Relazione: Progetto di Simulazione Phishing

Corso: Cyber Security & Ethical Hacking **Tool:** GoPhish (Kali Linux) & Mailtrap (SMTP Sandbox)

Parte 1: Progettazione dello Scenario (Teoria)

1. Contesto e Obiettivo

- **Contesto:** Un "Avviso di Sicurezza Microsoft 365". Questo scenario è stato scelto perché sfrutta la leva psicologica della **paura** e dell'**urgenza** in un contesto realistico. I dipendenti sono condizionati a reagire immediatamente agli avvisi di "accesso non autorizzato" per proteggere i dati aziendali.
- **Obiettivo: Credential Harvesting** (Furto di Credenziali). L'obiettivo è ingannare l'utente affinché clicchi su un link e inserisca le proprie credenziali aziendali (email e password) su un portale fraudolento.

2. Contenuto dell'Email di Phishing

L'email è stata progettata utilizzando Gemini e raffinata per includere indicatori tipici di phishing mescolati a elementi di autorità convincenti.

- **Oggetto:** ACTION REQUIRED: Microsoft 365 Security Alert - Unusual Sign-in Activity
- **Mittente:** Microsoft Security Team `<security-alert@mircosoft-onIine.com>`
    - *Nota sulla tecnica di spoofing:* È stato utilizzato un sottile errore di battitura (`mircosoft`) e una sostituzione di caratteri (`I` maiuscola invece di `l` in "online") per impersonare il dominio ufficiale.
- **Dettagli dello Scenario:** L'email segnala un tentativo di accesso da **Lagos, Nigeria** (IP: 102.12.33.11) per forzare una reazione immediata di "verifica account".

3. Analisi della Credibilità vs Campanelli d'Allarme

- **Elementi Credibili:** Schema colori ufficiale, terminologia tecnica ("Unusual sign-in activity") e dettagli specifici (IP, Posizione, Piattaforma) che rendono l'email convincente.
- **Campanelli d'Allarme (Red Flags):**

- **Urgenza:** La dicitura "Action Required" implica conseguenze negative se ignorata.
- **Destinazione del Link:** Il pulsante reindirizza a un URL non Microsoft (il nostro server di simulazione).
- **Dominio Spoofato:** L'indirizzo del mittente non è `@microsoft.com`.

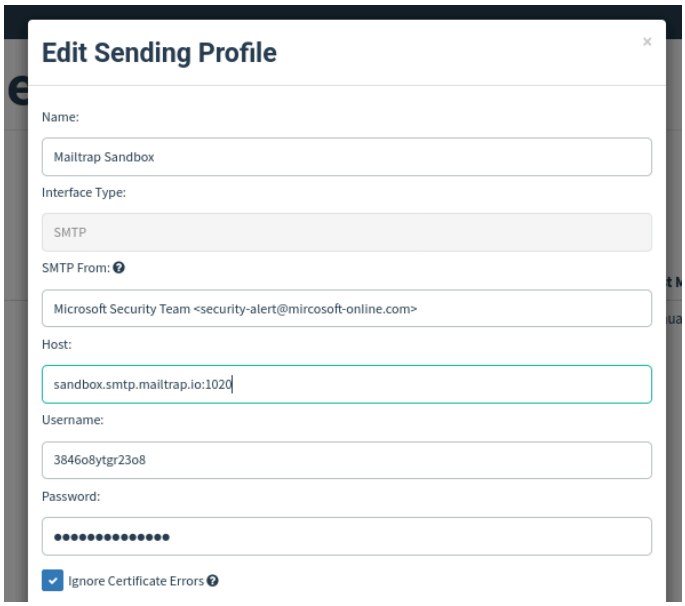
Parte 2: Implementazione Tecnica (Pratica)

Per questa simulazione, abbiamo implementato il framework **GoPhish** su **Kali Linux**. Per garantire la sicurezza etica ed evitare filtri antispam reali durante i test, abbiamo utilizzato **Mailtrap** come Sandbox SMTP.

