

LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1

PERTEMUAN 2

**Eksplorasi Nmap & Pemantauan Trafik HTTP dan HTTPS dengan
menggunakan Wireshark**



DISUSUN OLEH

Nama : Muhamad Alan Dharma Saputro S
NIM : 21/481348/SV/19761
Hari, Tanggal : Selasa, 21 Februari 2023
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Kelas : RI4AA

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

2022

A. Tujuan

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

B. 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.

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

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

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

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

C. Alat dan Bahan

1. CyberOps Workstation virtual machine
2. Internet Access

D. Instruksi Kerja

a. Eksplorasi nmap

1. Eksplorasi Nmap

Start CyberOps Workstation

Buka terminal kemudian ketikkan

```
[analyst@secOps ~]$ 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
    Manual page nmap(1) line 1 (press h for help or q to quit)
```

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

    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
    determine whether they are open or closed. Nmap reports the state
    combinations open|filtered and closed|filtered when it cannot determine
    which of the two states describe a port. The port table may also
    include software version details when version detection has been
    requested. When an IP protocol scan is requested (-s0), Nmap provides
    information on supported IP protocols rather than listening ports.

    In addition to the interesting ports table, Nmap can provide further
    information on targets, including reverse DNS names, operating system
    Manual page nmap(1) line 19 (press h for help or q to quit)
```

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

In addition to the interesting ports table, Nmap can provide further
information on targets, including reverse DNS names, operating system
guesses, device types, and MAC addresses.

A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
Manual page nmap(1) line 40 (press h for help or q to quit)
```

Apa itu Nmap?

Nmap (Network Mapper) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan.

Apa fungsi dari Nmap?

Nmap berfungsi untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal.

2. Localhost Scanning

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

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

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 3
|   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 19.04 seconds
[analyst@secOps ~]$
```

Port dan layanan apa yang terbuka?

21/tcp dengan layanan ftp

22/tcp dengan layanan ssh

23/tcp dengan layanan telnet

Software apa yang digunakan pada port yang terbuka tersebut?

Vsftpd 2.0.8

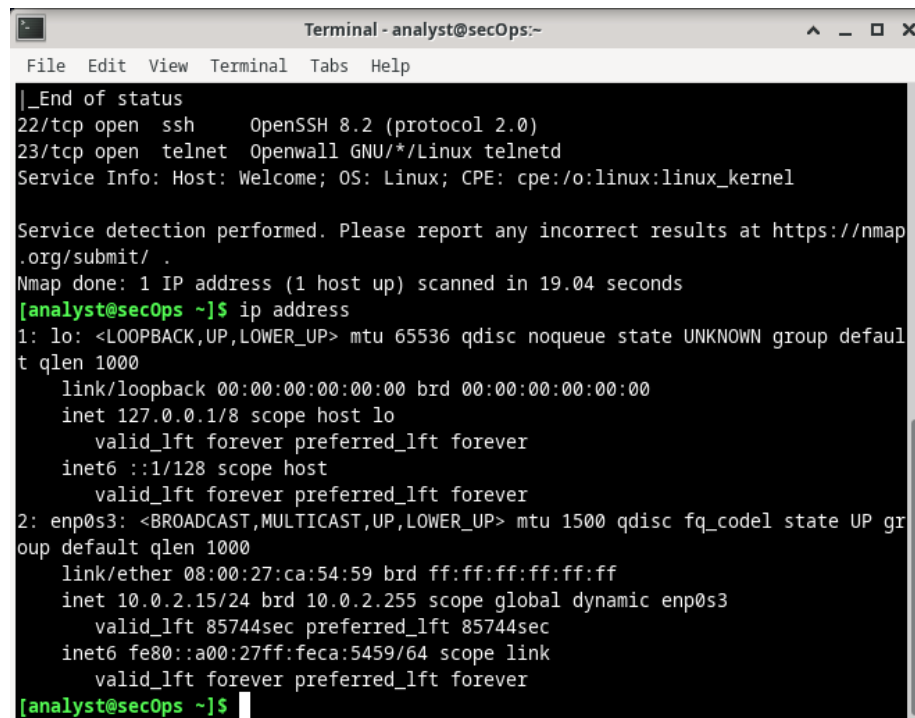
OpenSSH 8.2 (protocol 2.0)

Openwall GNU/*/Linux telnetd

3. Network Scanning

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

[analyst@secOps ~]\$ ip address



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

|_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 19.04 seconds
[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:ca:54:59 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 85744sec preferred_lft 85744sec
    inet6 fe80::a00:27ff:feca:5459/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Berapakah alamat IP dan subnet mask dari PC host?

10.0.2.15 dengan subnet mask 24

Lakukanlah port scanning dengan menggunakan Nmap

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

