TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“INVESTIGACION SIEM”

UNIDAD 3

Sistemas de Detección y Prevención IDS e IPS

Son muchos los delincuentes que, con ahínco, se esfuerzan en lograr acceder libremente a nuestros sistemas, para obtener algún tipo de beneficio: sea directamente económico –exigiendo un rescate para recuperar nuestra información, como tras un ataque ransomware-, o con la finalidad de espiar a la compañía, para lograr alguna ventaja competitiva. Para luchar contra esas intromisiones, actualmente disponemos de diversos medios. Y, con la ayuda de Punt Informàtic, podemos hacerlo tanto de forma reactiva, como ya de manera proactiva.

Monitorizar el tráfico entrante

Tanto los Sistemas de Detección de Intrusos (IDS) como los Sistemas de Prevención de Intrusos (IPS) aumentan la seguridad de nuestras redes. Ambos sistemas se encargan de vigilar el tráfico, y para ello examinan la red y los puertos, analizando paquetes de datos, para detectar patrones sospechosos. El factor que asegura el éxito de un IDS o un IPS es su capacidad para identificar firmas ya reconocidas. Y la diferencia más destacada entre los dos sistemas, es cómo reaccionan cuando han detectado un ataque.

Los IDS contienen una extensa base de datos actualizada, con multitud de firmas de ataque conocidas. La solución IDS se encarga de monitorizar el tráfico entrante -mediante un exhaustivo análisis de red y un barrido de puertos-, y todo ello va comparándolo con la información que dispone sobre elementos maliciosos. Ante cualquier actividad sospechosa, este sistema de detección emite una alerta anticipada, que dirige a los administradores del sistema. Y son estos responsables TI quienes deben tomar las correspondientes medidas.

Decidir sobre el control de acceso

Por otra parte, los IPS surgieron como extensiones de las soluciones IDS -con las que continúan en relación-, y fueron desarrollados para, no sólo encargarse de la búsqueda de actividad maliciosa, sino también intentar detenerla. Estos dispositivos proactivos de seguridad de red, monitorizan el tráfico de la misma de forma continua, así como las todas las actividades de un entorno TI. El IPS controla de acceso en una red informática, protegiendo a los sistemas computacionales de abusos y ataques.

Situando sistemas de detección en las vías de tráfico, los IPS resuelven ambigüedades en las tareas de monitorizar de forma pasiva las redes de computadoras. Para combatir las actividades potencialmente maliciosas, este software es capaz de tomar decisiones sobre el

control de acceso, basándose en los contenidos del tráfico -en lugar de puertos o direcciones IP-. Por ello, debemos reconocer que los IPS representan una importante mejora respecto a las tradicionales tecnologías de cortafuegos.

Diversas formas de detección

El IPS se sitúa entre el firewall y el resto de la red de la empresa, supervisando los paquetes de entrada. Y, como antes de decidir dejarlos entrar, comprueba para qué se usan realmente, consigue evitar que el tráfico sospechoso acceda al resto de la red corporativa. Según la forma de detección, un IPS puede señalar tráfico malicioso basándose en firmas -como lo haría un antivirus-. También puede hacerlo si se basa en anomalías, en función del patrón de un comportamiento normal de tráfico. O incluso puede intervenir tomando como base políticas de seguridad muy específicas.

Así, pues, tanto los IDS como los IPS, basan su éxito en la habilidad para identificar firmas ya reconocidas de ataques maliciosos. En el otro extremo, lo que diferencia a estos dos sistemas, son las subsiguientes acciones que emprenden cuando ya han detectado un ataque. De ahí que se afirme que un IDS protege a una red o equipo de manera reactiva, mientras que un IPS lo hace de manera proactiva. Otra función destacable de estos dispositivos de red, es que permiten grabar información, para mantener un histórico de la actividad desarrollada, así como generar informes.