Muhammad Hafiz Reza Syaputra
09011381621061
Sk7Bukit

ILUSTRASI SERANGAN ICMP

Ilustrasi Serangan ICMP

Kesederhanaan protokol ICMP dan kurangnya kesadaran terkait masalah keamanan protokol telah menuntun saya untuk meletakkan makalah ini untuk mencoba menggambarkan beberapa kemungkinan serangan menggunakan ICMP sebagai alat. Juga disertakan dalam makalah ini adalah referensi ke beberapa alat yang tersedia untuk digunakan dan dalam beberapa kasus, ini telah digunakan untuk beberapa serangan dunia nyata.

Dasar-dasar ICMP

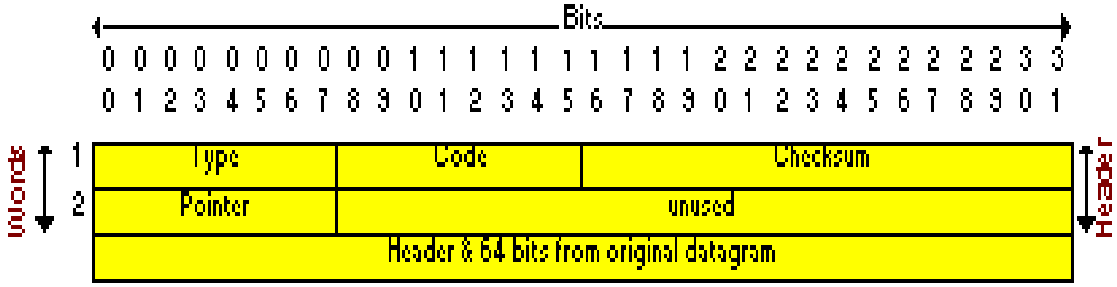
ICMP, Protokol Pesan Kontrol Internet adalah bagian integral dari IP apa pun pelaksanaan. Meskipun pesan ICMP dikirim dalam paket IP dan menggunakan IP seolah-olah levelnya lebih tinggi protokol, ICMP sebenarnya merupakan bagian internal dari IP, dan harus diterapkan di setiap IP modul. Pesan ICMP diklasifikasikan ke dalam 2 kategori utama yaitu :

- Pesan Kesalahan ICMP.
- Pesan Kueri ICMP.

Tujuan dan fitur-fiturnya sebagaimana diuraikan dalam RFC 792 adalah untuk menyediakan sarana untuk mengirim kesalahan pesan untuk kondisi kesalahan non-sementara, dan untuk menyediakan cara untuk menyelidiki jaringan masuk untuk menentukan karakteristik umum tentang jaringan.

Kode angka, juga dikenal sebagai "tipe pesan", ditetapkan untuk setiap pesan ICMP; saya t menentukan jenis pesan. Kode angka lain mewakili "kode" untuk tipe ICMP yang ditentukan; bertindak sebagai sub-tipe, dan interpretasinya bergantung pada jenis pesan.

Diagram di bawah ini menunjukkan format paket ICMP umum.



Ilustrasi Serangan

Fase I - Pengintaian & Pemindaian

ICMP Sweep

Dalam setiap skenario serangan tipikal, penyerang akan terlebih dahulu melakukan beberapa pengintaian dan kegiatan pemindaian untuk

- Lebih memahami lingkungan target
- Kumpulkan informasi tentang target untuk merencanakan pendekatan serangan
- Gunakan teknik & alat yang tepat untuk fase serangan selanjutnya

Salah satu teknik yang paling umum (meskipun berisik) dan paling dipahami untuk menemukan kisaran host yang hidup di lingkungan target adalah melakukan Sapu ICMP dari seluruh jangkauan jaringan target.

ICMP Sweep pada dasarnya melibatkan mengirim serangkaian paket permintaan ICMP ke Internet jangkauan jaringan target dan dari daftar balasan ICMP menyimpulkan apakah host tertentu hidup dan terhubung ke jaringan target untuk diselidiki lebih lanjut.

