

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

PERTEMUAN 2

Eksplorasi Nmap serta Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark



Nama : Muhammad Lutfi Zunnur

Program Studi : Teknologi Rekayasa Internet A

NIM : 21/477650/SV/19204

Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

PROGRAM SARJANA TERAPAN

TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

A. Tujuan

- Mengexplorasi Nmap
- Melakukan *Scan* ke *Port* yang terbuka
- Merekam dan menganalisis trafik HTTP
- Merekam dan menganalisis trafik HTTPS

B. Landasan Teori

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*.

Hyper Text 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.

C. Alat dan Bahan

Alat dan bahan yang dibutuhkan pada praktikum kali ini yaitu

- *CyberOps Workstation virtual machine*
- Koneksi *Internet*

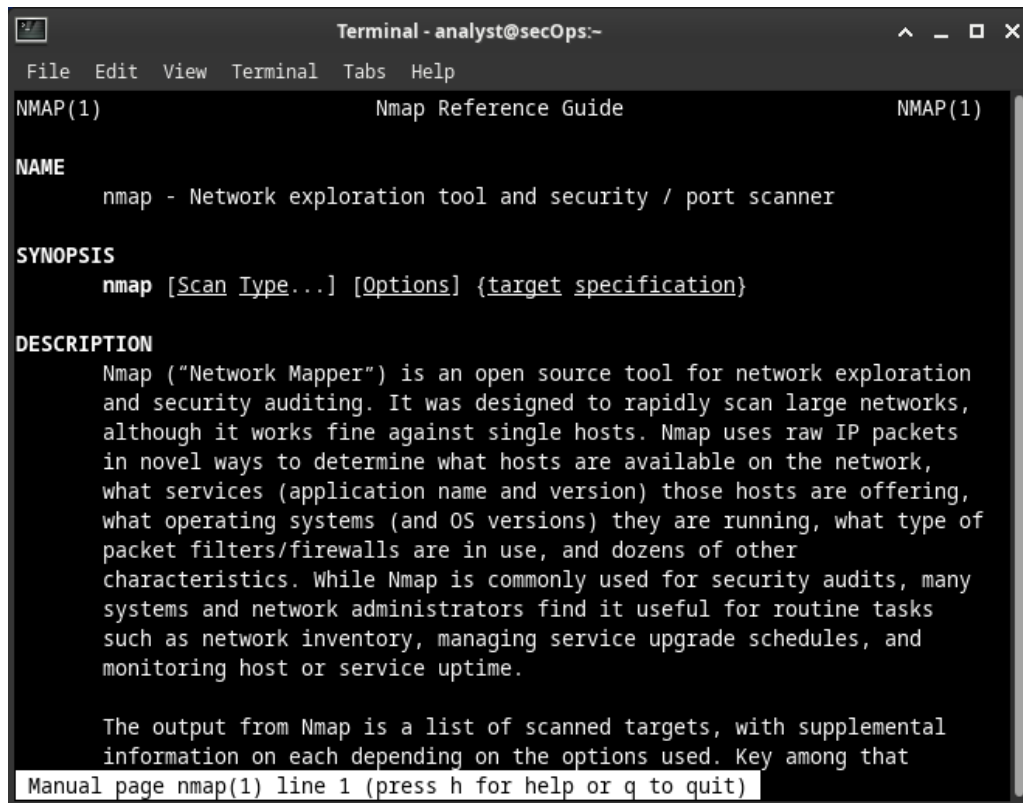
D. Instruksi Kerja

Eksplorasi Nmap

1. Eksplorasi Nmap

Start CyberOps Workstation, kemudian buka terminal kemudian ketikkan

```
[analyst@secOps ~]$ man nmap
```

