LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

Unit 2 – Eksplorasi Nmap

DISUSUN OLEH

Nama	: Sofiyanatul Munawaroh
NIM	: 21/474781/SV/19035
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 – Eksplorasi Nmap

I. Tujuan

- Mengeksplorasi Nmap.
- Melakukan *Scan* ke *Port* yang terbuka.

II. 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.*

Network Mapper atau yang dapat disebut dengan NMAP adalah sebual *tool* yang dapat digunakan tanpa berbayar atau *open source*. NMAP memiliki peran penting dalam audit dan juga eksplorasi yang berkaitan dengan keamanan jaringan.

Pada dasarnya, NMAP memiliki cara kerja yakni mengirimkan sebuah paket pada target tujuannya dengan bantuan IP *raw* yang bekerja dengan canggihnya. Oleh karena itu, dapat ditentukan *host* mana saja yang sedang aktif.

Tak hanya itu, NMAP juga melakukan *bruteforce* pada *port host* yang aktif ke *port list* baik dengan *filter, close*, hingga *open* sekalipun.

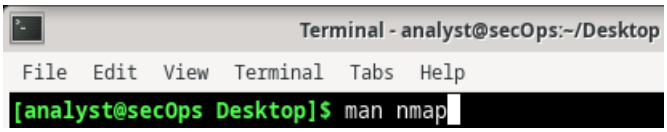
Kemampuan dan bagaimana NMAP bekerja tidak hanya sampai di situ saja. NMAP dapat melihat dan mengecek sebuah sistem operasi apakah sudah terinstal dengan lengkap bersama dengan versi yang digunakan. Untuk mendapatkan semua informasi tersebut, NMAP secara khusus dibantu dengan *port* yang sedang aktif.

III. Alat dan Bahan

- CyberOps *Workstation Virtual Machine.*
- Koneksi Internet.

IV. Instruksi Kerja

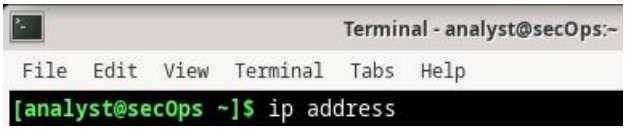
1. Eksplorasi Nmap
   Start CyberOps *Workstation,* dan buka terminal kemudian ketikkan *command* :
   [analyst@secOps~]$ **man nmap**



2. *Localhost Scanning*
   Coba lakukan *command* **nmap -A -T4 localhost.**

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

3. *Network Scanning*
   Sebelum melakukan *scanning,* ketahui alamat IP *host* terlebih dahulu dengan *command* **ip address.**



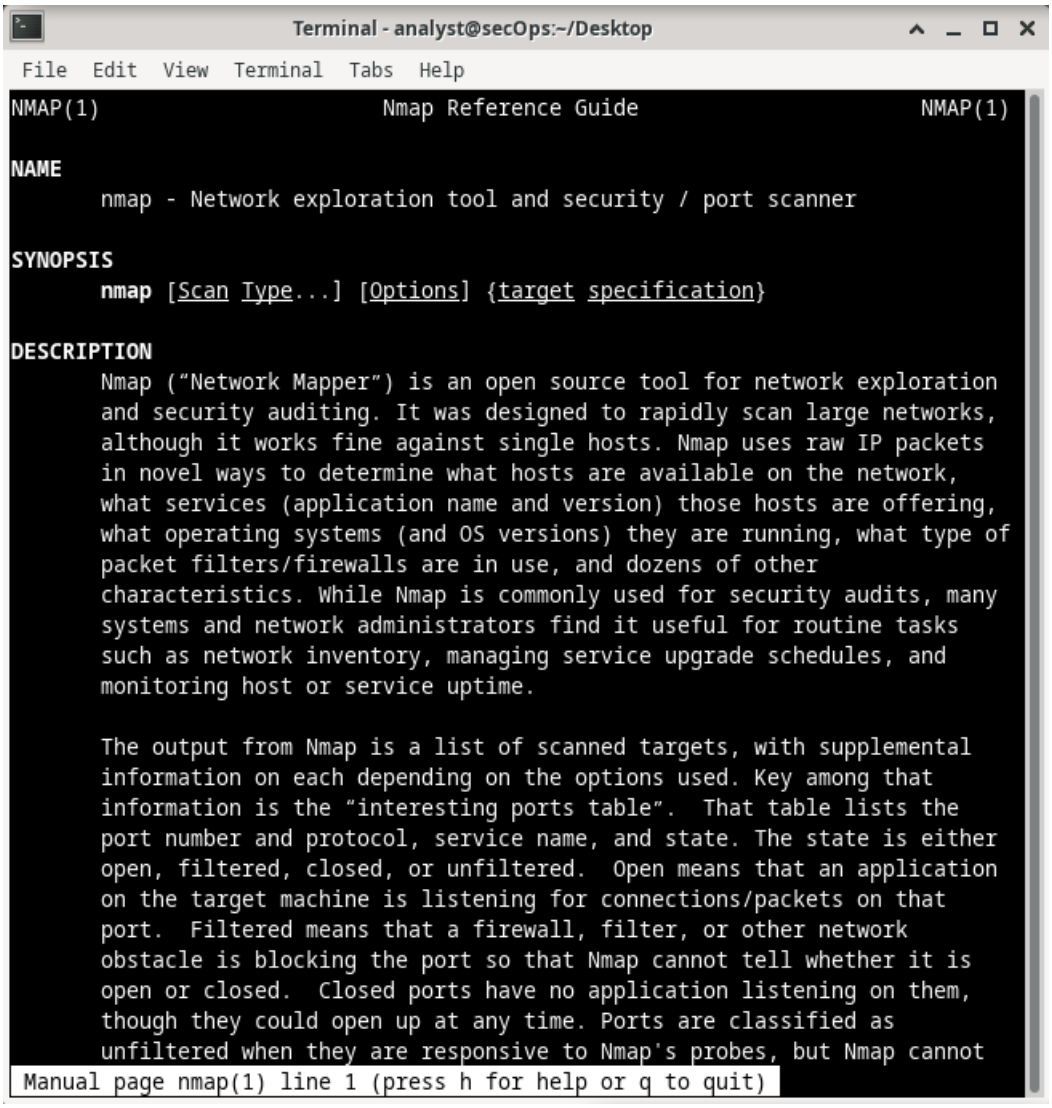
Setelah itu, lakukan *port scanning* dengan menggunakan Nmap dengan *command* **nmap -A -T4 10.0.2.0/24.** Menyesuaikan dengan alamat IP *host* yang ada.

