ESTUDIO DE CASO 1

Exposición de Credenciales en el Punto de Entrada: Simulación Controlada de Phishing en Localhost

Por: Joseph Gonzalez

ZERODAY TECH LABS

Alcance	Simulación solamente en localhost usando credenciales de prueba autogeneradas y páginas controladas por el investigador; fines educativos y analíticos únicamente
Entorno	Terminal de Kali Linux, página local de inicio de sesión de práctica, Firefox, SEToolkit y tráfico solamente en localhost
Evidencia principal	Captura de lanzamiento de SET, selección de ataque, pantalla de inicio de sesión fuente, clon en localhost y captura terminal redactada con barras negras
Vector de ataque principal	Interfaz de inicio de sesión clonada y credenciales enviadas por el usuario, capturadas en el punto de entrada dentro de un flujo controlado en localhost

Para uso educativo y analítico únicamente. Los detalles de direcciones locales y los valores enviados en las figuras fueron redactados con barras negras opacas.

Introducción

Los hogares son objetivos atractivos para el robo de credenciales porque los inicios de sesión diarios ocurren en teléfonos, computadoras portátiles, tabletas y dispositivos familiares compartidos. Las personas suelen iniciar sesión mientras están distraídas, reutilizan contraseñas entre servicios y confían en una página porque se ve familiar. Una interfaz clonada no tiene que ser perfecta; solo necesita parecer creíble el tiempo suficiente para que el usuario escriba y envíe sus credenciales.

Este estudio de caso utiliza una simulación local controlada para examinar el momento en que las credenciales quedan expuestas. El objetivo no es crear una guía operativa, sino mostrar cómo la confianza visual, el comportamiento rutinario de inicio de sesión y un mensaje de error creíble pueden convertir una acción normal en un evento de seguridad.

Metodología

Se realizó una simulación de ciberseguridad en un laboratorio virtual aislado usando Kali Linux, una página HTML local de inicio de sesión, un navegador web y SEToolkit como capa de instrumentación para observar el comportamiento del envío de formularios. El alcance se limitó a tráfico en localhost y datos de prueba autogenerados. No participaron víctimas reales, hosts públicos, cuentas de terceros ni sistemas de producción.

1. Resumen

Una página de inicio de sesión clonada es una interfaz engañosa que imita una pantalla esperada y captura datos en el momento en que se envía el formulario. En este escenario, la pregunta analítica fue si una página local de práctica, clonada y presentada nuevamente por localhost, registraría credenciales de prueba durante una interacción controlada.

2. Análisis de Amenaza: Vector, Técnica y Factor Humano

Vector de ataque usado	Recolección de credenciales mediante una interfaz de inicio de sesión clonada y servida en un entorno controlado de localhost. La exposición ocurre cuando el usuario envía el formulario.
Técnicas de ingeniería social	Phishing, suplantación visual de interfaz, explotación de familiaridad y normalización del error después del envío.
Factor humano explotado	Confianza en diseños familiares de inicio de sesión, entrada rutinaria de contraseñas, presión de tiempo, reutilización de contraseñas y tendencia a culpar al usuario o al servidor cuando ocurre un error.
Relevancia defensiva	La similitud visual no debe tratarse como prueba de confianza. La verificación del dominio, los gestores de contraseñas, las passkeys, las llaves de seguridad y MFA resistente al phishing reducen la probabilidad de una toma de cuenta.

Idea clave para el lector: el ataque funciona en el punto de decisión donde el usuario confía lo suficiente en la página para escribir. Los controles del backend importan después, pero la exposición comienza antes de que el servicio legítimo vea la contraseña.

3. Preparación del Ataque

El host de laboratorio se usó para preparar el flujo controlado de captura de credenciales. La Figura 1 documenta el entorno de lanzamiento de SET, mientras que la Figura 2 registra la ruta de selección del recolector de credenciales usada en la simulación. La importancia de esta fase no está en la sintaxis del comando, sino en que el entorno de prueba pudo presentar una experiencia normal de inicio de sesión mientras registraba lo ocurrido al enviar el formulario.

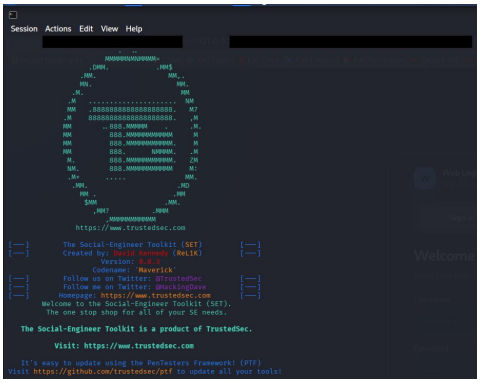

Figura 1. Entorno de lanzamiento de SET en el host de laboratorio, con detalles de direcciones locales redactados mediante barras negras.

