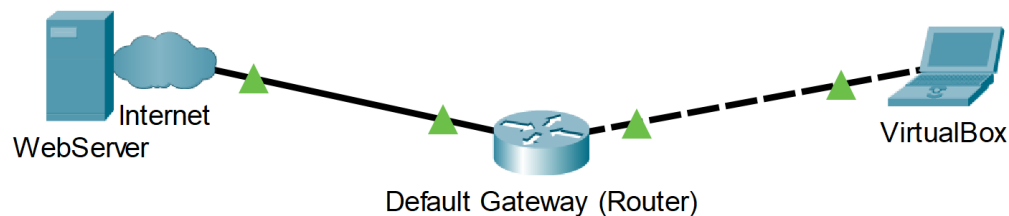


Sesi I : 09.00 - 12.00 WITA
Cabang Lomba : Teknologi Keamanan Siber (Cyber Security)
Nama Kegiatan :
Bagian 1 - Penggunaan Tools NMAP
Bagian 2 - Capture dan Tampilkan Jalur HTTP
Bagian 3 - Capture dan Tampilkan Jalur HTTPS

Topologi pada Soal ini :



Skenario Kegiatan :

Pada sesi Lab ini yaitu melakukan *port scanning* yang mana banyak dilakukan oleh seseorang yang melakukan pengintaian pada sebuah aplikasi. Ada berbagai macam metode *port scanning* yang dapat digunakan oleh seorang yang berkerja pada bidang Cyber Security.

Teknologi HyperText Transfer Protocol (HTTP) adalah protokol lapisan aplikasi yang menyajikan data melalui Web Browser. Tidak ada perlindungan untuk pertukaran data antara dua perangkat yang saling berkomunikasi dengan menggunakan protokol HTTP. Sedangkan HTTPS (Hypertext Transfer Protocol Secure), protokol komunikasi dienkripsi menggunakan TLS (Transport Layer Security) atau yang sebelumnya seperti SSL (Secure Sockets Layer). Enkripsi ini menyembunyikan makna sebenarnya dari data yang sedang ditukarkan.

Diharapkan sesi ini peserta dapat mengikuti langkah demi langkah secara seksama dan hati-hati. Langkah-langkah yang diberikan bertujuan untuk dapat membantu peserta menggunakan *tool* NMAP dan menjelaskan beberapa permintaan terkait *capture* serta analisa hasil dari *tool* PCAP (Wireshark).

Kebutuhan sistem yang harus dipersiapkan :

- ✓ Menjalakan aplikasi Virtual Box dan Import file **LKS_SMK.ova** yang telah disediakan oleh Juri.
- ✓ Hubungkan salah satu port interface Virtual Machine dengan akses Internet yang sedang anda gunakan.
- ✓ Gunakan Username : **analyst** & password : **cybercops** untuk mengakses pada VM.

Bagian 1 : Penggunaan Tools NMAP

Soal A : Silahkan gunakan Terminal dan tampilkan screenshot dari Terminal anda serta jelaskan bagaimana cara anda memanggil menu Tools NMAP melalui Terminal tersebut.

```
[analyst@secOps ~]$ nmap --help
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>

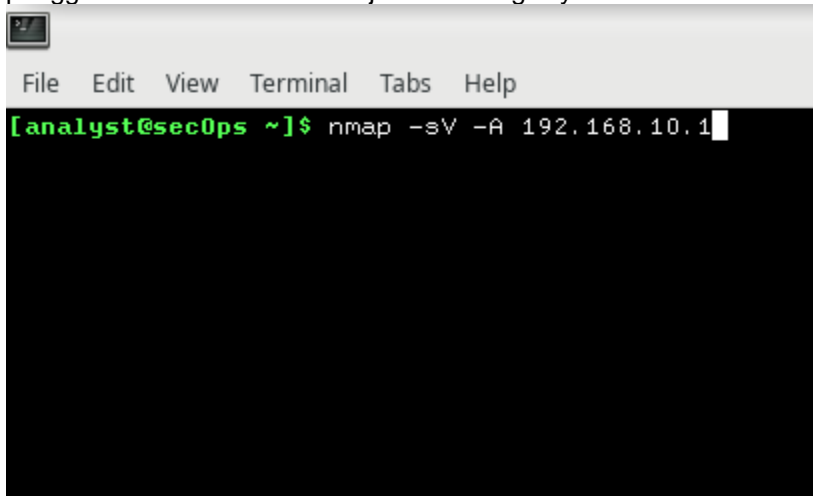
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)

SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<n1=v1[,n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
    script-categories.

OS DETECTION:
```

