Network Attacks

Bayu Krisna, Jim Geovedi
{krisna,jim}@corebsd.or.id

1 Pendahuluan

Tulisan ini bertujuan untuk memberikan penjelasan mengenai network attacks, bagaimana sebuah attacks bisa terjadi dan bagaimana tren attacks network saat ini. Keamanan dari sebuah network merupakan suatu kebanggaan bagi perusahaan yang memiliki nilai keamanan yang tinggi. Hal ini tidak hanya berhubungan dengan kerugian materi yang ditimbulkan oleh kerusakan pada network baik device maupun data, tetapi sudah berhubungan dengan nama baik sebuah perusahaan. Banyak perusahaan di Indonesia yang sering kali tidak terlalu memperhatikan permasalahan ini.

Network attacks sendiri jika dikategorikan menurut letak dapat dibagi menjadi dua yaitu network attacks yang berasal dari dalam network itu sendiri dan network attacks yang berasal dari luar network. Sedangkan bentuk network attacks dapat berasal dari sebuah host dan dapat juga berupa sebuah device/perangkat keras yang berhubungan dengan target, sebagai contoh kasus wiretapping. Yang menjadi sasaran atau target dari sebuah attacks dapat berupa host maupun network itu sendiri. Jika diasumsikan bahwa pengamanan terhadap infrastruktur dari sebuah network telah dilakukan, maka yang perlu diwaspadai adalah serangan dari luar network, dimana hanya proteksi saja yang dapat diandalkan untuk menghindari bahaya dari network attacks yang berasal dari luar. Untuk mengetahui bagaimana cara untuk memproteksi sebuah network dari attacks yang berasal dari luar network maka ada baiknya mengetahui apa yang menjadi motifasi adanya sebuah attacks.

1.1 Tujuan Network Attacks

Berdasarkan tujuannya maka network attacks dapat dibedakan menjadi beberapa kategori yaitu:

- *Berbahaya* - Attack terjadi karena seseorang atau sekelompok orang bermaksud untuk melumpuhkan sistem, mencuri atau memodifikasi data dari sebuah network atau memanfaatkan resource yang dimiliki oleh network sistem yang diserang.

- *Tidak Berbahaya* - Attack yang terjadi akibat kelalaian atau ketidak sengajaan seseorang dan tidak sama sekali tidak pernah berniat untuk melakukannya.

Jika dilihat dari tujuan seseorang dalam melakukan attack maka dapat dibedakan menjadi:

- *Kontrol Akses* - Attacker ingin menguasai secara penuh akses pada sebuah target. Attacker dapat melakukan apa saja setelah mendapatkan akses penuh pada sebuah target termasuk didalamnya melangsungkan attack berseri ke target lain.

- *Pemanfaatan Resource* - Attacker ingin memanfaatkan resource yang tersedia pada sistem atau network seperti CPU dan koneksi internet.

- *Pencurian dan Manipulasi Data* - Sistem atau network memiliki data yang diinginkan oleh attacker, data tersebut dapat berupa informasi penting seperti: profil kesehatan seseorang, laporan keuangan, atau rencana kerja sebuah perusahaan.

- *Merusak atau Menghancurkan* - Attacker bermaksud merusak atau menghancurkan sebuah sistem atau network. Biasanya attack yang seperti ini didasarkan oleh alasan personal atau permintaan orang lain.

- *Just for Fun* - Dalam beberapa kasus, seringkali ditemukan attacker hanya bermaksud untuk pamer dikomunitasnya dengan melakukan attack pada sistem atau network yang terkenal.

2 Proses Attacks

Serangan atau attacks pada sebuah network biasanya mempunyai proses atau tahap atau fase yang harus dilalui. Disini kami memberikan tiga buah fase yang dilalui oleh attackers. Fase pertama adalah fase persiapan. Dalam fase persiapan, attacker akan mengumpulkan informasi sebanyak mungkin mengenai target yang menjadi sasaran mereka. Fase kedua adalah fase eksekusi, fase ini merupakan attack yang sebenarnya dimana attacker melangsungkan attack pada sebuah sistem. Antara fase pertama dan fase kedua terkadang ditemui kasus dimana saat fase pertama berlangsung, berlangsung juga fase kedua. Contoh scanning untuk mendapatkan informasi pada sebuah host sama dengan attack pada network yang melingkupinya. Fase ketiga adalah fase akhir yang kami sebut dengan fase post-attack. Fase ketiga merupakan fase akibat dari fase pertama dan fase kedua. Bisa jadi terjadinya kerusakan pada sebuah network, atau dikuasainya sebuah sistem network yang kemudian digunakan kembali oleh attacker untuk melakukan serangan pada sistem network lainnya.

