

LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN KE-2
EKSPLORASI NMAP SERTA PEMANTAUAN TRAFIK HTTP DAN
HTTPS DENGAN MENGGUNAKAN WIRESHARK



Di susun oleh :

Nama : Natasya Ovelia Zamris
NIM : 21/475446/SV/19121
Kelas : TRI kelas A
Dosen pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng

PROGRAM SARJANA TERAPAN DIPLOMA IV
TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

Unit 2 dan Unit 3

Eksplorasi Nmap

Pemantauan Trafik HTTP dan HTTPS dengan Menggunakan Wireshark

A. TUJUAN

1. Praktikan dapat mengeksplorasi Nmap.
2. Praktikan dapat melakukan scan ke port yang terbuka.
3. Praktikan dapat merekam dan menganalisis trafik HTTP.
4. Praktikan dapat merekam dan menganalisis trafik HTTPS.

B. LANDASAN TEORI

Network Mapper (Nmap) merupakan sebuah *software* yang digunakan untuk eksplorasi jaringan digital serta melakukan audit terhadap keamanan digital. Pada dasarnya ini memindai *host* dan layanan di jaringan komputer yang berarti mengirimkan paket dan menganalisis responsnya. Nmap menggunakan paket IP mentah dengan cara baru untuk menentukan *host* apa yang tersedia di jaringan, layanan apa yang ditawarkan *host* tersebut, sistem operasi apa yang dijalankan, jenis Firewall apa yang sedang digunakan, dan karakteristik lainnya. Ini dirancang untuk memindai jaringan besar dengan cepat, tetapi bekerja dengan baik terhadap *host* tunggal.

Port scanning biasanya merupakan bagian dari serangan pengintaian. Ada berbagai metode *Port scanning* yang dapat digunakan. Nmap merupakan *software* jaringan yang digunakan untuk audit keamanan dengan menggunakan metode *port scanning*.

Beberapa status hasil *Port scanning* dan artinya, diantaranya yaitu :

- Open, artinya layanan mendengarkan *port*.
- Closed, artinya layanan tidak mendengarkan di *port* tersebut.
- Filtered, artinya *port* difilter oleh sistem keamanan seperti Firewall dan apakah *port* terbuka atau tertutup tidak ditentukan. Jika *host* mengirimkan respons yang tidak biasa maka *port* juga difilter.
- Open | Filtered, artinya tidak ada jawaban yang diberikan oleh *host* sehingga *port* dapat difilter oleh Firewall.

Hyper Text Transfer Protocol (HTTP) merupakan protokol lapisan aplikasi yang menyajikan data melalui browser web. Dengan HTTP, tidak ada perlindungan untuk pertukaran data antara dua perangkat yang berkomunikasi.

Hyper Text Transfer Protocol Secure (HTTPS) merupakan kombinasi dari HTTP dengan protokol *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS). SSL bekerja dengan menggunakan kunci publik untuk mengenkripsi data yang ditransfer melalui koneksi SSL. TLS merupakan protokol otentikasi dan

keamanan yang diterapkan secara luas di browser dan server web. Sebagian besar browser web mendukung SSL.

Dengan HTTPS, enkripsi digunakan melalui algoritma matematika. Algoritma ini menyembunyikan arti sebenarnya dari data yang sedang dipertukarkan. Hal ini dilakukan melalui penggunaan sertifikat.

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

Wireshark merupakan penganalisis protokol jaringan atau aplikasi yang menangkap paket dari koneksi jaringan, seperti dari komputer ke kantor pusat atau internet. Paket adalah nama yang diberikan untuk unit data diskrit dalam jaringan Ethernet biasa.

Wireshark melakukan tiga hal, diantaranya yaitu :

- Pengambilan paket, wireshark mendengarkan koneksi jaringan secara real time dan kemudian mengambil seluruh aliran lalu lintas.
- Penyaringan, wireshark mampu mengirim dan memotong semua data langsung acak menggunakan filter. Dengan menerapkan filter, dapat memperoleh informasi yang perlu dilihat saja.
- Visualisasi, wireshark memungkinkan menyelam ke tengah-tengah paket jaringan. Ini memungkinkan untuk memvisualisasikan seluruh percakapan dan aliran jaringan.

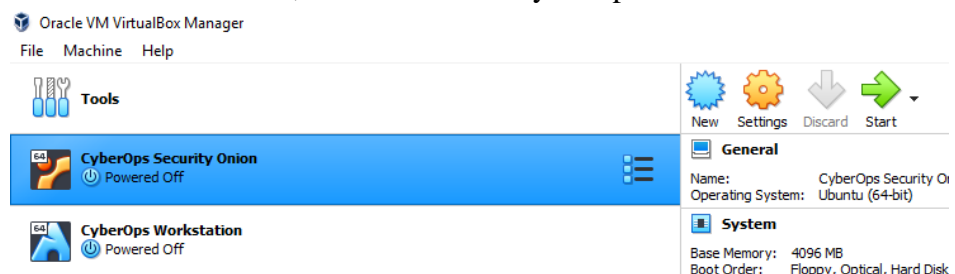
C. ALAT DAN BAHAN

Alat dan bahan yang di butuhkan yaitu :

