

**LAPORAN PRAKTIKUM  
KEAMANAN INFORMASI 1  
UNIT 2**



**DI SUSUN OLEH**

Nama : Bintang Nur K  
NIM : 21/481453/SV/19790  
Kelas : RI4AA  
Hari, tanggal : Selasa, 21 Februari 2023  
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng  
Asisten Praktikum : Gabriella Alvera Chaterine

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

## UNIT 2

### EKSPLORASI NMAP & Pemantauan Trafik HTTP dan HTTPS menggunakan Wireshark

#### I. TUJUAN

- Mengexplorasi Nmap
- Melakukan Scan ke Port yang terbuka
- Merekam dan menganalisis trafik http
- Merekam dan menganalisis trafik https

#### II. LATAR BELAKANG

*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*.

Nmap (“*Network Mapper*”) merupakan sebuah tool *open source* untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal

*Wireshark* adalah sebuah aplikasi *capture paket data* berbasis *open-source* yang berguna untuk memindai dan menangkap trafik data pada jaringan internet. Aplikasi ini umum digunakan sebagai alat *troubleshoot* pada jaringan yang bermasalah, selain itu juga biasa digunakan untuk pengujian *software* karena kemampuannya untuk membaca konten dari tiap paket trafik data

*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.

### III. ALAT DAN BAHAN

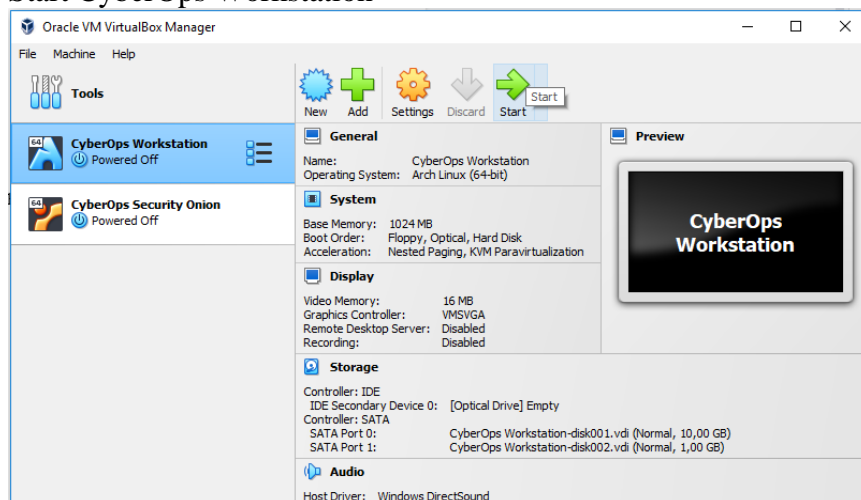
Alat dan Bahan yang dibutuhkan untuk melaksanakan praktikum adalah

