

**LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 2
EKSPLORASI NMAP**



DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

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

EKSPLORASI NMAP

A. TUJUAN

- Mengeksplorasi Nmap
- Melakukan Scan ke Port yang terbuka

B. DASAR TEORI

- **Nmap**

Network Mapper (Nmap) merupakan sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. Nmap dirancang untuk memeriksa jaringan besar secara cepat, meskipun dapat juga bekerja terhadap *host* tunggal. Nmap menggunakan paket IP *raw* dalam cara yang canggih untuk menentukan *host* mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal *upgrade* layanan, dan melakukan *monitoring uptime host* atau layanan.

Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Hal kunci di antara informasi itu adalah “tabel *port* menarik”. Tabel tersebut berisi daftar angka *port* dan protokol, nama layanan, dan status. Selain tabel *port* yang menarik, Nmap dapat pula memberikan informasi lebih lanjut tentang target, termasuk nama *reverse DNS*, prakiraan sistem operasi, jenis *device*, dan alamat MAC.

- **Port Scanning**

Port Scanning adalah tahapan awal untuk mendeteksi *port-port* yang terbuka dan mendapatkan informasi dari *port* yang terbuka pada target, servis apa yang sedang dijalankan, versi dari *server* dan lain sebagainya. Ada berbagai metode *Port scanning* yang dapat digunakan. Nmap adalah *software* jaringan yang digunakan untuk audit keamanan dengan menggunakan metode *port scanning*

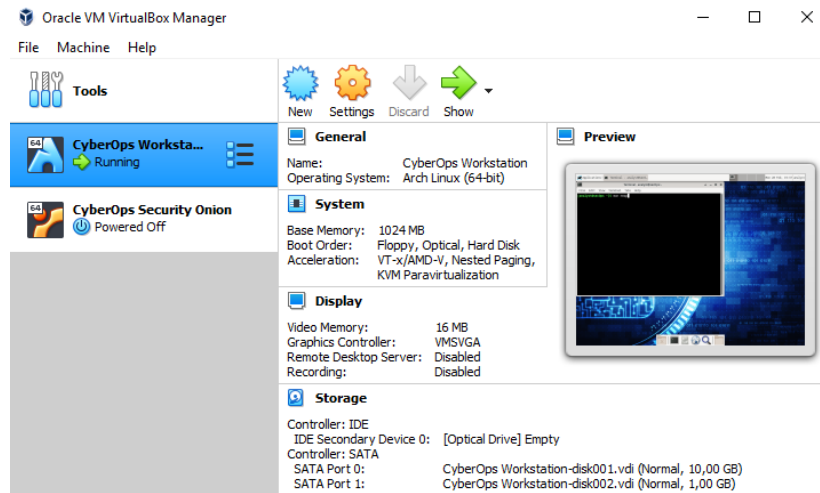
C. ALAT DAN BAHAN

- *CyberOps Workstation Virtual Machine*
- Akses internet

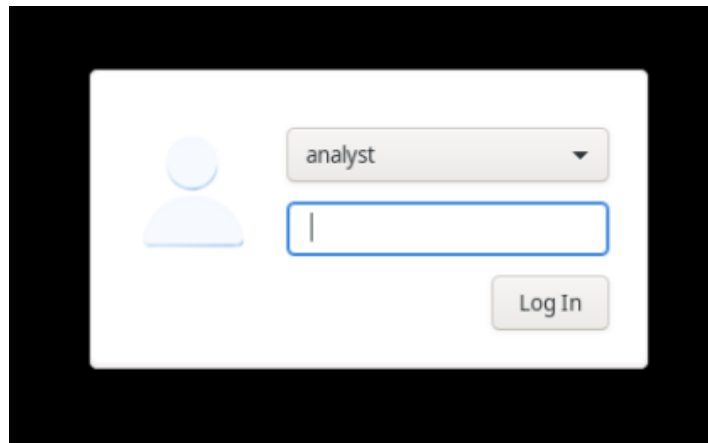
D. HASIL DAN ANALISIS

1. Eksplorasi Nmap Start, CyberOps Workstation

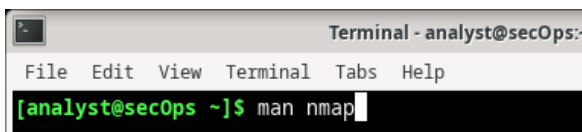
Buka terminal kemudian ketikkan **[analyst@secOps ~]\$ man nmap**



Klik Start



Masukkan *password* cyberops



Buka terminal, kemudian ketikkan **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
    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

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

Output dari perintah pada terminal tadi berupa pengertian dari Nmap serta fungsinya

