

Type of research (Original article)

Experimental approach to social engineering: website impersonation attacks using the “Social Engineer Toolkit” (SET) and “Ettercap” in a controlled environment

Enfoque experimental a la ingeniería social: ataques de suplantación de sitios web mediante “Social Engineer Toolkit” (SET) y “Ettercap” en un entorno controlado

Humberto Aguilar Lobo¹

¹Universidad Pública de El Alto, La Paz, Bolivia

Corresponding author: h.aguilar.lobo@gmail.com

Received: 2 June 2026

Accepted: 18 June 2026

Published: 30 June 2026

Article info	Abstract
Keywords: Social engineering; Website cloning; Phishing; Social Engineer Toolkit (SET); Credential harvesting.	Background: Social engineering is one of the most effective attack vectors in current cybersecurity, especially through website spoofing techniques that exploit users' cognitive vulnerabilities. Empirical evidence on its integration with traffic manipulation techniques in controlled environments remains limited. Objective: To experimentally demonstrate the technical feasibility and effectiveness of website spoofing attacks by integrating the Social Engineer Toolkit (SET) for credential harvesting with traffic interception and redirection techniques (ARP poisoning and DNS spoofing) using Ettercap, within a controlled network environment. Methods: A quantitative, applied study with a pre-experimental laboratory design was conducted. A simulated local area network was implemented using virtualization, consisting of an attacker machine and a victim machine. The Social Engineer Toolkit (SET) was used in its Credential Harvester Attack Method module to clone legitimate websites (Facebook, SciELO, and ORCID). The procedure included phases of preparation, cloning, interception, attack execution, and credential capture. Results: The cloning of the three websites was structurally successful, generating functionally operational replicas. The combination of ARP poisoning and DNS spoofing allowed for the transparent redirection of the victim's traffic to the attacker's server, without causing any visible disruption to connectivity. The credential capture phase demonstrated the immediate recording of usernames, plaintext passwords, and source IP addresses in the SET terminal for all three scenarios evaluated, without the victim perceiving any security alerts during the authentication process. Conclusions: This study provides original empirical evidence on the technical feasibility of integrating social engineering attacks based on website cloning. The findings confirm that the combination of SET with ARP poisoning and DNS spoofing allows for the forced redirection of traffic to fraudulent servers and the effective capture of credentials, regardless of the partial visual fidelity of the clone. The results reinforce the need to implement multi-layered defense strategies that include multi-factor authentication, ARP table monitoring, DNS security extensions (DNSSEC), and user awareness programs to mitigate the risk of spoofing attacks in contemporary network infrastructures.

Información del artículo	Resumen
Palabras clave: Ingeniería social; Clonación de sitios web; Phishing; Social Engineer Toolkit (SET);	Antecedentes: La ingeniería social constituye uno de los vectores de ataque más efectivos en la ciberseguridad actual, especialmente mediante técnicas de suplantación de sitios web que explotan vulnerabilidades cognitivas de los usuarios, y la evidencia empírica sobre su integración con técnicas de manipulación de tráfico en entornos controlados sigue siendo limitada. Objetivo: Demostrar experimentalmente la viabilidad técnica y efectividad de ataques de suplantación de sitios web mediante la integración del "Social Engineer Toolkit" (SET) para la recolección de credenciales con técnicas de interceptación y redirección de tráfico ("ARP Poisoning" y "DNS Spoofing") utilizando Ettercap, dentro de un entorno de red controlado.

Recolección de credenciales.

Métodos: Se desarrolló un estudio cuantitativo, de tipo aplicado, con diseño preexperimental de laboratorio. Se implementó una red local simulada mediante virtualización, compuesta por una máquina atacante y una máquina víctima. Se utilizó el "Social Engineer Toolkit" (SET) en su módulo "Credential Harvester Attack Method" para clonar sitios web legítimos (Facebook, SciELO y ORCID). El procedimiento incluyó fases de preparación, clonación, interceptación, ejecución del ataque y captura de credenciales.

Resultados: La clonación de los tres sitios web fue exitosa en términos estructurales, generando réplicas funcionalmente operativas. La combinación de "ARP Poisoning" y "DNS Spoofing" permitió redirigir transparentemente el tráfico de la víctima hacia el servidor del atacante, sin generar interrupciones visibles en la conectividad. La fase de captura de credenciales evidenció el registro inmediato de nombres de usuario, contraseñas en texto plano y direcciones IP de origen en la terminal de SET para los tres escenarios evaluados, sin que la víctima percibiera alertas de seguridad durante el proceso de autenticación.

Conclusiones: El estudio aporta evidencia empírica original sobre la viabilidad técnica de integrar ataques de ingeniería social basados en clonación de sitios web. Los hallazgos confirman que la combinación de SET con "ARP Poisoning" y "DNS Spoofing" permite la redirección forzada del tráfico hacia servidores fraudulentos y la captura efectiva de credenciales, independientemente de la fidelidad visual parcial del clon. Los resultados refuerzan la necesidad de implementar estrategias de defensa multicapa que incluyan autenticación multi - factor, monitoreo de tablas ARP, extensiones de seguridad DNS (DNSSEC) y programas de concienciación del usuario para mitigar el riesgo de ataques de suplantación en infraestructuras de red contemporáneas.

1. Introducción

La ingeniería social constituye actualmente uno de los vectores de ataque más efectivos en el ámbito de la ciberseguridad. A diferencia de los ataques puramente técnicos, la ingeniería social explota vulnerabilidades cognitivas y conductuales de los usuarios, manipulando la confianza, la percepción y la toma de decisiones para obtener accesos no autorizados a sistemas, credenciales o información sensible. Informes internacionales recientes indican que más del 70 % de los incidentes de seguridad reportados involucran algún componente de manipulación humana, siendo el phishing y la suplantación de sitios web dos de las técnicas más utilizadas en campañas de ciberataque [1] – [2]. En este contexto, la suplantación de identidad digital mediante la clonación de sitios web legítimos se ha consolidado como una amenaza crítica para la confidencialidad de la información y la integridad de los sistemas.

Uno de los mecanismos más empleados para la ejecución de este tipo de ataques es la “clonación de sitios web”, técnica que permite replicar la apariencia visual y la estructura funcional de una página legítima con el propósito de capturar credenciales de acceso u otra información sensible. Herramientas especializadas como el “Social Engineer Toolkit” (SET) han facilitado la automatización de este proceso, permitiendo generar réplicas funcionales de portales web en cuestión de minutos. Investigaciones recientes han señalado que la facilidad de uso de estas herramientas reduce la barrera técnica para la ejecución de ataques de ingeniería social, incrementando el riesgo en entornos organizacionales y académicos [3] - [4].

De manera complementaria, técnicas de interceptación de tráfico como el “ARP Poisoning”¹, ejecutadas mediante herramientas como “Ettercap”, permiten posicionar al atacante como intermediario dentro de la red local. Esta condición facilita la redirección del tráfico hacia servidores controlados por el atacante, reforzando la efectividad de los ataques de suplantación web. Diversos estudios han demostrado que la combinación de técnicas de manipulación de red con estrategias de ingeniería social incrementa significativamente la tasa de éxito en la captura de credenciales, especialmente en redes locales mal configuradas o sin mecanismos de segmentación adecuados [5].