Untuk memanggil menu Tools NMAP, bisa menggunakan perintah sebagai berikut yaitu `$nmap -help`

Soal B : Silahkan gunakan Terminal dan tampilkan screenshot dari Terminal, contoh satu baris perintah penggunaan Tools NMAP dan jelaskan fungsinya.



Untuk menggunakan Tools NMAP, bisa menggunakan perintah sebagai berikut: **\$nmap <options> <ip target/url name>**

-sV digunakan untuk mengecek versi dari protocol yang digunakan oleh target

-A digunakan untuk melakukan pengecekan secara menyeluruh seperti system operasi apa yang digunakan oleh target

Soal C : Ketika diminta untuk ketikkan Terminal

nmap -A -T4 scanme.nmap.org

Maka apakah yang akan terjadi, silahkan ambil screenshotnya dan jelaskan maksud dari fungsi tersebut.

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

analyst@secOps:-
analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2022-09-18 21:39 EDT
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: 993 closed 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)
25/tcp    filtered  smtp
53/tcp    open      domain      (generic dns response: NOTIMP)
80/tcp    open      http        Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
1723/tcp  filtered  pptp
9929/tcp  open      nping-echo  Nping echo
31337/tcp open      tcpwrapped

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=9/18%Time=6327C87A%P=x86_64-unknown-linux-gnu%r
SF:(DNSStatusRequestTCP,E,"\0\0c\0\0\0x90\04\0\0\0\0\0\0\0");
Service Info: 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 79.09 seconds
analyst@secOps ~]$
```

Berdasarkan gambar diatas, bisa disimpulkan sebagai berikut:

-A berfungsi untuk mengecek sistem operasi apa yang digunakan dan versi berapa yang digunakan serta melihat protokol apa saja yang digunakan. Dari gambar diatas dapat diketahui bahwa sistem operasi yang digunakan adalah

Linux Ubuntu dengan versi 2.13 dengan protokol ssh.

-T berfungsi untuk mengatur kecepatan dari pemindaian atau waktu scan yang dilakukan oleh Terminal. Semakin tinggi angka yang digunakan semakin cepat waktu pemindaian nya (0-5)

Soal D : Ketika diminta untuk ketikan pada Tools Nmap tersebut perintah berikut

nmap -A -T4 localhost

Maka apakah yang akan terjadi, silahkan ambil screenshotnya dan jelaskan maksud dari fungsi tersebut.

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
analyst@secOps:~  
[analyst@secOps ~]$ nmap -A -T4 localhost  
Starting Nmap 7.70 ( https://nmap.org ) at 2022-09-18 21:39 EDT  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000044s latency).  
Other addresses for localhost (not scanned): ::1  
Not shown: 998 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 4  
|   | vsFTPd 3.0.3 - secure, fast, stable  
|_End of status  
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)  
| ssh-hostkey:  
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)  
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)  
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)  
Service Info: Host: Welcome  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds  
[analyst@secOps ~]$
```

Dari gambar diatas, dapat disimpulkan sebagai berikut:

-A berfungsi untuk mengecek sistem operasi apa yang digunakan dan versi berapa yang digunakan serta melihat protokol apa saja yang digunakan. Dapat diketahui bahwa protokol yang digunakan adalah ftp dengan versi 2.0.8

Soal E : Bagiamankah cara untuk melihat alamat ip yang dimiliki oleh komputer virtual anda (Virtual Box) dan berikan screenshotsnya serta jelaskan berapa alamat network yang anda dapatkan.