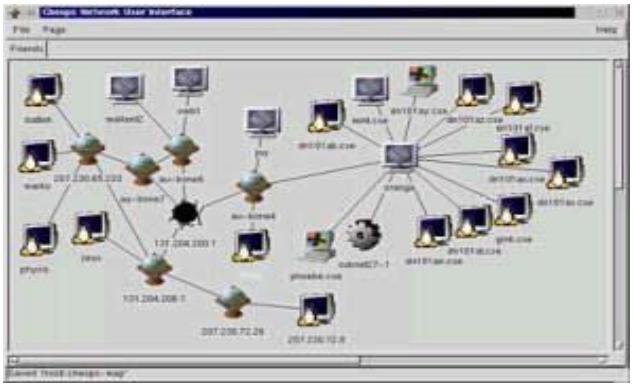
Meskipun serangan di atas dapat dilakukan secara manual melalui ping perintah yang sangat sederhana, banyak alat pemindaian akan mempercepat keseluruhan proses pemindaian dengan melakukan pemindaian semacam itu pada semua rentang alamat IP yang mungkin diberikan target jaringan.

Traceroute

Alat lain yang sangat berguna untuk memetakan konfigurasi jaringan target adalah penggunaan traceroute panggilan perintah yang sangat sederhana. Apa yang pada dasarnya dilakukan oleh perintah ini adalah, ia akan mengirimkan serangkaian paket secara progresif dengan set nilai TTL (Time to Live) yang meningkat. Saat router perantara menerima paket penerusan, ia akan menurunkan nilai TTL paket sebelum meneruskannya ke router berikutnya. Pada saat ini jika nilai TTL paket mencapai nol, pesan "waktu terlampaui" ICMP akan dikirim kembali ke host asal. Dengan mengirim paket dengan nilai TTL awal 1 akan memungkinkan router pertama di jalur paket untuk sekarang mengirim kembali pesan "waktu terlampaui" ICMP yang kemudian akan memungkinkan penyerang untuk mengetahui alamat IP dari router pertama. Paket selanjutnya dikirim dengan meningkatkan nilai TTL dalam paket sebanyak 1 setiap kali, sehingga penyerang akan dapat mengetahui setiap lompatan antara dia dan target.

Dengan menggunakan teknik ini, penyerang tidak hanya dapat melacak jalur yang diambil oleh suatu paket saat ia bergerak ke target tetapi juga memberinya informasi tentang topologi jaringan target. Informasi ini sangat penting dalam memungkinkan penyerang merencanakan pendekatannya ketika menyerang jaringan.

Alat pemetaan jaringan seperti Cheops (http://www.marko.net/cheops) akan memungkinkan penyerang dengan cepat memetakan seluruh jaringan target menggunakan ping dan traceroute. Alat ini adalah alat yang sangat bising dari perspektif lalu lintas dan dapat dengan mudah diambil oleh sistem deteksi intrusi serta log firewall.



Firewalk

Berkembang lebih jauh dari ide traceroute, teknik selanjutnya (Firewalk) ini dapat digunakan untuk mengidentifikasi port yang terbuka pada firewall packet filtering. Tujuan melakukannya adalah benar-benar memetakan aturan penyaringan yang sedang diatur dalam firewall penyaringan paket. Firewalking biasanya dilakukan dalam 2 fase, fase 1 melibatkan melakukan traceroute dari penyerang ke firewall target untuk memastikan jumlah lompatan yang diperlukan untuk sebuah paket untuk mencapai firewall. Selama fase pemindaian, nilai TTL dari paket akan ditetapkan ke satu lebih besar dari firewall dan kirim ke host yang dikenal di balik firewall. Jika pesan "waktu melebihi" ICMP diterima, itu berarti bahwa paket tersebut telah berhasil melewati firewall dan dengan demikian menyebabkan paket ICMP dikembalikan oleh host yang dikenal karena nilai TTL sekarang telah mencapai nol, jika tidak maka dapat disimpulkan bahwa ada aturan penyaringan pada firewall yang menghentikan lalu lintas.

Inverse Mapping

Inverse Mapping adalah teknik yang digunakan untuk memetakan jaringan internal atau host yang dilindungi oleh perangkat penyaringan. Biasanya beberapa dari sistem tersebut tidak dapat dijangkau dari Internet. Kami menggunakan router, yang akan memberikan informasi arsitektur internal jaringan, bahkan jika pertanyaan yang mereka tanyakan tidak masuk akal, untuk jenis pemindaian ini. Kami menyusun daftar IP yang mencantumkan apa yang tidak ada di sana, dan menggunakannya untuk menyimpulkan di mana segala sesuatu mungkin berada.

Serangan Pemetaan Terbalik diilustrasikan di bawah ini:

Langkah 1. Penyerang mengirim pesan balasan ICMP ke berbagai alamat IP mungkin di belakang perangkat penyaringan.