2.1 Fase Persiapan

Efektifitas attacker diukur dalam konteks seberapa jauh attacker melakukan penetrasi pada sistem dan seberapa baik attacker dalam menghindari deteksi dari sistem yang diserang. Hal ini berpengaruh terhadap seberapa banyak data atau informasi mengenai target.

Korespondensi informasi yang didapatkan pada fase ini digolongkan menjadi dua yaitu:

- Informasi Umum Informasi dari sebuah dari sistem, baik kelemahan maupun bagaimana metode yang tepat untuk masuk kedalam host target. Informasi ini dapat juga berupa informasi mengenai konfigurasi sebuah network target, software yang digunakan, users, maupun informasi yang sifatnya personal yang nantinya dapat digunakan dalam menebak password.

- Informasi Sensitif Merupakan informasi yang lebih spesifik dari sebuah target. Jika seorang attacker mendapatkan informasi ini maka attacker akan lebih mudah masuk dalam sistem target.

2.2 Fase Eksekusi

Fase ini merupakan proses yang sebenarnya dimana attacker berusaha untuk melumpuhkan target berbekal dengan informasi yang telah didapatkannya. Jika diasumsikan X adalah attacker yang diartikan sebagai person yang melakukan penyerangan atau sebuah program yang digunakan untuk attack kesebuah target. Sedangkan Y merupakan sasaran attack, yang dapat berupa host, atau network, P merupakan perantara dalam melakukan attack, dalam hal ini nilai P bervariasi.

[skema]

Dalam sebuah network attack, nilai P merupakan variasi dimana semakin besar nilai P, maka semakin lama pula Y akan mengetahui bahwa X lah sebenarnya yang menyerang mereka. Jika nilai P tidak sama dengan nol maka nilai Pn lah yang dianggap sebagai attacker yang menyerang Y. Tahap ini sebenarnya merupakan gabungan dengan tahap berikutnya yaitu Tahap Post Attack. Attack bisa terjadi ketika Y menawarkan layanan/sevices yang digunakan untuk kepentingan komunikasi dengan network/host untuk kepentingan Y dan pada saat itu X dapat memaksakan services yang disediakan tersebut untuk dapat diambil alih. Services yang dimaksudkan disini dibedakan menjadi dua bagian yaitu:

- *Network Level Services* Services yang disediakan oleh sebuah network biasanya berhubungan dengan diteruskan atau tidaknya sebuah paket. Salahnya konfigurasi dalam pengaturan network services merupakan hal yang fatal yang dapat mengakibatkan seluruh host/network yang terdapat didalam network dibawahnya tidak dapat memberikan layanan, dikarenakan jalur komunikasi yang menghubungkan host/network dengan internet terputus, selain itu kesalahan ini juga dapat mengakibatkan attacker mengambil resource dalam network target untuk digunakan dalam attack berikutnya.

- *Host Level Services* Services yang disediakan pada host sangatlah banyak, tergantung dari fungsi sebuah host tersebut. Sebuah host dapat memiliki services yang berfungsi sebagai penyedia layanan web(Web Server), penyedia layanan mail(Mail server), penyedia layanan database, dan banyak lagi layanan lainnya. Pada level ini sebagai seorang administrator sebuah server memperhatikan banyak hal-hal

sebelum attacker mencoba untuk memaksa masuk melalui services yang disediakan dalam sebuah server. Kunci dari segi keamanan berada pada seorang administrator, bagaimana supaya services yang diberikan tetap aman dari X walaupun diketahui bahwa software yang menawarkan layanan tersebut diketahui potensial terhadap attack(chroot() method). Ketika X dapat mengambil alih sebuah host melalui services yang diberikan maka dapat dipastikan services yang dipaksakan tersebut tidak dapat berjalan secara maksimal. Services yang berjalan tidak normal masih masih merupakan level resiko kecil dibandingkan ketika X mencuri dan menyembunyikan sebuah program yang mengirimkan informasi-informasi penting ke X. Kegagalan dalam menangani attack pada level ini merupakan mimpi buruk yang akan menjadikan penyedia layanan tidak dipercaya oleh mereka yang memanfaatkan layanan tersebut.