1. PC Host dengan minimal RAM 8GB dan Hardisk 40GB,
2. Internet access,
3. CyberOps Workstation Virtual Machine.

D. INSTRUKSI KERJA

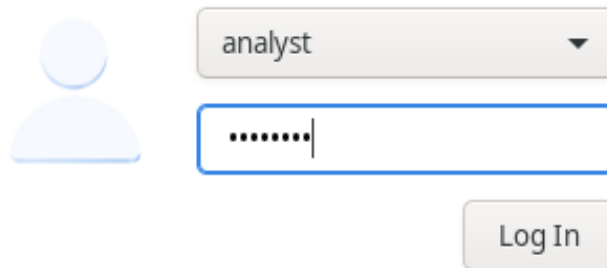
1. Membuka VirtualBox, kemudian Start CyberOps Workstation.



2. Memasukkan username dan password dengan ketentuan :

Username : analyst

Password : cyberops

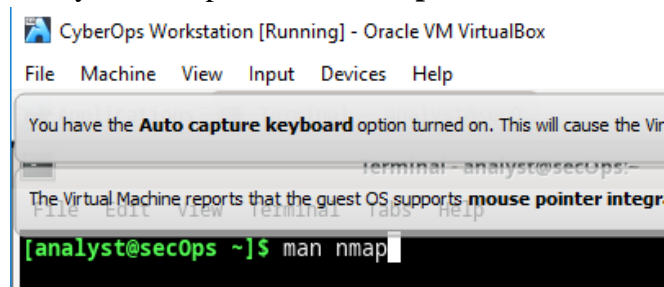


A login interface featuring a light blue user icon on the left. To its right is a dropdown menu with 'analyst' selected. Below the dropdown is a password input field with a blue border and masked characters (dots). A 'Log In' button is positioned to the right of the password field.

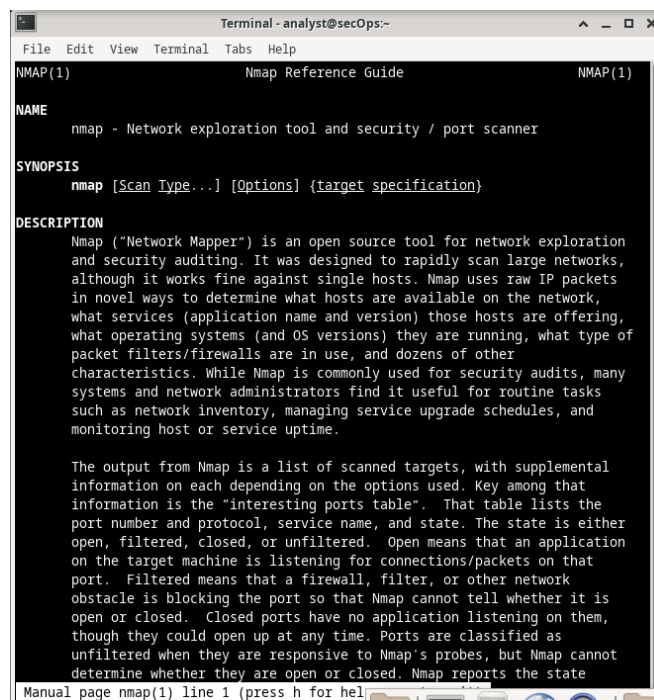
- Unit 2

1. Mengeksplorasi Nmap, kemudian ketikkan.

[analyst@secOps~]\$ **man nmap**



Hasil setelah di run :



Apa itu Nmap?

Nmap (*Network Mapper*) merupakan sebuah *tool open source* yang digunakan untuk eksplorasi jaringan digital serta melakukan audit terhadap keamanan digital. Nmap menggunakan alamat IP baru untuk menentukan *host* apa yang tersedia dalam jaringan tersebut.

Apa fungsi dari Nmap?

- Sebagai pemeriksaan jaringan besar dalam waktu singkat.
- Sebagai *scanning* pada *port* jaringan komputer yang dapat membedakan antara aplikasi yang satu dengan lainnya.
- Sebagai *discover vulnerabilities* dan *version detection* dalam menemukan kerentanan.