```
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 07:11 EST
Nmap scan report for 10.0.2.15
Host is up (0.000095s 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 35.03 seconds
[analyst@secOps ~]$
```

Berapakah jumlah host yang terdeteksi?

256 IP address (1 host up)

b. Pemantauan trafik http dan https dengan menggunakan wireshark

1. Jalankan VM dan Login

Username: analyst

Password: cyberops

2. Buka terminal dan menjalankan tcpdump. Pengecekan alamat IP dengan menggunakan perintah:

[analyst@secOps ~]\$ ip address

```
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:ca:54:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.134/24 brd 192.168.100.255 scope global dynamic enp0s3
        valid_lft 3580sec preferred_lft 3580sec
    inet6 2001:448a:404a:3150:a00:27ff:feca:5459/64 scope global dynamic mngtmpa
        valid_lft 580sec preferred_lft 580sec
    inet6 fe80::a00:27ff:feca:5459/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

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

[sudo] password for analyst:

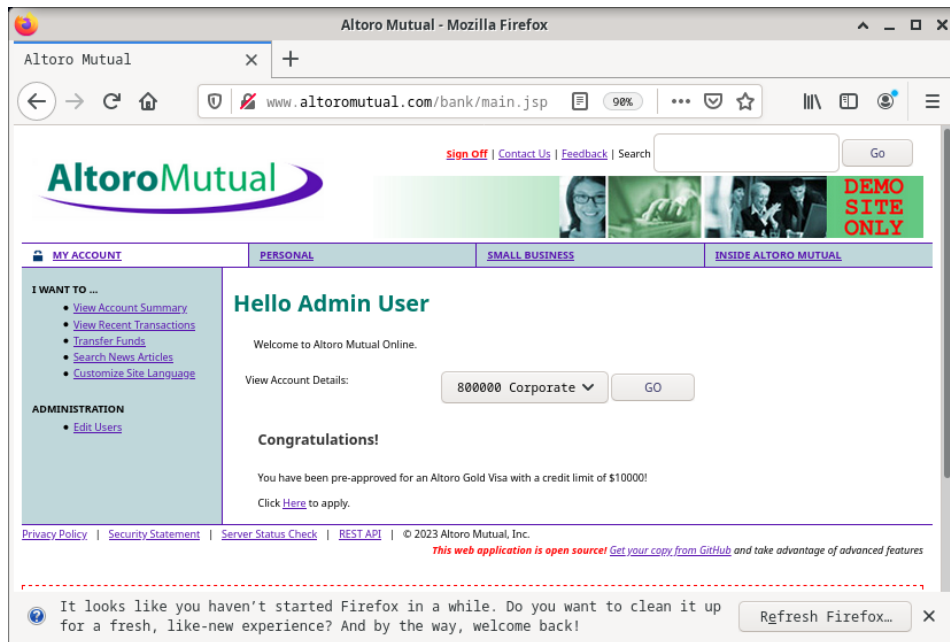
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