2.3 Fase Post Attack

Fase post attack merupakan fase setelah terjadinya attack. Sebuah sistem target akan terus menunjukan perubahan-perubahan pada sistemnya bahkan setelah aktivitas attack terjadi. Perubahan-perubahan sistem yang menjadi target bisa dikarenakan attacker memang menginginkan hal itu terjadi dengan tujuan attacker dapat mengambil keuntungan setelah proses attack berhasil. Pencurian data yang berkelanjutan, pemanfaatan resouce target dan banyak hal lain yang merupakan motifasi seorang attacker. Pemanfaatan resource pada sistem bisa saja mengakibatkan target menjadi tertuduh untuk proses attack berikutnya. Pada proses attack gambar diatas sebenarnya sudah diketahui bahwa melalui perantara maka seorang attacker dapat menggunakan target sebagai tempat untuk melangsungkan proses attack pada target berikutnya. Untuk lebih jelasnya dapat dilihat pada gambar dibawah ini dimana Z merupakan target attack berikutnya.

[skema]

Selain pemanfaatan resource ini maka banyak hal lain yang menjadi akibat setelah proses attack berhasil. Jika dilihat dari tujuan dari sebuah proses attack maka dapat dikatakan proses ini merupakan proses dimana tahap pengenapan tujuan dari attack.

3 Tren Network Attack

Dari data CERT/CC (Computer Emergency Response Team/Coordination Center) yang merupakan sebuah organisasi yang , jumlah network attacks yang dilaporkan terus meningkat dua kali lipat dari tahun yang sebelumnya. Hal ini merupakan peringatan bagi kita terutama penyedia services yang menggunakan media network untuk lebih konsen dipermasalahan keamanan network. CERT/CC telah mengamati berbagai aktivitas network attacks sejak tahun 1998 dan berikut merupakan data yang didapatkan dari website CERT/CC yang menunjukan kenaikan dari incidents yang dilaporkan.

[table]

Berdasar dari pengamatan CERT/CC yang telah mengamati network attack sejak tahun 1998, melaporkan bahwa trend network network attack yang terjadi adalah sebagai berikut:

- **Otomatisasi**; Kecepatan Attack Tools. Saat ini tools yang dipergunakan untuk melakukan scanning telah menjadi sangat cepat dan efektif untuk melakukan identifikasi. Ketika tools dapat digunakan tanpa intervensi manusia (mampu berjalan secara otomatis), kerusakan yang mungkin terjadi dapat semakin banyak dan parah. Sebagai contoh: Code Red dan Nimda yang mampu menggandakan diri untuk menyebarluas ke seluruh penjuru dunia dalam kurun waktu kurang dari 18 jam.
- **Peningkatan Kemampuan Untuk Mengelabui Dari Attack Tools**, akan semakin sulit untuk membedakan signatures yang dimiliki oleh attack tools dari terdapat pada network traffic. Attacker dapat menggunakan teknik anti-forensik yang akan membuatnya semakin sulit dideteksi. Terdapat banyak tools umum yang menggunakan protokol seperti IRC (Internet Relay Chat) atau HTTP (HyperText Transfer Protocol) untuk mengirimkan data atau commands dari attacker ke system yang menjadi target. Dalam perkembangannya, attack tools yang dibuat agar dapat bekerja secara otomatis dan mempunyai teknik menyembunyikan diri dan berperilaku yang bermacam-macam, beberapa diantaranya bahkan memiliki kemampuan untuk memperbanyak-diri sehingga tool yang sama akan tampak berbeda pada setiap kondisi.
- **Kecepatan Dalam Mendeteksi Ada-**

nya Vulnerabilities. Jumlah ditemukannya vulnerabilities yang baru selalu meningkat setiap tahunnya, membuat banyak perusahaan akan sulit dalam melakukan proses update terutama jika perusahaan-perusahaan tersebut mempunyai dana yang terbatas untuk melakukan maintenance. Hackers seringkali menemukan vulnerabilities dalam code sebelum vendors dapat membenahinya. Penemuan vulnerabilities yang meningkat drastis akan mengurangi waktu untuk melakukan patching.

