LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

UNIT 2 dan 3

Eksplorasi Nmap

Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark

Disusun Oleh :

Nama	:	Abu Alif Raharjo
NIM	:	21/479770/SV/19537
Hari, tanggal	:	Selasa, 14 Februari 2023
Dosen Pengampu	:	Anni Karimatul Fauziyyah, S. Kom., M. Eng.

PROGRAM STUDI DIPLOMA IV TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

A. Tujuan

- Mengesplorasi Nmap
- Melakukan Scan ke Port yang terbuka
- Merekam dan menganalisis trafik http
- 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 Protoco*l (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

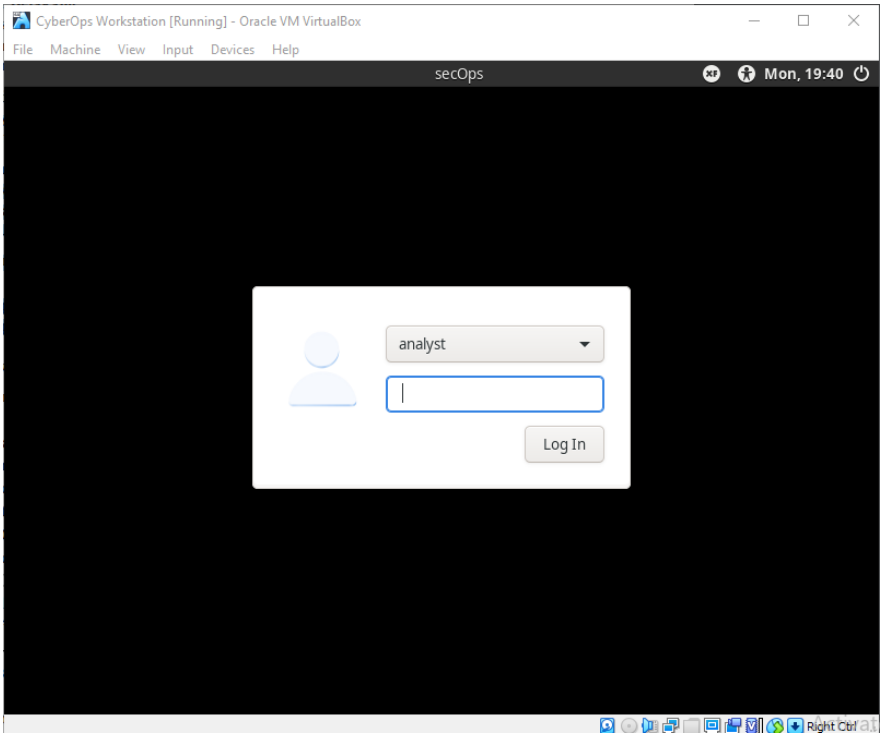
C. Alat dan Bahan

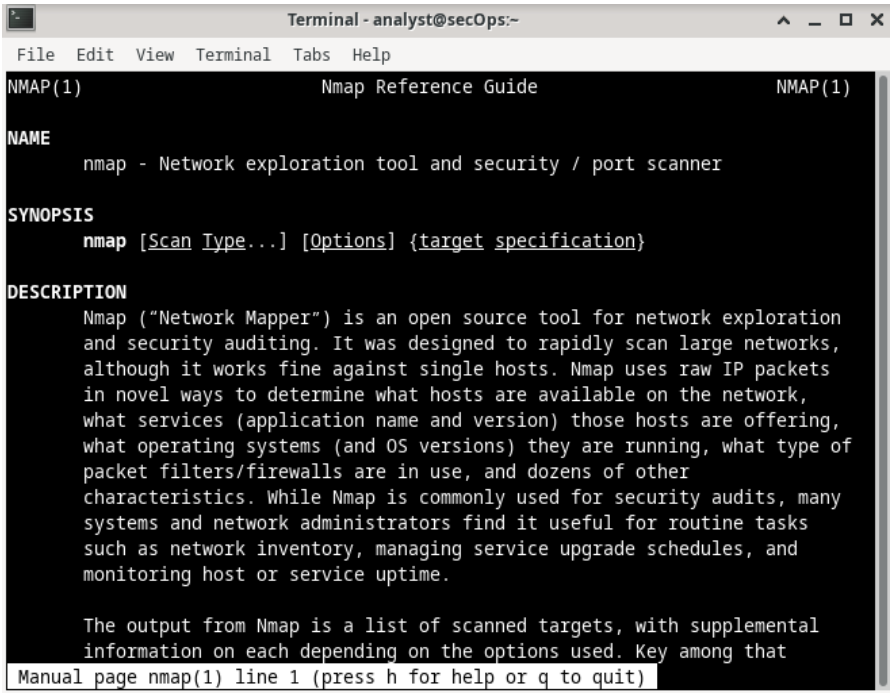
- CyberOps Workstation virtual machine
- Internet access

