FIDE VIRTUAL

Curso introductorio de Ethical Hacking

Semana 02

Profesor: Randall Barnett Villalobos

Aplicación de la etapa de Escaneo

Sesión 05

FIDE VIRTUAL

Objetivos del módulo

- Familiarizar al estudiante con la configuración de OpenVAS, como escáner de vulnerabilidades, para la identificación de fallas de seguridad.
- Mostrar al estudiante la importancia de identificar, analizar y evaluar vulnerabilidades.
- Mostrar al estudiante como generar reportes de análisis de vulnerabilidades.

Requerimientos iniciales

- Se requiere que el estudiante trabaje con las máquinas virtuales configuradas en la sesiones anteriores, tales como: Ubuntu y Metasploitable.
- Se requiere que ambas máquinas virtuales puedan comunicarse en red (comprobación con ping).
- Se requiere que le estudiante haya instalado previamente OpenVas.
- Se requiere que el estudiante detenga cualquier ejecución de Antivirus o Firewall en su computadora anfitrión, para que estos interrumpan la ejecución normal del laboratorio.

Pasos para la evaluación de vulnerabilidades

Evaluación de las debilidades en la infraestructura tecnológica.

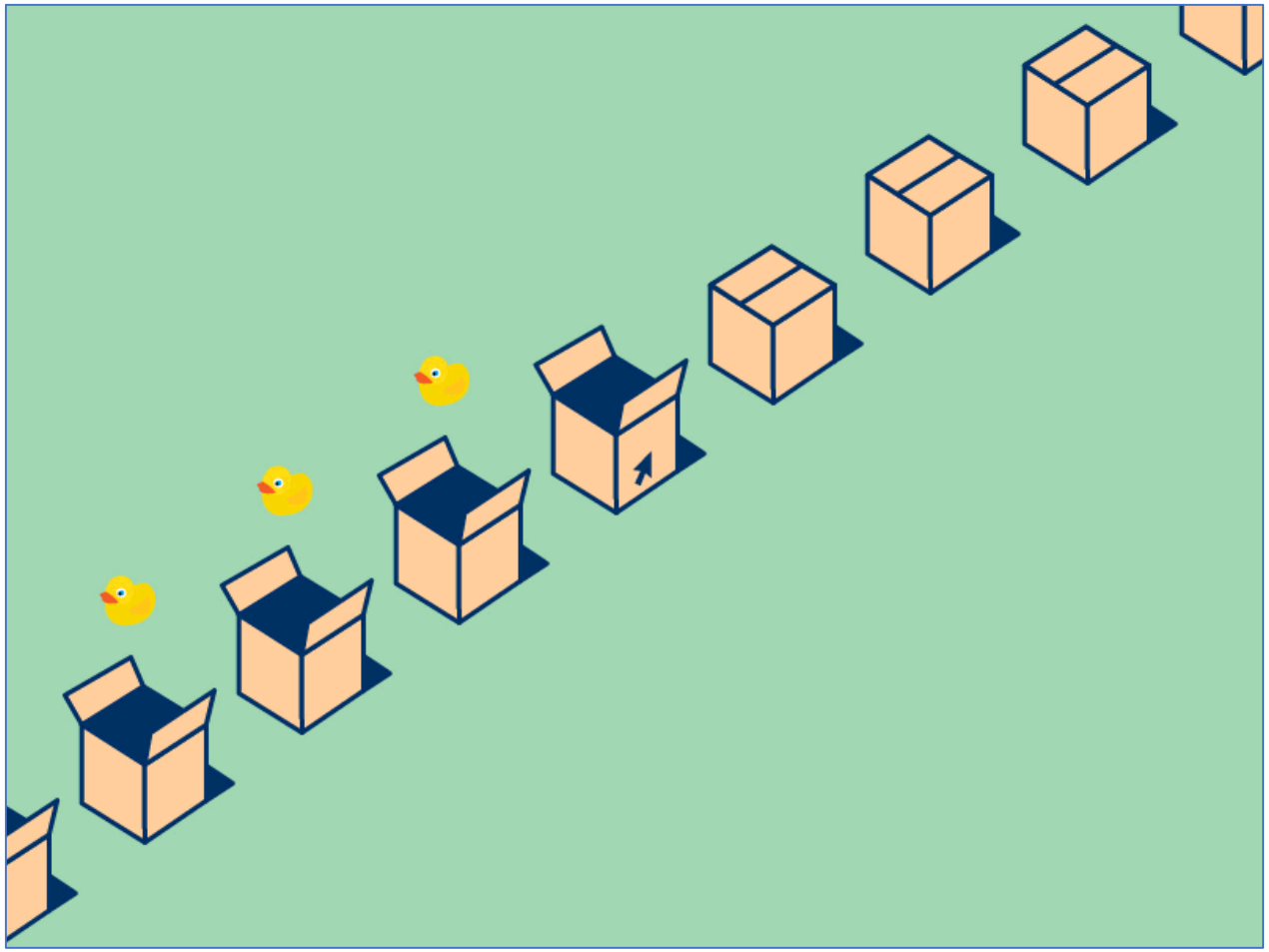
FIDE VIRTUAL

¿Qué es?

- También conocida como análisis de vulnerabilidades, se le considera una evaluación ya que además de abarcar la fase de análisis, también involucra una valoración de las debilidades identificadas, utilizando para ello diferentes criterios que permiten calificar y cuantificar su impacto.

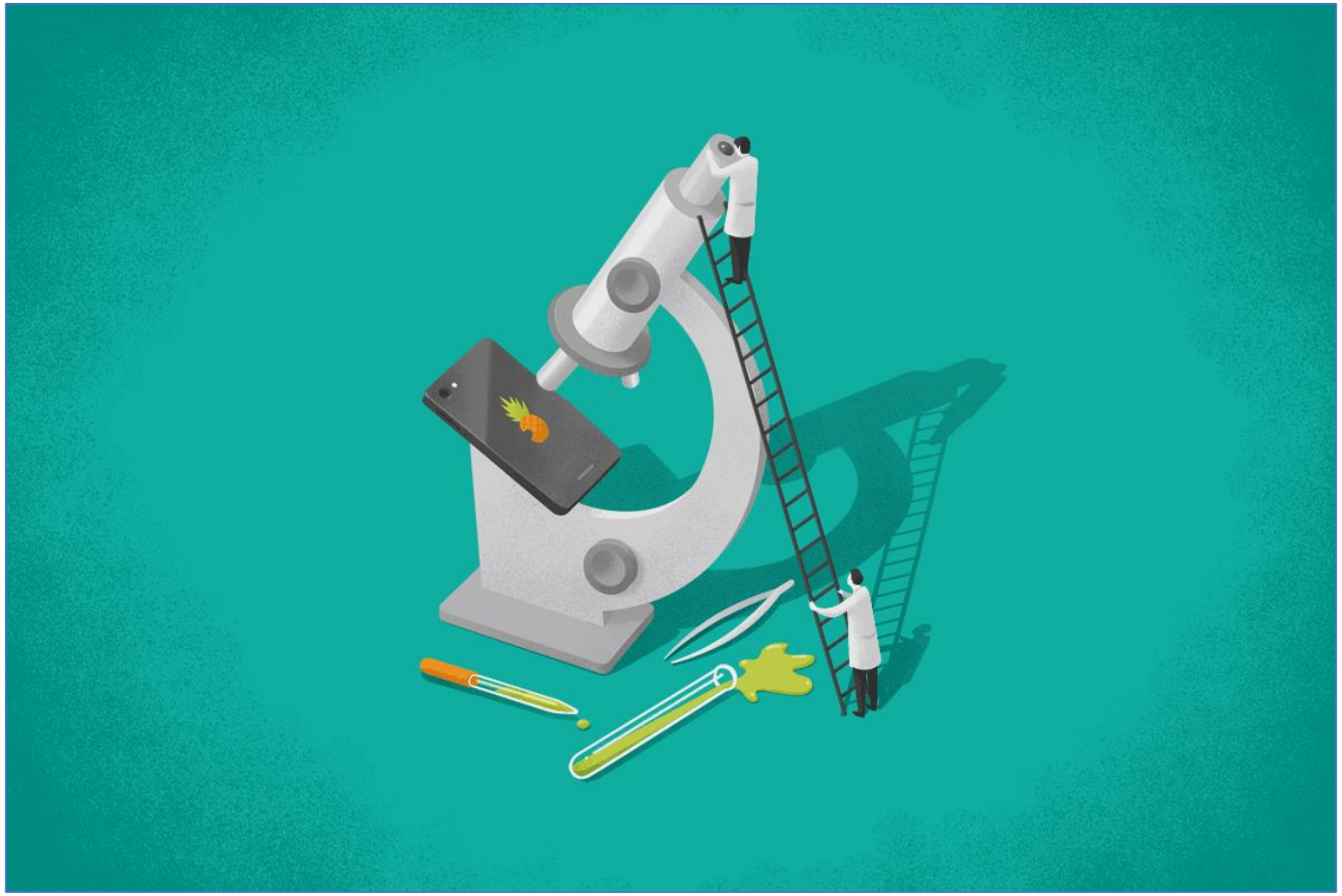
Obtener la aprobación para la evaluación de vulnerabilidades