- CyberOps Workstation Virtual Machine
- Koneksi Internet

### IV. LANGKAH KERJA DAN HASIL

#### UNIT 2


1. Eksplorasi Nmap  
Buka VM VirtualBox  
Start CyberOps Workstation



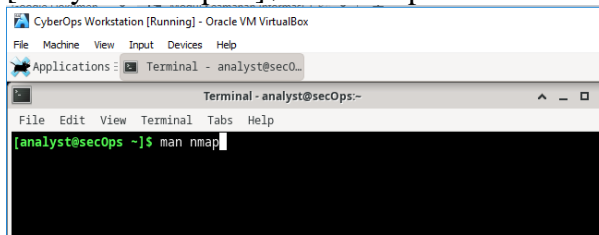
Masukkan username dan password

Username: analyst

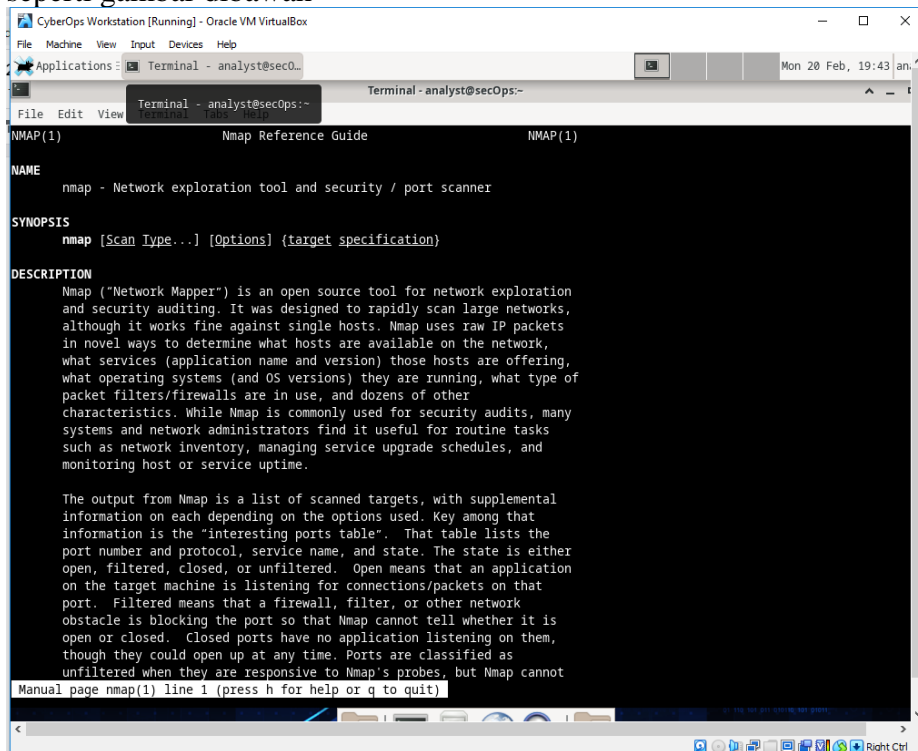
Password: cyberops



Buka terminal kemudian ketikkan  
[analyst@secOps ~]\$ man nmap



Setelah mengetik “man nmap” klik enter lalu akan muncul penjelasan seperti gambar dibawah

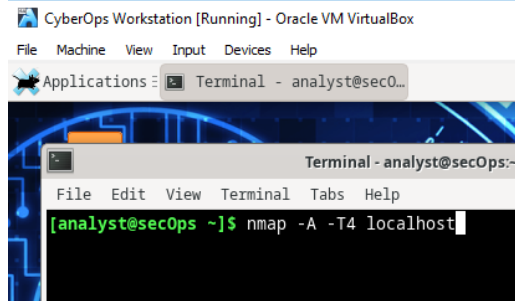


Apa itu Nmap? Apa fungsi dari Nmap?

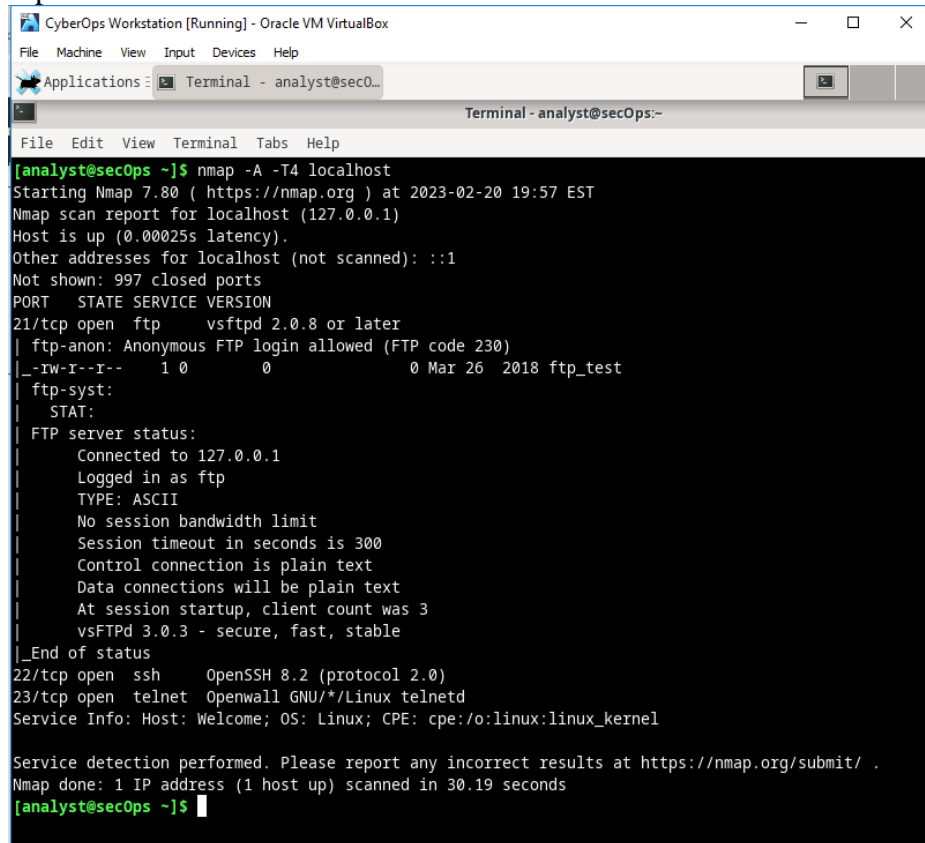
Nmap ("Network Mapper") adalah alat untuk eksplorasi jaringan dan audit keamanan. Ini dirancang untuk memindai jaringan besar dengan cepat, meskipun bekerja dengan baik terhadap host tunggal. Nmap menggunakan paket IP mentah dengan cara baru untuk menentukan host apa yang tersedia di jaringan, layanan apa (nama aplikasi dan versi) host yang ditawarkan, sistem operasi apa (dan versi OS) yang mereka jalankan, filter paket/firewall jenis apa yang digunakan, dan puluhan karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, banyak sistem dan administrator jaringan merasa berguna untuk tugas rutin seperti inventaris jaringan, mengelola jadwal peningkatan layanan, dan memantau host atau uptime layanan.

