SIMULAZIONE DI PHISHING

Tramite prompt su ChatGPT ho chiesto di scrivermi una potenziale mail di phishing per poter intercettare i dati dell'account Facebook dell'azienda Theta S.p.a. Per farlo mi sono finto il supporto Facebook che richiede con urgenza di verificare il proprio account.

Di seguito il prompt e la mail generata da ChatGPT.

Gentile [Nome Cognome],

Recentemente abbiamo riscontrato attività insolite nell'account Facebook aziendale di *Theta SPA*. Per garantire la sicurezza del vostro profilo e proteggere le informazioni aziendali, è necessario completare una verifica dell'account entro le prossime 24 ore.

Ti preghiamo di accedere tramite il nostro **portale di verifica** e confermare le tue credenziali aziendali per evitare la sospensione temporanea dell'account.

> **Link di verifica dell'account:** www.facebook-verifica.com/ThetaSPA

Per completare la procedura, sarà sufficiente accedere con le tue credenziali aziendali di Facebook.
Se hai domande o hai bisogno di supporto, rispondi a questa email e il nostro team ti assisterà.

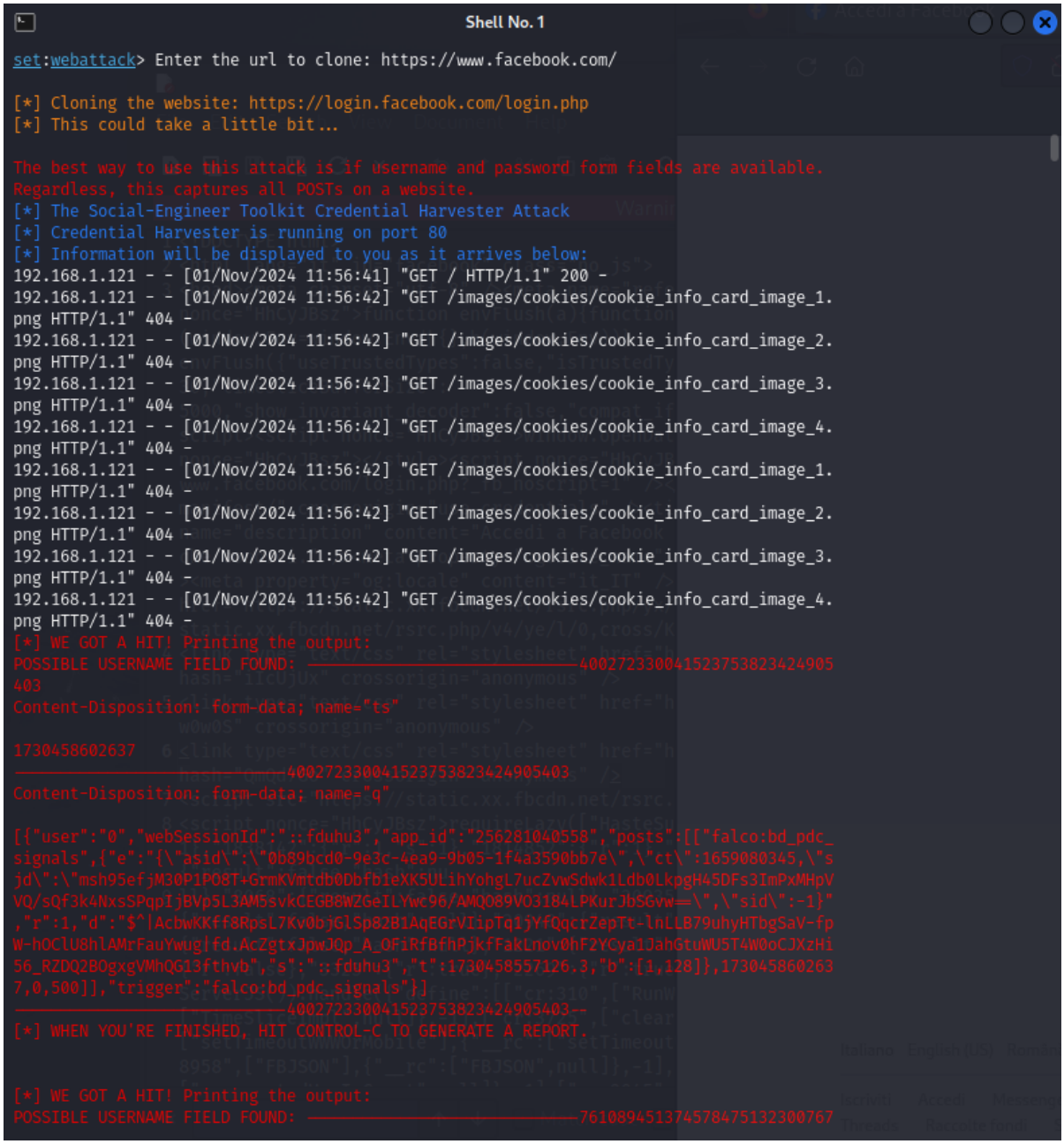
Grazie per la collaborazione.

