

**LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1**  
**Unit 2 & 3 – Eksplorasi NMAP dan Pemantauan Trafik HTTP &**  
**HTTPS Menggunakan Wireshark**



**DI SUSUN OLEH**

Nama : M Abdul Aziz  
NIM : 21/474516/SV/18951  
Hari, Tanggal : Selasa, 21 Februari 2023  
Kelas : RI4AA

**LABORATORIUM PERANGKAT KERAS DAN LUNAK**  
**PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI**  
**REKAYASA INTERNET**  
**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**  
**SEKOLAH VOKASI**  
**UNIVERSITAS GADJAH MADA**  
**2023**

## **Praktikum Keamanan Informasi 1**

### **Unit 2 & 3 – Eksplorasi NMAP, HTTP, HTTPS**

#### **I. Tujuan**

- Mengeksplorasi Nmap
- Melakukan Scan ke Port yang terbuka
- Merekam dan menganalisis trafik HTTP & HTTPS

#### **II. Latar Belakang**

Dalam keamanan jaringan, seorang hacker sebelum melakukan penyerangan akan melakukan beberapa tahapan terlebih dahulu. Tahapan pertama yang dilakukan oleh seorang hacker adalah *reconnaissance*. *Reconnaissance* adalah tahap kegiatan dimana penyerang mengumpulkan informasi sebanyak mungkin mengenai target. Informasi yang diperoleh dari hasil kegiatan ini berupa informasi dasar yang berguna, seperti IP Address, topology network, network resources dan informasi personal tentang user yang diperlukan untuk tahap selanjutnya. Kemudian *Footprinting* merupakan kegiatan mengumpulkan informasi target yang akan di-hack sistemnya, sebelum melakukan penguasaan sistem sesungguhnya. Biasanya, *Footprinting & Reconnaissance* dilakukan menjadi satu tahap yang sama.

*Network Scanning* merupakan tahapan setelah proses pengumpulan informasi pada tahapan *FootPrinting & Reconnaissance*. *Port scanning* merupakan salah satu hal yang sering digunakan dalam *Network Scanning*, yang biasanya merupakan bagian dari serangan pengintaian. Ada berbagai metode *Port scanning* yang dapat digunakan. Nmap adalah salah satu *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 kita 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 selain mempelajari cara kerja NMAP, kita juga akan akan menjelajahi dan menangkap lalu lintas HTTP dan HTTPS menggunakan Wireshark.

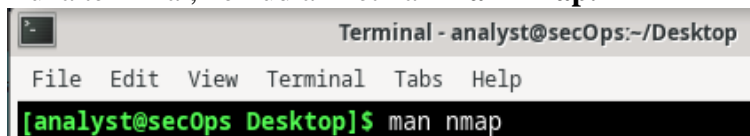
### III. Alat & Bahan

- CyberOps Workstation VM
- Wireshark
- Internet Access

### IV. Instruksi Kerja

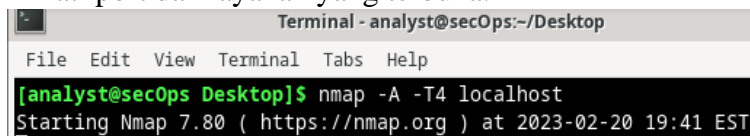
#### UNIT 2

1. Jalankan CyberOps Workstation VM
2. Buka terminal, kemudian ketikkan **man nmap**.



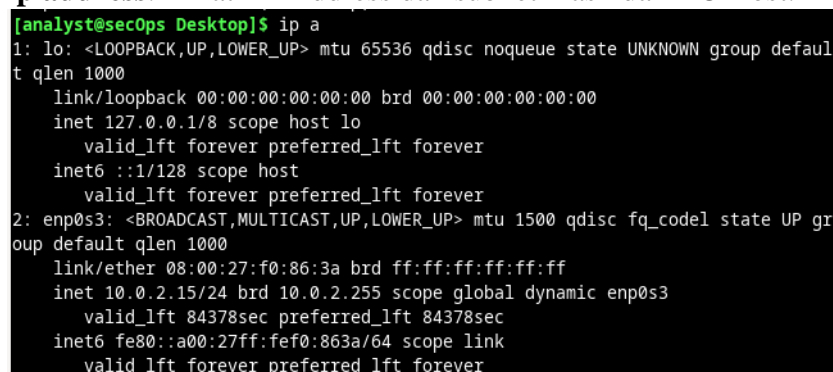
```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ man nmap
```