## 2. Localhost Scanning

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



Setelah mengetik “nmap -A -T4 localhost” maka akan muncul keterangan seperti dibawah



Port dan layanan apa yang terbuka?

Port yang terbuka adalah 21/tcp, 22/tcp, dan 23/tcp,

Untuk layanan yang terbuka adalah ftp, ssh, telnet

Software apa yang digunakan pada port yang terbuka tersebut?

vsftpd, OpenSSH 8.2, Openwall GNU/\*/Linux telnetd

### 3. Network Scanning

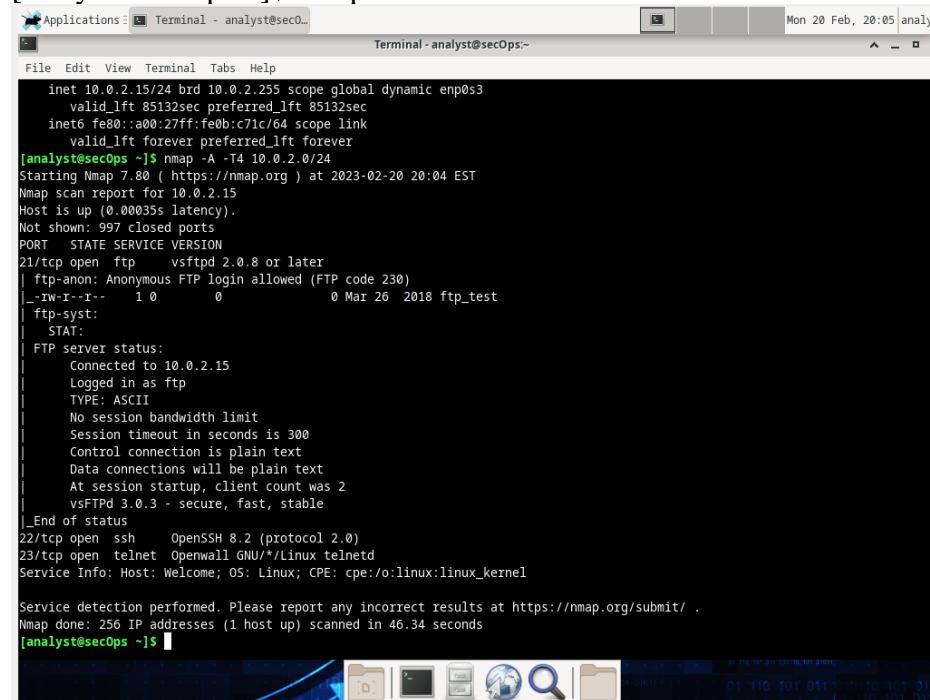
Sebelum melakukan scanning alangkah lebih baiknya untuk mengetahui alamat IP host terlebih dahulu.

[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 group default qlen 1000
    link/ether 08:00:27:0b:c7:1c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85132sec preferred_lft 85132sec
    inet6 fe80::a00:27ff:fe0b:c71c/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Berapakah alamat IP dan subnet mask dari PC host?  
10.0.2.15/24

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



```
File Edit View Terminal Tabs Help
Terminal - analyst@secOps
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
    valid_lft 85132sec preferred_lft 85132sec
    inet6 fe80::a00:27ff:fe0b:c71c/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 20:04 EST
Nmap scan report for 10.0.2.15
Host is up (0.00035s 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 46.34 seconds
[analyst@secOps ~]$
```

Berapakah jumlah host yang terdeteksi?  
1 (host up)

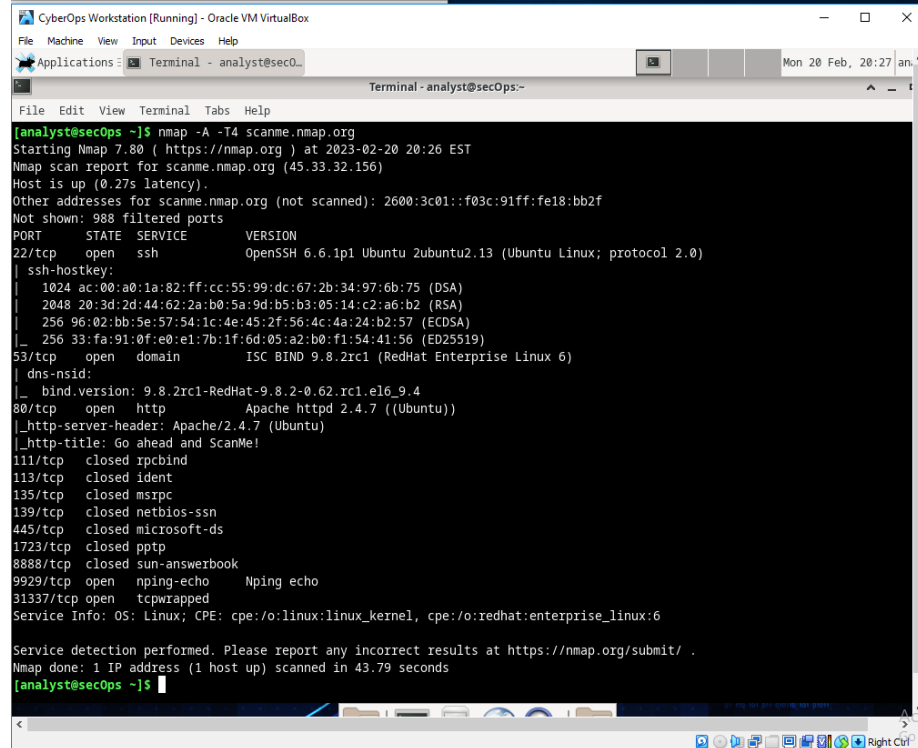
4.

