**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 03**

**Basic tools for exploiting vulnerability**

1. **Port pada TCP/IP**

Didalam dunia networking dan internet kita sering mendengar kata port. Sebenarnya apa yang dimaksud dengan port ini? Dalam dunia computer ada dua jenis port yaitu port physical dan port logical. Port physical dapat kita lihat secara fisik, misalnya port USB adalah tempat dimana untuk membuat koneksi antara computer dengan perangkat lain yang dapat dihubungkan melalui port USB ini. Selain itu kita juga bisa melihat port HDMI, port serial dan sebagainya. Semua port ini berguna untuk menghubungkan computer dengan perangkat lainnya.

Port logical tidak dapat kita lihat, tetapi fungsi utamanya adalah sama yaitu untuk menghubungkan antara satu object dengan object yang lainnya. Dalam hal ini adalah menghubungkan antara computer atau operating system dengan aplikasi, servis atau software. Misalnya, kita mempunyai computer dengan operating system linux dan kita ingin membuat computer kita ini sebagai web server, untuk itu kita harus menginstall software apache pada computer kita. Tujuan dari mengintall apache ini adalah supaya webserver ini bisa terhubung ke dunia luar melalui internet. Untuk mengkoneksikan server ini dengan dunia luar maka perlu adanya port. By default, setelah menginstall apache maka port 80 akan terbuka sebagai tempat koneksi dengan dunia luar melalui internet. Dengan menginstall apache untuk web server berarti kita membuka port 80. Bagaimana kalau kita ingin menutup port 80? Dengan meng-uninstall apache tersebut berarti kita menutup port 80. Kadang kadang kita juga mendengar port yang terbuka harus ditutup untuk menjaga keamanan. Ini artinya adalah kita harus meng-uninstall aplikasi apalikasi yang tidak kita gunakan. Dengan pengertian ini maka semakin banyak aplikasi atau service yang terinstall pada computer berarti semakin banyak port yang dibuka.

Nomor dari port dimulai 0 sampai 65536 atau sejumlah 16 bit dan dibagi menjadi tiga kelompok, yaitu:

1. Well known port: pada kelompok ini menggunakan nomor port antara 0 sampai 1023. Yang masuk kelompok ini adalah port port yang sering digunkan dan sudah terdaftar di IANA (Internet Assigned Number Authority).
2. Registered Port: nomor yang digunakan antara 1024 sampai 49151. Nomor port pada range ini digunakan oleh perusahaan besar yang berhubungan atau memproduksi alat jaringan, operating system atau aplikasi yang sudah dipake luas.
3. Dynamically Assigned Port: sisa dari port yang tersedia masuk dalam kelompok ini. Port ini dapat digunakan sesuai dengan kebutuhan kita.

Untuk lebih mengerti tentang aspek teknik dari port ini dapat mengunjungi website dibawah ini: <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>

1. **Scanning Tools**

Scanning tools adalah alat utama dari seorang hacker. Ada banyak jenis scanning tool baik yang dapat di download secara gratis di internet dan juga yang harus dibeli dengan harga yang cukup mahal. Dalam hal ini kita bisa bagi dua jenis scanning tool yaitu port scanning dan vulnerability scanning.

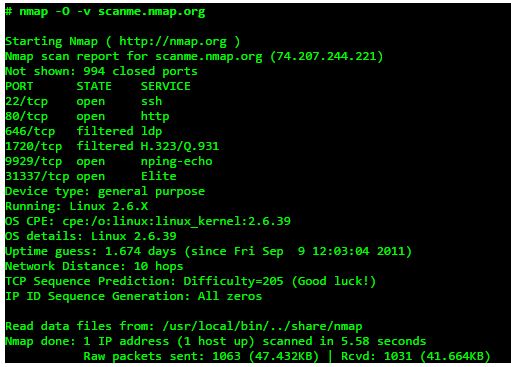
Port scanning adalah tool atau software yang digunakan untuk mengetahui port mana saja yang terbuka. Di dalam computer jumlah port yang tersedia ada 65535 buah port. Nomor dari port ada ditulis dalam packet header terdiri dari 16 bit. Port adalah berhubungan dengan service atau applikasi. Sehingga apabila kita mengatakan scanning port untuk mengetahui port mana saja yang terbuka, kita dapat artikan scanning untuk mengetahui aplikasi atau service apa saja yang terinstall pada computer yang di scan. Setelah attacker mengetahui service atau aplikasi yang terinstall pada computer target maka selanjutnya attacker akan mencari vulnerability atau kerentanan dari service atau aplikasi yang terinstall pada computer tersebut.

Port scanning dapat dilakukan dengan menggunakan three way handshake, yaitu mengirimkan paket SYN kepada setiap nomor port mulai dari port nomor 0 sampai port nomor 65535. Teknik ini disebut “SYN Scan”. Jika port meresponds atau membalas dengan packet SYN-ACK maka disimpulkan port tersebut terbuka. Tetapi bila port tertutup maka akan dibalas dengan paket RST.

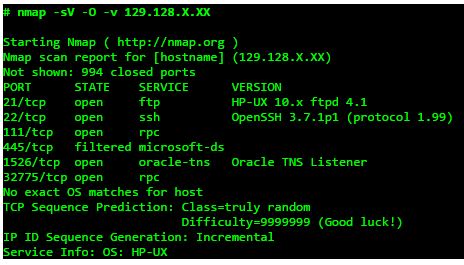
Salah satu tool yang paling terkenal adalah nmap (Network Mapper) yang merupakan open source dan dapat di download secara gratis pada nmap.org. Berikut adalah screenshot dari penggunaan nmap untuk melihat open port dan juga operating system dari computer dengan menggunakan #nmap –O –v scanme.nmap.org seperti pada gambar 1. Option penggunaan nmap sangat banyak, contoh lainnya dalam penggunaan nmap adalah dengan menggunakan #nmap –sV –O –v 129.128.x.xx seperti pada gambar 2. Berikut adalah beberapa arti dari perintah pada nmap yang diambil dari nmap.org.

