Informe de avance

Analitiks®

Santiago de Chile

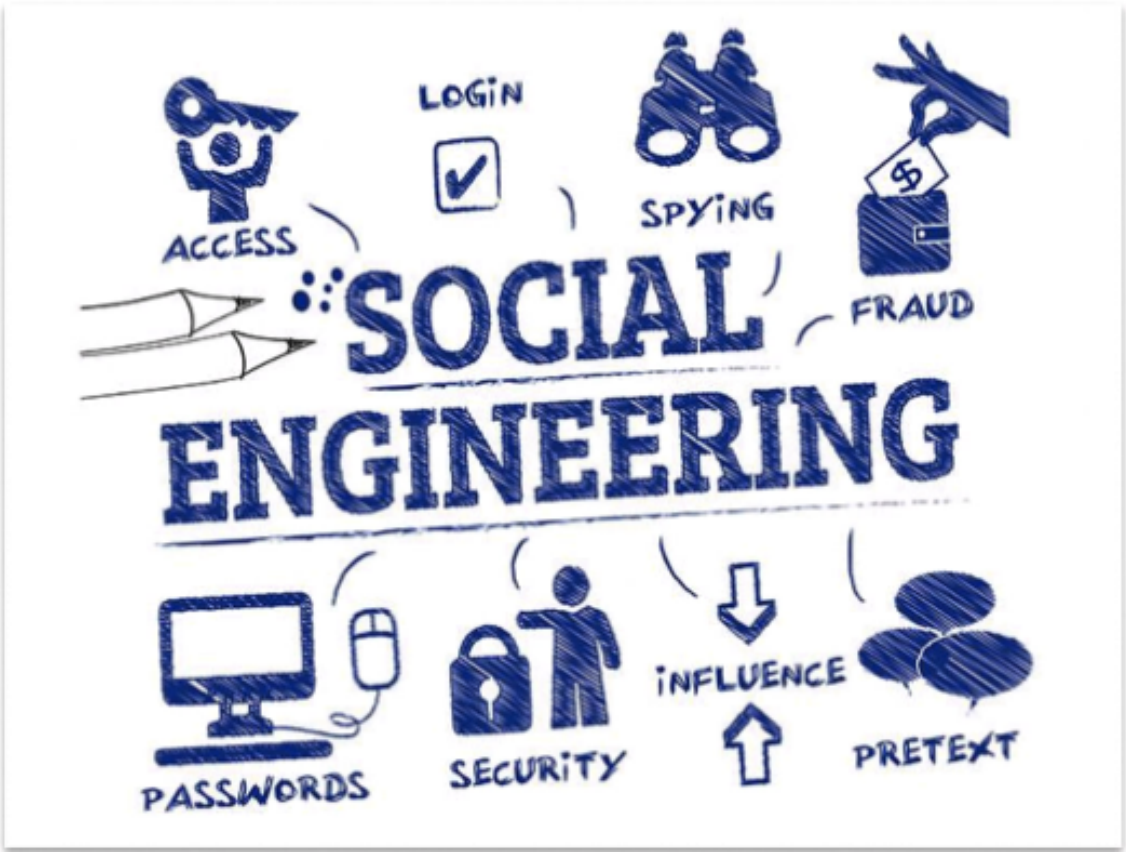
Viernes, 30 de septiembre de 2022

Índice

1. Ingeniería Social

1.1. ¿Qué es la Ingeniería Social?

La ingeniería social es una técnica de manipulación psicológica que se utiliza para engañar a las personas y obtener información confidencial. Es una de las herramientas más utilizadas en el mundo de la ciberseguridad, ya que no se necesita ser un experto en tecnología para entender cómo funciona. Imaginate que alguien te llama por teléfono haciéndose pasar por un representante de tu banco. Te hablan de un problema con tu cuenta y, con tono amigable, te piden que confirmes tus datos personales o inclusive tu contraseña. Aunque parezca totalmente creible, pueden ganarse tu confianza con palabras, manipulando tus emociones con el fin de obtener información personal y confidencial.
De eso se trata la ingeniería social, el arte de manipular a las personas para que entreguen información privada sin darse cuenta. El entender la ingeniería social no solo nos ayuda a protegernos de estos engaños, sino también a reconocer cómo los ciberdelincuentes aprovechan nuestra psicología para violar nuestra seguridad.



2. Tipos de Ingeniería Social

2.1. Social Engineer Toolkit (SET)

El Social Engineer Toolkit (SET) es un conjunto útil de herramientas que, además de ser de código abierto, es una de las más populares en el mundo de la ciberseguridad. Es ampliamente utilizado por testers de penetración y equipos de seguridad (los famosos Red Teams) para evaluar la seguridad de una organización imitando ataques de ingeniería social dirigiros al personal.
SET ofrece una amplia gama de métodos para realizar ataques, como puede ser la clonación de sitios web, cargas maliciosas, spear phishing o la creación de medios infectados. Lo anteriormente mencionado son ataques dificiles de defender, ya que se aprovechan de las debilidades humanas ya que son inevitables dentro de una organización.