Cordiali saluti,
Il Team di Assistenza Facebook

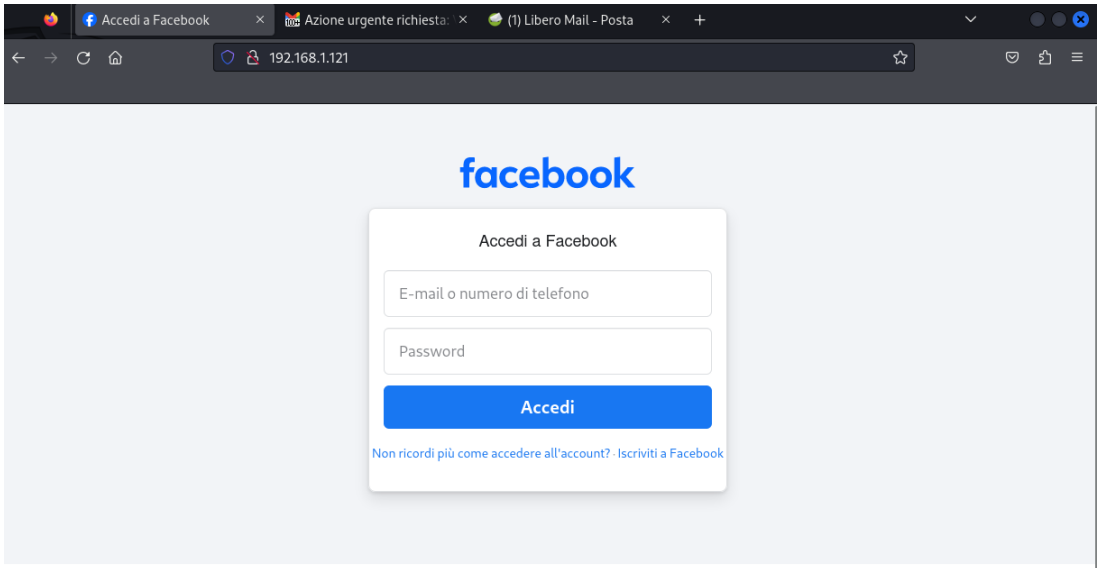
Una volta creata la mail iniziamo con la fase di clonazione della pagina di login di Facebook, utilizzato il tool di Kali SET, che è un software open-source scritto in python che offre diversi opzioni di attacco di ingegneria sociale.

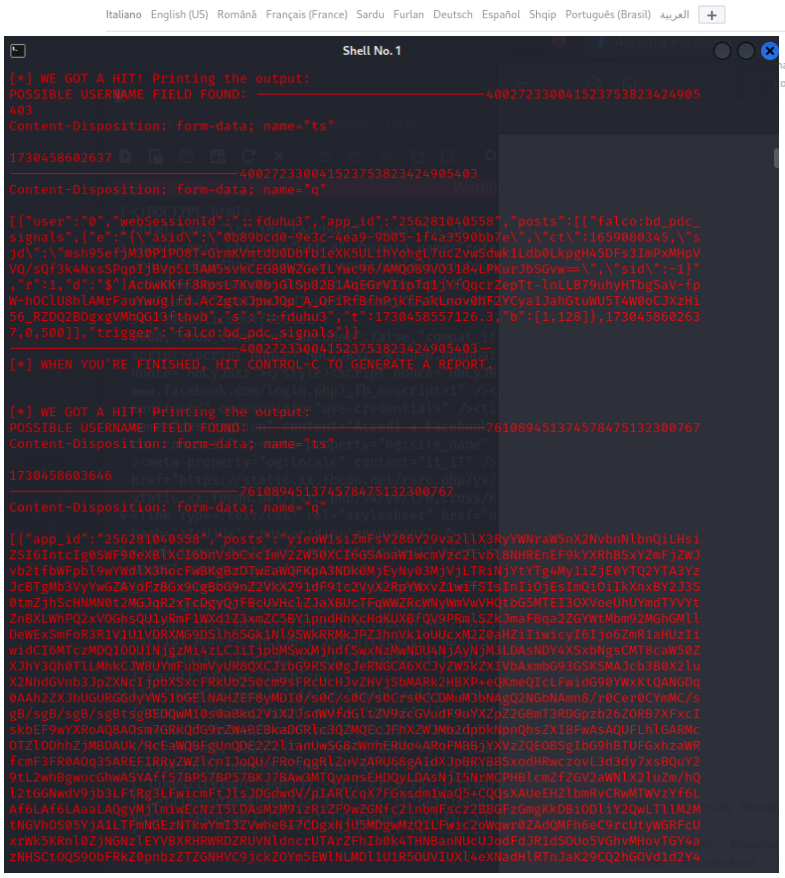
Per poter clonare la pagina di login, dal menù principale di SET selezioniamo: **Website Attack Vectors,** poi **Credential Harvester Attack Method** e infine **Site Clone.**

