7 Jenis Serangan Cracker

MUHAMMAD HAFIS

muhammadhafis@raharja.info

Abstrak

Seringkali ketika kita menemukan kerawanan ataupun missconfiguration pada system sendiri, kita akan menganggap hal itu adalah hal yang kecil, karena kita menanggapinya bukan sebagai lubang keamanan. Tools maupun teknik yang digunakan cracker kebanyakan adalah variasi dari serangan yang mereka lakukan sebelumnya. Sebagai Administrator baik system maupun jaringan ataupun end user, Anda haruslah banyak belajar dari pengalaman penyerangan yang terjadi sebelumnya (walaupun serangan tersebut terjadi pada orang lain) untuk menghindari serangan yang akan terjadi berikutnya.

Kata Kunci: Maintenace,Hacking, Lambat

Pendahuluan

Mengetahui jenis serangan sangat penting untuk menjaga stabilitas system, sehingga anda tidak perlu repot untuk menginstall system baru agar lebih aman, anda hanya perlu mempatch atau bahkan sedikit mengkonfigurasi system anda Mungkin bagi beberapa orang tulisan ini merupakan tulisan yang sangat mendasar, tapi tidak ada salahnya jika anda sebagai seorang Profesional untuk mereview sesuatu yang dasar dari waktu ke waktu.. Artikel ini bukan ditujukan untuk menyerang tetapi sebaliknya yaitu untuk bertahan, karena menurut hemat saya untuk bertahan anda harus tahu cara menyerang. Dalam artikel ini terdapat serangan yang sering dilakukan oleh cracker dan disetiap serangan mempunyai metode-metode tersendiri, contohnya saja dalam melakukan IP spoofing yang mempunyai banyak metode diantaranya *man in the middle attack*. Dengan alasan diatas saya akan mencoba menggaris besarkan serangan-serangan umum yang sering dilakukan cracker dan harus diketahui oleh seorang Administrator maupun end user, sedangkan metode-metode yang lebih spesifik mungkin akan saya tuangkan dalam tulisan saya berikutnya baik itu penyerangan ataupun metode yang dilakukan untuk bertahan. Saya tahu tulisan berikut adalah jauh dari sempurna, untuk itu saran dan kritik sangat saya harapkan.

Pembahasan

1. IP Spoofing

IP Spoofing juga dikenal sebagai *Source Address Spoofing*, yaitu pemalsuan alamat IP attacker sehingga sasaran menganggap alamat IP attacker adalah alamat IP dari host di dalam network bukan dari luar network. Misalkan attacker mempunyai IP address type A 66.25.xx.xx ketika attacker melakukan serangan jenis ini maka Network yang diserang akan menganggap IP attacker adalah bagian dari Networknya misal 192.xx.xx.xx yaitu IP type C. IP Spoofing terjadi ketika seorang attacker ‘mengakali’ packet routing untuk mengubah arah dari data atau transmisi ke tujuan yang berbeda. Packet untuk routing biasanya di transmisikan secara transparan dan jelas sehingga membuat attacker dengan mudah untuk memodifikasi asal data ataupun tujuan dari data. Teknik ini bukan hanya dipakai oleh attacker tetapi juga dipakai oleh para security profesional untuk men tracing identitas dari para attacker.

Protokol yang menangani komunikasi antar komputer kebanyakan berhasil di spoof. ICMP (Internet Control Message Protocol) adalah salah satunya(vulnerable) karena protokol ini dilewati oleh informasi dan pesan-pesan kesalahan diantara dua node dalam network. Internet Group Message Protocol(IGMP) dapat dieksploitasi dengan menggunakan serangan tipe ini karena IGMP melaporkan kondisi kesalahan pada level user datagram, selain itu juga protokol

ini mengandung Informasi routing dan Informasi Network. (UDP) User Datagram Protocol juga dapat ‘diminta’ untuk menampilkan identitas host sasaran.

