

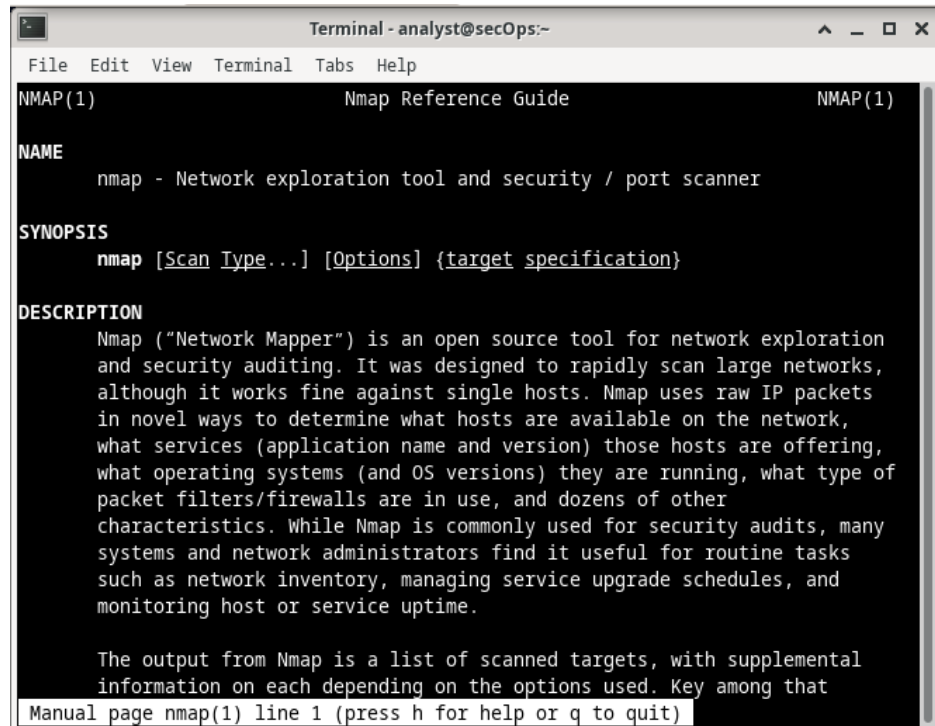
## A. Eksplorasi nmap

### 1. Eksplorasi Nmap

Start CyberOps Workstation

Buka terminal kemudian ketikkan

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



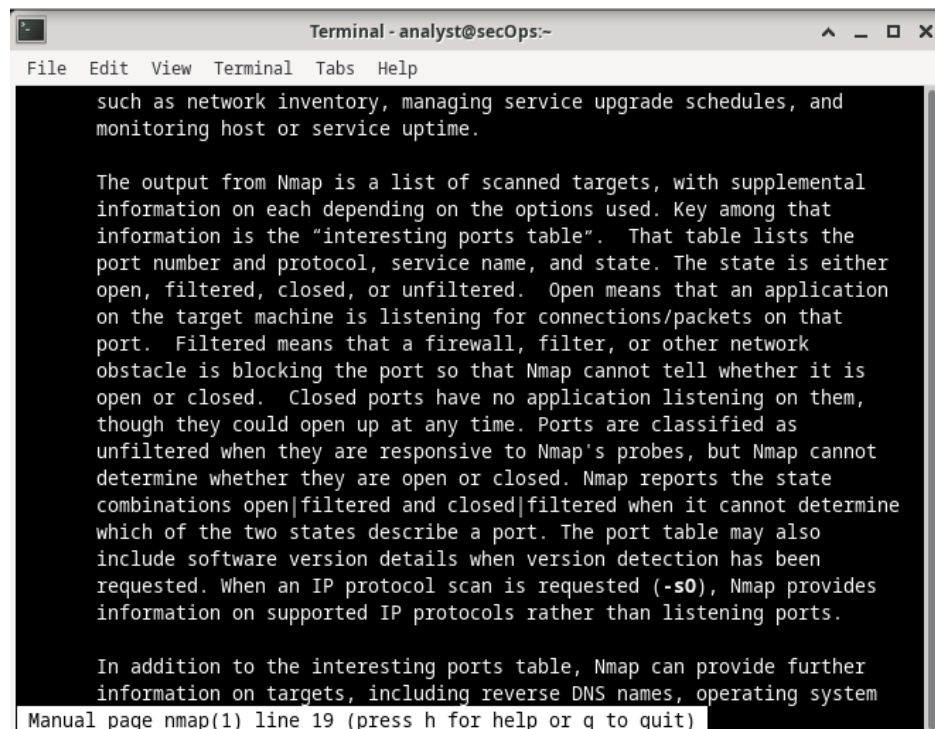
```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
NMAP(1)                                Nmap Reference Guide                                NMAP(1)

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)
```