#### Remote Server Scanning

Buka web browser dan kunjungi scanme.nmap.org

Ketikkan perintah berikut:

[analyst@secOps Desktop]\$ nmap -A -T4 scanme.nmap.org



```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:26 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 988 filtered 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)
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!
111/tcp   closed rpcbind
113/tcp   closed ident
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
445/tcp   closed microsoft-ds
1723/tcp  closed pptp
8888/tcp  closed sun-answerbook
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 43.79 seconds
[analyst@secOps ~]$
```

Port dan layanan apa yang terbuka?

Port yang terbuka:

- 22/tcp
- 53/tcp
- 80/tcp
- 111/tcp
- 113/tcp
- 135/tcp
- 139/tcp
- 445/tcp
- 1723/tcp
- 8888/tcp
- 9929/tcp
- 31337/tcp

Layanan yang terbuka: open ssh, nping-echo, tcpwrapped

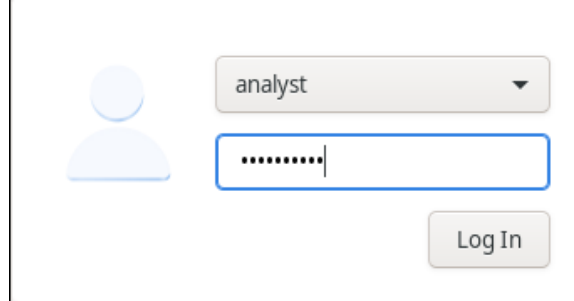
Apa sistem operasi yang digunakan oleh server?

Linux

### UNIT 3

#### Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark

1. Jalankan VM dan Login Username: analyst Password: cybercops



A login form with a user icon, a dropdown menu showing 'analyst', a password field with masked characters, and a 'Log In' button.

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]
```

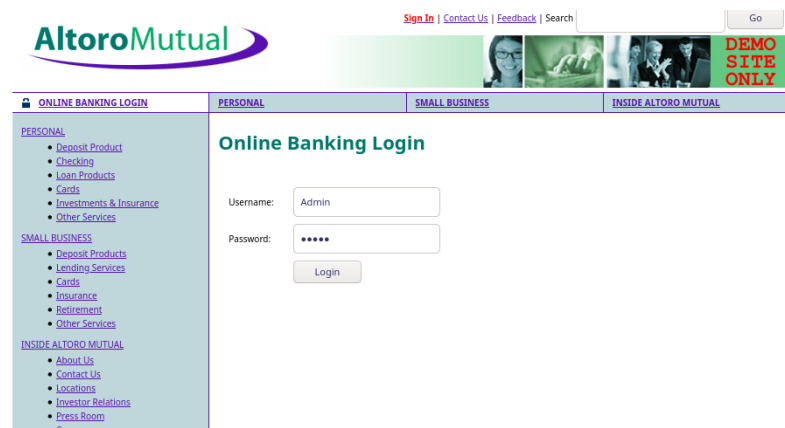
password for analyst: (diisi dengan cyberops)

