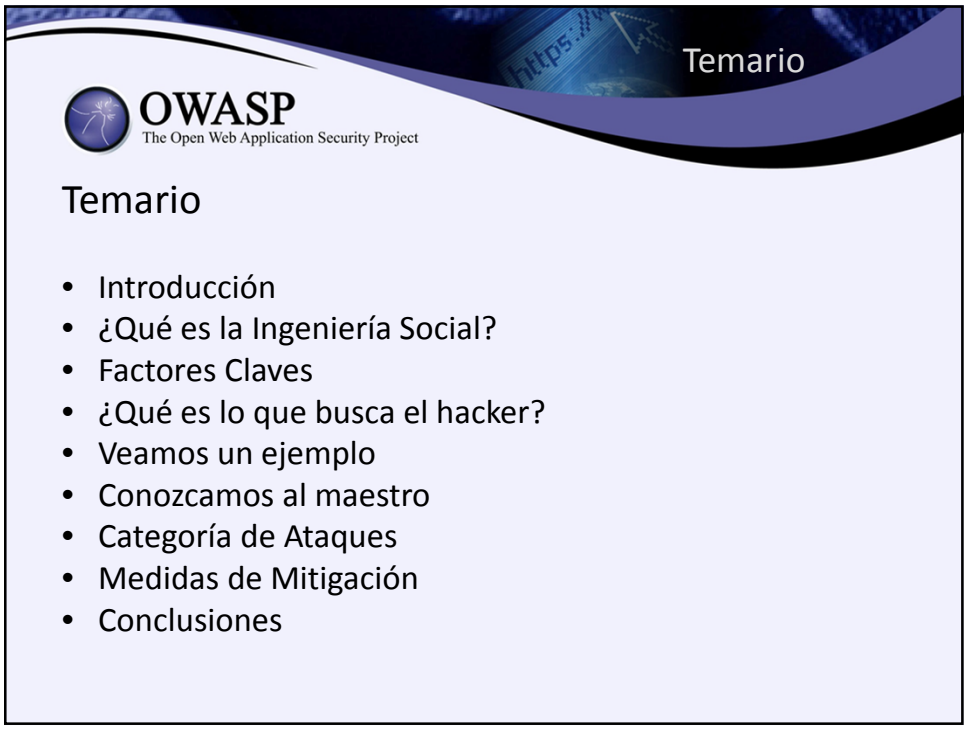

OWASP LatamTour
Rep.Dominicana 2016
INGENIERIA SOCIAL:
HACKING PSICOLÓGICO
OWASP
The Open Web Application Security Project
OWASP
LATAM
2016
LATIN AMERICA TOUR


Temario
OWASP
The Open Web Application Security Project
Temario
• Introducción
• ¿Qué es la Ingeniería Social?
• Factores Claves
• ¿Qué es lo que busca el hacker?
• Veamos un ejemplo
• Conozcamos al maestro
• Categoría de Ataques
• Medidas de Mitigación
• Conclusiones

OWASP
The Open Web Application Securi

Introducción

¿Cuál es el activo más importante para la organización?

A: Información

B: Instalaciones

C: Procesos

D: Hardware

Introducción

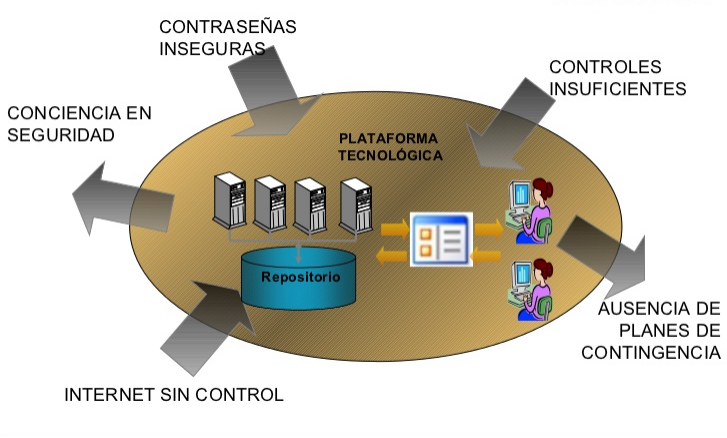
OWASP
The Open Web Application Security Project

Los riesgos presentes en nuestro ecosistema

Introducción

OWASP
The Open Web Application Security Project

Somos humanos, somos falibles… y se nota !