Untuk melakukan pengecekan IP yang dimiliki, bisa menggunakan 2 perintah yaitu sebagai berikut:

1. Menggunakan perintah **\$ifconfig**

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 20.20.20.3 netmask 255.255.255.0 broadcast 20.20.20.255  
    inet6 fe80::a00:27ff:fe25:6b4e prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:25:6b:4e txqueuelen 1000 (Ethernet)  
    RX packets 3785 bytes 388809 (379.6 KiB)  
    RX errors 0 dropped 1360 overruns 0 frame 0  
    TX packets 1593 bytes 127437 (124.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 2247 bytes 126975 (123.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2247 bytes 126975 (123.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[analyst@secOps ~]$
```

Dengan menggunakan perintah **ifconfig**, dapat diketahui interface apa saja yang sedang aktif. Dari gambar diatas interface saya adalah enp0s3 dan mendapatkan alamat IP 20.20.20.3.

2. Menggunakan perintah **\$ip address**

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
analyst@secOps:~  
[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 08:00:27:25:6b:4e brd ff:ff:ff:ff:ff:ff  
    inet 20.20.20.3/24 brd 20.20.20.255 scope global dynamic enp0s3  
        valid_lft 516sec preferred_lft 516sec  
    inet6 fe80::a00:27ff:fe25:6b4e/64 scope link  
        valid_lft forever preferred_lft forever  
[analyst@secOps ~]$
```

Dengan menggunakan perintah **ip address**, dapat diketahui interface apa saja yang sedang aktif. Dari gambar diatas interface untuk internet saya adalah enp0s3 dan mendapatkan alamat IP 20.20.20.3 dengan prefix /24

Bagian 2 : Capture dan Tampilkan Traffic pada HTTP

Di bagian ini, peserta akan menggunakan **tcpdump** untuk menangkap konten traffic protokol HTTP. Peserta akan menggunakan tcpdump untuk menyimpan traffic ke file packet capture (**pcap**). Catatan ini kemudian dapat dianalisis menggunakan aplikasi Wireshark .

Langkah 1: Jalankan Virtual Machine dan Login.

Jalankan CyberOps Workstation VM.