A screenshot of a terminal window titled "Terminal - analyst@secOps:-". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The main content area displays the "Nmap Reference Guide" for "NMAP(1)". The guide is structured with sections: "NAME" (nmap - Network exploration tool and security / port scanner), "SYNOPSIS" (nmap [Scan Type...] [Options] {target specification}), and "DESCRIPTION". The description explains that Nmap is an open-source tool for network exploration and security auditing, designed to scan large networks but also works on single hosts. It details how Nmap uses raw IP packets to determine host availability, services, operating systems, and packet filters. It also mentions its common use for security audits and its utility for network administrators for tasks like inventory, service upgrade scheduling, and host uptime monitoring. At the bottom, it states that the output is a list of scanned targets with supplemental information. A status bar at the very bottom reads "Manual page nmap(1) line 1 (press h for help or q to quit)".

```
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

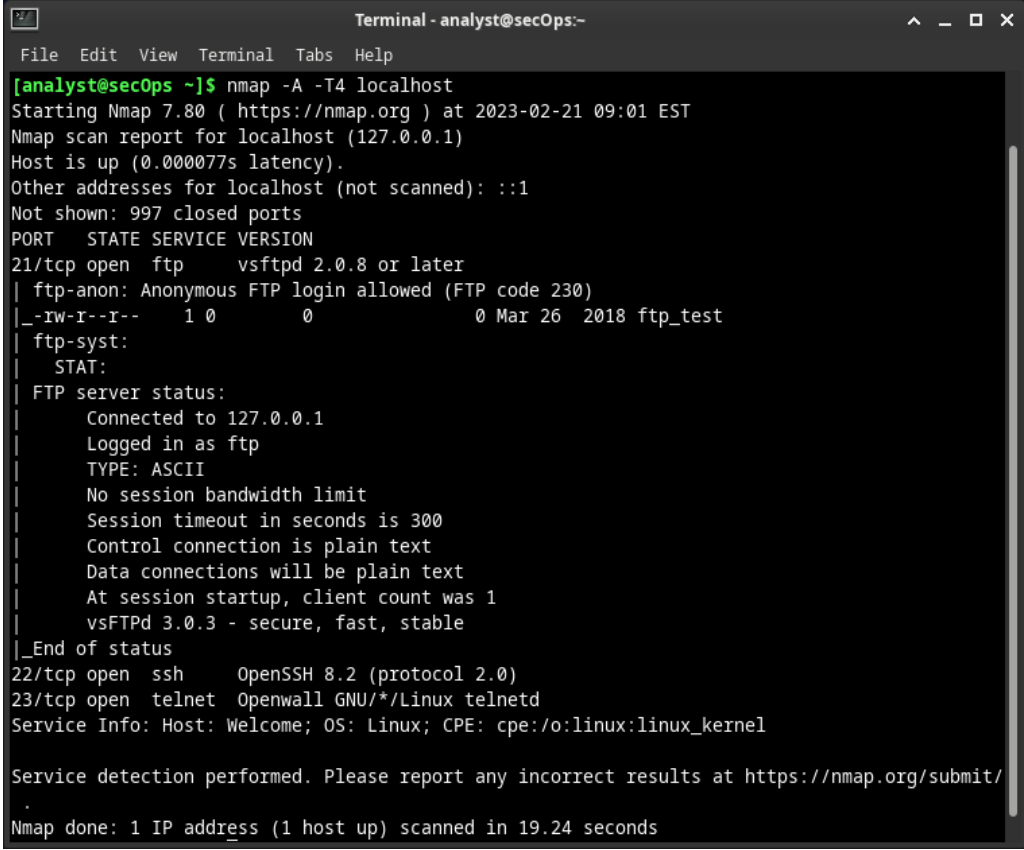
Manual page nmap(1) line 1 (press h for help or q to quit)
```

- Nmap ("Network Mapper") merupakan sebuah *tool open source* untuk eksplorasi dan *audit* keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap *host* tunggal. 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.
- Fungsi Nmap yaitu digunakan untuk memeriksa jaringan, Nmap bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Meskipun begitu, Nmap juga mampu bekerja pada *host* tunggal. Cara kerjanya adalah dengan menggunakan IP *raw* yang berfungsi untuk menentukan mana *host* yang tersedia di dalam jaringan. Selain itu, Nmap juga bisa melakukan *scanning* pada *port* jaringan, *Port* adalah nomor yang berguna untuk membedakan antara

aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer. Dengan menggunakan Nmap, maka seseorang bisa melakukan scanning terhadap *port-port* tersebut. Maka seseorang bisa mengetahui aplikasi mana saja yang terpasang pada suatu perangkat.

