S5L5

Obiettivo:

Creare una simulazione di un'email di phishing utilizzando ChatGPT.

Istruzioni:

1. Creare uno scenario : Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc. Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).

2. Scrivere l'email di phishing: Utilizzate ChatGPT per generare il contenuto dell'email. Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).

3. Spiegare lo scenario: Descrivete lo scenario che avete creato. Spiegate perché l'email potrebbe sembrare credibile alla vittima. Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua

SCENARIO

L’obiettivo di questo esercizio è analizzare un potenziale scenario di phishing mirato, basato su tecniche di social engineering e utilizzo di informazioni pubbliche raccolte dai social media.

Scenario ipotetico

Un utente (il bersaglio) condivide abitualmente aggiornamenti sul proprio profilo Facebook, tra cui foto della sua auto in diversi contesti. In una delle immagini pubbliche, appare chiaramente la targa del veicolo. A partire da questa informazione, un attaccante con intenti malevoli potrebbe ricercare, tramite fonti pubbliche e strumenti di open-source intelligence (OSINT), dati relativi alla polizza assicurativa legata al veicolo.

Poniamo il caso che l'attaccante, sfruttando informazioni pubblicamente accessibili, riesca a individuare:

- La compagnia assicurativa (Zurich, ad esempio).

- La data di scadenza della polizza, che si avvicina.

Questi dati offrono all'attaccante un contesto sufficientemente dettagliato per creare un attacco di phishing credibile. Il malintenzionato può redigere un'email fraudolenta fingendosi rappresentante della compagnia assicurativa, avvisando l'utente di una scadenza imminente per il pagamento del premio assicurativo. Nell'email verrebbe incluso un link verso una falsa area di login per il pagamento, progettata per carpire le credenziali d’accesso e i dati della carta di credito dell'utente.

Obiettivo dell'esercizio

Questo scenario è stato sviluppato per evidenziare come una combinazione di social engineering e tecniche di raccolta dati OSINT possa essere utilizzata per realizzare un attacco di phishing efficace e mirato. L'esercizio vuole fornire esempi concreti di:

- Raccolta di informazioni di base tramite i social media e fonti aperte.

- Costruzione di attacchi di phishing realistici basati su queste informazioni.

- rubare le credenziali di accesso alla piattaforma dell’assicurazione e dati della carta di credito dopo che effettuato il pagamento

Questa simulazione è finalizzata a rafforzare la consapevolezza dei rischi derivanti dalla condivisione di dati personali sui social media e a migliorare la formazione degli utenti nel riconoscere potenziali tentativi di phishing.

EMAIL DI PHISHING

Oggetto: Attenzione: URGENTE! Scadenza imminente della Sua Polizza Auto [Zurich]

Mittente (simulato): assistenza-cliente@zuriich-italia.com

Contenuto dell'email:

Gentile Cliente,

La Sua polizza auto con targa [inserisci t arga vista dalla foto] scade tra pochi giorni! E’ necessario completare il rinnovo per evitare problemi con la copertura assicurativa.

ATTENZIONE: Se non effettua il pagamento entro [inserire data di scadenza], i Suoi vantaggi assicurativi potrebbero essere sospesi. Agisca subito!

Per rinnovare la polizza, clicchi qui: [sito clonato da noi 🡪 Accedi ora alla tua area personale ]

Nota Bene: Per assistenza immediata, risponda a questa email con i suoi dati.

Cordiali saluti,

Zurich Assicurazioni Italia Servizio Clienti

assistenza-cliente@zuriich-italia.com

SPIEGARE LO SCENARIO

Caratteristiche di Phishing Incorporate

1. Indirizzo Email Sospetto: L'indirizzo simula quello reale, ma ha una piccola modifica ("zuriich" anziché "zurich"), cosa comune negli attacchi.

2. Richiesta Urgente: L'email spinge l'utente ad agire subito, creando fretta e senso di necessità.

3. Link Fraudolento: Il link "Accedi ora alla tua area personale" potrebbe puntare a un sito falso. Si può istruire l'utente a passare sopra il link per controllare l'URL senza cliccare.

