OWASP

Open Web Application Security Project

Seguridad por Decepción

David F. Plazas G.

OWASP

Open Web Application Security Project

Agenda:

- Introducción
- Antecedentes
- Concepto
- Potencialidades
- Ejemplos
- Demostración

OWASP

Open Web Application Security Project

Introducción:

Desde hace unos años el uso de técnicas de seguridad por decepción se han utilizado amplia y eficazmente como una estrategia adicional de respuesta frente a amenazas.

OWASP
Open Web Application Security Project

Introducción:

La mayoría de los profesionales de la seguridad han manejado el concepto de Honeypots y de hecho estas soluciones utilizan la decepción como una estrategia clave para detectar y comprender detalles técnicos de nuevos ataques y exploits.

Honeynet Project

OWASP

Open Web Application Security Project

Introducción:

Sin embargo, considero que es posible utilizar la decepción más allá de la detección y utilizar la seguridad por decepción como una técnica de prevención y como un desvío de la sinergia de las amenazas y sus perpetradores.

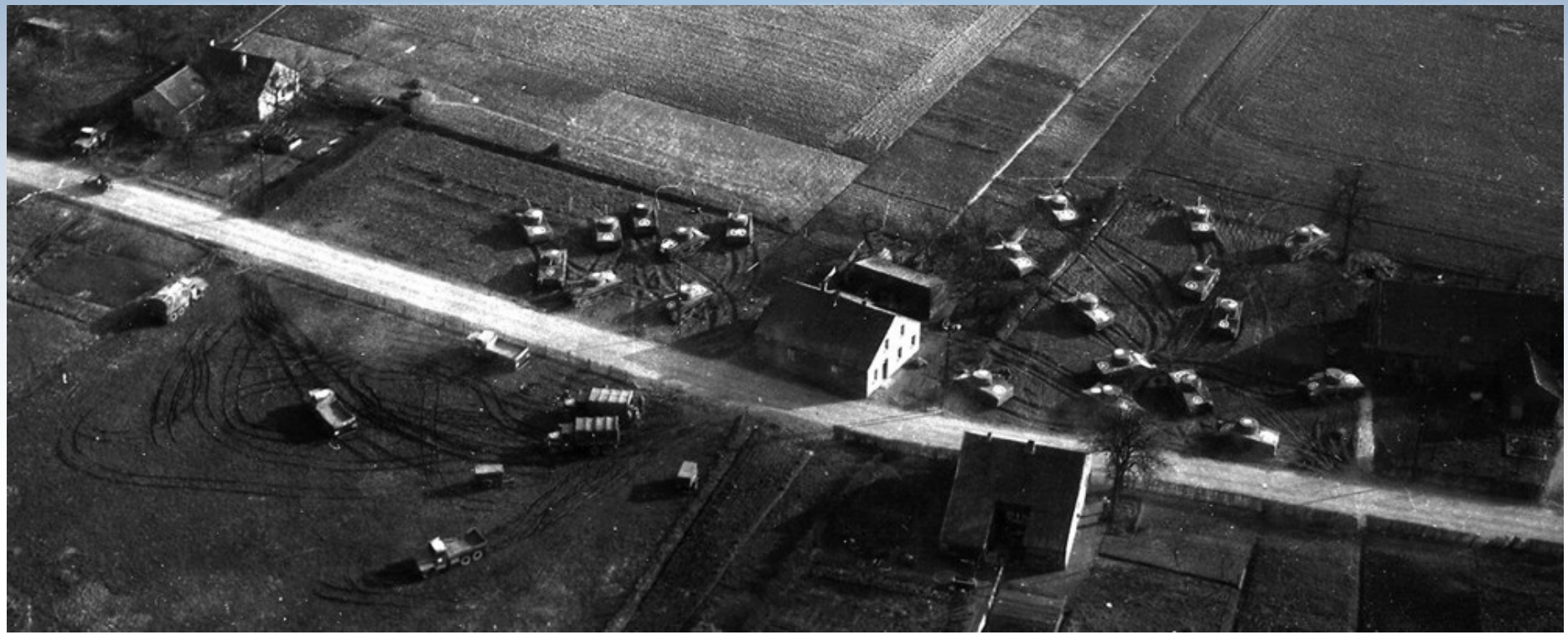
OWASP
Open Web Application Security Project

Introducción:

Smarter With Gartner

Why leverage deception?

By 2018, Gartner predicts that 10 percent of enterprises will use deception tools and tactics, and actively participate in deception operations against attackers.