Generar un inventario de activos

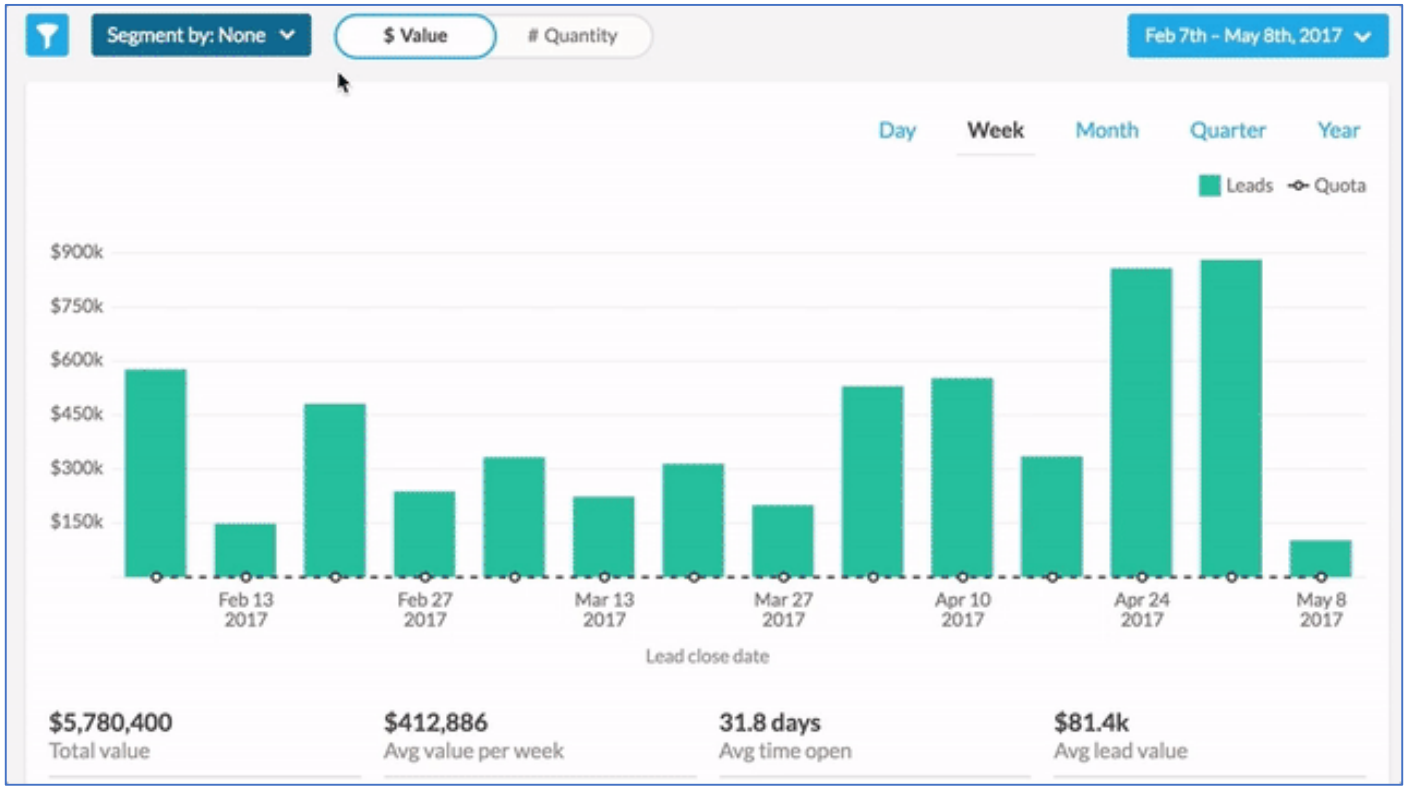


Definir el alcance de la evaluación

Recabar información, identificar y evaluar vulnerabilidades



Generar un informe de resultados



Generar un plan de remediación