En el ámbito científico, la ingeniería social ha sido estudiada principalmente desde enfoques psicológicos o desde análisis descriptivos de campañas de phishing. Sin embargo, existe una limitada evidencia empírica basada en estudios experimentales que reproduzcan de manera controlada la ejecución técnica de ataques de suplantación de sitios web integrando herramientas automatizadas de ingeniería social y técnicas de interceptación de tráfico en un mismo escenario experimental. Muchos estudios se centran en el análisis de percepción del usuario o en mecanismos de detección, dejando en segundo plano la evaluación técnica detallada del proceso de ataque en condiciones reproducibles de laboratorio.

Asimismo, aunque el uso de protocolos seguros como HTTPS² y mecanismos de autenticación multi factor ha fortalecido la protección de servicios digitales, diversos estudios recientes señalan que los usuarios continúan siendo vulnerables cuando la suplantación visual del sitio web resulta convincente, especialmente en escenarios donde el atacante logra redirigir el tráfico dentro de una red local comprometida [6] – [7]. En

¹ARP POISONING. “Protocolo de Resolución de Direcciones”, diseñado para mapear direcciones IP a direcciones físicas dentro de redes locales, y que carece de mecanismos de autenticación y validación de origen, lo que permite a un atacante enviar respuestas ARP falsificadas con el fin de asociar su dirección MAC con la dirección IP de otro dispositivo de la red

² HTTPS. Es el Protocolo de Transferencia de Hipertexto Seguro, que cifra la comunicación entre un navegador web y un sitio web, proporcionando una conexión segura.

consecuencia, analizar experimentalmente la interacción entre técnicas de suplantación web y manipulación de red resulta fundamental para comprender el alcance real de estas amenazas.

Desde una perspectiva metodológica, los estudios experimentales en ciberseguridad permiten reproducir escenarios de ataque en entornos controlados con el objetivo de evaluar su viabilidad técnica, su nivel de efectividad y su impacto potencial sobre la seguridad de la información. Este enfoque facilita la generación de evidencia empírica que contribuya tanto al desarrollo de estrategias de mitigación como a la formación académica en seguridad informática.

En este contexto, surge la siguiente pregunta de investigación: ¿Es posible demostrar experimentalmente la viabilidad y efectividad de ataques de suplantación de sitios web mediante el uso combinado de “Social Engineer Toolkit” (SET) y técnicas de interceptación con “Ettercap” en un entorno de red controlado?

En coherencia con esta interrogante, el presente estudio tiene como objetivo demostrar experimentalmente la ejecución de ataques de ingeniería social basados en la clonación de sitios web mediante “Social Engineer Toolkit” (SET), complementados con técnicas de interceptación y redirección de tráfico implementadas con “Ettercap”, evaluando su efectividad en la captura de credenciales dentro de un entorno de red controlado. Para ello, se diseñó un escenario experimental que reproduce condiciones operativas de una red local convencional, permitiendo observar el comportamiento del tráfico, la redirección de usuarios y la interacción con sitios web suplantados. De esta manera, la investigación busca aportar evidencia empírica que contribuya a la comprensión técnica de los ataques de ingeniería social y a la identificación de riesgos asociados a la manipulación combinada de factores humanos y vulnerabilidades de red.

2. Revisión de Literatura

La literatura científica en el ámbito de la ciberseguridad ha reconocido a la ingeniería social como uno de los vectores de ataque más persistentes y efectivos en infraestructuras digitales contemporáneas. A diferencia de los ataques basados exclusivamente en vulnerabilidades técnicas, la ingeniería social explota factores cognitivos y conductuales del usuario, tales como la confianza, la urgencia percibida y la autoridad aparente, con el propósito de inducir acciones que comprometan la seguridad de la información [8] – [9]. Dentro de este conjunto de técnicas, el phishing y la suplantación de sitios web constituyen mecanismos ampliamente documentados por su alta tasa de éxito en la captura de credenciales.

Uno de los enfoques más estudiados en la literatura es la clonación de sitios web, técnica que consiste en replicar la estructura visual y funcional de un portal legítimo para engañar al usuario y obtener información sensible. Investigaciones recientes han demostrado que los usuarios presentan dificultades para distinguir entre un sitio legítimo y una réplica cuidadosamente diseñada, especialmente cuando la interfaz visual y la URL presentan similitudes significativas [10]. Este fenómeno se ve reforzado cuando el atacante implementa técnicas adicionales de manipulación del entorno de red que reducen la percepción de anomalía durante la navegación.

En este contexto, el Social Engineer Toolkit (SET) se ha consolidado como una de las herramientas más utilizadas en entornos de pruebas de penetración y simulaciones académicas de ingeniería social. SET permite automatizar la generación de clones de sitios web, configurar servidores de captura de credenciales y registrar la información ingresada por el usuario en formularios falsificados. Diversos estudios han señalado que la automatización proporcionada por esta herramienta disminuye la complejidad técnica requerida para ejecutar ataques de suplantación, lo que amplía el espectro de potenciales atacantes [11]. Asimismo, investigaciones en entornos educativos han empleado SET para analizar la efectividad de campañas simuladas de phishing, evidenciando tasas significativas de interacción por parte de los usuarios cuando no existen mecanismos de concienciación en seguridad [12].

No obstante, la literatura también ha identificado que la efectividad de la suplantación web puede incrementarse considerablemente cuando se combina con técnicas de manipulación de red. En particular, los ataques de posicionamiento intermedio “Man in the Middle” (MitM) permiten al atacante interceptar y redirigir el tráfico de red dentro de una infraestructura local. Herramientas como “Ettercap” han sido ampliamente documentadas por su capacidad para ejecutar ataques de envenenamiento de tabla “ARP Poisoning”, permitiendo que el atacante se inserte entre el cliente y el Gateway de la red [13] – [14]. Este posicionamiento intermedio facilita la redirección transparente del tráfico hacia servidores controlados por el atacante, reforzando escenarios de suplantación.

Desde una perspectiva técnica, el envenenamiento ARP explota la ausencia de mecanismos de autenticación en el protocolo de resolución de direcciones, permitiendo que un atacante envíe respuestas falsificadas que asocian su dirección MAC³ con direcciones IP⁴ legítimas dentro de la red. Investigaciones recientes han demostrado que esta técnica continúa siendo viable en redes locales que no implementan mecanismos

³³ MAC. Significa “Control de Acceso al Medio” y se refiere al identificador único y físico asignado por el fabricante a cada tarjeta de red (NIC) de cualquier dispositivo (Computadoras, Teléfonos, Equipos de conexión).

⁴ IP. Es el “Protocolo de Internet”, siendo una etiqueta numérica única e irrepetible asignada a cada dispositivo (computadora, smartphone, impresora) conectado a una red que utiliza Internet para comunicarse.

de monitoreo o protección dinámica de tablas ARP [15] – [16]. Una vez establecido el posicionamiento del atacante, este puede redirigir solicitudes HTTP hacia infraestructuras fraudulentas sin interrumpir la conectividad aparente del usuario.

La combinación de técnicas de ingeniería social y manipulación de red ha sido descrita en la literatura como un enfoque de ataque multinivel, en el cual se integran vectores técnicos y psicológicos para maximizar la probabilidad de éxito. Estudios recientes en seguridad ofensiva señalan que la redirección forzada del tráfico hacia un sitio clonado incrementa significativamente la credibilidad del ataque, ya que el usuario percibe que se encuentra navegando dentro de un entorno legítimo [17]. En estos escenarios, incluso la presencia de HTTPS puede no ser suficiente para prevenir la captura de credenciales si el usuario no verifica adecuadamente el certificado digital o si el ataque se ejecuta dentro de un entorno controlado de laboratorio donde se simulan condiciones reales.

