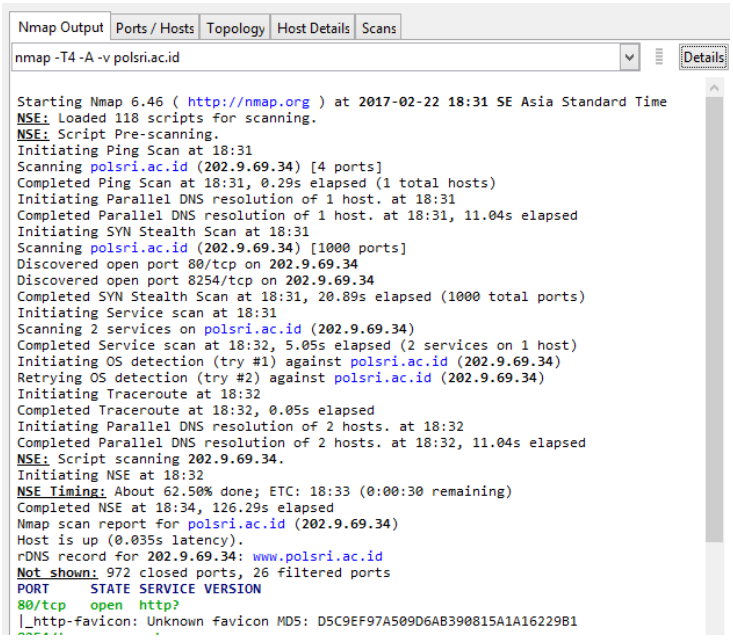
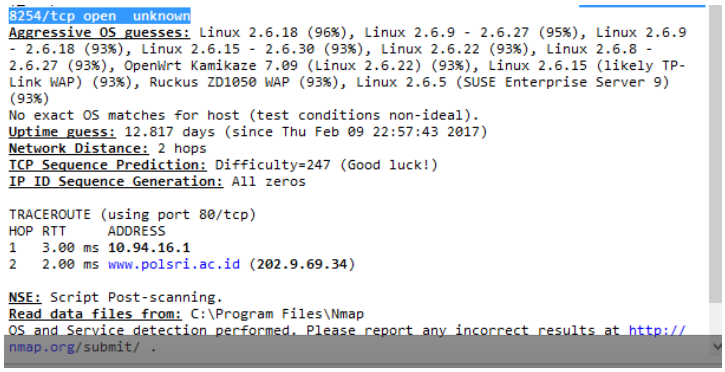
Nama : Riki Andika
NIM : 09011181320015

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;

a. 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.
b. 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 dilancarkannya atau diberikan.

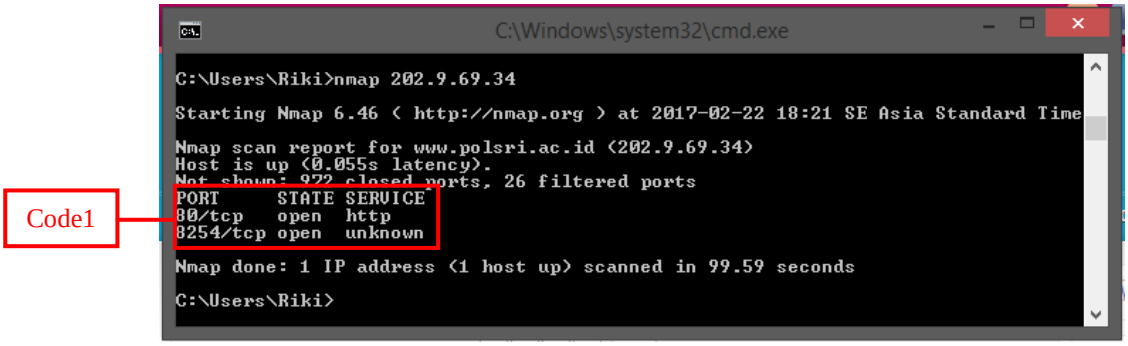
Scanner biasanya bekerja dengan men-scan port TCP /IP dan servis servisnya dan mencatat respon dari komputer target. Dari scanner ini dapat diperoleh informasi mengenai port-port mana saja yang terbuka. Kemudian yang dilakukan adalah mencari tahu kelemahan-kelemahan yang mungkin bisa dimanfaatkan berdasar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





