Task 06/12/24: Simulazione di un'email di Phishing

Traccia

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

Task 06/12/24: Simulazione di un'email di Phishing

Sviluppo della traccia

1. Obiettivo del progetto

A. Creare una simulazione realistica di un'email di phishing utilizzando **Gophish**, con l'obiettivo di sensibilizzare e formare le persone sui rischi delle minacce informatiche.
B. Evidenziare i principali segnali di phishing, come errori grammaticali, domini falsi e richieste urgenti.
C. Analizzare il comportamento dei destinatari in un ambiente controllato per migliorare la loro consapevolezza e sicurezza online.

2. Scenario creato

Contesto:

L'esercitazione si basa su un'email di phishing che simula una comunicazione ufficiale da parte di **Disney+**. L'email informa l'utente di un problema con il pagamento del proprio abbonamento e richiede un'azione immediata per evitare la sospensione del servizio.

Obiettivo del phishing:

- Indurre la vittima a cliccare su un link fraudolento.
- Simulare la raccolta di credenziali o dati personali (senza mai salvarli).

Motivazione della scelta:

Disney+ è un servizio popolare e altamente riconoscibile, il che rende l'esercitazione più realistica e pertinente. Il problema del pagamento è una scusa comune nei veri attacchi di phishing.

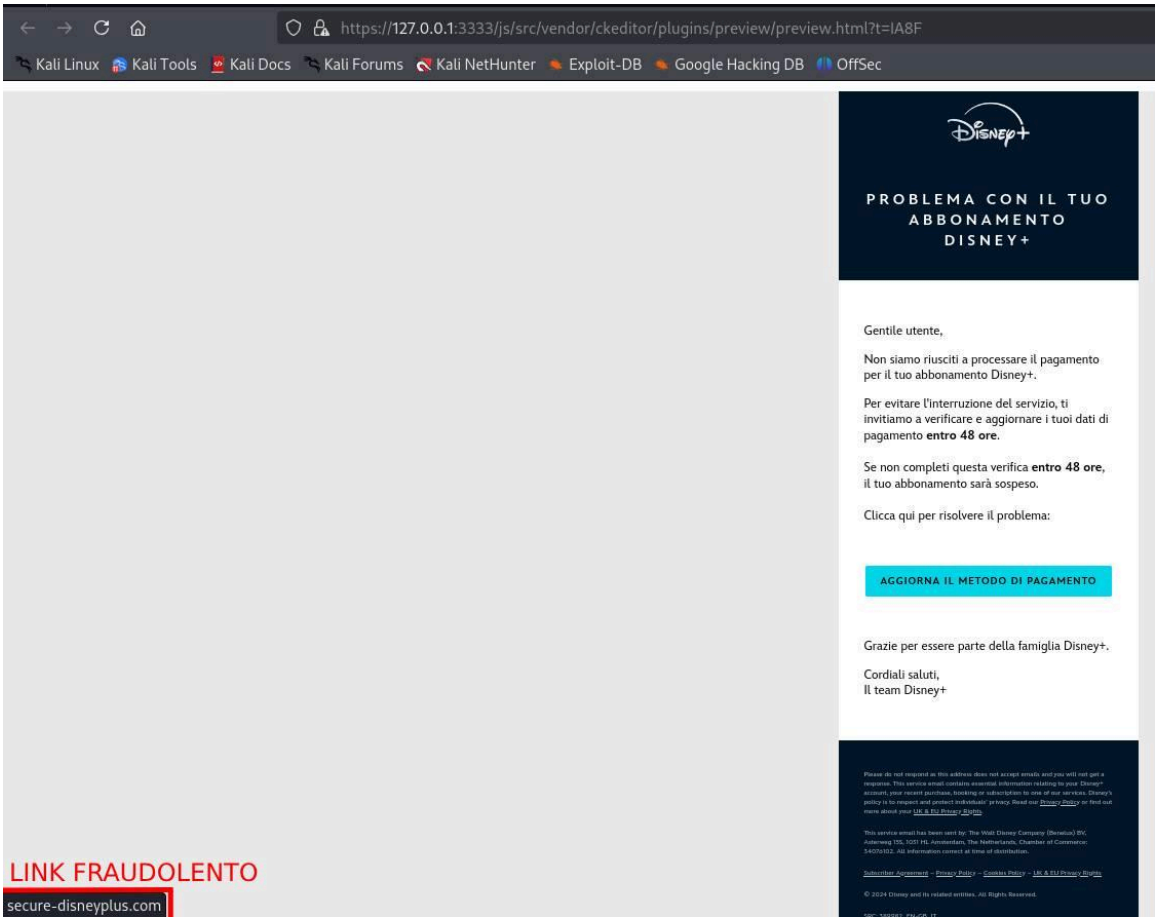
3. Contenuto dell'email di phishing

Oggetto:
Avviso urgente: Problema con il tuo abbonamento Disney+

Mittente:
noreply@secure-disneyplus.com

Corpo del messaggio:

```
Gentile utente,


Non siamo riusciti a processare il pagamento per il tuo abbonamento Disney+. Per evitare l'interruzione del
servizio, ti invitiamo a verificare e aggiornare i tuoi dati di pagamento entro 48 ore.


Clicca qui per risolvere il problema: [Aggiorna il metodo di pagamento](http://secure-disneyplus.com)


Se non completi questa verifica entro 48 ore, il tuo abbonamento sarà sospeso.


Grazie per essere parte della famiglia Disney+.

Cordiali saluti,

Il team Disney+
```



4. Elementi che rendono l'email sospetta

Assenza di dettagli personali:
L'email si rivolge in modo generico con "Gentile utente".

Errori grammaticali e di battitura:
"Processare il pagamento" è una traduzione poco fluida.

Dominio falso:
Il link fraudolento utilizza il dominio `secure-disneyplus.com`, che non è quello ufficiale di Disney+.

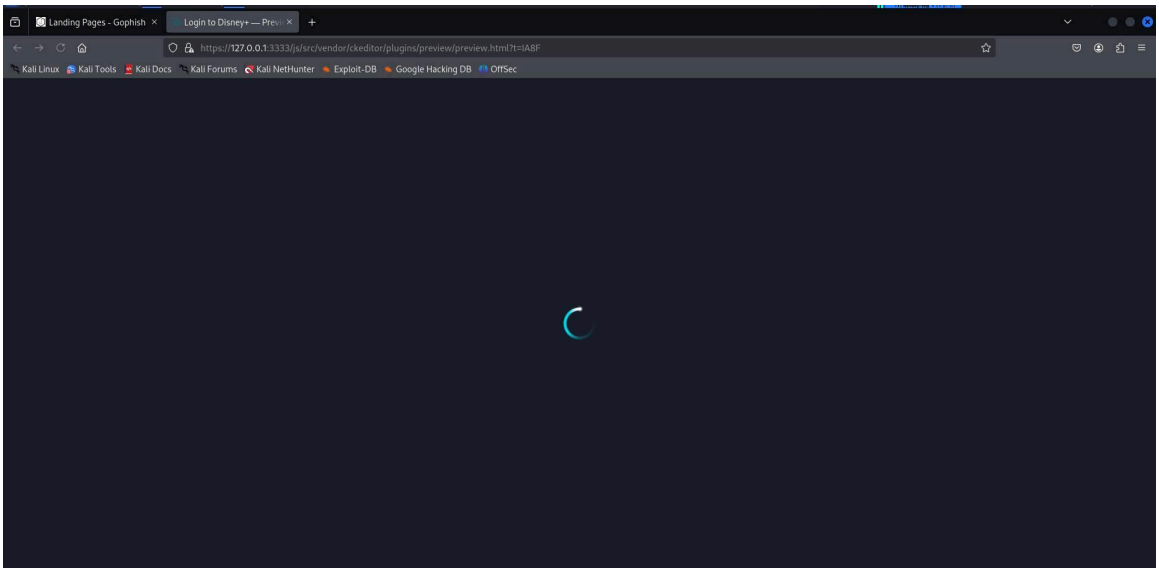
Senso di urgenza:
Frasi come "entro 48 ore" creano pressione psicologica sulla vittima.