Impostiamo il nostro indirizzo IP e infine **SET** ci chiederà di inserire l'**URL** del sito da clonare, in questo caso inseriamo *www.facebook.com* , ci troveremo poi di fronte a questa schermata:



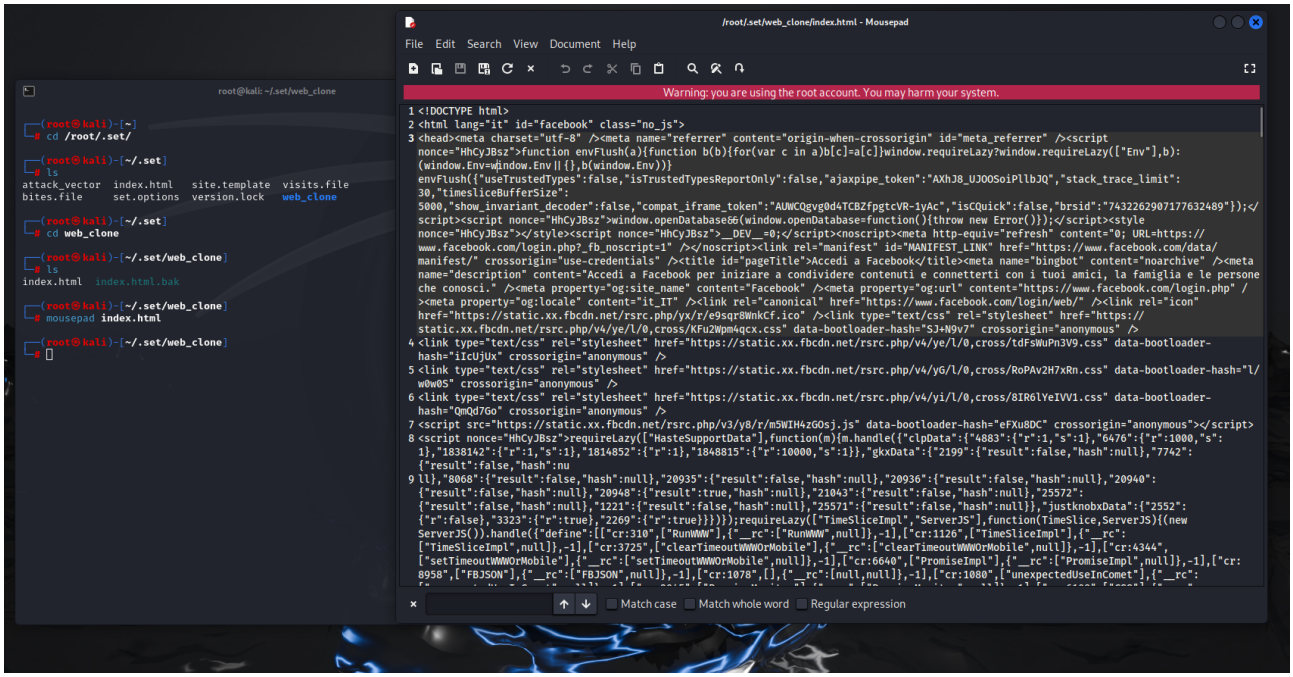
Dopo che SET ha finito la clonazione del sito, possiamo andare nel browser e digitare il nostro indirizzo IP (192.168.1.121) dove viene hostato il clone di Facebook come si vede dall'immagine seguente.