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 19:48 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 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
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 30.45 seconds
```

Ketikkan **nmap -A -T4 localhost**, *output*-nya berisikan *port* dan layanan yang terbuka serta *software* yang digunakan pada *port* yang tadi terbuka

3. Network Scanning

Sebelum melakukan scanning ketahui 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 08:00:27:9a:7e:24 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85213sec preferred_lft 85213sec
    inet6 fe80::a00:27ff:fe9a:7e24/64 scope link
        valid_lft forever preferred_lft forever
```

Output-nya berupa *IP Address* dan *Subnet Mask* dari *PC Host*

Lakukanlah port scanning dengan menggunakan Nmap

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

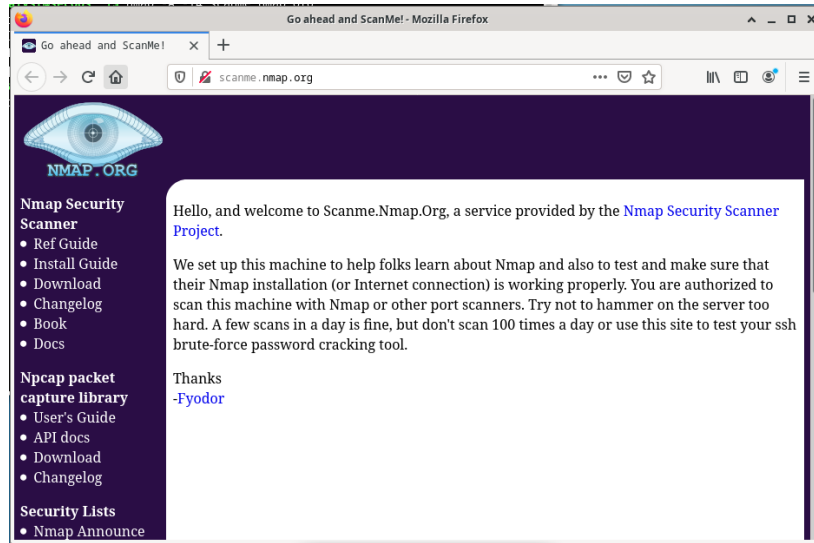
```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:56 EST
Nmap scan report for 10.0.2.15
Host is up (0.00026s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous 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 46.84 seconds
```

Output dari perintah tersebut berisikan,

4. Remote Server Scanning

Buka web browser dan kunjungi scanme.nmap.org



Tampilan website scanme.nmap.org

Ketikkan perintah berikut:

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

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

[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:24 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.37s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 986 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!
110/tcp   closed pop3
111/tcp   closed rpcbind
143/tcp   closed imap
554/tcp   closed rtsp
1025/tcp  closed NFS-or-IIS
1723/tcp  closed pptp
3389/tcp  closed ms-wbt-server
5900/tcp  closed vnc
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
```

Hasil *scanning*

PEMBAHASAN:

Pada praktikum kali ini ada beberapa hal yang dieksplorasi di dalam Nmap. Antara lain;

1. Pengertian Nmap dan fungsi Nmap
2. *Port* dan layanan yang terbuka
3. *IP Address* dan subnet *PC host*
4. Jumlah *host* yang terdeteksi
5. *IP Server*
6. Sistem operasi yang digunakan *server*

Praktikum ini diawali dengan, mencari tahu pengertian dan fungsi Nmap. Secara garis besar, Nmap adalah pemindai jaringan yang digunakan untuk menemukan *host* dan layanan di jaringan komputer dengan mengirimkan paket dan menganalisis responnya.

Informasi yang didapat dari *localhost scanning* sebagai berikut:

- localhost: 127.0.0.1
- 597 port tertutup
- 21/tcp terbuka dengan versi 2.0.8 atau lebih baru
- 22/tcp ssh terbuka (OpenSSH 8.0 dengan protokol 2.0)
- 23/tcp terbuka telnet SNU/Linux telnet
- Informasi layanan:
- Host: Welcome
- OS: Linux
- CPE: cpe:/o:linux:linux_kernel

Sebelum memulai *network scanning*, ketahuilah *IP Host* terlebih dahulu. Dapat dilihat *IP host*-nya adalah 10.0.2.15/24. *Port scanning* di sini berfungsi untuk mengetahui jumlah *host*. Setelah melakukan *port scanning* dapat diketahui bahwa *host* yang terdeteksi ada 3 yaitu, 10.0.2.4, 10.0.2.3, dan 10.0.2.2.

Bagian terakhir, lakukan *remote server scanning* dengan mengakses scanme.nmap.org setelah tampilan *website* sudah terlihat, lanjutkan dengan mengetik perintah pada *terminal*. *Output* dari perintah yang telah diketikkan berupa, *port* yang terbuka yaitu:

- 22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
- 80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
- 9929/tcp open nping-echo Nping echo
- 31337/tcp open tcpwrapped

Selain itu ada juga alamat *IP Server* (45.33.32.156) dan OS yang digunakan *server*, sebagai berikut, *Service Info*:

- OS: Linux
- CPE: cpe:/o:linux:linux_kernel

E. KESIMPULAN

- Nmap adalah pemindai jaringan yang digunakan untuk menemukan *host* dan layanan di jaringan komputer
- *Localhost scanning* dilakukan untuk mengetahui port apa saja yang terbuka
- Untuk melakukan *Network scanning*, sebaiknya cek IP dan subnet mask dari PC host. Dilanjutkan dengan *Port scanning* untuk mendeteksi jumlah host
- *Remote server scanning* dilakukan untuk mengetahui port dan layanan apa yang terbuka, IP server, dan sistem operasi dari server

F. DAFTAR PUSTAKA

NMAP.ORG. (n.d.). *Panduan Refensi Nmap (Man Page, bahasa Indonesia)*. Nmap.

Retrieved Februari 21, 2023, from <https://nmap.org/man/id/index.html>

Y Kusuma. (2020). PENDAHULUAN. In (p. 1). Sekolah Vokasi Institut Pertanian Bogor.

