

**LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 2**



DISUSUN OLEH:

Nama : Ardy Nugroho
NIM : 21/479068/SV/19428
Kelas : TRI A
Hari, Tanggal : Selasa, 21 Februari 2023
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M. Eng.

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

A. TUJUAN

- Mengesplorasi Nmap
- Melakukan Scan ke Port yang terbuka
- Merekam dan menganalisis trafik http
- 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.

C. ALAT DAN BAHAN

- CyberOps Workstation VM
- Koneksi Internet

D. LANGKAH KERJA

Eksplorasi Nmap

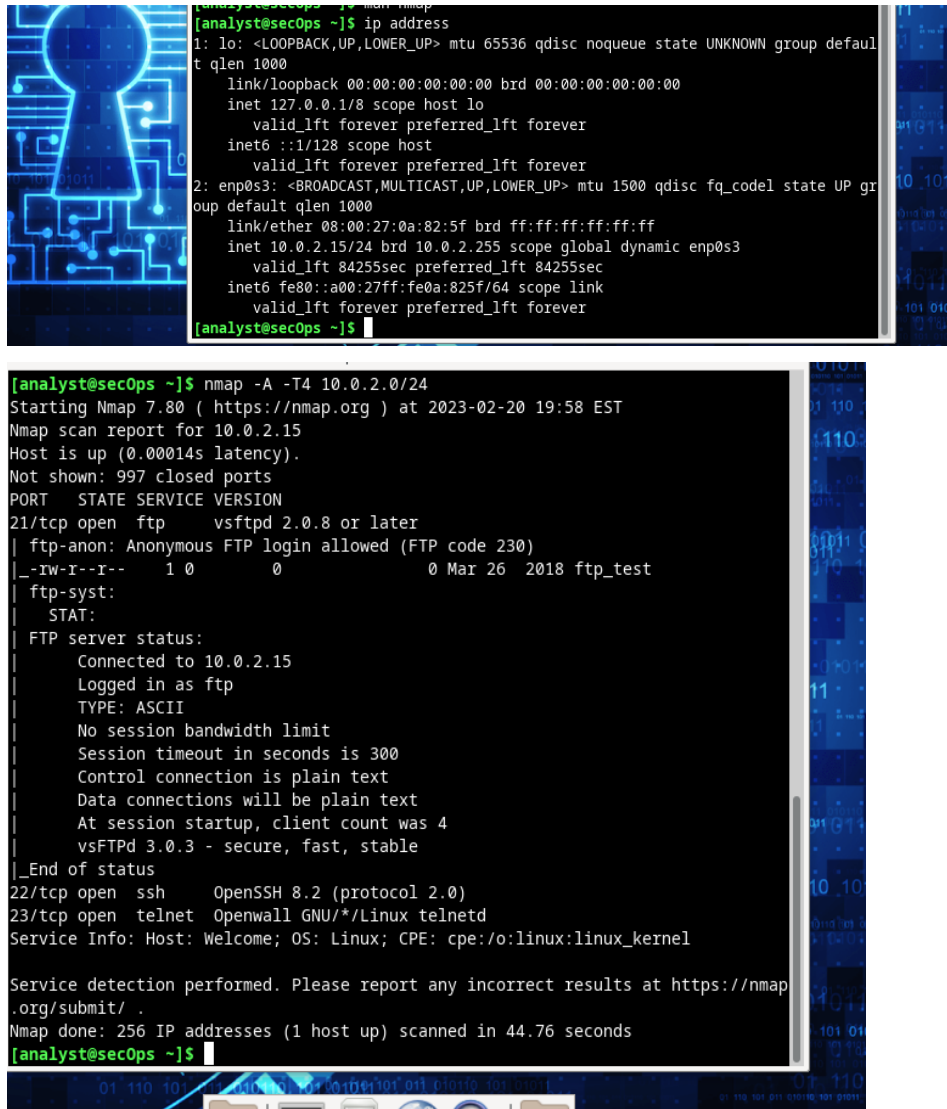
1. Eksplorasi Nmap dengan perintah **man nmap**

```
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  
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  
Manual page nmap(1) line 1 (press h for help or q to quit)
```

