¿Cómo el bloque del control de tráfico de la capa 4 trafica?

Pregunta:

¿Cómo el control de tráfico de la capa 4 bloquea el tráfico si está recibiendo solamente el tráfico duplicado?

Entorno:

Control de tráfico de la capa 4 - L4TM configurado para bloquear el tráfico sospechoso

Solución:

El dispositivo de seguridad de la red de Cisco (WSA) tiene un servicio incorporado del control de tráfico de la capa 4 (L4TM) que pueda bloquear las sesiones sospechosas a través de todos los puertos de red (TCP/UDP 0-65535).

Para poder monitorear o bloquear el tráfico de estas sesiones se debe reorientar al WSA, usando un dispositivo del GOLPECITO (puerto de acceso de la prueba), o configurando un puerto del espejo en los dispositivos de red (puertos SPAN en los dispositivos de Cisco). El modo de instalación en línea L4TM no se soporta todavía.

Aunque el tráfico se duplica solamente (copiado) de las sesiones originales al dispositivo, el WSA puede todavía bloquear el tráfico sospechoso descansando a una sesión TCP o enviando ICMP “imposible acceder al host” mensajes para las Sesiones UDP.

Para las sesiones TCP

Cuando el WSA L4TM recibe un paquete a o desde un servidor y el tráfico hace juego una acción del bloque, L4TM enviará un datagrama TCP RST (restauración) al cliente o al servidor dependiendo del escenario. Un datagrama TCP RST es apenas un paquete regular con el indicador TCP RST fijado a 1.

El receptor de un RST primero valida lo, después el estado de los cambios. Si el receptor estaba en el estado del ESCUCHAR, lo ignora. Si el receptor estaba en el estado SYN-RECEIVED y había estado previamente en el estado del ESCUCHAR, después el receptor vuelve al estado del ESCUCHAR, si no el receptor aborta la conexión y va al estado cerrado. Si el receptor estaba en cualquier otro estado, aborta la conexión y aconseja al usuario y va al estado cerrado.

Hay dos casos a considerar (en ambos usuarios/clientes de los casos esté detrás de un Firewall):

- Primer uno es cuando el paquete sospechoso está viniendo desde fuera del Firewall hacia un cliente en la red interna. El RST será enviado al servidor y en este caso conseguirá al Firewall que no remitirá generalmente el RST pero terminará la sesión pues creerá que el RST vino realmente del cliente. En este caso el IP de la fuente del RST será el IP del spoofed del cliente.

El cliente terminará la sesión.

Un segundo caso sería cuando el paquete está viniendo del cliente en la red interna y va a un servidor externo (fuera del Firewall). El RST entonces se envía al cliente y el IP de la fuente RST será IP del spoofed del servidor.

Para las Sesiones UDP

Un comportamiento similar es realizado por WSA cuando el tráfico sospechoso es de una Sesión UDP, pero en vez de enviar TCP RST, el L4TM enviará los mensajes ICMP imposible acceder al host (código del tipo 3 ICMP 1) al cliente o al servidor. Sin embargo, no hay IP spoofing en estos casos pues los estados del mensaje ICMP que el host es inalcanzable así que él no pueden enviar los paquetes. El IP de la fuente en este caso será el IP WSA.

Estos RST y paquetes icmp se envían del WSA usando la tabla de ruteo de los datos, vía el M1, el P1, o el P2, dependiendo del despliegue.