- **Peningkatan Kemampuan Untuk Menembus Firewall**. Firewall seringkali menjadi harapan satu-satunya untuk melindungi network dari attacker. Namun pada kenyataannya telah berkembang teknologi yang secara tidak langsung dapat dipergunakan untuk memby-pass firewall seperti: IPP (Internet Printing Protocol) dan WebDAV (Web-based Distributed Authoring and Versioning), dan beberapa applikasi protocol lain yang telah ditandai sebagai firewall friendly.

- **Peningkatan Threat Secara Asimetris**. Attacker dapat menggunakan banyak perantara yang dikontrol penuh olehnya untuk secara bersamasama melakukan attack pada system target.

- **Peningkatan Threat dari Attack Pada Infrastruktur**. Beberapa kategori besar yang termasuk dalam attack pada infrastruktur adalah:

  - **Distributed Denial of Service (DDoS)**. Sejumlah systems yang menyerang satu atau lebih targetnya, menyebabkan services tidak dapat berjalan dengan baik.
  - **Worms**. Tidak seperti virus yang membutuhkan intervensi user untuk melakukan aksinya, worms dapat memperbanyak-dirinya sendiri dan kemudian menyebarluas untuk melakukan attack seperti DoS (Denial of Service), defacement pada website, dan menyebabkan system overload.
  - **Attack pada DNS Internet**. Dimaksudkan untuk mengelabui DNS agar menyimpan pada informasi yang telah dimodifikasi atau palsu (cache poisoning); eksploitasi servers yang vulnerable untuk memodifikasi data yang disimpannya yang nantinya akan digunakan oleh system yang menjadi target; Melakukan DoS pada DNS; dan mengambil alih kepemilikan sebuah domain (domain hijacking).
  - **Attack pada routers**. Attacker akan memanfaatkan router yang lemah sebagai platform untuk melakukan attack pada target lain. Attacker dapat menyebabkan kerusakan dengan mengeksploitasi koneksi yang berlangsung antar routers dengan cara memodifikasi, menghapus, atau memasukkan route kedalam routing Internet secara global untuk melakukan redirect traffic yang ditujukan dari sebuah network ke network yang lain. Hal ini dapat dikategorikan sebagai DoS karena network menjadi tidak beroperasi akibat tidak adanya traffic yang masuk atau menerima traffic secara berlebihan.

4 Rangkuman dan Kesimpulan

Network attacks berdasar tujuannya tidak hanya berdasarkan atas dasar penguasaan/kontrol resouce terhadap target, melainkan juga berdasarkan atas kesenangan/kepuasan pribadi. Dalam hal ini siapapun dapat menjadi target sasaran tidak hanya target yang memiliki data berharga saja.

Proses attacks dari seorang attacker memiliki fase-fase attack yaitu:

- Fase Persiapan
- Fase Eksekusi
- Fase Post Attack

Fase attack merupakan fase yang berbahaya, hal ini dikarenakan motifasi bagi seorang attacker yang bermacam-macam. Target dari seorang attacker dapat menjadi sasaran/tertuduh ketika attacker melakukan attack terhadap host/network lain melalui host/network kita. Network attacks merupakan sebuah rantai yang tidak diketahui ujungnya kecuali oleh sang attacker.

Administrator dari host level services harus dapat mengerti service-service yang disediakan bagi umum beserta resiko-resikonya dan harus dapat meminimalisasi resiko terjadinya sebuah attack yang berhasil.

Dengan melihat tren dari network attacks, dapat dilihat bahwa semakin berkembang teknologi, maka semakin berkembang pula pola attack yang terjadi. Begitupula dengan kuantitas dari attacks yang selalu berkembang dua kali lipat setiap tahunnya.