2. Localhost Scanning

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

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:53 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s 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)
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 30.36 seconds
```

Port dan layanan apa yang terbuka?

Port 21 : layanan ftp

Port 22 : layanan ssh

Port 23 : layanan telnet

Software apa yang digunakan pada port yang terbuka tersebut?

Port 21 : software vsftpd

Port 22 : software openSSH

Port 23 : software openwall

3. Network Scanning

Sebelum melakukan *scanning* alangkah lebih baik 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 08:00:27:26:1f:a4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85464sec preferred_lft 85464sec
    inet6 fe80::a00:27ff:fe26:1fa4/64 scope link
        valid_lft forever preferred_lft forever
```

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

Alamat IP : 10.0.2.15/24

Subnet mask : 255.255.255.0

Melakukan *port scanning* dengan menggunakan Nmap

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:59 EST
Nmap scan report for 10.0.2.15
Host is up (0.00028s 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

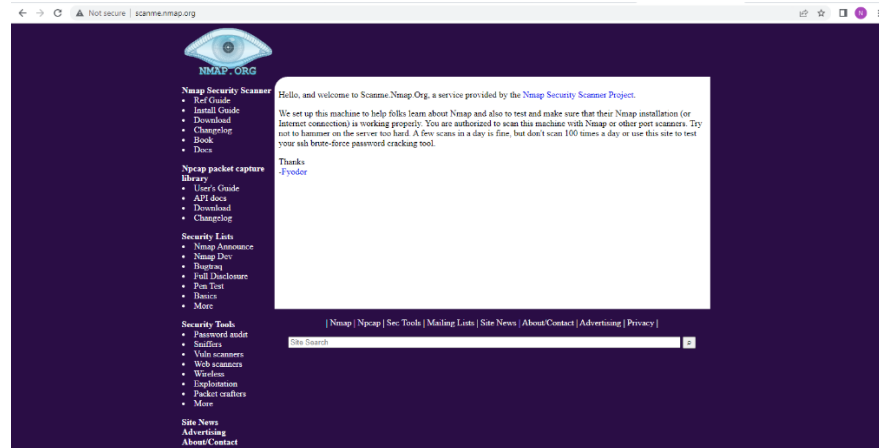
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 46.13 seconds
```

Berapakah jumlah *host* yang terdeteksi?

Terdapat 1 *host* yang aktif.

4. Remote Server Scanning

Membuka web browser dan kunjungi scanme.nmap.org



[analyst@secOps ~]\$ **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 20:21 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 985 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    closed ftp
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)
23/tcp    closed telnet
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!
110/tcp   closed pop3
135/tcp   closed msrpc
443/tcp   closed https
554/tcp   closed rtsp
587/tcp   closed submission
1723/tcp  closed pptp
5900/tcp  closed vnc
8080/tcp  closed http-proxy
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 a false positive to https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned
```

Port dan layanan apa yang terbuka?

Port 22 : layanan ssh

Port 53 : layanan domain

Port 80 : layanan http

Port 9929 : layanan nping-echo

Port 31337 : layanan tcpwrapped

Berapa alamat IP server?

45.33.32.156

Apa sistem operasi yang digunakan oleh server?

Linux

- **Unit 3**

1. Menjalankan **tcpdump**

Pengecekan alamat IP dengan menggunakan perintah :

[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 08:00:27:26:1f:a4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86042sec preferred_lft 86042sec
    inet6 fe80::a00:27ff:fe26:1fa4/64 scope link
        valid_lft forever preferred_lft forever
```

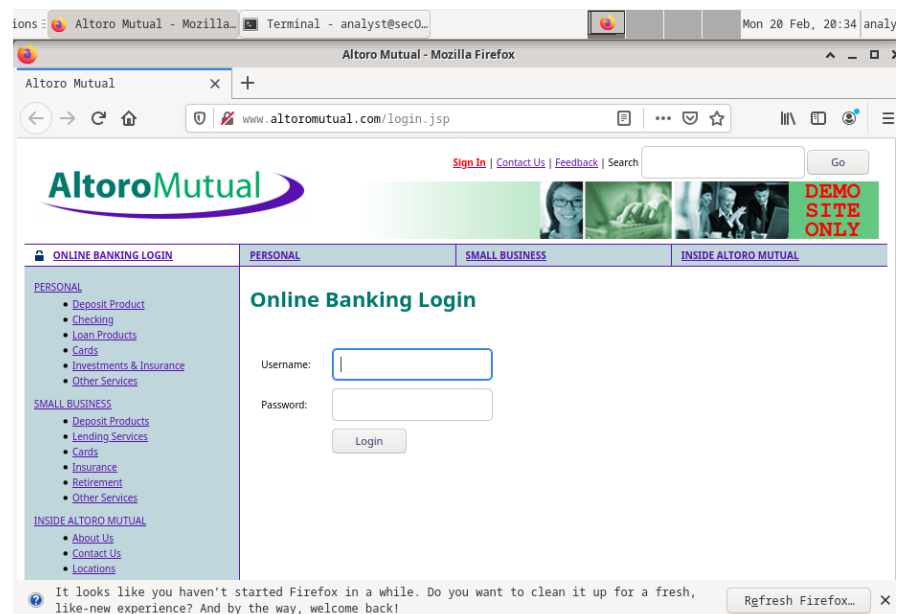
[analyst@secOps ~]\$ **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**