3. Lakukan *localhost scanning* dengan mengetikkan **nmap -A -T4 localhost**. Amati port dan layanan yang terbuka.



```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:41 EST
```

4. Lakukan *network scanning* dengan menggunakan IP Address. Sebelumnya, lakukan pengecekan IP Address PC Host terlebih dahulu dengan mengetikkan **ip address**. Amati IP Address dan subnet mask dari PC Host.



```
[analyst@secOps Desktop]$ ip a
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:f0:86:3a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 84378sec preferred_lft 84378sec
    inet6 fe80::a00:27ff:fe0:863a/64 scope link
        valid_lft forever preferred_lft forever
```

Kemudian lakukan *network scanning* dengan mengetikkan **nmap -A -T4 [ip address]**. Amati jumlah host yang terdeteksi.

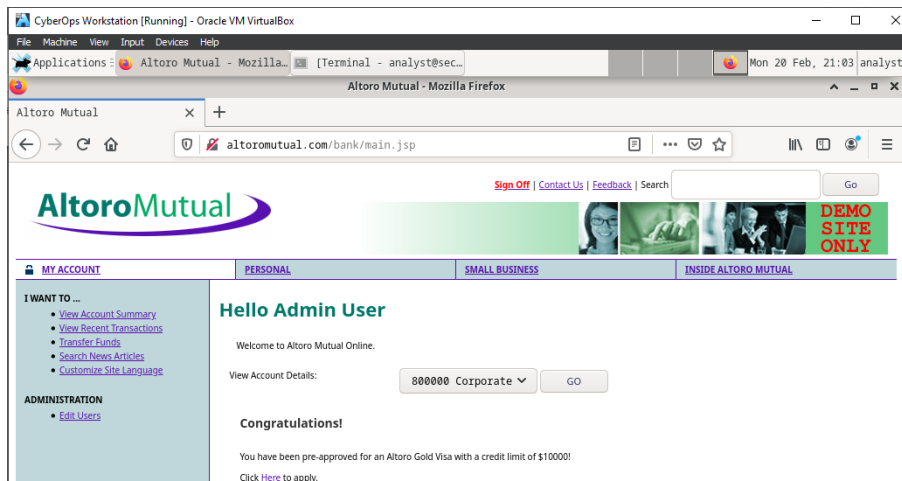
```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:16 EST
```

### UNIT 3

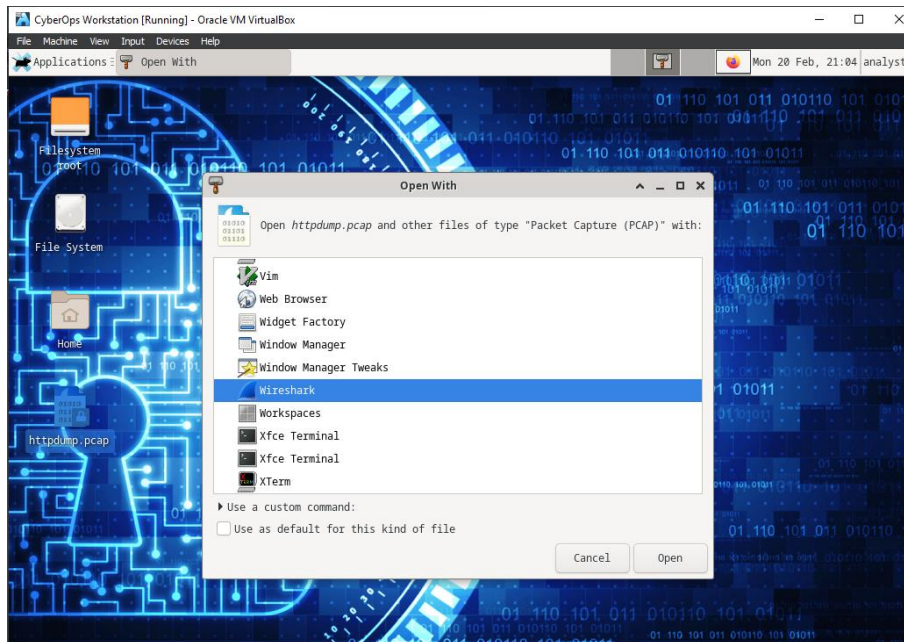
5. Buka terminal dan jalankan TCP Dump

```
CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications: [Terminal - analyst@sec0...]
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ ip a
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:f0:86:3a brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86228sec preferred_lft 86228sec
   inet6 fe80::a00:27ff:fef0:863a/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps Desktop]$ 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
```