OWASP
The Open Web Application Security

¿Cuál es el eslabón más débil cuando hablamos de Seguridad de la Información?

A: Software

B: Internet

C: Usuario

D: Hardware

¿Qué es la Ingeniería **Social**?

OWASP
The Open Web Application Security Project

Conjunto de técnicas psicológicas y habilidades sociales (tales como: la influencia, la persuasión y la sugestión)

Busca directa o indirectamente que un usuario revele información sensible. Sin estar conscientes de los riesgos que esto implica.

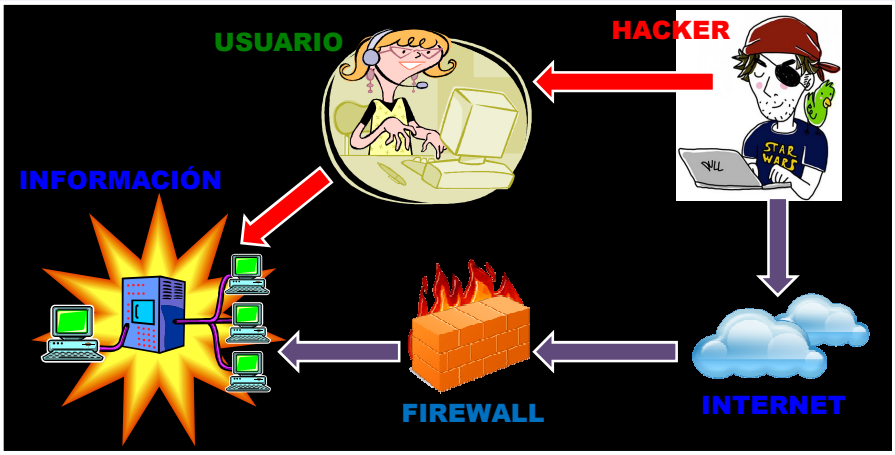
* Basada en Computadoras
  - Phishing

* Basada en Contacto Humano
  - Presencial
  - Telefónico
  - Etc…

¿Qué es la Ingeniería Social?

OWASP
The Open Web Application Security Project

Es bastante similar al hacking normal, con la única diferencia que no se interactúa con una máquina, sino con una persona.



¿Por qué Ingeniería Social?

OWASP
The Open Web Application Security Project

- Es Mas fácil que tratar de hackear un sistema con códigos y algoritmos
- No es necesario violar o burlar sistemas de detección de intrusos o firewalls
- Las herramientas para utilizar son gratis o de muy bajo costo
- Sin registro y con 100 % de efectividad aprox.
- Porque las personas son la vulnerabilidad mas grande en cualquier Empresa

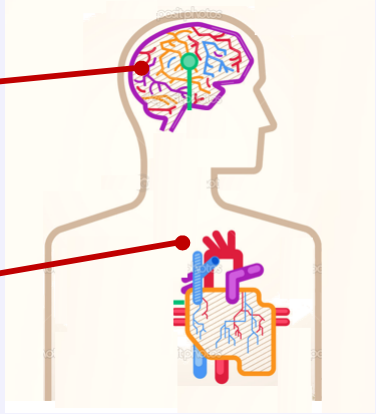
Factores Claves

OWASP
The Open Web Application Security Project

En Ingeniería Social existen 2 puntos claves.

PSICOLOGÍA

INTERACCIÓN SOCIAL



¿Que es lo que busca el hacker?