D. Instruksi kerja

Unit 2

1. Eksplorasi Nmap
   Start CyberOps Workstation
   Buka terminal kemudian ketikkan
   [analyst@secOps ~]$ man nmap
   Apa itu Nmap?
   Apa fungsi dari Nmap?





2. Localhost Scanning
   [analyst@secOps ~]$ **nmap -A -T4 localhost**
   Starting Nmap 7.40 (https://nmap.org) at 2017-05-01 17:20 EDT
   Nmap scan report for localhost (127.0.0.1)
   Host is up (0.000056s latency).

Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 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 Apr 19 15:23 ftp_test
<some output omitted>
Port dan layanan apa yang terbuka?
Software apa yang digunakan pada port yang terbuka tersebut?

```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:46 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00026s 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 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: 1 IP address (1 host up) scanned in 30.35 seconds
```

3. *Network Scanning*

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

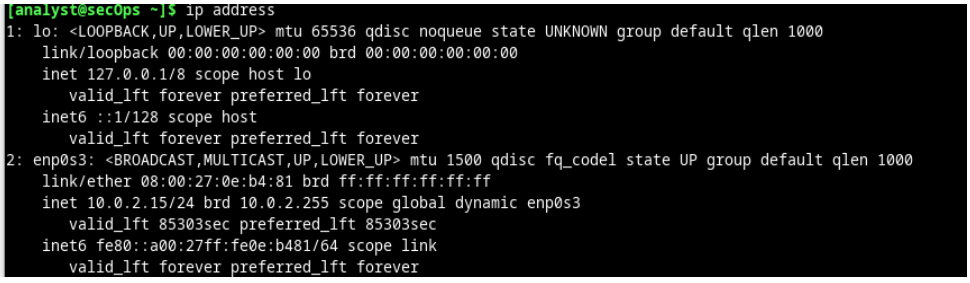
[analyst@secOps ~]$ **ip address**
<output omitted>
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255
scope global dynamic enp0s3
valid_lft 85777sec preferred_lft 85777sec
inet6 fe80::a00:27ff:feed:af2c/64 scope link
valid_lft forever preferred_lft forever

Berapakah alamat IP dan subnet mask dari PC host?
Lakukanlah port scanning dengan menggunakan Nmap
[analyst@secOps ~]$ **nmap -A -T4 10.0.2.0/24**
Starting Nmap 7.40 (https://nmap.org) at 2017-05-01 17:13 EDT
<output omitted>

```
Nmap scan report for 10.0.2.15
Host is up (0.00019s 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 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

Post-scan script results:
| clock-skew:
|   0s:
|     10.0.2.4
|     10.0.2.3
|_    10.0.2.2
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 346.89 seconds
```

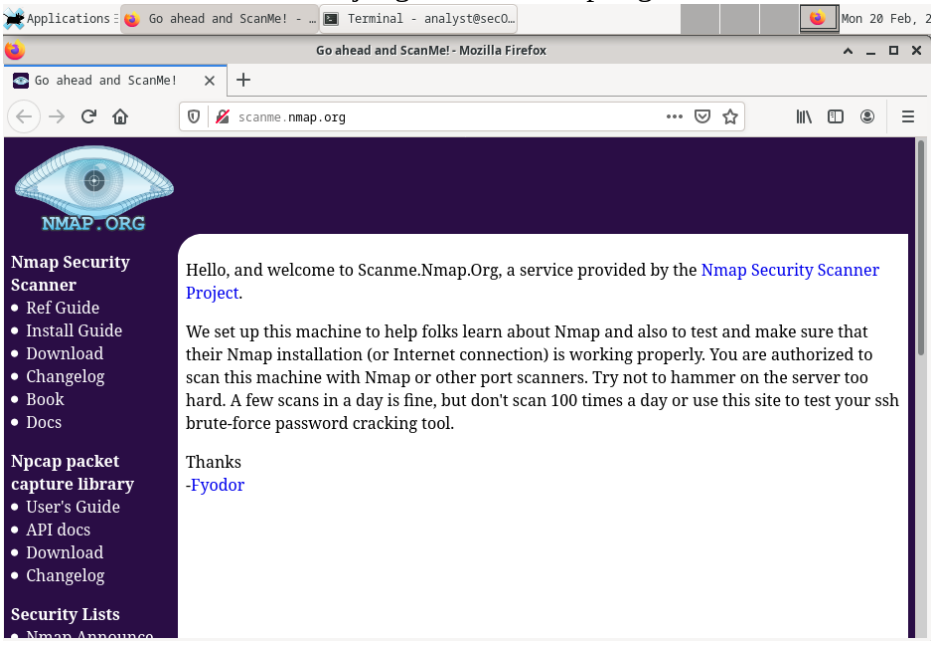
Berapakah jumlah host yang terdeteksi?



```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:02 EST
Nmap scan report for 10.0.2.15
Host is up (0.00030s 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 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: 256 IP addresses (1 host up) scanned in 45.95 seconds
```