Username: **analyst**

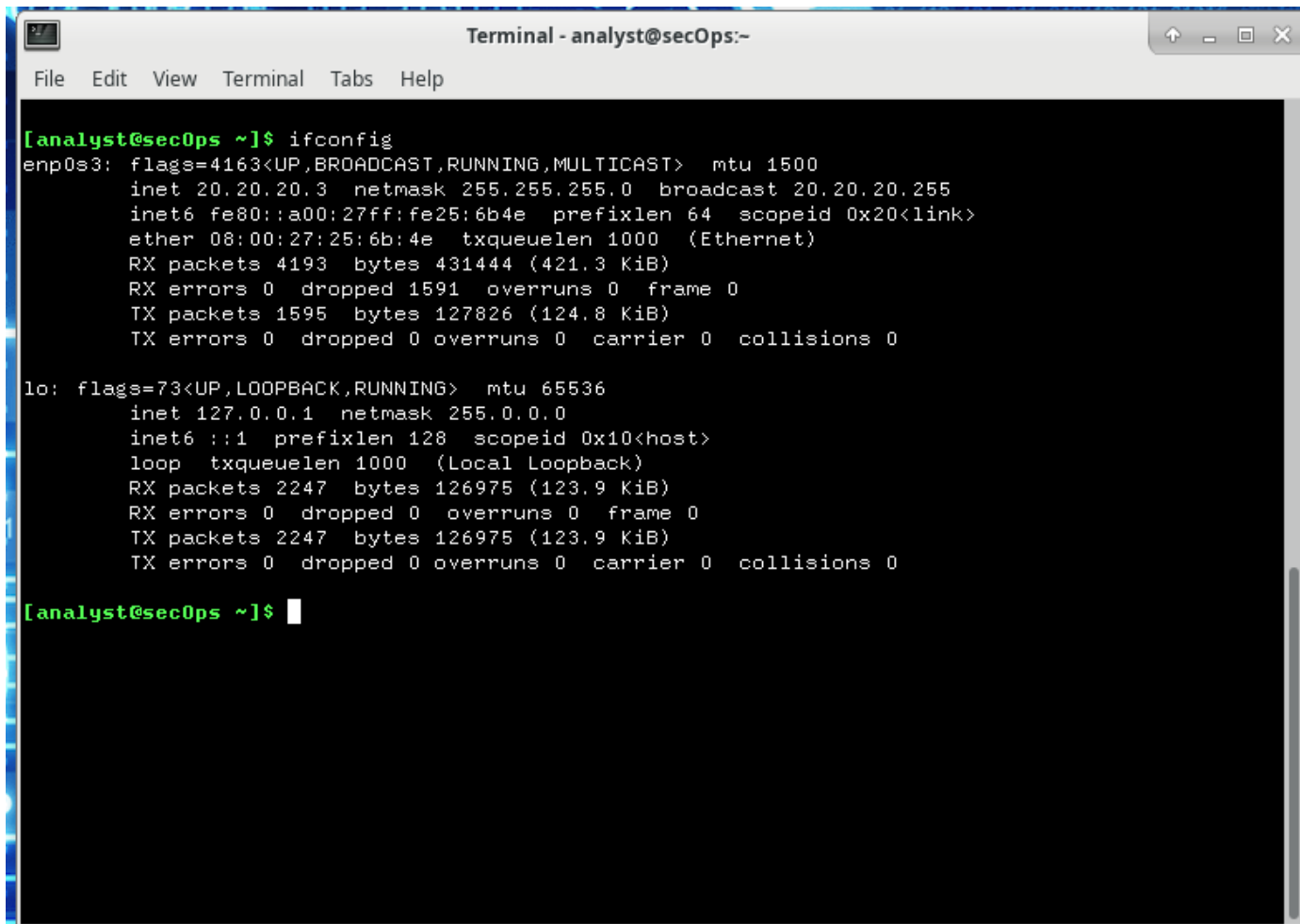
Password: **cyberops**

Langkah 2: Buka terminal dan jalankan tcpdump.

- Buka terminal dan ketikkan command **ifconfig**.

```
[analyst@secOps ~]$ ifconfig
```

- List daftar interface dan alamat IP yang ditampilkan!



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 20.20.20.3 netmask 255.255.255.0 broadcast 20.20.20.255  
    inet6 fe80::a00:27ff:fe25:6b4e prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:25:6b:4e txqueuelen 1000 (Ethernet)  
    RX packets 4193 bytes 431444 (421.3 KiB)  
    RX errors 0 dropped 1591 overruns 0 frame 0  
    TX packets 1595 bytes 127826 (124.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 2247 bytes 126975 (123.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2247 bytes 126975 (123.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[analyst@secOps ~]$
```

List daftar IP yang muncul adalah sebagai berikut:

- enp0s3 memiliki alamat IP 20.20.20.3 dengan netmask 255.255.255.0 dan memiliki broadcast 20.20.20.255
- lo atau IP Loopback dengan alamat IP 127.0.0.1 dengan netmask 255.0.0.0

- c. Melalui terminal, masukkan perintah **sudo tcpdump -i enp0s3 -s0 -w tcpdump.pcap**, masukkan kata sandi **cyberops** saat diminta.