Solusi untuk mencegah IP spoofing adalah dengan cara mengamankan packet-packet yang ditransmisikan dan memasang *screening policies*. Enkripsi Point-to-point juga dapat mencegah user yang tidak mempunyai hak untuk membaca data/packet. Autentikasi dapat juga digunakan untuk menyaring source yang legal dan bukan source yang sudah di spoof oleh attacker. Dalam pencegahan yang lain, Admininistrator dapat menggunakan signature untuk paket-paket yang berkomunikasi dalam networknya sehingga meyakinkan bahwa paket tersebut tidak diubah dalam perjalanan.

Anti Spoofing rules(peraturan anti spoof) yang pada dasarnya memberitahukan server untuk menolak packet yang datangnya dari luar yang terlihat datangnya dari dalam, umumnya hal ini akan mematahkan setiap serangan spoofing.

2. FTP Attack

Salah satu serangan yang dilakukan terhadap File Transfer Protocol adalah serangan buffer overflow yang diakibatkan oleh *malformed command*. tujuan menyerang FTP server ini rata-rata adalah untuk mendapatkan command shell ataupun untuk melakukan Denial Of Service.

Serangan Denial Of Service akhirnya dapat menyebabkan seorang user atau attacker untuk mengambil resource didalam network tanpa adanya autorisasi, sedangkan command shell dapat membuat seorang attacker mendapatkan akses ke sistem server dan file-file data yang akhirnya seorang attacker bisa membuat anonymous root-acces yang mempunyai hak penuh terhadap system bahkan network yang diserang.

Tidak pernah atau jarang mengupdate versi server dan mempatchnya adalah kesalahan yang sering dilakukan oleh seorang admin dan inilah yang membuat server FTP menjadi rawan untuk dimasuki. Sebagai contoh adalah FTP server yang populer di keluarga UNIX yaitu WU-FTPD yang selalu di upgrade dua kali dalam sehari untuk memperbaiki kondisi yang mengizinkan terjadinya bufferoverflow

Mengexploitasi FTP juga berguna untuk mengetahui password yang terdapat dalam sistem, FTP Bounce attack(menggunakan server ftp orang lain untuk melakukan serangan), dan mengetahui atau mensniff informasi yang berada dalam sistem

3. Unix Finger Exploits

Pada masa awal internet, Unix OS finger utility digunakan secara efficient untuk men sharing informasi diantara pengguna. Karena permintaan informasi terhadap informasi finger ini tidak menyalahkan peraturan, kebanyakan system Administrator meninggalkan utility ini (finger) dengan keamanan yang sangat minim, bahkan tanpa kemanan sama sekali. Bagi seorang

attacker utility ini sangat berharga untuk melakukan informasi tentang footprinting, termasuk nama login dan informasi contact. Utility ini juga menyediakan keterangan yang sangat baik tentang aktivitas user didalam sistem, berapa lama user berada dalam sistem dan seberapa jauh user merawat sistem.

Informasi yang dihasilkan dari finger ini dapat meminimalisasi usaha cracker dalam menembus sebuah sistem. Keterangan pribadi tentang user yang dimunculkan oleh finger daemon ini sudah cukup bagi seorang atacker untuk melakukan social engineering dengan menggunakan social skillnya untuk memanfaatkan user agar 'memberitahu' password dan kode akses terhadap system.

4. Flooding & Broadcasting

Seorang attacker bisa menguarangi kecepatan network dan host-host yang berada di dalamnya secara significant dengan cara terus melakukan request/permintaan terhadap suatu informasi dari sever yang bisa menangani serangan classic Denial Of Service(Dos), mengirim request ke satu port secara berlebihan dinamakan flooding, kadang hal ini juga disebut spraying. Ketika permintaan flood ini dikirim ke semua station yang berada dalam network serangan ini dinamakn broadcasting. Tujuan dari kedua serangan ini adalah sama yaitu membuat network resource yang menyediakan informasi menjadi lemah dan akhirnya menyerah.