4. Remote Server Scanning
   Buka web browser dan kunjungi scanme.nmap.org

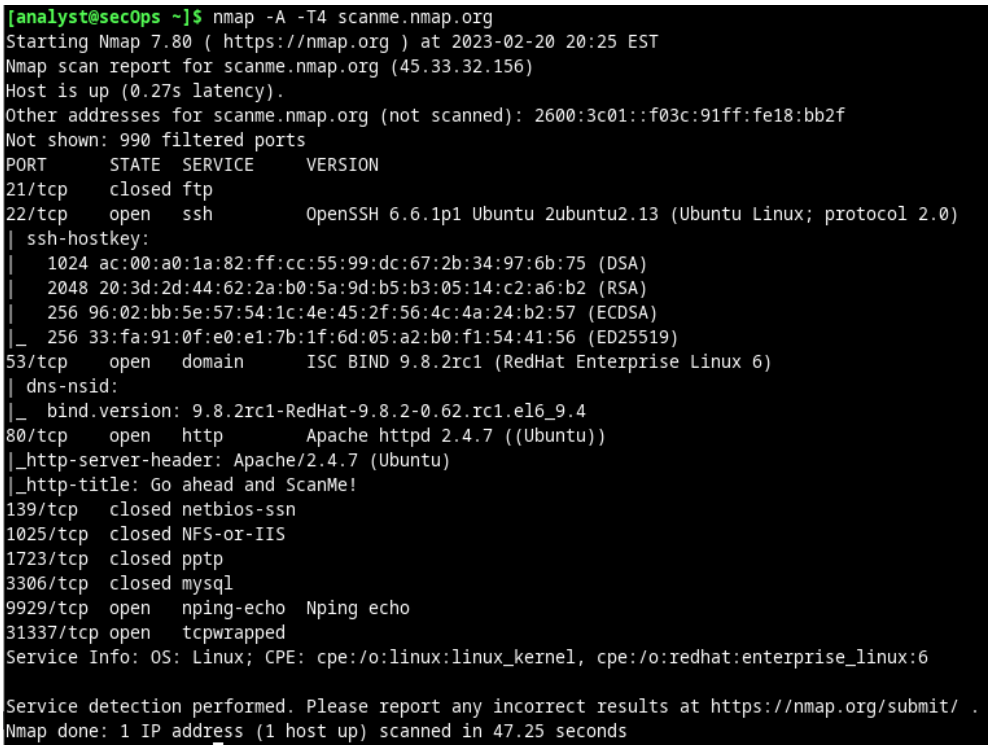


Ketikkan perintah berikut:

[analyst@secOps Desktop]$ **nmap -A -T4 scanme.nmap.org**
Starting Nmap 7.40 (https://nmap.org) at 2017-05-01 16:46 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156) Host is up (0.040s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (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)
25/tcp filtered smtp
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_httptitle: Go ahead and ScanMe!
135/tcp filtered msrpc
139/tcp filtered netbios ssn
445/tcp filtered microsoft
593/tcp filtered http-- rpc
4444/tcp filtered krb524
9929/tcp open nping--ds epmap echo Nping echo
31337/tcp open tcpwrapped
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 23.96 seconds