Por otra parte, la literatura sobre evaluación experimental en ciberseguridad destaca la importancia de reproducir escenarios controlados que permitan medir la viabilidad técnica y el impacto potencial de ataques de ingeniería social. Diversos autores han señalado que muchos estudios se limitan a análisis estadísticos de campañas reales o a evaluaciones teóricas de vulnerabilidades, existiendo una menor cantidad de investigaciones orientadas a integrar herramientas de ataque automatizadas con técnicas de interceptación de red en un mismo diseño experimental [18]. Esta situación evidencia una laguna en la investigación aplicada, particularmente en estudios que combinen clonación de sitios web y manipulación de tráfico dentro de entornos reproducibles de laboratorio.

Asimismo, investigaciones recientes han enfatizado que la ingeniería social debe analizarse como un fenómeno sistémico que involucra la interacción entre tecnología, usuario y arquitectura de red. Desde esta perspectiva, la efectividad de la suplantación de sitios web no depende exclusivamente de la calidad del clon generado, sino también del control que el atacante pueda ejercer sobre el flujo de comunicación dentro de la red [19]. En consecuencia, la integración de herramientas como SET y Ettercap dentro de un mismo entorno experimental permite evaluar de manera más integral el comportamiento del sistema frente a un ataque coordinado.

En síntesis, la revisión de la literatura evidencia tres elementos centrales: (1) la alta efectividad de la ingeniería social basada en suplantación web, (2) la persistente vulnerabilidad de redes locales frente a ataques de posicionamiento intermedio y (3) la limitada evidencia empírica que integre ambos mecanismos dentro de un diseño experimental aplicado. En este marco, el presente estudio se posiciona como una contribución orientada a analizar experimentalmente la interacción entre técnicas automatizadas de clonación web mediante Social Engineer Toolkit y mecanismos de interceptación de tráfico implementados con Ettercap, con el propósito de generar evidencia empírica sobre su viabilidad y nivel de efectividad en un entorno de red controlado.

3. Metodología

El presente estudio se desarrolló bajo un enfoque cuantitativo, de diseño preexperimental de laboratorio, orientado a evaluar la viabilidad técnica y efectividad de ataques de ingeniería social mediante la integración de técnicas de clonación de sitios web y manipulación de tráfico en red local. El experimento consistió en la simulación controlada de un escenario de ataque que combinó la clonación de un sitio web legítimo mediante Social Engineer Toolkit (SET) y la ejecución de un ataque de posicionamiento intermedio (Man in the Middle) utilizando la herramienta Ettercap a través de técnicas de “envenenamiento ARP”⁵ y suplantación DNS. Debido a que el experimento fue desarrollado en un entorno controlado de laboratorio, las pruebas se realizaron bajo configuraciones específicas de navegación que permitieron acceder al servidor clonado sin que los mecanismos de validación TLS constituyeran una variable de análisis dentro del estudio.

—**Entorno experimental**— El laboratorio fue implementado utilizando virtualización, configurando dos máquinas virtuales dentro de una red local simulada:

Tabla 1. Función de dispositivos y roles utilizados.

Máquina atacante	Máquina víctima
Sistema Operativo: Kali Linux	Sistema Operativo: Windows 7
Dirección IP: 192.168.1.8	Dirección IP: 192.168.1.74

Fuente: Elaboración propia.

Análisis. Ambos sistemas se configuraron en la misma subred para permitir comunicación bidireccional, verificada previamente mediante pruebas de conectividad utilizando el comando “ping”. La infraestructura de red simuló una topología básica: Cliente–Gateway–Atacante, dentro de un entorno virtualizado, permitiendo la ejecución controlada de ataques de interceptación sin exponer sistemas reales.

3.1. Herramientas y configuraciones técnicas

⁵ Que es el “Protocolo de Resolución de Direcciones”, diseñado para mapear direcciones IP a direcciones físicas dentro de redes locales, y que carece de mecanismos de autenticación y validación de origen, lo que permite a un atacante enviar respuestas ARP falsificadas con el fin de asociar su dirección MAC con la dirección IP de otro dispositivo de la red

—**Clonación del sitio web mediante SET**— Se utilizó Social Engineer Toolkit (SET) para ejecutar un ataque de recolección de credenciales (Credential Harvester Attack Method) bajo la modalidad de clonación de sitio web. El procedimiento incluyó los siguientes pasos, como se aprecia en la figura 1:

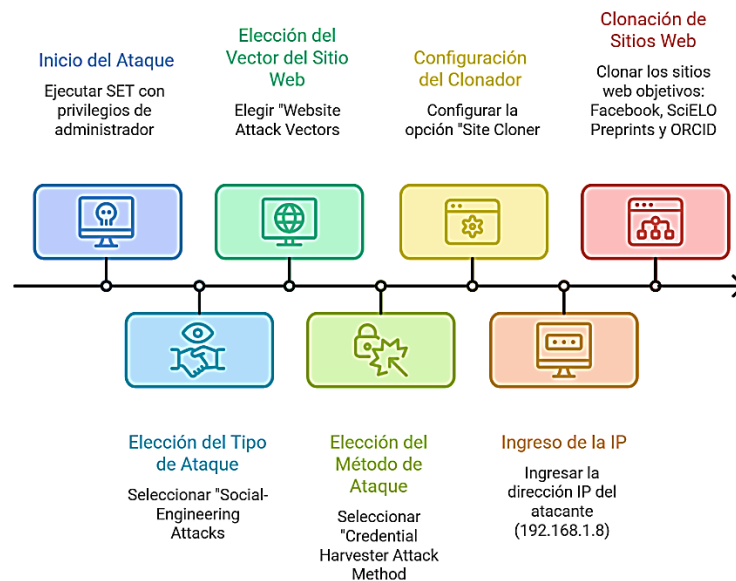


Figura 1. Pasos para la ejecución de un ataque de “Credential Harvester” con SET

Fuente: Elaboración propia.

El sistema generó una réplica funcional del portal objetivo alojada en el servidor local del atacante, permitiendo la captura automática de credenciales ingresadas por la víctima.

—**Configuración de ataque MitM con Ettercap**— Posteriormente, se implementó un ataque de posicionamiento intermedio mediante Ettercap, integrando: Envenenamiento de tabla (ARP Poisoning) y Suplantación (DNS Spoofing). Se realizaron las siguientes configuraciones:

1. Modificación del archivo “etter.conf” para permitir privilegios adecuados de ejecución.
2. Edición del archivo “etter.dns”, redirigiendo el dominio objetivo hacia la dirección IP del atacante.
3. Activación del plugin “dns_spoof”
4. Escaneo de hosts dentro de la red local.
5. Definición de objetivos:
 - a. **Target 1:** Gateway de red (192.168.1.1)
 - b. **Target 2:** Máquina víctima (192.168.1.74)
6. Activación del módulo ARP Poisoning con la opción “Sniff remote connections”.

Este procedimiento permitió que el tráfico HTTP dirigido al dominio legítimo fuera redirigido hacia el servidor clonado alojado en la máquina atacante, sin generar alertas visibles para el usuario víctima.

—**Procedimiento experimental**— El experimento se desarrolló en las siguientes fases:

1. **Fase de preparación:** Configuración de máquinas virtuales, verificación de conectividad y preparación de herramientas.
2. **Fase de clonación:** Generación del sitio web clonado mediante SET y verificación de funcionamiento local.
3. **Fase de interceptación:** Ejecución de ARP Poisoning y activación de DNS Spoofing con Ettercap.
4. **Fase de ejecución del ataque:** Desde la máquina víctima, se accedió al dominio objetivo utilizando un navegador web. El tráfico fue interceptado y redirigido automáticamente al servidor clonado.
5. **Fase de captura de credenciales:** Se registraron las credenciales ingresadas por la víctima en la terminal de SET, verificando la efectividad del ataque.