```
[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 08:00:27:0b:c7:1c brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 86189sec preferred_lft 86189sec  
    inet6 fe80::a00:27ff:fe0b:c71c/64 scope link  
        valid_lft forever preferred_lft forever  
[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
```

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

Username: Admin

Password: Admin



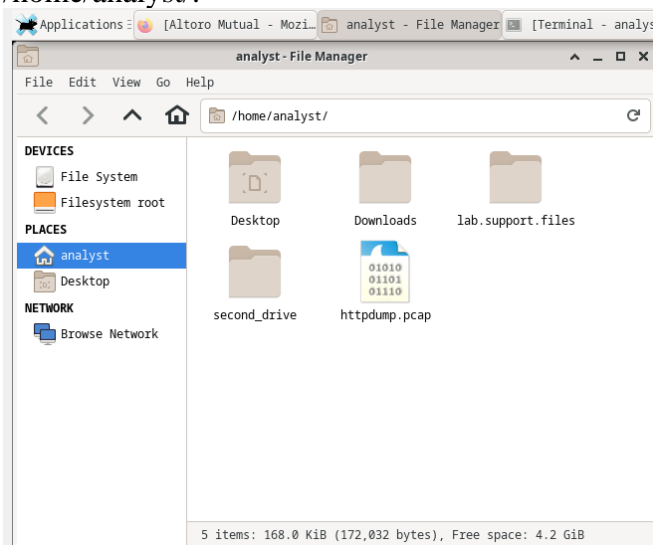
The screenshot shows the AltoroMutual website's online banking login page. The header includes the AltoroMutual logo, navigation links (Sign In, Contact Us, Feedback, Search), and a 'Go' button. The main content area is titled 'Online Banking Login' and features a login form with fields for 'Username' (containing 'Admin') and 'Password' (masked with dots), and a 'Login' button. The left sidebar contains a menu with categories: PERSONAL (Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services), SMALL BUSINESS (Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services), and INSIDE ALTORO MUTUAL (About Us, Contact Us, Locations, Investor Relations, Press Room, Careers).



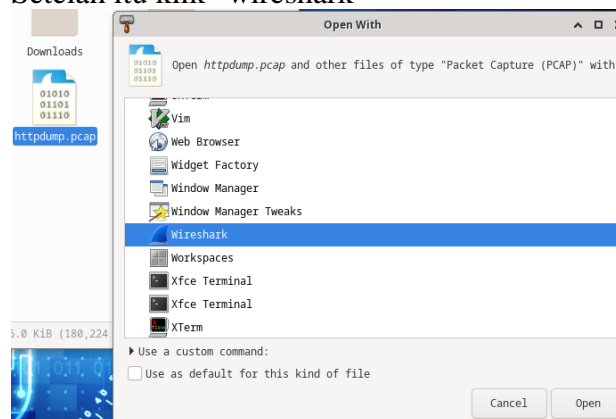
Setelah login akan muncul tampilan seperti ini



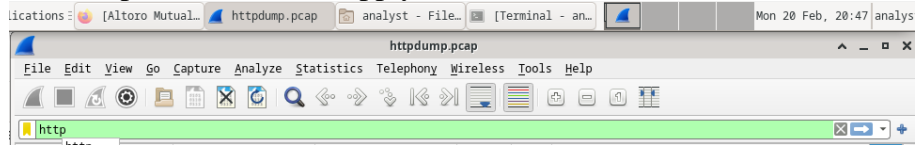
4. Merekam Paket HTTP  
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/.



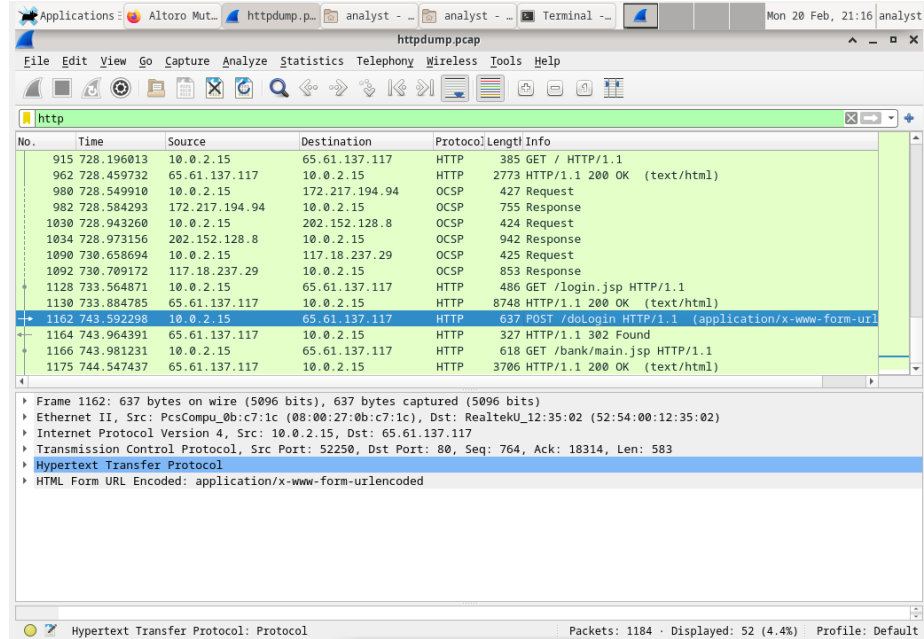
Setelah itu klik “wireshark”



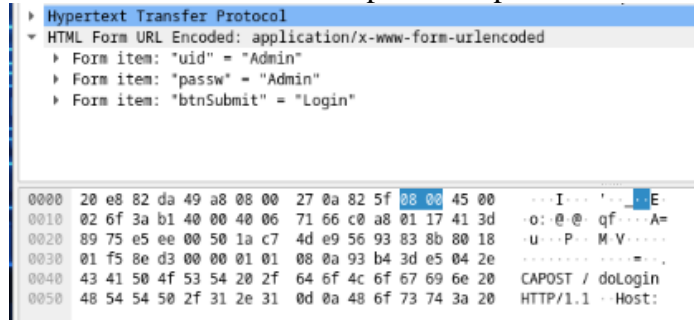
## 5. Filter http kemudian klik Apply



## 6. Pilih POST

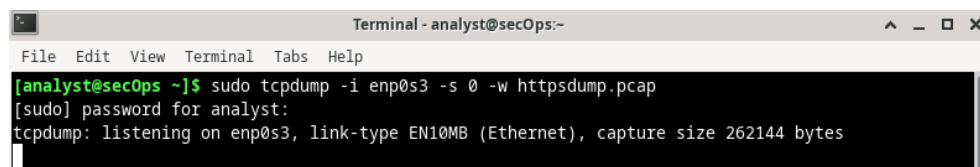


## 7. Lakukanlah analisis terhadap uid dan password

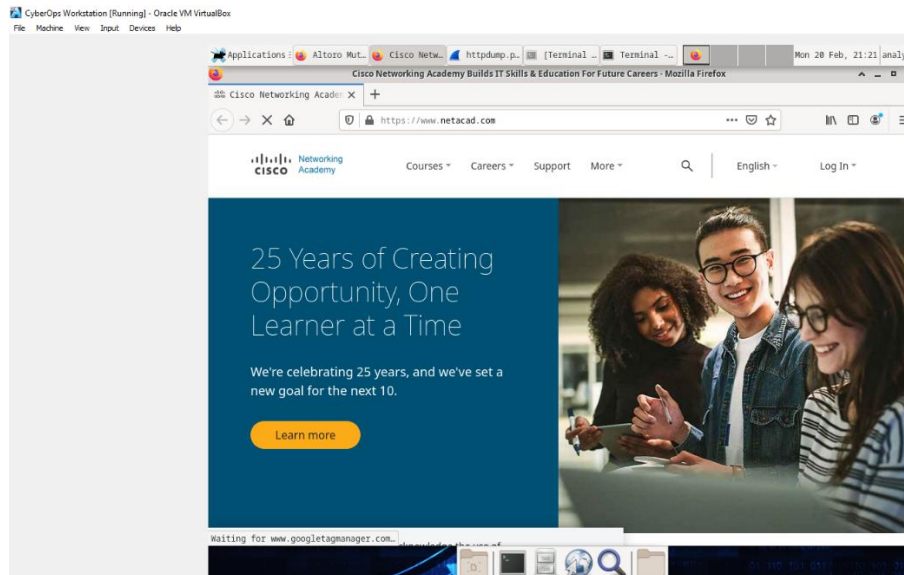


## 8. Merekam Paket HTTPS

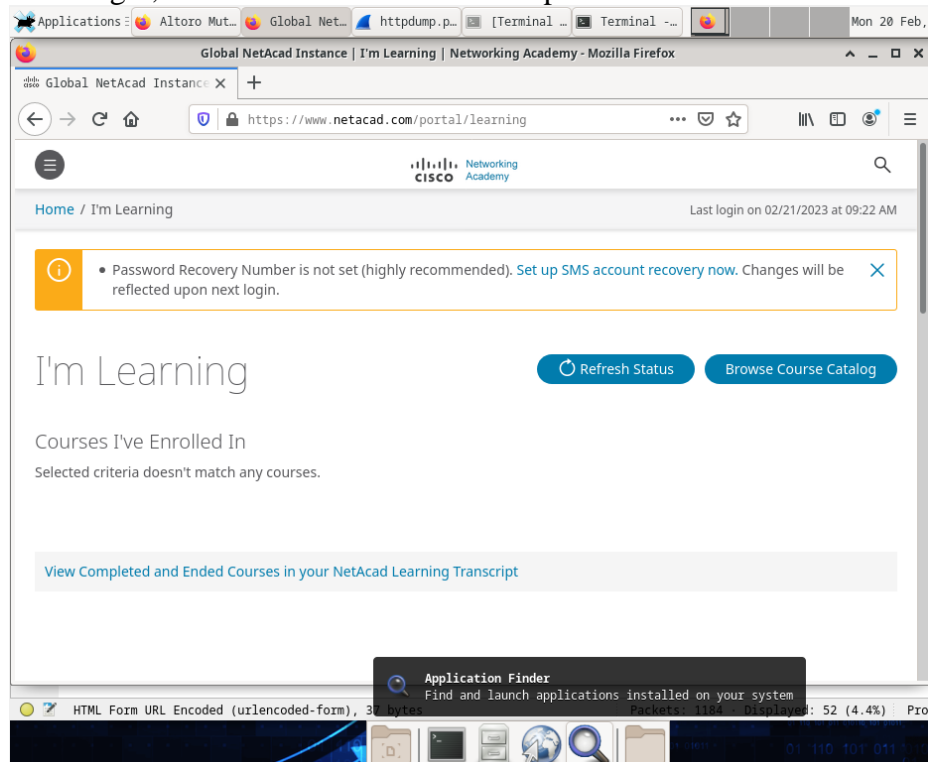
[analyst@secOps ~]\$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap  