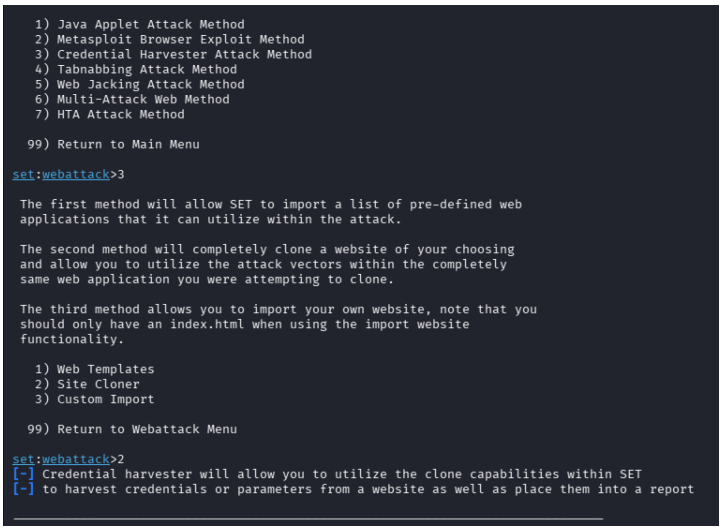

Figura 2. Vista de selección del recolector de credenciales de SET, documentando la ruta controlada usada en la simulación de laboratorio.

4. Ejecución y Evidencia Recopilada

La Figura 3 muestra la interfaz de inicio de sesión fuente usada como página de práctica. La Figura 4 muestra la interfaz clonada después del envío del formulario, donde la página permaneció visible y presentó un error de alcance del servidor en lugar de una redirección limpia. Ese detalle importa: un usuario puede interpretarlo como un problema normal de conectividad e intentarlo otra vez, aunque el primer envío ya ocurrió.

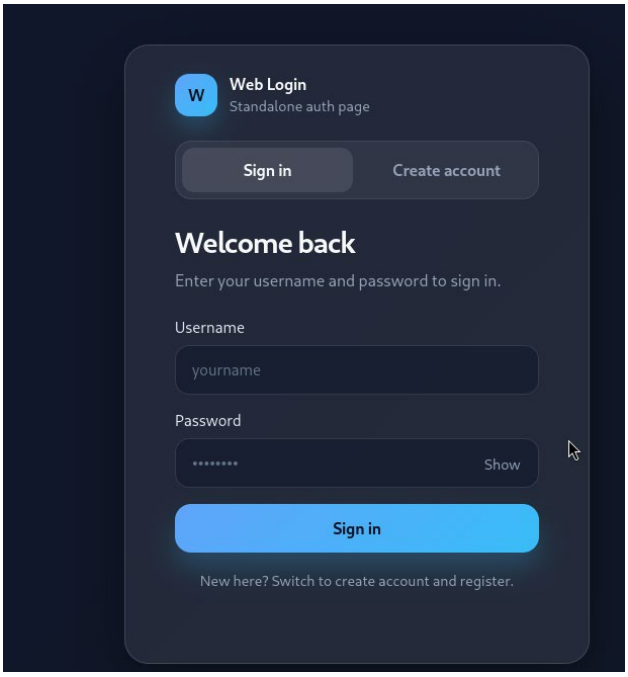

Figura 3. Interfaz de inicio de sesión fuente usada en la simulación controlada en localhost.

