

Nama : Riki Andika NIM : 09011181320015
--

Network scanner adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network target yang akan dicari titik kelemahannya. Cara kerja network scanner adalah sebagai berikut;

- Untuk mendapatkan akses ke host, harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, sudah mengetahui bahwa host menjalankan proses ftp server, ia dapat menggunakan kelemahan-kelemahan yang ada pada ftp server untuk mendapatkan akses.
- Biasanya scanning dijalankan secara otomatis mengingat scanning pada multiple-host sangat menyita waktu. Informasi dari hasil scanning ini sangatlah dibutuhkan sebagai bahan acuan untuk menyiapkan serangan yang akan dilancarkanya atau diberikan.

Scanner biasanya bekerja dengan men-scan port TCP /IP dan servis servisnya dan mencatat respon dari komputer target. Dari scanner ini dapat diperoleh informasi mengenai port-port mana saja yang terbuka. Kemudian yang dilakukan adalah mencari tahu kelemahan-kelemahan yang mungkin bisa dimanfaatkan berdasar port yang terbuka dan aplikasi serta versi aplikasi yang digunakan. Berikut hasil dari scanning yang telah dilakukan;

```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans
-----
nmap -T4 -A -v polsri.ac.id

Starting Nmap 6.46 ( http://nmap.org ) at 2017-02-22 18:31 SE Asia Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 18:31
Scanning polsri.ac.id (202.9.69.34) [4 ports]
Completed Ping Scan at 18:31, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:31
Completed Parallel DNS resolution of 1 host. at 18:31, 11.04s elapsed
Initiating SYN Stealth Scan at 18:31
Scanning polsri.ac.id (202.9.69.34) [1000 ports]
Discovered open port 80/tcp on 202.9.69.34
Discovered open port 8254/tcp on 202.9.69.34
Completed SYN Stealth Scan at 18:31, 20.89s elapsed (1000 total ports)
Initiating Service scan at 18:31
Scanning 2 services on polsri.ac.id (202.9.69.34)
Completed Service scan at 18:32, 5.05s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against polsri.ac.id (202.9.69.34)
Retrying OS detection (try #2) against polsri.ac.id (202.9.69.34)
Initiating Traceroute at 18:32
Completed Traceroute at 18:32, 0.05s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 18:32
Completed Parallel DNS resolution of 2 hosts. at 18:32, 11.04s elapsed
NSE: Script scanning 202.9.69.34.
Initiating NSE at 18:32
NSE Timing: About 62.50% done; ETC: 18:33 (0:00:30 remaining)
Completed NSE at 18:34, 126.29s elapsed
Nmap scan report for polsri.ac.id (202.9.69.34)
Host is up (0.035s latency).
rDNS record for 202.9.69.34: www.polsri.ac.id
Not shown: 972 closed ports, 26 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http?
|_http-favicon: Unknown favicon MD5: D5C9EF97A509D6AB390815A1A16229B1

```

```

8254/tcp open unknown
Aggressive OS guesses: Linux 2.6.18 (96%), Linux 2.6.9 - 2.6.27 (95%), Linux 2.6.9
- 2.6.18 (93%), Linux 2.6.15 - 2.6.30 (93%), Linux 2.6.22 (93%), Linux 2.6.8 -
2.6.27 (93%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (93%), Linux 2.6.15 (likely TP-
Link WAP) (93%), Ruckus ZD1050 WAP (93%), Linux 2.6.5 (SUSE Enterprise Server 9)
(93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 12.817 days (since Thu Feb 09 22:57:43 2017)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=247 (Good luck!)
IP ID Sequence Generation: All zeros

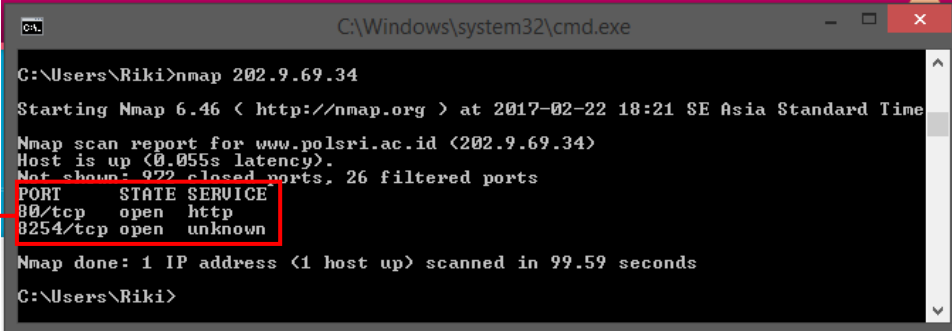
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 3.00 ms 10.94.16.1
2 2.00 ms www.polsri.ac.id (202.9.69.34)

NSE: Script Post-scanning.
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://
nmap.org/submit/ .