[sudo] password for analyst:



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

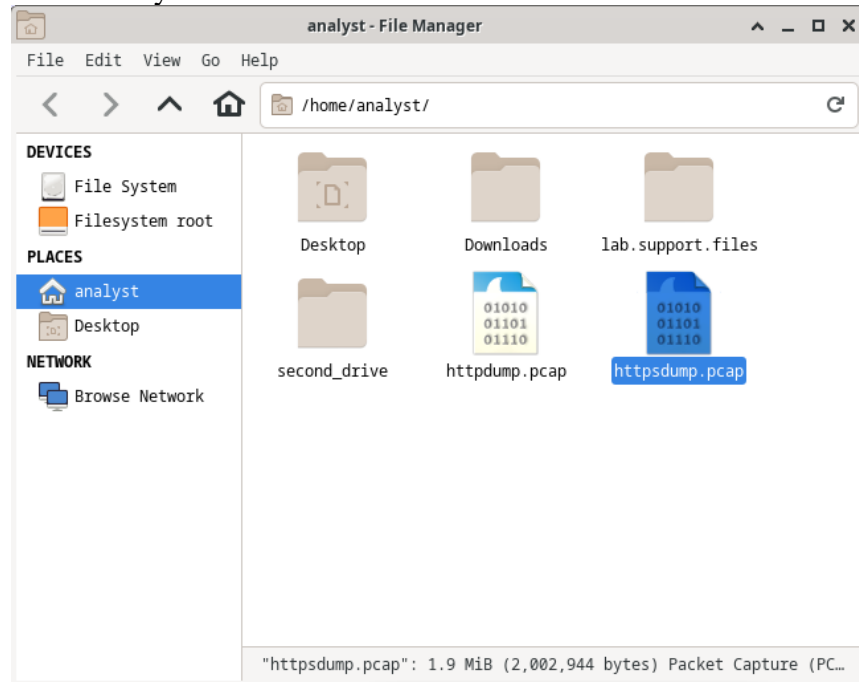


10. Klik Login, dan masukkan username dan password anda

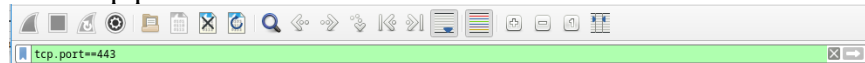


## 12. Melihat Rekaman Paket HTTPS

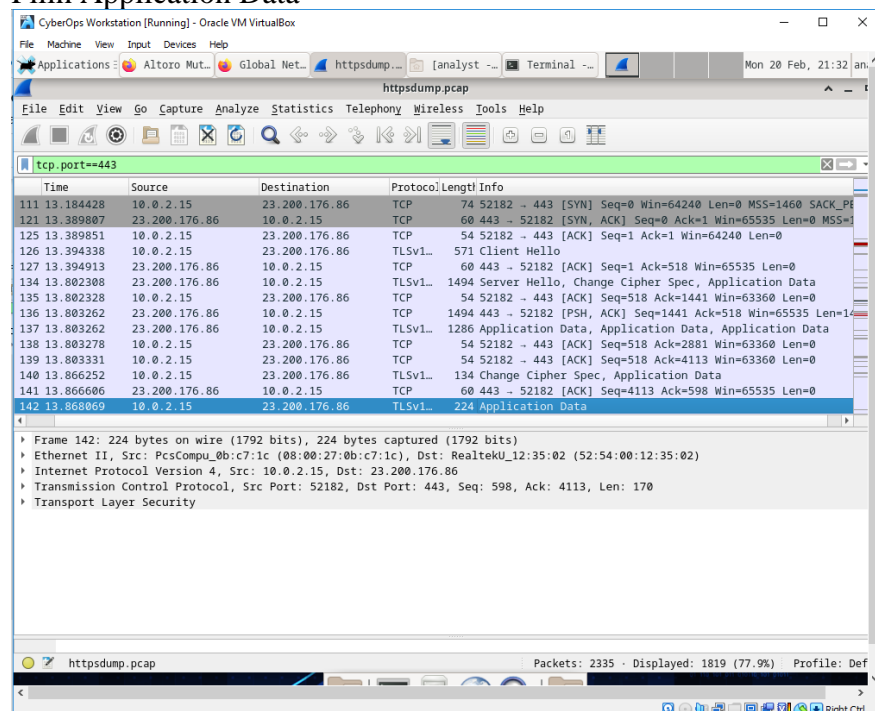
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama `httpsdump.pcap`. File ini terletak pada folder `/home/analyst/`.



## 13. Filter tcp.port==443



## 14. Pilih Application Data



## V. ANALISIS

Pada praktikum keamanan informasi 1 kali ini melakukan dua praktikum yaitu pertama eksplorasi Nmap serta melakukan scan ke port yang terbuka dan yang kedua adalah Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark.

Hal pertama yang dilakukan ialah membuka VM VirtualBox lalu klik bagian CyberOps Workstation dan klik start kemudian login dengan memasukkan username dan password (username: analyst dan password: cyberops).

Pada unit eksplorasi Nmap buka terminal lalu ketik “man nmap” klik enter maka akan muncul keterangan penjelasan Nmap dan sebagainya. Kemudian melakukan Localhost Scanning dengan mengetik “nmap -A -T4 localhost” klik enter lalu akan terlihat port dan layanan yang digunakan serta jenis software yang dipakai yaitu vsftpd, OpenSSH 8.2, Openwall GNU/\*/Linux telnetd. Lalu pada langkah ketiga Network Scanning, pada langkah ini Sebelum melakukan scanning alangkah lebih baiknya untuk mengetahui alamat IP host terlebih dahulu kemudian pada terminal ketik “ip address” klik enter maka akan muncul alamat IP serta subnet mask yang digunakan dari PC host, kemudian ketik “nmap -A -T4 10.0.2.0/24” klik enter lalu akan muncul jumlah host yang terdeteksi. Langkah selanjutnya yaitu Remote Server Scanning dengan membuka web browser terlebih dahulu dan kunjungi link [scanme.nmap.org](https://scanme.nmap.org) lalu kembali pada terminal dengan ketik perintah "nmap -A -T4 scanme.nmap.org" maka akan muncul jenis port dan layanan yang terbuka serta system operasi yang digunakan oleh server yakni Linux.