Step 1: Configurazione Infrastruttura (Sending Profile)

Abbiamo configurato un "Sending Profile" per agire come server di posta.

- **Strumento:** Mailtrap (SMTP Sandbox).
- **Configurazione:** Ci siamo autenticati usando le credenziali di Mailtrap, ma abbiamo impostato l'"Envelope Sender" con il nostro indirizzo Microsoft spoofato. Questo dimostra come gli attaccanti possano mascherare la propria identità pur utilizzando servizi di relay legittimi.

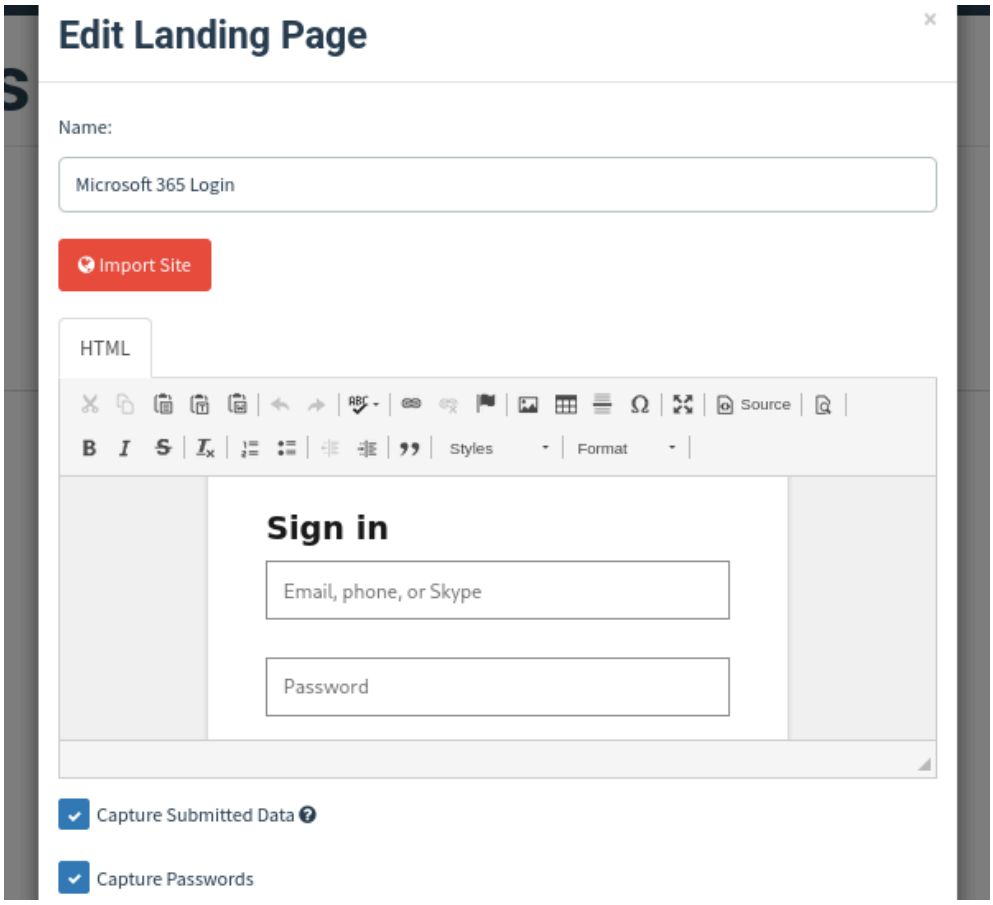


Didascalia: Configurazione del profilo SMTP in GoPhish con credenziali Mailtrap e mittente spoofato "Microsoft Security Team".

Step 2: La "Trappola" (Landing Page)

Abbiamo creato un clone della pagina di login Microsoft.

- **Dettaglio Tecnico:** Abbiamo utilizzato un template HTML statico con l'attributo `action` del form che punta a GoPhish. Questo permette al server di catturare username e password prima di reindirizzare la vittima al vero sito Microsoft (`https://www.microsoft.com`).
- **Impostazioni Chiave:** Abilitate "Capture Submitted Data" e "Capture Passwords".

