

**LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1**  
**UNIT 2 dan UNIT 3**  
**(EKSPLORASI NMAP dan PEMANTAUAN TRAFIK HTTP dan HTTPS**  
**DENGAN MENGGUNAKAN WIRESHARK)**



**DISUSUN OLEH**

**NAMA : ADITYA DARMASAPUTRA**  
**NIM : 21/480255/SV/19599**  
**KELAS : RI4AA**  
**DOSEN : ANNI KARIMATUL FAUZIYYAH, S.Kom., M.Eng.**

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

**2023**

## **A. Tujuan**

1. Mengexplorasi Nmap.
2. Melakukan scan ke port yang terbuka.
3. Merekam dan menganalisis trafik http.
4. Merekam dan menganalisis trafik https.

## **B. Alat dan Bahan**

1. Cyberops workstation virtual machine
2. Koneksi Internet.

## **C. Landasan Teori**

Virtual machine adalah program perangkat lunak atau sistem operasi virtual yang bisa digunakan pada sebuah perangkat keras bersamaan dengan OS asli perangkat tersebut. Fungsi utama virtual machine adalah untuk melakukan tugas-tugas yang tidak bisa dilakukan pada sistem operasi asli perangkat. Hal ini memungkinkan pengguna untuk menjalankan berbagai aplikasi pada virtual machine dan menggunakannya seperti biasanya pada perangkat tersebut. Setiap virtual machine akan menjalankan sistem operasinya sendiri dan berfungsi secara terpisah dari virtual machine lainnya, bahkan jika semuanya berjalan di perangkat yang sama. Cara kerja virtual machine sendiri juga sebenarnya cukup sederhana. Saat Anda membuka mesin virtual ini, VM akan berjalan sebagai proses di jendela aplikasi di OS perangkat fisik. Proses berjalannya virtual machine dikelola oleh perangkat lunak yang dikenal sebagai hypervisor. Hypervisor juga berfungsi untuk mengatur operasi di VM sehingga tidak membanjiri satu sama lain saat menggunakan sumber daya. Salah satu software yang sering digunakan untuk virtualisasi adalah VirtualBox.

VirtualBox adalah perangkat lunak virtualisasi untuk menginstal sistem operasi. Kata virtualisasi yaitu mengubah atau mengkonversi sesuatu menjadi bentuk simulasi dari bentuk real atau nyata. VirtualBox dapat menjalankan banyak OS secara bersamaan dalam satu waktu. Seperti *cyberops workstation* dan *security onion* yang merupakan sebuah sistem utama dan tidak dapat bekerja tanpa paket di dalamnya.

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.

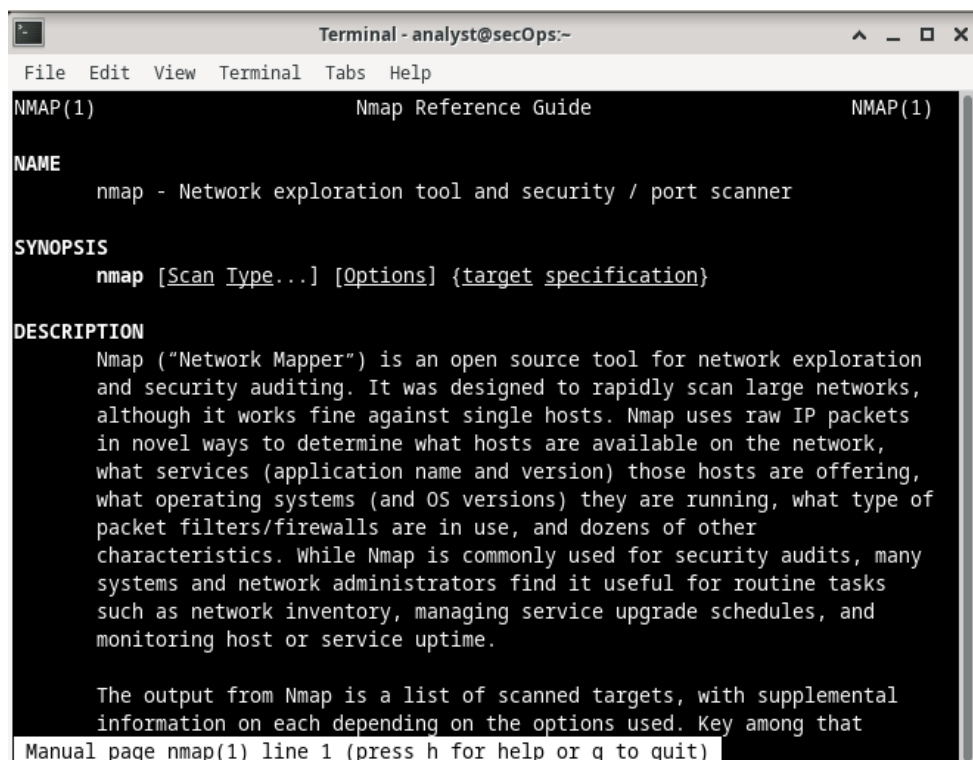
Terlepas dari HTTP atau HTTPS, hanya disarankan untuk bertukar data dengan situs web yang Anda percayai. Hanya karena sebuah situs menggunakan HTTPS tidak berarti itu adalah situs yang dapat dipercaya. Pelaku ancaman biasanya menggunakan HTTPS untuk menyembunyikan aktivitas mereka.

