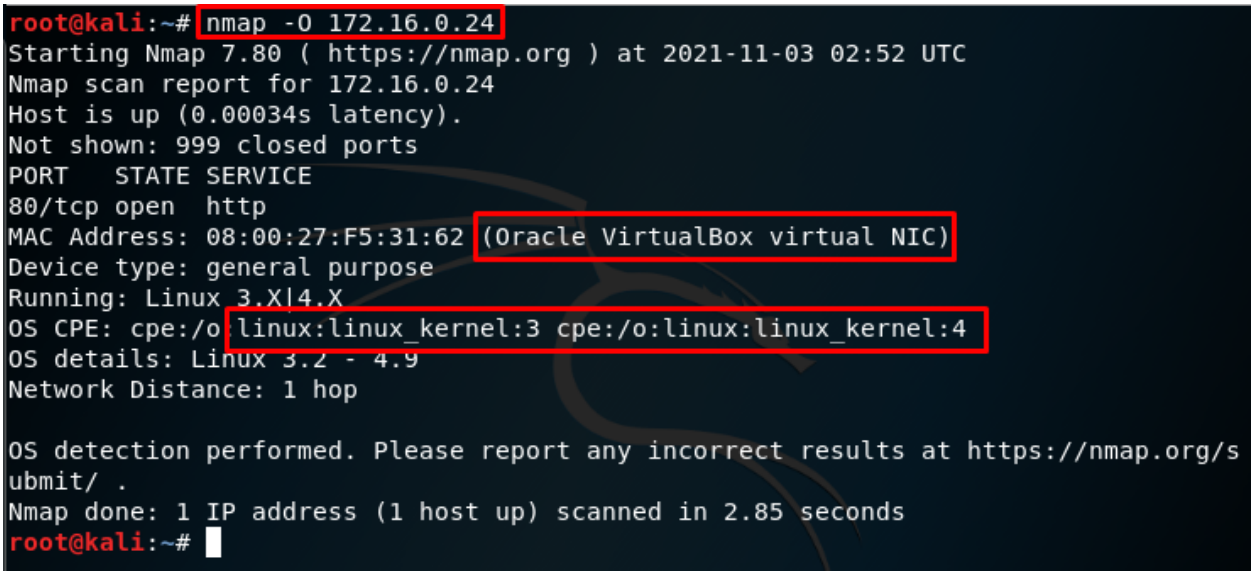
LEMBAR KERJA SESI 1

Latihan

1. Untuk mengetahui sistem operasi dari suatu host digunakan perintah apa? beri contohnya!

   (nmap -O x.x.x.x)

   ket = x.x.x.x = ip address tertentu.



Dari percobaan scanning nmap tersebut akan menscan sistem operasi yang digunakan setiap host

2. Untuk memindai port dari suatu host dengan 3-way handshake digunakan perintah apa? berikan contohnya!

   (nmap x.x.x.x -sT)

   ket = x.x.x.x = ip address tertentu

```
root@kali:~# nmap -sT 172.16.0.24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 02:54 UTC
Nmap scan report for 172.16.0.24
Host is up (0.00044s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:F5:31:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@kali:~#
```

Dari gambar tersebut dapat dilihat bahwa nmap akan mencari port yang sudah terbuka pada setiap system operasi.

(nmap x.x.x.x -sS)

ket = x.x.x.x = ip address tertentu

```
root@kali:~# nmap -sS 172.16.0.24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 03:23 UTC
Nmap scan report for 172.16.0.24
Host is up (0.00032s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:F5:31:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Dari percobaan diatas dapat dilihat bahwa membuka tidak koneksi TCP secara utuh dan tersembunyi.

(nmap x.x.x.x -sF)

ket = x.x.x.x = ip address tertentu

```
root@kali:~# nmap 172.16.0.24 -sF
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-03 03:46 UTC
Nmap scan report for 172.16.0.24
Host is up (0.00037s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:F5:31:62 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Dari percobaan diatas dapat dilihat status scan dari nmap akan mengecek state dari pada layanan.

3. Apa perbedaan –sT dan –sS pada perintah scan options nmap?

-sS (TCP SYN scan)

SYN scan merupakan opsi scan baku dan terpopuler dengan alasan yang baik. Ia dapat dilakukan dengan cepat, memeriksa ribuan port per detik pada jaringan yang cepat tidak dihalangi oleh firewall yang membatasi. Scan SYN relatif tidak mengganggu dan tersembunyi, karena ia tidak pernah melengkapi koneksi TCP. Ia juga bekerja terhadap stack TCP yang sesuai alih-alih tergantung pada platform khusus sebagaimana scan FIN/NULL/Xmas, Maimon dan idle. Ia juga memungkinkan pembedaan yang tegas dan handal antara status open, closed, dan filtered.

Teknik ini seringkali diacu sebagai pemeriksaan setengah terbuka (half-open scanning), karena anda tidak membuka seluruh koneksi TCP. Anda mengirim sebuah paket SYN, seperti anda ingin melakukan koneksi sesungguhnya dan kemudian menunggu tanggapan. SYN/ACK menandakan port sedang mendengarkan (open), RST (reset) menandakan tidak sedang mendengarkan. Jika tidak ada tanggapan setelah beberapa kali pengiriman ulang, port ditandai sebagai tersaring (filtered). Port juga ditandai sebagai tersaring bila diterima kesalahan ICMP unreachable (tipe 3, kode 1, 2, 3, 9, 10, atau 13).

-sT (TCP connect scan)

Scan TCP connect merupakan jenis scan baku TCP ketika scan SYN tidak dapat digunakan. Hal ini terjadi ketika user tidak memiliki privilege untuk paket raw atau ketika melakukan pemeriksaan jaringan IPv6. Alih-alih menulis paket raw sebagaimana dilakukan jenis scan lainnya, Nmap meminta SO membuat koneksi dengan mesin target dan port dengan memberikan system call connect. Ini merupakan system call yang digunakan oleh web browsers, klien P2P, dan kebanyakan aplikasi jaringan lainnya untuk membuat koneksi. Ia merupakan bagian dari interface pemrograman yang dikenal sebagai Berkeley Sockets API. Nmap juga menggunakan API ini untuk memperoleh informasi status setiap usaha koneksi.

Ketika tersedia SYN scan, ia merupakan pilihan yang lebih baik. Nmap kurang memiliki kendali atas call connect daripada paket raw, membuatnya kurang

efisien. System call membuat koneksi lengkap untuk membuka port target daripada membuat reset setengah-terbuka (half-open reset) yang dilakukan SYN scan. Hal ini tidak saja lebih lambat dan membutuhkan lebih banyak paket untuk memperoleh informasi yang sama, namun juga mesin target kemungkinan mencatat koneksi. IDS yang baik akan mendeteksi hal ini, namun kebanyakan mesin tidak memiliki sistem alarm tersebut. Kebanyakan layanan pada sistem Unix umum akan membuat catatan ke syslog, dan seringkali pesan kesalahan yang rumit, ketika Nmap membuka dan menutup koneksi tanpa mengirim data. Layanan yang benar-benar buruk akan crash ketika hal ini terjadi, meskipun tidak umum. Administrator yang melihat serangkaian usaha koneksi dari sistem tunggal di lognya seharusnya tahu bahwa ia telah diperiksa dengan metode connect.