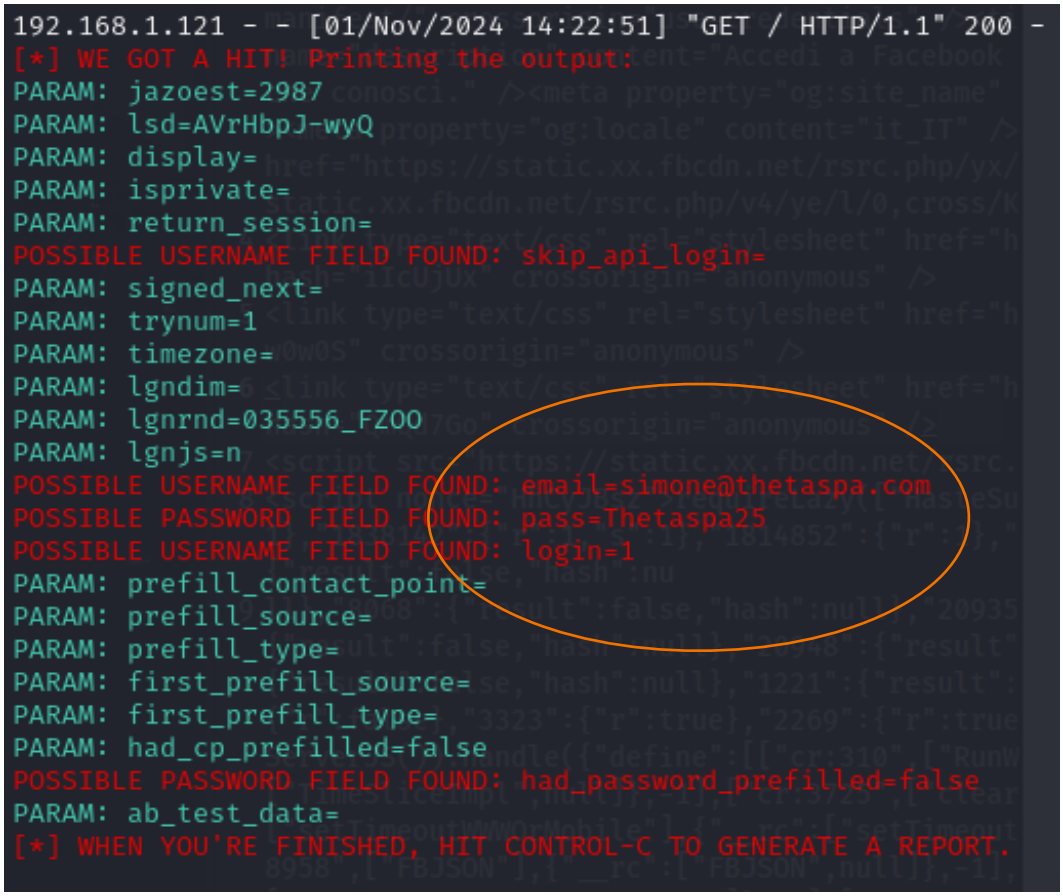


Ora se proviamo ad inserire le credenziali possiamo vedere come i dati inseriti non sono visibili in chiaro su SET, questo accade perchè all'interno del codice sorgente della pagina web sono presenti degli script BigPipe che non permette la visualizzazione in chiaro dei dati, è come se fosse un sistema di sicurezza che reindirizzano la pagina in HTTPS. Togliendoli visualizziamo la pagina in HTTP.