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

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

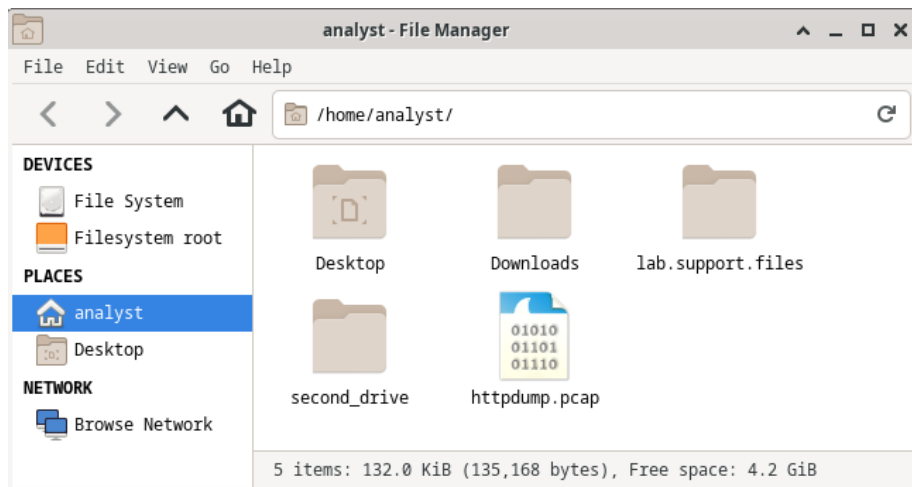
Username : Admin

Password : Admin

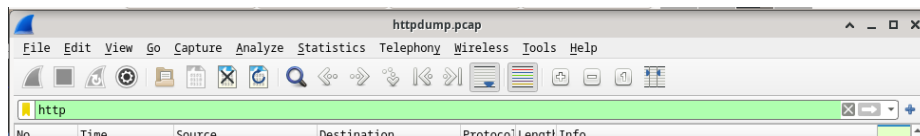


4. Merekam Paket HTTP

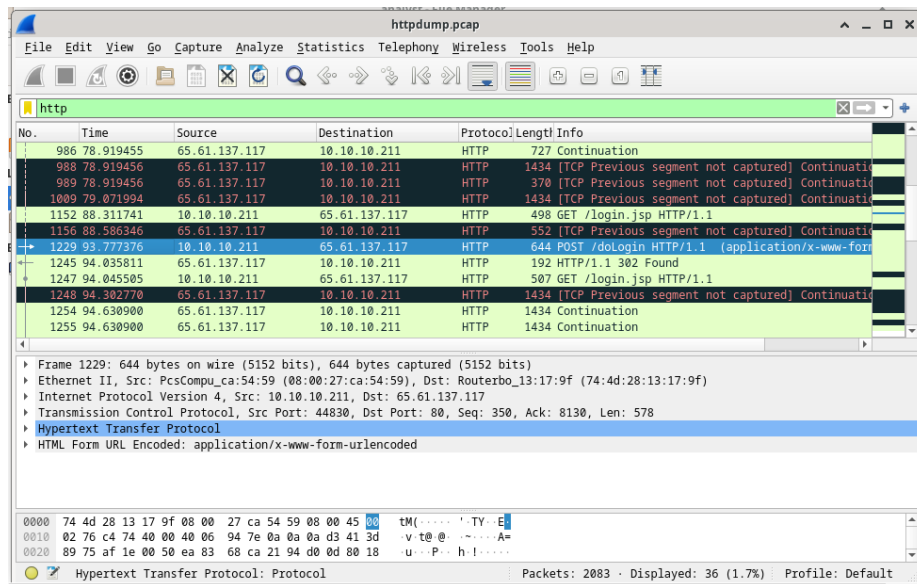
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/.



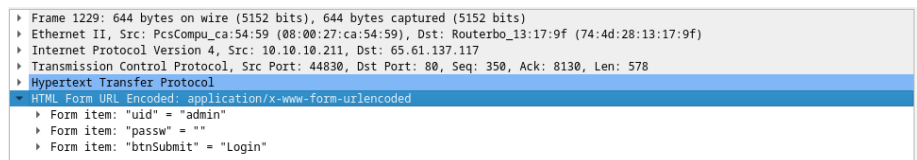
5. Filter http kemudian klik Apply



6. Pilih POST



7. Lakukanlah analisis terhadap uid dan passw

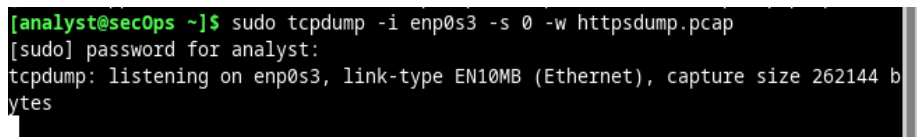


8. Merekam Paket HTTPS

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

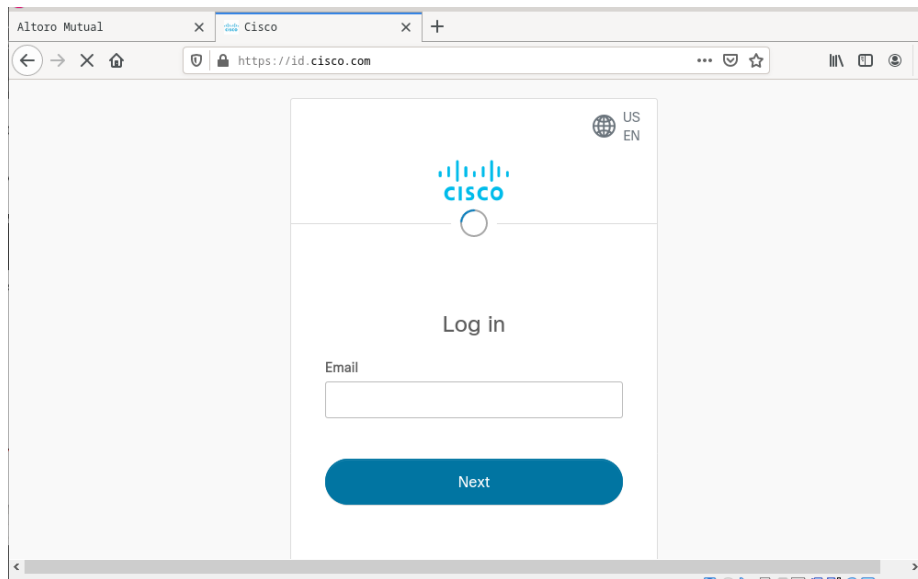
[sudo] password for analyst:

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

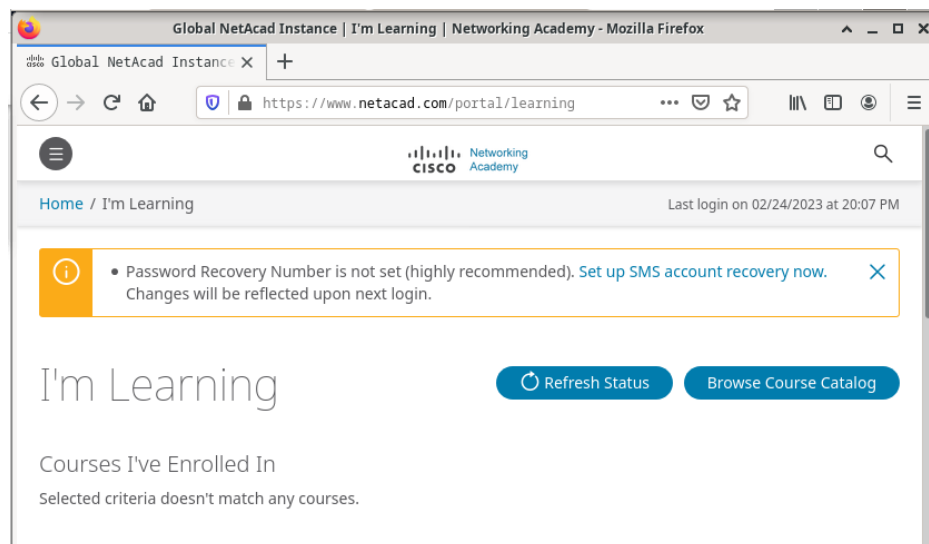


9. Buka link <https://www.netacad.com/> melalui browser di CyberOps Workstation VM.

10. Klik Login

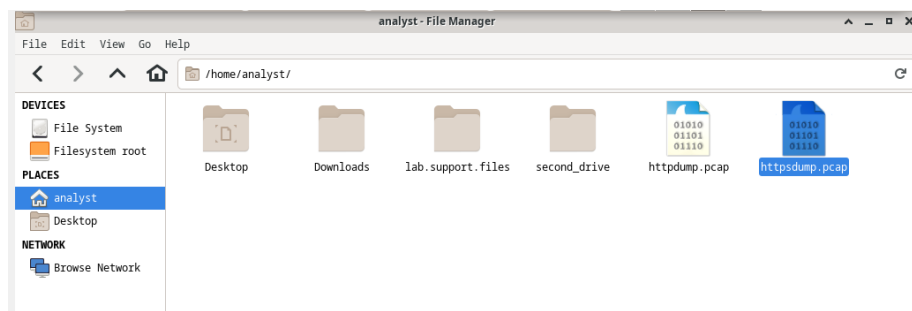


11. Masukkan username dan password anda

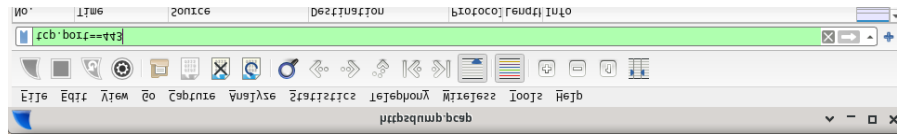


12. Melihat Rekaman Paket HTTPS

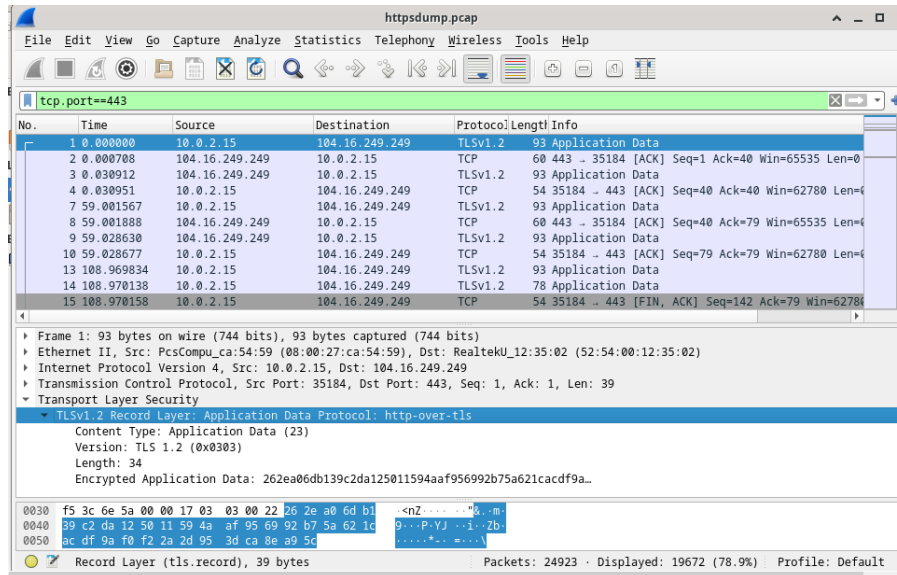
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpsdump.pcap. File ini terletak pada folder /home/analyst/.



13. Filter tcp.port==443



14. Pilih Application Data



15. Analisis hasil yang didapatkan

E. Pembahasan

Modul 2

1. Apa itu Nmap?

- Sesuai deskripsi yang berada pada terminal Nmap (Network Mapper) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Yang dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal.

Apa fungsi dari Nmap?

- Nmap berfungsi untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan apa yang diberikan, sistem operasi apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

2. Port dan layanan apa yang terbuka?

- Untuk port 21/tcp menggunakan layanan ftp (file transfer protocol) yang bertugas untuk menjembatani pertukaran informasi di dalam suatu komputer melalui suatu jaringan dengan koneksi tcp (transmission control protocol).

- Port 22/tcp menggunakan layanan ssh memiliki fungsi untuk mengelola lalu-lintas transfer data yang menggunakan enkripsi.
- Port 23/tcp menggunakan layanan telnet yang memungkinkan penggunaanya untuk login dan mengakses jaringan komputer lain secara remote atau jarak jauh.

Software apa yang digunakan pada port yang terbuka tersebut?