Link sospetto:
Passando il mouse sul link, si nota che il dominio non corrisponde a quello ufficiale.

5. Landing Page simulata

La landing page riproduce fedelmente la schermata di login di Disney+, includendo:

- Logo e design simile all'originale.
- Campi per email e password.
- Un messaggio generico mostrato dopo l'inserimento dei dati: "Errore nel login! Riprova più tardi."



6. Strumenti utilizzati

I. **Gophish:**
   A. Per creare e gestire l'invio delle email di phishing.
   B. Per monitorare i tassi di apertura, clic sui link e interazioni con la landing page.
II. **HTML personalizzato:**
   A. Per creare la landing page simulata.
III. **Server SMTP simulato:**
   A. Per inviare le email senza utilizzare un provider reale, garantendo la sicurezza dell'ambiente.

7. Risultati attesi

Destinatari formati:
I partecipanti imparano a riconoscere i segnali di phishing nell'email.

Analisi comportamentale:
Dati raccolti in modo anonimo per valutare quanti utenti:

A. Aprono l’email.
B. Cliccano sul link.
C. Inseriscono informazioni nella landing page (simulata).

Miglioramento della consapevolezza:
Dopo l'esercitazione, i destinatari saranno in grado di identificare email sospette in futuro.

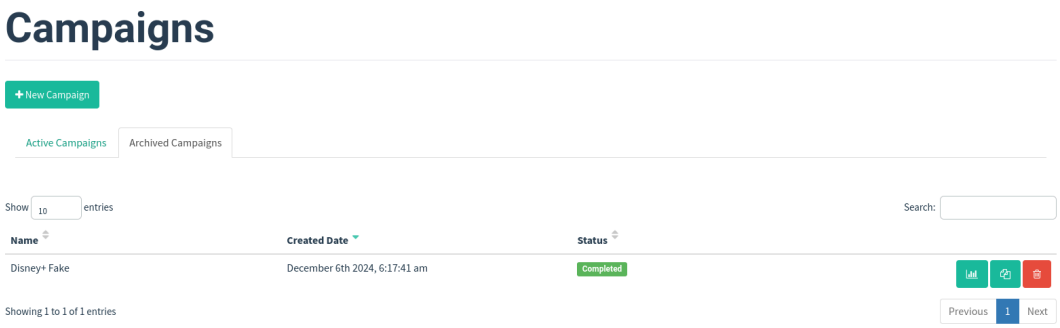
8. Conclusioni

Questo progetto dimostra come una simulazione ben progettata possa aumentare la consapevolezza sulle minacce di phishing. Con strumenti come Gophish, è possibile creare esercitazioni pratiche e coinvolgenti, rispettando sempre le norme etiche e la sicurezza dei partecipanti.