Di lab ini, Anda akan menjelajahi dan menangkap lalu lintas HTTP dan HTTPS menggunakan Wireshark.

## D. Data

### Unit 2

1. Melanjutkan dari praktikkum sebelumnya, sekarang buka terminal dan ketikkan **man nmap**. Jika ingin keluar, pencet **q**.



```
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)
```

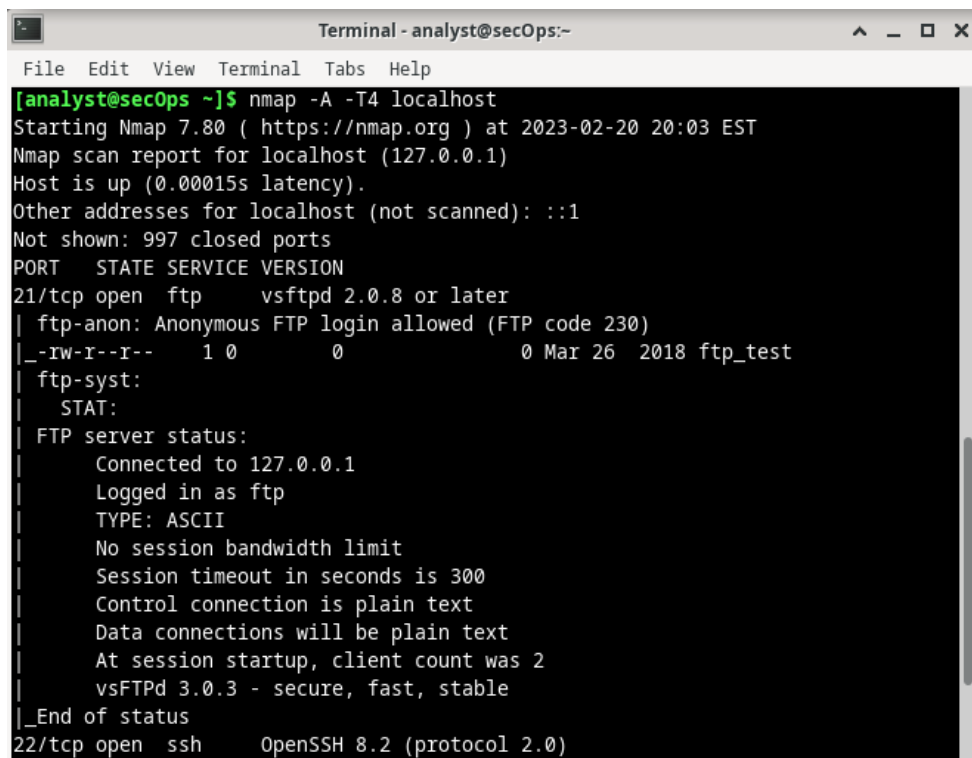
## Apa itu Nmap?