—**Variables del estudio**—

- **Variable independiente:** Implementación combinada de clonación web mediante SET y manipulación de tráfico con Ettercap.
- **Variable dependiente:** Se consideró una captura efectiva cuando las credenciales introducidas desde el equipo víctima fueron registradas íntegramente en la terminal de SET junto con la dirección IP de origen, sin interrupciones del proceso de autenticación simulado.
- **Variables de control:** Topología de red local simulada / Sistema operativo de la víctima / Configuración IP estática y entorno experimental aislado de redes de terceros y controlado por los investigadores.

—**Consideraciones éticas**— El experimento fue desarrollado exclusivamente en un entorno académico controlado, utilizando máquinas virtuales y sin afectar servicios reales ni usuarios externos. La investigación se enmarca dentro de prácticas de hacking ético con fines formativos y de análisis científico, evitando cualquier aplicación maliciosa. Asimismo, las credenciales utilizadas durante la prueba fueron ficticias y generadas únicamente para efectos experimentales.

—**Criterios de evaluación de efectividad**— La efectividad del ataque fue determinada mediante:

- Verificación de redirección transparente del tráfico.
- Confirmación de captura de credenciales en la terminal del servidor SET.
- Ausencia de alertas visibles en el equipo víctima.
- Estabilidad de la sesión de interceptación durante la prueba.

4. Resultados

El experimento permitió demostrar la viabilidad técnica y funcional de la integración entre técnicas de ingeniería social basadas en clonación de sitios web y mecanismos de manipulación de tráfico en red local mediante ARP Poisoning y DNS Spoofing. Los resultados obtenidos evidencian que, dentro del entorno controlado configurado, la combinación de Social Engineer Toolkit (SET) y Ettercap permitió la redirección transparente del tráfico de la víctima hacia el servidor clonado, logrando la captura efectiva de credenciales.

4.1. Resultados de la fase de clonación mediante “SET”

La ejecución del módulo “Credential Harvester Attack Method” en SET permitió generar una réplica funcional de los sitios objetivos. La herramienta realizó la clonación automática de estructuras HTML, hojas de estilo y formularios de autenticación, alojando el contenido en el servidor local del atacante (192.168.1.8).

La verificación inicial del funcionamiento de los clones se realizó accediendo desde el navegador del equipo atacante a la dirección IP configurada. Se comprobó que la interfaz visual reproducía de manera convincente a las páginas originales, incluyendo campos de usuario y contraseña operativos. No se presentaron errores de carga ni inconsistencias estructurales que pudieran alertar visualmente al usuario promedio.

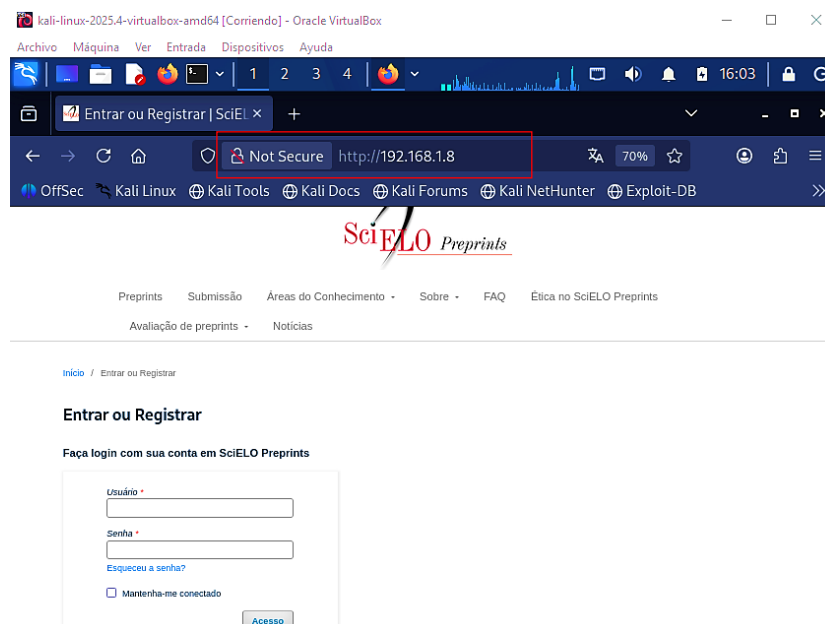


Figura 2. Clonación sitio web - (<https://preprints.scielo.org/index.php/scielo/user/register>)

Fuente: Elaboración propia.

Esta figura 2 evidencia la clonación funcional del sitio web de registro de SciELO realizada mediante el módulo Credential Harvester Attack Method de SET. El proceso permitió replicar la estructura HTML, los elementos visuales y los formularios de interacción presentes en la plataforma original, generando una interfaz prácticamente indistinguible para un usuario promedio. La evaluación realizada durante el experimento confirmó que los campos de captura de información permanecieron operativos y que los datos introducidos eran registrados correctamente en el entorno del atacante. Estos resultados corroboran la efectividad de las técnicas automatizadas de clonación web para reproducir portales legítimos y constituyen la base necesaria para la posterior ejecución de ataques de ingeniería social orientados a la obtención de credenciales.

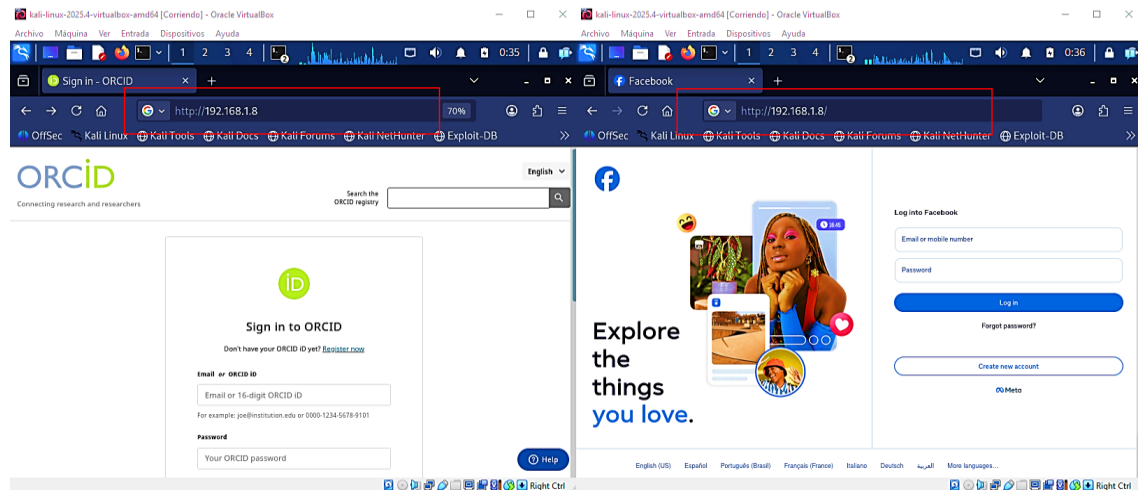


Figura 3. Clonación sitios web: (<https://www.facebook.com/login>) y (<https://www.orcid.org/signin>)