2. Localhost scanning; **nmap -A -T4 localhost**

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:40 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)  
|_-Iw-Ir-- 1 0      0      0 Mar 26 2018 ftp_test  
| ftp-syst:  
|   STATE:  
|   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 29.17 seconds  
[analyst@secOps ~]$
```

3. Network Scanning



The image shows a terminal window with a blue and black background featuring a stylized key icon. The terminal displays the output of the 'ip address' command and an nmap scan.

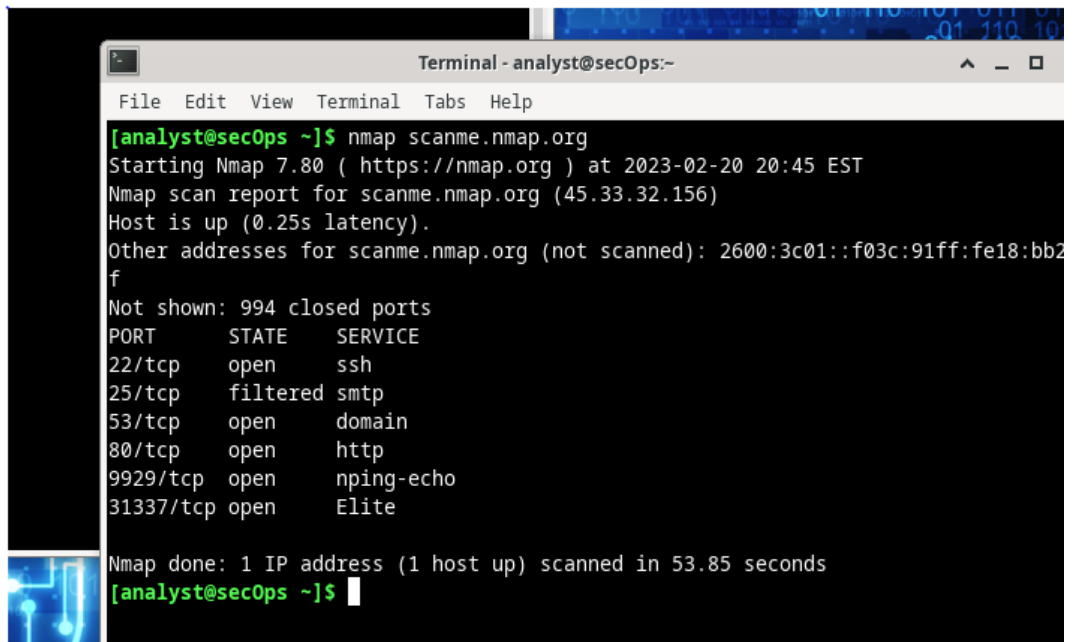
```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        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 08:00:27:0a:82:5f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 84255sec preferred_lft 84255sec
    inet6 fe80::a00:27ff:fe0a:825f/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```



```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:58 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_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 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: 256 IP addresses (1 host up) scanned in 44.76 seconds
[analyst@secOps ~]$
```