Nmap ("Network Mapper") adalah utilitas sumber terbuka dan gratis untuk penemuan jaringan dan audit keamanan. Banyak sistem dan administrator jaringan juga menganggapnya berguna untuk tugas-tugas seperti inventaris jaringan, mengelola jadwal peningkatan layanan, dan memantau waktu aktif host atau layanan.

## Apa fungsi dari Nmap?

Digunakan untuk memeriksa jaringan, menganalisa port, dan mengetahui sistem operasi yang digunakan.

2. Lalu ketikkan **nmap -A -T4 localhost**.



```
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 20:03 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00015s 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)
```

## Port dan layanan apa yang terbuka?

Terdapat 3 port, yaitu port 22 dengan layanan SSH, port 23 dengan layanan telnet, dan port 21 dengan layanan FTP.

## Software apa yang digunakan pada port yang terbuka tersebut?

Linux.

3. Sekarang kita akan melihat berapa IP address kita dengan perintah **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 group default qlen 1000
    link/ether 08:00:27:ee:60:0c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85637sec preferred_lft 85637sec
    inet6 fe80::a00:27ff:feee:600c/64 scope link
        valid_lft forever preferred_lft forever
```

**Berapakah alamat IP dan subnet mask dari PC host?**

IPnya adalah 10.0.2.15 dengan subnet mask 255.255.255.0 .

Setelah mengetahui ip addressnya, masukkan perintah **nmap -A -T4 10.0.2.0/24**.

```
Terminal - analyst@secOps:-
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 20:10 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 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
```

**Berapakah jumlah host yang terdeteksi?**

Ada 1 host aktif yaitu miliknya sendiri.

### Unit 3

1. Buka terminal dan ketikkan **tcpdump**.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
21:04:42.825319 IP 10.33.207.220.62864 > 172.217.194.94.https: UDP, length 1250
21:04:43.111707 IP 10.33.207.220.53457 > 172.253.118.147.https: UDP, length 1250
21:04:43.286235 IP 10.33.207.220.50004 > 35.186.224.39.https: Flags [P.], seq 86
0:903, ack 801, win 511, length 43
21:04:43.577976 ARP, Request who-has 10.33.192.1 (4c:5e:0c:59:78:45 (oui Unknown
)) tell 10.33.207.220, length 46
21:04:43.629139 ARP, Reply 10.33.192.1 is-at 4c:5e:0c:59:78:45 (oui Unknown), le
ngth 46
21:04:43.854459 IP 10.33.207.220.53457 > 172.253.118.147.https: UDP, length 1250
21:04:44.525203 IP 10.33.207.220.50471 > 202.61.204.169.krb524: Flags [S], seq 6
27495899, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
21:04:44.528642 IP 172.217.194.94.https > 10.33.207.220.62864: UDP, length 790
21:04:44.746624 IP 172.217.194.94.https > 10.33.207.220.62864: UDP, length 1250
21:04:44.748553 IP 10.33.207.220.62864 > 172.217.194.94.https: UDP, length 1250
21:04:44.749521 IP 10.33.207.220.62864 > 172.217.194.94.https: UDP, length 73
21:04:45.076778 IP 172.217.194.94.https > 10.33.207.220.62864: UDP, length 176
21:04:45.110667 IP 10.33.207.220.62864 > 172.217.194.94.https: UDP, length 33
21:04:45.342726 IP 10.33.207.220.53457 > 172.253.118.147.https: UDP, length 1250
21:04:46.447702 IP 10.33.207.220.53457 > 172.253.118.147.https: UDP, length 1250
^C
2699 packets captured
2699 packets received by filter
0 packets dropped by kernel
```