2. Localhost Scanning

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



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-21 09:01 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000077s 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

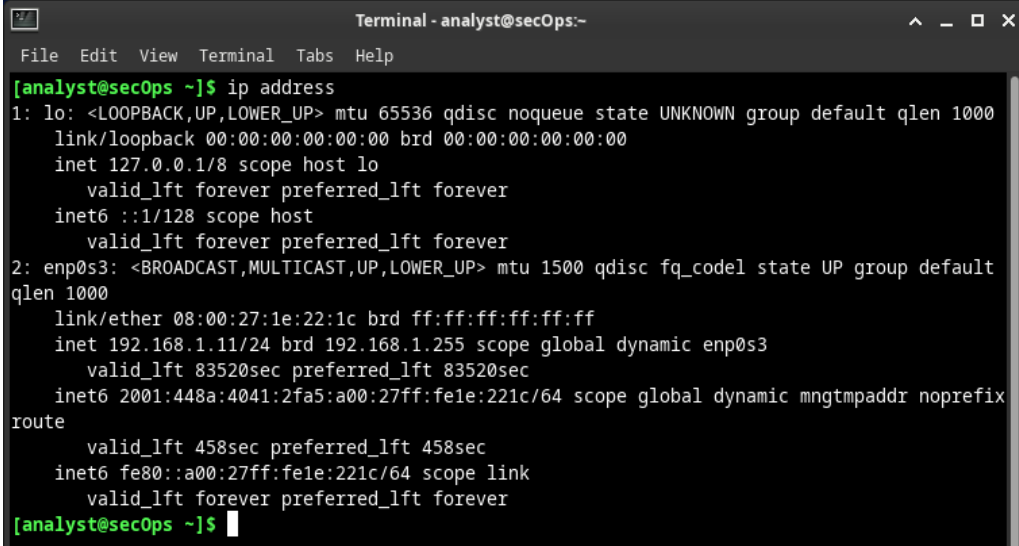
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 19.24 seconds
```

- *Command* tersebut digunakan untuk melakukan *scanning* pada *local host* sehingga bisa mengetahui *port* mana saja yang terbuka. Pada hasil tersebut didapatkan bahwa *port* yang terbuka yaitu *port* 21/tcp dengan layanan ftp dan *software* yang digunakan vsftpd 2.0.8, port 22/tcp dengan layanan ssh dan *software* yang digunakan OpenSSH 8.2, serta port 23/tcp dengan layanan *telnet* dan *software* yang digunakan 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  
[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 08:00:27:1e:22:1c brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic enp0s3  
        valid_lft 83520sec preferred_lft 83520sec  
    inet6 2001:448a:4041:2fa5:a00:27ff:fe1e:221c/64 scope global dynamic mngtmpaddr noprefix route  
        valid_lft 458sec preferred_lft 458sec  
    inet6 fe80::a00:27ff:fe1e:221c/64 scope link  
        valid_lft forever preferred_lft forever  
[analyst@secOps ~]$
```

- *Command* tersebut untuk mengetahui IP Address pada *local host*. IP dari PC *host* tersebut yaitu 192.168.1.11/24.

Kemudian melakukan *port scanning*.