```

Gambar 1. Output NMAP 1

Berikut cara untuk mengetahui PORT yang terbuka menggunakan command Prompt, dengan menjalankan perintah nmap 202.9.69.34 dengan output yang dihasilkan sebagai berikut;



```

C:\Windows\system32\cmd.exe
C:\Users\Riki>nmap 202.9.69.34
Starting Nmap 6.46 < http://nmap.org > at 2017-02-22 18:21 SE Asia Standard Time
Nmap scan report for www.polsri.ac.id (202.9.69.34)
Host is up (0.055s latency).
Not shown: 972 closed ports, 26 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
8254/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 99.59 seconds
C:\Users\Riki>

```

Gambar 2. Hasil dari nmap 202.9.69.34

Hasil dari perintah nmap 202.9.69.34 (alamat IP target) merupakan perintah untuk melihat PORT yang terbuka pada alamat IP 202.9.69.34 (www.polsri.ac.id), hasilnya menunjukkan bahwa ada dua PORT yang terbuka, yakni PORT 80/TCP dengan service HTTP dan PORT 8254/TCP dengan service yang tidak diketahui.

PORT 80 merupakan port default yang digunakan untuk membentuk hubungan antara klien dan server yang menggunakan HTTP untuk menerima permintaan, kemudian server menjawab dengan baris status dan pesan. Sedangkan PORT 8254 menggunakan TCP (*Transmission Control Protocol*) merupakan salah satu protokol utama dalam jaringan TCP / IP. TCP merupakan protokol berorientasi koneksi, memerlukan handshaking untuk mengatur komunikasi end-to-end. Hanya bila sambungan diatur data pengguna dapat dikirim lebih terarah melalui koneksi tersebut.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Riki>nmap -sF 202.9.69.34

Starting Nmap 6.46 < http://nmap.org > at 2017-02-22 18:37 SE Asia Standard Time

Nmap scan report for www.polsri.ac.id <202.9.69.34>
Host is up <0.018s latency>.
All 1000 scanned ports on www.polsri.ac.id <202.9.69.34> are open/filtered

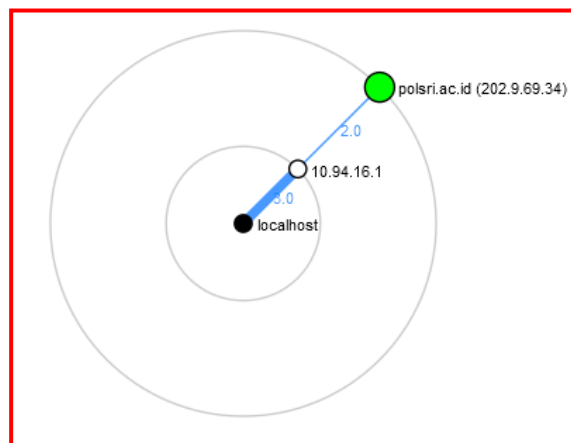
Nmap done: 1 IP address <1 host up> scanned in 19.24 seconds