```
[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
```

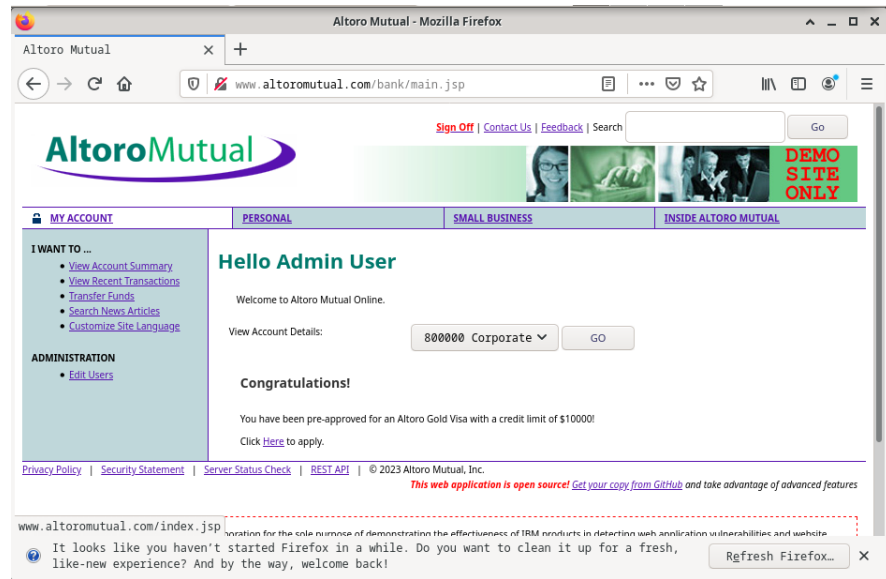
2. Membuka *link* <http://www.altoromutual.com/login.jsp> melalui *browser* di *CyberOps Workstation Virtual Machine*.

Username : Admin

Password : Admin

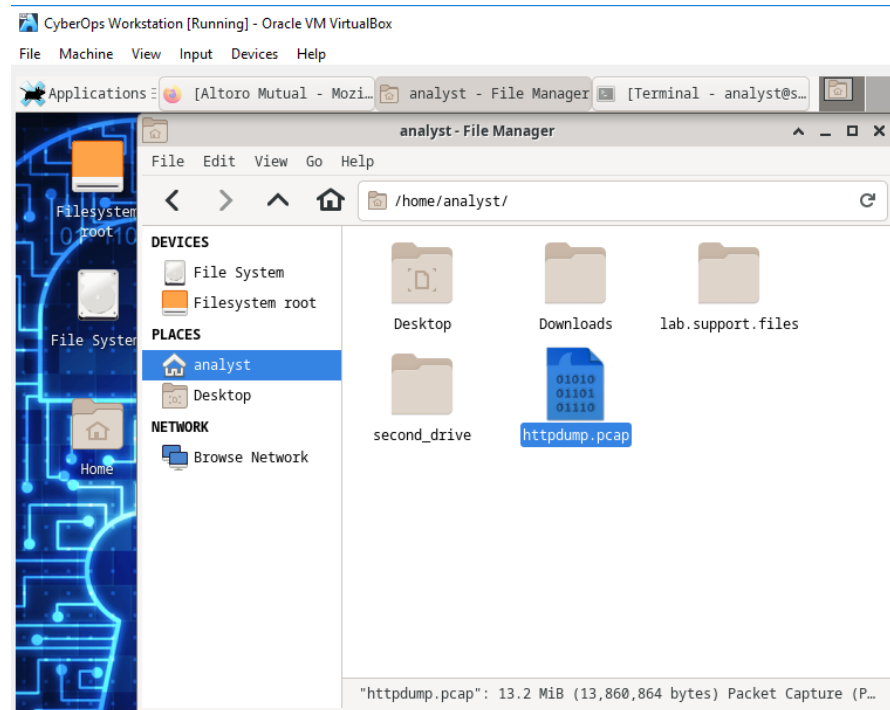


Hasil setelah memasukkan *username* dan *password* :

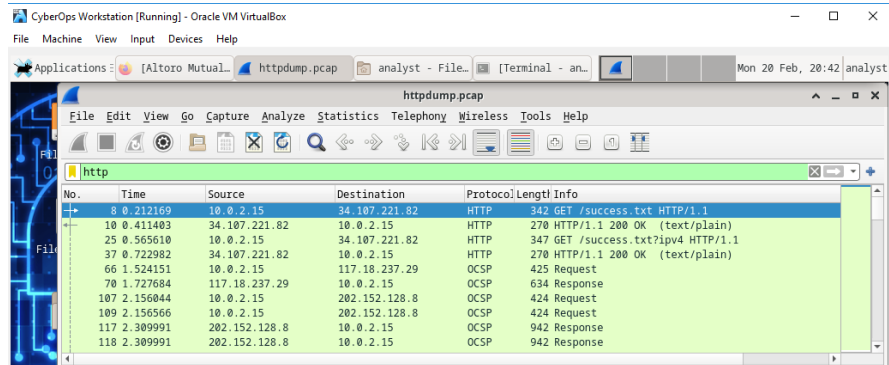


3. Merekam paket HTTP.

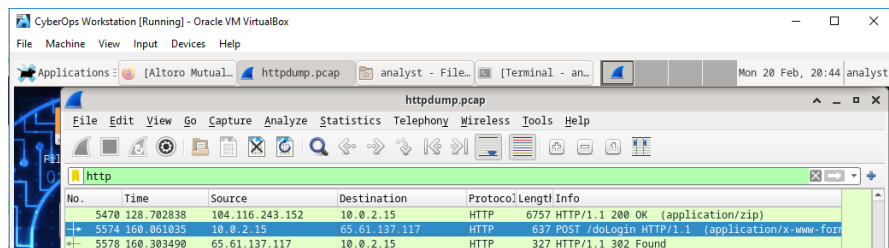
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam *file* bernama *httpdump.pcap*. *File* ini terletak pada folder */home/analyst/*.