OWASP
The Open Web Application Security Project

Cual es el botín que persigue el hacker.

Información Confidencial

¿Y cuál es el impacto?

* Personal
* Financiero
* Imagen
* Legal

Veamos un ejemplo…

OWASP
The Open Web Application Security Project

Usuario: Hola?
Atacante: Si, buenos días, habla Pedro de acá de Sistemas.
Usuario: Pedro?...de Sistemas?
Atacante: Si! (*con voz segura*) tienes algún problema con tu usuario de red?. Acá en la pantalla me figuras con error.
Usuario: Que yo sepa no…
Atacante: Quizás sea un error nuestro, a ver, dígame su nombre de usuario.
Usuario: Si…ehhhh...es "msilva".
Atacante: Ummm…segura?...déjame buscarlo en el listado de usuarios…Ok, acá está. ¿ahora deme su actual contraseña para cambiarla por una nueva?.
Usuario: Si… es "marcela80".
Atacante: Ok, muchas gracias. Hasta luego.

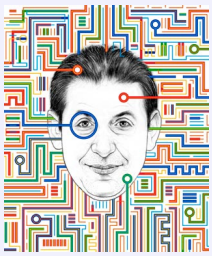
Conozcamos al maestro…

OWASP
The Open Web Application Security Project

Kevin Mitnick (El Cóndor) es uno de los hackers más famosos del mundo.

Su primera incursión en el *hacking* lo tiene a los 16 años cuando penetra el sistema administrativo de su colegio.

En 1981 accede al Sistema COSMOS (*Computer System for Mainframe Operation*)



En 1994 accede al computador personal de Tsutomu Shimomura (*Netcom On-Line Communications*)

En 1995 el FBI lo apresa y condenado a 5 años de cárcel.

Hoy es un millonario charlista internacional y best-seller.

Conozcamos al maestro…

OWASP
The Open Web Application Security Project

Según Mitnick, existen cuatro conceptos básicos:

* Todos queremos ayudar.

* El primer movimiento es siempre de confianza hacía el otro.

* No nos gusta decir "NO".

* A todos nos gustan que nos alaben.

Categoría de Ataques

OWASP
The Open Web Application Security Project

4 categorías de ataques por Ingeniería Social:

+ Ataques Técnicos

+ Ataques al Ego

+ Ataques de Simpatía

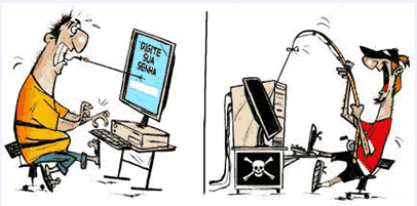
+ Ataques de Intimidación

Categoría de Ataques

OWASP
The Open Web Application Security Project

ATAQUES TÉCNICOS

- No existe contacto directo con las víctimas.
- El atacante utiliza emails, páginas web, boletines.
- El atacante simula ser una entidad reconocida y de confianza.
- Orientado a obtener información sensible de los usuarios.
- Altamente exitoso.



Ejemplo de Phishing

OWASP
The Open Web Application Security Project

Prueba de Concepto.

Demo práctica

Categoría de Ataques

OWASP
The Open Web Application Security Project

ATAQUES AL EGO

- El atacante apela a la vanidad y ego de la víctima.

- La víctima trata de probar su inteligencia y eficacia.

- Se busca que la víctima sienta que esta ayudando en un tema relevante (*y que posiblemente recibirá reconocimiento*).

- Usualmente la víctima nunca se da cuenta del ataque.

Dumpster Driving (Contenedor de Basura)

OWASP
The Open Web Application Security Project

También conocido como "***Trashing***" (***Buscar en la Basura***), es otro método de Ingeniería Social. Mucha información puede ser encontrada en la basura.

Ejemplos: Anotaciones, Manuales, Políticas, Memos, **CONTRASEÑAS**!

