Study on Linkage Mechanism of IDS and Firewall Based on

SNMP Protocol

Analisa:

Didalam journal ini memperkenalkan karakteristik Firewall dan Intrusion Detection Systems (IDS) dan menunjukkan kekurangan dari Firewall. Kemudian menganalisa mekanisme linkage dari Firewall dan IDS berdasarkan SNMP Protocol, dan mengedepankan sejenis model linkage berdasarkan IDS dan Firewall.

SNMP (Simple Network Management Protocol) dari IETF sekarang umum digunakan dalam manajemen jaringan. Model SNMP terutama terdiri dari stasiun manajemen jaringan, simpul manajemen, Agen SNMP. Jaringan manajemen menyelesaikan sebagian besar komputasi jaringan yang merupakan manajemen terpusat.



Simple manajemen jaringan adalah inti dari seluruh sistem. Manajemen node dapat berupa perangkat yang bertukar informasi dengan dunia luar seperti host, router, printer dan sebagainya. Manajemen harus mampu menjalankan SNMP Agent untuk memastikan komunikasi yang dengan stasiun manajemen jaringan, pada saat yang sama Agent SNMP juga mempertahankan database lokal yang menyimpan status agent SNMP dan historical informasi. Berdasarkan fitur struktur manajemen jaringan SNMP di atas, kita dapat mengatur variabel MIB untuk menyimpan aturan penyaringan paket dan variabel negara lainnya dalam node manajemen, sehingga SNMP Agent di node manajemen dapat membaca perintah langsung SNMP dan status dari firewall melalui loading modul.

Kini ada banyak toolkit yang berkembang dari SNMP di internet yang paling terkenal adalah dari NET-SNMP, kit ini menyediakan Agen SNMP di sistem operasi yang berbeda seperti Windows dan Linux, dan sebagian besar mendukung format pesan SNMPvl,SNMPv2c (berbasis komunitas berbasis string), SNMPv2u (user-based) dan protoco SNMPv3.

Setelah Implementasi SNMP interface, firewall bisa menggunakan ini untuk berkomunikasi dengan IDS. Saat hacker mengintrusi dari jaringan eksternal, firewall first bypass, sebagian intrusi dikecualikan karena melanggar peraturan keselamatan dari firewall, tapi mungkin ada bagian dari intrusi yang akan melewati firewall atau bahkan menyerang dari jaringan internal pelanggan dan akan melewati firewall. Serangan ini meski lolos tapi diperiksa oleh IDS setelah paket data yang dicurigai diurutkan berdasarkan modul pre-treatment, mereka akan dikirim sesuai modul untuk pemeriksaan lebih lanjut. IDS menemukan beberapa paket data sesuai dengan beberapa fitur serangan yang diatur library dengan memindai tree-rules dan memotong permintaan akses IP segera atau alarm kemudian dikirim perintah SNMP ke firewall untuk menambahkan atau memodifikasi peraturan keamanan baru. Lalu firewall mengirim sinyal respons SNMP yang sesuai dengan IDS untuk menginformasikan apakah modifikasi aturan firewall tersebut sukses