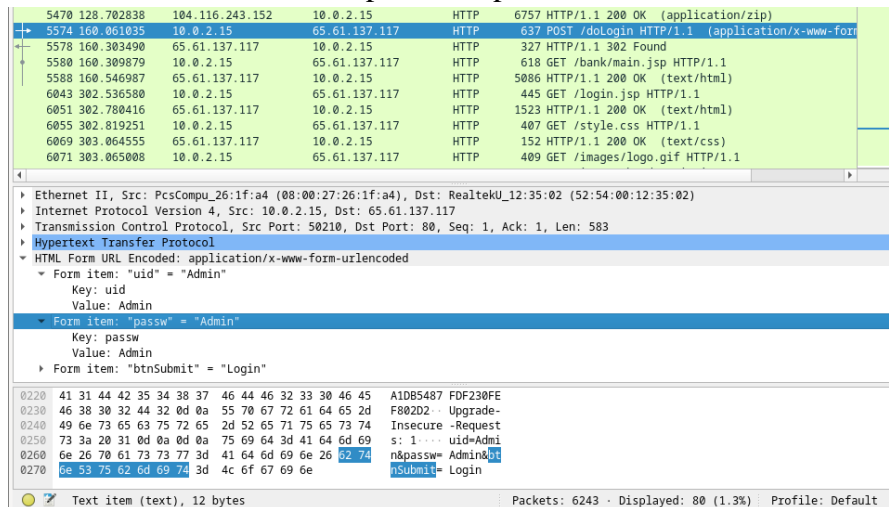
4. Filter http kemudian klik *Apply*.



5. Pilih POST.



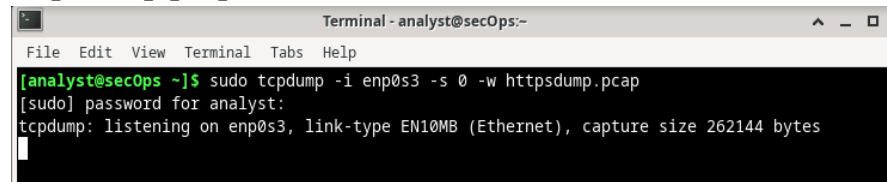
6. Lakukanlah analisis terhadap uid dan passw.



Uid dan passw yang terdapat diatas merupakan *username* dan *password* saat login pada link <http://www.altoromutual.com/login.jsp>.

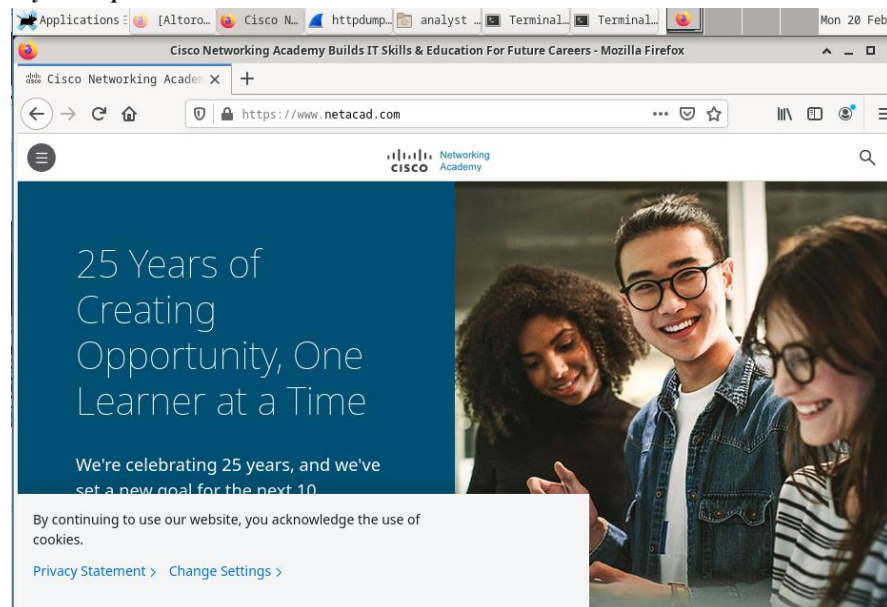
7. Merekam paket HTTPS

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



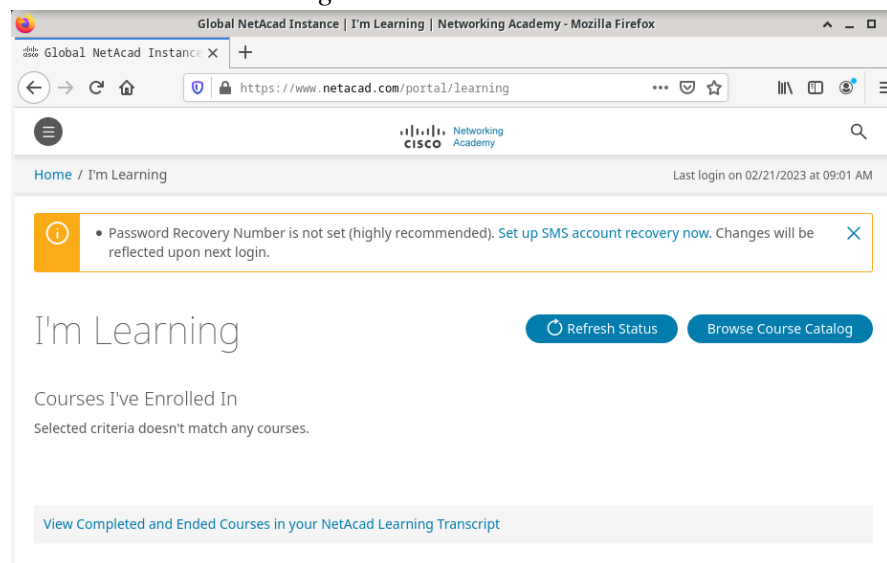
```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap  
[sudo] password for analyst:  
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

