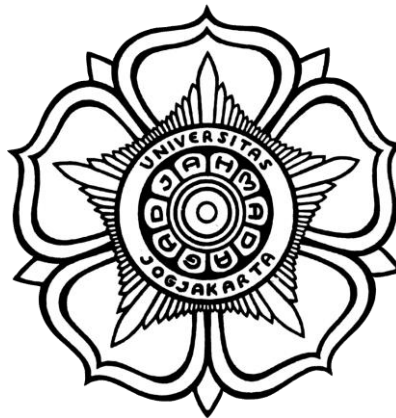


**LAPORAN PRAKTIKUM**  
**KEAMANAN INFORMASI 1**  
**PERTEMUAN 2**  
**(Eksplorasi HTTP & HTTPS dengan Wireshark)**



**DISUSUN OLEH**  
Indah Sekar Ningrum (21/478139/SV/19241)

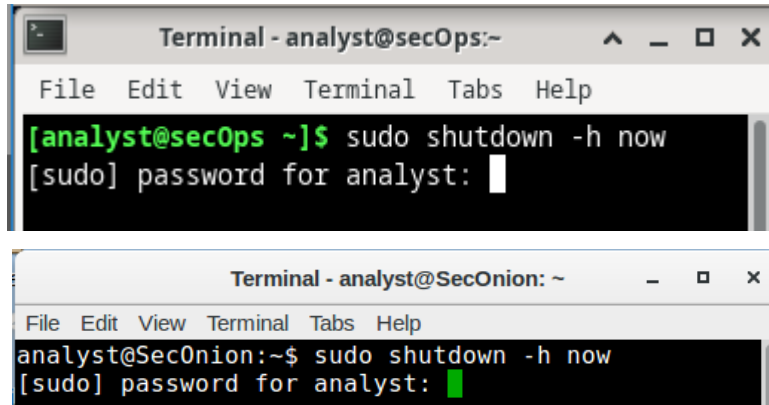
**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET**  
**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**  
**SEKOLAH VOKASI**  
**UNIVERSITAS GADJAH MADA**  
**YOGYAKARTA**

