Ingeniería social,

técnicas y prevención

Índice

Introducción: ¿Qué es la Ingeniería Social?

La Ingeniería Social es un procedimiento que posibilita la manipulación de una persona, mediante técnicas psicológicas y ciertas habilidades sociales, de forma premeditada con el fin de obtener información acerca de dicho individuo.

Tipos de ataques

- **Remotos:** Requieren una conexión de red y explotan conocimientos informáticos

- **Locales:** Son aquellos que pueden ser llevados a cabo sin tener ningún conocimiento de informática.

Ataques remotos

- Phishing
- Pharming
- Redes sociales

Ataques locales

- Pretexting / Impersonate
- Tailgating
- Fallo en controles físicos de seguridad
- Dumpster Diving
- Shoulder Surfing
- Distracción
- Baiting

¿Cómo prevenir la Ingeniería Social?

- Proteger nuestros bienes más valiosos
- Aprender a identificar un ataque
- Filtro de mayor seguridad en correo electrónico
- Actualizaciones de sistema y aplicaciones
- Separar el ámbito profesional del personal
- Buena administración de acceso
- Escepticismo
- Auditorías internas

Ataques más importantes de Ingeniería Social

- Ataque a ABM AMRO (Bélgica)
- Ataque a Ubiquiti Networks, Inc
- Phishing en mensajería y paquetería
- Escapada de un preso
- Brecha en SecurID de RSA
- Hidden Lynx Watering Hole on Bit9
- Hackeo de la cuenta de twitter de Associated Press

SET (Social engineer toolkit)

Herramienta dedicada a la realización de todo tipo de ataques de Ingeniería Social.

- Spear-Phishing
- Attack web vector
- Infectious Media Generator
- Payload and Listener
- SMS Spoofing

Experimento

Suplantación de identidad de Facebook utilizando SET y Ettercap para obtener contraseñas de usuario.

https://www.youtube.com/watch?v=U8zCA1LY6Mk&t=39s