M-CIB-003
Metodología de Pruebas de Ingeniería Social
Responsables

Elaboró:	Especialista Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Gerente de normatividad y cumplimiento

Control de versiones

Versión	Fecha	Descripción del cambio
1	29/09/2022	Emisión Inicial

Clave del formato de manual: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción

Silent4Business ha desarrollado una metodología propia tomando las mejores prácticas de metodologías mundialmente reconocidas como 560 del SANS Institute, a OSCP de Offensive Security, PTES y NIST 800-115, en conjunto con la experiencia de los consultores del equipo para realizar las pruebas de ingeniería social, la cual se describe a continuación.

A continuación, se muestra la metodología empleada para la realización de las pruebas de ingeniería social, y que contempla la ejecución de técnicas manuales, técnicas automatizadas y actividades de verificación que nos permiten descubrir las debilidades humanas y tecnológicas antes de que se materialicen.

2. Alcance

Este proceso es de uso del área de ciberinteligencia, es aplicable para servicios ejecutados a clientes externos y/o para Silent4Business.

3. Definiciones

Activo

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza

Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Comprometer

Evasión de controles de seguridad causando posible de pérdida o daño en un activo de cómputo.

Exploit

Código o técnica que es usada por una amenaza para tomar ventaja de una vulnerabilidad.

Impacto

Medición de la consecuencia al materializarse una amenaza.

Mitigación

Acciones para remediar vulnerabilidades identificadas en los activos.

Probabilidad

Es la posibilidad que existe entre una amenaza y las variables de entorno para que una vulnerabilidad sea aprovechada.

Riesgo

Es la probabilidad de que una amenaza explote una vulnerabilidad con su correspondiente impacto al negocio.

Vulnerabilidad

Son debilidades que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

4. Descripción de la Metodología

A. Técnicas de ataque por fase de la metodología

Por cada fase de la metodología, el equipo de Silent 4 Business está capacitado para realizar las distintas técnicas para llevar a cabo las actividades de ingeniería social. A continuación, se detallan algunas técnicas de ataque:

I. Definición de Alcance

- Se recopila la información de alcance y objetivo del cliente. Esta información incluye los objetivos (nombres, correos electrónicos, números de teléfono, departamentos, ubicaciones físicas) y objetivos de compromiso para ayudarnos a enfocar nuestros ataques.

- También es posible realizar un compromiso de ingeniería social de conocimiento cero, en el que el equipo de prueba descubre los objetivos por su cuenta utilizando inteligencia de código abierto que pueden recopilar.

II. Reconocimiento

- Esta fase implica la recopilación de inteligencia de fuentes abiertas (OSINT), lo cual incluye una revisión de la información y los recursos disponibles públicamente. El objetivo de esta fase es identificar cualquier información que pueda ayudar durante las siguientes fases de prueba, que podría incluir direcciones de correo electrónico, nombres de usuario, números de teléfono, información sobre la empresa que puede usarse para hacernos parecer infiltrados, títulos de trabajo, organización gráficos, terceros con los que trabaja, tecnología específica en uso, etc.

- Además, este paso incluirá la búsqueda de información confidencial que no debería estar disponible públicamente, como comunicaciones internas, información salarial u otra información potencialmente dañina.

III. Modelado de Amenazas

- La fase de modelado de amenazas permite evaluar los tipos de amenazas más probable a los que sean susceptibles los objetivos de acuerdo con la información que se pueda identificar durante la etapa de reconocimiento.

- El ataque está diseñado para emular los métodos del mundo real que utilizan los atacantes, en función de filtraciones de datos recientes e inteligencia de amenazas.

- Durante la etapa de modelado de amenazas, el equipo de consultores desarrollará la campaña para que se puedan implementar rápidamente durante la fase de ataque, lo que reduce la posibilidad de detección.

IV. Análisis de vulnerabilidades

- La fase de análisis de vulnerabilidades implica la entrega de la campaña para evaluar si el objetivo se puede persuadir para caer en la trampa. Por ejemplo, para los ataques de phishing basados en correo electrónico,

se pueden emplear imágenes ocultas y tecnología de seguimiento para determinar cuántos objetivos abrieron el correo electrónico, hicieron clic en el enlace, ingresaron su contraseña, etc. Esto permite rastrear si un objetivo cayó en la trampa, estos datos se utilizarán para proporcionar estadísticas en nuestro informe final.

V. Explotación

- La parte de explotación se incorpora en cada campaña y se desarrolla durante la etapa de modelado de amenazas de la prueba.

- Según el objetivo y alcance de la campaña, la explotación puede ser un recolector de credenciales en un portal de inicio de sesión falso que captura las contraseñas de los empleados cuando inician sesión, una puerta trasera que llega a un servidor controlado o simplemente información que el consultor puede capturar del empleado.

- Según la información de seguimiento recibida durante la fase de análisis de vulnerabilidades de la prueba, es posible que las campañas deban modificarse para que sean más efectivas. Por ejemplo, es posible que la puerta trasera deba ofuscarse aún más para eludir un antivirus en particular.

VI. Post-Explotación

- Después de la fase de explotación, el objetivo principal del consultor es cuantificar el riesgo que presenta un compromiso exitoso para la organización. Ahora que un objetivo divulgó información o hizo clic en un enlace, se buscará verificar el alcance que puede tener un atacante.

- En caso de que el empleado ingrese su contraseña en un portal falso, se puede intentar su reutilización para iniciar sesión en la VPN, su correo electrónico o cualquier otro sitio en particular.

- Para las puertas traseras ejecutadas, se podrán tomar capturas de pantalla del escritorio, intentar ubicar y filtrar información sensible o intentar hacer movimientos laterales a través de la red

5. Anexos

NA