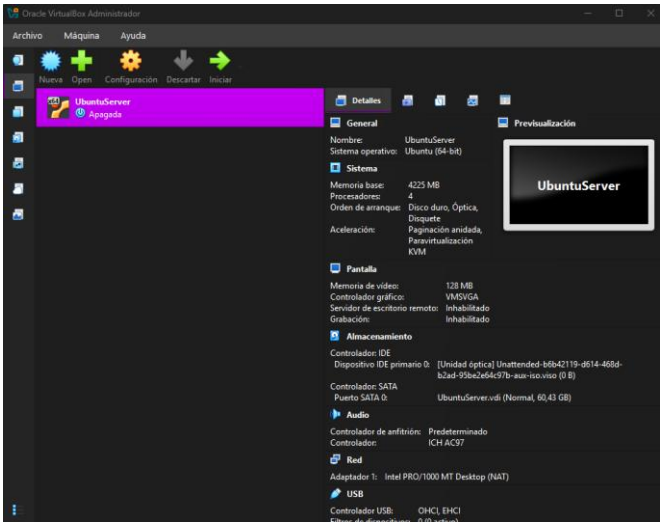
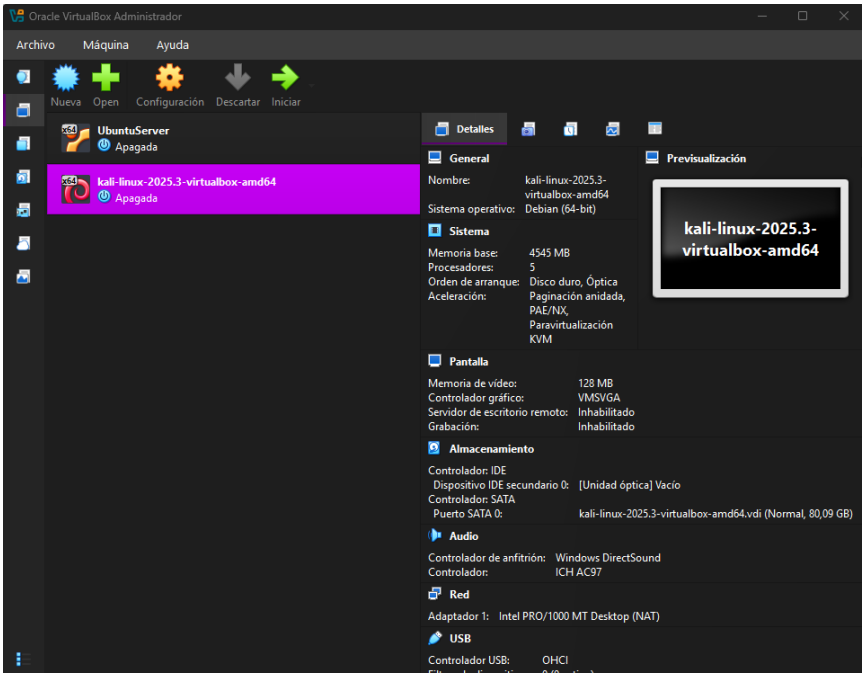
Simular Phishing