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

V. Hasil dan Pembahasan

Pada pertemuan ini (Unit 2-Eksplorasi Nmap) dilakukan eksplorasi Nmap dan mencoba melakukan *scan* ke *port* yang terbuka. Berikut merupakan hasil dari instruksi kerja yang dilakukan:

1. Eksplorasi Nmap



Eksplorasi Nmap dilakukan dengan *command* **man nmap** yang memunculkan berbagai informasi terkait Nmap. Berdasarkan informasi tersebut. Nmap ("*Network Mapper*") adalah *open source tool* untuk eksplorasi jaringan dan audit keamanan. Nmap dirancang untuk memindai jaringan besar dengan cepat, meskipun Nmap bekerja dengan baik terhadap *host* tunggal. Nmap menggunakan paket IP *raw* dengan cara baru untuk menentukan *host* apa yang tersedia di jaringan, layanan apa (nama

dan versi aplikasi) yang ditawarkan *host* tersebut, sistem operasi (dan versi OS) apa yang mereka jalankan, jenis filter/*firewall* paket apa sedang digunakan, dan lusinan karakteristik lainnya.

Sementara Nmap umumnya digunakan untuk audit keamanan, banyak administrator sistem dan jaringan menganggapnya sebagai tugas rutin yang berguna seperti inventaris jaringan, mengelola jadwal peningkatan layanan, dan memantau *host* atau waktu aktif layanan.

2. *Localhost Scanning*

```
[analyst@secOps Desktop]$ nmap -A -T4 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:51 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00044s 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 20.88 seconds
```

Localhost Scanning menggunakan *command* **nmap -A -T4 localhost** yang mana berfungsi untuk melakukan *scanning* pada *localhost* sehingga dapat mengetahui *port* dan layanan mana saja yang terbuka serta *software* apa yang digunakan pada *port* yang terbuka tersebut.

Pada hasil *localhost scanning* tersebut *port* yang terbuka adalah 21/tcp yang menyediakan layanan FTP dengan *software* yang digunakan vsftpd 2.0.8 *or later*. Kemudian terdapat *port* 22/tcp yang menyediakan layanan SSH dengan *software* yang digunakan OpenSSH 8.2 (*protocol* 2.0). Terakhir yaitu *port* 23/tcp yang menyediakan layanan telnet dengan *software* yang digunakan Openwall GNU/*/Linux telnetd.

3. *Network Scanning*

```
[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 08:00:27:8f:86:2a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86266sec preferred_lft 86266sec
    inet6 fe80::a00:27ff:fe8f:862a/64 scope link
       valid_lft forever preferred_lft forever
```

Sebelum melakukan *scanning* perlu mengetahui alamat IP *host* terlebih dahulu dengan menggunakan *command* **ip address.** Dari *command* tersebut dapat diketahui bahwa IP *Address host* yaitu 10.0.2.15/24. Karena menggunakan /24 maka *subnet mask*-nya adalah 255.255.255.0.

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:15 EST
Nmap scan report for 10.0.2.15
Host is up (0.00027s 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 4
|      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 39.31 seconds
```

Setelah mengetahui IP *Address host*, baru melakukan *port scanning* dengan menggunakan Nmap. Berdasarkan alamat IP *host* maka *scanning* dilakukan pada jaringan 10.0.2.0/24 yang mana terdeteksi 1 *host* yang aktif yaitu PC *host* sendiri dengan IP *Address* 10.0.2.15/24.

VI. Kesimpulan

1. Nmap ("*Network Mapper*") merupakan *open source tool* untuk eksplorasi jaringan dan audit keamanan.
2. Perlu diketahui IP *Address host* sebelum melakukan *port scanning* dengan Nmap.

VII. Daftar Pustaka

Sutiono. (Tanpa Tahun). *Pengertian NMAP, Fungsi dan Cara Kerjanya*. Diakses pada 21 Februari 2023 dari https://dosenit.com/software/network-mapper