Serangan dengan cara Flooding bergantung kepada dua faktor yaitu: ukuran dan/atau volume (size and/or volume). Seorang attacker dapat menyebabkan Denial Of Service dengan cara melempar file berkapasitas besar atau volume yang besar dari paket yang kecil kepada sebuah system. Dalam keadaan seperti itu network server akan menghadapi kemacetan: terlalu banyak informasi yang diminta dan tidak cukup power untuk mendorong data agar berjalan. Pada dasarnya paket yang besar membutuhkan kapasitas proses yang besar pula, tetapi secara tidak normal paket yang kecil dan sama dalam volume yang besar akan menghabiskan resource secara percuma, dan mengakibatkan kemacetan.

Attacker sering kali menggunakan serangan flooding ini untuk mendapatkan akses ke system yang digunakan untuk menyerang network lainnya dalam satu serangan yang dinamakan Distributed Denial Of Service(DDOS) . Serangan ini seringkali dipanggil *smurf* jika dikirim melaluli ICMP dan disebut *fraggles* ketika serangan ini dijalakan melewati UDP.

Suatu node (dijadikan tools) yang menguatkan broadcast traffic sering disebut sebagai *Smurf Amplifiers*, tools ini sangat efektif untuk menjalankan serangan flooding. Dengan melakukan spoofing terhadap network sasaran, seorang attacker dapat mengirim sebuah request ke smurf amplifier, Network yang di amplifiying(dikuatkan) akan mengirim respon kesetiap host di dalam network itu sendiri, yang berarti satu request yang dilakukan oleh attacker akan menghasilkan pekerjaan yang sama dan berulang-ulang pada network sasaran, hasil dari serangan ini adalah sebuah denial of service yang tidak meninggalkan jejak. Serangan ini dapat diantisipasi dengan cara menolak broadcast yang diarahkan pada router.

TCP-level Flooding (kebanyakan SYN ATTACK) telah digunakan pada bulan februari tahun 2000 untuk menyerang Yahoo!, eBay dll yang menggunakan serangan DDOS(Distributed Denial Of Service). Network yang tidak menggunakan firewall untuk pengecekan paket-paket TCP biasanya bisa diserang dengan cara ini.

Beberapa fungsi penyaringan pada firewall (Firewall Filtering Function) biasanya akan mampu untuk menahan satu serangan flooding dari sebuah alamat IP, tetapi serangan yang dilakukan melalui DDOS akan sulit di cegah karena serangan ini seperti kita ketahui datangnya dari berbagai alamat IP secara berkala. Sebenarnya salah satu cara untuk menghentikan serangan DDOS adalah dengan cara mengembalikan paket ke alamat asalnya atau juga dengan cara mematikan network(biasanya dilakukan oleh system yang sudah terkena serangan sangat parah).

5. Fragmented Packet Attacks

Data-data internet yang di transmisikan melalui TCP/IP bisa dibagi lagi ke dalam paket-paket yang hanya mengandung paket pertama yang isinya berupa informasi bagian utama(kepala) dari TCP. Beberapa firewall akan mengizinkan untuk memroses bagian dari paket-paket yang tidak mengandung informasi alamat asal pada paket pertamanya, hal ini akan mengakibatkan beberapa type system menjadi crash. Contohnya, server NT akan menjadi crash jika paket-paket yang dipecah(fragmented packet) cukup untuk menulis ulang informasi paket pertama dari suatu protokol.

Paket yang dipecah juga dapat mengakibatkan suasana seperti serangan flooding. Karena paket yang dipecah akan tetap disimpan hingga akhirnya di bentuk kembali ke dalam data yang utuh, server akan menyimpan paket yang dipecah tadi dalam memori kernel. Dan akhirnya server akan menjadi crash jika terlalu banyak paket-paket yang telah dipecah dan disimpan dalam memory tanpa disatukan kembali.

