

Published based on [Apa Itu Port Scan? Haruskah Saya Khawatir?](#)

Apa Itu Port Scan? Haruskah Saya Khawatir?

Port scan terjadi setiap saat. Maksudnya setiap saat, setiap detik terjadi di internet. Mungkin anda mengenal istilah "*internet background radiation*" yang mengacu pada *traffic* jaringan di internet yang terjadi secara acak dan terjadi terus menerus yang diakibatkan mesin-mesin (komputer) terinfeksi dan tidak "teramankan", dan juga berasal dari mesin lainnya yang terus men-scan internet untuk mencari komputer lain yang bisa diinfeksi.

Itu sebabnya kenapa semua pengguna internet membutuhkan firewall.

Beberapa jenis celah pada sistem operasi/OS (Windows, Mac, Linux - urutan bukan berdasarkan preferensi :)) yang anda gunakan- terutama yang lama tidak diupdate - membuat komputer lain dapat terhubung langsung pada komputer anda dan mengambil alih kendali.

Dulu arti "mengambil alih ini" ini selalu menyebabkan masalah yang terlihat jelas; menghapus data, membuat komputer *hang*, dan berbagai hal serupa lainnya. Sekarang semuanya lebih tersembunyi. Komputer yang tercemar seringkali tidak menunjukkan tanda-tanda terinfeksi, tapi sebenarnya komputer tersebut siap digunakan untuk mengirimkan *spam* atau melakukan *scanning* untuk mencari korban berikutnya tanpa anda sebagai pemilik atau pengguna sadari.

Komputer yang terinfeksi ini biasanya memilih sebuah *IP address* (alamat mesin di internet), dan mencoba membuat koneksi dengan mesin lainnya yang mungkin ada pada IP tersebut. Mencoba mendeteksi berbagai port pada komputer calon korban, terutama port-port yang memang diketahui memiliki berbagai celah keamanan yang dapat ditembus, dan melihat bagaimana reaksi komputer korban. *Port scan* pada dasarnya adalah upaya dari satu komputer yang mencoba mendeteksi adanya "kebocoran" yang dapat dieksploitasi pada komputer lainnya.

Sebuah *firewall* baik dari jenis *software* maupun *hardware* memegang peranan penting dalam mengamankan situasi ini. *Firewall*, terutama yang jenis *hardware* seperti *router*, dapat mencegah upaya *port scan* agar tidak dapat menjangkau komputer yang dilindunginya.

Jadi selama komputer anda terlindung oleh *firewall* dan OS-nya selalu *up to date* maka keamanan anda relatif terjamin. Walaupun *port scan* dan deteksi kelemahan terjadi setiap saat, anda bisa bernapas lega kalau berada di balik sebuah *firewall*.

Namun seperti yang kita tahu, jaman sekarang metode *port scan* seperti di atas bukan satu-satunya cara mengambil alih komputer anda. *Attachment* yang terinfeksi, dan metode *phishing via email*, bukanlah hal yang dapat dihentikan oleh *firewall*. Jadi *firewall* sendiri tidak cukup, namun tetap memegang peranan penting dalam mengamankan sistem anda.

Ada teman yang menanyakan :

"Mengapa setiap saya menyalakan komputer saya selalu mencoba mengirim paket UDP ke sebuah IP dari Chinanet?"

Hmm... ada yang nggak beres nih.

Pastikan bahwa *firewall* anda memang kira-kira memberi pesan seperti itu, karena pesan dari komputer seringkali salah diinterpretasikan, terutama oleh orang awam. Tapi kalau memang komputer anda mencoba menghubungi sebuah *IP address* di Cina tanpa anda harapkan, ketahui, atau inginkan - *well, that's not good*. Apa yang dilakukan komputer anda bukan aktivitas *port scan* (menerima dari luar), namun lebih berupa "infeksi" yang sudah menyerang, mencoba "menelpon balik ke rumahnya" dan memberitahu komputer di seberang sana bahwa komputer anda sudah terinfeksi dan siap untuk menerima instruksi selanjutnya.

Seringkali *anti virus* juga tidak mendeteksi adanya infeksi, terutama bila anda jarang meng-update *anti virus* yang digunakan.

Seperti yang sudah saya bilang, yakinkan apa yang diberitahukan oleh *firewall* anda. Upaya koneksi masuk yang

berhasil diblok tidak perlu terlalu dirisaukan. Namun adanya upaya koneksi keluar yang tidak anda harapkan, itu baru masalah.

Kalau saya jadi anda, saya akan cepat melakukan *backup data*, dan melakukan scan *anti virus* dan *anti spyware* tambahan dari vendor yang berbeda dari yang saat ini saya gunakan. Saya tekankan bahwa scan *anti spyware* diperlukan selain scan *anti virus*. Karena virus dan *spyware* memang tidak sama dan *scanner* nya pun tidak sama cara kerjanya.

Dengan cara tersebut, diharapkan masalah kebocoran dapat ditanggulangi.

Kalau tidak, setidaknya selama *firewall* dapat mencegah *outbound connection* yang tidak diharapkan, maka secara teknis aman-aman saja, namun saya pribadi tidak bisa merasa tenang, terutama karena tidak tahu kenapa komputer saya bisa terinfeksi.

You can also find this article published on [Apa Itu Port Scan? Haruskah Saya Khawatir?](#), and on the tag pages [Computer](#), [Firewall](#), [Hardware](#), [Software](#), [Virus](#).