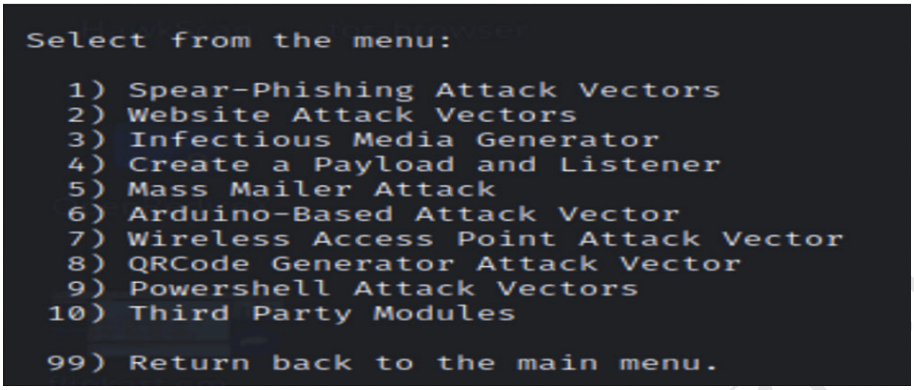
2.1.1. Instalación de SET

Para instalar SET, primero debemos clonar el repositorio de GitHub. Para ello, abrimos una terminal y ejecutamos el siguiente comando:

```
git clone https://github.com/trustedsec/social-engineer-toolkit
```

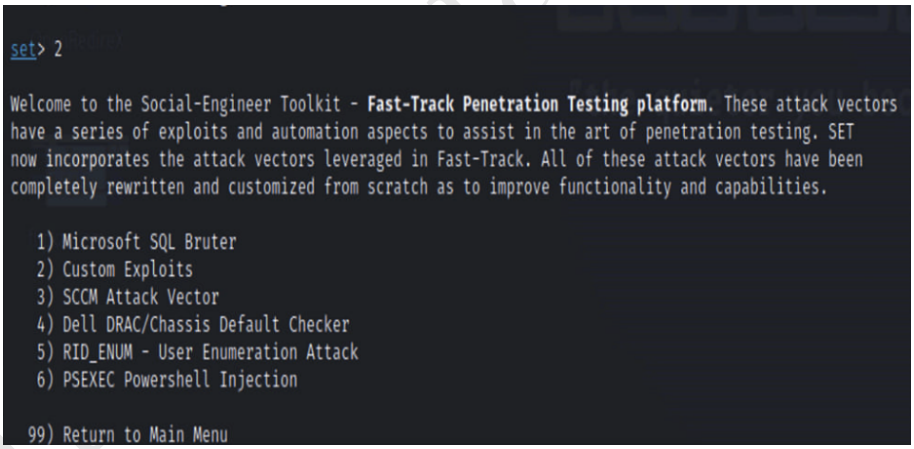
Cuando ya estemos dentro del SET, encontraremos diferentes opciones en el menu.

2.2. Social-Engineer Attacks



La primera opción que encontramos en el SET se centra en diferentes vectores de ataque utilizados en la ingeniería social, como puede ser el phishing, la clonación de sitios web, entre otros. Los usuarios pueden usarla para probar y simular varios escenarios de ataque basados en el comportamiento humano.

2.3. Penetration Testing (Fast-Track)



La segunda opción que encontramos en el SET es el Fast-Track, que es una herramienta que automatiza el proceso de pruebas de penetración, permitiendo identificar rápidamente las vulnerabilidades y aprovechar fallos de seguridad. Es una herramienta muy útil para los equipos de seguridad que buscan identificar y corregir vulnerabilidades en sus sistemas.

2.4. Third Party Modules

La tercera opción que encontramos en el SET es la de los módulos de terceros, que son herramientas adicionales que se pueden instalar para ampliar las capacidades del SET. Estos módulos ofrecen cargas utiles adicionales, exploits y rutas de ataque para el toolkit.

2.5. Update the Social-Engineer Toolkit

La cuarta opción que encontramos en el SET es la de actualizar el toolkit. Es importante mantener el SET actualizado para asegurarse de que se tengan las últimas actualizaciones y parches de seguridad para garantizar su funcionalidad y confiabilidad.

2.6. Update SET configuration

Con esta opción puedes editar el archivo de configuración de SET para personalizar la configuración del toolkit y adaptarla a tus necesidades y preferencias.

2.7. Help, Credits, and About

La última opción que encontramos en el SET es la de ayuda, créditos y acerca de. Esta opción proporciona información sobre cómo utilizar el toolkit, los créditos de los desarrolladores y una descripción general del toolkit.

3. Conclusión

Existen muchas más opciones disponibles además de las mencionadas. Podemos utilizar las herramientas diversas y potentes del invaluable Social Engineer Toolkit (SET) para realizar phishing, recolectar credenciales, clonar sitios web, entre otros.
Es siempre importante usar estas herramientas de manera consciente y solo con fines de investigación en seguridad y aprendizaje.

4. Referencias