Langkah 2. Setelah menerima serangkaian pesan balasan ICMP, karena perangkat pemfilteran tidak menyimpan daftar permintaan ICMP, ia akan memungkinkan paket-paket ini ke tujuannya.

Langkah 3. Jika ada router internal, router akan merespons dengan "Host Unreachable" ICMP untuk setiap host yang tidak dapat dijangkau, sehingga memberikan pengetahuan penyerang dari semua host yang ada di belakang perangkat penyaringan.

Fingerprinting OS

Sebelum serangan apa pun dapat diluncurkan, selain mengetahui keberadaan host target, akan sangat bermanfaat untuk mengetahui sistem operasi yang mendasari serta daftar layanan yang dijalankannya. Sementara port scanner dapat menentukan jenis layanan yang ditawarkan pada sistem, ICMP kembali dapat terlibat dalam membantu penyerang menentukan sistem operasi yang mendasarinya.

Keuntungan menggunakan protokol ICMP dalam latihan sidik jari OS jarak jauh menawarkan penyerang cara yang lebih tersembunyi dalam proses identifikasi OS. Dalam beberapa kasus hanya satu paket yang dikirim untuk menentukan sistem operasi yang digunakan oleh sistem target. Remote OS Fingerprinting adalah teknik yang mengeksploitasi fakta bahwa vendor sistem operasi yang berbeda telah membangun cara penanganan lalu lintas jaringan yang sedikit berbeda. Sebuah studi terperinci mengenai sidik jari OS jarak jauh

aktif dan pasif telah dilakukan dan laporan terperinci dapat ditemukan di (http://www.sys-security.com/html/projects/X.html).

Serangan Fingerprinting OS jarak jauh diilustrasikan di bawah ini:

Langkah 1. Penyerang mengirim paket UDP dengan bit DF yang diatur ke host target yang port UDP-nya ditutup.

Langkah 2. Pesan ICMP "Destination unreachable port" akan dikembalikan ke penyerang.

Langkah 3. Karena kenyataan bahwa host yang berbeda akan mengirim paket ICMP sedikit berbeda, sistem operasi dapat ditentukan dengan memeriksa beberapa bit dalam paket kembali. Misalnya. Jika kita melihat bidang bit prioritas dari paket dan nilainya 0xc0, sistem operasi yang mendasari kemungkinan besar dapat disimpulkan menjadi mesin berbasis kernel Linux 2.0.x / 2.2.x / 2.4.x atau router berbasis Cisco atau sakelar Jaringan Ekstrim

Dalam hal ini, untuk membedakan antara kernel Linux dan kernel dari perangkat jaringan, metode sidik jari ICMP Error Quoting size dapat digunakan. Dalam metode ini, paket ICMP yang dikembalikan diperiksa untuk jumlah byte yang dikembalikan. Kernel Linux akan mengembalikan jumlah byte yang berbeda dibandingkan dengan perangkat jaringan, sehingga kami dapat membedakannya.

Satu langkah lebih jauh adalah untuk dapat membedakan antara berbagai versi kernel Linux. Dalam hal ini kita akan melihat nilai IP TTL yang diatur dalam paket, kernel Linux 2.0.x telah mendapat nilai awal 64 sedangkan 2.2.x dan 2.4.x akan menggunakan nilai awal 255. Sekarang untuk membedakan antara 2.2.x dan 2.4.x adalah untuk melihat nilai ID IP paket, 2.4.1 - 2.4.4 telah mendapat nilai sama dengan nol tidak seperti 2.2.x. Jadi hanya dengan melihat 1 paket kembali dari target, penyerang dapat menelusuri ke jenis dan versi sistem operasi yang mendasarinya.

Teknik lain seperti memeriksa bagaimana tuan rumah menanggapi permintaan cap waktu ICMP dibuat juga digunakan untuk membedakan antara sistem operasi.