8. Membuka *link* <https://www.netacad.com/> melalui *browser* di *CyberOps Workstation Virtual Machine*.



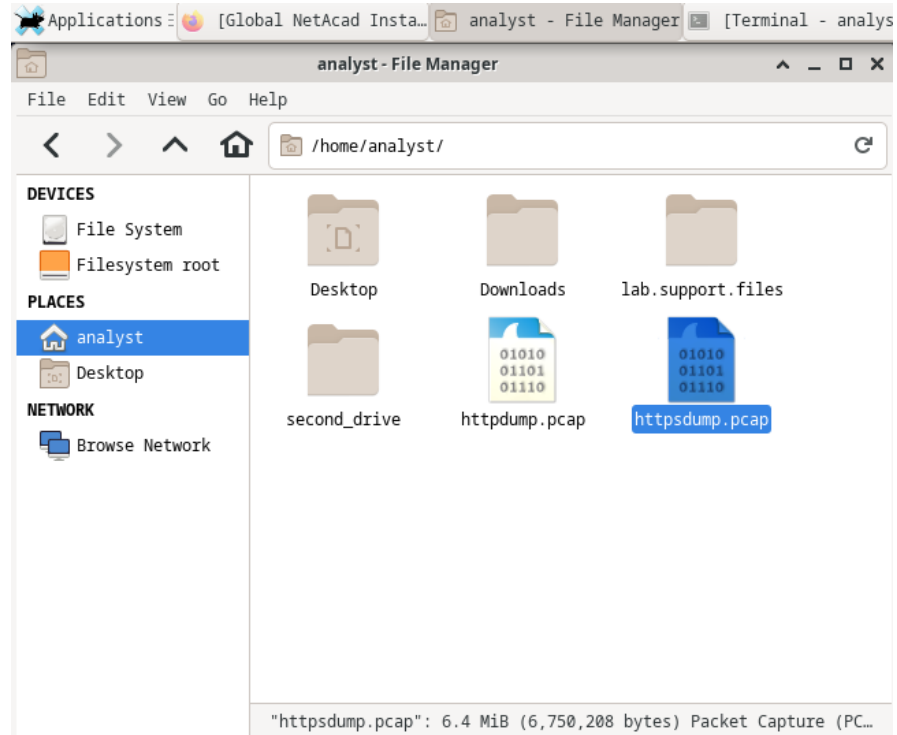
9. Klik *login*, kemudian masukkan *username* dan *password*.

Hasil setelah berhasil *login* :

