Desarrollo de exploits

génesis

OWASP

The Open Web Application Security Project

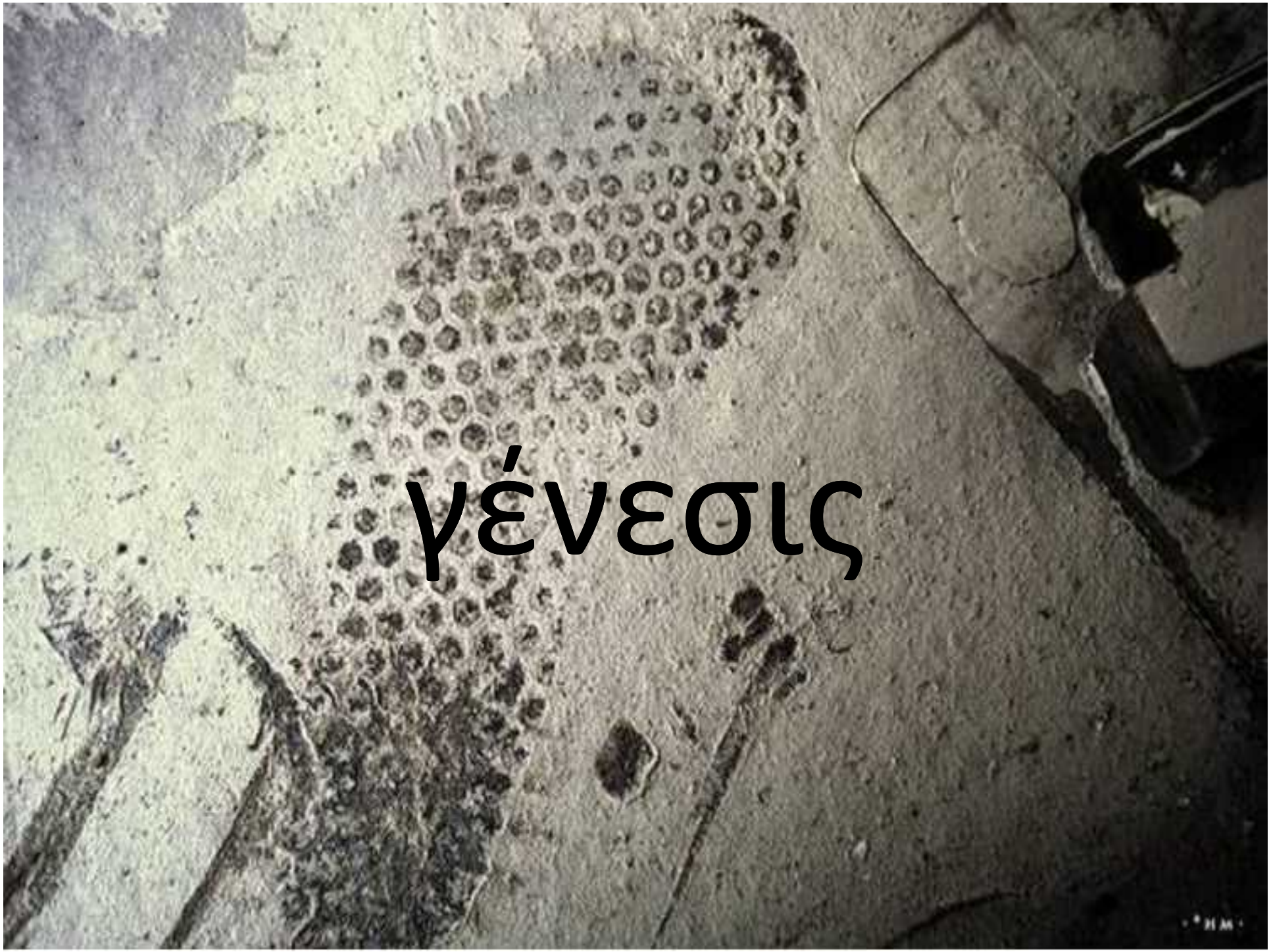
γένεσις

OWASP
The Open Web Application Security Project

Ing. Deyvi Bustamante Perez

1. Esposo
2. Padre de familia
3. Cristiano Evangelico

4. Profesor: UMRPSFX
5. Consultor: ISB


γένεσις

OWASP
The Open Web Application Security Project

Definiciones

- INGENIERÍA INVERSA
- ANÁLISIS DE VULNERABILIDADES
- EXPLOIT
- HACKING

OWASP
The Open Web Application Security Project

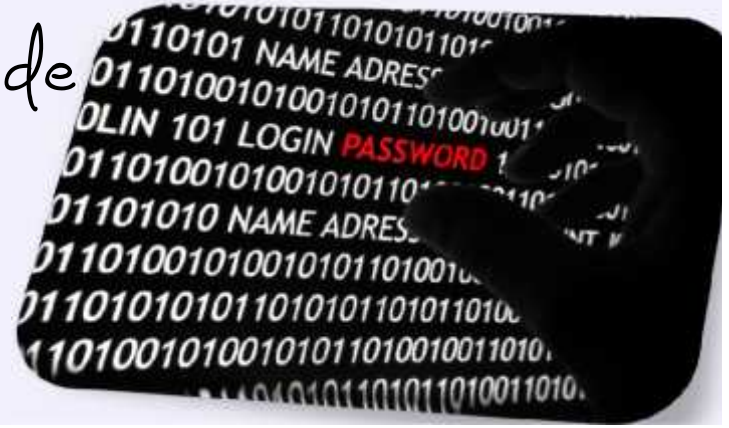
Ingeniería inversa

Una metodología sistemática para analizar el diseño de un dispositivo o sistema, ya sea como un enfoque para estudiar el diseño o como un requisito previo para re-diseño.

OWASP
The Open Web Application Security Project

Análisis de Vulnerabilidades

El análisis de vulnerabilidad, también conocida como evaluación de la vulnerabilidad, es un proceso que define, identifica y clasifica los agujeros de seguridad (vulnerabilidades) en una computadora, red o infraestructura de comunicación.



OWASP
The Open Web Application Security Project

Exploit

Exploit (del inglés to exploit, "explotar" o 'aprovechar') es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. Por ejemplo : Acceso de forma no autorizada, toma de control de un sistema de cómputo, escalar privilegios, denegación de servicio, aun la ingeniería social, se considera un exploit.

EXPLOIT

OWASP
The Open Web Application Security Project

INGENIERÍA INVERSA

El acto de averiguar el diseño e implementación del sistema.

ANÁLISIS DE VULNERABILIDAD

El acto de encontrar defectos y debilidades en cualquier parte de dicho sistema.

EXPLOIT

El acto de aprovechar la vulnerabilidad en un medio real de comprometer la confidencialidad, integridad y/o la disponibilidad de un sistema

HACKING

Utilizar el exploit.

OWASP

The Open Web Application Security Project

Exploit

Explotar

1. Corrupcion de memoria
2. Buffer Overflow
3. SHELL CODE
4. Nop sled

OWASP
The Open Web Application Security Project

Corrupcion de memoria?