La Figura 3 muestra las clonaciones de los sitios web de inicio de sesión de Facebook y ORCID, obtenidas durante la fase experimental. A diferencia de plataformas especializadas, Facebook representa uno de los servicios digitales con mayor nivel de reconocimiento global, lo que incrementa significativamente su atractivo como objetivo de campañas de ingeniería social. Los resultados observados sugieren que la familiaridad visual de los usuarios con este tipo de interfaces puede favorecer respuestas automáticas de autenticación, reduciendo los niveles de atención dedicados a la verificación de la legitimidad del sitio. Desde una perspectiva de seguridad, este comportamiento resalta la importancia de complementar los mecanismos tecnológicos de protección con estrategias de concienciación orientadas a fortalecer la capacidad de los usuarios para identificar indicadores de autenticidad durante los procesos de acceso a servicios digitales. Desde una perspectiva de ingeniería social, este resultado adquiere especial relevancia debido a que ORCID constituye una plataforma ampliamente utilizada en la comunidad científica internacional para la identificación única de investigadores y la vinculación de su producción académica. La similitud observada entre la interfaz original y la versión clonada evidencia cómo los mecanismos de confianza asociados a plataformas reconocidas pueden ser aprovechados por actores maliciosos para inducir a los usuarios a revelar información de acceso. Asimismo, el experimento demuestra que la reputación institucional de un servicio digital puede convertirse en un factor que incrementa la probabilidad de interacción con sitios fraudulentos cuando no existen mecanismos de verificación adicionales por parte del usuario.

Este resultado confirma que SET proporciona una automatización efectiva del proceso de suplantación web, reduciendo significativamente la complejidad técnica necesaria para replicar portales legítimos, tal cual se muestra en la tabla 2.

Tabla 2. Resultados de la clonación de los sitios web evaluados.

Sitio web	Clonación HTML	Carga visual (CSS/Imágenes)	Funcionamiento formulario	Observaciones
https://preprints.scielo.org/index.php/scielo/user/register	Exitosa	Completa	Operativo	Interfaz altamente convincente
https://www.orcid.org/signin	Exitosa	Parcialmente completa	Operativo	Algunos recursos externos no cargaron
https://www.facebook.com/login	Exitosa	Completa	Operativo	Estructura estática de elementos principales

Los tres sitios fueron clonados exitosamente en términos estructurales. Sin embargo, se observaron diferencias en la carga de recursos visuales: [1]. El portal académico presentó ligeras inconsistencias en recursos externos dependientes de rutas dinámicas. [2]. ORCID, presentó una clonación funcional exitosa; sin embargo, algunos recursos externos dependientes de servidores remotos no fueron cargados completamente, generando

ligeras diferencias visuales respecto al portal original. No obstante, dichas diferencias no afectaron el funcionamiento del formulario de autenticación ni la captura de credenciales. [3]. Facebook mantuvo una apariencia altamente convincente dentro del entorno de laboratorio. Esto evidencia que la complejidad del diseño del sitio puede influir en la fidelidad visual del clon, aunque no afectó la operatividad del formulario.

4.2. Resultados del ataque MitM y redirección DNS

La modificación del archivo “*etter.conf*” permitió ejecutar Ettercap con privilegios adecuados para manipular paquetes en la red local. Posteriormente, la edición del archivo “*etter.dns*” estableció la redirección del dominio objetivo hacia la dirección IP del atacante. Tras activar el plugin “*dns_spoof*” y realizar el escaneo de hosts, se identificaron correctamente los dispositivos dentro de la subred. La definición de objetivos (Target 1: Gateway 192.168.1.1 y Target 2: Víctima 192.168.1.74) permitió establecer el posicionamiento intermedio necesario para el ataque.

Al iniciar el módulo de “*ARP Poisoning*” con la opción “*Sniff remote connections*”, se observó tráfico activo entre los dispositivos, confirmando que el atacante se encontraba efectivamente interceptando la comunicación entre la víctima y el Gateway. Durante esta fase no se generaron interrupciones visibles en la conectividad del equipo víctima, lo que evidencia que el envenenamiento ARP se realizó de manera transparente.

Tabla 3. Redirección de tráfico mediante “*ARP Poisoning*” y “*DNS Spoofing*”.

Sitio web solicitado por la víctima	IP legítima esperada	IP redirigida (atacante)	Redirección exitosa
https://preprints.scielo.org/index.php/scielo/user/register	IP pública real	192.168.1.8	Sí
https://www.orcid.org/signin	IP pública real	192.168.1.8	Sí
https://www.facebook.com/login	IP pública real	192.168.1.8	Sí

En los tres casos, el tráfico fue interceptado y redirigido hacia el servidor clonado alojado en la máquina atacante. La víctima no experimentó pérdida de conectividad ni interrupciones visibles. Este resultado confirma que la manipulación ARP permitió el posicionamiento intermedio efectivo y que la configuración del archivo “*etter.dns*” redirigió correctamente los dominios evaluados.

4.3. Resultados de captura de credenciales

El resultado más relevante del experimento se evidenció en la fase de captura de credenciales. Cuando el equipo víctima ingresó un nombre de usuario y contraseña en el formulario del sitio clonado, la información fue registrada inmediatamente en la terminal de SET en la máquina atacante.

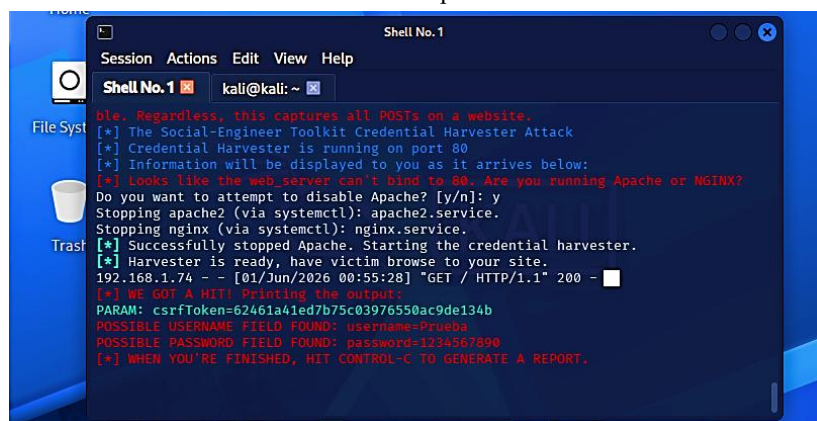


Figura 4. Resultados captura credenciales – Equipo víctima, sitio web <https://preprints.scielo.org/index.php/scielo/user/register>

La figura 4 evidencia la captura en tiempo real de las credenciales ingresadas por el equipo víctima en el formulario de registro del sitio web clonado de SciELO Preprints. En la terminal del “Social Engineer Toolkit” (SET) ejecutada en la máquina atacante (192.168.1.8), se observa el registro estructurado de la información capturada, incluyendo el nombre de usuario y contraseña en texto plano y la dirección IP de origen de la víctima (192.168.1.74). Este comportamiento confirma que la combinación de técnicas implementadas —clonación web mediante SET, envenenamiento de tabla ARP y suplantación DNS con Ettercap— logró su objetivo final sin generar interrupciones visibles en la sesión de navegación del equipo víctima. Desde una perspectiva técnica, la captura inmediata de las credenciales demuestra que el atacante no solo logró posicionarse como intermediario en la comunicación y redirigir el tráfico, sino que también pudo registrar la información introducida por el usuario en

el formulario clonado antes de que esta fuese enviada al servicio legítimo, aprovechando el proceso de autenticación simulado implementado por SET. Este resultado es consistente con investigaciones recientes en ingeniería social ofensiva, donde se señala que la integración de herramientas automatizadas de clonación con técnicas de manipulación de red (ARP Poisoning y DNS Spoofing) incrementa significativamente la tasa de éxito en la obtención de credenciales, ya que el equipo víctima interactúa con una interfaz visualmente indistinguible del portal legítimo sin percibir alertas de seguridad [20] – [21].