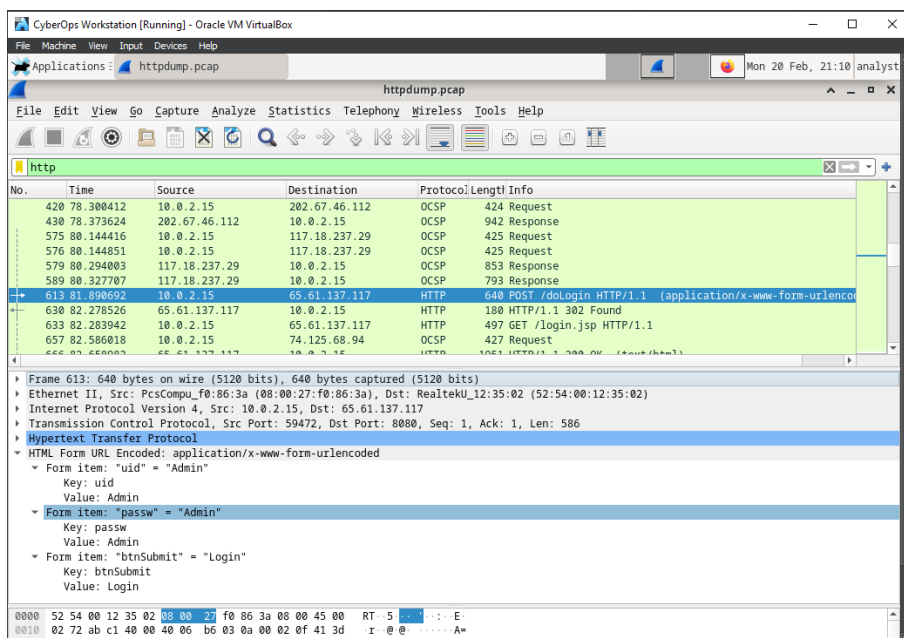
6. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM. Login dengan user & password **Admin**



## 7. Buka file **httpdump.pcap** menggunakan Wireshark

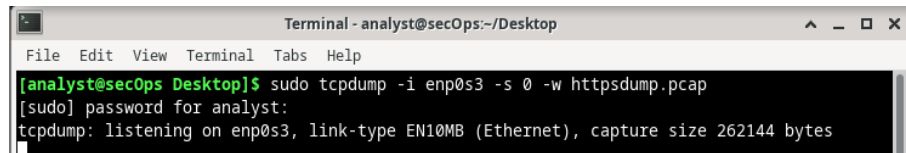


Pilih **POST**, lalu klik pada **HTML Form Url Encoded....** untuk mengetahui **uid** dan **password**



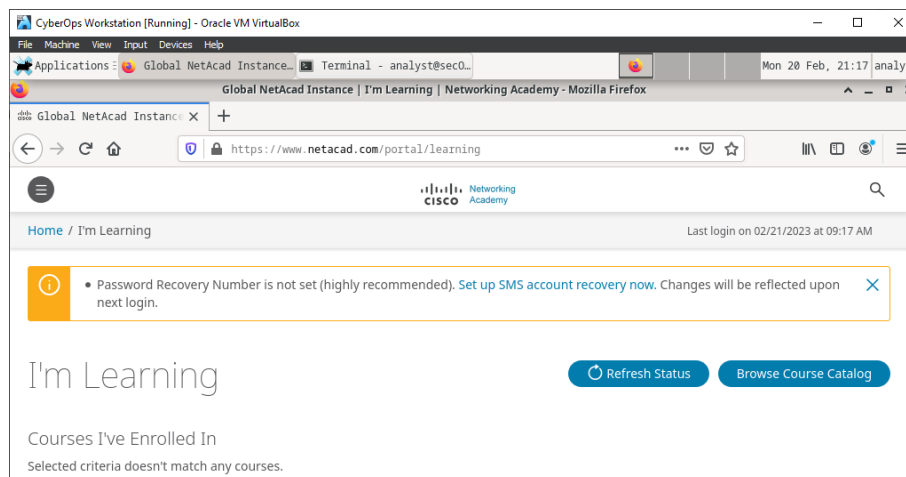
## 8. Kemudian hentikan proses perekaman *traffic* http dengan menggunakan kombinasi tombol **ctrl+c**

9. Lalu buka kembali terminal dan jalankan TCP Dump untuk merekam traffic https dengan mengetikkan perintah **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**