Gambar 1. Output NMAP 1

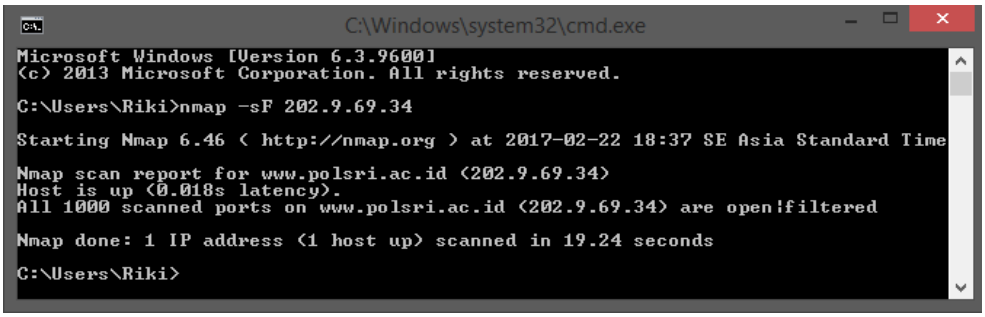
Berikut cara untuk mengetahu PORT yang terbuka menggunakan command Prompt, dengan menjalankan perintah nmap 202.9.69.34 dengan output yang dihasilkan sebagai berikut;



Gambar 2. Hasil dari nmap 202.9.69.34

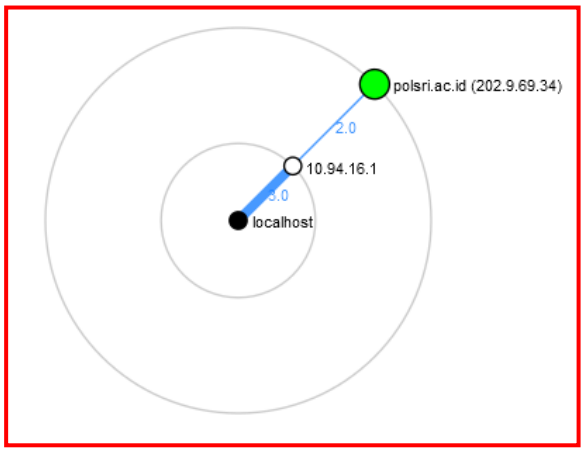
Hasil dari perintah nmap 202.9.69.34 (alamat IP target) merupakan peritah untuk meliha PORT yang terbuka pada alamat IP 202.9.69.34 (www.polsri.ac.id), hasilnya menunjukkan bahwa ada dua PORT yang terbuka, yakni PORT 80/TCP dengan service HTTP dan PORT 8254/TCP dengan service yag tidak diketahui.

PORT 80 merupakan port default yang digunakan untuk membentuk hubungan antara clien 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.



