Laporan Pendahuluan Praktikum Keamanan Data

Network Scanner & Network Probing

Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

***Overview***

Pada pemrograman berbasis socket, server adalah host yang menyediakan sebuah layanan (service) dan client adalah host yang mengakses atau menggunakan layanan tersebut. Socket sendiri merupakan gabungan dari alamat IP dan nomor port, contohnya adalah penggunaan socket 202.9.85.49:25 (IP address kampus dengan port SMTP 25). Dapat dikatakan juga host dengan IP 202.9.85.3 membuka port nomor 25 untuk menyediakan layanan SMTP.

Layanan jaringan dapat diserang dalam berbagai cara. Aplikasi layanan tersebut pastinya memiliki beberapa kelemahan seperti kesalahan pemrograman, bug, tidak terenkripsinya beberapa data dan lainnya. Kelemahan tersebut memungkinkan host yang menyediakan layanan tersebut sangat rentan terhadap serangan. Oleh karena itu, sebaiknya host hanya menyediakan layanan yang diperlukan saja, atau dengan kata lain meminimalkan port yang terbuka.

***Port Scanner Sebagai Gejala Awal Serangan***

Seperti yang diketahui, kesalahan dalam pemrograman layanan pada port tertentu dapat mengakibatkan serangan yang ditujukan kepada layanan tersebut. Namun bukan karena adanya error pemrograman yang menenggarai adanya serangan, melainkan tereksposnya penggunaan port pada layanan tersebut ke penyerang. Penyerang seringkali melakukan port scanning untuk melakukan scanning terhadap port yang ada, tujuannya adalah untuk melihat mana saja port yang aktif, lalu kelemahan/exploit apa saja yang dapat digunakan oleh penyerang. Contohnya, penyerang melakukan port scanning dan menemukan bahwa port Telnet terbuka, maka penyerang akan mencoba menggunakan kelemahan dari port milik Telnet untuk melakukan serangan. Untuk mengurangi resiko keamanan ini, sebaiknya tidak perlu memasang layanan yang tidak terlalu diperlukan

***Aplikasi Port Scanner***

Nmap (“Netowrk Mapper”) merupakan tool open source untuk melakukan eksplorasi dan audit keamanan jaringan. Nmap menggunakan paket IP raw untuk mendeteksi host yang terhubung dengan jaringan lengkap dengan informasi layanan, sistem operasi, jenis firewall, dan properti lainnya pada sebuah sistem.

Nmap dapat mendeteksi dan melaporkan beberapa informasi pada sebuah sistem, yaitu,

* Nomor port
* Nama layanan,
* Status port, apakah terbuka (open), filtered, tertutup(closed), atau tidak difilter (unfiltered)
* Nama reverse DNS
* Perkiraan versi sistem dan informasi sistem operasi yang digunakan
* Jenis device yang digunakan pada sistem,
* Dan Alamat MAC (Physical Address)

***Beberapa Tipe Scanning pada Nmap***

* Connect scan (-sT)

Jika menggunakan connect scan, nmap akan melakukan scanning port menggunakan metode three-way handshaker (SYN, SYN/ACK, ACK).

* -sS (TCP SYN Scan)

Merupakan scanning default pada konfigurasi nmap. SYN scan sulit terdeteksi karena tidak sampai menggunakan metode three-way handshake secara penuh. Mode scan ini juga dapat membedakan tiga state port yaitu open, filtered atau closed. Cara kerjanya adalah hanya dengan mengirimkan satu packet SYN ke port sasaran, jika port tersebut merespon dengan SYN/ACK, maka port tersebut aktif. Dengan cara seperti ini, nmap akan sulit terdeteksi oleh mesin target.

* TCP FIN scan (-sF)

Dengan mode ini, packet yang dikirimkan ke port sasaran adalah packet FIN. Jika sebuah port yang tertutup dikirimi packet FIN, akan mengirim balik suatu RST, sehingga dapat diketahui port yang dalam state closed

* TCP Xmas Tree scan (-sX)

Metode ini mengirimkan suatu packet FIN, URG dan PUSH ke port sasaran. Sistem akan mengembalikan suatu RST untuk semua port yang tertutup.

* TCP ACK scan (-sA)

Mode ini digunakan untuk memetakan set aturan firewall. Dengan mengetahui aturan firewall tentunya dapat membantu penyerang merencanakan penyerangannya dengan menentukan apakah firewall tu merupakan suatu simple packet filter yang hanya memperbolehkan koneksi tertentu atau suatu firewall yang menerapkan advance packet filtering.

* TCP Window scan

Mode ini dapat mendeteksi port yang terbuka atau tertutup maupun yang terfilter atau tidak terfilter pada suatu sistem, sehubungan dengan anomali dari ukuran window TCP yang dilaporkan