Melalui cara enumerasi tentang topographi network sasaran, seorang attacker bisa mempunyai banyak pilihan untuk meng- crash packet baik dengan cara menguji isi firewall, load balancers atau content – based routers. Dengan tidak memakai system pertahanan ini, network sasaran jauh lebih rawan untuk perusakan dan pembobolan.

Karena paket yang dipecah(fragmented packet) tidak dicatat dalam file log sebelum disatukan kembali menjadi data yang utuh, packet yang dipecah ini memberikan jalan bagi hacker untuk masuk ke network tanpa di deteksi. Telah banyak Intrusion Detection System (IDS) dan saringan firewall(firewall filters) yang memperbaiki masalah ini, tapi masih banyak juga system yang masih dapat ditembus dengan cara ini.

6. E-mail Exploits

Peng-exploitasian e-mail terjadi dalam lima bentuk yaitu: mail floods, manipulasi perintah (command manipulation), serangan tingkat transportasi(transport level attack), memasukkan berbagai macam kode (malicious code inserting) dan social engineering(memanfaatkan sosialisasi secara fisik). Penyerangan e-mail bisa membuat system menjadi crash, membuka dan menulis ulang bahkan mengeksekusi file-file aplikasi atau juga membuat akses ke fungsi fungsi perintah (command function).

Serangan mail flood (flood =air bah) terjadi ketika banyak sekali e-mail yang dikirimkan oleh attacker kepada sasaran yang mengakibatkan transfer agent kewalahan menanganinya, mengakibatkan komunikasi antar program lain menjadi tidak stabil dan dapat membuat system menjadi crash. Melakukan flooding merupakan cara yang sangat kasar namun efektif, maksudnya untuk membuat suatu mail server menjadi down. Salah satu jalan yang menarik dalam melakukan serangan mail-flooding adalah dengan meng-exploitasi fungsi auto -responder (auto-responder function) yang terdapat dalam kebanyakan aplikasi email, ketika seorang attacker menemukan auto-responder yang sedang aktif dalam dua system yang berbeda, sang attacker bisa saja mengarahkan yang satu ke yang lainnya, karena kedua-duanya di set untuk merespond secara sacara otomatis untuk setiap pesan, maka kedua-duanya akan terus mengenarate lebih banyak e-mail secara loop(bolak-balik) dan akhirnya kedua-duanya akan kelelahan dan down.

Serangan memanipulasi perintah (command manipulation attack) dapat mengakibatkan sebuah system menjadi crash dengan cara menggulingkan mail transfer agent dengan sebuah buffer overflow yang diakibatkan oleh perintah (fungsi) yang cacat (contoh: EXPN atau VRFY). Perbedaan antara mail flood dan command manipulation: command manipulation meng-exploit kekuasaan milik *sendmail* yaitu memperbolehkan attacker untuk mengakses system tanpa informasi otorisasi(menjadi network admin tanpa diketahui) dan membuat modifikasi pada penjalanan program lainnya. Mengaktifkan command yang cacat seperti diatas juga dapat mengakibatkan seorang attacker mendapatlan akses untuk memodifikasi file, menulis ulang, dan tentunya saja membuat trojan horses pada mail server.

Penyerangan tingkat transport (transport level attack) dilakukan dengan cara mengexploit protokol pe-rute-an/pemetaan e-mail diseluruh internet: Simple Mail Tranport Protocol (SMTP). Seorang attacker dapat mengakibatkan kondisi kesalahan sementara (temporary error) di target system dengan cara meng-overload lebih banyak data pada SMTP buffer sehingga SMTP buffer tidak bisa menanganinya, kejadian ini dapat mengakibatkan seorang attacker terlempar dari sendmail program dan masuk kedalam shell dengan kekuasaan adminitsrasi bahkan dapat mengambil alih root. Beberapa serangan exploitasi juga sering terjadi pada POP dan IMAP.