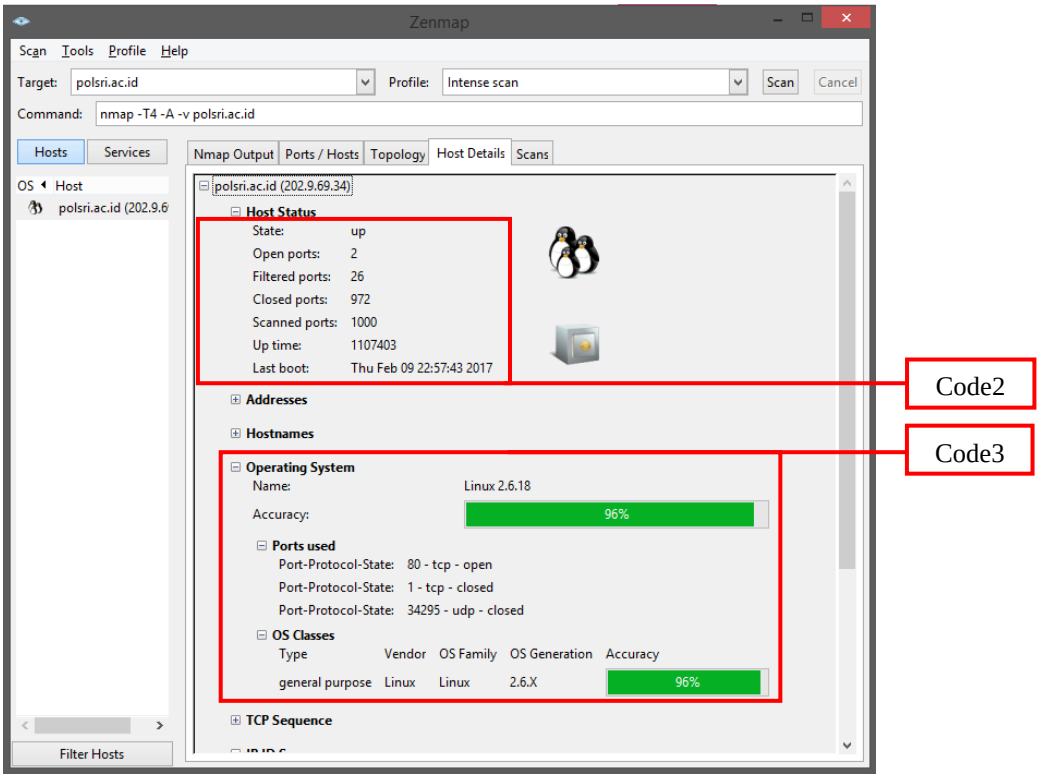
Gambar 3. Perintah nmap –Sf 202.9.69.34

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;



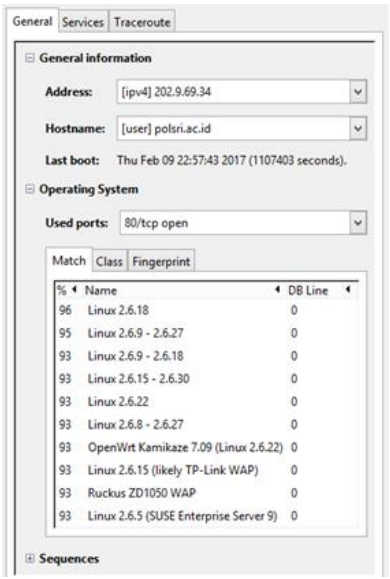
Gambar 4. Topology tracer route yang dilalui

Hasil yang didapat juga mengenai detail host yang digunakan untuk beroperasi, mulai darri sistem operasi yang digunaka, 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 keaukrasian data yang diperoleh sebesar 96%, maka dapat disimpulkan bahwa data diatas benar-benar falid (Code3).

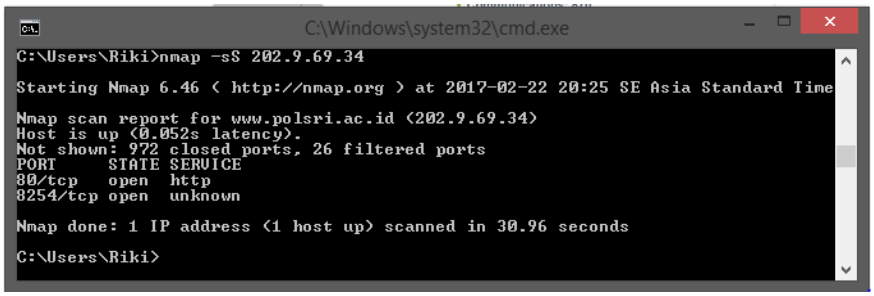


Gambar 6. Hosts Viewer

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 mengguanakan 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;



Gambar 8. Hasil dari proses SYN

Hasil CVE dari website www.polsri.ac.id