FORTINET
NSE Training Institute

NSE 2 Sandbox Scripts—Spanish Version

¡Hola! En esta clase, veremos qué es un sandbox, por qué se creó y cómo ha evolucionado.

Un sandbox, en el contexto de la seguridad informática, es un sistema que limita las acciones de una aplicación, como abrir un documento de Word o un explorador, a un entorno virtual aislado. En este entorno seguro, se analizan las distintas interacciones de una aplicación en busca de posibles intentos maliciosos. Si ocurre algo inesperado o peligroso, solo afecta al sandbox, y no a las otras computadoras o dispositivos de la red.

En general, la tecnología de sandbox es administrada por el equipo de seguridad de la información de una empresa, pero también la utilizan los equipos de operaciones de escritorio, redes y aplicaciones para reforzar la seguridad en sus respectivos ámbitos.

Las amenazas aprovechan las vulnerabilidades de las aplicaciones legítimas para poner en riesgo un dispositivo y, a partir de ahí, moverse por la red para infectar a otros. Aprovechar una vulnerabilidad desconocida se conoce como ataque de día cero. Antes de que existieran los entornos seguros, no había un método efectivo para detener un ataque de este tipo. Tanto los firewalls como los programas antivirus podían frenar una amenaza conocida, pero ante un ataque de día cero no podían hacer nada.

El sandbox proporcionaba un entorno virtual aislado que imitaba distintos equipos informáticos, sistemas operativos y aplicaciones. Permitía que las amenazas potenciales se ejecutaran dentro de estos sistemas virtuales seguros. Si el entorno determinaba que el archivo o la actividad sospechosos no eran maliciosos, no se requería ninguna otra medida. En cambio, si se detectaba un intento malicioso, el archivo podía ponerse en cuarentena o la actividad podía detenerse en el dispositivo real.

Muchos de los primeros entornos de sandbox no podían integrarse del todo con otros dispositivos de seguridad dentro de la red. Aun si el entorno podía identificar y detener un ataque de día cero, la información vital sobre la amenaza no siempre se compartía a

tiempo con el resto de los dispositivos de seguridad de la red. Sin embargo, esta falla en la comunicación y la coordinación no se debía a un defecto en la tecnología de sandbox, sino más bien a una arquitectura de seguridad que estaba diseñada para brindar soluciones puntuales. Con este tipo de soluciones, que no podían integrarse por completo en productos de otros proveedores, los centros de operaciones de seguridad (SOC) necesitaban una consola de administración para cada producto. De este modo, los intentos por reunir información sobre amenazas resultaban difíciles e requerían mucho tiempo.

Los entornos de sandbox de segunda generación llegaron para corregir este enfoque fragmentario y gradual. Contaban con más herramientas de integración o trabajaban en conjunto con productos de otros proveedores para mejorar la integración. Como resultado, podían compartir de manera más efectiva información sobre amenazas con otros dispositivos de seguridad, como firewalls, gateways de correo electrónico y endpoints. Este nuevo enfoque de seguridad de red permitía a los analistas relacionar centralizadamente la información sobre amenazas y responder a ellas desde un único panel. Además, mediante un entorno integrado de seguridad de red, era posible compartir dicha información con un servidor en la nube, a fin de abarcar otras redes.

Actualmente, las amenazas están innovando en cuanto a técnicas de automatización e inteligencia artificial para acelerar la creación de nuevas versiones de malware. También buscan descubrir vulnerabilidades más rápido, con el objetivo de evadir y superar los métodos de defensa existentes. Para estar al día y agilizar la detección de las amenazas más recientes, es imprescindible incorporar la inteligencia artificial al proceso de análisis de amenazas en los entornos de sandbox.

Los ataques basados en la inteligencia artificial hicieron que fuera necesaria una tercera generación de entornos de sandbox, regida por un estándar de análisis de amenazas. Asimismo, había que hacer frente a las superficies expuestas a ataques cada vez más amplias, que son una consecuencia de la transformación digital de las empresas. Por

transformación digital entendemos la migración de datos, aplicaciones e infraestructura empresariales a la nube.

El reto de los análisis de amenazas basados en estándares surgió a partir de la dificultad para interpretar y comprender los métodos de ciberamenazas, que impedían que hubiera una respuesta eficiente. MITRE, una organización sin fines de lucro, propuso el marco ATT&CK, que describe las características más comunes de malware y las clasifica en categorías. Muchas organizaciones lo adoptaron como estándar para el análisis de amenazas. Así, los productos de seguridad tuvieron que ajustarse al marco ATT&CK. Este dotó a los dispositivos de seguridad de un lenguaje común para identificar, describir y categorizar las amenazas. Dicho lenguaje podía compartirse con dispositivos de otros proveedores y era fácil de comprender.

Por último, a medida que más empresas adoptan la transformación digital, son cada vez más las organizaciones, o partes de ellas, que están expuestas a ataques. Un ejemplo es la tecnología operativa (OT), que encontramos en el sector de servicios públicos, la industria manufacturera, el sector del petróleo y el gas, entre otros. Tradicionalmente, las empresas de estas industrias mantenían las redes operativas para uso interno, separadas de sus redes corporativas. Sin embargo, hoy es cada vez más frecuente que las redes de OT tengan acceso a las redes corporativas y a otras de proveedores externos. Otro ejemplo son las empresas que ofrecen aplicaciones, plataformas e infraestructura como servicio en la nube pública, como AWS y Azure, entre otros. Alojan aplicaciones para otras empresas, a las que se accede a través de internet. Estas nuevas áreas requieren una protección similar contra amenazas de día cero para reducir los riesgos de seguridad y asegurar la continuidad de la actividad empresarial. En consecuencia, la tecnología de sandbox evolucionó y ahora es capaz de cubrir las necesidades de estas y otras áreas a la par de su desarrollo.

El producto para entornos seguros de Fortinet es FortiSandbox™ e incluye todas las tecnologías más recientes que se mencionan aquí. Puede trabajar en conjunto con otros productos de seguridad para impulsar una defensa común que puede administrarse

desde un único panel, que en Fortinet se conoce como Security Fabric. Una pieza fundamental de Security Fabric es FortiGuard® Labs, que aporta AI learning a la tecnología sandbox.

Gracias por su tiempo, y no olvide responder el cuestionario a continuación.