Pada saat kerawanan SMTP sulit untuk di exploitasi, attacker mungkin saja berpindah ke serangan tranport level jika ia tidak berhasil menyerang dengan cara command manipulation ataupun mail-flood. Serangan ini lebih digunakan untuk membuat gangguan daripada untuk menjebol suatu system. Seorang attacker biasanya akan menggunakan serangan jenis untuk mem flood Exchange Server dan memotong lalu lintas e-mail (trafic e-mail). Serangan ini juga dapat digunakan untuk membuat reputasi suatu organisasi menjadi buruk dengan mengirimkan

spam atau offensive e-mail ke organisasi lainnya dengan sumber dan alamat dari organisasi tersebut.

Mail relaying, proses memalsukan asal/source email dengan cara meroutekannya ke arah mesin yang akan dibohongi, adalah type lain dari serangan transport-level. Teknik ini sangat berguna untuk membuat broadcasting spam secara anonymous. Berbagai macam isi(content) yang sering dikirim lewat e-mail

dengan teknik ini biasanya adalah content-content yang merusak. Beberapa Virus dan Worms akan disertakan dalam e-mail sebagai file attachment yang sah, seperti variant Melissa yang nampak sebagai Ms Word Macro atau loveletter worm yang menginfeksi system dan mengemailkan dirinya sendiri ke users yang berada dalam address booknya outlook. Kebanyakan antivirus scanner akan menangkap attachment seperti ini, tetapi visrus dan worm baru serta variannya masih tetap berbahaya.

Serangan yang terakhir yang dilakukan oleh seorang attacker selain serangan diatas adalah dengan cara melakukan social enginering, kadang sang attacker mengirim e-mail dengan source memakai alamat admin agar users mengirimkan passwordnya untuk mengupgrade system.

7. DNS and BIND Vulnerabilities

Berita baru-baru ini tentang kerawanan (vulnerabilities) tentang aplikasi Barkeley Internet Name Domain (BIND) dalam berbagai versi mengilustrasikan kerapuhan dari Domain Name System (DNS), yaitu krisis yang diarahkan pada operasi dasar dari Internet (basic internet operation).

Kesalahan pada BIND sebenarnya bukanlah sesuatu yang baru. Semenjak permulaanya, standar BIND merupakan target yang paling favorite untuk diserang oleh komunitas cracker karena beberapa kerawanannya. Empat kerawanan terhadap buffer overflow yang terjadi pada bulan Januari lalu hanya beberapa bagian dari kerawanan untuk diexploitasi oleh para cracker agar mendapat akses terhadap system dan melakukan perintah dengan hak penuh (command execution priviledge).

Kerawanan pada BIND merupakan masalah yang sangat serius karena lebih dari 80 persen DNS yang berada di Jagat Internet dibangun menggunakan BIND. Tanpa adanya DNS dalam lingkungan Internet Modern, mungkin transmisi e-mail akan sulit, navigasi ke situs-situs web terasa rumit dan mungkin tidak ada hal mudah lainnya yang menyangkut internet.

Kerawanan BIND bukan hanya terletak pada DNS. System penerjemah alamat (number-address translator) merupakan subject dari kebanyakan exploit, termasuk untuk melakukan penyerangan di tingkat informasi, penyerangan Denial Of Service, pengambil alihan kekuasaan dengan hijacking.

Penyerangan di tingkat Informasi bertujuan untuk membuat server menjawab sesuatu yang lain dari jawaban yang benar. Salah satu cara untuk melakukan serangan jenis ini adalah melalui *cache poisoning*, yang mana akan mengelabui remote name server agar menyimpan jawaban dari third-party domain dengan cara menyediakan berbagai macam informasi kepada domain server yang mempunyai autorisasi. Semua pengimplementasian serangan terhadap DNS akan mempunyai kemungkinan besar untuk berhasil dilakukan jika jawaban dari suatu pertanyaan yang spesisfik bisa dibohongi (spoof).

