

Monitoreo con puerto SPAN - Realizado por Aar3n Mizrachi en fecha 26/05/2008

Monitoreo con puerto SPAN

Por Aar3n Mizrachi <unmanarc@gmail.com>, 26/05/2008 – 17:16

<http://www.unmanarc.com/v1/?q=node/8>

Revisi3n 1.1, 24/05/2009

Muchos administradores de red utilizan incorrectamente el puerto SPAN para aplicaciones de monitoreo en red, IDS y otros equipos que requieran analizar el tráfico de la red, no están conscientes que ese puerto fue diseñado para redes Half-Duplex, y jamas para redes Full-Duplex.

Cuando la red esta en full-duplex, el SPAN port tiene una **perdida natural de paquetes** que no varía con el hardware.

¿Porque ocurre esto?

Imagínense que el switch tiene 3 puertos y es de 100Mbps, el puerto 1 es el uplink (Conectado a un router), el puerto 2 es una computadora cualquiera, y el puerto 3 es el SPAN port.

Si usted conectase un servicio de monitoreo y detección de intrusos tipo SNORT en el SPAN port, este recibiría un canal de 100Mbps RX con los paquetes replica de los puertos del switch 1 y 2.

Pero hasta que punto es cierto que recibes los paquetes replica?

Imaginemos que solo queremos capturar el puerto 1 (Uplink) donde veremos si se esta produciendo un ataque, este puerto tiene un TX de 100Mbps y un RX de 100Mbps. En dicho caso, si en upload usa 50Mbps y en download usa 51Mbps, ambos (101Mbps) tendrían que ser enviados por un TX de 100Mbps via SPAN port.

En el peor de los casos, donde el consumo TX/RX del uplink este al 100%, se tendrían que enviar 200Mbps por un canal TX de 100Mbps (SPAN PORT), ya que el RX del SPAN port no se usa para enviar data.

Generalmente que hace un equipo avanzado?

1. Buffering hasta donde pueda (Es saturado en pocos segundos)
2. Descartar paquetes y no enviarlos, lo cual hace que libnids y otros sistemas de reconstrucción sean poco efectivos detectando patrones via TCP

Que debo hacer para monitorear mi red?

Existen varias soluciones a ello:

- La utilización de un BRIDGE entre el switch y el cable de uplink, el cual dejará pasar los paquetes de forma transparente. Usted puede configurar un bridge en linux con dos tarjetas de red utilizando brctl (Instalar bridge-utils). Dentro del bridge usted podrá utilizar SNORT para monitorear
- La utilización de bonding+network tap. Un network TAP es una solución parecida al SPAN port, sin embargo, utiliza dos cables de TX para enviar el TX del cable del uplink y el RX del cable del uplink, luego se puede mezclar eso en una interfaz bond0 (linux)
- Utilización de Half-Duplex o un Hub. Se puede configurar el puerto de uplink en modo half-duplex (Los administradores odian esto porque puede reducir el performance), el hub es como un network tap, pero en realidad es la emulación viva del half duplex que se puede configurar en el switch.
- Utilización de un puerto de mayor al doble de la velocidad del uplink como puerto SPAN.

En conclusión, no es buena idea realizar mirroring de paquetes a un puerto sin conocer los riesgos y la poca efectividad que esto tiene. Muchos administradores de red no lo notan porque simplemente no se realiza un estudio detallado de eficiencia, en caso de ver un registro en el SNORT que llegó cuando la red no estaba saturada, o por azar, asumen que el sistema funciona perfectamente cuando no es asi.