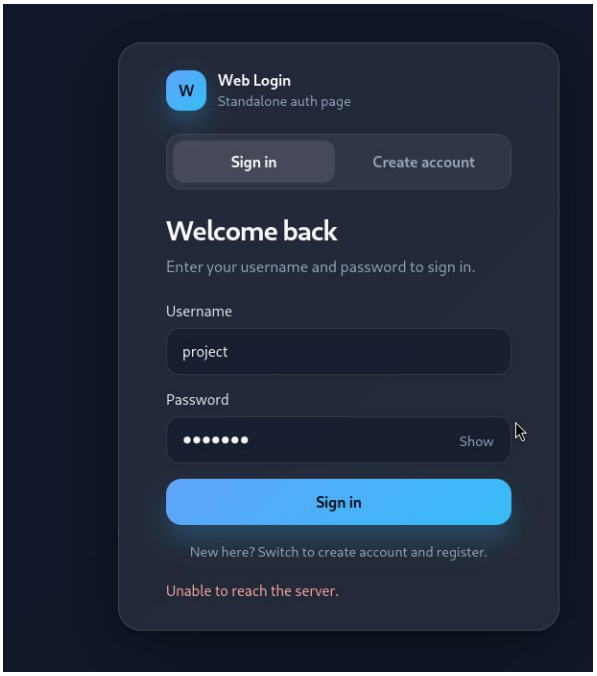

Figura 4. Clon en localhost después del envío del formulario, mostrando un error de alcance del servidor en lugar de una redirección limpia.

La salida de terminal en la Figura 5 funciona como el artefacto forense principal. Muestra que la página local de práctica fue clonada, servida al navegador y seguida por un evento de envío registrado que identifica posibles campos de usuario y contraseña. Los detalles de direcciones locales y los valores enviados fueron redactados antes de la publicación.

Figura 5. Captura cercana de terminal que documenta el evento de envío registrado, con direcciones locales y datos de credenciales ocultos por barras negras opacas.

5. Por Qué Ocurrió la Exposición

La exposición ocurrió porque la página preservó el patrón de interacción principal de un inicio de sesión normal. El usuario vio campos familiares, ingresó credenciales y presionó el botón esperado. La captura sucedió al momento del envío, antes de que el almacenamiento legítimo, el hashing de contraseñas o el monitoreo de cuenta fueran relevantes.

El componente humano es central. Las personas suelen explicar un inicio de sesión fallido como un error de escritura, una conexión débil o un problema temporal del servidor. Una página que permanece visible y muestra un error puede mantener al usuario dentro del engaño en vez de activar sospecha inmediata.

6. Impacto Real para el Individuo

Para un usuario individual, una sola contraseña capturada puede causar consecuencias que van mucho más allá de una página. Si la contraseña se reutiliza, puede facilitar toma de correo electrónico, abuso de restablecimiento de contraseñas, compras fraudulentas, bloqueo de cuentas, exposición de documentos personales o compromiso de almacenamiento en la nube y fotos familiares.

El impacto aumenta en el hogar porque las personas son menos formales en dispositivos personales. Guardan contraseñas en navegadores, comparten dispositivos con familiares, siguen enlaces desde mensajes de texto y actúan distraídas. La recuperación puede requerir bancos, proveedores de correo, restablecimiento de cuentas, revocación de sesiones y muchas horas de limpieza.

7. Mitigación, Parches y Prevención

La meta defensiva es hacer que la verificación del destino sea más fuerte que la confianza visual. Los gestores de contraseñas que solo autocompletan en el dominio correcto pueden interrumpir una página clonada de inmediato. Las passkeys, las llaves de seguridad y MFA resistente al phishing reducen la dependencia de contraseñas reutilizables y dificultan mucho el replay de credenciales.

Los usuarios deben preferir marcadores o aplicaciones oficiales para inicios de sesión importantes, mantener contraseñas únicas para cada servicio, activar alertas de inicio de sesión en correo y cuentas financieras, y tratar un error inesperado justo después de ingresar credenciales como una señal de advertencia, no como una simple equivocación.

8. Lista de Preparación para el Lector

Antes de ingresar credenciales	Verificar el dominio, usar un marcador o aplicación oficial para cuentas sensibles y permitir que el gestor de contraseñas valide el destino antes de autocompletar.
Durante un inicio sospechoso	No seguir intentando después de un error inesperado. Detenerse, cerrar la página y regresar por una ruta confiable en lugar de confiar solo en el diseño visible.
Después de posible exposición	Cambiar la contraseña desde un dispositivo confiable, revocar sesiones activas, revisar alertas de cuenta y habilitar MFA resistente al phishing cuando esté disponible.

9. Consideración Ética

Este estudio de caso se realizó en un entorno controlado estrictamente con fines educativos y analíticos. La interfaz fuente y la interfaz clonada fueron alojadas localmente, y todas las credenciales utilizadas fueron autogeneradas. No participaron usuarios reales, sistemas externos, hosts públicos ni servicios de terceros.

La lección defensiva es directa: verificar el destino, reducir la reutilización de contraseñas y tratar errores inesperados de inicio de sesión como posibles pistas de detección en lugar de ruido de fondo.