192.168.1.25	216.239.38.120	TLSv1.3	583	Client Hello
154	7.947733	216.239.38.120	192.168.1.25	TCP	66	443 → 49878 [ACK] Seq=1 Ack=518 Win=66816 Len=0
155	7.947733	216.239.38.120	192.168.1.25	TLSv1.3	2866	Server Hello, Change Cipher Spec
156	7.947775	192.168.1.25	216.239.38.120	TCP	66	49878 → 443 [ACK] Seq=518 Ack=2601 Win=63488 Len=0
157	7.949136	216.239.38.120	192.168.1.25	TLSv1.3	1556	Application Data

### 14. Pilih Application Data

The screenshot shows the Wireshark interface with the filter 'tcp.port==443' applied. The packet list shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
2365	18.477253	192.28.147.68	192.168.1.25	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
3055	51.549742	23.207.184.162	192.168.1.25	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
3686	61.474775	192.168.1.25	72.163.10.10	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
3687	61.494496	192.168.1.25	72.163.10.10	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
3725	68.488424	192.168.1.25	72.163.10.10	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
3918	71.888811	23.207.184.162	192.168.1.25	TLSv1.2	117	[TCP Fast Retransmission], Change Cipher Spec
2198	72.409232	142.251.10.154	192.168.1.25	TLSv1.3	118	Application Data
1452	13.606408	142.251.10.154	192.168.1.25	TLSv1.3	120	Application Data
2340	18.234066	31.13.95.35	192.168.1.25	TLSv1.3	120	Application Data
2343	18.234066	31.13.95.35	192.168.1.25	TLSv1.3	120	Application Data