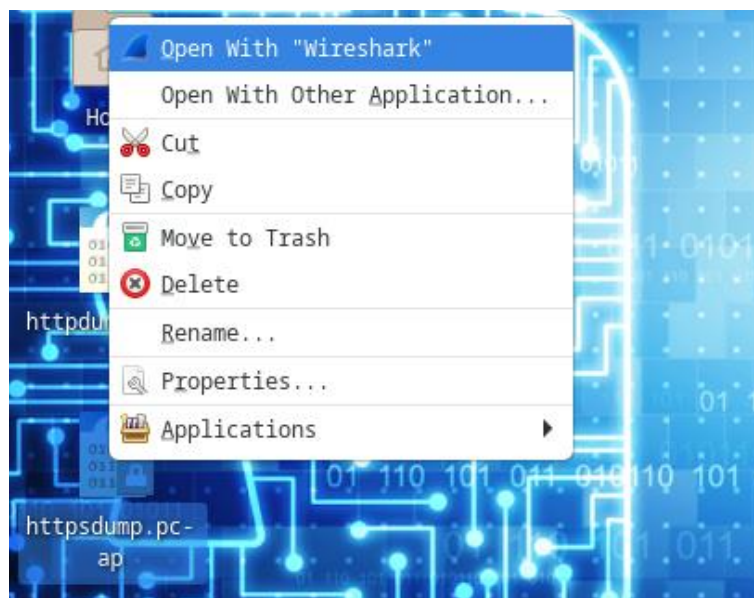


```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

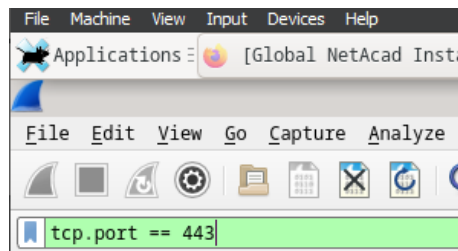
10. Selanjutnya buka web <https://netacad.com> dan login menggunakan akun netacad yang dimiliki.



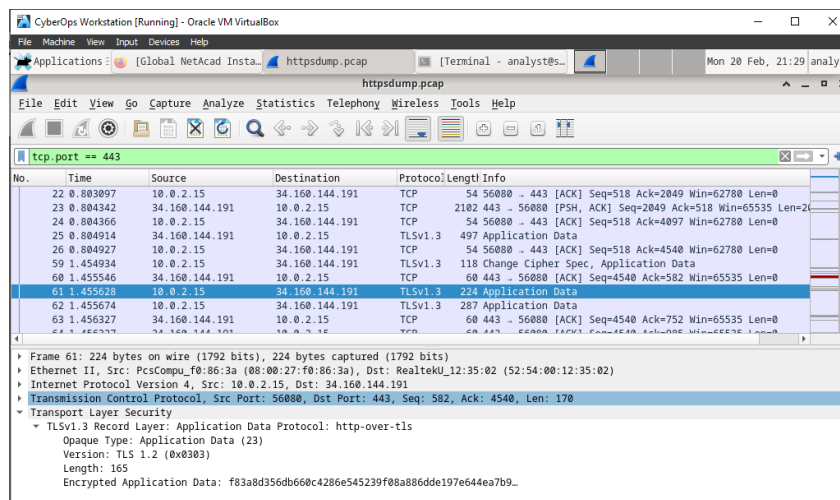
11. Buka file **httpsdump.pcap** menggunakan wireshark



Berikan filter **tcp.port == 443**



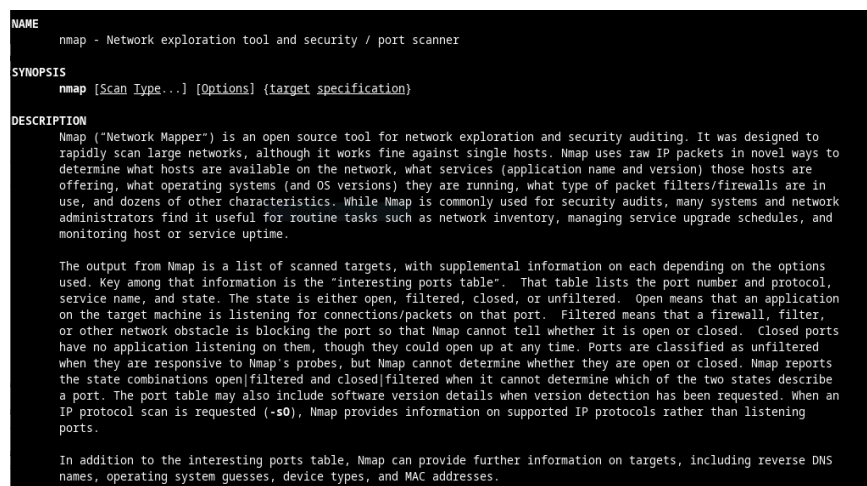
Pilih Application Data, lalu expand pada *Transport Layer Security*



## V. Pembahasan

Pada praktikum kali ini, mahasiswa akan melakukan pengujian *tools scanning network* menggunakan NMAP (*Network Mapping*) serta melakukan perekaman trafik HTTP & HTTPS menggunakan *software* Wireshark.