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

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
information is the "interesting ports table". That table lists the
port number and protocol, service name, and state. The state is either
open, filtered, closed, or unfiltered. Open means that an application
on the target machine is listening for connections/packets on that
port. Filtered means that a firewall, filter, or other network
obstacle is blocking the port so that Nmap cannot tell whether it is
open or closed. Closed ports have no application listening on them,
though they could open up at any time. Ports are classified as
unfiltered when they are responsive to Nmap's probes, but Nmap cannot
determine whether they are open or closed. Nmap reports the state
combinations open|filtered and closed|filtered when it cannot determine
which of the two states describe a port. The port table may also
include software version details when version detection has been
requested. When an IP protocol scan is requested (-sO), Nmap provides
information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further
information on targets, including reverse DNS names, operating system
Manual page nmap(1) line 19 (press h for help or q to quit)
```

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

In addition to the interesting ports table, Nmap can provide further
information on targets, including reverse DNS names, operating system
guesses, device types, and MAC addresses.

A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
Manual page nmap(1) line 40 (press h for help or q to quit)
```

Apa itu Nmap?

**Nmap (Network Mapper) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan.**

Apa fungsi dari Nmap?

**Nmap berfungsi untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal.**

## 2. Localhost Scanning

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

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

21/tcp open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Tw-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 19.04 seconds
[analyst@secOps ~]$
```

Port dan layanan apa yang terbuka?

**21/tcp dengan layanan ftp**

**22/tcp dengan layanan ssh**

**23/tcp dengan layanan telnet**

Software apa yang digunakan pada port yang terbuka tersebut?

**Vsftpd 2.0.8**

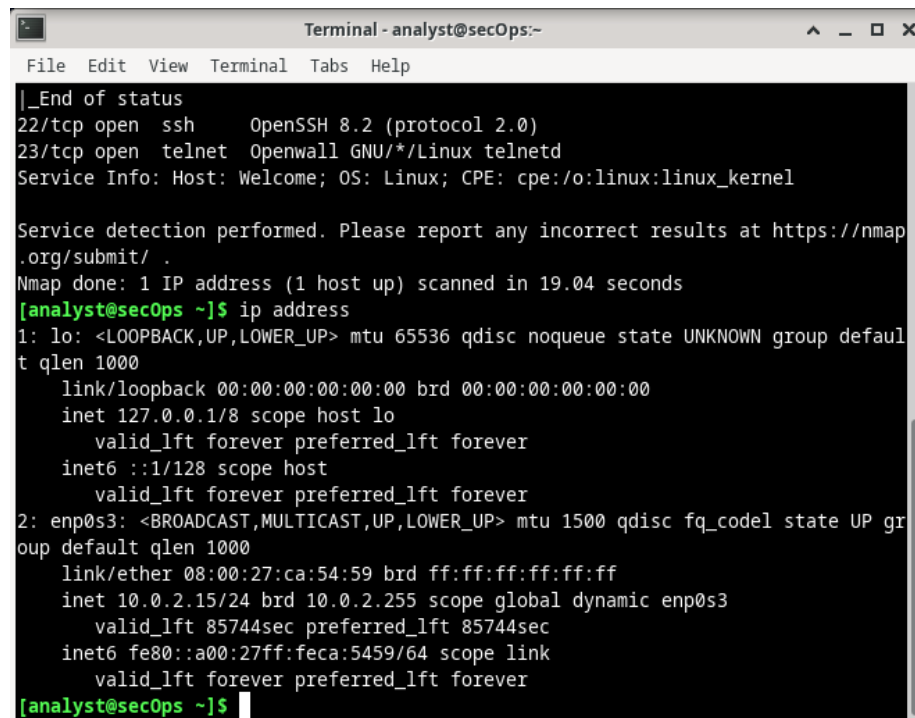
**OpenSSH 8.2 (protocol 2.0)**

**Openwall GNU/\*/Linux telnetd**

### 3. Network Scanning

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

[analyst@secOps ~]\$ ip address



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

|_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 19.04 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:ca:54:59 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85744sec preferred_lft 85744sec
    inet6 fe80::a00:27ff:feca:5459/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Berapakah alamat IP dan subnet mask dari PC host?

**10.0.2.15 dengan subnet mask 24**

Lakukanlah port scanning dengan menggunakan Nmap

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