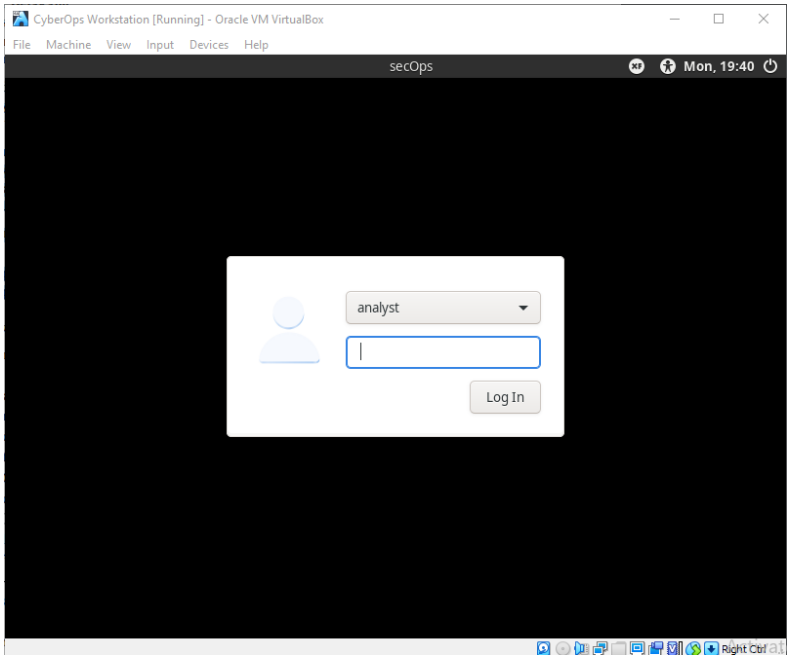
Port dan layana n apa yang terbuka?

Berapa alamat IP server?
Apa sistem operasi yang digunakan oleh server?

5. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok

Unit 3

1. Jalankan VM dan Login
   Username: **analyst**
   Password: **cyberops**

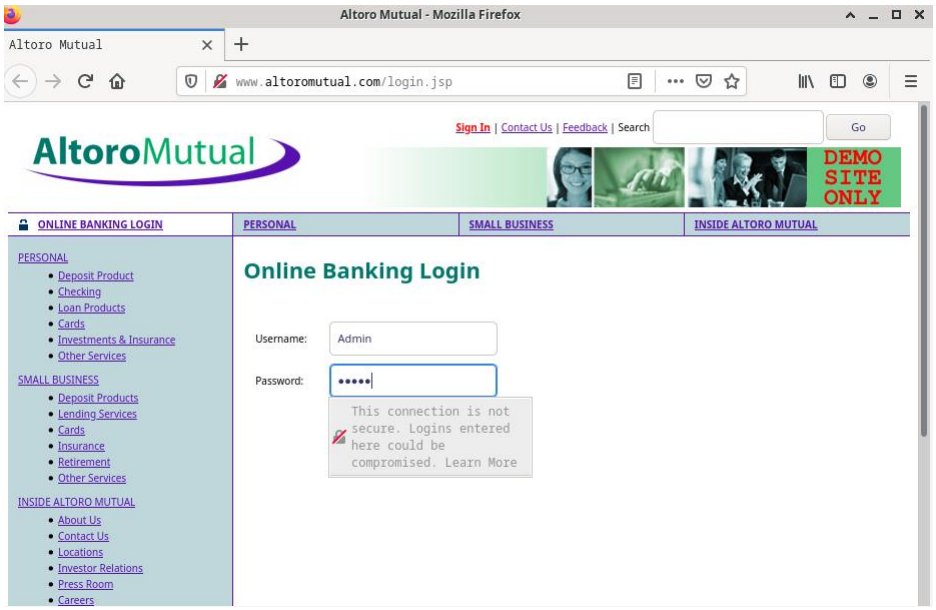


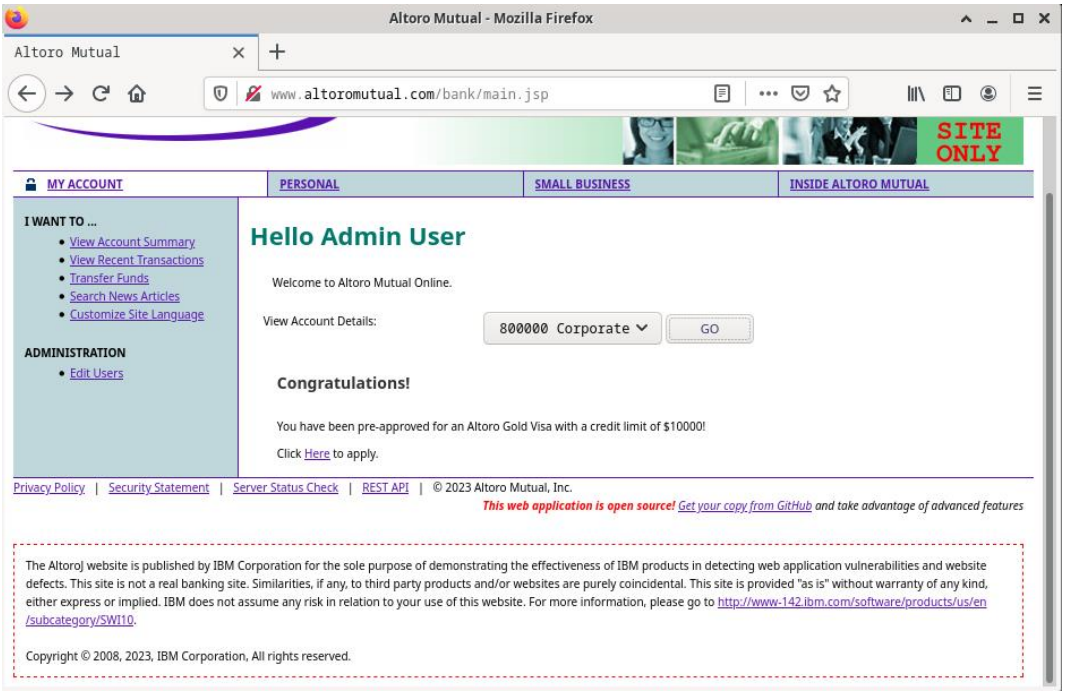
2. Buka terminal dan menjalankan **tcpdump**
   Pengecekan alamat IP dengan menggunakan perintah:
   [analyst@secOps ~]$ **ip address**
   [analyst@secOps ~]$ **sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap**
   [sudo] password for analyst:
   tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

```
[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 08:00:27:0e:b4:81 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 85303sec preferred_lft 85303sec
    inet6 fe80::a00:27ff:fe0e:b481/64 scope link
       valid_lft forever preferred_lft forever
```

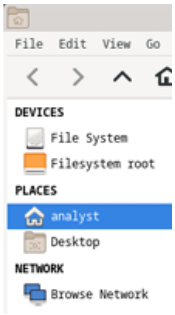
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

3. Buka link http://www.altoromutual.com/login.jsp melalui browser di CyberOps
   Username : **Admin**
   Password : **Admin**

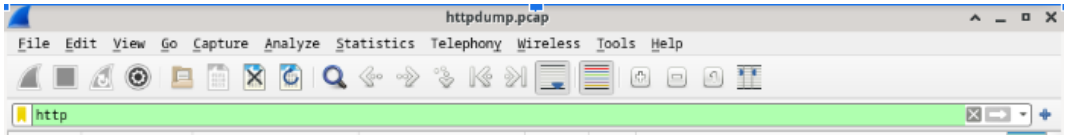




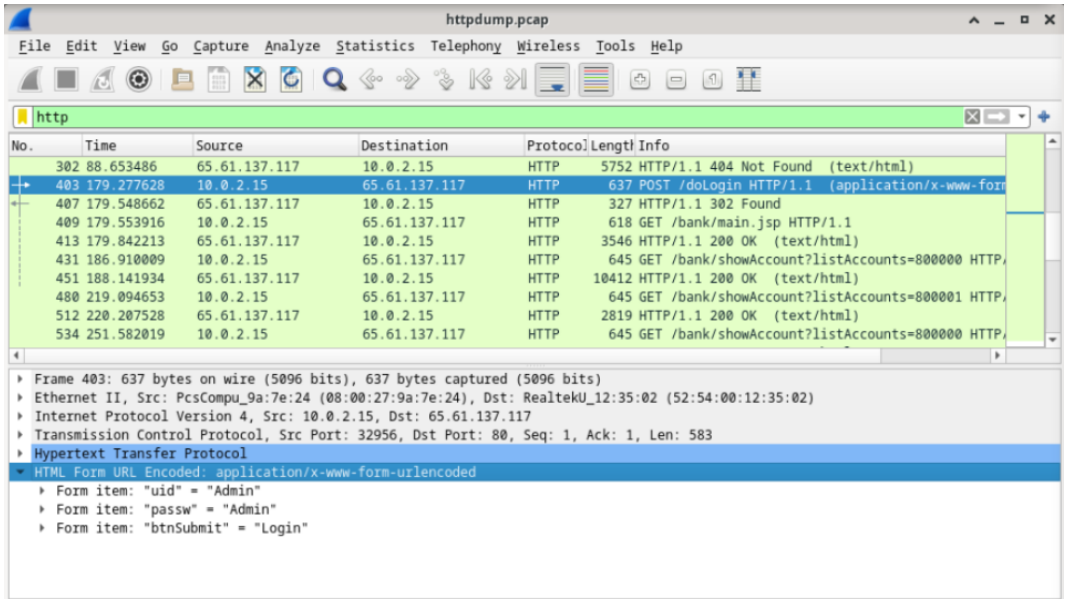
4. Merekam Paket HTTP
   Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan kedalam file bernama httpdump.pcap. file ini terletak pada folder **/home/analyst/**.