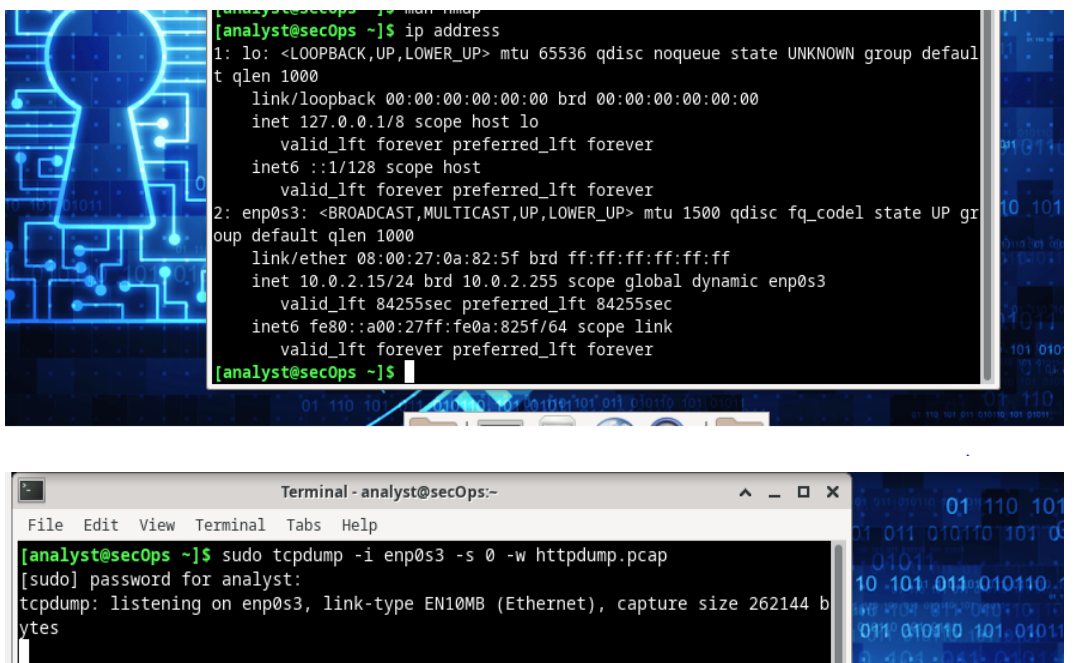
4. Remote Server Scanning



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ nmap scanme.nmap.org  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:45 EST  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.25s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 994 closed ports  
PORT      STATE      SERVICE  
22/tcp    open      ssh  
25/tcp    filtered  smtp  
53/tcp    open      domain  
80/tcp    open      http  
9929/tcp  open      nping-echo  
31337/tcp open      Elite  
  