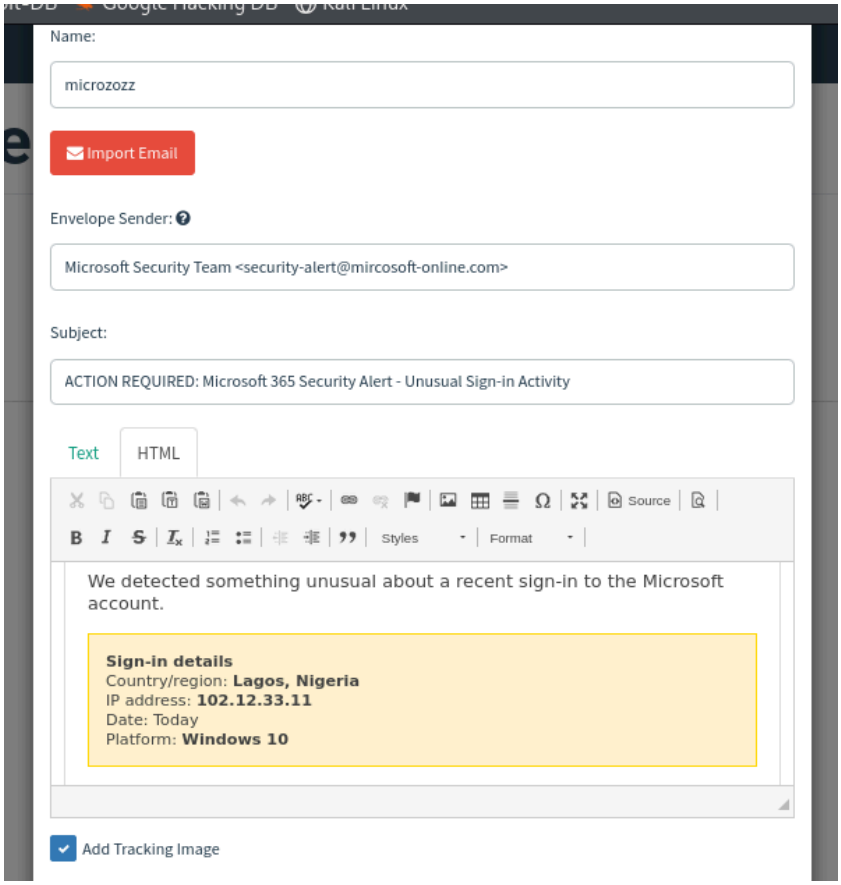


Didascalia: Configurazione della Landing Page per catturare le credenziali e reindirizzare al sito reale.

Step 3: L'"Esca" (Email Template)

Abbiamo implementato l'email HTML progettata nella Fase 1.

- **Tracciamento:** Il pulsante "Review recent activity" è stato configurato con il tag `{{.URL}}`. GoPhish sostituisce automaticamente questo tag con un link di tracciamento univoco per ogni vittima.