**2023**

## A. LANGKAH – LANGKAH

### LAB 1

1. Mematikan VM Ketikkan perintah `sudo shutdown -h now` pada terminal untuk mematikan VM.

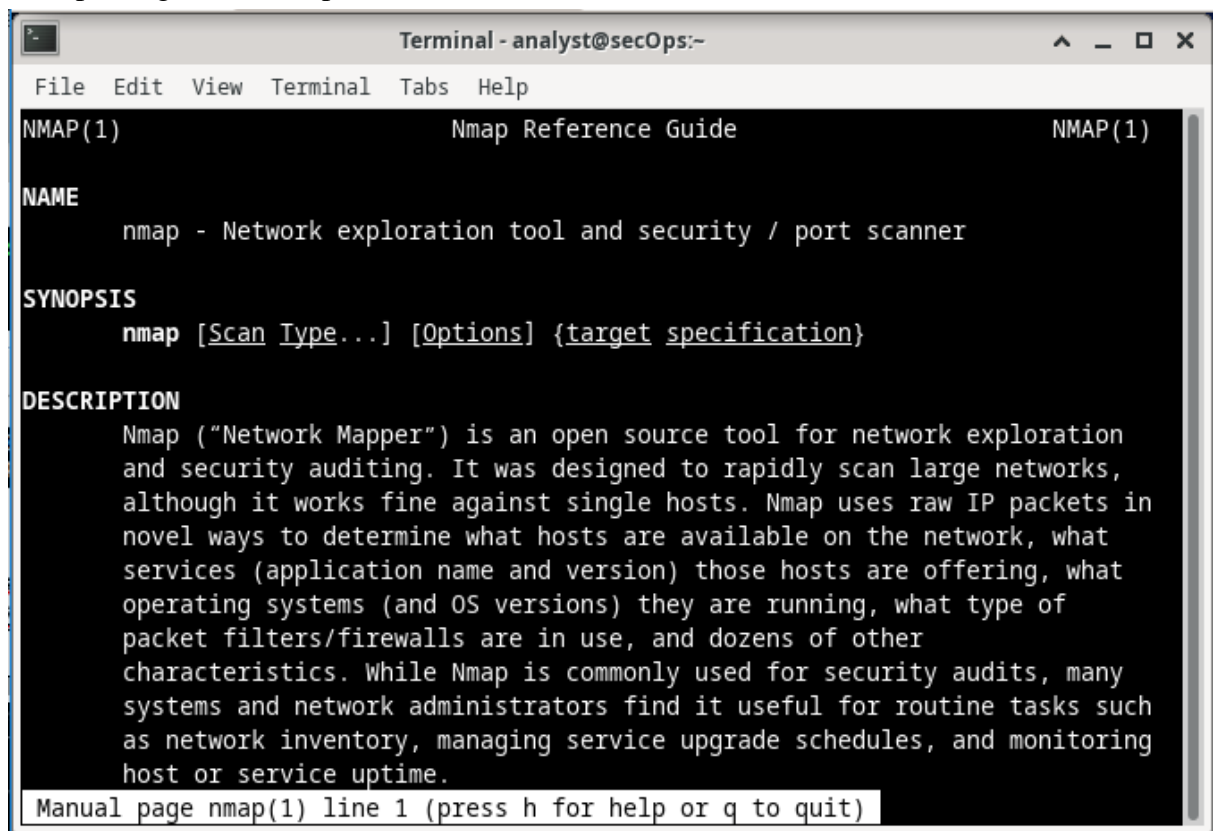


### LAB 2

1. Eksplorasi Nmap Start CyberOps Workstation Buka terminal kemudian ketikkan  
`[analyst@secOps ~]$ man nmap`  
`[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?

```
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 19:56 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 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 29.08 seconds  
[analyst@secOps ~]$ S
```

### 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 gro  
up default qlen 1000  
    link/ether 08:00:27:64:c4:29 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 85095sec preferred_lft 85095sec  
    inet6 fe80::a00:27ff:fe64:c429/64 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

Berapakah jumlah host yang terdeteksi?

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:21 EST
Nmap scan report for 10.0.2.15
Host is up (0.00014s 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_tes
st
| 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

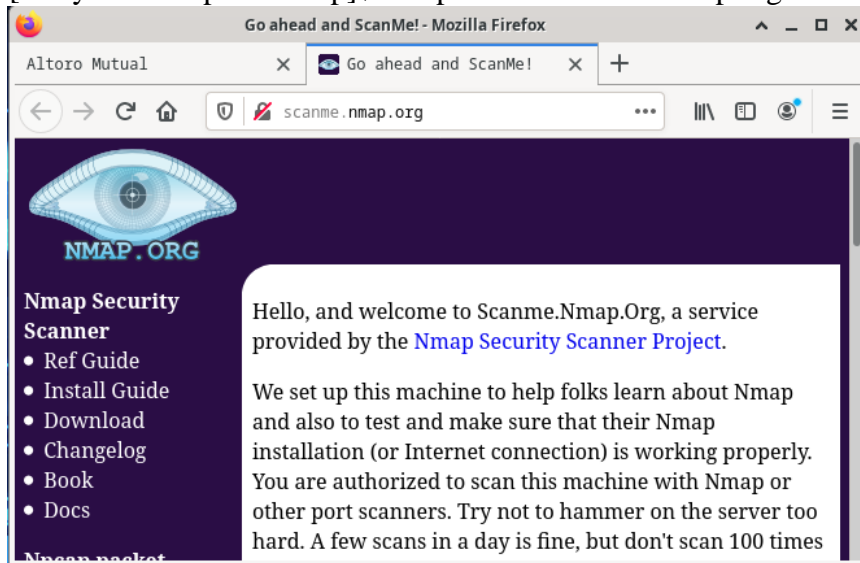
Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 64.14 seconds
```

#### 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?

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:59 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f0
3c: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: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)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
)
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 40.64 seconds
```

### LAB 3

1. Jalankan VM dan Login

Username: analyst

Password: cybercops

(pada laporan praktikum pertemuan 1)

2. Buka terminal dan menjalankan tcpdump

Pengecekan alamat IP dengan menggunakan perintah:

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

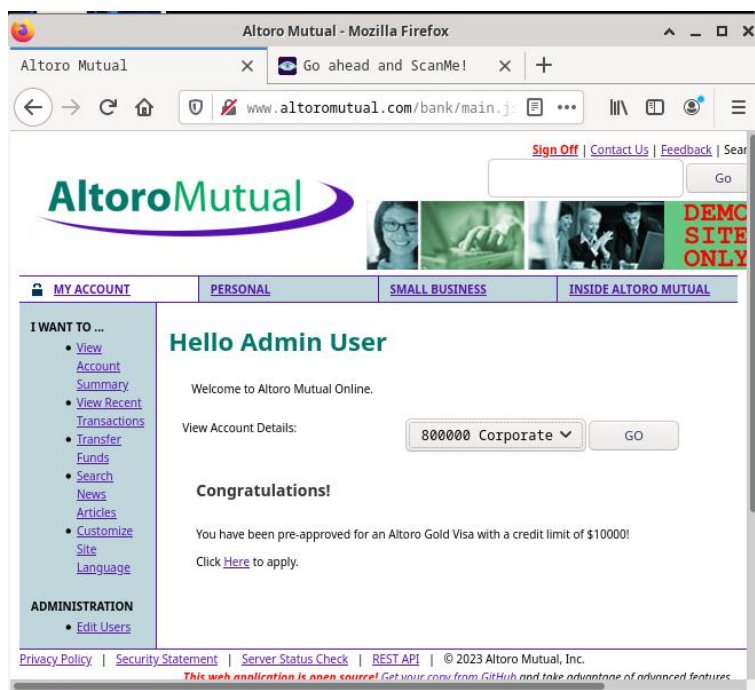
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN
OWN 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_c
odel state UP group default qlen 1000
    link/ether 08:00:27:64:c4:29 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fe64:c429/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), captu
re size 262144 bytes
^C438 packets captured
439 packets received by filter
0 packets dropped by kernel
```