<https://ereport.ipb.ac.id/id/eprint/4228/4/j3d117089-04-yanuar-pendahuluan.pdf>

**LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 3
PEMANTAUAN TRAFIK HTTP DAN HTTPS DENGAN
MENGUNAKAN WIRESHARK**



DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

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

PEMANTAUAN TRAFIK HTTP DAN HTTPS DENGAN MENGGUNAKAN WIRESHARK

A. TUJUAN

- Merekam dan menganalisis trafik http
- Merekam dan menganalisis trafik https

B. DASAR TEORI

• HTTP

Hypertext Transfer Protocol (HTTP) adalah aturan dasar yang mengatur komunikasi antara *client* dan *server*. Pada HTTP, port yang digunakan adalah berukuran port 80. HTTP adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia. Klien yang mengirimkan permintaan HTTP juga dikenal dengan user agent. Server yang meresponnya, yang menyimpan sumber daya seperti berkas HTML dan gambar, dikenal juga sebagai origin server. Di antara user agent dan juga origin server, bisa saja ada penghubung, seperti halnya proxy, gateway, dan juga tunnel.

• HTTPS

Hypertext Transfer Protocol Secure (HTTPS) merupakan versi lebih aman dari HTTP, tugasnya sama persis namun dalam pertukaran data https menggunakan autentikasi dan komunikasi tersandi. HTTPS menggunakan port ukuran 443. Dengan menggunakan HTTPS maka informasi yang didapat menjadi lebih aman karena hanya melakukan proses 'Enkripsi' terhadap pengiriman informasi.

Adapun beberapa informasi yang dikirim hanya bisa diakses oleh client dengan server aktif terakhir. Protokol ini membungkus lapisan terenkripsi di sekitar HTTP dan Transport Layer Security (TLS) sehingga client dan server akan berkomunikasi dengan aman menggunakan HTTP. Dengan kata lain, protokol ini akan dienkripsi untuk meningkatkan keamanan transfer data sensitif, misalnya ketika mengakses web rekening bank, layanan email, atau penyedia asuransi kesehatan.

• WIRESHARK

Wireshark adalah *tool* yang ditujukan untuk penganalisisan paket data jaringan. *Wireshark* melakukan pengawasan paket secara waktu nyata (*real time*) dan kemudian menangkap data dan menampilkannya selengkap mungkin. *Wireshark* bisa digunakan secara gratis karena aplikasi ini berbasis sumber terbuka. Aplikasi *Wireshark* dapat berjalan di banyak *platform*, seperti *Linux*, *Windows*, dan *Mac*. Struktur dari *wireshark graphical user interface* adalah sebagai berikut :

- Command menu*: daftar yang dibutuhkan pada wireshark
- Display filter specification*: untuk memfilter paket data
- Listing of captured packets*: paket data yang tertangkap oleh wireshark
- Details of selected packet header*: data lengkap tentang header dari suatu paket.
- Packet contents*: isi dari suatu paket data

C. ALAT DAN BAHAN

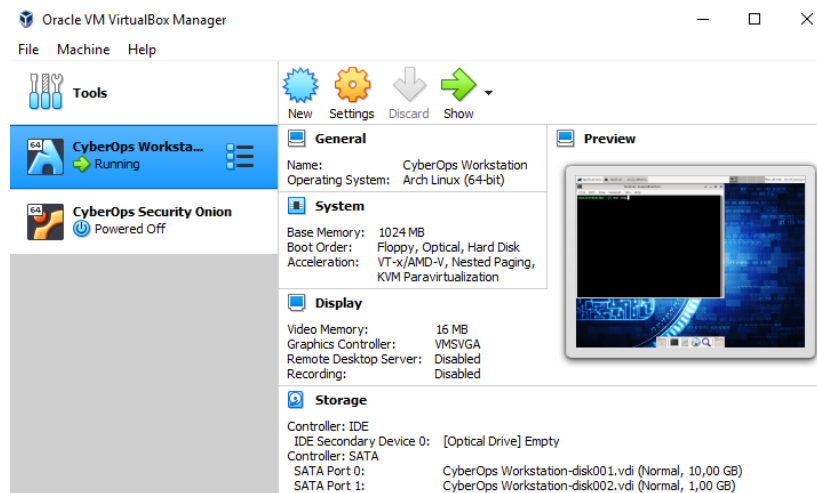
- *CyberOps Workstation Virtual Machine*
- Koneksi internet

D. HASIL DAN ANALISIS

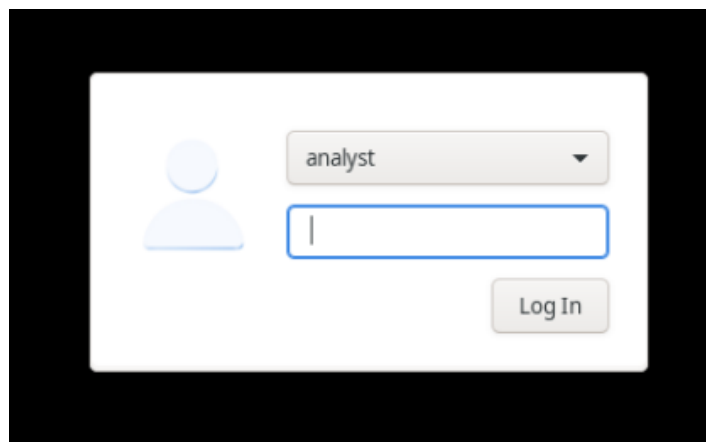
1. Jalankan VM dan Login

Username: analyst

Password: cyberops



Klik Start



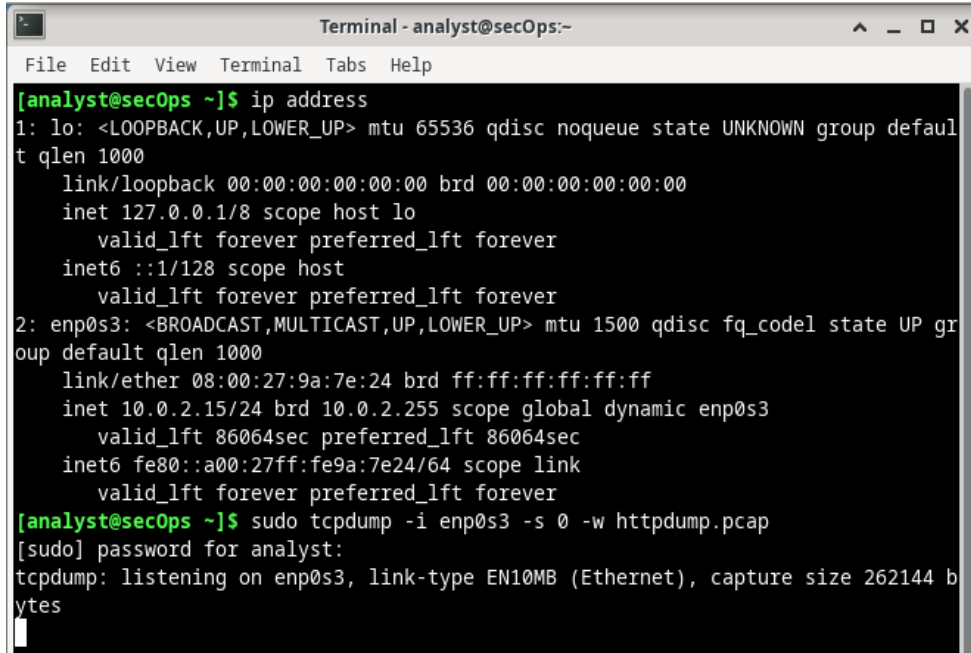
Masukkan *password* **cyberops**

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
```



