LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

UNIT 2

EKSPLORASI NMAP

Disusun oleh :

Nama	: Aura Nisa' Hidayat
NIM	: 21/482690/SV/19983
Kelas	: TRI A
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Hari, Tanggal	: Selasa, 21 Februari 2023

PROGRAM STUDI DIV TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

Laporan Praktikum Kamanan 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. Pada umumnya digunakan oleh *network administrator* untuk *network inventory*, mengatur servis jadwal *upgrade*, serta monitoring host atau waktu servis. Nmap memiliki cara kerja yaitu mengirim paket khusus ke target host lalu menganalisa respon yang diperoleh, ini dapat dilakukan pada skala besar seperti ratusan ribu komputer. Nmap memiliki TCP dan UDP *port scanning*, OS *detection*, *version detection, ping sweeps*, dan lain-lain.

Terdapat berbagai jenis Teknik *scanning* Nmap yang masing-masing memiliki kelebihan dan kekurangan tersendiri. Berikut beberapa Teknik scanning Nmap:

- **Teknik TCP SYN Scan (-sS)** yang dapat membedakan status *port Open, closed,* dan *filtered* dalam waktu yang cepat. Dengan mengirimkan sebuah paket SYN, kemudian menunggu jawaban dari system target. Mendapat jawaban paket SYN/ACK berarti *port open,* paket RST berarti *port closed,* tidak mendapat jawaban maka *port filtered.*
- **TCP connect() Scan (-sT)** digunakan bila kita tidak memiliki privilege (admin/root) dengan fungsi *system call connect* pada OS. Metode ini membutuhkan waktu lebih lama.
- **UDP Scan -sU** untuk mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP.
- **FIN Scan (-sF),** Xmas Tree Scan (-sX) dan Null Scan (-sN) Teknik ini sering disebut teknik *stealth*. Banyak digunakan pada jaringan yang dilindungi Firewall. Tetapi hasil scan akan sulit membedakan status *open* dan *filtered.*
- **Ping Scan (-sP)** scanning yang paling cepat, umumya digunakan untuk menemukan host yang hidup pada suatu jaringan.
- **Version Detection (-sV)** untuk mengetahui versi dari aplikasi yang digunakan pada komputer target.
- **Scan IP Protocol (-sO)** dapat menemukan protokol IP pada komputer target, misalnya ICMP, TCP, dan UDP
- **Scan ACK (-sA)** untuk menemukan port yang terbuka, tapi berguna pada jaringan yang dilindungi firewall maupun packet filter. Hasil scanning bisa digunakan untuk menentukan tipe firewal yang digunakan apakah statefull atau tidak serta port mana yang difilter.

- **RPC Scan (-sR)** untuk menemukan aplikasi yang menggunakan remote call procedure pada target.
- **Idlescan (-sI)** bila kita tidak memiliki akses langsung ke komputer target, karena biasanya target dilindungi firewall.

III. ALAT DAN BAHAN

- CyberOps Workstation virtual machine
- Internet access

IV. INSTRUKSI KERJA

1. Langkah pertama adalah melakukan eksplorasi Nmap dengan membuka terminal dan mengetikkan [analyst@secOps ~]$ **man nmap**

Apa itu Nmap?

