LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1 (SVRI214404)

Unit 2, Eksplorasi Nmap

DISUSUN OLEH:

Nama : Reyhan Gusnur Putra

NIM : 21/477927/SV/19223

Hari, Tanggal : Selasa, 21 Februari 2023

Kelas : A

PROGRAM STUDI TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

A. Tujuan

- Mengeksplorasi Nmap
- Melakukan scan ke port yang terbuka

B. Dasar Teori

Port Scanning adalah aktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah mesin. Banyak aplikasi yang menawarkan fasilitas untuk melakukan pemeriksaan port pada sebuah mesin, seperti netcat, unicornscan, nmap, dll.

Secara sederhana dapat dimisalkan bahwa port adalah sebuah pintu, maka scanning adalah proses untuk mengamati atau meninjau. Jadi, dari kedua pengertian di atas, dapat kita tarik kesimpulan bahwa port scanning adalah suatu kegiatan atau aktifitas atau proses untuk mencari dan melihat serta meneliti port pada suatu komputer atau perlengkapan dan peralatannya. Tujuan dari kegiatan ini adalah meneliti kemungkinan-kemungkinan kelemahan dari suatu sistem yang terpasang pada suatu komputer atau perlengkapan dan peralatannya melalui port yang terbuka. Pada intinya, melakukan port scanning ialah untuk mengidentifikasi port-port apa saja yang terbuka, dan mengenali OS target.

Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan "port scanning" untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan firewall atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan. Jika yang dilakukan hanya untuk menambah ilmu atau hanya mengetahui saja tanpa ada niat untuk merusak atau membocorkan sebuah informasi, maka aktivitas ini dapat di katakan bukan merupakan cyber crime.

C. Alat dan Bahan

- CyberOps Workstation
- Jaringan Internet

D. Instruksi Kerja

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?

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?

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)
|_http-title: Go ahead and ScanMe!
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
4444/tcp filtered krb524
9929/tcp open nping-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 layanan apa yang terbuka?

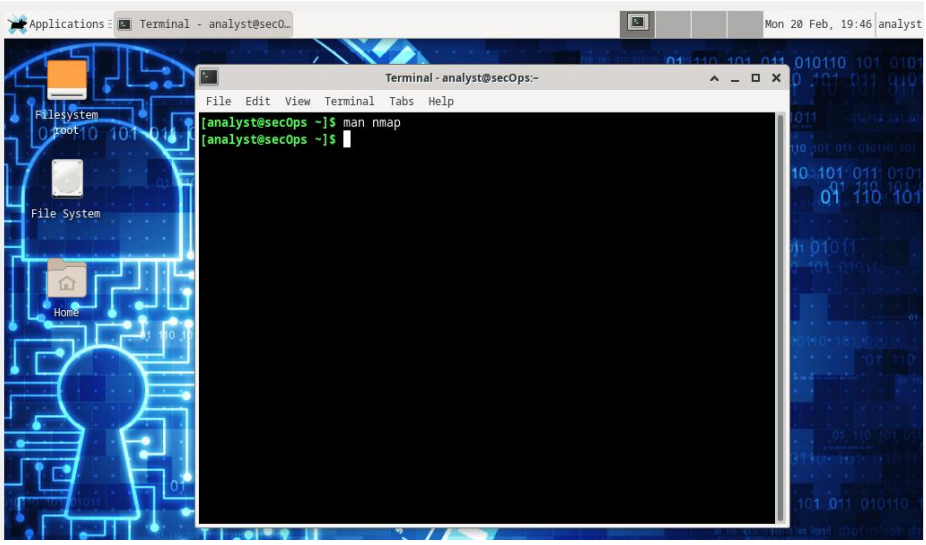
Berapa alamat IP server?