```
[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
```

Perintah ini memulai **tcpdump** dan mencatat traffic jaringan pada interface enp0s3. Jelaskan maksud dari beberapa fungsi perintah berikut!

Command **-i** : Perintah **-i** ditujukan untuk Interfaces apa yang digunakan. Perintah diatas, ditujukan bahwa interface yang digunakan adalah enp0s3

Command **-s** : Perintah **-s** berfungsi untuk menangkap byte atau bit dari setiap packet yang diinginkan. Sebaiknya perintah **-s** ini diatur ke 0 karena 0 merupakan ukuran default dari fungsi perintah **-s** itu sendiri.

Command **-w** : Perintah **-w** berfungsi untuk menulis paket mentah menjadi sebuah file daripada memunculkan mereka langsung di terminal.

- d. Buka web browser yang tersedia pada VM. Ketikkan alamat ke www.altoromutual.com/bank/login.aspx

Sign In | Contact Us | Feedback | Search

Go

DEMO SITE ONLY

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers

Online Banking Login

Username:

Password:

This connection is not secure. Logins entered here could be compromised. Learn More

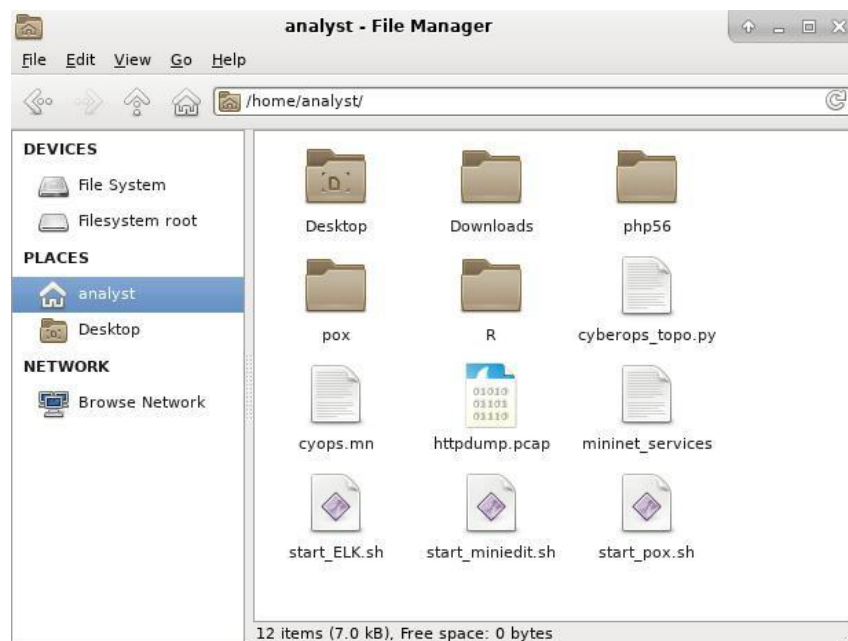
Karena situs web ini menggunakan HTTP, maka traffic tidak terenkripsi. Click the Username field to see the warning pop up.

- e. Masukan username **LKSSMK@2022** dan password **LKSSMK@2022** lalu klik **Login**.
- f. Kembali ke Terminal tempat **tcpdump** berjalan. Masukkan CTRL+C untuk menghentikan pengambilan paket.

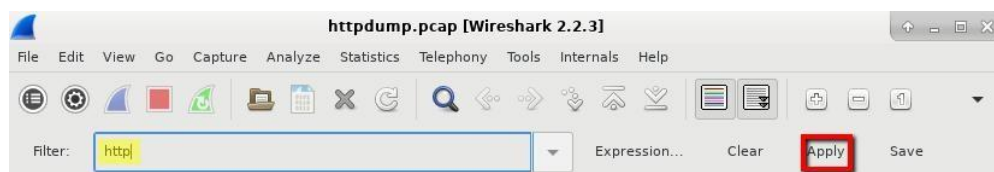
Langkah 3: Lihat hasil tangkapan pada protokol HTTP.

Setelah **tcpdump** dieksekusi pada langkah sebelumnya, hasil output disimpan ke dalam file **httpdump.pcap**. File ini terletak di direktori home untuk dianalisis.

- a. Klik File Manajer pada desktop, lalu klik ke folder **analyst**. Double klik file **httpdump.pcap** untuk membukanya menggunakan Wireshark.