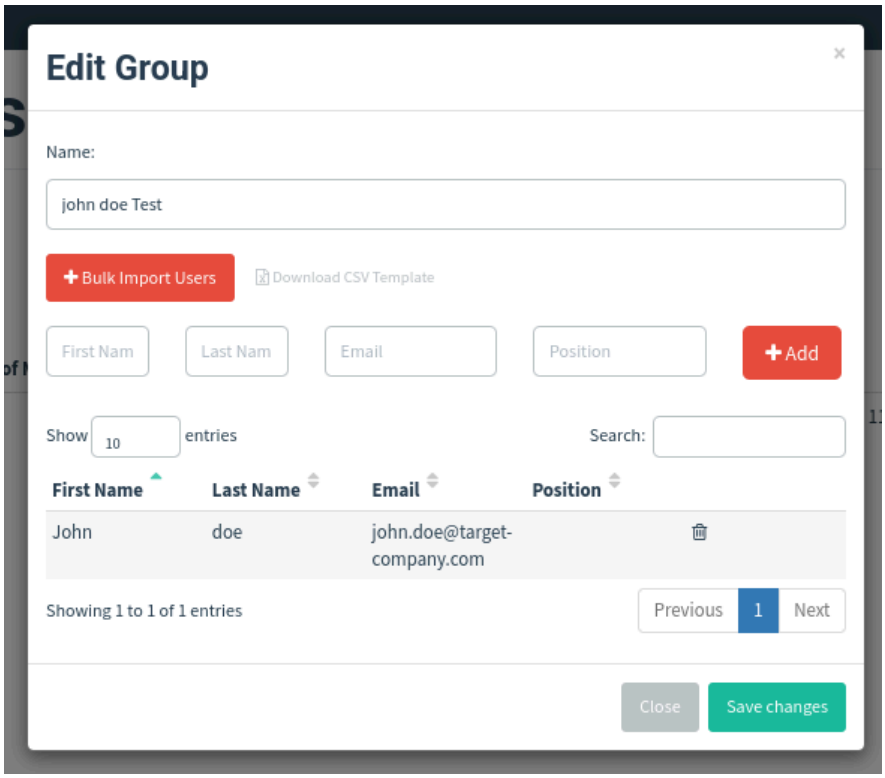


Didascalia: Il template email HTML con il contesto dell'avviso di sicurezza da "Lagos, Nigeria".

Step 4: Il Bersaglio (Users & Groups)

Abbiamo creato un gruppo target simulato.

- **Bersaglio:** "John Doe" (`john.doe@target-company.com`).
- **Scopo:** Dimostrare come apparirà l'header dell'email alla vittima.

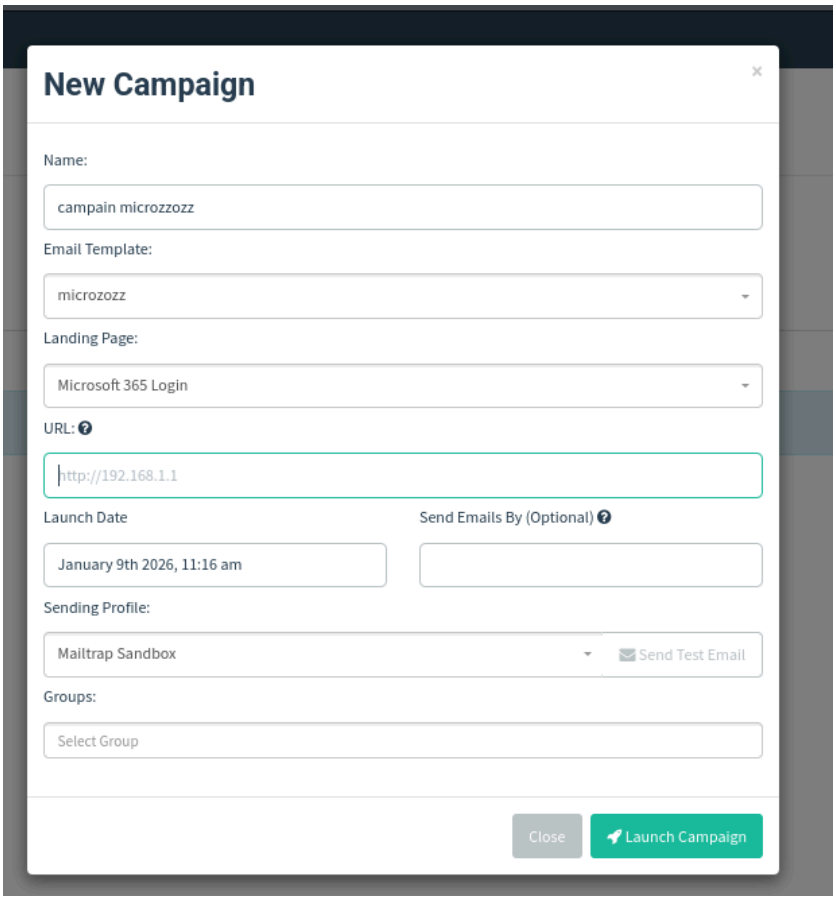


Didascalia: Definizione della lista dei bersagli per la campagna.

