El Arte del Engaño

Revelando la Fascinante
Danza entre la Seguridad
Fisica y la Ingenieria Social

Por David Probinsky para
OWASP Lima 08/22/2023

#whoami

- Líder del Red Team | Seguridad Ofensiva @ Elevate Consult
- Red Teaming | Seguridad física | Ingeniero Social | Hacker ético
- Profesional de InfoSec con más de 7 años de experiencia en TI y Seguridad Ofensiva.
- AS en Seguridad Informática y de Redes
- Network+, Security+, PenTest+, eJPT y algunos otros
- Presentado en HackMiami, RedTeamRD, EkoParty, Texas Cyber Summit, BSides Orlando, y aparición en documental de Telemundo.

TABLA DE CONTENIDO

Fundamentos de la Ingeniería Social

Que es la ingeniería social?

En Red Teaming: Es la manipulación psicológica para obtener información o acceso no autorizado.

Tipos de ataques:

Phishing, pretexting, tailgating, quid pro quo, etc.

Selección de Víctimas y Objetivos:

Recopilan información sobre posibles objetivos, como empleados, directivos o contratistas.

El Ingeniero Social

Adaptación

Ajustar estrategias según el objetivo y el entorno.

Manipulación

Cómo los ingenieros sociales utilizan principios psicológicos para influenciar decisiones. Reciprocidad, la autoridad y la consistencia.

Empatía

Cómo los ingenieros sociales aprovechan las emociones para influir en las decisiones.

Relación de Confianza

Identificar objetivos más propensos a interactuar y compartir información.

Flexibilidad

Reconocimiento de cambios en la dinámica: estar preparado para ajustar enfoques.

Ética y Límites

Uso responsable de las habilidades de ingeniería social. Consideración de los posibles daños emocionales y profesionales.

Fases de un Ataque de Ingeniería Social

Reconocimiento y Selección de Objetivos:

- Uso de fuentes abiertas y redes sociales para recopilar información. Google Maps, Bienes Raíces, Redes Sociales.
- Identificación de objetivos vulnerables.

Preparación y Creación de Escenarios:

- Desarrollo de pretextos creíbles y personalizados.
- Diseño de mensajes y llamadas persuasivas.

Contacto Inicial y Establecimiento de Confianza:

- Selección de canales de comunicación: correo electrónico, redes sociales, etc.
- Creación de conexiones genuinas con la víctima. Ej: Entrevistas de Trabajo.

Manipulación y Extracción de Información:

- Uso de tácticas de persuasión y manipulación psicológica.
- Obtención de información confidencial.

Explotación y Mantenimiento de Acceso:

- Utilización de información recopilada para otros ataques.
- Mantenimiento del acceso a sistemas y datos.

Jose Manuel

Edad: 35

Empleo: Ingeniero Contratista

Empresa: ISP o Entidad local

HOBBIES: Fotografia o Deportes

Amistades en comun: 13+

PRETEXTOS

	Descripción	PRETEXTO
Mantenimiento de IT	El ingeniero social se presenta como un técnico de mantenimiento de TI o un empleado de soporte técnico. Aprovecha la confianza que las personas suelen tener en el personal de TI para acceder a áreas restringidas.	Puede afirmar que está allí para solucionar un problema con la red, realizar actualizaciones de software o verificar problemas de seguridad en los sistemas.
Inspección de Seguridad	El ingeniero social se hace pasar por un inspector de seguridad de la organización o de una agencia reguladora. Aprovecha la disposición de las personas a cumplir con regulaciones y normas de seguridad.	Afirma que debe realizar una inspección de seguridad de rutina, verificar el cumplimiento de normativas o evaluar posibles riesgos en las instalaciones.
Entrega de Paquetes	El ingeniero social se disfraza como un mensajero de paquetes o mensajería. Aprovecha la naturaleza cotidiana de este tipo de interacciones para ganar acceso.	Afirma que está allí para entregar un paquete importante o un mensaje urgente a un empleado específico. Puede mencionar que requiere la firma de alguien autorizado.

SCENARIOS

GENDER

AGE

CLIENTS

HEALTH

LAW

TECHNOLOGY

INSURANCE

RETAIL

ENERGY

Background de un Ingeniero Social

30%

Observación y Análisis del Comportamiento Humano

40%

Habilidades de Comunicación y Persuasión

30%

Capacidad de Improvisación y Adaptación

- Clip Board
  - Lockpicks e Implantes
- Cascos
- High Visibility Vest
- Uniformes con logos
- IDs de Badge falsos
- Imprentas magneticas para vehiculos
- Formularios falsos
- Tarjetas Profesionales falsas
- Radios o Celulares
- Pretexto y pretexto del pretexto

Atuendos

El Tecnico

El Enfermero

El Auditor

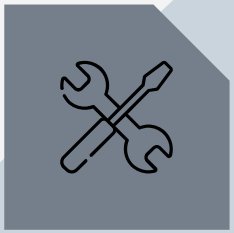
RED TEAMING

Ingeniería Social

Seguridad Fisica

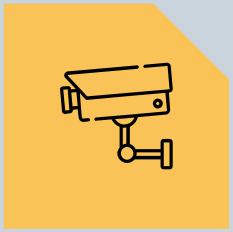
Ethical Hacking

Seguridad Física



Importancia de evaluar la seguridad física en pruebas ofensivas.

Enfoque en puntos de entrada y vulnerabilidades físicas.