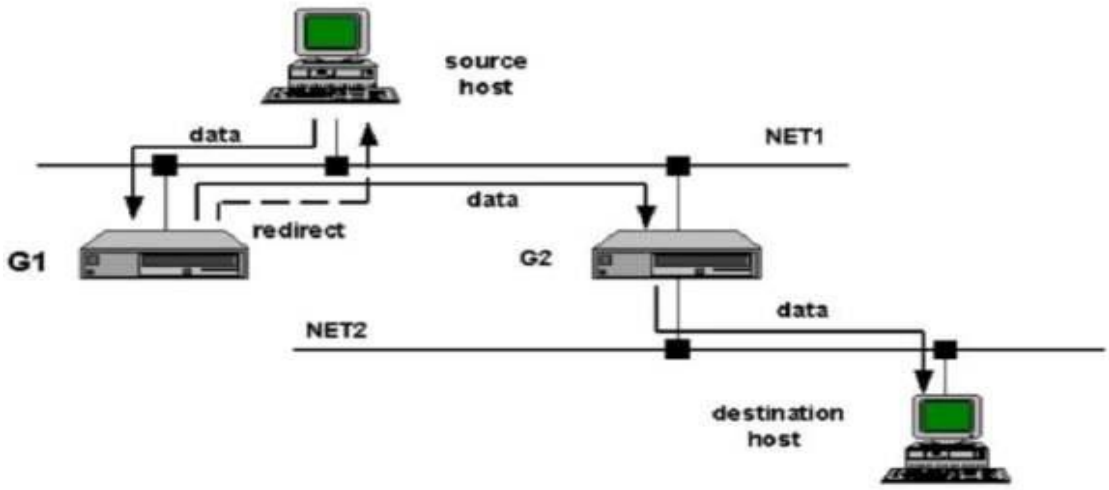
Probe X tersedia di (http://xprobe.sourceforge.net/) adalah alat bantu untuk memungkinkan Anda melakukan hal di atas secara otomatis

Fase 2 - Sistem Pemanfaatan

Pengalihan Rute ICMP

Pesan ICMP Route Redirect dikirim ketika gateway menerima lalu lintas IP dari host dan menemukan dalam tabel peruteannya bahwa gateway berikutnya yang akan dirutekan untuk lalu lintas ini berada di jaringan yang sama dengan host.

Melihat pertama kali pada hal ini tidak benar-benar mengungkapkan masalah dengan ini, tetapi mari kita melihat skenario untuk melihat bagaimana ini dapat dieksploitasi untuk memungkinkan serangan Man-In-The-Middle diluncurkan.



Langkah 1. Penyerang berhasil mengambil alih gateway G1 sekunder dari host sumber.

Langkah 2. Penyerang mengirimkan paket terbuka TCP ke host sumber yang bertindak sebagai host tujuan.

Langkah 3. Ketika balasan sedang dalam transit dari host sumber ke host tujuan melalui gateway G2, penyerang mengirimkan pesan pengalihan rute ICMP ke host sumber spoofing sebagai G2.

Langkah 4. Host sumber akan menerima pesan kontrol perubahan rute sebagai valid dan dengan demikian mengubah tabel peruteannya untuk sekarang merutekan semua lalu lintas yang terikat untuk host tujuan melalui Gateway G1.

Langkah 5. Sekarang penyerang akan dengan tenang membaca / memodifikasi dan meneruskan semua lalu lintas yang terikat untuk host tujuan ke Gateway G2 yang bertindak sebagai host Man-In-The-Middle.

Pesan informasi ICMP

Dengan mengirim pesan ICMP "kebesaran" ke host target dapat berpotensi crash / reboot host target. Hal ini disebabkan oleh kenyataan bahwa beberapa OS tidak tahu bagaimana menangani paket yang lebih besar dari ukuran maksimum sebagaimana diatur dalam RFC.

Spesifikasi TCP / IP memungkinkan maksimum 65536 oktet dalam satu paket informasi. Eksploitasi ini dapat dengan mudah dieksploitasi melalui penggunaan perintah ping (dengan bendera untuk menunjukkan ukuran paket yang akan dikirim) dengan menggunakan ukuran paket lebih besar dari 65536 oktet. Beberapa OS akan melakukan pemeriksaan pada ukuran paket ping keluar dan tidak akan mengizinkan paket lebih besar dari 65536 oktet. Ada banyak alat yang tersedia untuk diunduh yang akan memungkinkan penyerang untuk membuat paket ping yang disesuaikan. Salah satu contohnya adalah hping2 (http://www.securityfocus.com/tools/641).

Jika host target tidak ditambal dengan benar, OS akan membeku atau reboot setelah menerima hanya 1 paket besar.

Dengan mengeksploitasi sifat fragmentasi serta paket ICMP yang terlalu besar, eksploit lain dimungkinkan yang akan menyebabkan beberapa OS berhenti merespons dan harus beralih ke reboot untuk pulih dari serangan ini.

SSPing (http://packetstormsecurity.org/Exploit_Code_Archive/ssping.zip) adalah alat yang melakukan hal itu. Berkembang lebih jauh dari ide ini adalah alat lain Jolt2 (http://razor.bindview.com/publish/advisories/adv_Jolt2.html) Dalam serangan ini, mengirimkan sejumlah besar paket IP yang terfragmentasi identik ke host target akan menyebabkan tuan rumah berhenti merespons selama periode waktu ketika serangan sedang berlangsung.