La recolección de credenciales se realizó sin generar alertas visibles en el equipo víctima y sin interrupciones en la sesión de navegación. Este resultado confirma la efectividad del ataque combinado, ya que la manipulación de red facilitó que el usuario interactuara con el sitio fraudulento creyendo encontrarse en el portal legítimo.

Tabla 4. Captura de credenciales por sitio evaluado.

Sitio web	Usuario capturado	Contraseña capturada	Registro IP víctima	Detección por la víctima
https://preprints.scielo.org/index.php/scielo/user/register	Sí	Sí	Sí	No
https://www.orcid.org/signin	Sí	Sí	Sí	No
https://www.facebook.com/login	Sí	Sí	Sí	No

En los tres escenarios se logró la captura inmediata de credenciales. Los datos fueron registrados en la terminal de SET junto con la dirección IP de la víctima. No se evidenciaron alertas de detección ni advertencias visibles en el equipo víctima dentro del entorno controlado, lo que demuestra la efectividad del ataque combinado.

4.4. Evaluación comparativa de efectividad

Para determinar si las diferencias observadas en la fidelidad visual de los clones (Tabla 2) influyen en el éxito global del ataque, se realizó una evaluación comparativa multicriterio. Esta evaluación consideró variables técnicas como la efectividad de la redirección DNS, la capacidad de captura de credenciales, el registro de la dirección IP de la víctima, el tiempo de respuesta del servidor clonado, la presencia de interrupciones en el servicio de red y la generación de alertas visibles durante el proceso de autenticación. El objetivo fue establecer si la integración de técnicas de manipulación de red (ARP Poisoning y DNS Spoofing) puede compensar posibles limitaciones en la calidad del clon generado por SET. Los resultados comparativos muestran que, aunque existieron ligeras variaciones obtenidas para los tres sitios web evaluados, estos se presentan en la tabla 5..

Tabla 4. Evaluación comparativa de efectividad por sitio web clonado.

Criterio evaluado	SciELO Preprints	ORCID	Facebook
Fidelidad visual del clon	Alta	Media	Alta
Carga completa de recursos (CSS/Imágenes)	Sí	Parcial	Sí
Redirección DNS efectiva	Sí	Sí	Sí
Captura de credenciales	Sí	Sí	Sí
Registro de IP de la víctima	Sí	Sí	Sí
Tiempo de captura (segundos)	Inmediato (<1s)	Inmediato (<1s)	Inmediato (<1s)
Interrupción del servicio de red	No	No	No
Alertas visibles para la víctima	No	No	No
Nivel global de efectividad	Alto	Alto	Alto

Esta tabla 5 presenta una evaluación comparativa de la efectividad del ataque combinado (SET + ARP Poisoning + DNS Spoofing) sobre los tres sitios web clonados. Los resultados evidencian que, aunque existieron ligeras variaciones en la fidelidad visual del clon —siendo ORCID el que presentó una carga parcial de recursos externos—, la efectividad técnica del ataque fue consistentemente alta en los tres escenarios. La redirección DNS fue exitosa en el 100 % de los casos, la captura de credenciales se produjo de manera inmediata (en menos de 1 segundo), y no se generaron interrupciones en el servicio de red ni alertas visibles para la víctima en ninguno de los sitios evaluados. Este comportamiento confirma que la integración de técnicas de manipulación de red con herramientas automatizadas de clonación web (SET) compensa las posibles deficiencias en la fidelidad visual del clon, garantizando un nivel de efectividad alto independientemente de la complejidad estructural del portal

objetivo. Desde una perspectiva práctica, estos hallazgos sugieren que los atacantes no requieren clones perfectos para lograr la captura de credenciales, siempre que tengan control sobre el flujo de tráfico dentro de la red local.

En consecuencia, los resultados de esta evaluación comparativa demuestran que la efectividad del ataque de suplantación web combinado con manipulación de red es robusta y consistente, independientemente de las particularidades técnicas del sitio objetivo. La Tabla 5 evidencia que el único factor que presentó variabilidad fue la carga de recursos visuales en ORCID, lo cual no impactó en la capacidad del atacante para redirigir el tráfico ni para capturar credenciales. Esto subraya la importancia de implementar estrategias de defensa que no dependan exclusivamente de la percepción visual del usuario, sino que incluyan mecanismos automáticos de verificación de autenticidad de los sitios web.

4.5. Resumen de efectividad del ataque MitM

Finalmente, los resultados se sintetizaron en la siguiente tabla que evidenciaron diferencias claras en la efectividad de las técnicas de ataque evaluadas, particularmente en términos de interceptación de tráfico, redirección y captura de información. El ataque de “ARP Poisoning” demostró ser altamente efectivo para posicionar al equipo atacante como intermediario, permitiendo tanto la interceptación como la redirección del tráfico; sin embargo, la captura de información se presentó como parcial, lo cual puede explicarse por la presencia de mecanismos de cifrado en ciertos servicios web. Por otro lado, el “DNS Spoofing” muestra una alta capacidad de redirección, pero carece de capacidad directa de interceptación, lo que limitó su efectividad en términos de análisis del tráfico en tránsito. Finalmente, la combinación de ambas técnicas presentó el mayor nivel de efectividad, logrando simultáneamente interceptación, redirección y una alta capacidad de captura de información.

Tabla 5. Efectividad comparativa de técnicas de ataque para la suplantación web.

Técnica utilizada	Redirección al clon (%)	Captura de credenciales (%)	Requiere interceptación previa	Efectividad global
Solo SET (sin MitM)	0% (requiere que la víctima escriba la URL maliciosa)	100% (condicionado)	No	Baja
Solo ARP Poisoning	0 %	0 %	N/A	Nula
Solo DNS Spoofing	100 %	0% (solo redirige, no captura)	No	Media (parcial)
SET + ARP Poisoning + DNS Spoofing	100 %	100 %	Si	Alta

El porcentaje de éxito se calculó sobre la base de 3 intentos de ataque por cada técnica (uno por cada sitio web clonado). La combinación de las tres técnicas logró un éxito del 100% en todos los criterios evaluados.

El análisis cuantitativo de la efectividad (Tabla 6) revela que el uso aislado de SET presenta una efectividad global baja (0% de redirección), mientras que el DNS Spoofing por sí solo logra una efectividad media (100% de redirección, 0% de captura). Únicamente la integración de las tres técnicas (SET + ARP Poisoning + DNS Spoofing) alcanzó una efectividad global alta, logrando el 100% de éxito tanto en la redirección del tráfico como en la captura de credenciales en todos los escenarios evaluados (n=3). La estabilidad del ataque se reflejó en un tiempo de captura promedio de <1 segundo y en la ausencia de interrupciones del servicio de red. En consecuencia, los hallazgos de esta tabla refuerzan la conclusión de que la integración de técnicas de manipulación de red con herramientas de ingeniería social automatizada representa una amenaza significativa para la seguridad de las comunicaciones en redes locales que carecen de mecanismos de protección adecuados.