Relazione Tecnica

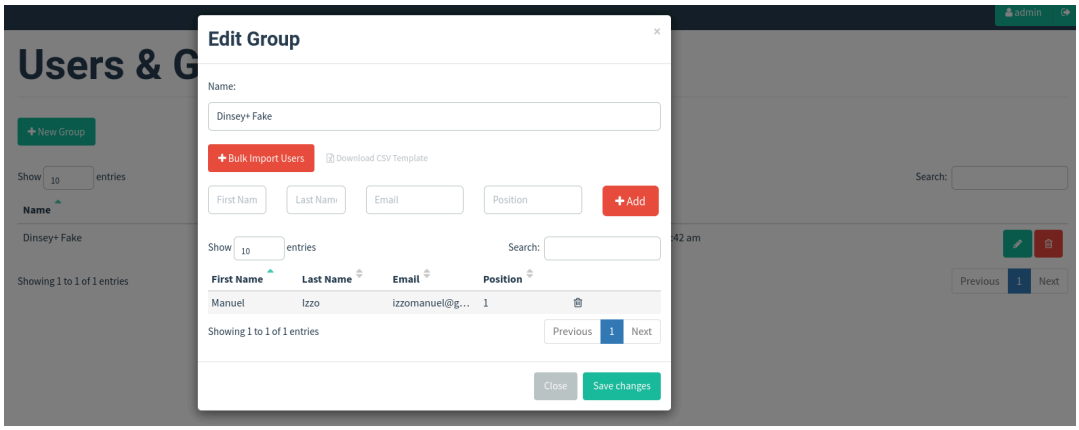
1. Configurazione della Campagna

La campagna è stata configurata per inviare un'email simulata a un gruppo di destinatari test. L'obiettivo era indurre i destinatari a cliccare su un link fraudolento e raccogliere dati statistici sulle loro azioni.



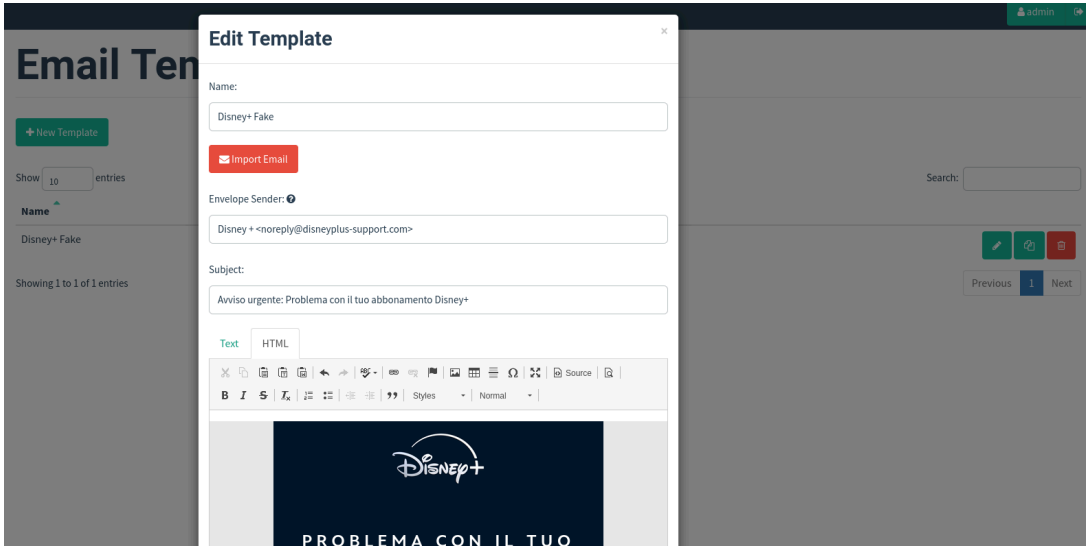
2. Configurazione del Gruppo di Destinatari

Il gruppo di destinatari è stato configurato con indirizzi email di test. Ogni utente è stato inserito manualmente per garantire un controllo completo sulla simulazione.