1. Documentación del Proceso Técnico



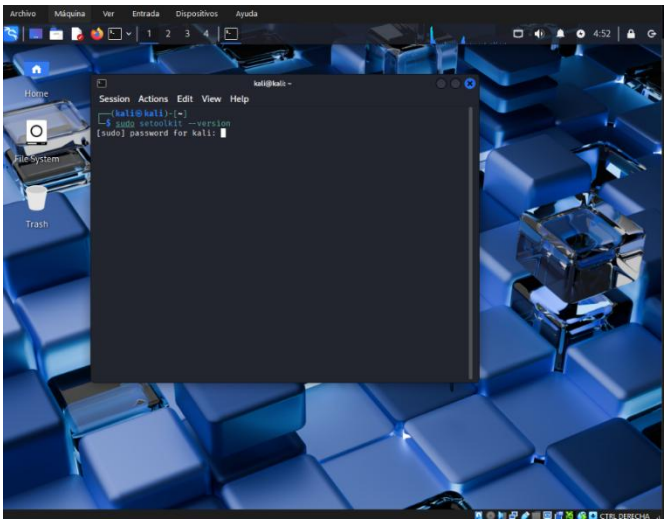
1.1 Instalación del Entorno

- Descarga de Kali Linux en VirtualBox.
- Configuración de la máquina virtual (por defecto viene con los requisitos mínimos).
- Inicio de sesión con usuario y contraseña por defecto.



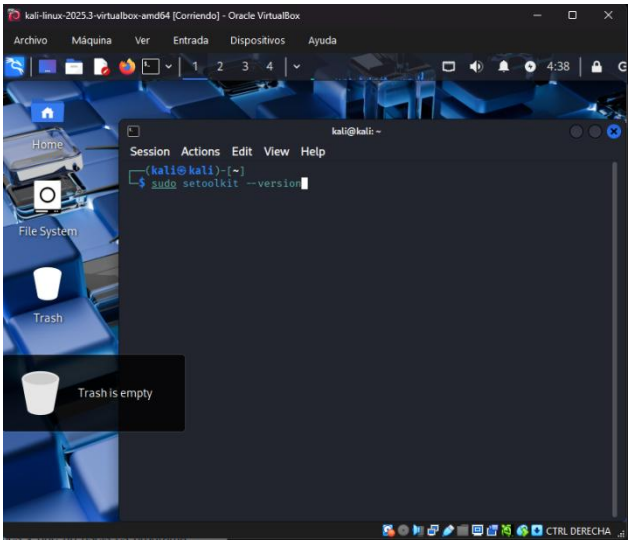
1.2 Verificación de SET

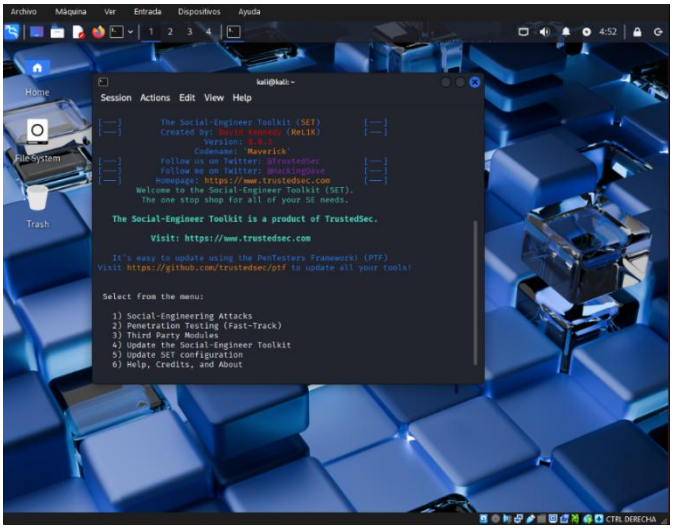
- Comando:
- sudo setoolkit --version
- Aceptación de términos de uso.