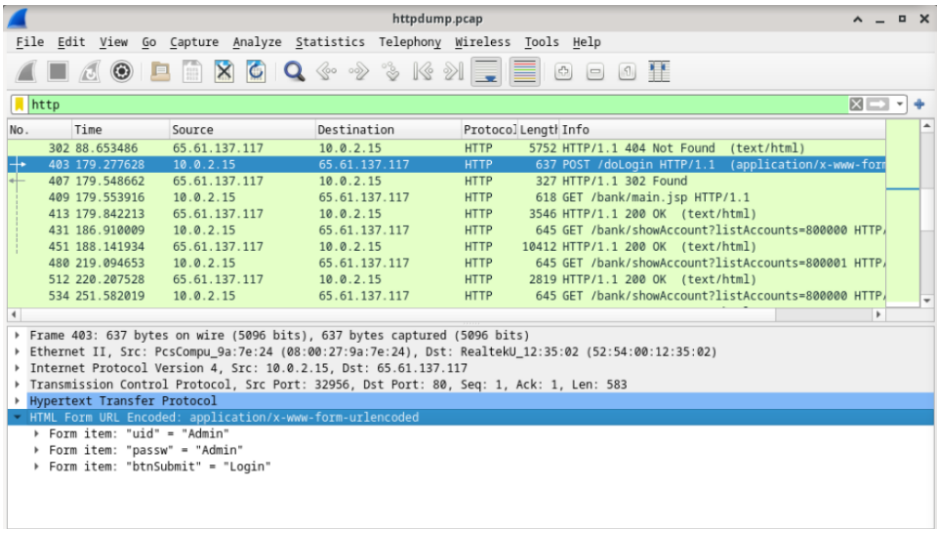
5. Filter **http** kemudian klik **Apply**



6. Pilih **POST**



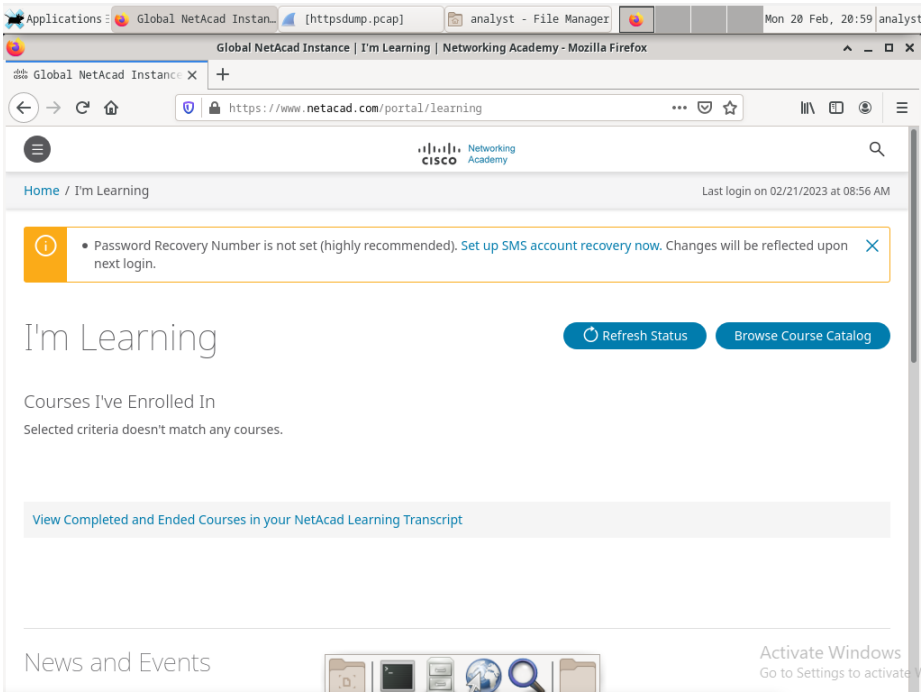
7. Lakukanlag analisis terhadap **uid** dan **passw**