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

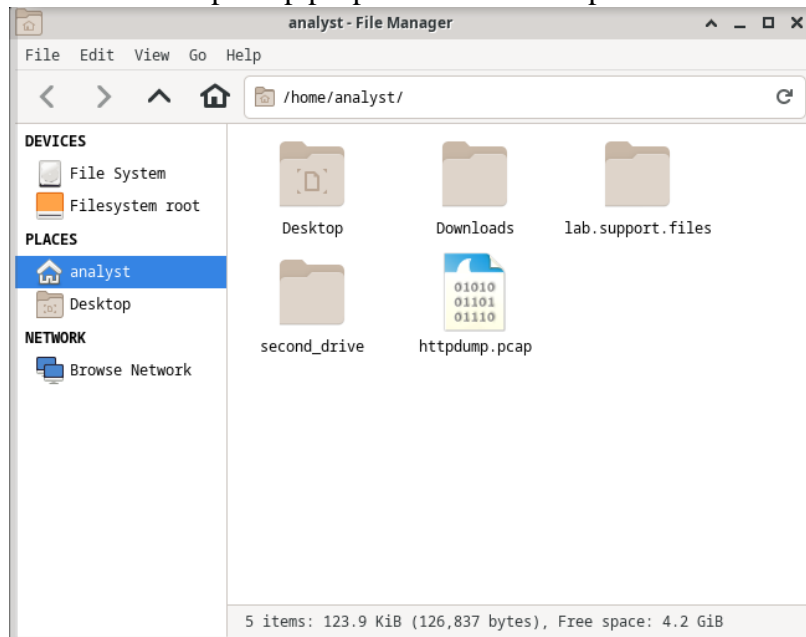
Username : Admin

Password : Admin

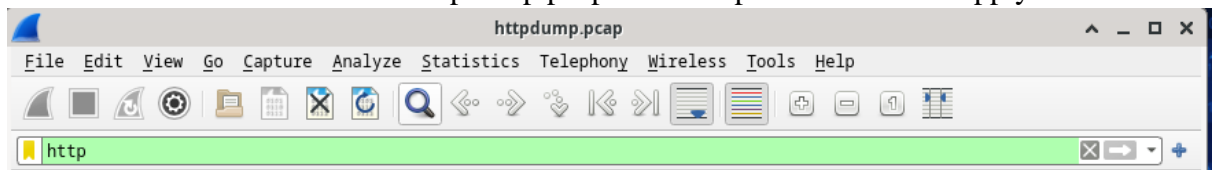


4. Merekam Paket HTTP

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



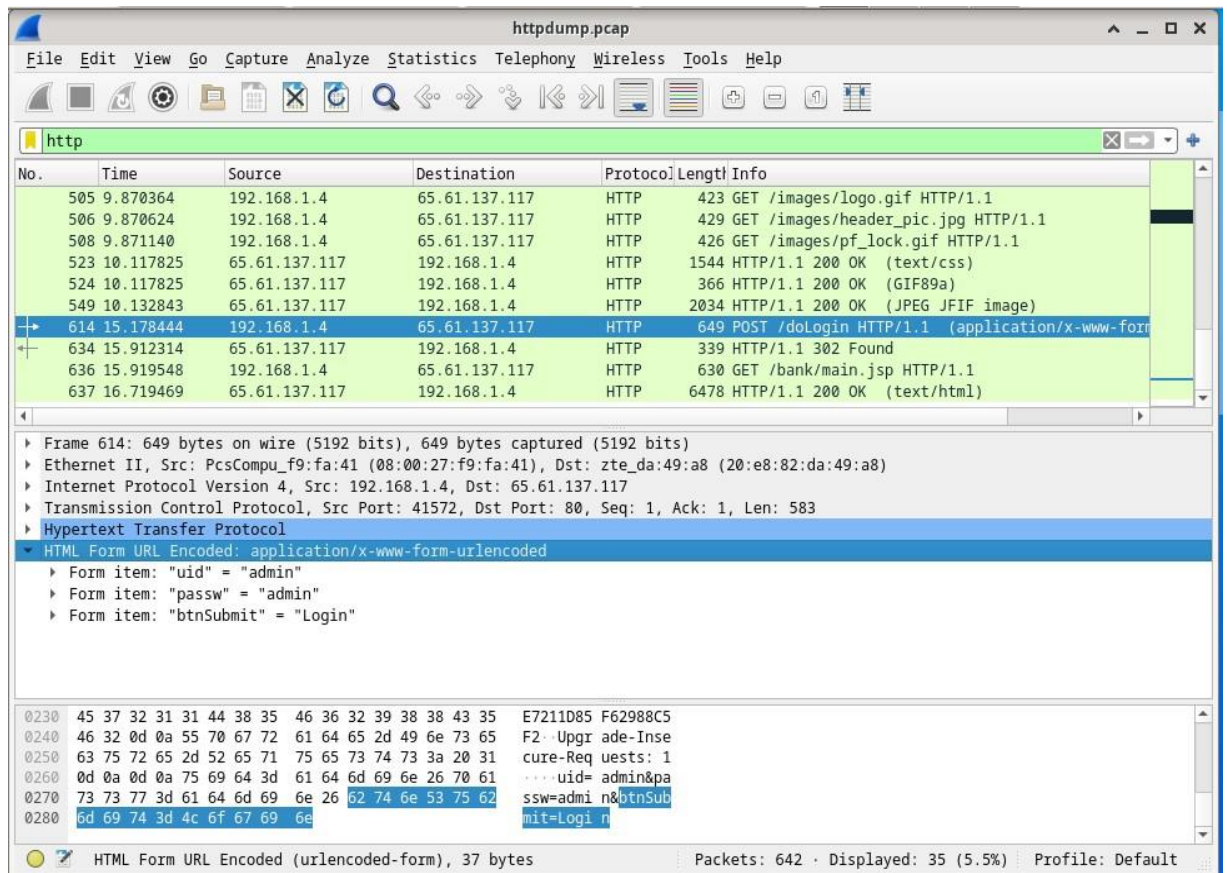
5. Buka Wireshark dalam file httpdump.pcap. Filter http kemudian klik Apply.



6. Pilih POST



7. Lakukanlah analisis terhadap uid dan password



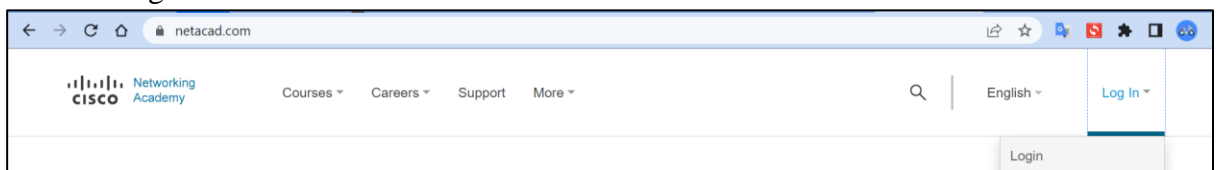
8. Merekam Paket HTTPS

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