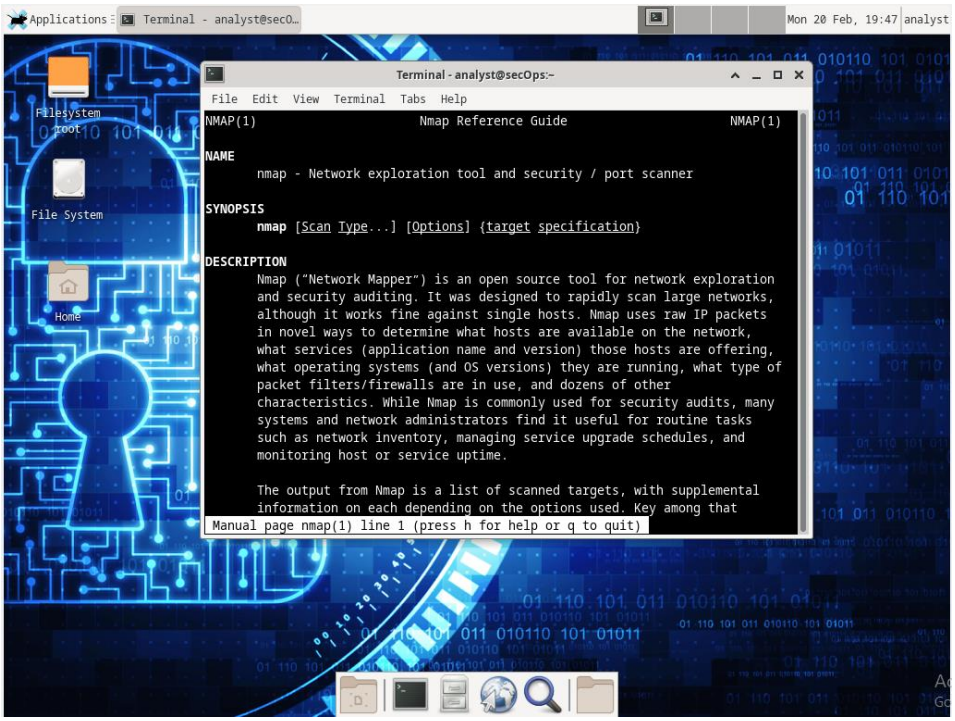
Apa sistem operasi yang digunakan oleh server?

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

E. Hasil dan Pembahasan

1. Eksplorasi Nmap





- Apa itu Nmap?

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.Nmap ini dapat ditemukan pada semua platform mulai dari Microsoft Windows, Linux, Mac OS, OpenBSD, FreeBSD, NetBSD, Amiga, Sun Solaris, HP-UX, dan masih banyak lagi.

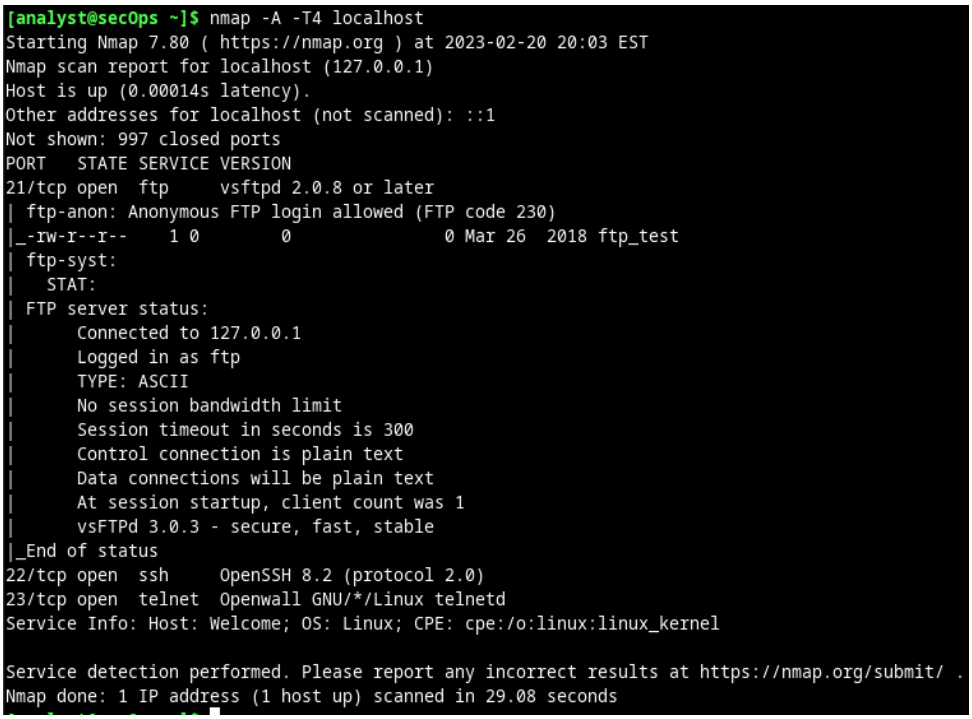
- Apa fungsi dari Nmap?