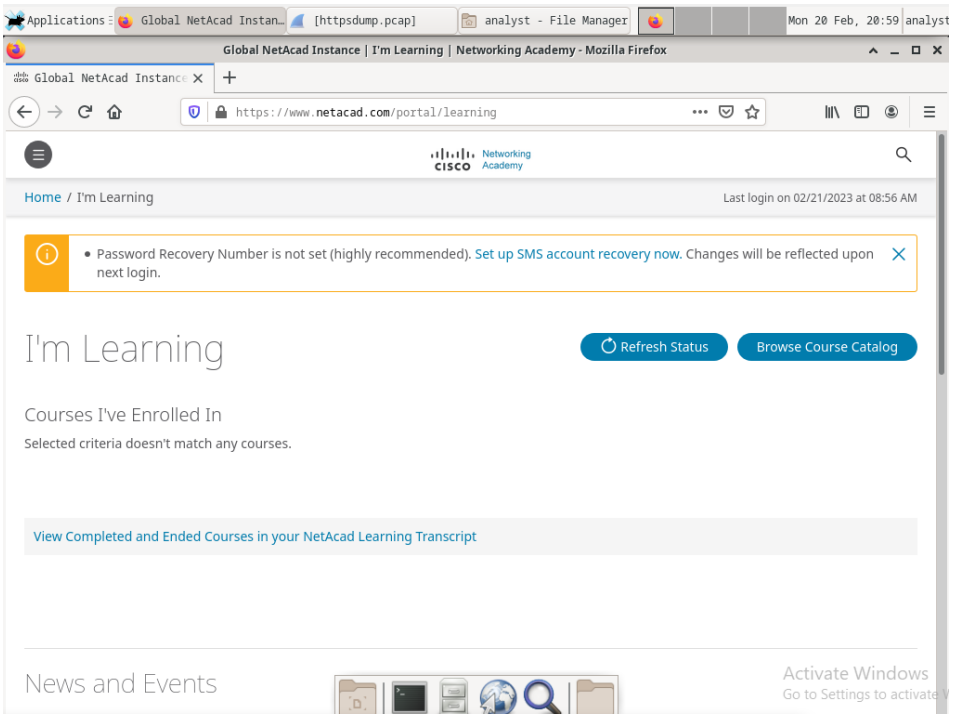
8. Merekam paket HTTPS
   [analyst@secOps ~]$ **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**
   [sudo] password for analyst:
   tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

```
[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

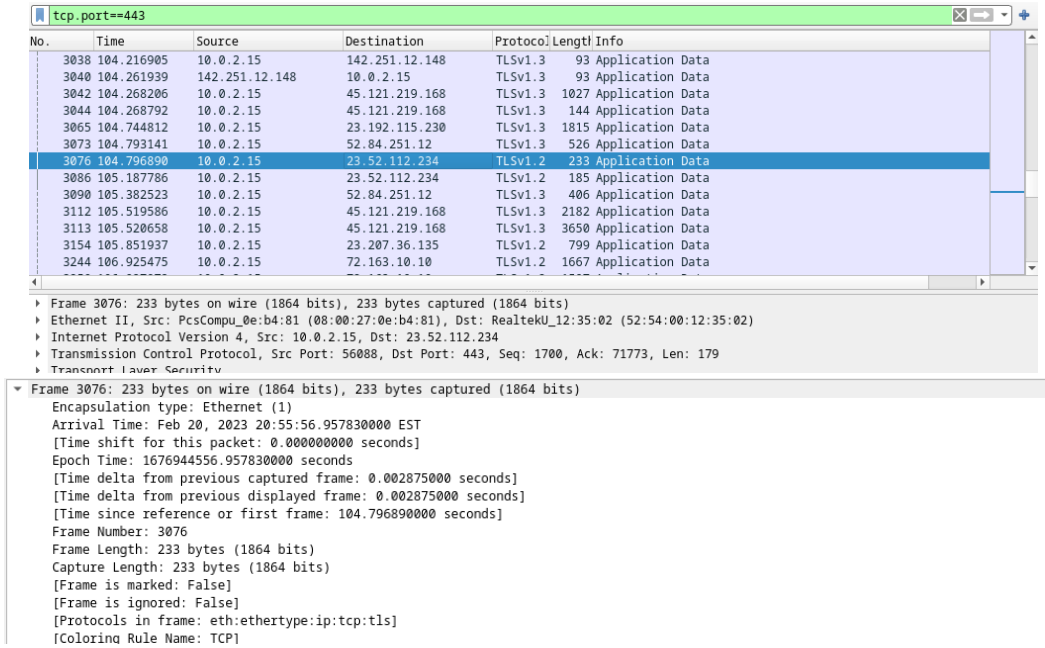


12. Melihat rekaman paket HTTPS

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

13. Filter **tcp.port==443**

14. Pilih **Application Data**



15. Analisislah hasil yang didapatkan
16. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.

E. Pembahasan

Unit 2

Pada praktikum kali ini yaitu mengeksplorasi Nmap. Buka virtualBox dan start file CyberOps Workstation. Setelah itu masukkan username dan password. Buka terminal setelah itu mengetik $man nmap. Nmap (Network Mapper) adalah 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 NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Fungsi kedua dari adanya NMAP adalah untuk melakukan scanning terhadap suatu port jaringan komputer. Port adalah nomor yang berguna untuk membedakan antara aplikasi yang satu dengan aplikasi yang lainnya yang masih berada dalam jaringan komputer. Setelah itu melakukan Localhost Scanning yang berfungsi untuk men scanning localhost dan mengetahui port dan layanan apa yang terbuka dan software apa yang digunakan pada port yang

terbuka tersebut. Sebelum melakukan network scanning alangkah lebih baiknya untuk mengetahui alamat IP host terlebih dahulu yaitu dengan $ip address pada terminal. Setelah itu dapat diketahui alamat ip dan subnet mask dari pc host yaitu 10.0.2.15/24. Setelah mengetahui alamat ip, lakukan port scanning dengan cara $ nmap -A – T4 10.0.2.15.0/24. Case selanjutnya yaitu melakukan remote server scanning dengan cara membuka terlebih dahulu web browser yaitu scanme.nmap.org. setelah itu lakukan scanning dengan cara mengetikan $ nmap -A -T4 scanme.nmap.org. maka kita akan mengetahui port dan layanan apa yang terbuka yaitu port tcp, berapa alamat IP server yaitu 45.33.32.156, apa sistem operasi yang digunakan oleh server yaitu OS Linux.