```
[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
```

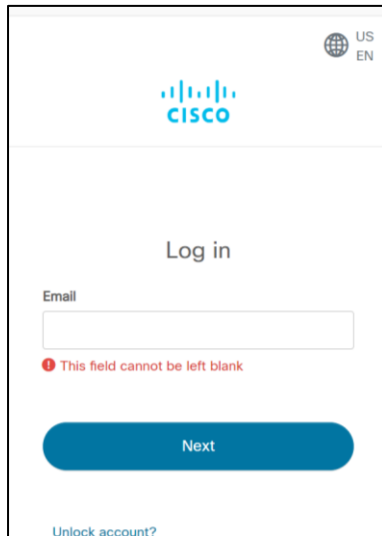
9. Buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM.

10. Klik Login



11. Masukkan username dan password anda

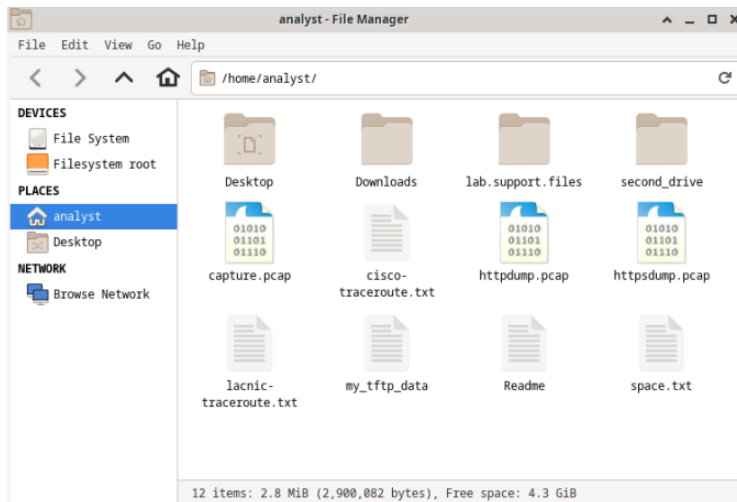




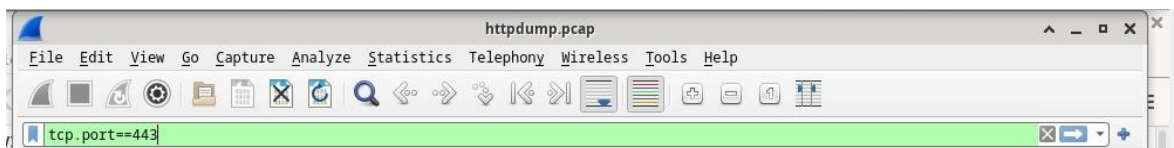
The image shows the Cisco login page. At the top right, there is a globe icon and the text "US EN". Below this is the Cisco logo. In the center, the text "Log in" is displayed. Underneath, there is an "Email" label followed by a text input field. Below the input field, a red error message states "This field cannot be left blank". At the bottom, there is a blue "Next" button. A link "Unlock account?" is located at the very bottom left.

## 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

httpdump.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==443

No.	Time	Source	Destination	Protocol	Length	Info
44	6.100118	192.168.1.4	216.239.38.120	TLSv1.3	130	Change Cipher Spec, Application Data
45	6.100750	192.168.1.4	216.239.38.120	TLSv1.3	236	Application Data
46	6.100816	192.168.1.4	216.239.38.120	TLSv1.3	258	Application Data
47	6.213615	192.168.1.4	216.239.38.120	TCP	258	[TCP Retransmission] 52416 - 443 [PSH, ACK] Seq
48	6.248797	192.168.1.4	216.239.38.120	TLSv1.3	101	Application Data
49	6.307817	216.239.38.120	192.168.1.4	TLSv1.3	642	[TCP Previous segment not captured] , Applicat
50	6.307817	216.239.38.120	192.168.1.4	TLSv1.3	224	Application Data
51	6.307817	216.239.38.120	192.168.1.4	TLSv1.3	98	Application Data
52	6.307817	216.239.38.120	192.168.1.4	TLSv1.3	97	Application Data
53	6.307817	216.239.38.120	192.168.1.4	TLSv1.3	105	Application Data

Frame 52: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)

Ethernet II, Src: zte\_da:49:a8 (20:e8:82:da:49:a8), Dst: PcsCompu\_f9:fa:41 (08:00:27:f9:fa:41)

Internet Protocol Version 4, Src: 216.239.38.120, Dst: 192.168.1.4

Transmission Control Protocol, Src Port: 443, Dst Port: 52416, Seq: 5702, Ack: 944, Len: 31

Transport Layer Security

- TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
  - Opaque Type: Application Data (23)
  - Version: TLS 1.2 (0x0303)
  - Length: 26
  - Encrypted Application Data: 78a0dbb66129f346269924b0e3c7612fb59786f2e3087e17...

0000 08 00 27 f9 fa 41 20 e8 82 da 49 a8 08 00 45 80 .!.A .I.E.

0010 00 53 d3 a1 00 00 77 06 ae 6f d8 ef 26 78 c0 a8 .S...W..o.&x..

0020 01 04 01 bb cc c0 10 02 06 b3 1e c2 5a f3 80 18 .....Z...

0030 01 0d 4b 21 00 00 01 01 08 0a 13 89 44 7c 72 0d .K!....D|r...

0040 20 bd 17 03 03 00 1a 78 a0 db b6 61 29 f3 46 26 .....x...a)F&

0050 99 24 b0 e3 c7 61 2f b5 97 86 f2 e3 08 7e 17 c4 .\$.a/. ....~..

0060 38 8

Payload is encrypted applicati... data (tls.app\_data), 26 bytes Packets: 8263 · Displayed: 7755 (93.9%) Profile: Default