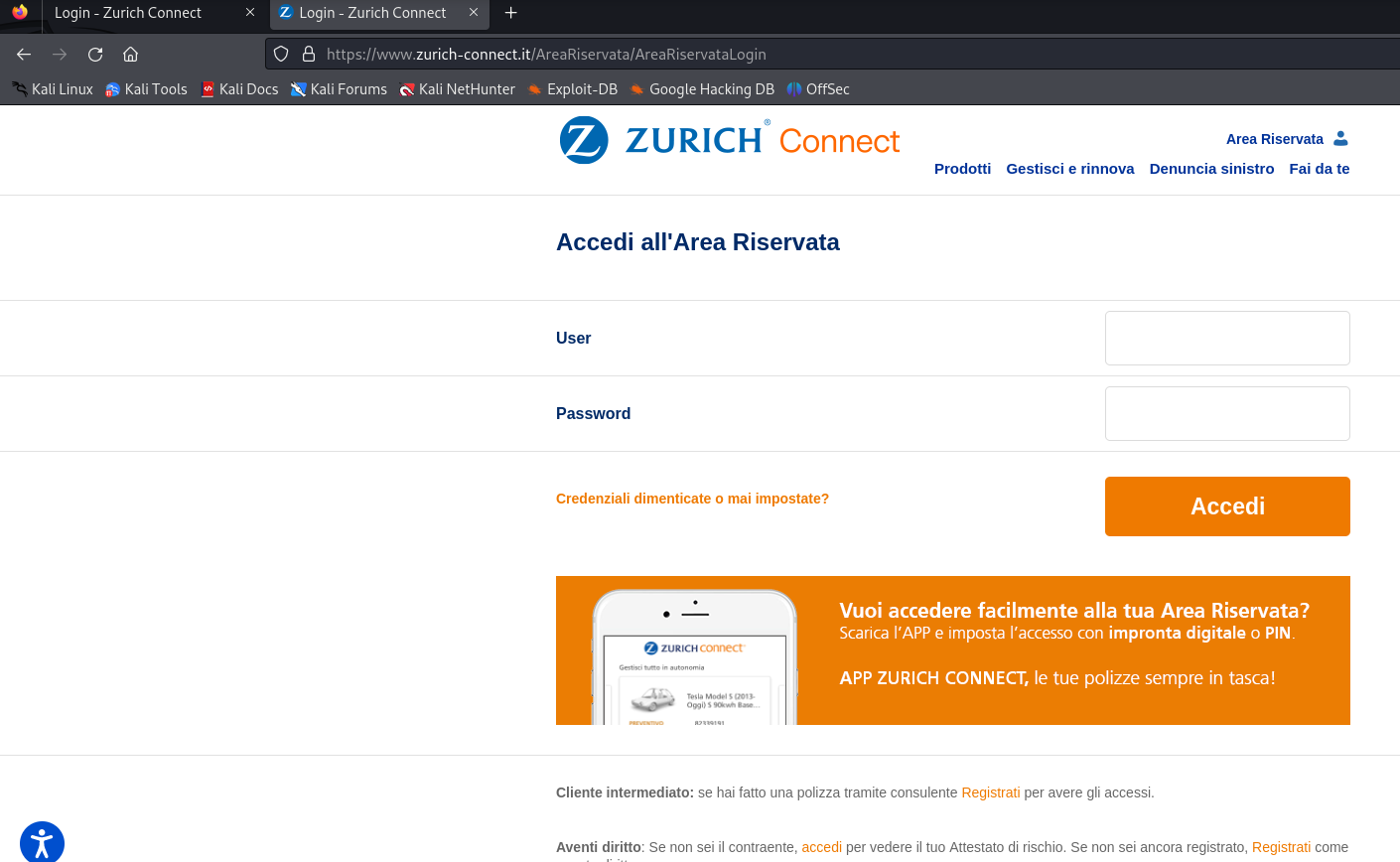
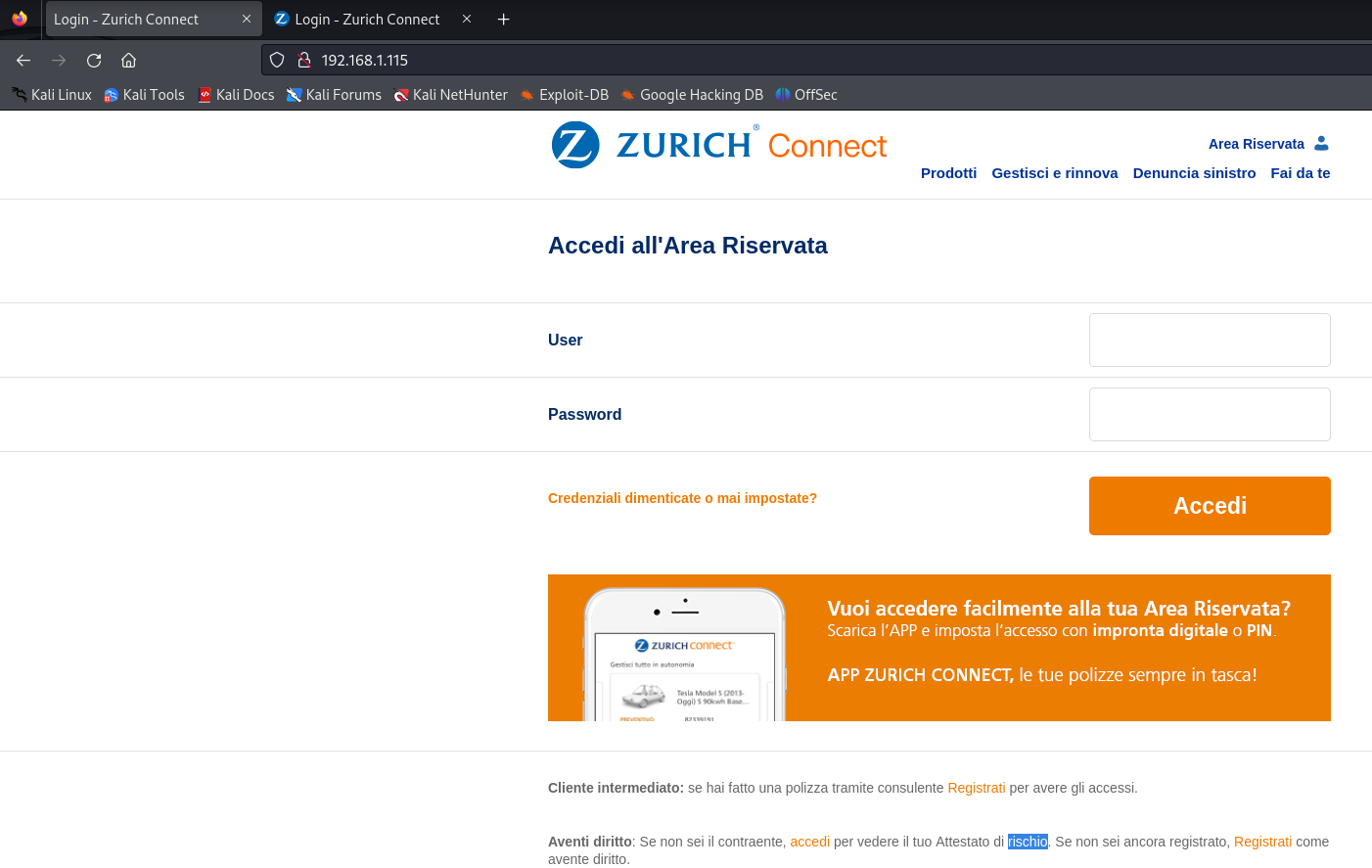
4. Errori e Formattazione: Leggere l'email attentamente potrebbe rivelare errori minimi di grammatica o di formattazione insolita.

Questi dettagli aiutano gli utenti a riconoscere le email sospette, insegnando loro come individuare caratteristiche tipiche del phishing e a non fornire informazioni sensibili tramite link o risposte non verificate.

L’email sembrerà convincente alla vittima perché effettivamente in questo contesto alla vittima sta per scadere l’assicurazione e viene inviata un’ emial dalla sua assicurazione dove riporta i suoi dati.

La vittima una volta cliccato sul sito vedendo che il sito effettivamente è quello giusto inserirà i suoi dati non sapendo che si tratta di un sito clonato.

DIFFERANZA SITO REALE E SITO CLONATO



Con kali partendo dal comando “ sudo setoolkit “ possiamo arrivare a clonare la pagina desiderata e vedere in chiaro i dati messi dalla vittima.