Pada unit Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark, Dalam persepsi yang positif, Wireshark berguna untuk pekerjaan analisis jaringan. Cara kerjanya yaitu dengan ‘menangkap’ paket-paket data dari protokol-protokol yang berbeda dari berbagai tipe jaringan yang umum ditemukan di dalam trafik jaringan internet.

Paket-paket data tersebut ‘ditangkap’ lalu ditampilkan di jendela hasil *capture* secara *real-time*. Pada awal proses analisis jaringan menggunakan Wireshark, semua paket data yang berhasil ditangkap tadi ditampilkan semua tanpa pilih-pilih (*promiscuous mode*). Semua paket data tersebut bisa diolah lagi menggunakan perintah *sorting* dan *filter*.

Hal pertama yang dilakukan sama yakni membuka VM VirtualBox sampai tahap login username dan password.

Buka terminal untuk menjalankan tcpdump melakukan pengecekan alamat IP dengan ketik perintah “ip address” dan “sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap”, masukkan password for analyst dengan password yang sama saat login (cyberops) maka akan muncul tipe alamat IP yang digunakan. Selanjutnya buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM dan masukkan “Username : Admin dan Password : Admin” kemudian lanjut pada tahap merekam paket HTTP, disini Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/. Dan pilih open with wireshark, setelah masuk ketik filter http dan klik apply maka akan muncul protocol dan pilih protocol HTTP dengan info POST.