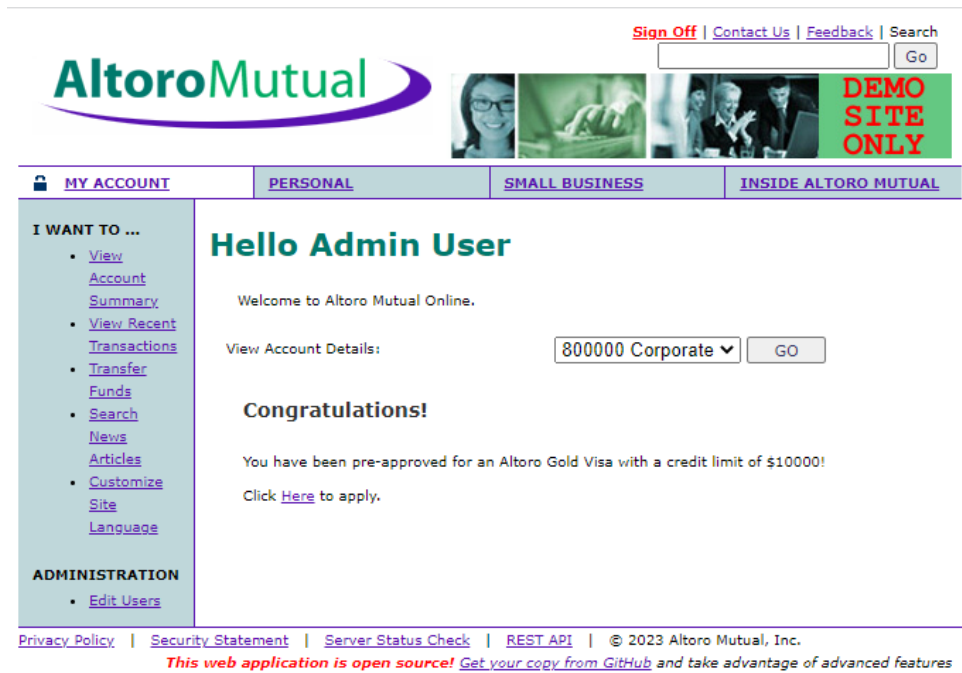
2. Cek IP address kita dengan perintah **ip address**.

```
[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 group default qlen 1000
    link/ether 08:00:27:ee:60:0c brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:feee:600c/64 scope link
        valid_lft forever preferred_lft forever
```

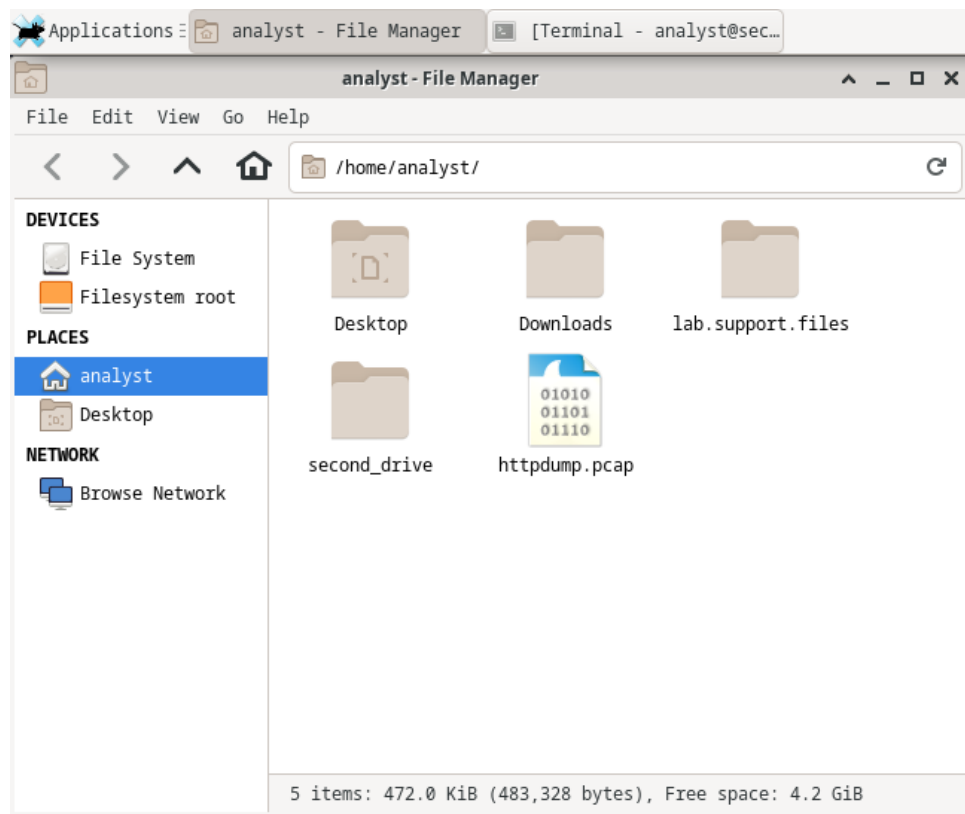
3. Setelah itu ketikkan **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap** dengan memasukkan password **cyberops**.

```
[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
```

