PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 439 di lunedì 12 novembre 2001

I termini da sapere - Un breve glossario sulla sicurezza in rete 2/2

Articolo a cura di Luca Garbato. Paura di perdersi tra le parole della sicurezza? Ecco un prontuario con quello che c'è da sapere sulla protezione delle reti.

Proseguiamo la pubblicazione dell'articolo a cura di Luca Garbato.

Paura di perdersi tra le parole della sicurezza? Ecco un prontuario con quello che c'è da sapere sulla protezione delle reti

Attacchi DoS
Denial of Service è il nome della famiglia di attacchi dell'ultima generazione. Questi attacchi non mirano alla distruzione o al furto dei dati, bensì all'interruzione di un servizio, come quello di un server Web o di un sever di posta. La loro particolarità sta nel trasmettere pacchetti che, in qualche modo, ingannano il protocollo producendo effetti imprevedibili. Gli attacchi appartenti a questa famiglia sono diversi: alcuni si basano su errori nell'implementazione dei protocolli, altri congestionano la rete vittima con traffico fittizio. Attualmente molti dei maggiori siti Internet sono stati vittime di uno di questi attacchi (o di una loro combinazione). Segue una breve panoramica dei più famosi.

Ping of Death
Questo è uno degli attacchi DoS più celebri (e anziani). Il gioco è semplice: basta inviare all'host preso di mira una pacchetto ICMP (con il programma di utilità PING) con un carico di dati maggiore di 64 Kb. La vittima, non sapendo come gestire le informazioni di frammentazione del pacchetto, produce effetti indesiderati, come il riavvio o, addirittura, il crash del sistema. Al giorno d'oggi i produttori di sistemi operativi hanno posto un rimedio a questo tipo di attacco, rendendo disponibili apposite patch.

SYN Flood
Questo attacco si basa su un difetto architetturale del protocollo e, più precisamente, sulla procedura di avvio delle transazioni TCP (tecnicamente conosciuta come three way handshake). Questa procedura ha luogo ogni volta che due macchine stabiliscono una sessione: la prima invia un segmento che contiene una richiesta SYN (sincronia); la macchina a cui viene spedito il segnale risponde con un segmento che contiene i messaggi SYN e ACK (acknowledge); a questo punto la prima macchina dovrebbe rispondere con un segnale ACK, in modo da far partire la sessione. Prima di inviare la risposta, le macchine che ricevono una richiesta di apertura di una sessione, accantonano in una zona della memoria la richiesta: se la procedura viene eseguita correttamente e la sessione viene stabilita, la richiesta verrà rimossa dalla memoria. Gli attacchi SYN Flood si basano proprio su questo particolare: se si riesce a fare in modo che l'invio di numerose richieste congestioni questa zona di memoria della vittima, la macchina presa di mira andrà in blocco, nel senso che non potrà più garantire il servizio di rete fino a che le numerose richieste non vengano soddisfatte (cosa che non avverrà mai). Con gli attacchi SYN Flood la procedura di avvio di una sessione tra due macchine viene eseguita per due terzi: invece di passare alla treza fase (ACK), chi attacca invia un nuovo segnale SYN, ricevendo una nuova risposta SYN/ACK e facendo ricominciare la procedura. Anche in questo caso, però, I produttori di sistemi operativi di rete hanno reso disponibili delle patch e quasi tutte le piattaforme Firewall attualmente in commercio permettono di difendersi da questo attacco.

Smurf Attack
Si tratta di un attacco molto pericoloso, diretto al router che collega la propria rete locale a Internet e che si basa sulla funzione di direct broadcast addressing. Chi attacca utilizzando questa tecnica dirige una serie di richieste di echo ICMP (con il comando PING) all'indirizzo di broadcast della rete vittima. Dal momento che tutto il traffico di rete generato è diretto a un indirizzo di broadcast, questo verrà inoltrato a tutti gli host della rete locale (cioè il 'broadcast domain'). Questo traffico, insieme alle risposte

alla richiesta echo del comando Ping genereranno un traffico molto sostenuto, soprattutto nel caso che la propria rete sia composta da molti host. Questo traffico finisce per saturare la rete, rendendo impossibile, di fatto, la comunicazione (e, quindi, si verifica un blocco dei servizi).

IP Spoofing
Si tratta di una tecnica, più che di un attacco, molto complessa. In pratica, chi attacca cerca di collegarsi a un server rubando l'identità (partendo dall'indirizzo IP) di una macchina di cui il server 'si fida'. Questa tecnica è molto complessa, dal momento che viene dapprima 'bloccata' una macchina con un attacco DoS, quindi ci si presenta alla vittima con l'identità della macchina bloccata (questo avviene simulando il traffico di ritorno che il vero host non sta più generando). Questa tecnica viene generalmente utilizzata per guadagnare l'accesso di amministratore su una rete privata.

Articolo a cura di Luca Garbato - Siosistemi.
Articolo pubblicato su Networking Italia.