[analyst@secOps ~]\$ **nmap -A -T4 192.168.1.0/24**

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
|_ start_date: N/A

Nmap scan report for 192.168.1.11
Host is up (0.00034s 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 192.168.1.11
|     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 (10 hosts up) scanned in 209.28 seconds
[analyst@secOps ~]$
```

- Host yang terdeteksi yaitu ada 10 IP Address yang aktif dari 256 IP Address.

Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark

1. Jalankan VM dan *Login*

Username : analyst

Password : cybercops

2. Buka terminal dan menjalankan **tcpdump**

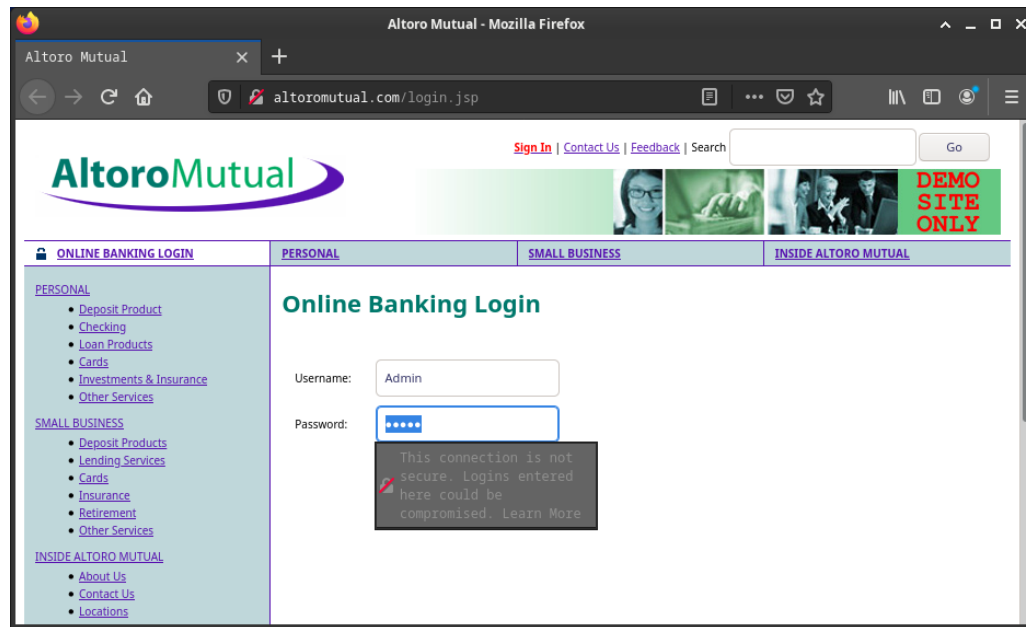
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