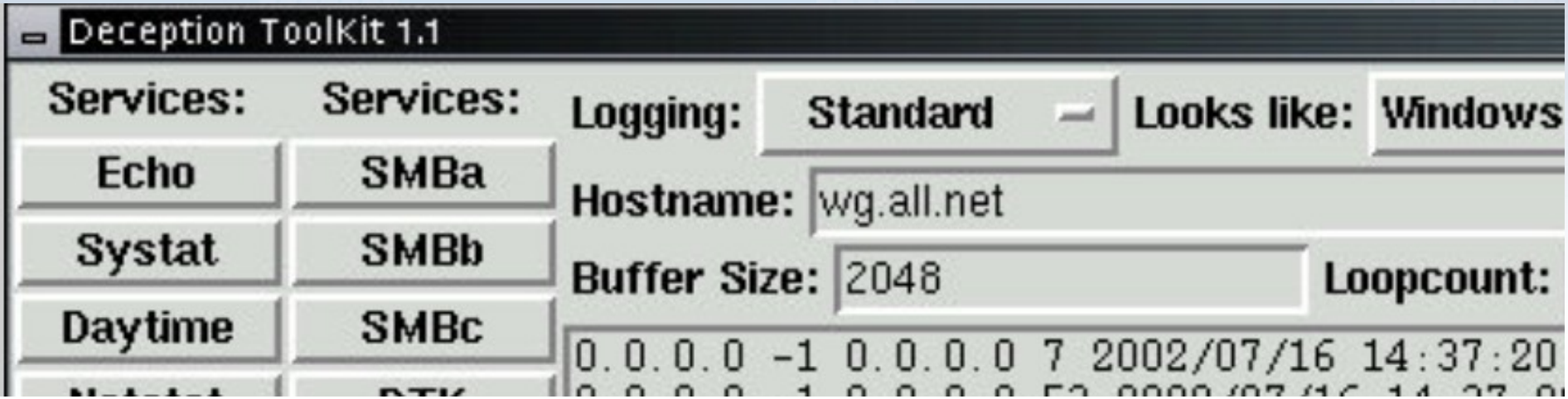


Antecedentes

OWASP
Open Web Application
Security Project

Antecedentes

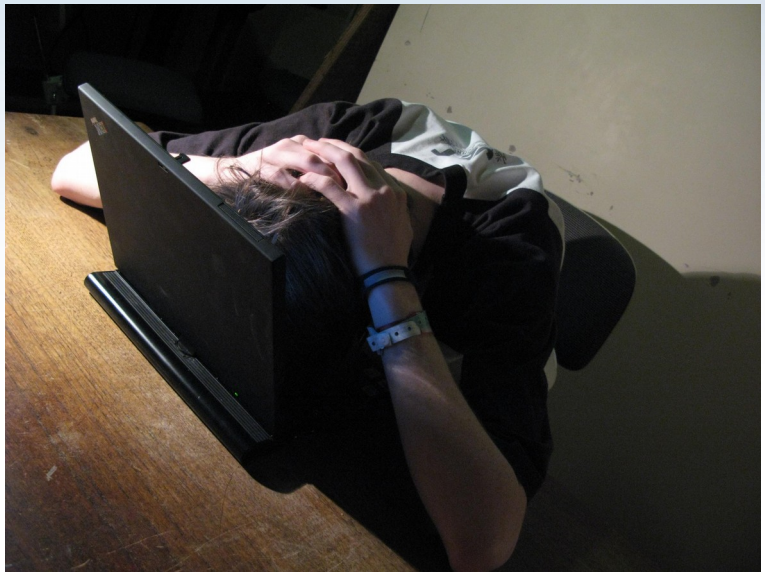
Antecedentes



OWASP
Open Web Application Security Project

Concepto

La Seguridad por Decepción consiste en cualquier medida defensiva a través del uso de engaños diseñados para frustrar,desviar o decepcionar al atacante.



OWASP
Open Web Application Security Project

Concepto

- Interrumpir las herramientas de automatización de un atacante.
- Retrasar las actividades de un atacante.
- Interrumpir el progreso del ataque.
- Afectar los procesos cognitivos del atacante.

OWASP

Open Web Application Security Project

Concepto

La decepción en este contexto se utiliza como una técnica para fines defensivos o disruptivos y no es de naturaleza ofensiva.

OWASP
Open Web Application Security Project

Ejemplos

WebLabyrinth crea un laberinto de páginas web falsas para confundir a los escáneres web.

OWASP

Open Web Application Security Project

Ejemplos

Port Spoof es una herramienta falsifica puertos haciéndolos parecer como abiertos y dignos de ser atacados, lo que confunde al atacante y le hace tomar más tiempo. Eventualmente se bloquea al atacante pero luego de cumplirse un umbral de tiempo definido.

OWASP
Open Web Application Security Project

Potencialidades

- Podemos incorporar la decepción en nuestros desarrollos y sistemas para degradar los ataques y posiblemente para afectar las capacidades del atacante.

OWASP
Open Web Application Security Project

Potencialidades

- La seguridad se basa realmente en la confianza por lo que es deseable que los atacantes tengan menos confianza en un sistema que sus usuarios legítimos.

OWASP

Open Web Application Security Project

Potencialidades

- Prefiero que un atacante deba invertir mas esfuerzo en tratar de comprometer mis sistemas que lo que yo deba invertir en mantenerlo fuera de ellos.

OWASP

Open Web Application Security Project

Demostración.

OWASP

Open Web Application Security Project

Preguntas o comentarios.

OWASP

Open Web Application Security Project

Muchas Gracias y feliz día.

•