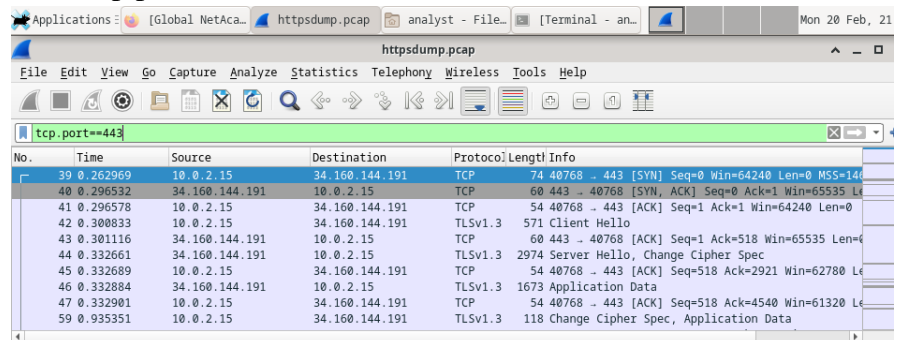


10. Melihat rekaman paket HTTPS.

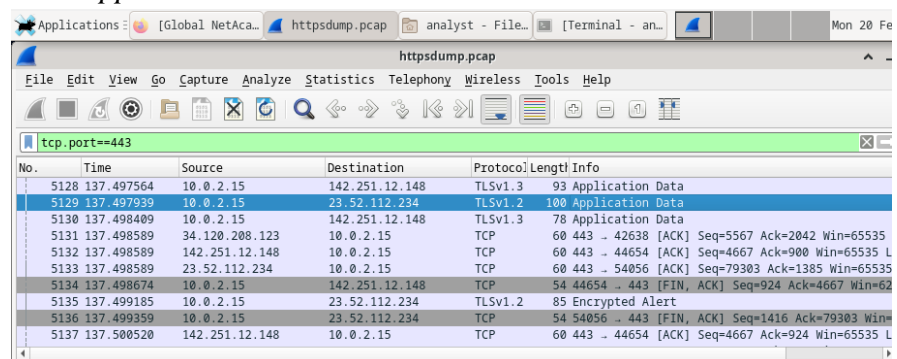
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama `httpsdump.pcap`. File ini terletak pada folder `/home/analyst/`.



11. Filter tcp.port==443.



12. Pilih Application Data.



13. Menganalisis hasil yang di dapatkan.

```
▼ Frame 5129: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 20, 2023 20:58:53.706538000 EST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1676944733.706538000 seconds
  [Time delta from previous captured frame: 0.000375000 seconds]
  [Time delta from previous displayed frame: 0.000375000 seconds]
  [Time since reference or first frame: 137.497939000 seconds]
  Frame Number: 5129
  Frame Length: 100 bytes (800 bits)
  Capture Length: 100 bytes (800 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:tls]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]

▼ Ethernet II, Src: PcsCompu_26:1f:a4 (08:00:27:26:1f:a4), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
    Address: RealtekU_12:35:02 (52:54:00:12:35:02)
    ....01. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: PcsCompu_26:1f:a4 (08:00:27:26:1f:a4)
    Address: PcsCompu_26:1f:a4 (08:00:27:26:1f:a4)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.52.112.234
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 86
  Identification: 0x5c53 (23635)
  ▼ Flags: 0x4000, Don't fragment
    0... .... = Reserved bit: Not set
    .1... .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
  Header checksum: 0x4a22 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.0.2.15
  Destination: 23.52.112.234

▼ Transmission Control Protocol, Src Port: 54056, Dst Port: 443, Seq: 1339, Ack: 79303, Len: 46
  Source Port: 54056
  Destination Port: 443
  [Stream index: 63]
  [TCP Segment Len: 46]
  Sequence number: 1339 (relative sequence number)
  Sequence number (raw): 1305288841
  [Next sequence number: 1385 (relative sequence number)]
  Acknowledgment number: 79303 (relative ack number)
  Acknowledgment number (raw): 11919304
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x018 (PSH, ACK)
  Window size value: 65535
  [Calculated window size: 65535]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x9475 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
  TCP payload (46 bytes)

▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http2
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 41
    Encrypted Application Data: 00000000000000701302ab1b5dd65fc7020958e7d1a1036...
```

E. PEMBAHASAN

Nmap (*Network Mapper*) merupakan sebuah *software* yang digunakan untuk eksplorasi jaringan digital. Nmap menggunakan alamat IP baru untuk menentukan *host* apa yang tersedia dalam jaringan tersebut. Nmap digunakan untuk audit keamanan dengan menggunakan metode *port scanning* yang dapat membedakan aplikasi yang satu dengan yang lainnya.

Pada praktikum unit 2 saya menggunakan **argument -A** yang digunakan untuk mengetahui *port*, layanan, dan sistem operasi yang digunakan. Kemudian **argument -T4** digunakan untuk memeriksa eksekusi yang lebih cepat.

Terdapat beberapa status *port* yang dikenali oleh Nmap. Pada praktikum ini terdapat 3 status *port* yang sering bermunculan, yaitu *open*, *closed*, dan *filtered*. **Status open** menunjukkan bahwa ada aplikasi yang menerima paket data dari pengirim. **Status closed** menunjukkan bahwa *port* dapat mengirim paket data tetapi tidak ada aplikasi yang merespons pada *port* tersebut. **Status filtered** menunjukkan bahwa paket data tidak dapat ditentukan statusnya apakah *open* atau *close*, ini juga menunjukkan bahwa *port* tersebut dilindungi atau ditolak oleh *firewall*.

Sebelum melakukan *scanning*, lebih baik untuk mengetahui alamat IP *host* terlebih dahulu. Alamat IP *host* yang didapat yaitu 10.0.2.15/24. Setelah itu, melakukan *scanning* dengan memasukkan IP *network* yaitu 10.0.2.0/24. Pada *localhost scanning* terdapat 997 *closed ports* dan 3 *open ports*. Pada *network scanning* terdapat 997 *closed ports* dan 3 *open ports*.