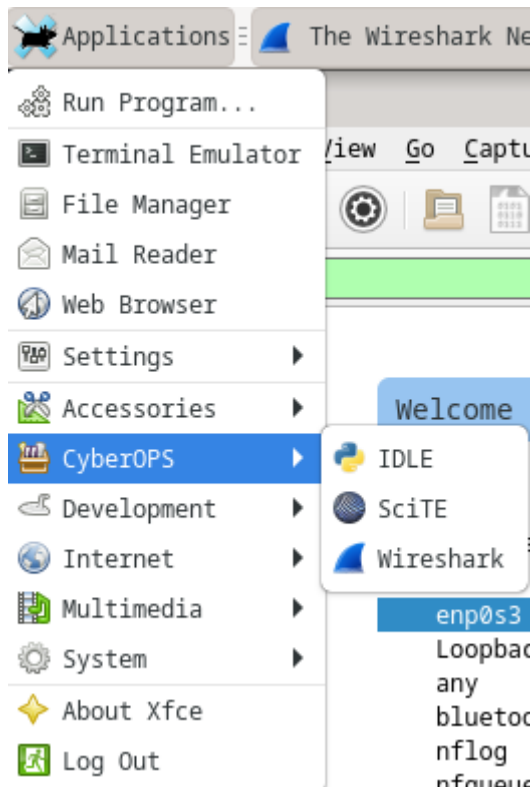
4. Masuk ke link <http://www.altoromutual.com/login.jsp>. Setelah muncul, masukkan user dan password dengan **admin**.



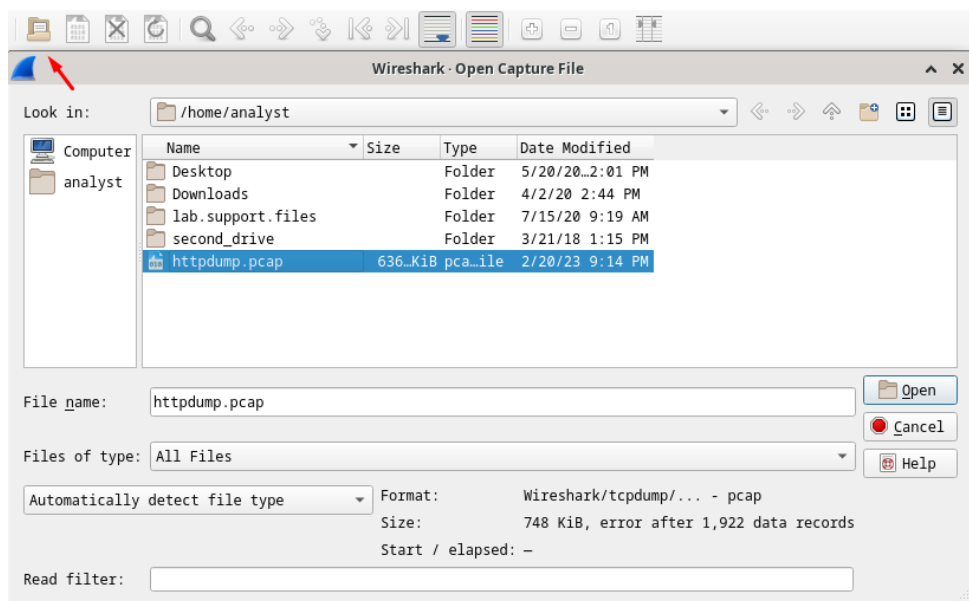
5. Tcpdump yang dijalankan akan berada pada **home – analyst**.



6. Kita akan menjalankan aplikasi wireshark yang sudah ada pada cyberops workstation dengan membuka menu **applications – cyberops**.