```
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 07:11 EST
Nmap scan report for 10.0.2.15
Host is up (0.000095s 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 35.03 seconds
[analyst@secOps ~]$
```

Berapakah jumlah host yang terdeteksi?

**256 address (1 host up)**

B. Pemantauan trafik http dan https dengan menggunakan wireshark

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

```
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
    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 gr
    link/ether 08:00:27:ca:54:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.134/24 brd 192.168.100.255 scope global dynamic enp0s3
        valid_lft 3580sec preferred_lft 3580sec
    inet6 2001:448a:404a:3150:a00:27ff:feca:5459/64 scope global dynamic mngtmpa
        valid_lft 580sec preferred_lft 580sec
    inet6 fe80::a00:27ff:feca:5459/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

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

[sudo] password for analyst:

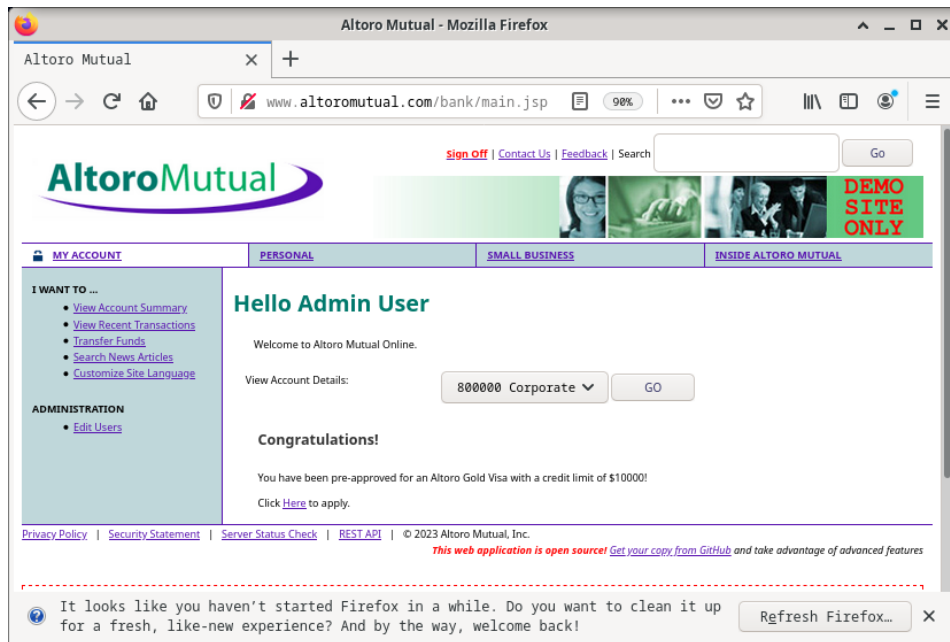
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