Pada praktikum unit 3 terdapat *command* TCPdump. TCPdump merupakan sebuah *tool packet sniffing* dan *packet analyzing* untuk sistem administrator yang bertujuan untuk memecahkan masalah konektivitas di linux. TCPdump digunakan untuk menangkap (*capture*), memfilter (*filter*), dan menganalisis lalu lintas jaringan (*analyze network traffic*). TCPdump sering digunakan sebagai alat keamanan karena TCPdump menyimpan informasi yang ditangkap dalam *file pcap*, *file pcap* ini kemudian dibuka melalui wireshark. Perbedaan utama TCPdump dengan wireshark yaitu TCPdump tidak melakukan analisa terhadap data, tetapi hanya melakukan *copy packet* secara keseluruhan.

TCPdump dijalankan dengan mencocokkan *packet* dengan opsi yang diberikan oleh *user*. Terdapat beberapa opsi yang digunakan pada praktikum ini, diantaranya yaitu **Opsi -i** artinya memberi tahu TCPdump agar menempatkan *interface* jaringan dalam *promiscuous* mode dan memerintahkan *interface* jaringan untuk mendengar semua trafik yang datang. **Opsi -s** artinya meng-*print absolute sequence numbers*. **Opsi -w** artinya menyimpan *packet* yang diambil ke dalam *file*.

Pada praktikum ini terdapat perintah **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**. Artinya perintah ini akan menangkap semua trafik pada enp0s3 dengan nomor urut TCP 0 dan menulisnya dalam *file* httpdump.pcap.

Praktikum ini melakukan pemantauan trafik HTTP dan HTTPS dengan menggunakan Wireshark. Setelah menjalankan TCPdump, buka *link* HTTP. Kemudian TCPdump yang dieksekusi pada langkah sebelumnya, disimpan kedalam file yang diberi nama *httpdump.pcap*. Setelah itu lakukan pemfilteran HTTP. Sama halnya dengan HTTP, HTTPS tidak jauh berbeda dengan HTTP. untuk HTTPS, yang difilter adalah *tcp.port==443*. Lalu pilih *Application Data*.

F. KESIMPULAN

Adapun kesimpulan dari praktikum ini yaitu :

1. *Argument -A* digunakan untuk mengetahui *port*, layanan, dan sistem operasi yang digunakan.
2. *Argument -T4* digunakan untuk memeriksa eksekusi yang lebih cepat.
3. Status *open* menunjukkan bahwa ada aplikasi yang menerima paket data dari pengirim.
4. Status *closed* menunjukkan bahwa *port* dapat mengirim paket data tetapi tidak ada aplikasi yang merespons pada *port* tersebut.
5. Status *filtered* menunjukkan bahwa paket data tidak dapat ditentukan statusnya apakah *open* atau *close*, ini juga menunjukkan bahwa *port* tersebut dilindungi atau ditolak oleh *firewall*.
6. TCPdump merupakan sebuah *tool packet sniffing* dan *packet analyzing* untuk sistem administrator yang bertujuan untuk memecahkan masalah konektivitas di linux.
7. TCPdump digunakan untuk menangkap (*capture*), memfilter (*filter*), dan menganalisis lalu lintas jaringan (*analyze network traffic*).
8. Opsi *-i* TCPdump artinya memberi tahu TCPdump agar menempatkan *interface* jaringan dalam *promiscuous* mode dan memerintahkan *interface* jaringan untuk mendengar semua trafik yang datang.
9. Opsi *-s* TCPdump artinya meng-*print absolute sequence numbers*.
10. Opsi *-w* TCPdump artinya menyimpan *packet* yang diambil ke dalam *file*.

DAFTAR PUSTAKA

Amit4856. 2022, September 8. *Nmap Memindai Keamanan Cyber dan Pengujian Penetrasi*. Di akses dari, <<https://www.geeksforgeeks.org/nmap-scans-for-cyber-security-and-penetration-testing/>>

HealthIT. 2019, September 10. *What Does HTTPS Web Address Mean*. Di akses dari <[https://www.healthit.gov/faq/what-does-https-web-address-mean#:~:text=Hypertext%20Transfer%20Protocol%20Secure%20\(https,in%20browsers%20and%20Web%20servers.>](https://www.healthit.gov/faq/what-does-https-web-address-mean#:~:text=Hypertext%20Transfer%20Protocol%20Secure%20(https,in%20browsers%20and%20Web%20servers.>)

CompTIA. *Apa Itu Wireshark dan Bagaimana Cara Menggunakannya?*. Di akses dari <<https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it#:~:text=Wireshark%20is%20a%20network%20protocol,packet%20sniffer%20in%20the%20world.>>

Rayhanx-id. 2022, November 7. *Menggunakan Nmap*. Di akses dari <[>](https://www.rayhanx.com/2022/11/cara-melakukan-port-scanning.html)