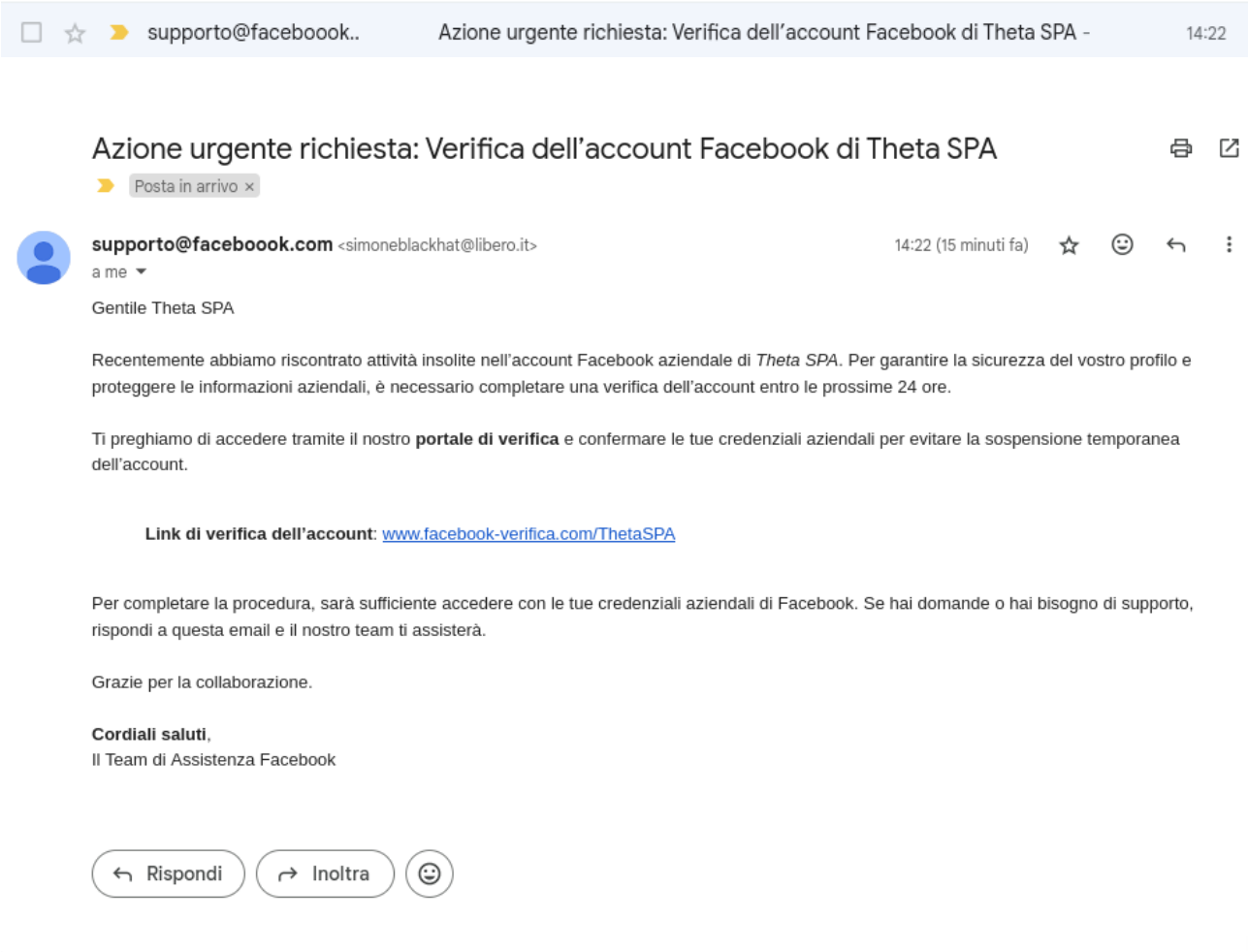
Per bypassare questo problema dobbiamo recarci nel file della nostra pagina web clonata e modificare il codice sorgente. Per farlo ci dobbiamo recare nella root della cartella di SET, aprire il file index.html e rimuovere gli script descritti sopra.



Ora che abbiamo rimosso gli script raggiorniamo la pagina e proviamo ad inserire le nostre credenziali per testare se tutto funziona correttamente e come possiamo vedere dall'immagine seguente ora riusciamo a leggere in chiaro i dati inseriti nel form di login.



Siamo quindi pronti a poter inviare la nostra email camuffando il link e reindirizzando la vittima al nostro sito clone, in questo specifico caso ho creato una mail su libero e mi sono inviato la mail sospetta al mio account gmail, di seguito possiamo vederne il risultato.



CONCLUSIONI

In questo progetto abbiamo ricreato uno scenario simulando un attacco di e-mail di phishing.

Lo scenario:

Ci siamo finti il supporto di Facebook che richiede di verificare l'account prima della sospensione, abbiamo di conseguenza inoltrato la mail al reparto marketing dell'azienda Theta S.p.A. inducendoli a cliccare sul link per la verifica, questo li rimanderà alla nostra pagina di login clonata che ci permetterà di vedere in chiaro i loro dati di accesso.

Perché l'email risulta credibile?

- L'email risulta credibile alla vittima sopratutto per il tono professionale utilizzato, il contenuto e la struttura del messaggio, nel dettaglio:
- Tono professionale e la personalizzazione indicando il nome dell'azienda
- L'urgenza e minaccia: inserire la frase di urgenza è una manipolazione psicologica che abbinata alla "minaccia" che l'account può essere sospeso spinge la vittima a reagire in fretta e senza riflettere
- Il link inserito sembra autentico
- Firma: ho inserito nella firma la tipica frase "se hai domande o hai bisogno..rispondi a questa email" questo simula un servizio clienti reale e rassicura la vittima.

Quali sono invece gli elementi di allarme?

Nonostante gli elementi sopracitati siano rassicuranti e indicano una tipica email di assistenza aumentandone la credibilità sono in realtà tutti dei **segnali di allarme** che dovrebbero far riflettere la vittima portandola a verificare accuratamente la veridicità prima di interagire con la mail.