TCP PORT SCANNER

Deskripsi

^ kembali ke atas ^

TCP Port Scanner yang dibuat berfungsi untuk mengecek apakah suatu port dari service dapat diakses atau tidak. Cara yang diterapkan adalah dengan melakukan TCP-scan, yaitu menginisiasi koneksi ke suatu pasangan IP:Port dan melakukan *three-way handshake connection*. Jika agen mendapat sinyal kembalian (ACK) dari IP:Port, koneksi segera diputus dengan sinyal RST. Koneksi yang dibuat adalah koneksi TCP non-blocking dengan timeout yang diatur dalam file konfigurasi. Pengembangan dilakukan dalam OS Ubuntu 18.04 (Bionic Beaver). Program dibuat dalam bahasa C.

Dokumen

^ kembali ke atas ^

Nama	Deskripsi
port_scanner.c	fungsi utama.
portsc.c	fungsi yang digunakan dalam scanning, parsing dan konstruksi (JSON, XML).
portsc.h	header untuk fungsi portsc.c.
config.xml	dokumen konfigurasi.

Batasan

^ kembali ke atas ^

1. CentOS/Ubuntu (12.04).
2. IP:Port yang dicek harus dalam 1 subnet dengan Agen.
3. Pengiriman informasi dikirim melalui port 10000 (*hardcoded* pada *portsc.c*).

Kebutuhan

^ kembali ke atas ^

1. GCC (C Compile).

2. Text Editor (untuk mengatur dokumen konfigurasi).

Instalasi

^ kembali ke atas ^

1. *Download* seluruh dokumen, tempatkan *portsc.c*, *portsc.h*, dan *port_scanner.c*.
2. Buat *object* untuk *portsc.c*.

```
gcc -c portsc.c -o portsc.o
```

3. Buat *agent* dengan meng-*compile port_scanner.c* dengan me *link portsc.o*.

```
gcc portscanner.c portsc.o -o __nama_agent__
```

contoh:

```
gcc portscanner.c portsc.o -o port_scanner
```

4. *File* yang dihasilkan akan menjadi agen, tempatkan agen pada *endpoint* yang memiliki *subnet* yang sama dengan **IP:PORT** yang mau di-*scan*.

Konfigurasi

^ kembali ke atas ^

Konfigurasi dapat diatur pada *config.xml* dengan struktur:

```
<root>
  <server_address>__alamat_penerima__</server_address>
  <timeout>___waktu_timeout__</timeout>
  <service>
    <address>__alamat_service__</address>
    <port>__nomor_port__</port>
  </service>
  <service>
    <address>__alamat_service__</address>
    <port>__nomort_port__</port>
  </service>
</root>
```

Keterangan Variable | Deskripsi — | — **alamat__penerima** | ip *endpoint* untuk pengiriman informasi hasil pengecekan **timeout** | batas waktu menunggu respon dari pengecekan setiap PORT **alamat__service** | ip *service* yang akan di-*scan* **nomor__port** | port *service* yang akan di-*scan*

Untuk menambahkan **IP:PORT** yang akan di-*scan*, tambahkan bagian seperti berikut seletah `</service>` terakhir.

```
<service>
  <address>__alamat_service__</address>
  <port>__nomort_port__</port>
</service>
```

Penggunaan

ˆ kembali ke atas ˆ

Untuk menjalankan (terminal): `./__nama_agen__`

Untuk menjalankan DEBUG_MODE (terminal): `./__nama_agen__ DEBUG`

Catatan

ˆ kembali ke atas ˆ

1. Semua dokumen ini tidak memerlukan **Receiver Socket** yang melakukan *listen* di *port* 10000.
2. Pengiriman ke *server* dilakukan dengan **TCP Blocking Connection**.
3. Kode ini tidak dapat mengecek *local port*.
4. Semua kode ditulis dengan bahasa **C**, namun untuk **Receiver Socket** bisa menggunakan bahasa apapun