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

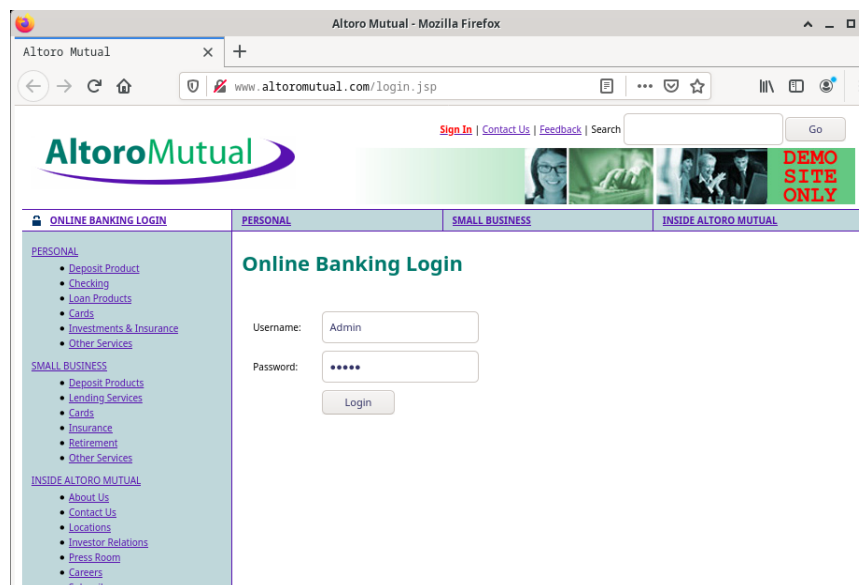
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9a:7e:24 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86064sec preferred_lft 86064sec
    inet6 fe80::a00:27ff:fe9a:7e24/64 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
```

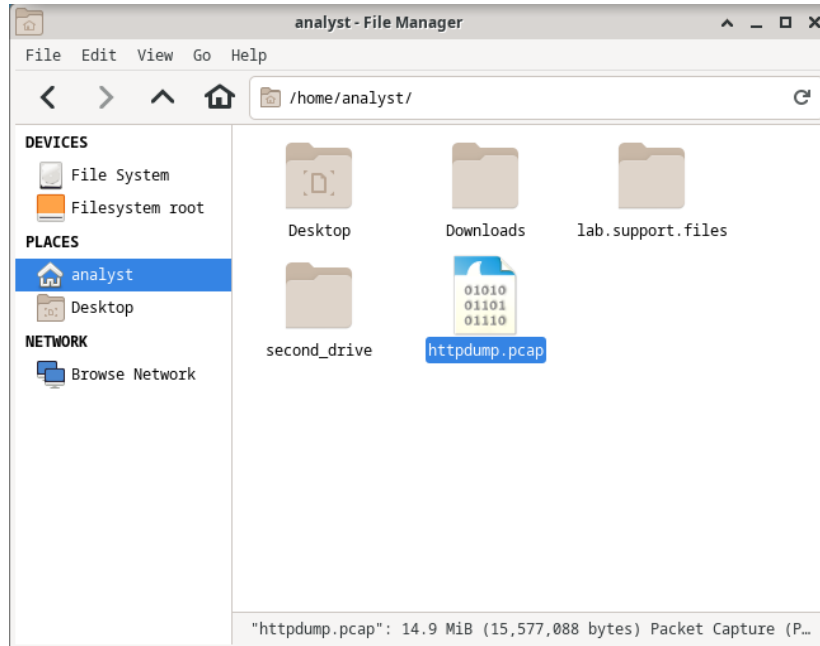
3. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM.

Username : Admin

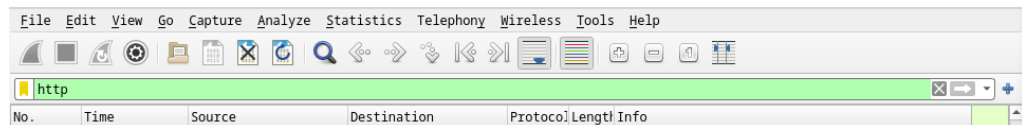
Password : Admin



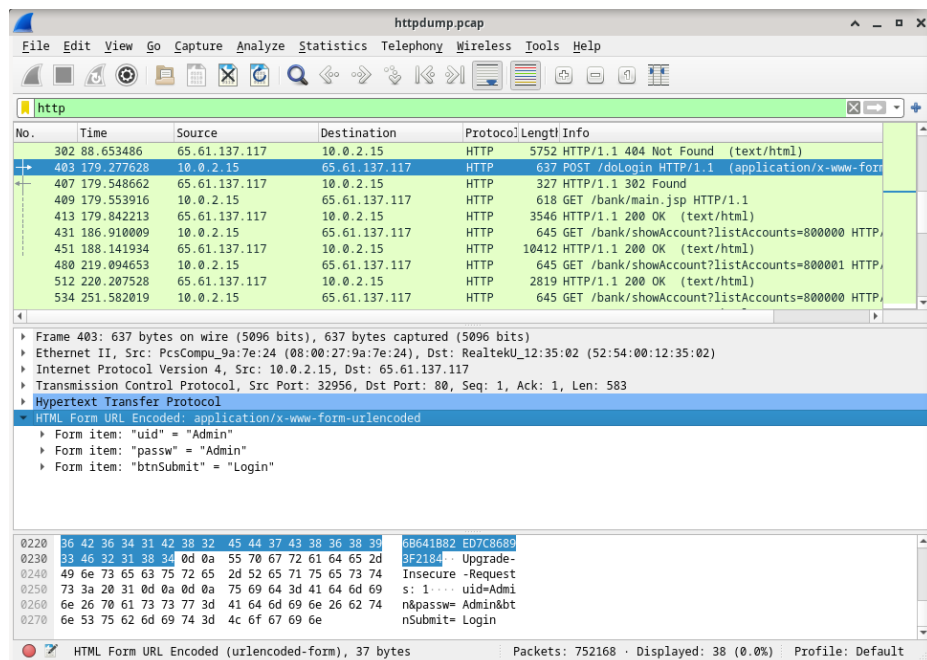
4. Merekam Paket HTTP Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan ke dalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/



5. Ketik http kemudian apply



6. Pilih post, pilih uid dan passw



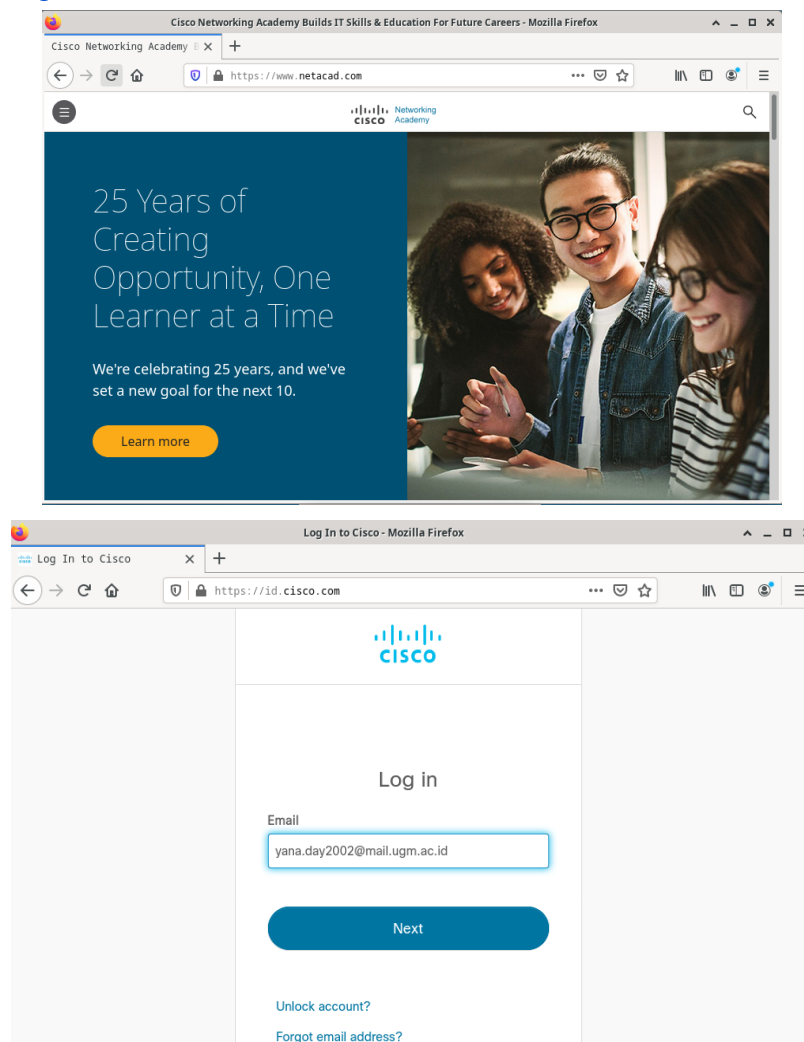
```