Unit 3

Pada unit ini yang bertujuan untuk merekam dan menganalisis trafik http serta https. Pada lab ini akan menjelajahi dan menangkap lalu lintas HTTP dan HTTPS menggunakan Wireshark. Dengan membuka terminal dan menjalankan tcpdump yang merupakan utilitas baris perintah yang dapat digunakan untuk capture dan melakukan inspeksi terhadap lalu lintas jaringan dari dan ke sistem. tcpdump adalah tools yang paling umum digunakan di antara security pentest atau administrator jaringan baik untuk mengatasi masalah jaringan dan pengujian keamanan. Lakukan pengecekan alamat ip dengan perintah $ip address. Setelah itu ketik perintah $ sudo tcpdump -I enp0s3 -s 0 -w httpdump.pcap. perintah tersebut digunakan untuk memulai dan merekam network traffic pada interface enp0s3. Perintah -i memungkinaan 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 snaplan 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 extensi. Tcpdump tadi akan mencetak output ke file bernama httpdump.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 pada praktikum kali ini yaitu Nmap digunakan secara khusus untuk eksplorasi jaringan serta melakukan audit terhadap keamanan dari jaringan. Fungsi NMAP yang pertama adalah sebagai alat untuk melakukan pengecekan pada jaringan. NMAP bisa digunakan untuk melakukan pengecekan terhadap jaringan besar dalam waktu yang singkat. Fungsi kedua dari adanya NMAP adalah untuk melakukan scanning terhadap suatu port jaringan komputer. 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

A, F. (2022, May 11). *Perbedaan HTTP dan HTTPS serta Pengertiannya*. Hostinger Tutorial. https://www.hostinger.co.id/tutorial/perbedaan-http-dan-https#:~:text=Perbedaan%20HTTP%2FHTTPS%20adalah%20pada

Pengertian NMAP Adalah : Fungsi, Cara Kerja & Penggunaannya. (n.d.). Www.nesabamedia.com. Retrieved February 24, 2023, from https://www.nesabamedia.com/pengertian-nmap/

xsand. (2020, January 22). *Pengertian dan Penggunaan Perintah Tcpdump di Linux*. LinuxID. https://www.linuxid.net/32373/pengertian-dan-penggunaan-perintah-tcpdump-di-linux/