- b. Pada aplikasi Wireshark, filter protokol **http** kemudian klik **Apply**.



- c. Jelajahi pesan HTTP yang berbeda dengan memilih **POST**.

httdump.pcap [Wireshark 2.2.3]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
124	10.252422	10.0.2.15	65.61.137.117	HTTP	514	[TCP Previous segment not captured]
138	10.332405	65.61.137.117	10.0.2.15	HTTP	761	HTTP/1.1 200 OK (text/html)
181	13.298897	10.0.2.15	65.61.137.117	HTTP	675	POST /bank/login.aspx HTTP/1.1
185	13.472733	65.61.137.117	10.0.2.15	HTTP	611	HTTP/1.1 302 Found (text/html)
187	13.476894	10.0.2.15	65.61.137.117	HTTP	579	GET /bank/main.aspx HTTP/1.1
195	13.603919	65.61.137.117	10.0.2.15	HTTP	171	HTTP/1.1 200 OK (text/html)

- d. Pesan ditampilkan melalui jendela bagian bawah. Perluas **HTML Form URL Encoded: application/x-www-form-urlencoded**.

▶ Frame 181: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits)

▶ Ethernet II, Src: PcsSyste_21:f3:5c (08:00:27:21:f3:5c), 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: 58652, Dst Port: 80, Seq: 462, Ack: 8988, Len: 621

▶ Hypertext Transfer Protocol

▶ **HTML Form URL Encoded: application/x-www-form-urlencoded**

- e. Apa isi dari dua informasi yang ditampilkan?
- Pada bagian proses penangkapan paket, terdapat informasi berupa No, Time, Source, Destination, Protocol, Length, dan Info
 - Pada bagian HTML Form, terdapat
 - Form item uid dengan key uid dan value berupa LKSSMK@2022
 - Form item passwd dengan key passwd dan value berupa LKSSMK@2022

Bagian 3 : Capture dan Tampilkan Traffic pada HTTPS

Peserta akan menggunakan kembali **tcpdump** untuk menangkap lalu lintas HTTPS. Setelah memulai tcpdump, Peserta akan memperoleh traffic protokol HTTPS kemudian dianalisis kembali menggunakan aplikasi Wireshark.

Langkah 1: Jalankan tcpdump melalui terminal.