▶ Ethernet II, Src: PcsCompu_9a:7e:24 (08:00:27:9a:7e:24), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117
▶ Transmission Control Protocol, Src Port: 32956, Dst Port: 80, Seq: 1, Ack: 1, Len: 583
▶ Hypertext Transfer Protocol
  HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "uid" = "Admin"
      Key: uid
      Value: Admin
    Form item: "passwd" = "Admin"
      Key: passwd
      Value: Admin
    Form item: "btnSubmit" = "Login"
```

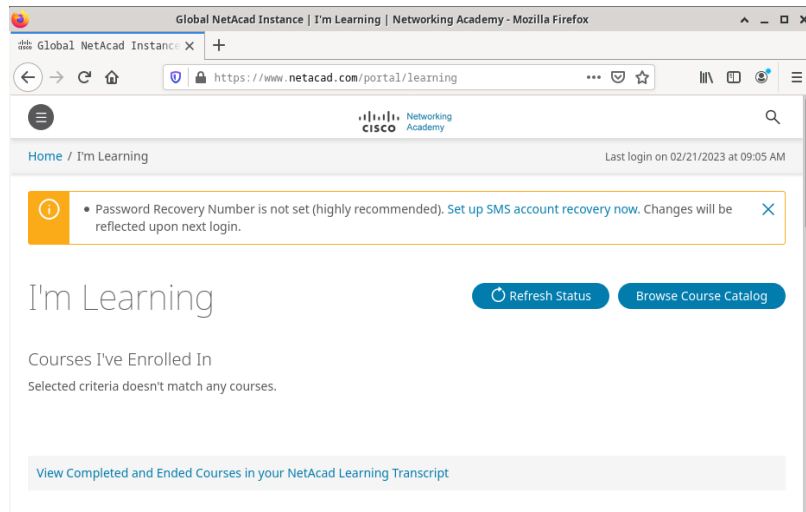
7. Merekam paket https

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

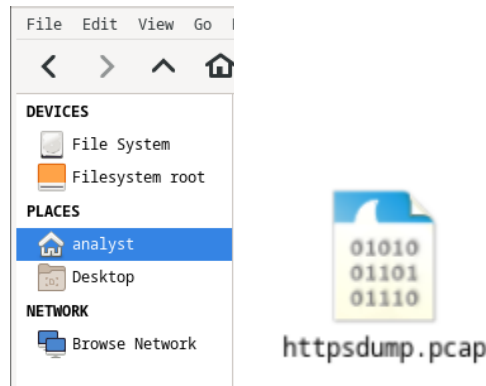
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

8. Login ke <https://www.netacad.com/>

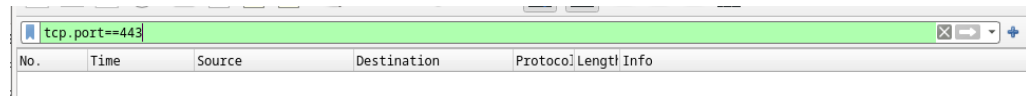




9. Melihat rekaman paket HTTPS



10. Filter tcp.port==443



11. Pilih application data

No.	Time	Source	Destination	Protocol	Length	Info