- Software yang digunakan pada port 21/tcp merupakan vsftpd version 2.0.8, port 22/tcp menggunakan OpenSSH version 8.2 (protocol 2.0), dan port 23/tcp menggunakan Openwall version GNU/*/Linux telnetd.

3. Berapakah alamat IP dan subnet mask dari PC host?

- Karena CyberOps Workstation pada VirtualBox diatur menggunakan jaringan NAT sehingga IP didapatkan yaitu 10.0.2.15 dengan subnet mask 24.

Berapa jumlah host yang terdeteksi?

- Nmap mendeteksi terdapat 256 IP address dengan 1 host.

Modul 3

Untuk modul 3 ini jaringan pada VirtualBox saya ubah dari NAT menjadi Bridged Adapter sehingga IP Address VirtualBox pun berubah sesuai network PC yang digunakan yaitu 192.168.100.134/24. Lalu terdapat perintah `sudo tcpdump -i enp0s3 -s 0 -w` yang akan dijelaskan nanti. Selanjutnya masuk pada website <http://www.altoromutual.com/login.jsp>, altoro mutual merupakan bank gadungan yang dirancang memiliki banyak celah keamanan sehingga cocok digunakan untuk melakukan praktikum keamanan jaringan ini.

Lalu buka file `httpdump.pcap` yang telah didownload tadi menggunakan wireshark yang merupakan tool untuk menganalisis paket data jaringan yang melakukan pengawasan paket secara real time dan menangkap data yang akan ditampilkan selengkap mungkin. Setelah masuk ke wireshark filter file tersebut dengan `http` agar menampilkan protocol `http` saja.

Sama seperti sebelumnya menggunakan perintah `sudo tcpdump`, namun file yang didownload merupakan file `https`. Tujuan mengganti jaringan menjadi Bridged Adapter agar dapat membuka netacad, karena saat menggunakan jaringan NAT netacad tidak dapat diakses. Setelah dapat mengakses netacad, login menggunakan akun yang telah dibuat sebelumnya. Dilanjut dengan membuka file `https` menggunakan wireshark tool lalu filter `tcp.port==443`.