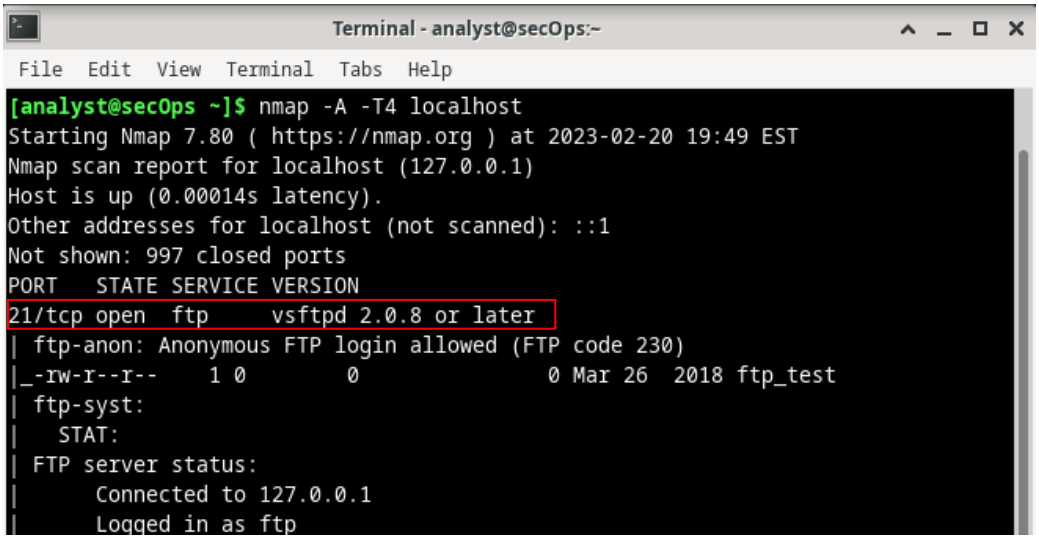
Nmap atau *Network Mapper* adalah sebuah *tool open source* yang digunakan untuk eksplorasi jaringan digital serta melakukan audit terhadap keamanan digital. Nmap menggunakan alamat IP baru untuk menentukan host apa yang tersedia dalam jaringan tersebut.

Apa fungsi dari Nmap?

- Memeriksa jaringan besar dalam waktu singkat
- Berfungsi untuk *scanning* pada port jaringan komputer yang dapat membedakan antara aplikasi yang satu dengan lainnya.
- Sebagai *discover vulnerebilities* dan *version detection* dalam menemukan kerentanan

Yang nantinya Nmap menunjukkan output daftar target yang dipindai dengan informasi tambahan pada masing-masing tergantung pada opsi yang digunakan.

2. Localhost scanning



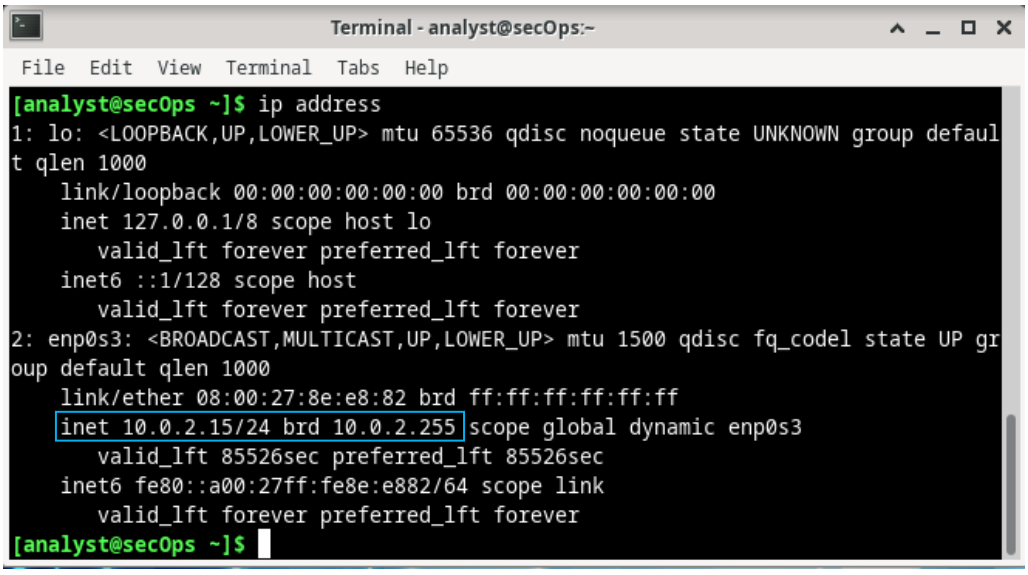
```
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     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 18.84 seconds
[analyst@secOps ~]$
```

Port dan layanan apa yang terbuka?
Port 21: meberikan layanan FTP
Port 22: memberikan layanan sebagai SSH
Port 23: memberikan layanan sebagai telnet

Software apa yang digunakan pada port yang terbuka tersebut?
Pada port tersebut menggunakan *software* vsftpd, openssh, dan openwall.

