Comment le bloc de moniteur du trafic de la couche 4 trafique-t-il ?

Question :

Comment la couche 4 trafique-t-elle le trafic de bloc de moniteur si elle reçoit seulement le trafic reflété ?

Environnement :

Moniteur du trafic de la couche 4 - L4TM configuré pour bloquer le trafic méfiant

Solution :

L'appliance de sécurité Web de Cisco (WSA) a un service intégré du moniteur du trafic de la couche 4 (L4TM) qui peut bloquer des sessions méfiantes à travers tous les ports de réseau (TCP/UDP 0-65535).

Pour pouvoir surveiller ou bloquer le trafic de ces sessions doit être réorienté au WSA, à l'aide d'un périphérique de PRISE (port d'accès de test), ou en configurant un port de miroir sur les périphériques de réseau (ports SPAN sur des périphériques de Cisco). Le mode intégré L4TM n'est pas pris en charge encore.

Quoique le trafic soit seulement reflété (copié) des sessions initiales à l'appliance, le WSA peut encore bloquer le trafic méfiant en reposant une session TCP ou en envoyant l'ICMP messages inaccessibles de « hôte » pour des sessions d'UDP.

Pour des sessions TCP

Quand le WSA L4TM reçoit un paquet à ou d'un serveur et le trafic apparie une action de bloc, L4TM enverra un datagramme du TCP RST (remise) au client ou au serveur selon le scénario. Un datagramme du TCP RST est juste un paquet régulier avec l'indicateur du TCP RST réglé à 1.

Le récepteur d'un RST d'abord le valide, puis change l'état. Si le récepteur était dans l'état d'ÉCOUTE, il l'ignore. Si le récepteur était dans l'état SYN-RECEIVED et avait précédemment été dans l'état d'ÉCOUTE, alors le récepteur revient à l'état d'ÉCOUTE, autrement le récepteur abandonne la connexion et va à l'état FERMÉ. Si le récepteur était dans n'importe quel autre état, il abandonne la connexion et informe l'utilisateur et va à l'état FERMÉ.

Il y a deux cas à considérer (dans les deux utilisateurs/clients de cas soyez derrière un Pare-feu) :

- Premier est quand le paquet méfiant est livré de l'extérieur du Pare-feu vers un client dans le réseau interne. Le RST sera envoyé au serveur et dans ce cas il obtiendra au Pare-feu qui n'expédiera habituellement pas le RST mais il terminera la session car il croire que le RST est provenu réellement le client. Dans ce cas le source ip du RST sera l'IP charrié du client. Le client terminera la session.

Un deuxième cas serait quand le paquet provient le client dans le réseau interne et va à un serveur externe (en dehors du Pare-feu). Le RST est alors envoyé au client et le source ip RST sera l'IP charrié du serveur.

Pour des sessions d'UDP

Un comportement semblable est exécuté par WSA quand le trafic méfiant est d'une session d'UDP, mais au lieu d'envoyer le TCP RST, le L4TM enverra les messages d'inaccessibilité d'hôte d'ICMP (code de type ICMP 3 1) au client ou au serveur. Cependant, il n'y a pas d'usurpation d'adresse IP dans des ces cas car le message ICMP déclare que l'hôte est inaccessible ainsi il ne peut pas envoyer des paquets. Le source ip dans ce cas sera l'IP de WSA.

Ces des paquets de RSTs et d'ICMP sont envoyés du WSA utilisant la table de routage de données, par l'intermédiaire de M1, P1, ou P2, selon le déploiement.