Shoulder Surfing (Espiar por encima del Hombro)

OWASP
The Open Web Application Security Project

Consiste en entablar una conversación y realizar ***notas mentales*** sobre las teclas que presiona el usuario al momento de ingresar sus datos de acceso a un sistema.

Categoría de Ataques

OWASP
The Open Web Application Security Project

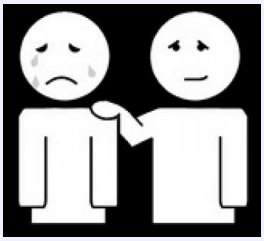
ATAQUES DE SIMPATÍA

- Se simula un escenario donde es urgente completar una tarea o actividad.

- Se apela a la empatía de la víctima.

- El atacante pide ayuda hasta que encuentra alguien que le pueda proporcionar lo que necesita.

- El atacante se muestra bastante desesperado, indicando que su trabajo está en juego si no completa su tarea.



Curiosidad (Hardware)

OWASP
The Open Web Application Security Project

El atacante deja un ***dispositivo de almacenamiento*** como pendrive, CD, memoria flash en un lugar donde pueda ser encontrado, mientras espera a que la víctima introduzca el dispositivo para infectarse con el código malicioso.

A través de la ***curiosidad*** humana es posible llevar a cabo este tipo de ataque.

Suplantación de ID

OWASP
The Open Web Application Security Project

Consiste en caracterizar a una persona, un rol. Generalmente los roles más empleados son ***soporte técnico*** y ***gerente***, etc.

En empresas grandes es difícil conocer a todos los empleados y falsificar las ID resulta Muy Simple!

Office Snooping (Espionaje en la Oficina)

OWASP
The Open Web Application Security Project

Muchos usuarios ***no dejan bloqueadas sus terminales*** cuando se levantan de sus escritorios o peor aún cuando se retiran del trabajo, por lo tanto es posible acceder a sus datos sin necesidad de identificarse.

Categoría de Ataques

OWASP
The Open Web Application Security Project

ATAQUES DE INTIMIDACIÓN

- El atacante simula ser alguien importante en la organización.

- Trata de utilizar su autoridad para forzar a la víctima a cooperar.

- Si existe resistencia utiliza la intimidación y amenazas (*pérdida de empleo, multas, cargos legales, etc.).*

Telefónico

OWASP
The Open Web Application Security Project

Un atacante llama por teléfono y trata de ***intimidar*** a alguien en la posición de autoridad o relevancia, de esa forma obtiene información.

Los Centros de Ayuda (***HelpDesk***) son generalmente vulnerables a este tipo de ataque.

Ingeniería Social Inversa

OWASP
The Open Web Application Security Project

Es el modo avanzado de la Ingeniería Social, conocido como "***Ingeniería Social Inversa***".

El atacante trata de parecer alguien de ***autoridad***, para que le pregunten a él y así obtener información.

Requiere mucha ***preparación***, ***investigación*** y saber relacionarse con las personas.

Medidas de Mitigación

OWASP
The Open Web Application Security Project

¿Cuál de las siguientes acciones NO es una medida de mitigación a la Ingeniería Social?

A: Capacitar

B: Documentar

C: Monitorear

D: Concientizar

Medidas de Mitigación

OWASP
The Open Web Application Security Project

Simples métodos para evitar un ataque:

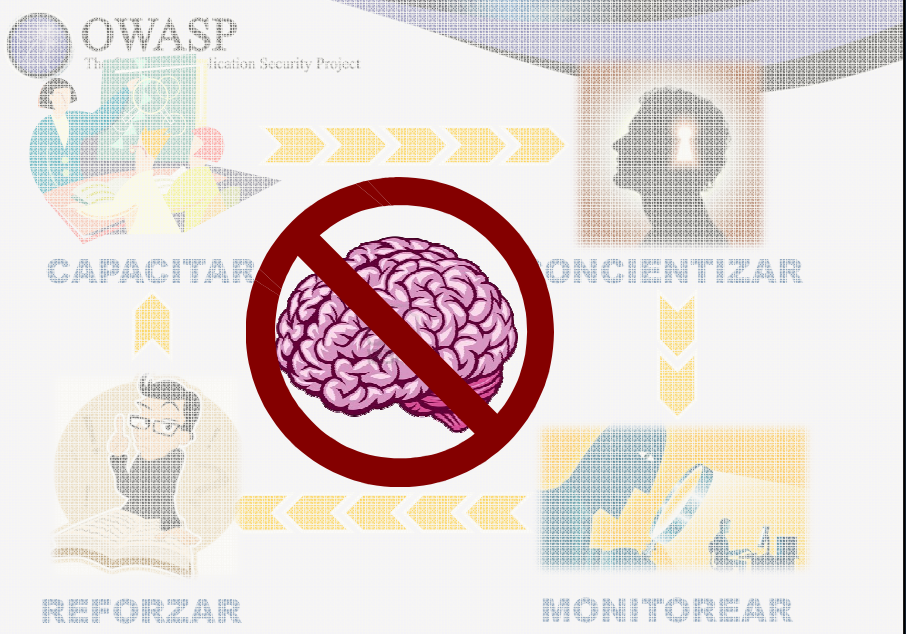
» "***No***" es lo primero, en algunas situaciones puede ser flexible, disuasivo y eficaz. Los "NO" son más fuertes cuando estamos seguros de tener razón.

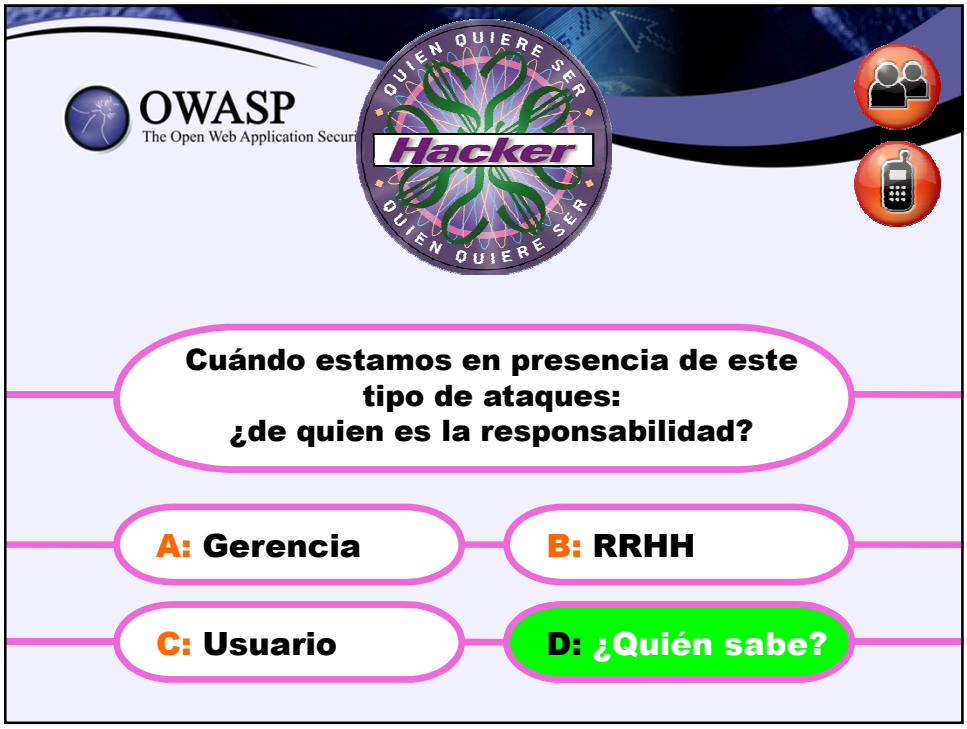
» ***Sí el conocimiento es un arma, la ignorancia es una armadura***. No dar mucha información o detalles sobre lo que nos preguntan.