DOS atau membuat Server tidak dapat beroperasi, bisa dilakukan dengan cara membuat DNS menyerang dirinya sendiri atau juga dengan cara mengirimkan traffic-flooding yang berlebihan dari luar, contohnya menggunakan “Smurf” ICMP flood. Jika suatu organisasi atau perusahaan memasang *authoritathive name server* dalam satu segment yang terletak dibelakang satu link atau dibelakang satu physical area, maka hal ini akan menyebabkan suatu kemungkinan untuk dilakukannya serangan Denial Of Service.

Cracker akan mencoba untuk menyerang system melalui DNS dengan cara buffer overflow, yaitu salah satu exploit yang sangan berpotensi pada kerawanan BIND. Gangguan exploit terjadi karena adanya kelemahan dalam pengkodean/pemrograman BIND yang mengizinkan seorang attacker untuk memanfaatkan code-code yang dapat dieksekusi untuk masuk kedalam system. Beberapa system operasi telah menyediakan patch untuk stack agar tidak dapat dieksekusi, sebagaimana juga yang dilakukan compiler (menyediakan patch) yang melindungi stack dari overflow. Mekanisme perlindungan ini stidaknya membuat cracker akan sulit menggunakan exploit.

Telah jelas bahwa mengupdate system secara berkala dan menggunakan patch adalah salah satu yang harus dilakukan untuk membangun security yang efektif, jika vendor dari DNS anda tidak menyediakan patch secara berkala, anda lebih baik mengganti software DNS anda yang menyediakan patch secara berkala, tentunya untuk menjaga kemanan system.

Pada system Unix , BIND harus dijalankan sebagai root untuk mengatur port yang lebih rendah (kode-kode mesin). Jika software DNS dapat dibodohi untuk menjalankan code-code berbahaya, atau membuka file-file milik root, user local mungkin saja bisa menaikan kekuasaannya sendiri didalam mesin.

Organisasi atau perusahaan yang mengubah authoritative server juga harus waspada bahwa mengganti server mereka dalam waktu yang bersamaan akan mengakibatkan domain mereka di hijack melalui cache poisoning. Mengubah server seharusnya dilakukan sebagai proses transisi. Untuk mencegah domain hijacking sebaiknya network admin terlebih dahulu menambahkn server barunya kedalam network infrastucture sebelum mengganti server yang lama.

Penutup

Mungkin Cukup Sekiat Ulasan saya Kali ini, Semoga bermanfaat untuk teman teman yang ingin belajar tentang komputer, Semoga kita selalu semangat dalam belajar ilmu komputer dan kedepan nya selalu bisa membuat Inovasi - inofais yang baru dan semoga Tulisan ini dapat Membatu kalian Terimakasih.

Referensi

brainbench.com/transcript.jsp?pid=4351894

alfinyusroni.blogspot.com/2013/07/macam-macam-serangan-pada-sistem.html

netsec.id/jenis-serangan-jaringan-komputer/

sobarudinfile.blogspot.com/2014/08/jenis-jenis-serangan-jaringan-pada_26.html

ayoksinau.com/macam-macam-serangan-pada-komputer-lengkap/

Biografi

Perkenalkan nama muhammad hafis, status mahasiswa di salah satu sekolah tinggi swasta ilmu computer, jurusan yang diambil Teknih Infomatika Konsentrasi Sofware Engineering, Hobi Traveling mencari cari tantangan,. Untuk Penulisan Sendiri Sedang berfokus dengan hal hal yang berhubungan dengan IT yang masih ada hubungan nya dengan jurusan, saya adalah pribadi yang pendiam saat baru kenal namun saat sudah kenal banyak orang yang kaged karena tidak seperti pikirian , kalo menurut mereka saya bawel dan kadang – kadang enggak jelas, tapi walau begitu saya orang yang bertanggung jawab jika diberi amanah dan senang mengamati jalan pembicaraan orang jika didalam forum. Kalo ada yang mau ditanya lebih lanjut bisa kirim kirim email di Muhammad.hafis@raharja.info. Trima kasih atas perhatian nya.