Untuk merekam paket HTTPS, ketik perintah sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap Lalu masukkan password for analyst: cyberops maka akan muncul link tipe serta ukuran gambar nya. Kemudian lanjut buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM, dilanjut dengan melakukan login akun netacad yang dimiliki.

Setelah melihat Rekaman Paket HTTPS. Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpsdump.pcap. File ini terletak pada folder /home/analyst/ pilih open with wireshark dan pada filter ketik tcp.port==443 pilih pada Application Data. Perbedaan HTTP/HTTPS adalah pada keamanannya, di mana HTTP adalah protokol yang belum menggunakan SSL/TLS.

HTTPS adalah versi yang lebih aman karena sudah menggunakan SSL/TLS untuk mengenkripsi koneksi antara web browser dan web server.

## VI. KESIMPULAN

Setelah melaksanakan praktikum yang saya dapatkan adalah

- Wireshark mendukung banyak format file paket capture/trace termasuk **.cap** dan **.erf**.
- Agar dapat bekerja dengan baik, Wireshark membutuhkan aplikasi bernama **WinPcap** atau **Npcap** sebagai pondasinya.
- Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan.
- Pemindaian port (Port Scanner) merupakan aplikasi yang digunakan untuk mendeteksi dan melihat sejumlah informasi atau status dari protokol maupun port yang terbuka (open) dari sebuah perangkat.

## VII. DAFTAR PUSTAKA

Prak KI 1. (2023). Instalasi Virtual Machine. Retrieved February 27, 2023, from Elok UGM

Saputro, N. (2022). Pengertian Wireshark : Fungsi dan Cara kerjanya (Lengkap). [online] [www.nesabamedia.com](http://www.nesabamedia.com). Available at: <https://www.nesabamedia.com/pengertian-wireshark/>.

NMAP.ORG. "Panduan Refensi Nmap (Man Page, Bahasa Indonesia)." Nmap.org, [nmap.org/man/id/index.html#:~:text=Nmap%20\(%E2%80%9CNetwork%20Mapper%E2%80%9D\)](http://nmap.org/man/id/index.html#:~:text=Nmap%20(%E2%80%9CNetwork%20Mapper%E2%80%9D).). Accessed 27 Feb. 2023.