```
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 bytes
|
```

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

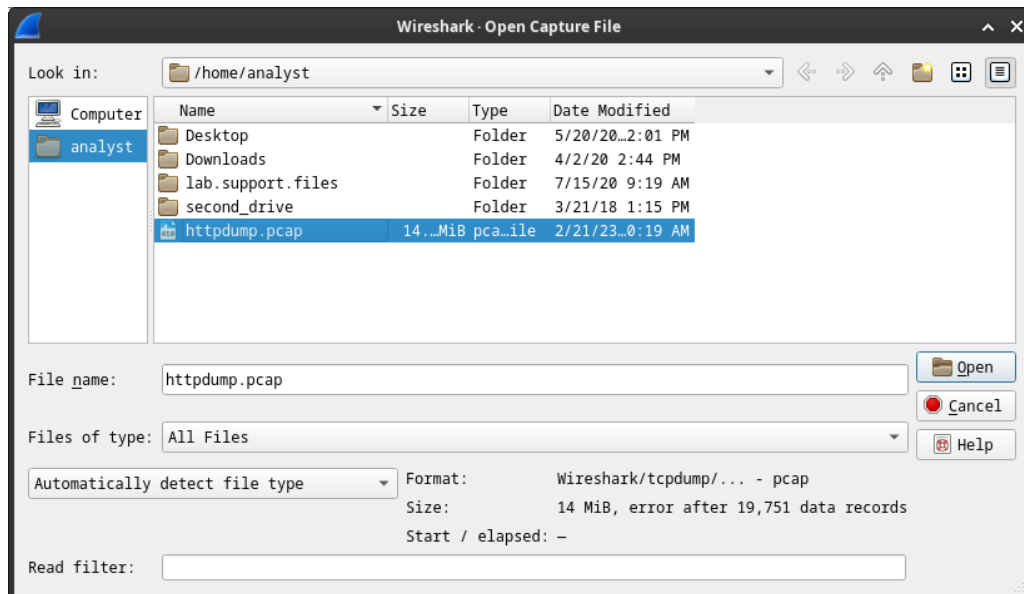
Username : **Admin**

Password : **Admin**

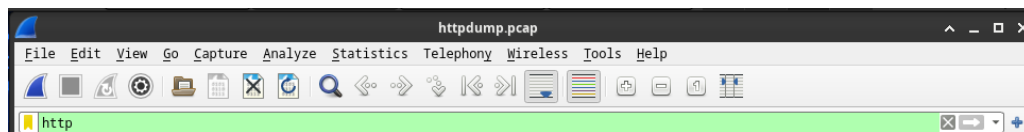


4. Merekam Paket HTTP

Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam *file* bernama *httpdump.pcap*. *File* ini terletak pada *folder /home/analyst/*. Untuk melihatnya kita bisa menggunakan *wireshark* kemudian meng-*export file httpdump.pcap*.



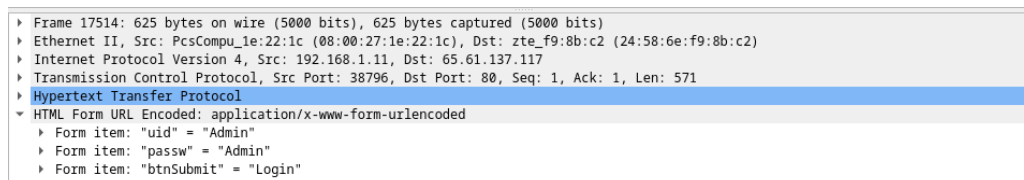
5. Filter *http* kemudian klik *Apply*



6. Pilih *POST*

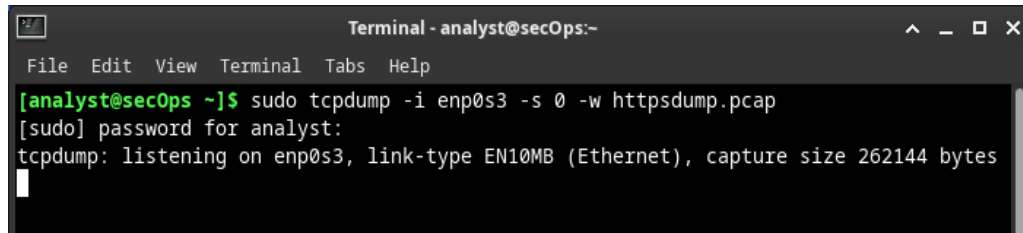
No.	Time	Source	Destination	Protocol	Length	Info
17319	901.390229	2600:1901:0:38d7::	2001:448a:4041:2fa5...	HTTP	302	HTTP/1.1 200 OK (text/plain)
17426	912.022365	192.168.1.11	34.107.221.82	HTTP	347	GET /success.txt?ipv4 HTTP/1.1