Nmap done: 1 IP address (1 host up) scanned in 53.85 seconds  
[analyst@secOps ~]$
```

Pemantauan Trafik HTTP dan HTTPS dengan Wireshark

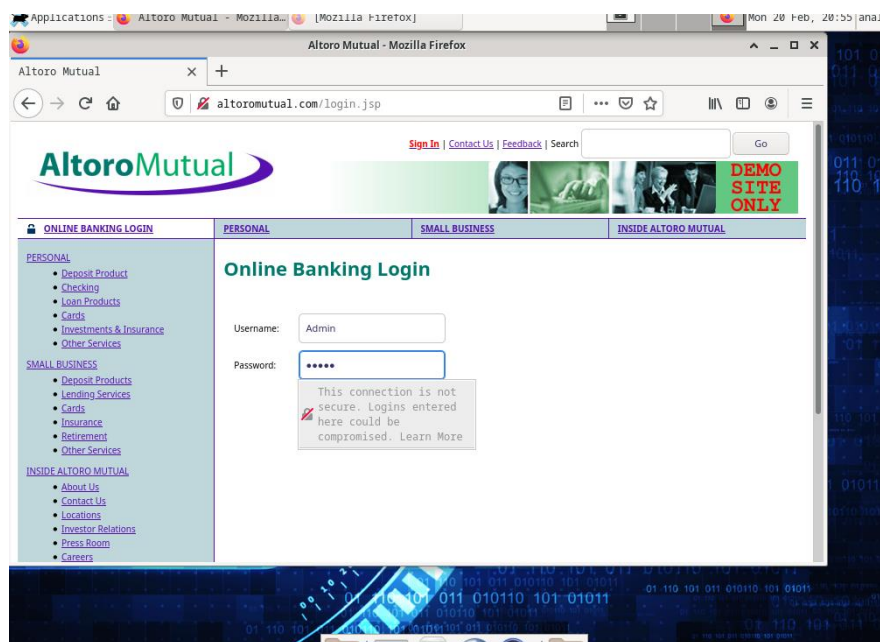
1. Jalankan perintah tcp dump



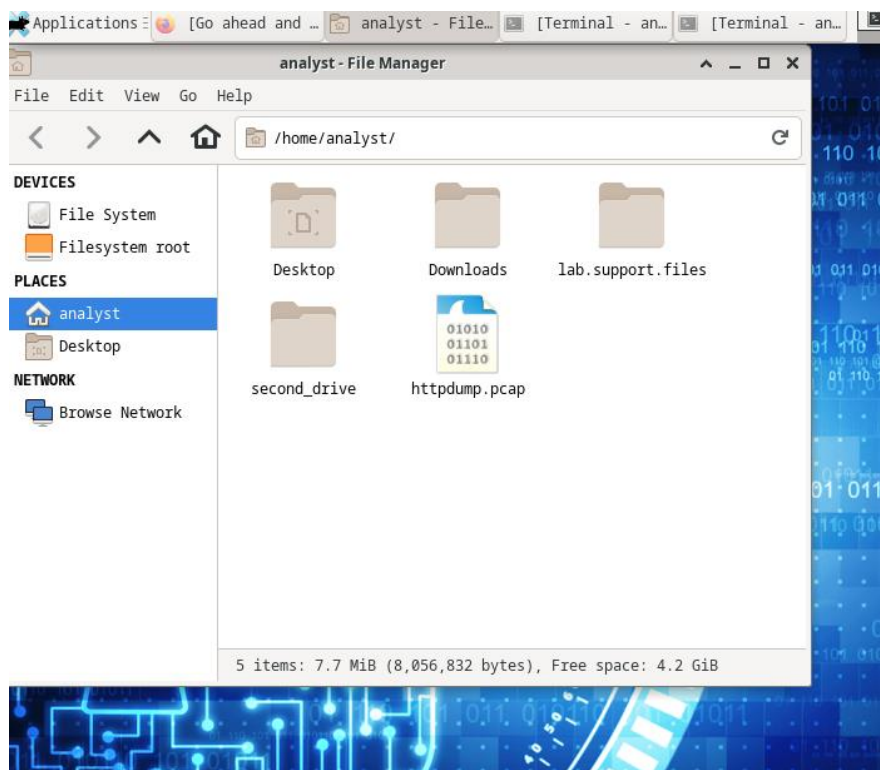
```
[analyst@secOps ~]$ ip address  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:0a:82:5f brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 84255sec preferred_lft 84255sec  
    inet6 fe80::a00:27ff:fe0a:825f/64 scope link  
        valid_lft forever preferred_lft forever  
[analyst@secOps ~]$
```

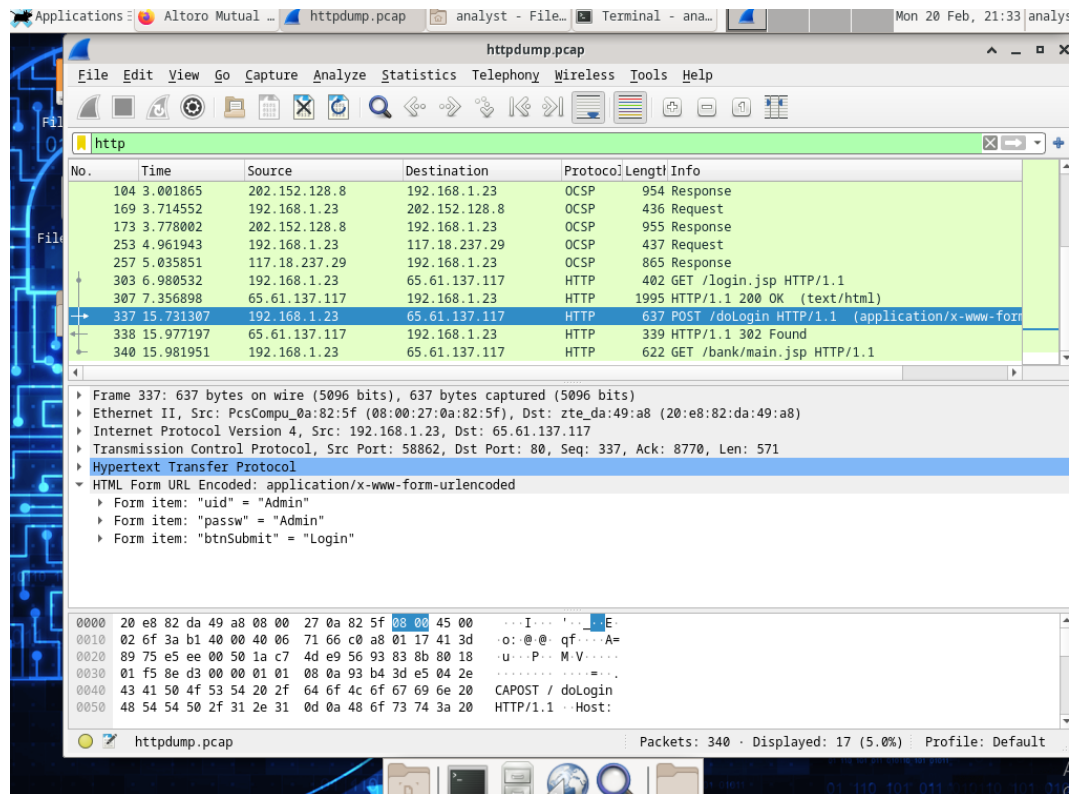
```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap  
[sudo] password for analyst:  
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes  
[analyst@secOps ~]$
```

2. Login ke web http

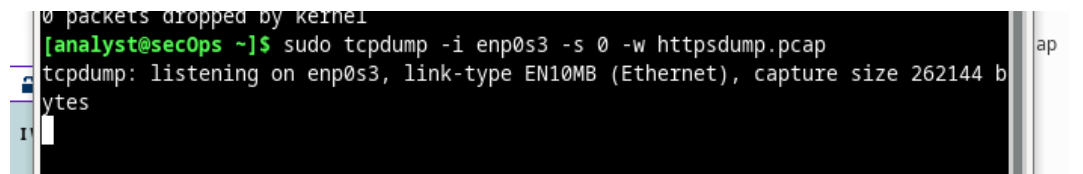