Alat lain teardrop (http://packetstormsecurity.org/Exploit_Code_Archive/teardrop.c) mengirimkan aliran paket yang terfragmentasi ke host target dan memintanya untuk menyatukannya kembali. Ketika tuan rumah mencoba untuk melakukannya, ia menemukan bahwa paket-paket itu bukan ukuran yang mereka katakan. Ini menyebabkan host target hang dan memerlukan boot ulang sebelum itu akan berfungsi lagi.

ICMP Router Discovery Messages

Sebelum sebuah host dapat mengirim pesan ke host di luar subnetnya sendiri, ia harus dapat mengidentifikasi alamat router langsung. Ini biasanya dilakukan dengan membaca file konfigurasi saat startup dan pada beberapa jaringan multicast dengan mendengarkan lalu lintas protokol routing.

Perpanjangan protokol ICMP yang disebut "ICMP Router Discovery Protocol" (didefinisikan dalam RFC 1256 -http: //www.faqs.org/rfcs/rfc1256.html) dapat menggunakan "iklan router" dan juga pesan "permintaan router" untuk memungkinkan host menemukan alamat IP router yang terhubung ke jaringan langsung mereka.

Ketika sebuah host sedang dijalankan, itu akan menggunakan pesan "router solicitation" untuk memeriksa alamat router langsung. Karena pesan-pesan ini tidak diautentikasi, penyerang di subnet yang sama dengan tuan rumah dapat menipu pesan-pesan ini.

Skenario serangan yang mungkin diilustrasikan di bawah ini:

Langkah 1. Host boot up dan mengeluarkan pesan “router solicitation” untuk mencari tahu router default di jaringan.

Langkah 2. Penyerang mendengarkan pesan dan menipu balasan ke host tersebut.

Langkah 3. Rute default dari host sekarang diatur ke alamat IP penyerang yang penyerang telah masukkan dalam jawabannya.

Langkah 4. Sekarang penyerang dapat menggunakan serangan sniffing, man-in-the-middle untuk semua lalu lintas keluar melalui mesin penyerang.

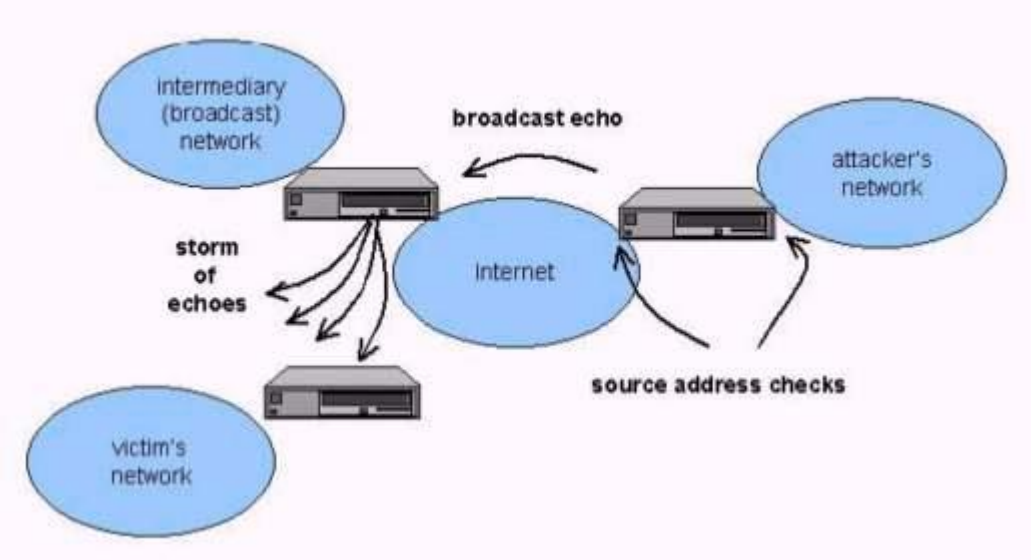
Langkah 5. Serangan penolakan layanan juga dimungkinkan dengan tidak meneruskan paket apa pun ke subnet yang benar

ICMP Floods

Dengan membanjiri host target dengan sejumlah besar pesan ICMP akan membuat host yang diserang dan jaringan yang terkait dengan kinerja yang menurun atau bahkan penolakan total layanan dalam beberapa kasus. Serangan Smurf (http://cs.baylor.edu/~donahoo/NIUNet/hacking/smurf/smurf.c) pintar:

Mereka menggunakan seluruh jaringan komputer untuk mengarahkan sejumlah besar lalu lintas ke mesin korban dan jaringannya.