Fungsi utama NMAP adalah mengecek dan memeriksa sebuah jaringan. Pengecekan oleh NMAP dapat dilakukan sekalipun pada jaringan yang besar dan kurun waktu yang singkat. NMAP dapat bekerja pada host tunggal dengan cara menggunakan IP raw sebagai penentu nama dari host yang disediakan pada suatu jaringan. IP raw ini dapat berfungsi untuk melihat dan mengetahui layanan apa saja yang tersedia dengan nama dan

versi aplikasi di dalamnya, sistem operasi lengkap dengan versinya, serta jenis – jenis firewall dan paket filter apa saja yang digunakan.

Fungsi NMAP selanjutnya adalah melakukan pemindaian pada port yang ada di dalam sebuah jaringan komputer. Port itu sendiri merupakan nomor yang digunakan dalam membedakan aplikasi satu dengan yang lainnya yang ada dalam satu jaringan komputer.

2. Localhost Scanning



- Port dan layanan apa yang terbuka?

Port 21/tcp terbuka, Port 21 merupakan port yang biasa digunakan pada koneksi FTP. FTP klien akan menggunakan port 21 agar dapat terhubung ke FTP server.

Port 22/tcp terbuka, Port 22 adalah port standar untuk SSH (Secure Shell). Port ini berfungsi mengirimkan data melalui jaringan dalam bentuk terenkripsi. Dapat digunakan untuk menjalankan fungsi atau tugas yang bisa diakses dari jarak jauh, misalnya menghubungkan ke host atau server.

Port 23/tcp terbuka, Port 23 TELNET adalah port untuk menghubungkan komputer dan server jarak jauh. Fungsinya mirip dengan SSH, hanya saja port 23 TELNET tidak menggunakan enkripsi pada koneksinya.

- Software apa yang digunakan pada port yang terbuka tersebut?

Software yang digunakan untuk port 21 adalah vsftpd versi 2.0.8 atau lebih tua
Software yang digunakan untuk port 22 adalah Open SSH 8.2 (protocol 2.0)
Software yang digunakan untuk port 23 adalah Openwall GNU/*/Linux telnetd

3. *Network Scanning*

Cek alamat IP host

```
[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:f9:fa:41 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 84760sec preferred_lft 84760sec
    inet6 fe80::a00:27ff:fef9:fa41/64 scope link
       valid_lft forever preferred_lft forever
```

Alamat IP dari PC Host yang didapat adalah 10.0.2.15/24, subnet mask yang didapat dari PC host adalah 10.0.2.255

Scanning dengan menggunakan Nmap

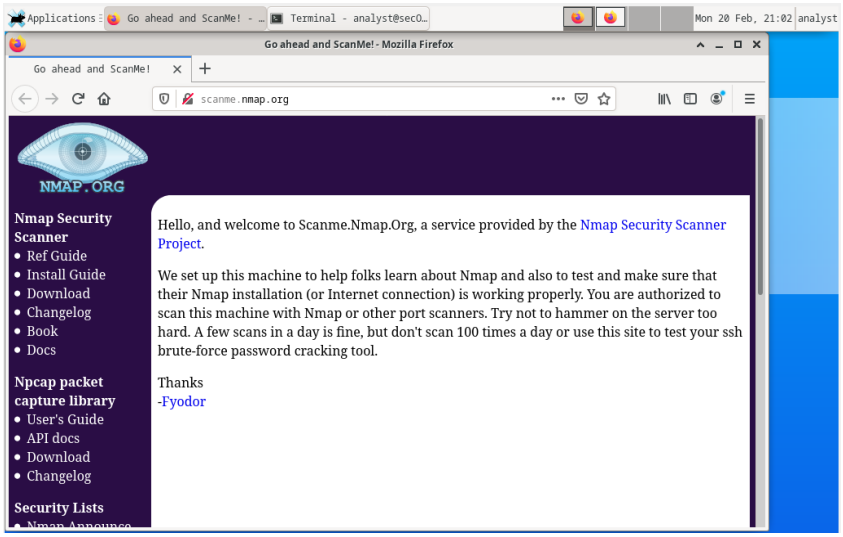
```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.15/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-20 20:06 EST
Nmap scan report for 10.0.2.15
Host is up (0.00014s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP 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 44.98 seconds
```

Beparakah jumlah host yang terdeteksi? Jumlah host yang terdeteksi ada 1 host yang aktif.