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

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

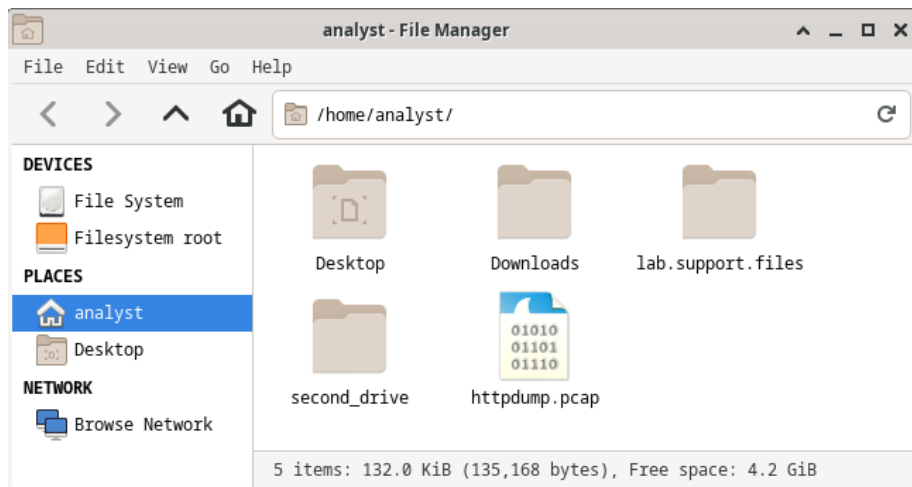
Username : Admin

Password : Admin

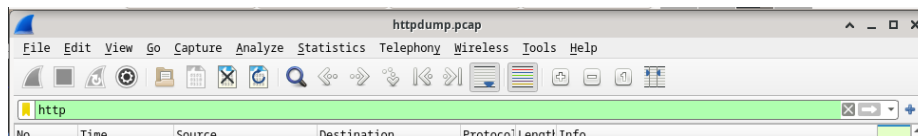


#### 4. Merekam Paket HTTP

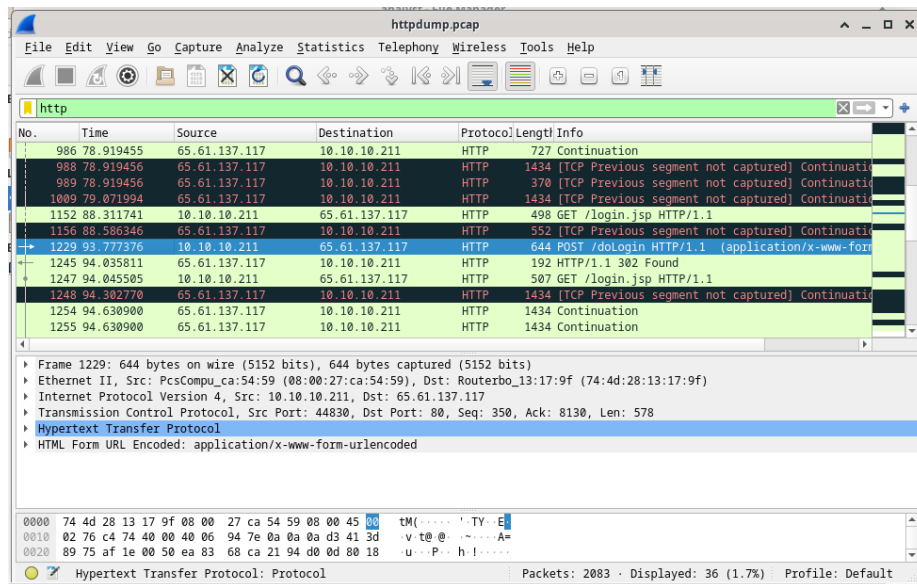
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/.



