Comment le Moniteur du trafic de couche 4 bloque-t-il le trafic ?

Question :

Comment le Moniteur du trafic de couche 4 bloque-t-il le trafic s'il ne reçoit que du trafic en miroir ?

Environnement :

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

Solution :

L'appareil de sécurité Web Cisco (WSA) dispose d'un service L4TM (Layer 4 Traffic Monitor) intégré qui peut bloquer les sessions suspectes sur tous les ports du réseau (TCP/UDP 0-65535).

Pour pouvoir surveiller ou bloquer ces sessions, le trafic doit être redirigé vers le WSA, soit à l'aide d'un périphérique TAP (Test Access Port), soit en configurant un port miroir sur les périphériques réseau (ports SPAN sur les périphériques Cisco). Le mode en ligne L4TM n'est pas encore pris en charge.

Même si le trafic est uniquement mis en miroir (copié) depuis les sessions d'origine vers l'appliance, le WSA peut toujours bloquer le trafic suspect en remettant une session TCP ou en envoyant des messages ICMP « hôte inaccessible » pour les sessions UDP.

Pour les sessions TCP

Lorsque le WSA L4TM reçoit un paquet à un serveur ou en provenance de celui-ci et que le trafic correspond à une action de blocage, le L4TM envoie un datagramme TCP RST (reset) au client ou au serveur selon le scénario. Un datagramme TCP RST est un paquet normal dont l'indicateur TCP RST est défini sur 1.

Le destinataire d'une TVD la valide d'abord, puis change d'état. Si le récepteur était à l'état LISTEN, il l'ignore. Si le récepteur était à l'état SYN-RECEIVED et qu'il était précédemment à l'état LISTEN, le récepteur revient à l'état LISTEN, sinon le récepteur abandonne la connexion et passe à l'état CLOSED. Si le récepteur se trouvait dans un autre état, il abandonne la connexion et informe l'utilisateur et passe à l'état CLOSED.

Deux cas doivent être pris en compte (dans les deux cas, les utilisateurs/clients sont derrière un pare-feu) :

- La première est lorsque le paquet suspect vient de l'extérieur du pare-feu vers un client du réseau interne. La TVD sera envoyée au serveur et, dans ce cas, elle sera acheminée au pare-feu qui habituellement ne transmettra pas la TVD, mais elle mettra fin à la session, car elle croit que la TVD provient du client. Dans ce cas, l'adresse IP source de la TVD sera l'adresse IP usurpée du client. Le client met fin à la session.

Un deuxième cas est celui où le paquet provient du client du réseau interne et est destiné à un serveur externe (en dehors du pare-feu). La TVD est ensuite envoyée au client et l'adresse IP source de la TVD est l'adresse IP usurpée du serveur.

Pour les sessions UDP

Un comportement similaire est exécuté par WSA lorsque le trafic suspect provient d'une session UDP, mais au lieu d'envoyer TCP RST , L4TM envoie des messages ICMP d'hôte inaccessible (code ICMP de type 3 1) au client ou au serveur. Cependant, il n'y a pas d'usurpation d'adresse IP dans ces cas, car le message ICMP indique que l'hôte est inaccessible et qu'il ne peut donc pas envoyer de paquets. L'adresse IP source dans ce cas sera l'adresse IP de WSA.

Ces paquets RST et ICMP sont envoyés depuis le WSA à l'aide de la table de routage des données, via M1, P1 ou P2, selon le déploiement.