Exploración de la **entrada táctica encubierta:** cómo los red teamers aprovechan situaciones para ingresar sin detección.

Herramientas y Tácticas de Seguridad Física

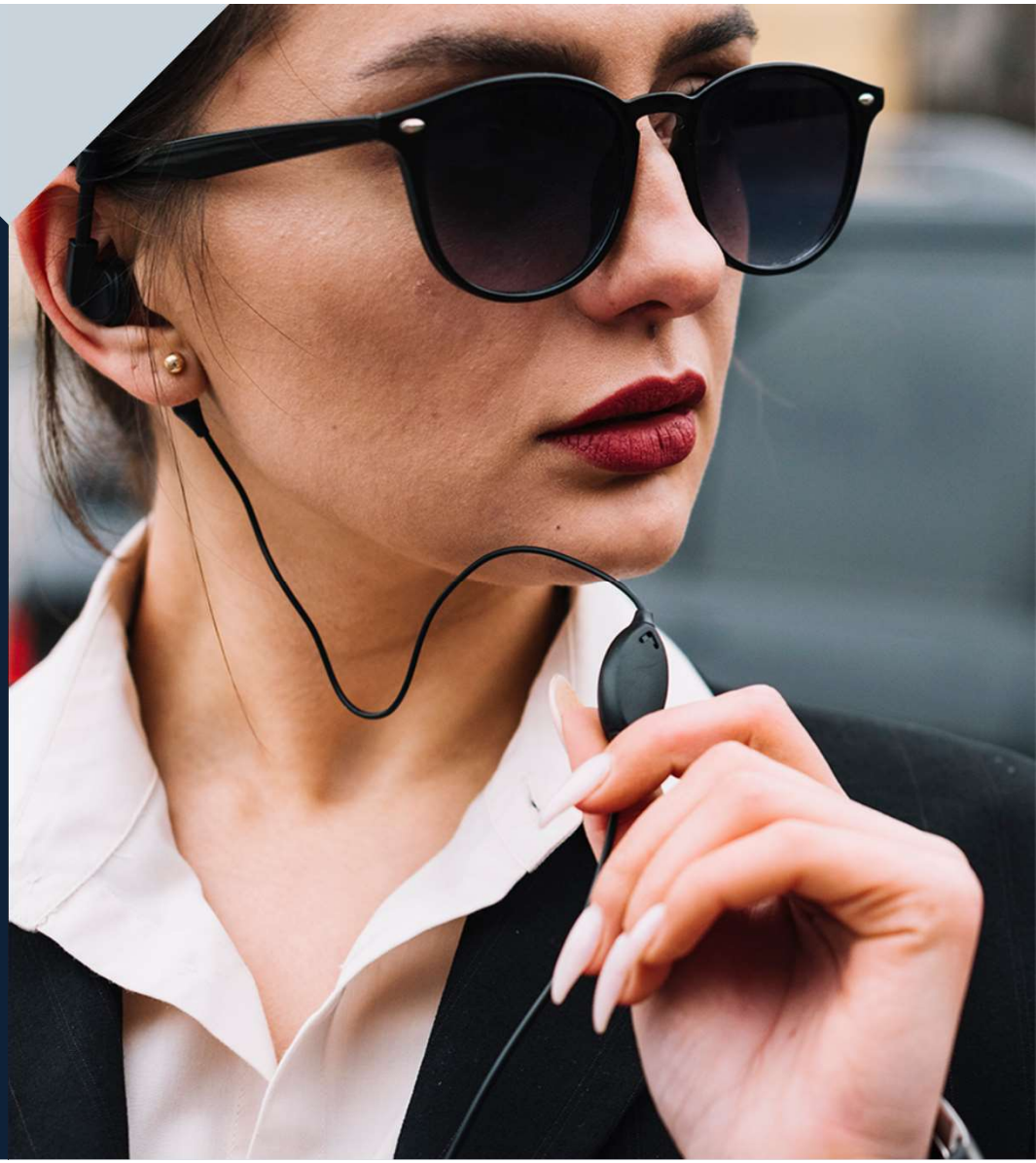
Lockpicking: Técnicas para abrir cerraduras.

Clonación de RFID: Lograr tener acceso no autorizado a instalaciones.

Implantes: WiFi, USB, RFID, etc


SPARROWS
https://github.com/DavidProbinsky/RedTeam-Physical-Tools

- Planificación y Preparación
- Reconocimiento y Vigilancia
- Creación de Perfiles y Disfraz
- Obtención de Herramientas y Equipamiento
- Ejecución de la Infiltración
- Mantenimiento del Acceso
- Exploración y Movimiento Interno
- Recopilación de Información
- Documentación y Reporte
- Exfiltración y Limpieza
- Análisis y Mejora



ATAQUES

01

Stuxnet.

02

Pwnd.

PhySec + Ing. Social

Mitigación y Defensa

Concienciación y entrenamiento del personal: identificar señales de ingeniería social.

Mejora de medidas de seguridad física: cámaras, alarmas, controles de acceso.

Implementación de políticas de seguridad robustas: verificación de identidad, procesos de autorización.

GRACIAS!

Preguntas?

dprobinsky@elevateconsult.com
https://www.linkedin.com/in/davidprobinsky/
https://github.com/DavidProbinsky/
https://www.youtube.com/@DavidProbinsky
Discord: `0xOverflow`