Jika sudah terbuka, import file yang tersimpan tadi ke dalam wireshark dengan klik ikon yang ditunjuk tanda panah dan open.



7. Cari protokol HTTP dengan informasi POST.



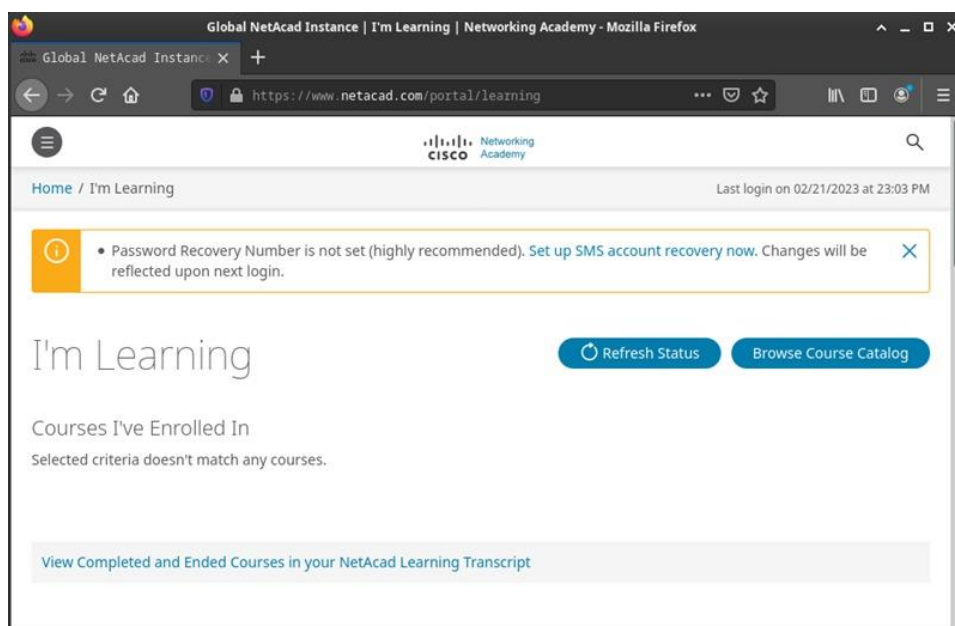
No.	Time	Source	Destination	Protocol	Length	Info
102	37.270590	10.33.207.220	65.61.137.117	HTTP	679	GET /login.jsp HTTP/1.1
114	37.601850	65.61.137.117	10.33.207.220	HTTP	8744	HTTP/1.1 200 OK (text/html)
337	49.264029	10.33.207.220	65.61.137.117	HTTP	679	GET /login.jsp HTTP/1.1
342	49.566854	65.61.137.117	10.33.207.220	HTTP	1844	HTTP/1.1 200 OK (text/html)
538	57.584792	10.33.207.220	65.61.137.117	HTTP	895	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
541	57.924507	65.61.137.117	10.33.207.220	HTTP	327	HTTP/1.1 302 Found
543	57.932312	10.33.207.220	65.61.137.117	HTTP	757	GET /bank/main.jsp HTTP/1.1
552	58.291507	65.61.137.117	10.33.207.220	HTTP	6466	HTTP/1.1 200 OK (text/html)

▶ Frame 538: 895 bytes on wire (7160 bits), 895 bytes captured (7160 bits)  
 ▶ Ethernet II, Src: LiteonTe\_73:54:6b (f8:a2:d6:73:54:6b), Dst: Routerbo\_59:78:45 (4c:5e:0c:59:78:45)  
 ▶ Internet Protocol Version 4, Src: 10.33.207.220, Dst: 65.61.137.117  
 ▶ Transmission Control Protocol, Src Port: 50489, Dst Port: 80, Seq: 1251, Ack: 17381, Len: 841  
 ▶ Hypertext Transfer Protocol  
 ▶ HTML Form URL Encoded: application/x-www-form-urlencoded