-sS (TCP SYN Scan)

SYN scan adalah default dan pilihan paling populer untuk melakukan port scanning. Hal ini dapat dilakukan dengan cepat, memeriksa ribuan port per detik pada jaringan yang cepat yang tidak dihalangi oleh firewall yang membatasinya. Hal ini juga relatif tidak mengganggu dan tersembunyi karena ia tidak pernah melengkapi koneksi TCP.



Gambar 1. Penggunaan scan domain #nmap –O –v scanme.nmap.org



Gambar 2. Penggunaan scan IP address #nmap –sV –O –v 129.128.x.xx.

Teknik ini sering disebut scanning setengah terbuka (half open scanning), karena Anda tidak membuka koneksi TCP penuh. Anda mengirim paket SYN, seperti jika Anda akan membuka hubungan nyata dan kemudian menunggu tanggapan. A SYN / ACK menandakan port sedang mendengarkan (open), RST (reset) merupakan indikasi dari non-pendengar (closed). Setelah penerima paket SYN/ACK maka tidak perlu mengirimkan ACK (yang seharusnya mengirim paket ACK pada koneksi normal), oleh karena itu teknik ini disebut half open scanning.

-sT (TCP connect scan)

TCP connect scan adalah default TCP scan apabila SYN scan tidak mau atau tidak dapat digunakan. Ketika SYN scan bisa digunakan, biasanya SYN scan adalah pilihan yang lebih baik. Sistem call membuat koneksi lengkap untuk mendeteksi port target, tidak seperti half open scan yang dilakukan SYN scan. Hal ini tidak hanya memakan waktu lebih lama dan membutuhkan lebih banyak paket untuk memperoleh informasi yang sama, tapi mesin target kemungkinan mencatat koneksi. Teknik TCP connect scan dapat dideteksi oleh IDS, namun kebanyakan mesin tidak memiliki sistem alarm tersebut.

-sN; -sF; -sX (NULL, FIN, and Xmas scan)

Ketiga jenis scan ini mengeksploitasi kelemahan dalam TCP RFC untuk membedakan antara port terbuka dan tertutup. Halaman 65 dari RFC 793 mengatakan bahwa "jika [tujuan] port TERTUTUP .... paket masuk yang tidak mengandung RST menyebabkan RST akan dikirim untuk merespon." Oleh karena itu, berikutnya mendiskusikan paket yang dikirim untuk open port tanpa SYN, RST, atau ACK flag, menyatakan bahwa: you are unlikely to get here, but if you do, drop the segment, and return.”

Ketika scanning sistem compliant dengan teks RFC ini, setiap paket yang tidak mengandung SYN, RST, atau ACK bit akan menghasilkan RST jika port tertutup dan tidak ada respon sama sekali jika port terbuka. Selama tidak satupun dari mereka tiga bit disertakan, kombinasi dari tiga lainnya (FIN, PSH, dan URG) adalah OK. Nmap mengeksploitasi celah ini dengan tiga jenis scan:

Null scan (-sN)

Does not set any bits (TCP flag header is 0)

FIN scan (-sF)

Sets just the TCP FIN bit.

Xmas scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Jenis scanning yang kedua adalah vulnerability scanning. Scanning jenis ini adalah untuk memeriksa semua kerentanan yang ada pada system kita, baik aplikasinya maupun system operasinya. Jadi vulnerability scanner adalah program komputer yang dirancang untuk mencari kelemahan atau kerentanan dari komputer, sistem komputer, jaringan atau aplikasi komputer. Sederhananya, scanner ini digunakan untuk menemukan titik lemah atau bagian buruk dari system yang dibangun atau yang digunakan. Sederhananya, scanner ini digunakan untuk menemukan titik lemah atau bagian buruk dibangun. Vulnerability scanner dapat dijalankan baik sebagai bagian dari manajemen kerentanan oleh mereka yang bertugas melindungi sistem atau oleh penyerang topi hitam untuk mencari atau untuk mendapatkan akses secara tidak sah. Menurut owasp.org, aplikasi Web Vulnerability Scanner adalah sebuah alat otomatis yang dapat men-scan aplikasi web, biasanya dilakukan dari luar network, untuk mencari kerentanan keamanan seperti Cross-site scripting, SQL Injection, Command Injection, Path Traversal dan konfigurasi server yang tidak aman. Tool tool ini sering juga disebut sebagai Dynamic Application Security Testing (DAST) Tools. Sejumlah besar kedua alat ada yang dijual secara komersial dan juga bisa didapat secara free atau open source.

**SIMPULAN**

1. Port dalam dunia internet berhubungan dengan aplikasi atau services
2. Port merupakan salah satu jalan untuk mengirimkan coding yang jahat
3. Scanning port dapat dilakukan dengan menggunakan tool yang tersedia di internet

**DAFTAR PUSTAKA**

1. Stallings, William. (2006). Cryptography and Network Security. 4th edition. Pearson Education.Whitman, M.E., Mattoro, H.J. (2013).
2. Scambray, Joel; Liu, Vincent; Sima, Caleb. (2011). Hacking Exposed Web Applications: Web Application Security Secrets and Solutions. 3rd Edition. McGraw-Hill. ISBN: 9780071740647.