C:\Users\Riki>

```

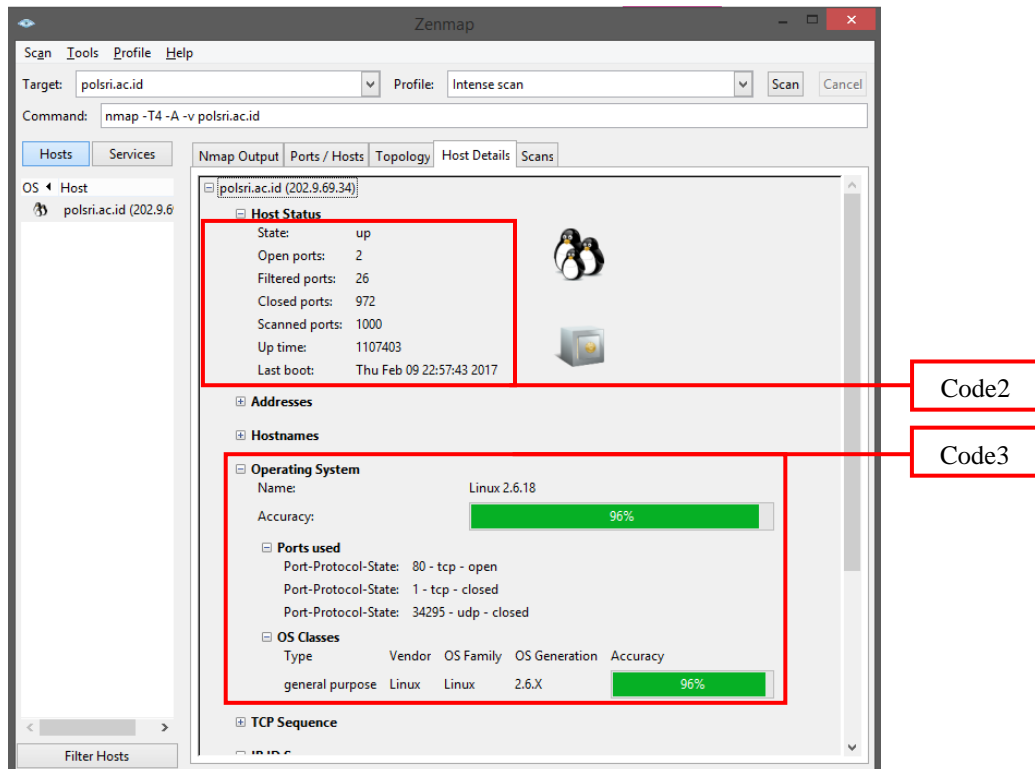
Gambar 3. Perintah nmap -sF 202.9.69.34

Teknik ini mengirim suatu paket FIN ke port sasaran. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk setiap port yang tertutup. Teknik ini hanya dapat dipakai pada stack TCP/IP berbasis UNIX. Berikut lompatan hops atau topologi yang dilalui untuk sampai ke alamat tujuan, dengan dua loncatan dari IP pengguna, dapat dilihat pada Gambar 4, sebagai berikut;



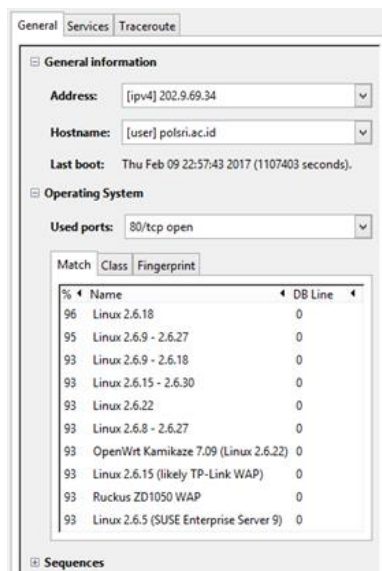
Gambar 4. Topology tracer route yang dilalui

Hasil yang didapat juga mengenai detail host yang digunakan untuk beroperasi, mulai dari sistem operasi yang digunakan, detail PORT yang ada (PORT terbuka, PORT tertutup), serta PORT yang sedang digunakan sekarang, lebih detailnya terdapat pada gambar 5.



Gambar 5. Host detail dari website www.polsri.ac.id

Pada Gambar 3 dilihat jumlah PORT yang ada pada website dengan alamat domain www.polsri.ac.id berjumlah 1000 PORT yang terbaca dengan menggunakan tools NMAP, dengan jumlah PORT yang tertutup sebanyak 972, PORT terbuka sebanyak 2 PORT, dan PORT yang tersaring berjumlah 26 PORT (Code2). Dengan menggunakan sistem operasi Linux 2.6.18, dan ada tiga PORT yang sedang digunakan, yakni PORT 80/tcp, PORT 1/tcp, dan PORT 34295/udp, dengan keakurasian data yang diperoleh sebesar 96%, maka dapat disimpulkan bahwa data diatas benar-benar valid (Code3).



Gambar 6. Hosts Viewer

Berikut hasil scanning menggunakan tools online dengan nama situs upguard (<https://app.upguard.com/webscan?url=http%3A%2F%2Fwww.polsri.ac.id%2F>) yang menghasilkan grafik penggunaan dari website tersebut.



Gambar 7. Hasil scanning dengan tools online upguard

Deteksi dengan menggunakan SYN scan juga susah terdeteksi, karena tidak menggunakan 3 way handshake secara lengkap, yang disebut sebagai teknik half open scanning. SYN scan juga efektif karena dapat membedakan 3 stat port, yaitu open, filterd ataupun close. Teknik ini dikenal sebagai half-opening scanning karena suatu koneksi penuh TCP tidak sampai terbentuk. Sebaliknya, suatu paket SYN dikirimkan ke port sasaran. Bila SYN/ACK diterima dari port sasaran, kita dapat mengambil kesimpulan bahwa port itu berada dalam status LISTENING, dengan tampilan sebagai berikut;

```
C:\Windows\system32\cmd.exe
C:\Users\Riki>nmap -sS 202.9.69.34
Starting Nmap 6.46 < http://nmap.org > at 2017-02-22 20:25 SE Asia Standard Time
Nmap scan report for www.polsri.ac.id (202.9.69.34)
Host is up (0.052s latency).
Not shown: 972 closed ports, 26 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
8254/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 30.96 seconds
C:\Users\Riki>
```

Gambar 8. Hasil dari proses SYN

Hasil CVE dari website www.polsri.ac.id