131	40.599732	23.52.112.234	10.0.2.15	TCP	60	443 → 48136 [FIN, ACK] Seq=78 Ack=47 Win=65535 Len=0
132	40.599776	10.0.2.15	23.52.112.234	TCP	54	48136 → 443 [ACK] Seq=47 Ack=78 Win=62780 Len=0
133	40.600225	10.0.2.15	23.52.112.234	TLSv1.2	100	Application Data
134	40.600592	10.0.2.15	23.52.112.234	TLSv1.2	85	Encrypted Alert
135	40.600778	10.0.2.15	23.52.112.234	TCP	54	48136 → 443 [FIN, ACK] Seq=124 Ack=79 Win=62780 Len=0
136	40.601893	23.52.112.234	10.0.2.15	TCP	60	443 → 48136 [ACK] Seq=79 Ack=93 Win=65535 Len=0
137	40.601893	23.52.112.234	10.0.2.15	TCP	60	443 → 48136 [ACK] Seq=79 Ack=124 Win=65535 Len=0
138	40.601894	23.52.112.234	10.0.2.15	TCP	60	443 → 48136 [ACK] Seq=79 Ack=125 Win=65535 Len=0
141	43.262881	10.0.2.15	35.241.9.150	TLSv1.2	93	Application Data
142	43.263798	10.0.2.15	35.241.9.150	TLSv1.2	78	Application Data