17487	918.637441	192.168.1.11	34.107.221.82	HTTP	347	GET /success.txt?ipv4 HTTP/1.1
17514	921.425302	192.168.1.11	65.61.137.117	HTTP	625	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
17517	921.700028	65.61.137.117	192.168.1.11	HTTP	298	HTTP/1.1 302 Found
17519	921.708084	192.168.1.11	65.61.137.117	HTTP	592	GET /bank/main.jsp HTTP/1.1
17527	921.976587	65.61.137.117	192.168.1.11	HTTP	1434	[TCP Previous segment not captured] Continuation
17530	921.976709	65.61.137.117	192.168.1.11	HTTP	946	[TCP Previous segment not captured] Continuation
17540	922.762574	65.61.137.117	192.168.1.11	HTTP	1434	[TCP Spurious Retransmission] Continuation
17596	929.312291	192.168.1.11	34.107.221.82	HTTP	347	GET /success.txt?ipv4 HTTP/1.1

7. Pada *HTML Form URL Encoded* terdapat data uid dan passw yang telah kita tuliskan pada *browser* tadi.



8. Merekam Paket HTTPS

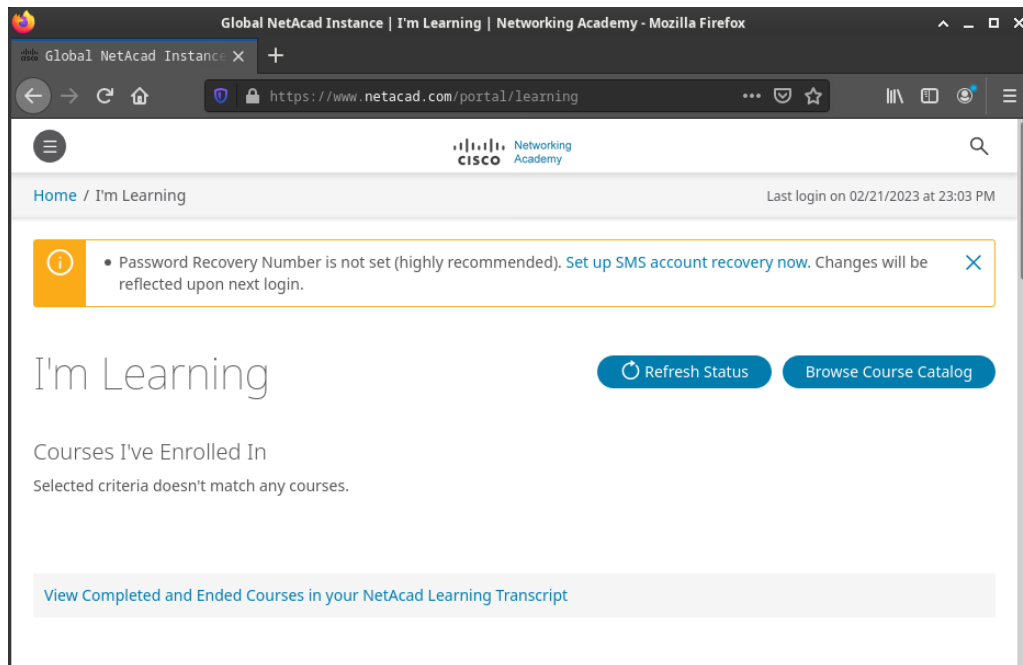
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
```