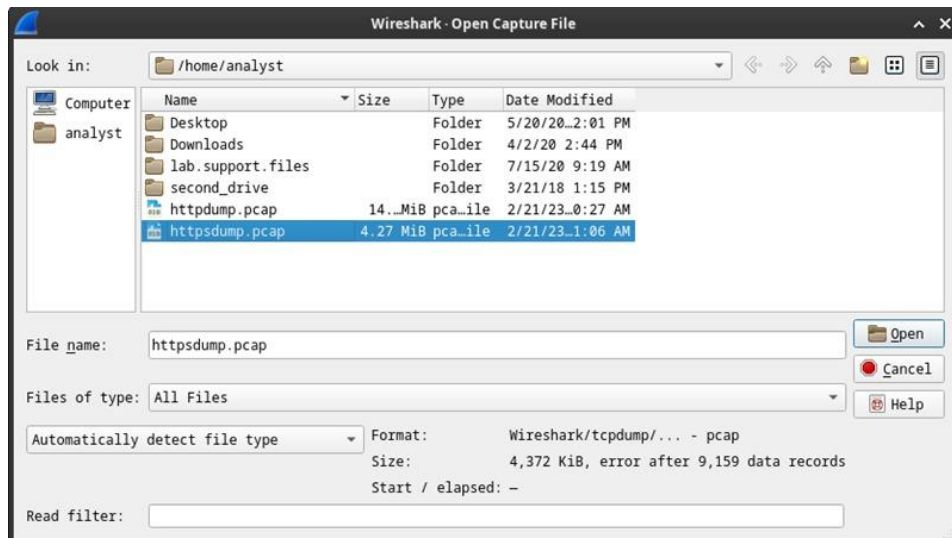
8. Kita akan cari informasi tentang user dan passwordnya dengan klik tulisan **Hypertext Transfer Protocol**.

Hypertext Transfer Protocol	
▶ HTML Form URL Encoded:	application/x-www-form-urlencoded
▶ Form item:	"uid" = "Admin"
▶ Form item:	"passw" = "Admin"
▶ Form item:	"btnSubmit" = "Login"

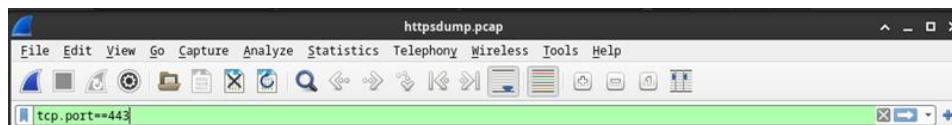
9. Selanjutnya kita akan membuka browser untuk login ke netacad pada OS ini. Letaknya ada pada **applications – internet**.



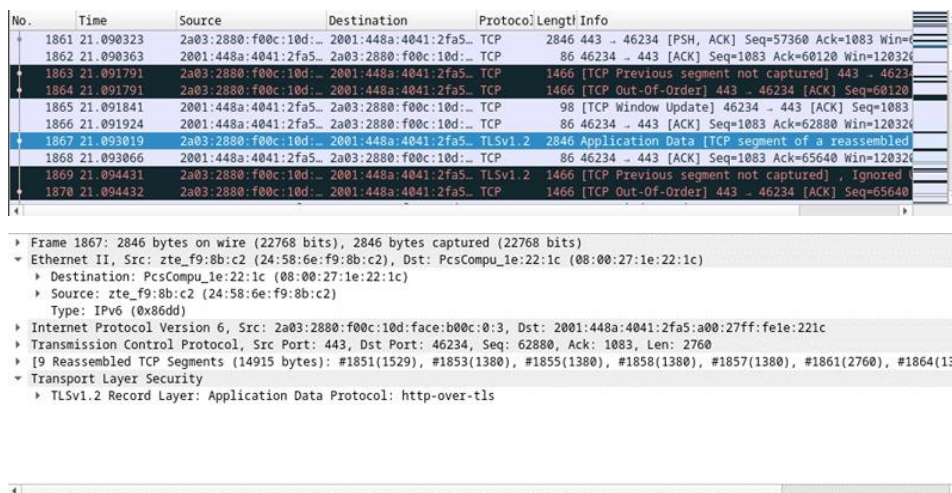
10. Netacad dibuka menggunakan https. Kita cek pada bagian **home – analyst** karena file akan tersimpan disana. Lalu buka menggunakan wireshark.