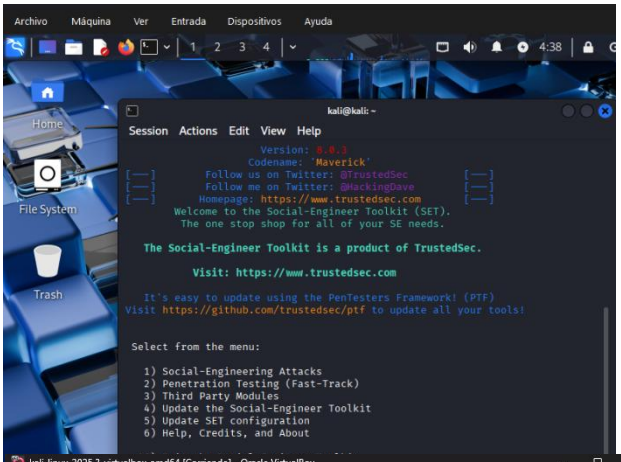


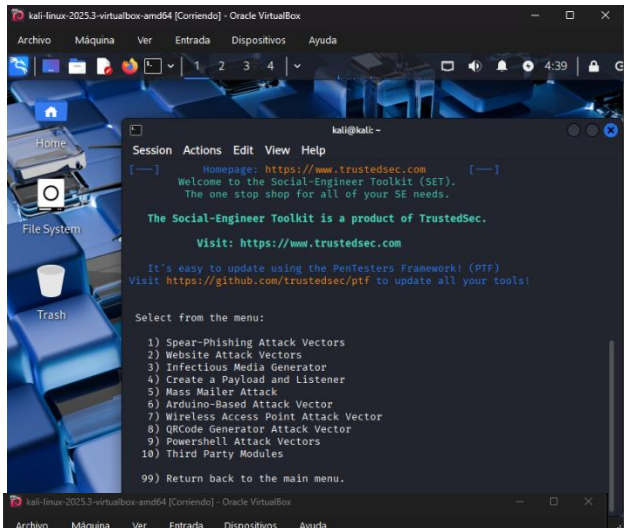
1.3 Configuración del Ataque de Phishing

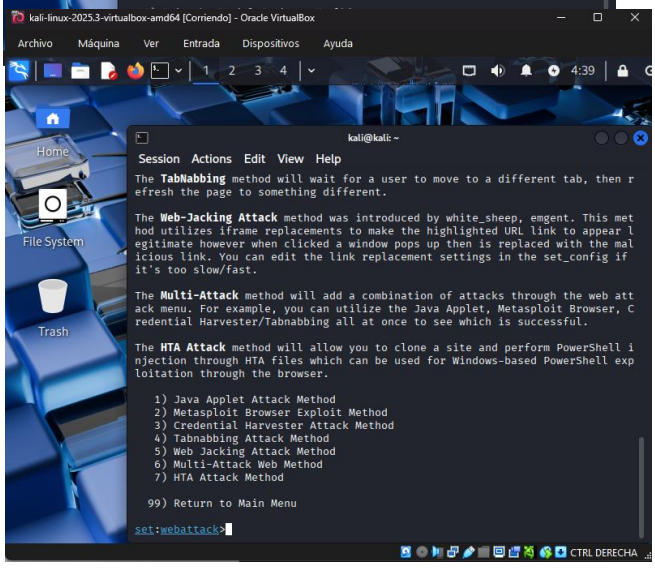
1. Abrir SET como root:
2. sudo setoolkit
3. Seleccionar opciones en el menú:
    - 1) Social-Engineering Attacks
    - 2) Website Attack Vectors
    - 3) Credential Harvester Attack Method
    - 2) Site Cloner
4. Introducir IP de la MV (Enter para predeterminada).
5. Indicar URL a clonar (ej. https://www.calasanzsalamanca.es/aulavirtual/login/index.php)