A terminal window titled "Terminal - analyst@secOps:-" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The command `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap` has been entered. The prompt shows the user is root. The output indicates that tcpdump is listening on enp0s3 with a capture size of 262144 bytes.

```
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
```

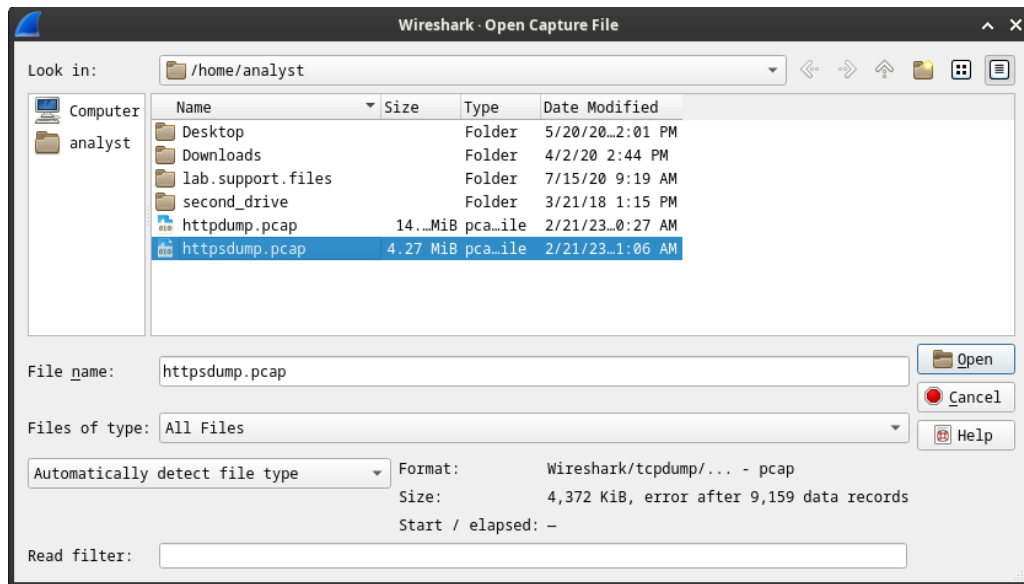
9. Buka *link* <https://www.netacad.com/> melalui *browser* di *CyberOps Workstation* VM.

Klik *login*

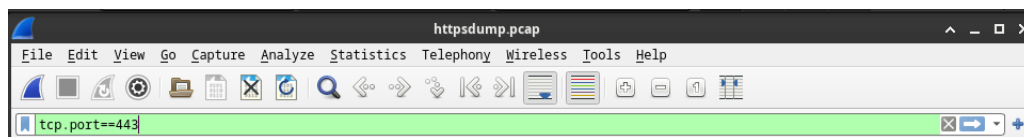


10. Melihat Rekaman Paket HTTPS

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



11. Filter tcp.port==443



12. Pilih Application Data

No.	Time	Source	Destination	Protocol	Length	Info
1861	21.090323	2a03:2880:f00c:10d:...	2001:448a:4041:2fa5...	TCP	2846	443 → 46234 [PSH, ACK] Seq=57360 Ack=1083 Win=...
1862	21.090363	2001:448a:4041:2fa5...	2a03:2880:f00c:10d:...	TCP	86	46234 → 443 [ACK] Seq=1083 Ack=60120 Win=120320
1863	21.091791	2a03:2880:f00c:10d:...	2001:448a:4041:2fa5...	TCP	1466	[TCP Previous segment not captured] 443 → 46234
1864	21.091791	2a03:2880:f00c:10d:...	2001:448a:4041:2fa5...	TCP	1466	[TCP Out-Of-Order] 443 → 46234 [ACK] Seq=60120
1865	21.091841	2001:448a:4041:2fa5...	2a03:2880:f00c:10d:...	TCP	98	[TCP Window Update] 46234 → 443 [ACK] Seq=1083
1866	21.091924	2001:448a:4041:2fa5...	2a03:2880:f00c:10d:...	TCP	86	46234 → 443 [ACK] Seq=1083 Ack=62880 Win=120320
1867	21.093019	2a03:2880:f00c:10d:...	2001:448a:4041:2fa5...	TLSv1.2	2846	Application Data [TCP segment of a reassembled
1868	21.093066	2001:448a:4041:2fa5...	2a03:2880:f00c:10d:...	TCP	86	46234 → 443 [ACK] Seq=1083 Ack=65640 Win=120320
1869	21.094431	2a03:2880:f00c:10d:...	2001:448a:4041:2fa5...	TLSv1.2	1466	[TCP Previous segment not captured] , Ignored
1870	21.094432	2a03:2880:f00c:10d:...	2001:448a:4041:2fa5...	TCP	1466	[TCP Out-Of-Order] 443 → 46234 [ACK] Seq=65640