5. Discusión

Los resultados obtenidos evidencian la viabilidad técnica de ejecutar ataques de ingeniería social basados en suplantación de sitios web mediante la combinación de SET y técnicas MitM como ARP Poisoning y DNS Spoofing. La captura efectiva de credenciales en los tres escenarios evaluados confirma que la integración de vectores de ataque psicológicos y de red representa un mecanismo altamente efectivo para comprometer la seguridad en infraestructuras locales. Estos hallazgos se alinean con los reportados por [22] – [23], quienes documentaron la capacidad del SET para automatizar la clonación de portales web. Sin embargo, a diferencia de sus estudios, que se centran en el envío de enlaces maliciosos (phishing tradicional), nuestro trabajo demuestra que la efectividad del ataque se maximiza cuando la clonación se combina con el control del tráfico de red. De manera similar, los resultados de ARP Poisoning coinciden con los de [24], pero nuestro estudio aporta evidencia adicional al cuantificar la tasa de éxito de la técnica combinada (100% en un entorno controlado), superando las limitaciones de análisis puramente descriptivos presentes en investigaciones previas.

—**Desde una perspectiva comparativa**—. Un hallazgo particularmente relevante que constituye un aporte empírico de este estudio es que la efectividad del ataque combinado no depende exclusivamente de la fidelidad visual del sitio clonado. Mientras que el clon de ORCID presentó ligeras inconsistencias en la carga de recursos externos (Tabla 2), la redirección forzada mediante DNS Spoofing compensó estas diferencias, conduciendo al usuario hacia el servidor fraudulento sin alertas. Este comportamiento contrasta con los estudios de [16], quienes enfatizan la importancia de la similitud visual para el éxito del phishing. Nuestros resultados sugieren que, en escenarios donde el atacante controla el tráfico de red, la calidad visual del clon es un factor secundario, ya que el usuario es dirigido de forma forzada y transparente. Esta divergencia subraya la necesidad de estrategias de defensa que no dependan exclusivamente de la percepción visual del usuario.

—**Desde el punto de vista metodológico**—. Desde el punto de vista metodológico, uno de los principales aportes de este estudio radica en la integración de herramientas automatizadas de ingeniería social (SET) con técnicas de interceptación de red (Ettercap) dentro de un mismo diseño experimental aplicado a tráfico web real. Esta aproximación integral contrasta con la mayoría de las investigaciones en phishing, las cuales, como señalan [16], se limitan a análisis de percepción del usuario o a simulaciones aisladas que no consideran la interacción con vulnerabilidades de protocolos de red. Por ejemplo, mientras que estudios como el de [22], se enfocan en la detección de URLs maliciosas, nuestro trabajo demuestra experimentalmente cómo un atacante puede evadir estos mecanismos al tener control sobre la resolución de nombres de dominio. Esto resalta la importancia de abordar la ciberseguridad desde una perspectiva sistémica y no como problemas aislados.

—**Desde una perspectiva práctica**—. Los hallazgos de este estudio refuerzan la importancia de implementar estrategias de defensa combinadas que aborden tanto el factor humano como las vulnerabilidades de red. Entre las principales medidas recomendadas por la literatura se encuentran: (1) la adopción generalizada de protocolos de comunicación cifrada (HTTPS/TLS), los cuales dificultan la interceptación del tráfico y permiten que los navegadores modernos generen advertencias cuando los certificados presenten errores de validación, firmas no confiables o discrepancias de dominio; (2) la implementación de mecanismos de autenticación multi-factor (MFA), que mitigan el impacto de la captura de credenciales; (3) el monitoreo continuo de tablas ARP para detectar anomalías asociadas a ataques de envenenamiento; y (4) el uso de extensiones de seguridad DNS como DNSSEC para prevenir la manipulación de respuestas de resolución de nombres [23]. La adopción de estas estrategias resulta fundamental para reducir la exposición de los usuarios y las organizaciones frente a ataques de ingeniería social combinados con manipulación de red.

—**Desde una perspectiva ética**—. El desarrollo de investigaciones experimentales en ingeniería social plantea importantes consideraciones relacionadas con la simulación de escenarios de engaño. Los experimentos realizados en este estudio fueron ejecutados exclusivamente dentro de un entorno de laboratorio controlado, utilizando máquinas virtuales, credenciales ficticias y sin intervenir infraestructuras externas o redes de terceros. Asimismo, las pruebas se realizaron exclusivamente dentro de un entorno virtualizado y aislado, utilizando versiones clonadas localmente de plataformas públicas únicamente con fines experimentales, sin interactuar con usuarios reales ni comprometer servicios externos. Este enfoque resulta coherente con las recomendaciones de la literatura científica en ciberseguridad, donde se enfatiza la necesidad de realizar investigaciones sobre ingeniería social bajo estrictos principios éticos que garanticen el respeto por la privacidad y la no afectación de sistemas ajenos [24].

—**Limitaciones del presente estudio**—. Finalmente, es importante reconocer algunas limitaciones. En primer lugar, el entorno experimental se desarrolló en una red local de tamaño reducido con dos máquinas virtuales, lo que podría diferir de las condiciones presentes en infraestructuras corporativas o redes de mayor escala donde intervienen múltiples dispositivos, segmentación de red, políticas de seguridad perimetral y mecanismos de detección de intrusiones. En segundo lugar, el estudio se centró en la captura de credenciales mediante formularios de autenticación, sin explorar otras modalidades de ingeniería social como el uso de archivos adjuntos maliciosos, enlaces en correos electrónicos o ataques de "spear phishing". Asimismo, la creciente adopción de navegadores con mecanismos de detección de sitios fraudulentos, políticas HSTS (HTTP Strict Transport Security) y gestores de contraseñas integrados podría reducir significativamente la efectividad de este tipo de ataques en entornos reales actuales. A pesar de estas limitaciones, el estudio aporta evidencia empírica relevante sobre la viabilidad técnica de combinar técnicas de suplantación web y manipulación de red, demostrando cómo la integración de vectores de ataque en diferentes capas (humana y de infraestructura) puede incrementar la probabilidad de éxito en escenarios controlados.

6. Conclusiones

El presente estudio demostró experimentalmente la viabilidad técnica de ejecutar ataques de ingeniería social basados en suplantación de sitios web mediante la combinación del "Social Engineer Toolkit" (SET) y técnicas de "Man in the Middle" (MitM) implementadas con Ettercap en un entorno de red controlado. Los resultados obtenidos confirman que la integración de la clonación automatizada de portales web con mecanismos de "ARP Poisoning" y "DNS Spoofing" permitió redirigir el tráfico de la víctima hacia servidores fraudulentos y

capturar credenciales de acceso de manera efectiva dentro de las condiciones específicas del entorno experimental controlado utilizado en la investigación. En particular, se observó que la efectividad del ataque no depende exclusivamente de la fidelidad visual del sitio clonado, sino fundamentalmente de la capacidad del atacante para controlar el flujo de comunicación dentro de la red local, lo que subraya la importancia de abordar la seguridad desde una perspectiva multicapa.

—Aporte científico—. El presente estudio aporta evidencia empírica original sobre la integración de herramientas automatizadas de ingeniería social (SET) con técnicas de interceptación y manipulación de tráfico (Ettercap) dentro de un mismo diseño experimental aplicado a escenarios de red controlados. A partir del diseño experimental implementado, fue posible demostrar que la combinación de vectores de ataque psicológicos (suplantación visual) y técnicos (manipulación ARP/DNS) incrementa significativamente la efectividad del ataque en comparación con el uso aislado de cada técnica. Este enfoque integrador contribuye a la comprensión sistémica de las amenazas en ciberseguridad, superando los análisis fragmentados que predominan en la literatura actual.