- Melalui terminal, ketikkan perintah **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**. Masukkan password **cyberops**.

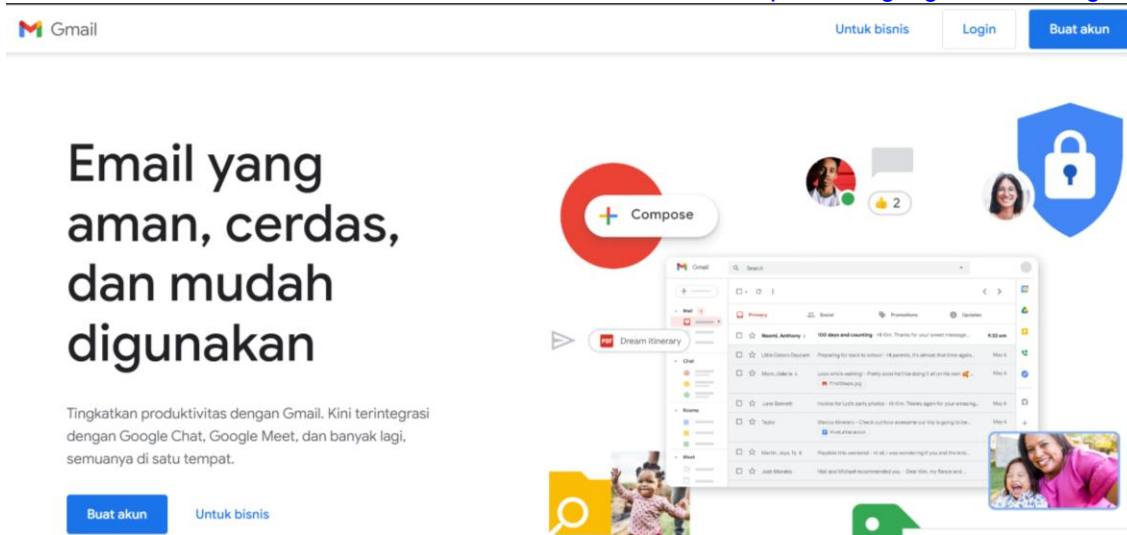
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
```

```
[sudo] password for analyst:
```

```
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Semua traffiic yang direkam akan disimpan ke file **httpsdump.pcap** di direktori home untuk dianalisis menggunakan Wireshark.

- Buka web browser dalam Linux Workstation. Akses ke halaman <https://www.google.com/intl/id/gmail/about/>

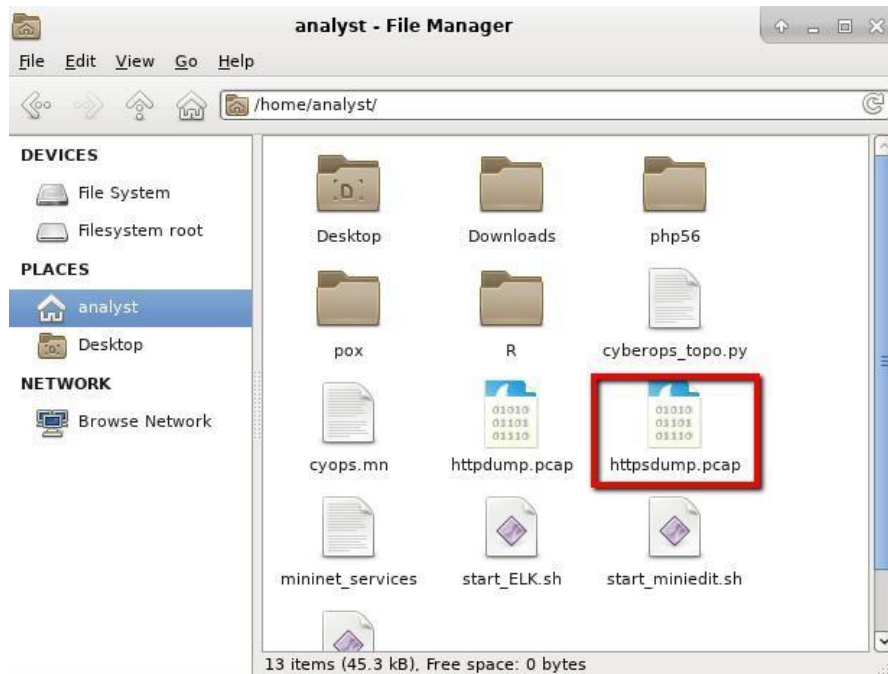


- Silahkan klik tombol login
- Masukkan username dan password akun Gmail.
- Tutup web browser.
- Kembali ke terminal tempat **tcpdump** berjalan. Masukkan **CTRL+C** untuk menghentikan pengambilan paket.

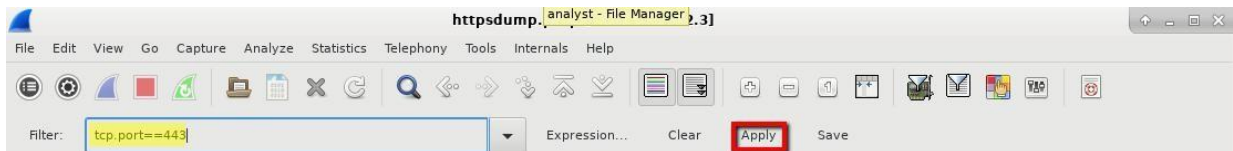
Langkah 2: Lihat hasil tangkapan pada protokol HTTPS.

Setelah **tcpdump** dieksekusi pada langkah sebelumnya, hasil output disimpan ke dalam file **httpsdump.pcap**. File ini terletak di direktori home untuk dianalisis.

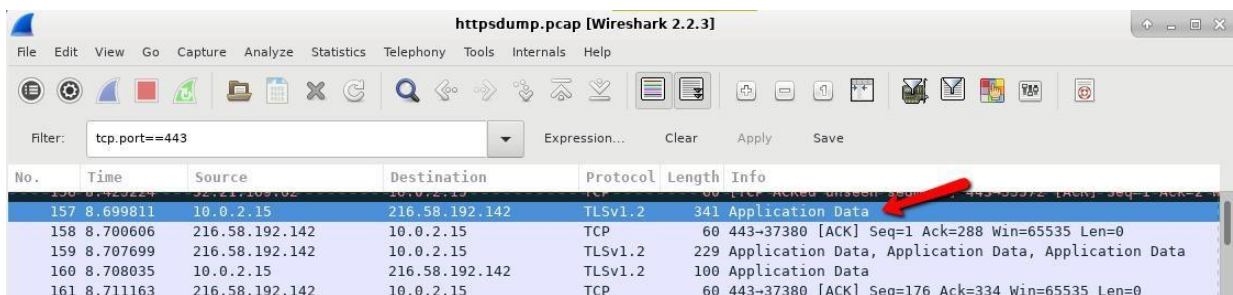
- Klik File Manajer pada desktop, lalu klik ke folder **analyst**. Double klik file **httpsdump.pcap** untuk membukanya menggunakan Wireshark.



- b. Melalui Wireshark, filter berdasarkan traffic HTTPS melalui port 443. Masukkan **tcp.port==443** pada filter, dan klik **Apply**.



- c. Jelajahi pesan HTTPS yang berbeda dan pilih pesan **Application Data**.



- d. Di jendela bawah, pesan akan ditampilkan.

Hal apa yang telah menggantikan bagian HTTP pada file screenshot sebelumnya?

Bagian yang berubah atau berganti dari HTTP ke adalah adanya enkripsi data yang melindungi informasi sensitif seperti username dan password kita.

- e. Perluas sepenuhnya bagian Secure Sockets Layer.