```

▼ Frame 133: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 20, 2023 21:20:31.176988000 EST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1676946031.176988000 seconds
  [Time delta from previous captured frame: 0.000449000 seconds]
  [Time delta from previous displayed frame: 0.000449000 seconds]
  [Time since reference or first frame: 40.600225000 seconds]
  Frame Number: 133
  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: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_9a:7e:24 (08:00:27:9a:7e:24)
  ▼ Destination: PcsCompu_9a:7e:24 (08:00:27:9a:7e:24)
    Address: PcsCompu_9a:7e:24 (08:00:27:9a:7e:24)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Address: RealtekU_12:35:02 (52:54:00:12:35:02)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 13.107.42.14, Dst: 10.0.2.15
  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: 0x0851 (2129)

▼ Flags: 0x0000
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
  Header checksum: 0x2eca [validation disabled]
  [Header checksum status: Unverified]
  Source: 13.107.42.14
  Destination: 10.0.2.15

▼ Transmission Control Protocol, Src Port: 443, Dst Port: 60154, Seq: 1, Ack: 47, Len: 46
  Source Port: 443
  Destination Port: 60154
  [Stream index: 20]
  [TCP Segment Len: 46]
  Sequence number: 1 (relative sequence number)
  Sequence number (raw): 5959256
  [Next sequence number: 47 (relative sequence number)]
  Acknowledgment number: 47 (relative ack number)
  Acknowledgment number (raw): 2498272490
  0101 .... = Header Length: 20 bytes (5)

```



```
▶ Flags: 0x018 (PSH, ACK)
  Window size value: 65535
  [Calculated window size: 65535]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x13d5 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0

▼ [SEQ/ACK analysis]
  [Bytes in flight: 39]
  [Bytes sent since last PSH flag: 39]

▼ [Timestamps]
  [Time since first frame in this TCP stream: 0.100190000 seconds]
  [Time since previous frame in this TCP stream: 0.099560000 seconds]
  TCP payload (39 bytes)

▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 34
    Encrypted Application Data: 308569ddd2f81076df535aa04c0d3f3cb44f5aea1c5da3be...
```

PEMBAHASAN:

Pada praktikum ini ditugaskan untuk merekam trafik HTTP dan HTTPS. Tools yang digunakan kali ini adalah Wireshark. Pertama, menjalankan tcpdump. Tcpdump berfungsi untuk merekam dan menginspeksi lalu lintas jaringan di sistem. Tcpdump merupakan tools untuk mengatasi masalah jaringan dan untuk melakukan uji keamanan.

Sebelum melakukan analisa dan perekaman *network traffic* pada enp0s3 lakukan pengecekan *IP Address* terlebih dahulu. Perintah **-I** pada **sudo tcpdump -I enp0s3 -s 0 -w httpdump.pcap** berfungsi untuk menentukan interface supaya tcpdump tidak menangkap semua lalu lintas pada tiap interface. Sedangkan perintah **-s** digunakan untuk menentukan panjang snapshot untuk setiap paket. Perintah **-w** digunakan untuk menulis hasil perintah tcpdump ke file dan menambahkan ekstensi. Tcpdump akan mencetak output yang akan tersimpan di file. Hasil uid, password, dan btnSubmit dapat dilihat pada **post > HTML form URL Encode: application/x-www-form-urlencoded**.

Untuk HTTPS langkahnya tidak jauh berbeda. Mula-mula buka web dengan HTTPS disini contohnya menggunakan netacad. Ketika menggunakan HTTPS, muatan data pesan akan dienkripsi dan hanya dapat dilihat oleh perangkat yang merupakan bagian dari percakapan terenkripsi. Setelah berhasil login file tcpdump akan tersimpan. Untuk menyaring tcp port gunakan filter `tcp.port==443` lalu pilih application data. Setelah section TCP, sekarang tampil section Secure Sockets Layer (SSL).

E. KESIMPULAN

- HTTP adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia
- HTTPS merupakan versi lebih aman dari HTTP, tugasnya sama persis namun dalam pertukaran data https menggunakan autentikasi dan komunikasi tersandi
- Perbedaan HTTP dengan HTTPS adalah pada keamanannya, HTTP adalah protokol yang belum menggunakan SSL/TLS, dan HTTPS adalah versi yang sudah menggunakan SSL/TLS untuk mengenkripsi koneksi antara web.

F. DAFTAR PUSTAKA

Admin Bidang E-Gov. (2020, October 13). *Apa Sih HTTP dan HTTPS itu?* | Dinas

Komunikasi dan Informatika - Kabupaten Kuburaya. Diskominfo Kubu Raya.

Retrieved Februari 21, 2023, from

<https://diskominfo.kuburayakab.go.id/read/63/apa-sih-http-dan-https-itu>

IdCloudHost. (n.d.). *Mengenal Apa itu Pengertian HTTP*. IDCloudHost. Retrieved

February 21, 2023, from <https://idcloudhost.com/kamus-hosting/http/>

Rosyida, M. (2022, September 5). *HTTPS: Arti, Manfaat, Cara Kerja, dan Bedanya*

Dengan HTTP. DomaiNesia. Retrieved February 21, 2023, from

https://www.domainesia.com/berita/https-adalah/#Apa_Itu_HTTPS