4. *Remote Server Scanning*

Web browser scanme.nmap.org



scanme.nmap.org adalah mesin yang dibuat untuk membantu orang-orang belajar tentang Nmap dan juga untuk menguji dan memastikan bahwa instalasi mereka (atau koneksi internet) berfungsi dengan baik. Pengguna diberi wewenang untuk memindai mesin tersebut menggunakan Nmap atau memindai port lainnya.

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/tcp terbuka, Port 22 adalah port standar untuk SSH (Secure Shell). Port ini berfungsi mengirimkan data melalui jaringan dalam bentuk terenkripsi. Dapat digunakan untuk menjalankan fungsi atau tugas yang bisa diakses dari jarak jauh, misalnya menghubungkan ke host atau server.
    - Port 53/tcp terbuka, Port 53 adalah jenis port untuk DNS yang berfungsi sebagai penerjemah alamat IP pada setiap host. Port ini mencocokkan nama domain yang dapat dibaca manusia dengan alamat IP yang dapat dibaca mesin.
    - Port 80/tcp terbuka Port 80 berfungsi untuk HTTP, yakni memungkinkan browser terhubung ke halaman web. Port ini akan menerima permintaan koneksi dari klien, kemudian setelah koneksi berhasil dibuat, kamu akan mendapat akses ke berbagai halaman web di internet. HTTP/ web server juga memiliki port alternatif, yaitu port 8080 dan 80.
    - Port 9929/tcp terbuka, Port TCP 9929 menggunakan Protokol Kontrol Transmisi. TCP adalah salah satu protokol utama dalam jaringan TCP/IP. TCP adalah protokol yang berorientasi pada koneksi, memerlukan jabat tangan untuk mengatur komunikasi ujung ke ujung. Hanya ketika koneksi telah diatur, data pengguna dapat dikirim dua arah melalui koneksi.
    - Port 31337/tcp terbuka, Nomor port ini berarti "elit" dalam ejaan peretas/cracker (3 = E, 1 = L, 7 = T) dan karena artinya yang khusus sering digunakan untuk hal-hal yang menarik... Banyak backdoor/trojan yang berjalan di port ini, yang paling terkenal adalah Back Orifice.
- Berapa alamat IP server?

  Alamat IP server adalah 45.33.32.156
- Apa sistem operasi yang digunakan oleh server?

  Sistem operasi yang digunakan adalah linux, Linux adalah jenis operating system (OS) yang bersifat open source sekaligus gratis. Salah satu kelebihan sistem operasi Linux adalah kamu bisa menggunakan dan mengembangkannya dengan bebas. Biasanya, OS ini dimanfaatkan dalam pengembangan perangkat. Berbeda dengan Windows yang menyasar user dan pemula.

F. Kesimpulan

Kesimpulan yang didapat dari praktikum ini adalah:

1. Port Scanning adalah aktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah mesin.
2. Hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya.
3. Pada intinya, melakukan port scanning ialah untuk mengidentifikasi port-port apa saja yang terbuka, dan mengenali OS target.

G. Daftar Pustaka

Ni Gusti Ayu Putri Valencia, Valentina. *Pengertian NMAP, Fungsi dan Cara Kerjanya.* Diakses pada 26 Februari 2023. https://dosenit.com/software/network-mapper

Shinta, Amelia. 2022. *Pengertian Port, Jenis, dan Fungsinya pada Jaringan Komputer.* Diakses pada 26 Februari 2023. https://www.dewaweb.com/blog/apa-itu-port/#Penomoran_Port

Fithroni. Wildan. 2016. *Pengertian Port Scanning jenisnya & Perintahnya.* Diakses pada 26 Februari 2023. https://wildanfithroni.blogspot.com/2016/08/pengertian-port-scanning-jenisnya.html