es uno de la clase más intratable de errores de programación, por dos razones:

1. La fuente de la corrupción de la memoria
2. Su manifestación

motivos La fuente de la corrupción de la memoria y su manifestación puede estar muy separados, por lo que es difícil relacionar la causa y el efecto

OWASP
The Open Web Application Security Project

Corrupcion de memoria?

- **INYECCION DE CODIGO**
  - Donde nos infectamos del código maliciosos?
  - Como generamos el código maliciosos (Shellcode)?
  - Como debemos redirigir el flujo de ejecución?

OWASP
The Open Web Application Security Project

Corrupcion de memoria?

- **REDIRECION DE FLUJO DE EJECUCION**
  - En x86, una forma es para controlar un registro llamado **EIP**, también conocido como el registro de puntero de instrucción.
  - Este registro es cómo la arquitectura x86 sabe que la instrucción se ejecute siguiente.
  - **EIP**, sin embargo, no está directamente controlado por el usuario.
- **PERO COMO SE CONTROLA EL EIP?**
  - Como una vulnerabilidad

OWASP
The Open Web Application Security Project

Buffer Overflow ?

- Todo caso en que un programa escribe más allá de la el final de la memoria asignada para cualquier tampón.
  - Un ejemplo perfecto se puede mostrar con strcpy () desbordamiento de pila.
  - gets () y read () son otro ejemplo

OWASP
The Open Web Application Security Project

Exploit

SHELL CODE ?

INYECCION DE CONDIGO

Código de la máquina utilizada como carga útil en la explotación de un error de software. Si bien en un flujo de programas, código shell se convierte en su continuación natural.

OWASP
The Open Web Application Security Project

NOP?

- Fácil de saltar a la dirección equivocada, donde se encuentra el código shell.
- ¡La Dirección puede cambiar por sistema!
- **NOP** ("ninguna operación") ayuda con este problema
  - Puede saltar en cualquier parte **NOP** trineo y simplemente deslizarse en el malicioso código shell.
  - En este **X86** es **0X90**

OWASP

The Open Web Application Security Project

GRACIAS POR SU ATENCION