Perintah `-i` memungkinkan kita untuk menentukan interface. Jika tidak ditentukan, `tcpdump` akan menangkap semua traffic pada semua interfaces. Perintah `-s` digunakan untuk menentukan panjang snapshot untuk setiap paket. Kita harus membatasi snaplen ke nomor terkecil yang akan menangkap informasi protokol yang diminati. Menyetel snaplen ke 0 dan menyetel nya ke default 262144, untuk kompatibilitas mundur dari versi `tcpdump` sebelumnya. Perintah `-w` digunakan untuk menulis hasil perintah `tcpdump` ke file dan menambahkan ekstensi.

`Tcpdump` tadi akan mencetak output ke file bernama `httdump.pcap`. file tersebut terletak pada file manager bagian analyst. Buka file tersebut menggunakan `Wireshark` dan cari `http`. Pilih `post` dan dapat dipilih bagian `HTML form URL Encode: application/x-www-form-urlencoded`. Jika dilihat dapat diketahui `uid`, `password`, dan `btnSubmit` pada `http` tersebut.

Untuk merekam paket `HTTPS` yaitu masukkan perintah `$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`. setelah itu, buka web `netacad` yang merupakan web dengan `https`. Untuk melihat rekaman paket `HTTPS` yang disimpan kedalam file bernama `httpsdump.pcap` yang terletak pada `/home/analyst/`. Cari `tcp.port==443` dan pilih `Application data`. Setelah section `TCP`, sekarang terdapat section `Secure Sockets Layer (SSL)`, bukan `HTTP`. Ketika menggunakan `HTTPS`, muatan data pesan akan dienkripsi dan hanya dapat dilihat oleh perangkat yang merupakan bagian dari percakapan terenkripsi.

F. Kesimpulan

Kesimpulan yang didapatkan dari praktikum kali ini yaitu:

1. `Nmap` (`Network Mapper`) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. `Nmap` berfungsi untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal.
2. `Wireshark` yang merupakan tool untuk menganalisis paket data jaringan yang melakukan pengawasan paket secara real time dan menangkap data yang akan ditampilkan selengkap mungkin.
3. `Tcpdump` akan mencetak output ke file bernama `httdump.pcap` dan `httpsdump.pcap`. file tersebut terletak pada file manager bagian analyst.
4. Perbedaan `HTTP/HTTPS` adalah pada keamanannya, di mana `HTTP` adalah protokol yang belum menggunakan `SSL/TLS`, dan `HTTPS` adalah versi yang lebih aman karena sudah menggunakan `SSL/TLS` untuk mengenkripsi koneksi antara web browser dan web server.

G. Daftar Pustaka

Andrian. (2014, November 26). File sharing FTP (vsftpd). TEKNIK INFORMATIKA. Retrieved February 26, 2023, from <http://andrian-tkj.blogspot.com/2014/11/file-sharing-ftp-vsftpd.html>

Apa ITU SSH, Pengertian, Fungsi Dan Cara Kerjanya: Biznet Gio. Apa itu SSH, Pengertian, Fungsi dan Cara Kerjanya | Biznet Gio. (2023). Retrieved February 26, 2023, from <https://www.biznetgio.com/en/news/apa-itu-ssh-pengertian-fungsi-dan-cara-kerjanya>

Ismail, J. (2019, September 23). Latihan 9 Keamanan Web – altoro. Latihan 9 Keamanan Web – Altoro. Retrieved February 26, 2023, from <https://julismail.staff.telkomuniversity.ac.id/latihan-9-keamanan-web-altoro/#:~:text=Altoro%20Mutual%20merupakan%20sebuah%20Bank,tentang%20ce lah%20keamanan%20di%20web.>

Panduan Refensi Nmap (Man Page, bahasa Indonesia). Panduan Refensi Nmap (man page, Bahasa Indonesia). (2023). Retrieved February 26, 2023, from [https://nmap.org/man/id/index.html#:~:text=Nmap%20\(%E2%80%9CNetwork%20M apper%E2%80%9D\),pula%20bekerja%20terhadap%20host%20tunggal.](https://nmap.org/man/id/index.html#:~:text=Nmap%20(%E2%80%9CNetwork%20M apper%E2%80%9D),pula%20bekerja%20terhadap%20host%20tunggal.)