**Aborda la ciberseguridad con la mentalidad de un atacante**

La ciberseguridad es un campo en constante cambio. Es un entorno de ritmo rápido en el que las nuevas amenazas y las tecnologías innovadoras pueden alterar tus planes en cualquier momento. Como profesional de la seguridad, debes prepararte anticipándote a los cambios..

Todo esto comienza con la identificación de las vulnerabilidades. En un video, aprendiste sobre la importancia de las **evaluaciones de vulnerabilidad,** el proceso de revisión interna de los sistemas de seguridad de una organización. En esta lectura, aprenderás cómo puedes utilizar los hallazgos de una evaluación de vulnerabilidad de manera proactiva al analizarlos desde la perspectiva de un atacante.

**Prepárate para todo**

Es importante tener un plan en caso de que algo salga mal. Pero ¿cómo puedes saber qué planear? En este campo, los equipos suelen realizar simulaciones de aquello que puede salir mal como parte de su estrategia de gestión de vulnerabilidades. Una forma de hacerlo es aplicando una mentalidad de atacante a las debilidades que se descubren.

Aplicar una mentalidad de atacante es muy parecido a realizar un experimento. Se trata de causar problemas en un entorno controlado y evaluar el resultado para obtener información. Adoptar una mentalidad de atacante es una habilidad beneficiosa en el campo de seguridad, ya que ofrece una perspectiva diferente sobre los desafíos que estás tratando de resolver. Los conocimientos que obtengas pueden ser valiosos cuando llegue el momento de establecer un plan de seguridad o modificar uno ya existente.



**Simulación de amenazas**

Un método para aplicar una mentalidad de atacante es utilizar simulaciones de ataque. Por lo general, estas actividades se realizan de una de dos maneras: de *forma proactiva* y *reactiva*. Ambas estrategias comparten un objetivo común, que es hacer que los sistemas sean más seguros.

* Las *simulaciones proactivas* asumen el papel de un atacante al explotar las vulnerabilidades y traspasar las defensas. Esto a veces se llama un ejercicio de equipo rojo.
* Las *simulaciones reactivas* asumen el papel de un defensor que responde a un ataque. Esto a veces se llama un ejercicio de equipo azul.

Cada tipo de simulación es un esfuerzo de equipo con el que podrías involucrarte como analista.

Los equipos proactivos tienden a dedicar más tiempo a planificar sus ataques que a realizarlos. Si te encuentras involucrado en uno de estos ejercicios, es probable que tu equipo despliegue una variedad de tácticas. Por ejemplo, podrían persuadir al personal para que divulgue sus credenciales de inicio de sesión mediante el uso de correos electrónicos ficticios para evaluar cuán conscientes son en la empresa  en cuanto a temas de seguridad.

Por otro lado, los equipos reactivos dedican sus esfuerzos a recopilar información sobre los activos que están protegiendo. Esto se hace comúnmente con la ayuda de herramientas de análisis de vulnerabilidades.

**Cómo escanear los problemas**

Quizá recuerdes que un **escáner de vulnerabilidades** es un software que compara automáticamente las vulnerabilidades y exposiciones comunes existentes con las tecnologías de la red. El escáner de vulnerabilidad se utiliza con frecuencia en el campo de la seguridad. Los equipos emplean una variedad de técnicas de escaneo para descubrir debilidades en sus defensas. Las simulaciones reactivas suelen valerse de los resultados de un escaneo para evaluar los riesgos y determinar formas de remediar un problema.

Por ejemplo, un equipo que realiza una simulación reactiva podría realizar un análisis de vulnerabilidad externo de su red. Todo el ejercicio podría seguir los pasos que aprendiste en un video sobre evaluaciones de vulnerabilidad:

* **Identificación:** Un servidor vulnerable se marca porque está ejecutando un sistema operativo (SO) desactualizado.
* **Análisis de vulnerabilidades:** Se investiga el sistema operativo desactualizado y sus vulnerabilidades.
* **Evaluación de riesgos:** Después de haber realizado tu debida diligencia, se califica la gravedad de cada vulnerabilidad y se evalúa el impacto de no solucionarla.
* **Remediación**: Finalmente, la información que recopilaste se puede usar para abordar el problema.

Durante una actividad como esta, a menudo generarás un informe de tus hallazgos. Estos pueden presentarse ante los proveedores de servicios o supervisores. Comunicar con claridad los resultados de estos ejercicios a otros es una habilidad importante para desarrollar como profesional de la seguridad.

**Encontrar soluciones innovadoras**

Muchos controles de seguridad que aprendiste se crearon como una respuesta reactiva ante riesgos. Esto se debe a que los agentes de amenaza buscan continuamente formas de eludir las defensas existentes. La aplicación efectiva de una mentalidad de atacante requerirá que te mantengas al tanto de las tendencias de seguridad y las tecnologías emergentes.

**Consejo profesional:** Recursos como la [Base de datos nacional de vulnerabilidades (NVD) de NIST](https://nvd.nist.gov/) pueden ayudarte a mantenerte al día en lo que respecta a vulnerabilidades comunes.

**Conclusiones clave**

Las evaluaciones de vulnerabilidad son una parte importante de la planificación de riesgos de seguridad. Como analista, es probable que participes en simulaciones proactivas y reactivas de estas actividades. Investigar las vulnerabilidades comunes solo alcanza hasta cierto punto. Es igual de importante que te mantengas al tanto de las nuevas tecnologías, para poder pensar con una mentalidad innovadora.