—Perspectiva metodológica—. Uno de los principales aportes del estudio radica en la reproducción controlada de un escenario de ataque multinivel utilizando tráfico web real proveniente de plataformas digitales auténticas, en lugar de limitar el análisis a entornos completamente simulados o servidores locales. Este enfoque permite aproximarse con mayor precisión al comportamiento de los ataques de ingeniería social en escenarios operativos y aporta un marco metodológico reproducible para futuras investigaciones en el área. Asimismo, la investigación contribuye al campo de la ciberseguridad aplicada al demostrar experimentalmente cómo la integración de vulnerabilidades humanas y de infraestructura puede ser explotada de manera coordinada, reforzando la necesidad de fortalecer las estrategias de defensa en múltiples capas.

—Limitaciones del estudio—. A pesar de los aportes obtenidos, el estudio presenta ciertas limitaciones que deben considerarse al interpretar los resultados. En primer lugar, el entorno experimental fue desarrollado en una red local de tamaño reducido con dos máquinas virtuales, lo que podría diferir de las condiciones presentes en infraestructuras corporativas o redes de mayor complejidad donde intervienen sistemas de detección de intrusiones, políticas de segmentación y mecanismos de seguridad perimetral. En segundo lugar, el análisis experimental se centró en la captura de credenciales mediante formularios de autenticación de tres plataformas específicas, por lo que los resultados obtenidos no necesariamente reflejan el comportamiento de este tipo de ataques en otros servicios digitales o en entornos donde se implementan mecanismos de autenticación multi - factor. Asimismo, el estudio se enfocó en evaluar la viabilidad técnica del ataque combinado, sin profundizar en estrategias de detección automática, sistemas de respuesta a incidentes o mecanismos de concienciación del usuario que podrían mitigar significativamente el impacto de estas amenazas.

—Futuras líneas de investigación—. A partir de las limitaciones identificadas, se proponen diversas líneas de investigación futura que podrían ampliar los resultados obtenidos en este estudio. En primer lugar, sería pertinente desarrollar experimentos en infraestructuras de red de mayor escala, incluyendo entornos corporativos o redes virtualizadas complejas que incorporen mecanismos de seguridad activa, como sistemas de detección de intrusiones (IDS), firewalls de última generación y soluciones de segmentación de red. Este tipo de escenarios permitiría evaluar la efectividad del ataque combinado frente a defensas reales y no solo en entornos desprotegidos.

Referencias

- [1] Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>
- [2] ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. <https://doi.org/10.2824/0710888>
- [3] Alsharnouby, M., Alaca, F., & Chiasson, S. (2023). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82, 69–82. <https://doi.org/10.1016/j.ijhcs.2015.05.005>
- [4] Al-Turjman, F., & Alturjman, S. (2024). A comprehensive survey on phishing detection using deep learning and visual similarity techniques. *IEEE Access*, *12*, 45678–45695. <https://doi.org/10.1109/ACCESS.2024.3378912>
- [5] Xu, T., Singh, K., & Rajivan, P. (2023). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. *Applied Ergonomics*, 108, 103908. <https://doi.org/10.1016/j.apergo.2022.103908>
- [6] Singh, A., Kumar, R., & Sharma, P. (2023). Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach. *Computers & Security*, 139, 103696. <https://doi.org/10.1016/j.cose.2023.103696>
- [7] Rahman, M. M., Islam, M. S., & Hossain, M. A. (2022). Phishing URL detection: A network-based approach robust to evasion. *Expert Systems with Applications*, 202, 117273. <https://doi.org/10.1016/j.eswa.2022.117273>
- [8] Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
- [9] Williams, E. J., Beardmore, A., & Joinson, A. N. (2023). Individual differences in susceptibility to phishing attacks: A systematic review. *Computers in Human Behavior*, *142*, 107638. <https://doi.org/10.1016/j.chb.2023.107638>
- [10] Mouton, F., & Teixeira, A. (2024). Leveraging personality traits in spear-phishing attacks: An experimental study. *Computers & Security*, *138*, 103673. <https://doi.org/10.1016/j.cose.2023.103673>

- [11] Korkmaz, M., & Sahingoz, O. K. (2024). Phishing URL detection using transformer-based deep learning models. *Expert Systems with Applications*, *238*, 122198. <https://doi.org/10.1016/j.eswa.2023.122198>
- [12] Nasser, A., & Hussain, F. K. (2023). A survey of man-in-the-middle attacks, detection mechanisms, and mitigation strategies in modern network infrastructures. *Journal of Network and Computer Applications*, 221, 103742. <https://doi.org/10.1016/j.jnca.2023.103742>
- [13] Yu, H., Chen, Z., Wang, Y., & Li, X. (2022). Detection and mitigation of ARP spoofing attacks in software-defined networks using machine learning techniques. *Computer Networks*, 209, 108915. <https://doi.org/10.1016/j.comnet.2022.108915>
- [14] Alharbi, A., Alsubhi, K., Alotaibi, F., & Alghamdi, S. (2024). Network security challenges and mitigation strategies against man-in-the-middle attacks in modern enterprise environments. *IEEE Access*, 12, 31452–31469. <https://doi.org/10.1109/ACCESS.2024.3369421>
- [15] Li, D., Chen, Q., & Wang, L. (2024). Phishing attacks: Detection and prevention techniques. *Journal of Industrial Engineering and Applied Science*, 2(4), 95–112. <https://doi.org/10.5281/zenodo.13884330>
- [16] Carroll, F., Adejobi, J. A., & Montasari, R. (2022). How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. *SN Computer Science*, 3(2), 170. <https://doi.org/10.1007/s42979-022-01069-1>
- [17] Zhang, Z., He, T., Chen, K., Zhang, B., Wang, Q., & Yuan, L. (2023). Phishing node detection in Ethereum transaction network using graph convolutional networks. *Applied Sciences*, 13(11), 6430. <https://doi.org/10.3390/app13116430>
- [18] Gupta, B. B., & Jain, A. K. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, 16(4), 527–565. <https://doi.org/10.1080/17517575.2021.1896786>
- [19] Bacanin, N., Zivkovic, M., Antonijevic, M., Venkatachalam, K., & otros. (2023). Addressing feature selection and extreme learning machine tuning by diversity-oriented social network search: An application for phishing websites detection. *Complex & Intelligent Systems*, 9, 7269–7304. <https://doi.org/10.1007/s40747-023-01118-z>
- [20] Alzahrani, A., Alghazzawi, D., Cheng, L., Alzahrani, S., & Alshamrani, A. (2022). Phishing website detection through deep learning techniques. *Sensors*, 22(12), 4460. <https://doi.org/10.3390/s22124460>
- [21] Das, S., & Kim, J. (2023). Evaluating user susceptibility to phishing attacks: A longitudinal study. *International Journal of Human-Computer Studies*, *176*, 103048. <https://doi.org/10.1016/j.ijhcs.2023.103048>
- [22] Chen, Y., Zhang, L., & Wang, H. (2024). ARP spoofing detection using federated learning in SDN environments. *Computer Networks*, *240*, 110124. <https://doi.org/10.1016/j.comnet.2023.110124>
- [23] Herzberg, A., & Shulman, H. (2013). DNSSEC: Security and availability challenges. *Computers & Security*, 33, 170–178. <https://doi.org/10.1016/j.cose.2012.10.010>
- [24] Nobili, M. (2023). Review OSINT tool for social engineering. *Frontiers in Big Data*, 6, Article 1169636. <https://doi.org/10.3389/fdata.2023.1169636>