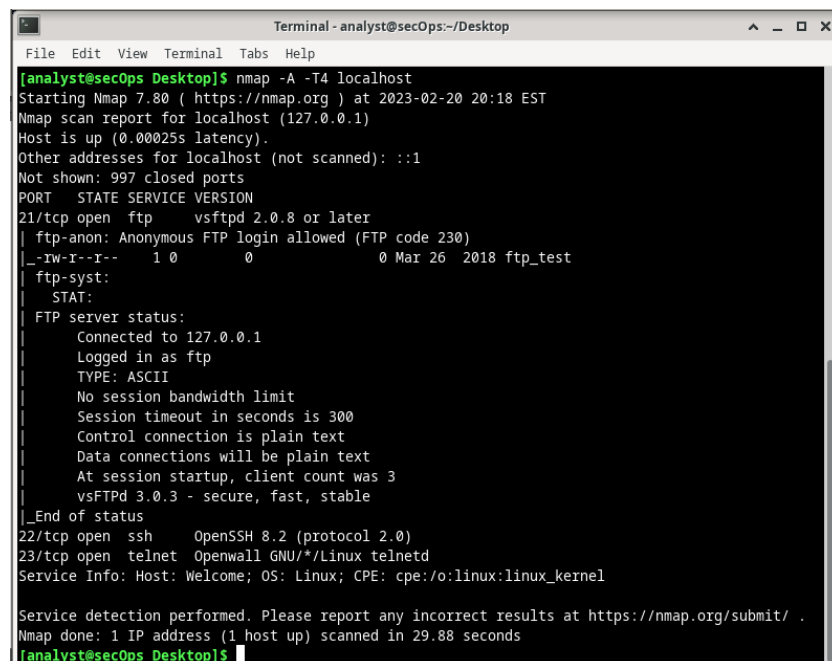
### [UNIT 2]





Syntax pertama yang digunakan adalah **man nmap**, yang digunakan untuk menampilkan semua detail opsi yang tersedia untuk NMAP. NMAP Sendiri adalah NMAP adalah singkatan dari *Network Mapper* yang merupakan sebuah tool atau alat yang bersifat *open source*. Alat ini hanya digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan.

Fungsi dari NMAP yaitu digunakan sebagai alat untuk melakukan pengecekan pada jaringan. NMAP mampu melakukan pengecekan terhadap suatu jaringan besar dalam waktu yang singkat. Kemudian fungsi lain dari NMAP adalah untuk melakukan *scanning* terhadap suatu port pada jaringan komputer.