Serangan smurf diilustrasikan di bawah ini:



Langkah 1. Penyerang menemukan beberapa jaringan perantara yang akan merespons ke alamat siaran jaringan.

Langkah 2. Penyerang memalsukan alamat IP host korban dan mengirimkan sejumlah besar paket permintaan gema ICMP ke alamat broadcast jaringan perantara di atas.

Langkah 3. Sekarang semua host di jaringan itu akan menanggapi permintaan gema ICMP dengan permintaan balasan ICMP yang sesuai kembali ke alamat IP palsu (korban).

Langkah 4. Ini akan mengirimkan sejumlah besar balasan gema ICMP ke korban dan jaringannya sehingga menyebabkan degradasi jaringan atau penolakan total layanan.

Fase 3 - Menjaga Akses & Menutupi Jejak

Setelah penyerang berhasil mengkompromikan suatu sistem, salah satu cara untuk menyembunyikan informasi saat sedang dikirim melalui jaringan adalah dengan menggunakan teknik yang disebut tunneling. Tunneling melibatkan penyembunyian satu protokol di dalam protokol lain.

Loki2 adalah salah satu implementasi yang digunakan Penerowongan protokol ICMP dan UDP untuk mendapatkan shell terbalik dari sistem yang diserang.

Langkah-langkah untuk menggunakan Loki2 diilustrasikan di bawah ini:

Langkah 1. Penyerang mendapatkan root pada sistem korban.

Langkah 2. Penyerang mendapatkan Loki2 dan mengkompilasinya di mesin.

Langkah 3. Penyerang sekarang meluncurkan klien Loki2 pada mesin penyerang dan mendapatkan shell terbalik pada host korban.

Langkah 4. Sekarang penyerang memiliki akses shell ke mesin korban sambil menyalurkan lalu lintas melalui paket data ICMP normal.

Dalam serangan seperti itu, lalu lintas yang dipertukarkan antara klien Loki & server Loki hampir terselubung karena tidak ada port mendengarkan yang dibuka pada mesin korban dan bahkan lalu lintas dapat dienkripsi dengan algoritma enkripsi seperti Blowfish atau DH untuk perlindungan tambahan. .

Loki2 ketika diimplementasikan sebagai modul kernel akan lebih tersembunyi karena bahkan tidak akan memiliki proses yang akan duduk dan menunggu lalu lintas ICMP yang berpotensi terdeteksi oleh administrator waspada.

Mencatat serangan Distributed Denial Of Service (DDOS) baru-baru ini, kita telah melihat bahwa ICMP telah digunakan di hampir semua alat tersebut untuk komunikasi rahasia antara klien DDOS dan program penangan penyerang. Beberapa contoh adalah TFN2K dan Stacheldraht.

Kesimpulan

Kami telah melihat di seluruh makalah ini bahwa ICMP dapat dan telah digunakan dalam banyak fase kemajuan penyerang dalam kompromi sistem. Dalam banyak kasus, alat mudah tersedia di Internet untuk diunduh.

Kami juga telah melihat bahwa ICMP tidak hanya digunakan dalam fase pengintaian & pemindaian yang paling dipahami tetapi juga telah digunakan untuk mengeksploitasi sistem serta dalam kasus tertentu sebagai saluran rahasia untuk komunikasi penyerang.

Referensi

1. Madalina Baltatu, Antonio Lioy, Fabio Maino, Daniele Mazzocchi. "Security Issues in Control, Management and Routing Protocols". 22-25 May 2000. URL : http://www.terena.nl/tnc2000/proceedings/3A/3a2.pdf
2. "Nmap" URL : http://www.insecure.org/nmap
3. "Firewalk" URL : http://packetstorm.decepticons.org/UNIX/audit/firewalk/
4. Craig A. Huegen. "Smurf Information". 7 February, 2000 URL : http://www.pentics.net/denial-of-service/white-papers/smurf.cgi
5. Mark Gibbs. "Attacked by Smurf". February 22, 1999. URL : http://www.nwfusion.com/archive/1999b/0222gearhead.html
6. "Denial Of Service Attack Swords". May 2000. URL : http://fravia1.virtualave.net/fraviamirror/dod1.htm