11. Search **tcp.port==443** pada wireshark.



12. Cari yang bertuliskan **application data** dan analisis.



## E. Pembahasan

Pada praktikum kali ini kita akan menganalisis cara kerja nmap dan tcpdump pada unit 2 dan unit 3.

Unit 2 percobaan 1 menampilkan pengenalan Nmap itu sendiri dimana dideskripsikan cukup lengkap. Percobaan 2 menganalisa keseluruhan localhost yang merupakan server lokal dari cyberops itu sendiri dengan menampilkan beberapa port/host yang aktif, dan juga layanan yang terdapat pada masing-masing port itu sendiri. Percobaan 3 menganalisa

berapa IP address yang didapat oleh host tersebut beserta subnet masknya. Percobaan 4 menganalisis apa saja yang terdapat pada IP address 10.0.2.15/24. Namun pada percobaan itu saya menuliskan networknya. Terlihat bahwa ada 1 host aktif menggunakan port FTP.

Unit 3 diminta untuk merekam paket http dan https yang aktif. Cara menghidupkannya adalah dengan mengetikkan **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap** dimana tcpdump mulai merekam trafik jaringan pada interface enp0s3. Sedangkan -i untuk menentukan interface mana yang akan direkam, lalu -s menentukan Ppanjang snapshot untuk setiap paket, dan -w untuk menulis hasil dari tcpdump. Kita bisa cek paket juga dengan membuka wireshark dan mencari http/https yang terdapat banyak informasi di dalamnya. Pada bagian POST di http dan jika kita klik kepanjangan http di bawah, akan muncul data user dan passwordnya. Pada saat pindah ke https, pada application data akan muncul SSL yang sebelumnya tidak ada ada http karena memang menggunakan https lebih secure daripada http dan pesannya terenkripsi dengan kode-kode.

## F. Kesimpulan

HTTPS memunculkan secure data dan pesan di dalamnya terenkripsi sehingga tidak bisa terbaca selain daripada perangkat tersebut yang mempunyai bagian terenkripsi.

## G. Daftar Pustaka

- *BAB IV ANALISA DAN PERANCANGAN*. (n.d.). Repository UIN Suska. Retrieved February 20, 2023, from <https://repository.uin-suska.ac.id/17326/9/9.%20BAB%20IV.pdf>
- *Pengertian, Sejarah, Fungsi dan Manfaat VirtualBox - Biro Administrasi Registrasi Kemahasiswaan dan Informasi*. (2022, January 4). Biro Administrasi Kemahasiswaan, Alumni dan Informasi. Retrieved February 20, 2023, from <https://barki.uma.ac.id/2022/01/04/pengertian-sejarah-fungsi-dan-manfaat-virtualbox/>
- *Security Onion: distro ideal Anda untuk mengaudit jaringan*. (n.d.). Linux Adictos. Retrieved February 20, 2023, from <https://www.linuxadictos.com/id/security-onion-distro-ideal-Anda-untuk-mengaudit-jaringan.html>
- *Virtual Machine: Pengertian, Jenis-jenis, dan Manfaatnya - Biro Administrasi Registrasi Kemahasiswaan dan Informasi*. (2021, December 30). Biro Administrasi Kemahasiswaan, Alumni dan Informasi. Retrieved February 20, 2023, from

<https://barki.uma.ac.id/2021/12/30/virtual-machine-pengertian-jenis-jenis-dan-manfaatnya/>

- (n.d.). Nmap: the Network Mapper - Free Security Scanner. Retrieved February 27, 2023, from <https://nmap.org/>
- *4.6.6.5 Lab – Using Wireshark to Examine HTTP and HTTPS (Instructor Version)*. (2019, June 27). ITExamAnswers.net. Retrieved February 27, 2023, from <https://itexamanswers.net/4-6-6-5-lab-using-wireshark-to-examine-http-and-https-instructor-version.html>
- *Pengertian dan Penggunaan Perintah Tcpdump di Linux*. (n.d.). LinuxID. Retrieved February 27, 2023, from <https://www.linuxid.net/32373/pengertian-dan-penggunaan-perintah-tcpdump-di-linux/>