In che modo il monitor del traffico di layer 4 blocca il traffico?

Domanda:

In che modo il monitor del traffico di layer 4 blocca il traffico se riceve solo traffico con mirroring?

Ambiente:

Monitoraggio del traffico di layer 4 - L4TM configurato per bloccare il traffico sospetto

Soluzione:

Cisco Web Security Appliance (WSA) dispone di un servizio L4TM (Layer 4 Traffic Monitor) incorporato che può bloccare le sessioni sospette su tutte le porte di rete (TCP/UDP 0-65535).

Per poter monitorare o bloccare queste sessioni, il traffico deve essere reindirizzato al server di archiviazione (WSA), utilizzando un dispositivo TAP (Test Access Port) o configurando una porta mirror sui dispositivi di rete (porte SPAN sui dispositivi Cisco). La modalità in linea L4TM non è ancora supportata.

Anche se il traffico viene solo sincronizzato (copiato) dalle sessioni originali all'accessorio, il server WSA può comunque bloccare il traffico sospetto rimuovendo una sessione TCP o inviando messaggi ICMP "host non raggiungibile" per le sessioni UDP.

Per sessioni TCP

Quando il WSA L4TM riceve un pacchetto da o verso un server e il traffico corrisponde a un'azione di blocco, L4TM invia un datagramma TCP RST (reset) al client o al server a seconda dello scenario. Un datagramma TCP RST è un normale pacchetto con il flag TCP RST impostato su 1.

Il destinatario di un RST prima lo convalida, quindi cambia stato. Se il ricevitore era nello stato LISTEN, lo ignora. Se il ricevitore si trovava nello stato SYN-RECEIVED ed era stato precedentemente nello stato LISTEN, il ricevitore torna allo stato LISTEN, altrimenti interrompe la connessione e passa allo stato CLOSED. Se il ricevitore si trovava in un altro stato, interrompe la connessione e avvisa l'utente, quindi passa allo stato CLOSED.

Esistono due casi da considerare (in entrambi i casi gli utenti/client sono dietro un firewall):

La prima si verifica quando il pacchetto sospetto proviene dall'esterno del firewall verso un client della rete interna. L'RST verrà inviato al server e in questo caso raggiungerà il firewall che di solito non inoltrerà l'RST ma terminerà la sessione in quanto crederà che l'RST sia effettivamente arrivato dal client. In questo caso, l'IP di origine dell'RST sarà l'IP oggetto di spoofing del client. Il client terminerà la sessione.

Un secondo caso si verificherebbe quando il pacchetto proviene dal client nella rete interna e

viene indirizzato a un server esterno (esterno al firewall). L'RST viene quindi inviato al client e l'IP di origine dell'RST sarà l'IP oggetto di spoofing del server.

Per sessioni UDP

Analogamente, il protocollo WSA esegue il traffico sospetto proveniente da una sessione UDP. Tuttavia, anziché inviare una richiesta TCP RST, l'L4TM invia messaggi ICMP "host non raggiungibile" (codice ICMP 3 1) al client o al server. Tuttavia, in questi casi non si verifica uno spoofing IP, poiché il messaggio ICMP indica che l'host non è raggiungibile e non può inviare i pacchetti. In questo caso, l'IP di origine sarà l'IP del WSA.

Questi pacchetti RST e ICMP vengono inviati dal WSA utilizzando la tabella di routing dei dati, tramite M1, P1 o P2, a seconda dell'implementazione.