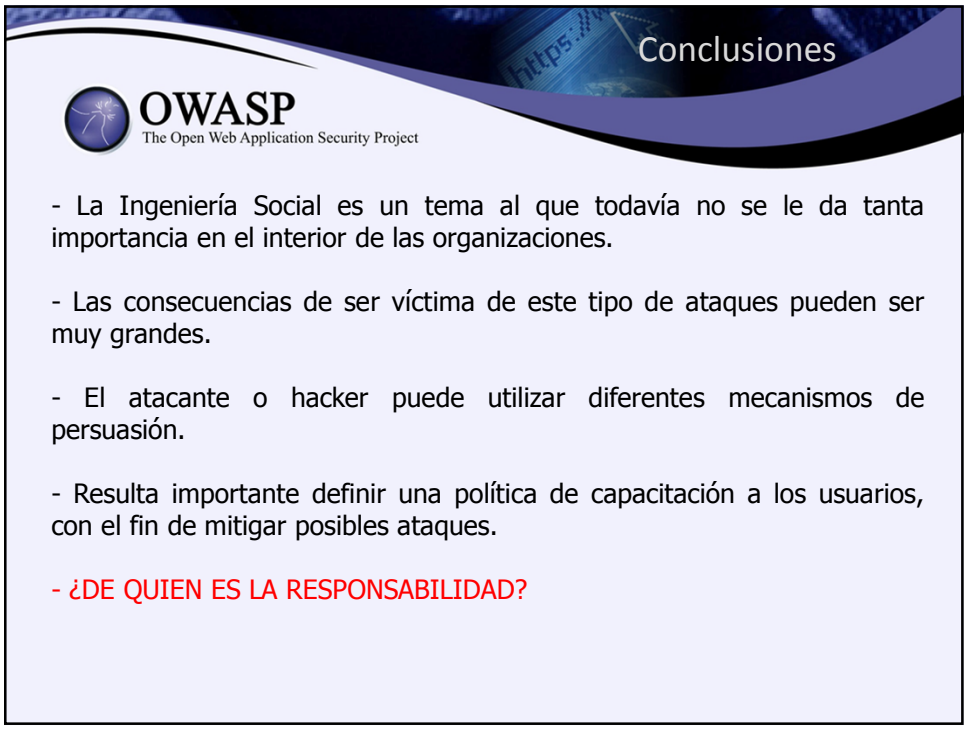
» Las ***políticas*** son buenas defensas contra la ingeniería social.

» ***Lo mejor manera de aumentar nuestras defensas es disminuir la posibilidad de evadirlas***. Utilizar seguridad física, biometría y restringir el acceso físico.

Medidas de Mitigación




OWASP
The Open Web Application Secur
QUIEN QUIERE SER
Hacker
QUIEN QUIERE SER
Cuándo estamos en presencia de este tipo de ataques: ¿de quien es la responsabilidad?
A: Gerencia
B: RRHH
C: Usuario
D: ¿Quién sabe?


Conclusiones
OWASP
The Open Web Application Security Project
- La Ingeniería Social es un tema al que todavía no se le da tanta importancia en el interior de las organizaciones.
- Las consecuencias de ser víctima de este tipo de ataques pueden ser muy grandes.
- El atacante o hacker puede utilizar diferentes mecanismos de persuasión.
- Resulta importante definir una política de capacitación a los usuarios, con el fin de mitigar posibles ataques.
- ¿DE QUIEN ES LA RESPONSABILIDAD?

Conclusiones

OWASP
The Open Web Application Security Project

"Aunque, el único computador seguro es el que está desenchufado…

Con ingeniería social, siempre se puede convencer a alguien para que lo enchufe".

Preguntas

OWASP
The Open Web Application Security Project