La ingeniería social es una técnica de manipulación psicológica utilizada para engañar a las personas y lograr que revelen información confidencial o realicen acciones que comprometan la seguridad de un sistema o una organización. A continuación, te proporcionaré una descripción más detallada sobre la ingeniería social, sus tipos y técnicas, así como estrategias para prevenirla.

**Tipos de Ingeniería Social**

1. **Phishing**: El atacante envía correos electrónicos o mensajes falsos que parecen legítimos, generalmente pretendiendo ser una entidad confiable, para engañar a las víctimas y que revelen información sensible, como contraseñas o datos bancarios.
2. **Spear Phishing**: Similar al phishing, pero dirigido a una persona específica o a una pequeña audiencia. Estos ataques suelen estar más personalizados y son más difíciles de detectar.
3. **Vishing**: Uso de llamadas telefónicas para obtener información sensible. Los atacantes pueden hacerse pasar por personal de soporte técnico, bancos u otras entidades confiables.
4. **Smishing**: Envío de mensajes de texto falsos para engañar a las víctimas y que revelen información sensible o hagan clic en enlaces maliciosos.
5. **Pretexting**: El atacante crea un escenario falso (pretexto) para obtener información. Por ejemplo, fingir ser un investigador o un empleado de una empresa para obtener datos sensibles.
6. **Baiting**: El atacante deja un dispositivo infectado, como una unidad USB, en un lugar público, esperando que alguien lo encuentre y lo conecte a su computadora, lo que permite al atacante acceder al sistema.
7. **Tailgating**: El atacante sigue a alguien que tiene acceso autorizado a un área restringida para ingresar sin tener que pasar por los controles de seguridad.
8. **Quid Pro Quo**: El atacante ofrece un beneficio o servicio a cambio de información sensible. Por ejemplo, ofrecer soporte técnico a cambio de credenciales de inicio de sesión.

**Técnicas Comunes de Ingeniería Social**

* **Impersonación**: Hacerse pasar por alguien con autoridad o una entidad de confianza.
* **Urgencia**: Crear un sentido de urgencia para que la víctima actúe rápidamente sin pensar.
* **Reciprocidad**: Ofrecer algo a la víctima para generar un sentimiento de obligación.
* **Aprobación social**: Usar la influencia de terceros confiables o conocidas.
* **Autoridad**: Pretender ser una figura de autoridad para obtener información.
* **Escasez**: Crear una percepción de escasez o una oportunidad limitada.

**Prevención de Ingeniería Social**

1. **Concienciación y Educación**: Capacitar a los empleados y usuarios sobre los riesgos de la ingeniería social y cómo reconocer los intentos de ataque.
2. **Verificación de Identidad**: Implementar procedimientos para verificar la identidad de las personas antes de proporcionar información sensible.
3. **Políticas de Seguridad**: Establecer y hacer cumplir políticas de seguridad rigurosas para manejar la información confidencial.
4. **Tecnología de Seguridad**: Utilizar tecnologías de seguridad, como filtros de spam, autenticación de dos factores y software de detección de fraudes.
5. **Pruebas de Seguridad**: Realizar simulaciones y pruebas de penetración para evaluar la vulnerabilidad a los ataques de ingeniería social.
6. **Control de Acceso**: Implementar controles de acceso físico y lógico para proteger la información y los sistemas críticos.

**Ejemplos de Ingeniería Social**

1. **Phishing**:
   * Un correo electrónico que parece ser de un banco, solicitando que el usuario haga clic en un enlace para verificar su cuenta.
2. **Pretexting**:
   * Un atacante llama a un empleado fingiendo ser del departamento de TI y pide las credenciales de acceso para solucionar un problema técnico.
3. **Baiting**:
   * Un dispositivo USB etiquetado como "bonificación anual" dejado en la sala de descanso de una empresa, esperando que un empleado curioso lo conecte a su computadora.

La ingeniería social es una amenaza significativa en el ámbito de la seguridad de la información. La mejor defensa es una combinación de educación, políticas de seguridad rigurosas y tecnologías de protección adecuadas.

SET (Social-Engineer Toolkit) es una herramienta muy conocida y ampliamente utilizada para realizar pruebas de penetración y simulaciones de ingeniería social. Aquí te menciono algunas herramientas similares o complementarias que podrías considerar:

1. **Phishing Frenzy**: Una plataforma de phishing automatizada que facilita la creación y gestión de campañas de phishing. Permite realizar seguimiento de correos electrónicos, analizar datos de phishing y automatizar respuestas a los usuarios.
2. **Gophish**: Una herramienta de phishing de código abierto y fácil de usar que permite a los equipos de seguridad llevar a cabo simulaciones de phishing y evaluar la conciencia de seguridad de los empleados.
3. **BeEF (Browser Exploitation Framework)**: Aunque no es exclusivamente una herramienta de phishing, BeEF se utiliza para explotar las vulnerabilidades de los navegadores web y puede ser utilizado para comprometer sistemas a través de ingeniería social, como ataques basados en el navegador.
4. **CredSniper**: Una herramienta diseñada específicamente para capturar credenciales a través de páginas de phishing, facilitando la creación y personalización de sitios web de phishing.
5. **Evilginx**: Una herramienta que facilita la captura de credenciales mediante ataques de phishing a sitios web que utilizan autenticación basada en cookies (como Google, Facebook, LinkedIn, etc.).
6. **King Phisher**: Una herramienta de phishing avanzada con una interfaz gráfica de usuario (GUI) que permite la creación y gestión de campañas de phishing, incluyendo plantillas personalizables y seguimiento de correos electrónicos.

Estas herramientas pueden ser útiles dependiendo de tus necesidades específicas y del entorno en el que estás realizando pruebas de penetración. Es importante recordar que el uso de estas herramientas debe ser ético y legal, y siempre se debe obtener el consentimiento adecuado antes de realizar pruebas de seguridad en cualquier sistema o red.