```
analyst@secOps Desktop$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:18 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 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 29.88 seconds
analyst@secOps Desktop$
```

Kemudian syntax kedua yang digunakan adalah **nmap -A -T4 localhost**, yang berfungsi untuk *scanning* port pada jaringan *localhost*. -A pada syntax tersebut digunakan untuk mengaktifkan pendeteksi OS dan Versi OS yang digunakan, *script scanning*, dan *traceroute*. Kemudian -T4 digunakan untuk *faster execution*.

Dari hasil *localhost scanning* tersebut didapatkan Port dan layanan yang terbuka adalah port 22 yang melayani SSH dan port 23 yang melayani telnet. *Software* yang dapat digunakan untuk mengakses layanan SSH yaitu MobaXterm, Putty, mRemoteNG, WinSCP, Terminals, dan SmarTY. Sedangkan *Software* yang



dapat digunakan untuk mengakses layanan Telnet adalah Putty, Xshell, MobaXterm, mRemoteNG, Radmin, dan ExtraPutty.

```
[analyst@secOps Desktop]$ ip a
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:f0:86:3a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 84378sec preferred_lft 84378sec
    inet6 fe80::a00:27ff:fe0:863a/64 scope link
        valid_lft forever preferred_lft forever
```

Sebelum melakukan *scanning network*, kita perlu melakukan pengecekan IP Address terlebih dahulu dengan mengetikkan perintah **ip address**. Dapat dilihat bahwa IP Address yang digunakan adalah 10.0.2.0/24.

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

[analyst@secOps Desktop]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:16 EST
Nmap scan report for 10.0.2.15
Host is up (0.00018s 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 45.46 seconds
[analyst@secOps Desktop]$
```

Syntax ketiga yang digunakan adalah **nmap -A -T4 [ip address]**, yang berfungsi untuk *scanning port* pada jaringan yang digunakan. -A pada syntax tersebut digunakan untuk mengaktifkan pendeteksi OS dan Versi OS yang digunakan, *script scanning*, dan *traceroute*. Kemudian -T4 digunakan untuk *faster execution*.

Dari hasil *scanning network* yang telah dilakukan, terdapat 1 host aktif yang terdeteksi pada jaringan tersebut, yaitu 10.0.2.15/24 yang merupakan IP dari device sendiri.

### [UNIT 3]

Untuk merekam *traffic* jaringan yang dapat diakses menggunakan Wireshark, syntax yang digunakan untuk menjalankan perekaman *traffic* adalah **sudo tcpdump -i enp0s3 -s 0 -w [nama\_file].pcap**. Setelah dijalankan, kita perlu mengakses suatu web yang menggunakan protokol HTTP. Kemudian dari file perekaman *traffic http*, kita perlu melakukan *filtering traffic* 'http' pada Wireshark. Kita juga perlu mencari *traffic* yang mengandung POST. Dari hasil tersebut karena pada saat mengakses web dengan protokol HTTP kita memasukkan user-id dan password, maka pada *traffic* POST tersebut kita dapat menemukan atau menampilkan UID dan Password yang telah digunakan pada saat mengakses web dengan protokol HTTP. Hal tersebut dikarenakan protokol HTTP tidak memiliki enkripsi dari data yang kita gunakan untuk mengakses suatu situs.

Setelah itu, jalankan Kembali syntax untuk menjalankan perekaman *traffic* dengan nama file yang berbeda. Kemudian akses situs dengan protokol HTTPS. Dari file perekaman *traffic https*, kita perlu melakukan *filtering traffic* 'tcp.port == 443' pada Wireshark, karena port HTTPS adalah 443. Kemudian cari *traffic* yang mengandung Application Data. Dari hasil perekaman tersebut, karena situs yang diakses menggunakan protokol HTTPS, maka user-id dan password akan terenkripsi. Hal ini dikarenakan pada protokol HTTPS menggunakan SSL/TLS untuk mengenkripsi koneksi antara web browser dengan web server.

## VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

1. NMAP merupakan salah satu *tools* yang digunakan untuk *Scanning Network*
2. NMAP dapat digunakan untuk mendapatkan informasi OS, Versi OS, jumlah host, serta port dan layanan yang terbuka dalam suatu jaringan
3. HTTP dan HTTPS merupakan suatu protokol jaringan yang berada pada lapisan aplikasi.
4. HTTPS merupakan versi lebih *secure* dari HTTP karena telah menggunakan SSL/TLS sebagai enkripsi.

## VII. Daftar Pustaka

- Wahyudi, D. (2014). Reconnaissance. Retrieved February 19, 2023, from [http://edocs.ilkom.unsri.ac.id/831/1/Dimas%20Wahyudi\\_0901128132000\\_4\\_KJK\\_Tugas\\_1.pdf](http://edocs.ilkom.unsri.ac.id/831/1/Dimas%20Wahyudi_0901128132000_4_KJK_Tugas_1.pdf)
- Batakuri. (August 23, 2016). FOOTPRINTING DAN RECONNAISSANCE (KEAMANAN JARINGAN). Retrieved February 19, 2023, from <https://batakuri.wordpress.com/2016/08/23/combinasi-materi-kelompok-xii-tkj-1/>
- Risyan, R. (July 2, 2020). 50 Perintah NMAP Pada Linux Dan Windows. Retrieved February 19, 2023, from <https://www.monitorteknologi.com/perintah-nmap-linux-dan-windows/#penci-Perintah-Perintah-NMAP>
- Zakaria, M. (April 10, 2022). Pengertian NMAP Beserta Fungsi dan Cara Kerjanya yang Perlu Diketahui. Retrieved February 19, 2023, from <https://www.nesabamedia.com/pengertian-nmap/>