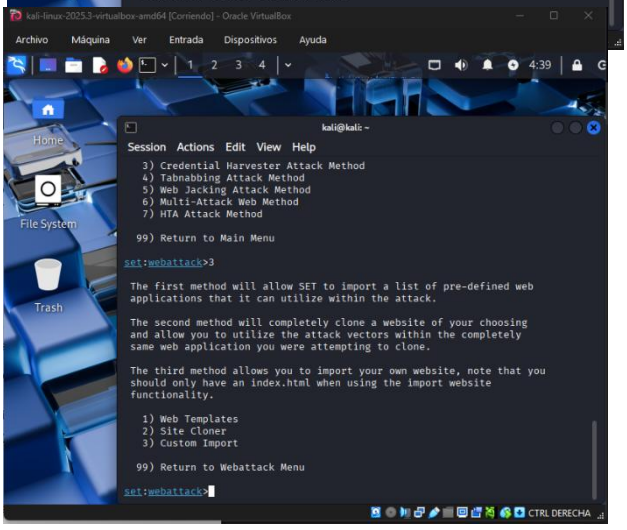


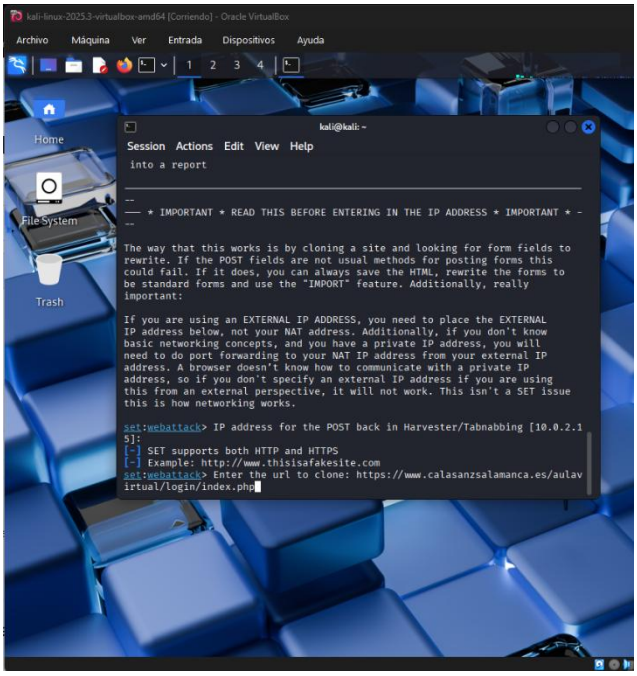






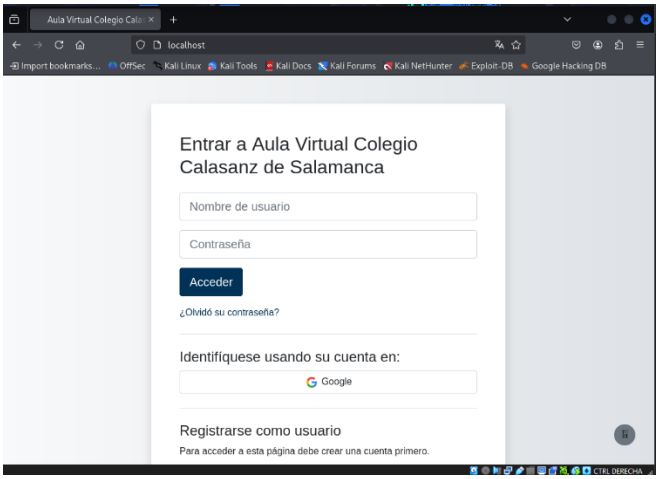


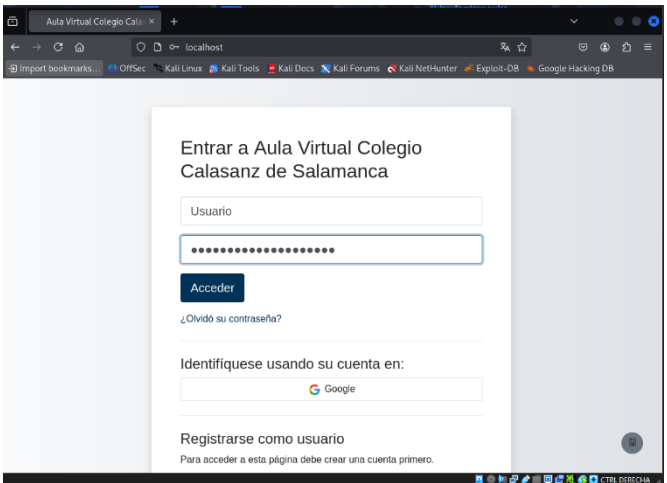


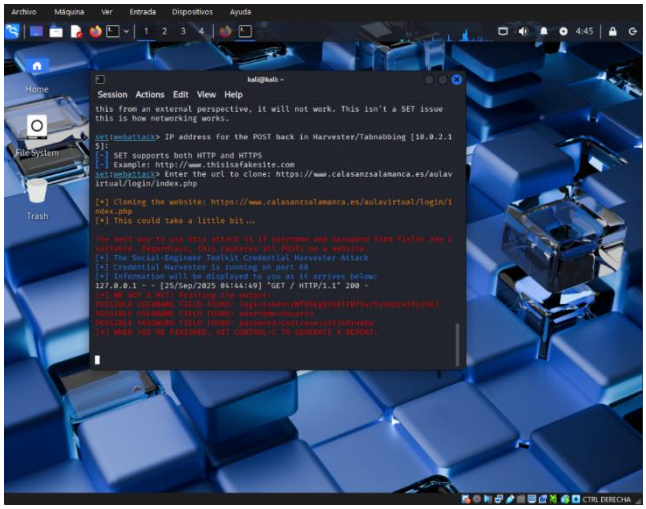


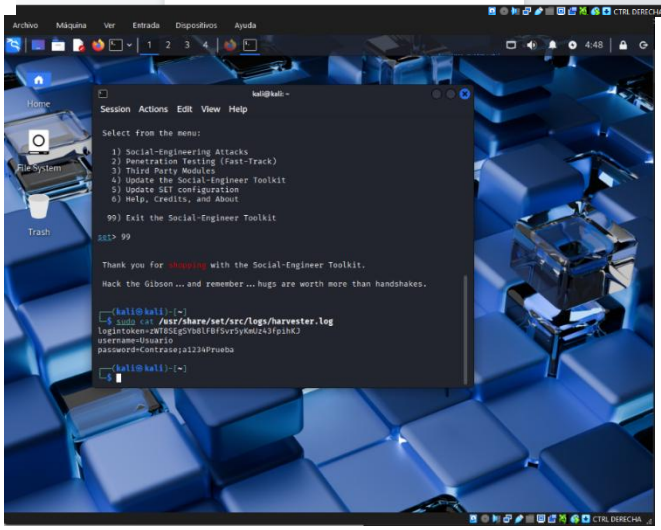
1.4 Captura de Credenciales

- En navegador abrir: http://localhost:80.
- Ingresar credenciales de prueba.
- En la terminal se muestra:
- [*] WE GOT A HIT!
- Ver logs capturados:
- sudo cat /usr/share/set/src/logs/harvester.log









2. Reflexión y Análisis

2.1 Vulnerabilidades explotadas

- Técnicas:
  - Clonación de páginas web mediante copia de HTML y formularios.
  - Uso de la red local para interceptar datos enviados por el usuario.
- Humanas:
  - Confianza del usuario en páginas aparentemente legítimas.
  - Falta de verificación de la URL o certificado SSL.
  - Impulsividad al ingresar datos en sitios familiares sin comprobar autenticidad.

2.2 Posibles consecuencias para una víctima real

- Robo de credenciales de correo, redes sociales o banca online.
- Pérdida de información personal y confidencial.
- Suplantación de identidad.
- Riesgos financieros (fraudes, compras no autorizadas, acceso a cuentas bancarias).

2.3 Medidas preventivas

1. Verificar siempre la URL y el certificado HTTPS antes de introducir credenciales.
2. Activar autenticación multifactor (MFA/2FA) en servicios importantes.
3. Mantener actualizado el navegador y usar filtros anti-phishing.
4. Formación y concienciación en ciberseguridad para usuarios.

2.4 Importancia del uso educativo

- Estas técnicas son ilegales si se aplican fuera de un entorno controlado.
- El objetivo es aprender cómo actúan los atacantes para estar preparados, no para dañar.
- Su mal uso puede conllevar responsabilidades penales y éticas.
- En el ámbito académico, contribuye a la formación en ciberseguridad defensiva.