Tips Mencari Target Server Dengan Bantuan Search Engine

Sony Arianto Kurniawan
sonyarianto@yahoo.com

Pada suatu hari ketika penulis sedang online di IRC di channel #aritechdev ada seorang teman yang bertanya begini, "Mas, gimana nih caranya untuk mencari target yang pake NT? Aku mau cobain cari target unicode nih, pleaseeeeee", demikian kata si penanya, kalo nggak salah si Jazzy_Tunes nih yang tanya. Penulis terdiam sesaat, bukan karena pertanyaannya, tetapi karena ada cewek cakep yang kebetulan lewat di depan penulis :) OK OK, kita kembali ke pokok permasalahan. Kalo dipikir-pikir sebenarnya mudah kok untuk mencari target server yang menggunakan Windows NT (yang bisa mengandung unicode bug, sql server, terminal services etc etc) atau server yang menggunakan Linux atau UNIX (yang bisa mengandung apache, sshd etc etc). Caranya ya dengan bantuan search engine. Gimana caranya? Ikuti dulu pesan-pesan berikut ini.

Penulis tidak bertanggung jawab atas segala isi dan akibat-akibat yang ditimbulkan oleh tulisan ini. Tulisan ini hanyalah semata-mata untuk tujuan pendidikan. Dilarang keras mengutip sebagian atau seluruh tulisan ini tanpa sepengetahuan penulis. Tulisan ini bersifat terbuka dan Anda bisa memberikan kritik dan saran dengan cara mengirimkannya ke sonyarianto@yahoo.com.

Anda bisa menggunakan search engine untuk mencari target untuk di-crack di internet. Caranya gimana? Ya mudah, Anda tinggal search saja dengan suatu keyword pada search engine. Kunci utamanya sebenarnya ada pada keyword yang Anda gunakan dan pengetahuan Anda yang mendasar terhadap internet dan operating system dan segala sesuatu yang berjalan di atas suatu operating system. Maksudnya begini, Anda harus bisa berimajinasi apa saja sih yang bisa menandakan suatu target itu menggunakan NT atau Linux misalnya. OK, sekarang mulailah berpikir lebih jauh, kalau di lingkungan Windows NT biasanya yang paling banyak digunakan untuk interface pada web adalah ASP (*Active Server Pages*). Ini ditandai dengan pengunaan file-file dengan ekstensi .asp pada web server-nya. Ahaaaaa, dengan modal ini saja Anda sudah bisa mendapatkan jutaan calon target NT lho. Ngerti maksud saya? Begini, ASP biasanya banyak digunakan sebagai interface web yang berbasis NT, file-file yang lazim yang ber-ekstensi .asp di internet misalnya:

1. login.asp
2. search.asp
3. privacy.asp
4. search.cfm

dan masih banyak lagi yang lainnya. Nah, dari sini kita coba deh memfilter internet agar kita mendapatkan target server yang menggunakan NT.

OK, sekarang siapkan search engine Anda. Penulis merekomendasikan google.com sebagai search engine untuk kasus ini. Ikuti langkah-langkah berikut untuk mendapatkan target NT kita:

1. Buka situs www.google.com.
2. Ketik search.asp sebagai keyword di Google dan tekan tombol untuk memulai pencarian.
3. Hanya sekejap mata maka akan muncul daftar hasil pencarian situs-situs yang mengandung file search.asp didalamnya.
4. Nah selesai deh pekerjaan kita. Anda bisa mulai coba satu-satu daftar target tadi mulai dari atas dengan pengetahuan vulnerabilitas yang Anda kuasai saat ini. Misalnya mencoba unicode bug, mencari sql server dengan login sa blank, mencari microsoft ftp, mencari terminal services host etc etc.

Nah, empat langkah diatas itu menunjukkan bahwa search engine sebenarnya bisa juga dianggap sebagai suatu hacking tool, dalam hal ini digunakan sebagai alat finger printing sederhana terhadap kemungkinan OS yang digunakan oleh suatu server. Dan ingat, cara ini adalah seuatu pembuka jalan dalam hal memilah-milah target yang kita inginkan. Ini sangat efektif daripada jika Anda menggunakan port scanner untuk mencari target awal. Tapi ingat file dengan ekstensi .asp tidak selalu identik dengan NT lho, kali ajah pake ChilliSoft ASP. Demikan pula jika Anda ingin mendapatkan target server yang menggunakan Linux atau UNIX misalnya. Anda bisa gunakan file-file dengan ekstensi .php, .php3, .pl atau .cgi. Misalnya daftar keyword yang sering digunakan adalah:

1. login.pl, login.php, login.cgi
2. search.pl, search.php, search.cgi

Nah berikutnya mungkin Anda belum puas dengan terlalu banyaknya hasil pencarian yang dikembalikan oleh si Google tadi. OK OK, mudah saja, Anda bisa memperkecil daftar target Anda dengan cara menambahkan keyword pada Google dengan suatu kata yang spesifik. Misalnya Anda pingin mencari target NT yang mengandung Indonesia atau dengan kata lain server NT di Indonesia lah. Untuk kasus ini masukkan saja keyword sebagai berikut di Google:

indonesia, search.asp

Nah, sekarang Anda akan mendapatan beberapa calon target yang mengandung kata Indonesia dan sekaligus juga ada file search.asp didalamnya. Mudah kan ;)

OK, sekarang penulis akan memberikan beberapa kasus yang penulis sempat terapkan ketika akan melakukan cracking di internet.

Kasus 1:
Aku ingin mencari calon target yang mengandung kata credit card dan target ini menggunakan NT. Keyword yang bisa digunakan adalah -- credit card, search.asp

Kasus 2:
Aku ingin mencari calon target yang mengandung kata government dan target ini menggunakan NT. keyword yang bisa digunakan adalah -- government, search.asp

Kasus 3:
Aku ingin mencari calon target yang mengandung kata database, yang situs-situs tentang perdagangan dan pake server NT. Keyword yang bisa digunakan adalah -- database, commerce, login.asp

OK, demikian contoh-contoh kasus sederhana. Kalo Anda jeli Anda bisa mengembangkannya lebih jauh lagi sesuai dengan imajinasi Anda. Ingat, disini kita hanya main imajinasi untuk mendapatkan keyword yang tepat dan sesuai keinginan Anda. Kelemahan dari teknik pencarian target dengan search engine adalah bahwa kita tidak akan bisa mendapatkan target server apabila dia tidak terdaftar dalam search engine hahahaha :) Tapi itu masih ada caranya juga kok supaya mengakali itu. Caranya gimana? Ya Anda bisa kombinasikan hasil pencarian dari search engine dengan port scanner yang Anda gunakan. Bingung? Ya udah kalo bingung sampe disini ajah dulu. Kapan-kapan kita lanjutkan lagi masalah teknik dan trik-trik pencarian target ini.

Penulis sudah mencoba cara diatas dengan search engine google.com dan teoma.com. Anda bisa mencobanya dengan search engine yang lain. Jika ada komentar kirim ajah ke sonyarianto@yahoo.com.

Selamat mencoba.