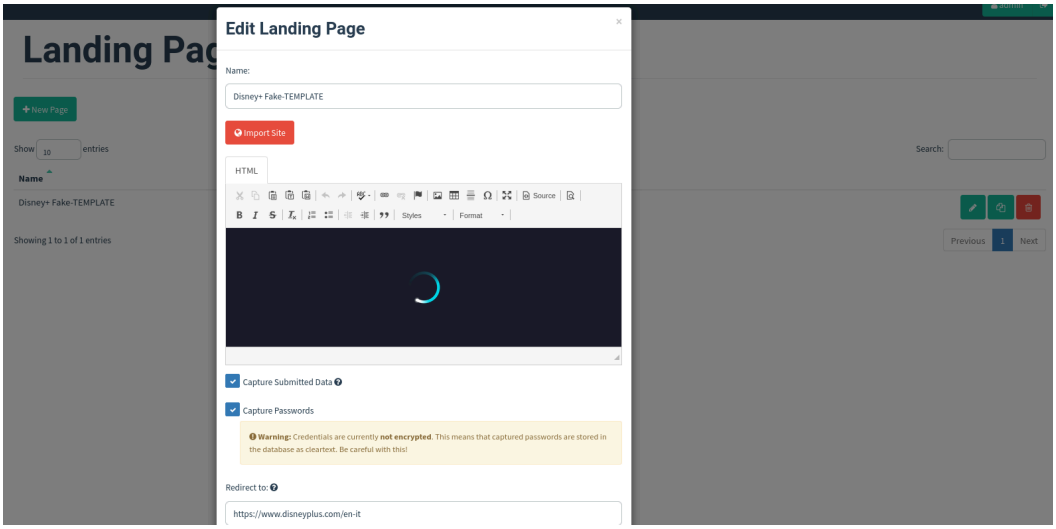
3. Creazione del Template Email

È stato creato un template email che riproduce una tipica comunicazione di Disney+, includendo elementi come un logo, un oggetto accattivante e un link fraudolento per aggiornare il metodo di pagamento.



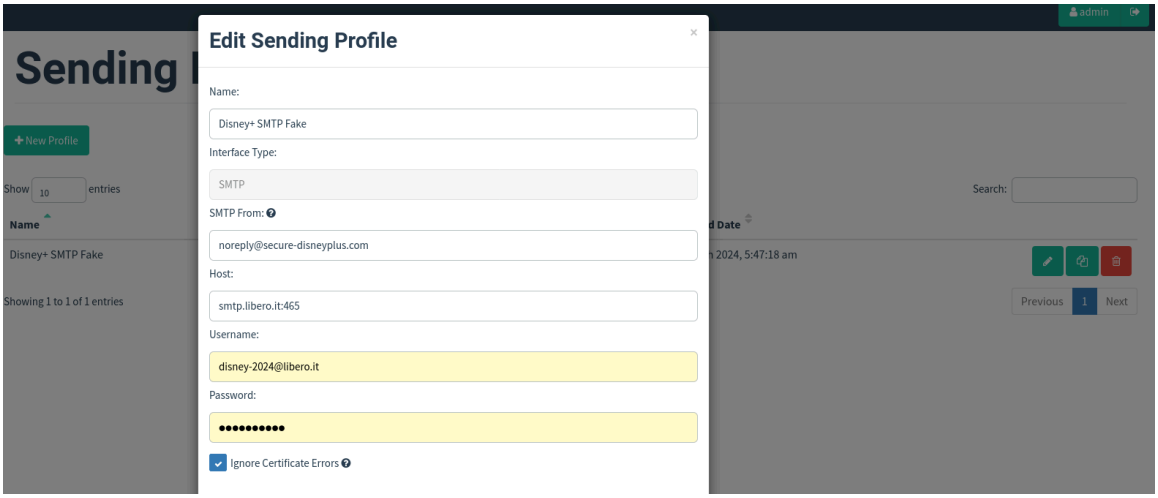
4. Configurazione della Landing Page

La landing page è stata progettata per simulare la schermata di login di Disney+. Quando l'utente tenta di inserire i propri dati, questi non vengono salvati, ma la simulazione termina mostrando un errore generico.



5. Configurazione del Profilo di Invio

È stato configurato un profilo SMTP per l'invio delle email. Il profilo utilizza un server simulato per garantire la sicurezza dell'ambiente di test.



6. Conclusioni

La campagna ha fornito dati utili su come i destinatari interagiscono con le email di phishing. Questi dati possono essere utilizzati per sviluppare ulteriori strategie di formazione e sensibilizzazione.