Step 5: Lancio della Campagna

Abbiamo collegato tutti i componenti in una Campagna.

- **Configurazione URL:** L'URL di ascolto è stato impostato sull'indirizzo IP di Kali Linux, assicurando che il browser della vittima potesse raggiungere il server GoPhish.

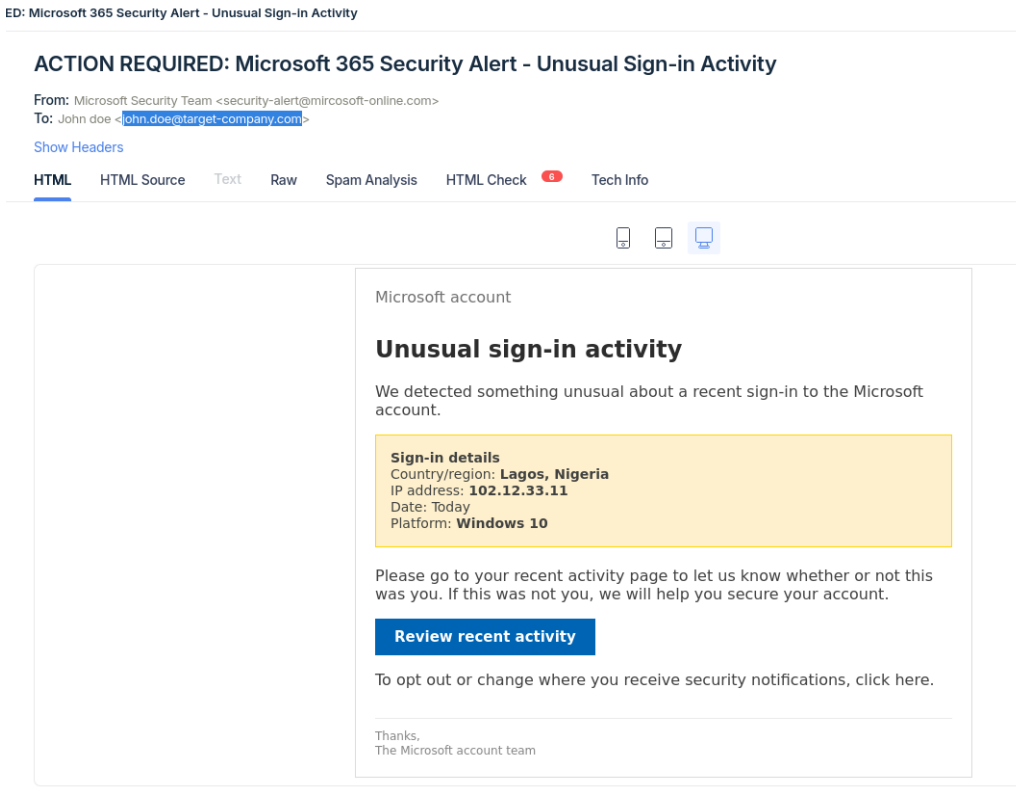


Didascalia: Configurazione finale della Campagna che collega Template, Landing Page e Profilo.