3. Buka file httpdump.pcap dengan wireshark

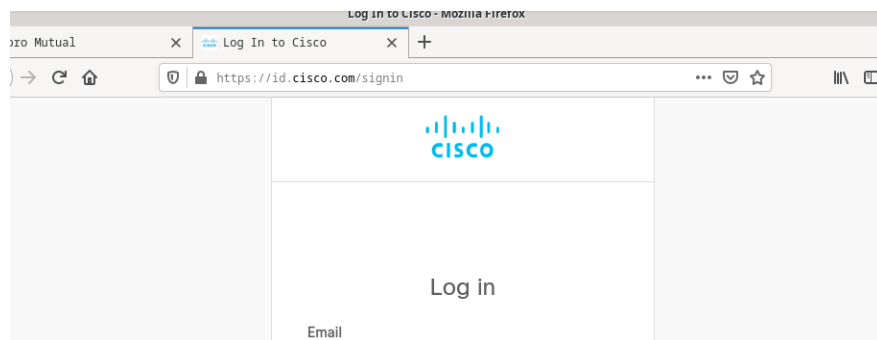




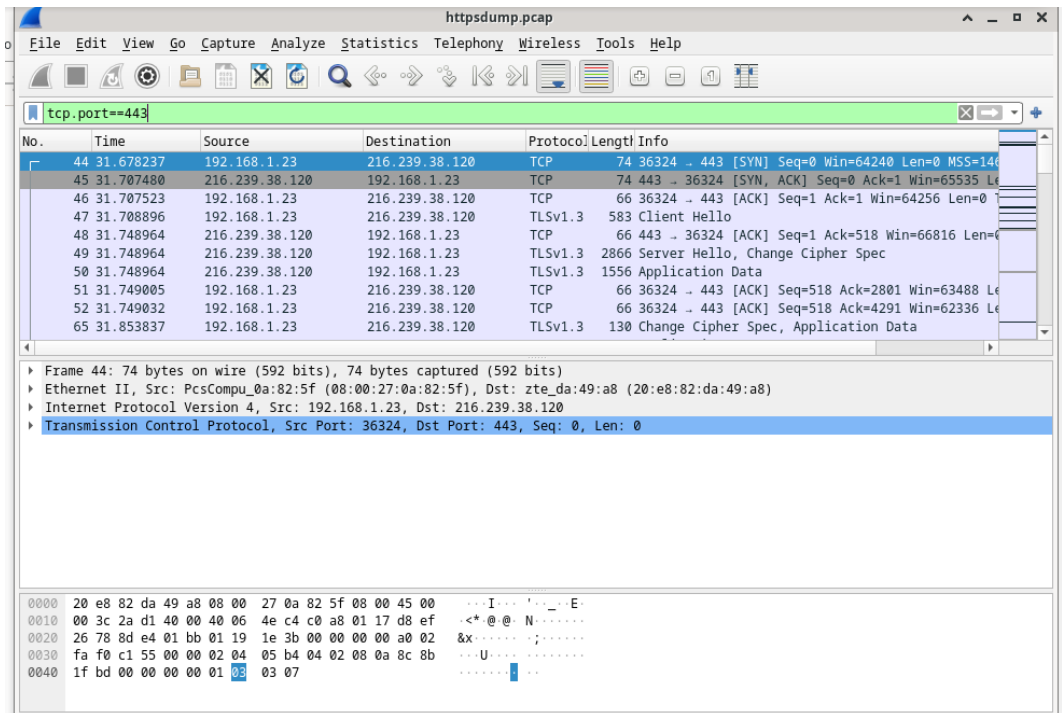
4. Merekam paket HTTPS, jalankan perintah tcpdump



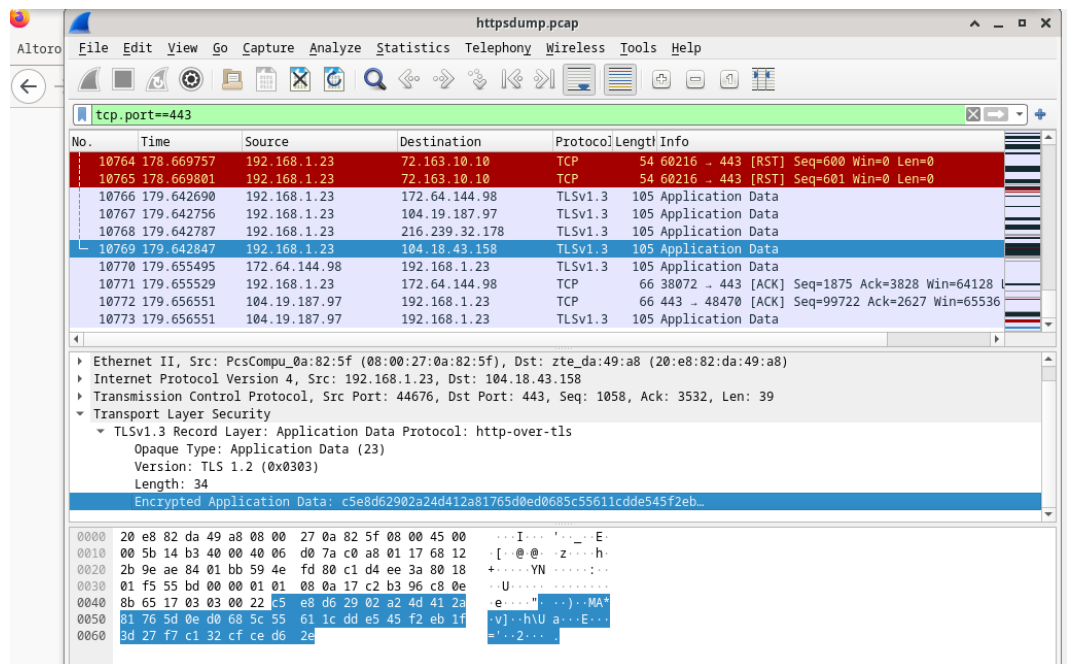
5. Login ke web https



6. Buka file httpsdump.pcap, kemudian lakukan filter **tcp.port == 443**



7. Pilih file application data



E. PEMBAHASAN

Praktikum ini dilaksanakan dengan melakukan eksplorasi pada *tools* yang terdapat di Nmap dan juga melakukan analisa trafik di HTTP dan HTTPS. Eksplorasi Nmap dilakukan pada terminal CyberOps workstation VM. Nmap dapat digunakan untuk melakukan *scanning* pada suatu host tertentu untuk mengetahui port-port yang terbuka. Nmap juga dapat digunakan untuk mengetahui layanan apa yang terbuka, alamat IP server dan sistem operasi yang digunakan oleh server.

Pemantauan trafik pada HTTP dan HTTPS dilakukan dengan bantuan Wireshark. Dengan menggunakan *command* *tcpdump* yang dituliskan di terminal, selanjutnya masuk pada situs web dengan mengisi *user information* dan *password*. Dari *command* *tcpdump* tadi, dihasilkan file dengan ekstensi *.pcap* yang dapat dianalisa dengan Wireshark. File yang berasal dari situs dengan protokol HTTP menampilkan UID dan kata sandinya, sementara file yang didapat dari situs HTTPS tidak dapat diperoleh informasi mengenai UID dan kata sandinya. Dari sini dapat disimpulkan bahwa protokol HTTPS dinilai lebih aman dibanding HTTP karena mengenkripsi data di dalamnya.

F. KESIMPULAN

Dari hasil praktikum ini diperoleh beberapa kesimpulan sebagai berikut.

- Nmap adalah alat yang digunakan untuk pemindaian jaringan
- Protokol HTTPS lebih aman daripada HTTP karena sudah mengenkripsi datanya