3. Network scanning



Berapakah alamat IP dan subnet mask dari PC host?
Alamat IP → 10.0.2.15/24
Subnet mask → 10.0.2.255

Melakukan port scanning dengan menggunakan Nmap:

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:54 EST
Nmap scan report for 10.0.2.15
Host is up (0.00016s 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

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 21.64 seconds
[analyst@secOps ~]$
```

4. Remote server scanning

```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 19:58 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 989 filtered ports
PORT      STATE  SERVICE       VERSION
22/tcp    open   ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (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)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
53/tcp    open   domain        ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
| dns-nsid:
|_  bind.version: 9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.4
80/tcp    open   http          Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   closed msrpc
554/tcp   closed rtsp
587/tcp   closed submission
993/tcp   closed imaps
3389/tcp  closed ms-wbt-server
5900/tcp  closed vnc
9929/tcp  open   nping-echo    Nping echo
31337/tcp open   tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel, cpe:/o:redhat:enterprise_linux:6

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.64 seconds
[analyst@secOps ~]$
```

Port dan layanan apa yang terbuka?
Port 22: layanan SSH
Port 53: layanan domain
Port 80: layanan http
Port 9929: layanan nping-echo
Port 31337: layanan tcp wrapped

Berapa alamat IP server?
45.33.32.156

Apa sistem operasi yang digunakan oleh server?
Linux

V. PEMBAHASAN

Nmap merupakan sebuah *software open source* yang digunakan untuk eksplorasi jaringan digital serta melakukan audit terhadap keamanan digital. Nmap menggunakan alamat IP baru untuk menentukan host apa yang tersedia dalam jaringan tersebut. *Tool* ini berfungsi untuk *scanning* pada port jaringan komputer yang dapat membedakan antara aplikasi yang satu dengan lainnya. Dan terdapat berbagai macam teknik *scanning* yang dapat digunakan. Pada praktikum ini saat melakukan *scanning* menggunakan **argument -A** untuk memeriksa system operasi, layanan, dan versi port, kemudian **argument -T4** digunakan untuk memeriksa eksekusi yang lebih cepat dan memeriksa nama host target.

Dari praktikum terdapat beberapa *output scanning* Nmap yaitu ***open*** atau terbuka yang berarti bahwa aplikasi pada mesin target sedang mendengarkan (*listening*) untuk koneksi atau paket pada port tersebut. Kemudian terdapat *output* ***closed*** berarti port tidak memiliki aplikasi yang sedang mendengarkan meskipun port tersebut dapat terbuka kapan saja. Selain itu terdapat *output* Nmap yang disebut ***filtered*** atau difilter yang memiliki arti bahwa sebuah *firewall* atau penghalang jaringan lainnya memblokir port tersebut sehingga Nmap tidak dapat mengetahui port tersebut terbuka atau tertutup.

Pada proses ***localhost scanning*** terdapat 997 *closed port* dan 3 *opened port.* Selanjutnya pada bagian ***network scanning*** dilakukan dengan menggunakan IP yang menunjukkan *output* yang sama seperti sebelumnya yaitu 997 *closed port* dan 3 *opened port*. Kemudian proses ***remote server scanning*** terdapat 989 *filtered port*, 5 *opened port*, dan 6 *closed port* yang terdeteksi dari IP 45.33.32.156 dengan system operasi Linux.

VI. KESIMPULAN

Dari praktikum keamanan informasi kali ini dapat disimpulkan bahwa:

1. Nmap merupakan *software* atau *tool open source* yang digunakan untuk eksplorasi jaringan digital terhadap keamanan jaringan.
2. *Scanning* Nmap terbagi menjadi beberapa jenis yang masing-masing memiliki kelebihan dan kekurangan tersendiri
3. Hasil *output* dari Nmap merupakan daftar target yang diperiksa dengan informasi seperti port, layanan, dan status.
4. Terdapat beberapa jenis status *scanning* Nmap yaitu *opened, closed, filtered,* dan *unfiltered.*

DAFTAR PUSTAKA

Admin. (2022, November 5). *Network Scanning Tool - Nmap*. Retrieved Februari 25, 2023, from SkillPlus: https://skillplus.web.id/network-scanning-tool-nmap/

Ismail, S. J. (n.d.). *Teknik Scanning Nmap*. Retrieved Februari 25, 2023, from https://julismail.staff.telkomuniversity.ac.id/teknik-scanning-nmap/

Panduan Referensi Nmap (Man Page, bahasa Indonesia). (n.d.). Retrieved Februari 25, 2023, from nmap.org: https://nmap.org/man/id/index.html