Parte 3: Proof of Concept (PoC) e Risultati

1. La Consegna (Vista Vittima)

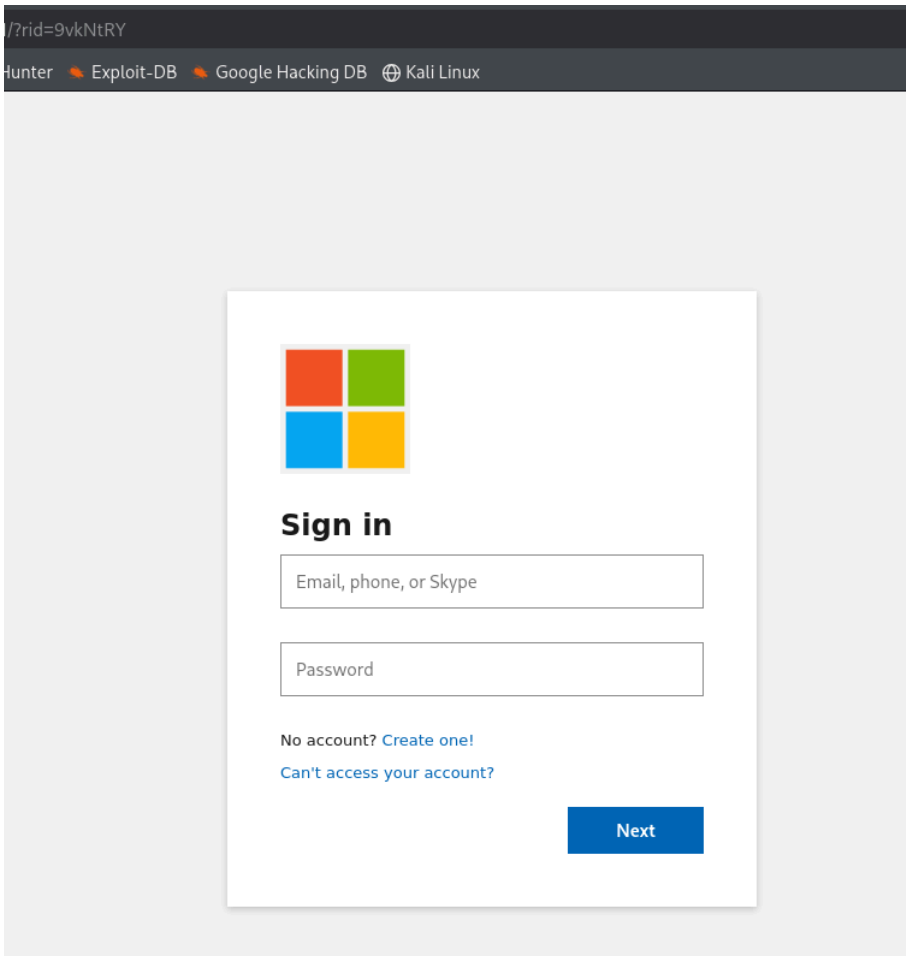
L'email è arrivata istantaneamente nella sandbox di Mailtrap. Lo spoofing ha avuto successo; il mittente appare come "Microsoft Security Team" e il layout rispecchia le notifiche ufficiali.



Didascalia: L'email di phishing vista nella casella di posta della vittima (Mailtrap Sandbox).

2. L'Attacco (Il Sito Falso)

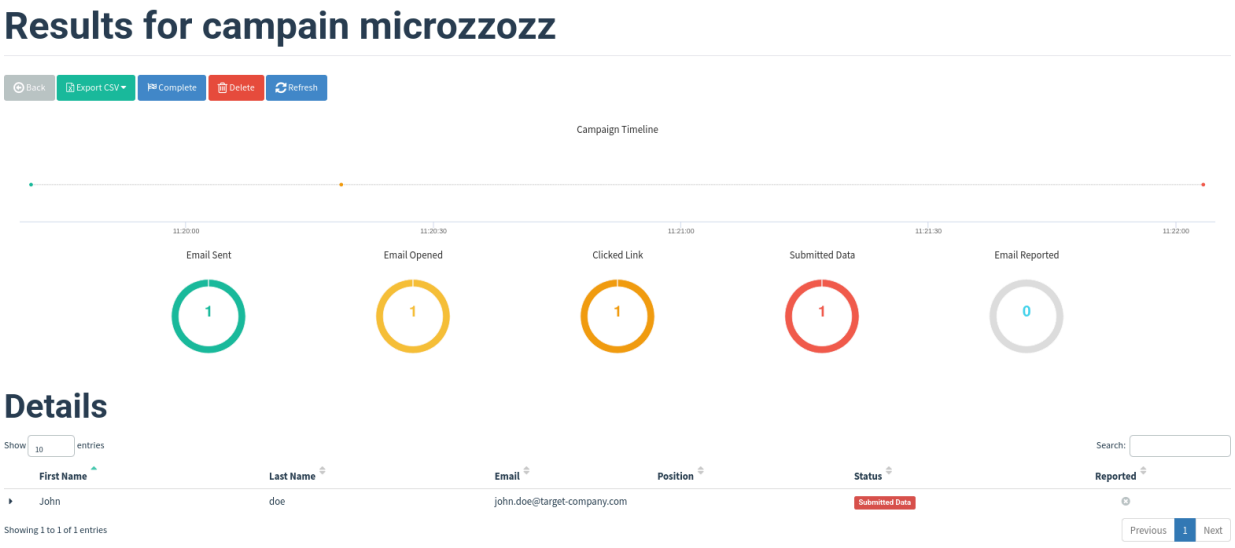
Cliccando sul link, il browser è stato reindirizzato al nostro server Kali Linux che ospita la pagina di login falsa. Visivamente, è indistinguibile dalla pagina di accesso standard.