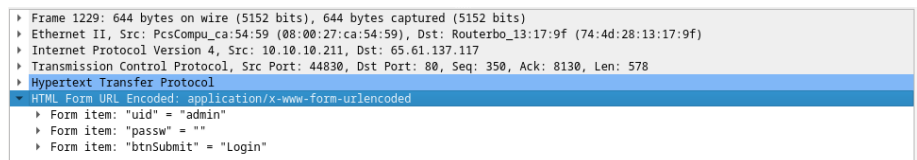
#### 5. Filter http kemudian klik Apply



#### 6. Pilih POST



## 7. Lakukanlah analisis terhadap uid dan passw

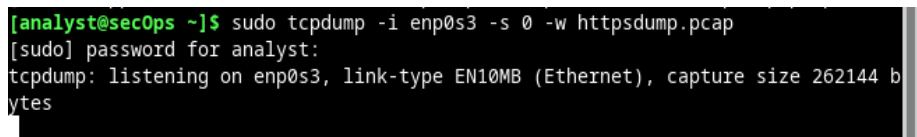


## 8. Merekam Paket HTTPS

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

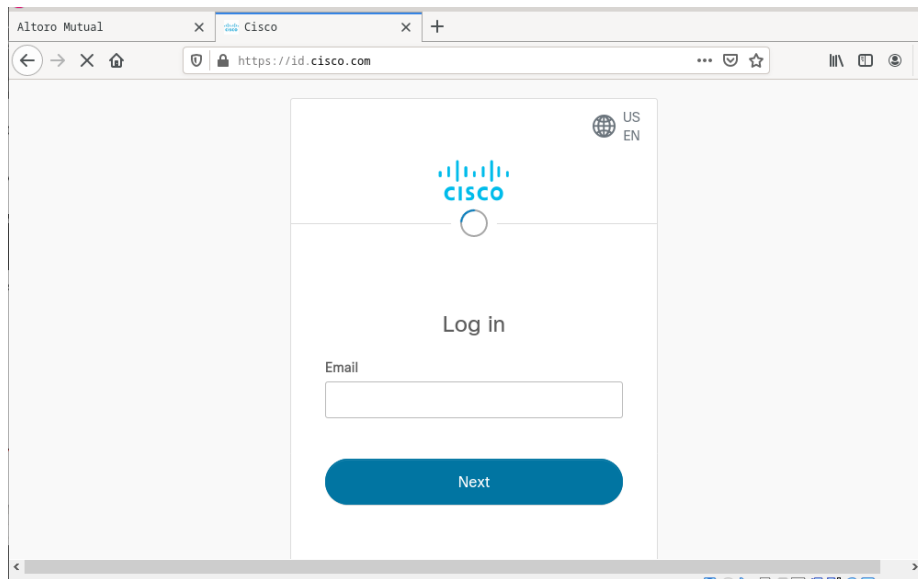
[sudo] password for analyst:

tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

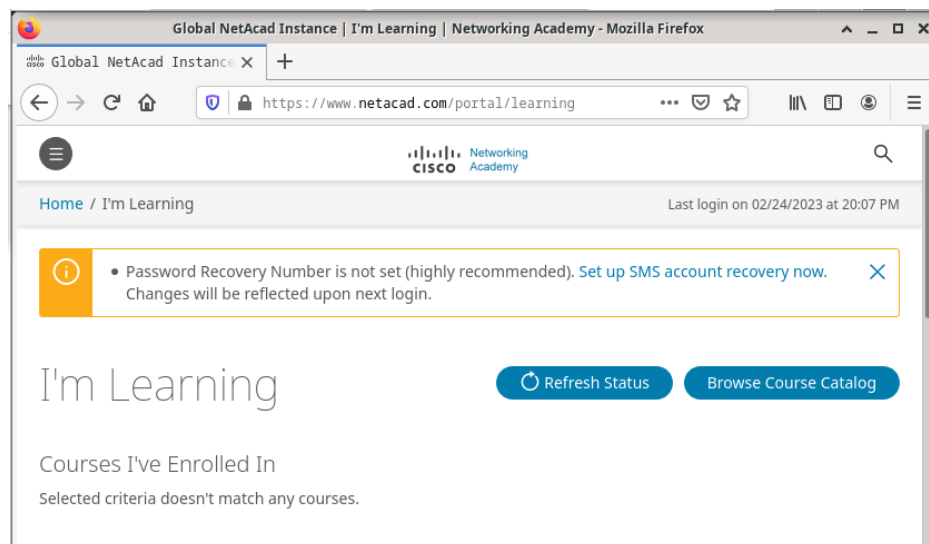


## 9. Buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM.

## 10. Klik Login

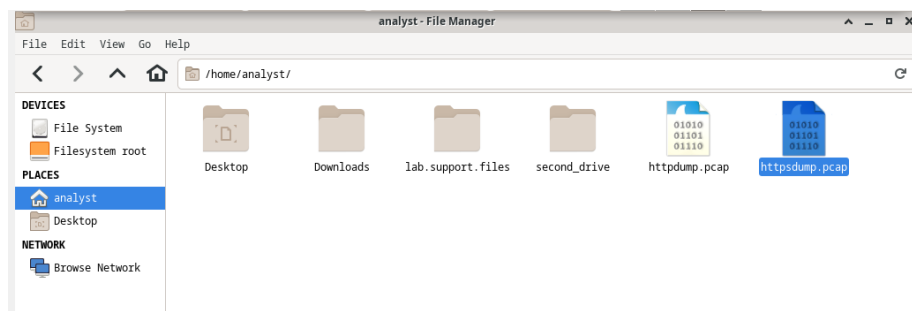


11. Masukkan username dan password anda



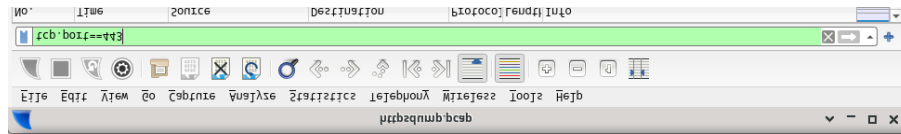
12. Melihat Rekaman Paket HTTPS

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

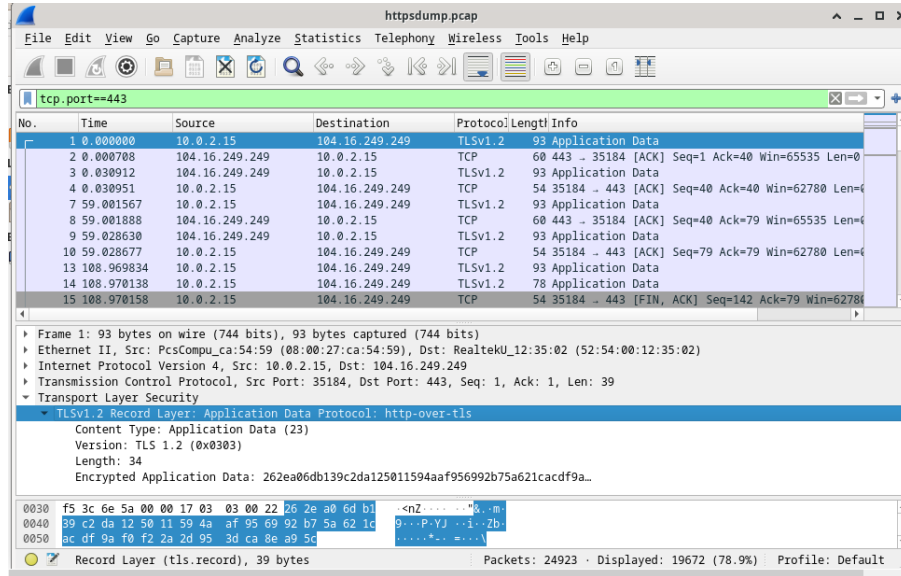


13. Filter tcp.port==443





#### 14. Pilih Application Data



#### 15. Analisis hasil yang didapatkan