In questo esercizio andrò a simulare una mail di phishing.
Utilizzerò una macchina Kali Linux, SET (Social-Engineer Toolkit) e chatGPT come strumenti per creare e cercare.

Immaginiamo uno scenario comune in cui l'email di phishing sembra provenire dal servizio clienti delle Poste Italiane. Questa mail avvisa la vittima di una "attività sospetta" sul proprio account e richiede un'azione urgente per proteggere le finanze. Il finto mittente (le PI) chiede alla vittima di accedere a un link per "verificare le proprie credenziali". Questo link porta a un sito falso creato per raccogliere username e password.

Obiettivo del phishing: Raccogliere le credenziali di accesso dell'utente per poi accedere al suo conto PI.
La mail si presenta così:

Oggetto: ⚠ Attenzione: Attività Sospetta sul Suo Conto Poste Italiane ⚠

Da: Servizio Clienti supporto@postinaitliana-verifica.com

Corpo dell'email:

Gentile Cliente,

Abbiamo notato un'attività sospetta sul Suo conto Poste Italiane e, per proteggere la Sua sicurezza, abbiamo temporaneamente limitato l'accesso fino a che non sarà confermata la Sua identità. **È molto importante che Lei verifichi le Sue credenziali entro 24 ore** per evitare ulteriori limitazioni.

Per favore, clicchi sul link sottostante per accedere alla Sua area personale e completare la verifica:

Verifica le Tue Credenziali Qui

Attenzione: Se non verificherà il Suo account entro 24 ore, sarà necessario sospendere l'accesso per garantire la sicurezza dei Suoi fondi.

Se ha domande, non esiti a contattarci. La ringraziamo per la collaborazione.

Cordiali saluti,
Servizio Clienti
Postino Italiane

Nota: Questa email è stata inviata automaticamente. Si prega di non rispondere a questo messaggio.

N.B. Ho inserito nel corpo della mail il link del sito che ho clonato, http://web.archive.org/web/20171108213739/https://securelogin.poste.it/jod-fcc/fcc-authentication.html, l'intento è quello di simulare un attacco realistico, ma per la correzione dell'esercizio ho inserito l'url che ho scelto di clonare

Poste Italiane

⚠️ Attenzione: Attività Sospetta sul Suo Conto Poste Italiane ⚠️

Gentile Cliente,

Abbiamo notato un'attività sospetta sul Suo conto Poste Italiane e, per proteggere la Sua sicurezza, abbiamo temporaneamente limitato l'accesso fino a che non sarà confermata la Sua identità. È molto importante che Lei verifichi le Sue credenziali entro 24 ore per evitare ulteriori limitazioni.

Per favore, clicchi sul link sottostante per accedere alla Sua area personale e completare la verifica:

Verifica le Tue Credenziali Qui

Attenzione: Se non verificherà il Suo account entro 24 ore, sarà necessario sospendere l'accesso per garantire la sicurezza dei Suoi fondi.

Se ha domande, non esiti a contattarci. La ringraziamo per la collaborazione.

Cordiali saluti,
Servizio Clienti
Postino Italiane

Nota: Questa email è stata inviata automaticamente. Si prega di non rispondere a questo messaggio.

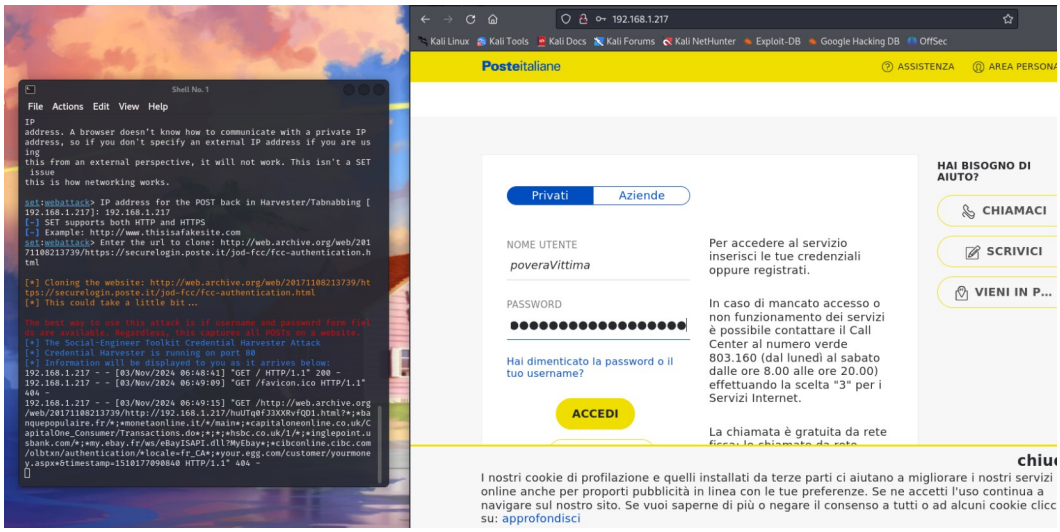
Ecco come dovrebbe essere visualizzata la mail dalla vittima

Spiegazione dello Scenario e Analisi dell'Email:

Mittente e contenuto realistico:
L'email sembra provenire da un indirizzo con il nome delle Poste Italiane e contiene un messaggio tipico di servizio clienti riguardante la sicurezza del conto.
Messaggio urgente:
L'email usa una frasi urgenti come "attività sospetta" e "24 ore per verificare le credenziali" che spinge la vittima a reagire subito senza pensarci troppo.
Rassicurazione e tono formale: La chiusura della mail è formale, cosa che le conferisce un'apparenza professionale.

Campanelli d'allarme:
Errore nel dominio dell'indirizzo email:
L'indirizzo email non è quello ufficiale della Poste; invece, utilizza un dominio simile, ma falso ("supporto@postinaitliana-verifica.com").
Link sospetto:
Il link "Verifica le Tue Credenziali Qui" punta a un sito che non è ufficiale, pur somigliando al sito della banca.
Urgenza e minaccia di blocco:
Questo tipo di pressione è tipica dei tentativi di phishing e dovrebbe allertare l'utente.
Assenza di personalizzazione:
L'email non menziona il nome del cliente, ma usa solo "Gentile Cliente,". Le comunicazioni ufficiali delle banche di solito personalizzano i messaggi.
Errori di scrittura: Si possono anche notare errori nel corpo della mail tra cui "Postino Italiane"

Se la vittima clicca sul link del sito clonato, viene indirizzata a una pagina che sembra simile al sito originale di accesso. Una volta sulla pagina, la vittima andrà a inserire le proprie credenziali di accesso e proverà il login. Una volta premuto accedi, i dati vengono inviati attraverso una richiesta POST al server di SET che cattura queste informazioni.



Nel terminale di SET, le credenziali inserite vengono stampate in tempo reale, permettendomi di raccogliere facilmente i dati sensibili della vittima