Didascalia: La pagina di login fraudolenta ospitata da GoPhish.

3. La Cattura (Analisi)

Dopo che la "vittima" ha inserito le credenziali e cliccato su "Next", GoPhish ha catturato con successo i dati. La dashboard mostra il ciclo di vita completo dell'attacco: **Email Inviata -> Email Aperta -> Link Cliccato -> Dati Inviati**.



Didascalia: Dashboard di GoPhish che mostra il successo del furto di credenziali ("Submitted Data").

Metodologia di Svolgimento e Supporto AI

Per lo svolgimento di questo esercizio, ho adottato un approccio di "Apprendimento Assistito" utilizzando una **Gem personalizzata** su piattaforma Gemini.

1. Il Ruolo del Tutor AI (Master Prompt) Ho attivato l'assistente tramite un **Master Prompt** specifico progettato per simulare un **Cybersecurity Tutor** dedicato. Il prompt istruiva l'AI a:

- Agire come esperto di sicurezza informatica focalizzato su sistemi **Linux (Ubuntu/Kali)**.
- Fornire istruzioni basate esclusivamente su documentazione ufficiale e best practice di sicurezza.
- Guidare passo dopo passo nella configurazione degli strumenti (GoPhish) e nel troubleshooting, evitando soluzioni pre-confezionate senza spiegazione.

2. Flusso della Collaborazione Il progetto si è sviluppato attraverso una conversazione interattiva strutturata in fasi logiche:

- **Analisi dell'Assignment:** Abbiamo analizzato il PDF fornito per estrapolare i requisiti chiave (creazione scenario, email convincente, analisi tecnica).
- **Definizione dello Scenario:** Insieme al Tutor, abbiamo selezionato il contesto "Microsoft 365 Security Alert" poiché ritenuto uno dei vettori più efficaci per il phishing aziendale.
- **Risoluzione Tecnica (Problem Solving):**
    - Durante la configurazione della **Landing Page**, abbiamo riscontrato che il codice originale Microsoft era dinamico (Javascript) e non catturabile da GoPhish. Il Tutor mi ha guidato nella creazione di una **replica statica HTML/CSS** (il codice "Trap") funzionante per il laboratorio.
    - Per l'invio delle email, abbiamo configurato insieme **Mailtrap** come server SMTP simulato, permettendo di bypassare i controlli SPF e visualizzare correttamente il mittente spoofato (`@mircosoft-onIine.com`) senza rischi reali.
- **Verifica Finale:** Attraverso domande dirette e screenshot di feedback, abbiamo validato ogni passaggio (dal template email alla configurazione dell'IP di Kali) fino al successo della campagna.

Conclusione

Questo esercizio ha dimostrato il ciclo di vita completo di un attacco di phishing. Utilizzando **GoPhish**, abbiamo automatizzato con successo la distribuzione e il tracciamento dell'attacco. L'uso di **Mailtrap** ha dimostrato che i controlli tecnici (come SPF) possono essere bypassati in un ambiente di test, e l'autenticità visiva dell'email e della landing page sottolinea l'importanza della formazione degli utenti (es. controllo degli URL e dei domini mittente) per prevenire il furto di credenziali.