13. Hasil yang didapatkan

- Frame 1867: 2846 bytes on wire (22768 bits), 2846 bytes captured (22768 bits)
- Ethernet II, Src: zte_f9:8b:c2 (24:58:6e:f9:8b:c2), Dst: PcsCompu_1e:22:1c (08:00:27:1e:22:1c)
 - Destination: PcsCompu_1e:22:1c (08:00:27:1e:22:1c)
 - Source: zte_f9:8b:c2 (24:58:6e:f9:8b:c2)
 - Type: IPv6 (0x86dd)
- Internet Protocol Version 6, Src: 2a03:2880:f00c:10d:face:b00c:0:3, Dst: 2001:448a:4041:2fa5:a00:27ff:fe1e:221c
- Transmission Control Protocol, Src Port: 443, Dst Port: 46234, Seq: 62880, Ack: 1083, Len: 2760
- [9 Reassembled TCP Segments (14915 bytes): #1851(1529), #1853(1380), #1855(1380), #1858(1380), #1857(1380), #1861(2760), #1864(1380)]
- Transport Layer Security
 - TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

E. Pembahasan

Pada praktikum ini yaitu melakukan eksplorasi Nmap. Terdapat beberapa *command* yang digunakan, contohnya yaitu **man nmap**, *command* tersebut digunakan untuk menampilkan sebuah modul, modul tersebut menunjukkan perintah-perintah yang akan digunakan. Selain itu juga terdapat perintah **nmap -A -T4 localhost** yang bisa digunakan untuk melihat apa saja *port* dan layanan yang terbuka. Kita juga bisa melihat IP Address menggunakan *command* **ip address**. Setelah mengetahui IP Address-nya, selanjutnya melakukan *scanning* menggunakan nmap dengan mengetikkan *command* **nmap -A -T4 192.168.1.0/24**. Angka tersebut merupakan *network* pada IP Address *host*. Dengan mengetikkan *command* tersebut kita juga bisa melihat *host* yang terdeteksi.

Selain itu, pada praktikum ini yaitu melakukan pemantauan trafik HTTP dan HTTPS dengan menggunakan *wireshark*. Ada beberapa *command* yang akan dicoba, contohnya **tcpdump**, Tcpdump adalah alat (*tool*) yang digunakan untuk menganalisa jaringan komputer. Selanjutnya mencoba membuka *link* <http://www.altoromutual.com/login.jsp> melalui *browser* di CyberOps. Tcpdump yang dieksekusi kemudian disimpan kedalam file bernama **httpdump.pcap**. Untuk melihat file tersebut bisa dengan cara meng-*export*-nya menggunakan *wireshark*, Ketika menggunakan *wireshark* kita bisa melihat beberapa penjelasan yang ada pada file tersebut. Pada bagian HTML Form URL Encoded terdapat data uid dan passw yang diketikkan di browser tadi. Selain merekam paket HTTP, bisa juga merekam paket HTTPS, kita hanya perlu mengganti *command*-nya menjadi **httpsdump.pcap**. Pada paket HTTPS, ketika di-*export* ke *wireshark* kita bisa mendapat informasi mengenai *internet protocol*, *transport layer security*, dll.

F. Kesimpulan

Kesimpulan yang didapatkan pada praktikum ini yaitu:

1. Kita dapat menjalankan aplikasi berbasis perangkat lunak didalam sistem operasi komputer lain tanpa harus menambah perangkat fisik menggunakan *virtual machine*.
2. Nmap merupakan salah satu aplikasi *open source* yang digunakan untuk melakukan *scanning* pada jaringan komputer.
3. Kita bisa melakukan pemantauan trafik HTTP dan HTTPS menggunakan *Wireshark*.

Daftar Pustaka

ZAKARIA, MUCHAMMAD. *Pengertian NMAP Beserta Fungsi dan Cara Kerjanya yang Perlu Diketahui*. Diakses pada 21 Februari 2023.
<https://www.nesabamedia.com/pengertian-nmap/>