```

▶ Frame 157: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits)
▶ Ethernet II, Src: PcsSyste_21:f3:5c (08:00:27:21:f3:5c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 216.58.192.142
▶ Transmission Control Protocol, Src Port: 37380, Dst Port: 443, Seq: 1, Ack: 1, Len: 287
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 282
    Encrypted Application Data: 0000000000000000bed2031d6dabc4c685ca7854a009a7a56...

```

f. **Klik Encrypted Application Data.**

Apakah **Application Data** dalam format plaintext ?

Tidak dalam format berupa plaintext, karena data yang muncul sudah di enkripsi.

Kesimpulan Hasil Sesi Lab ini

Apa keuntungan dari menggunakan websites yang memiliki akses menggunakan protocol HTTPS dari pada yang HTTP ?

Keuntungan menggunakan protokol HTTPS dibandingkan dengan protokol HTTP adalah keamanan yang lebih terjamin. Karena HTTPS mengenkripsi setiap data yang kita input ke dalam web, berbeda dengan HTTP yang menyimpan data kita dalam bentuk teks mentahan atau plaintext tanpa ada enkripsi sedikitpun. Adanya enkripsi data membuat data kita lebih sulit untuk diretas atau bocor ke publik.

Kesimpulan secara garis besar. HTTPS lebih aman dibandingkan dengan HTTP.
