Module 4 Social engineering Pentration testing

Task1 Create Fishing Page using Zphisher

Task 2 Create site cloner using Social Engineering tool

Task3 how to create fishing email and sent to the target using Social engineering tool

1 Extra Activity Using Set tool kit Generate the fake Q AR code

2 Extra Activity using website for fishing URL detections

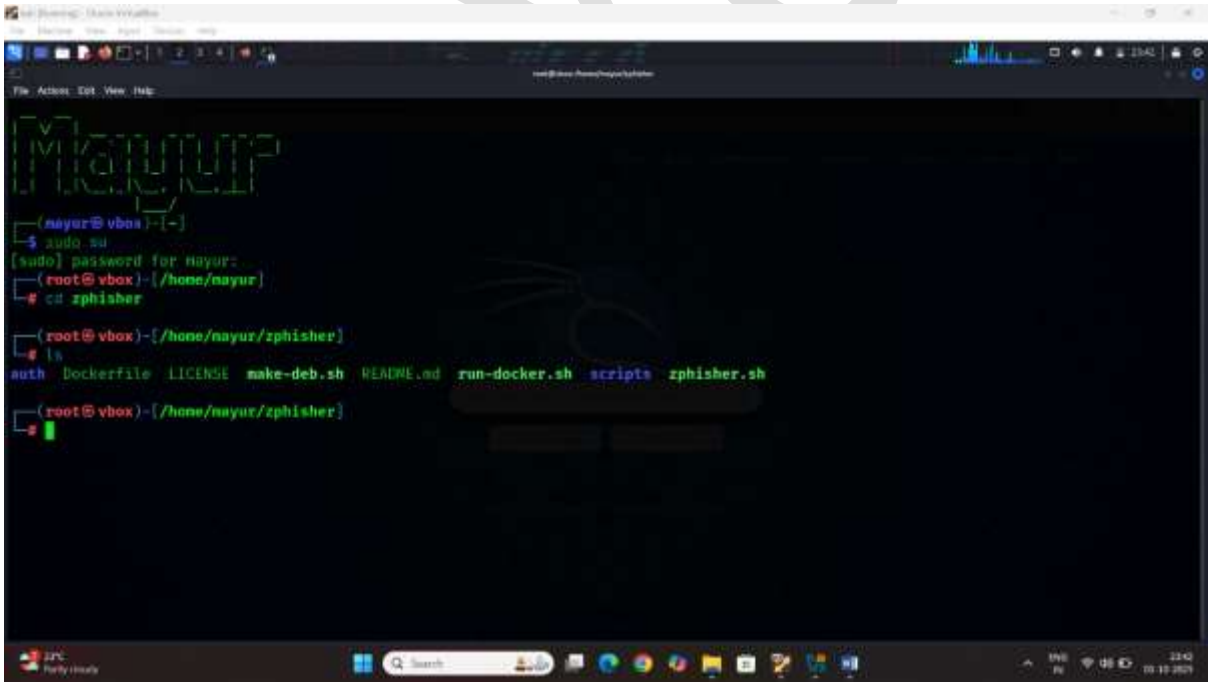
3 Extra Activity using website for fishing URL detections

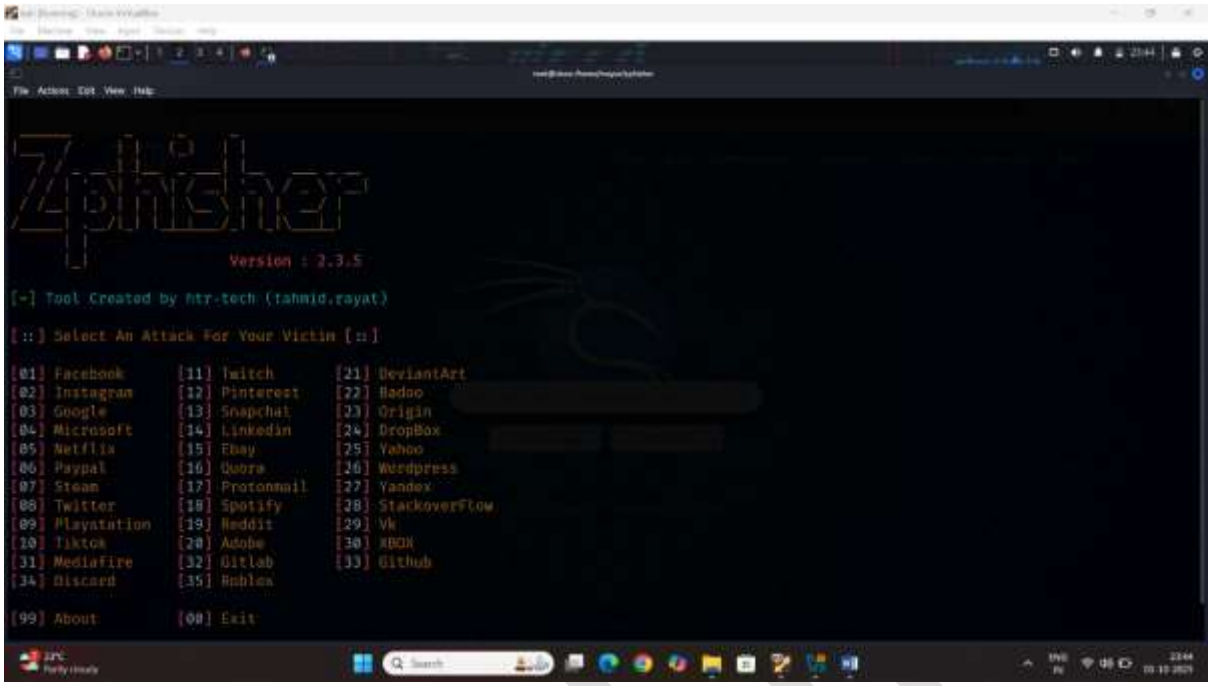
4 Extra Activity using website for fishing URL detections

Task1 Create Fishing Page using Zphisher

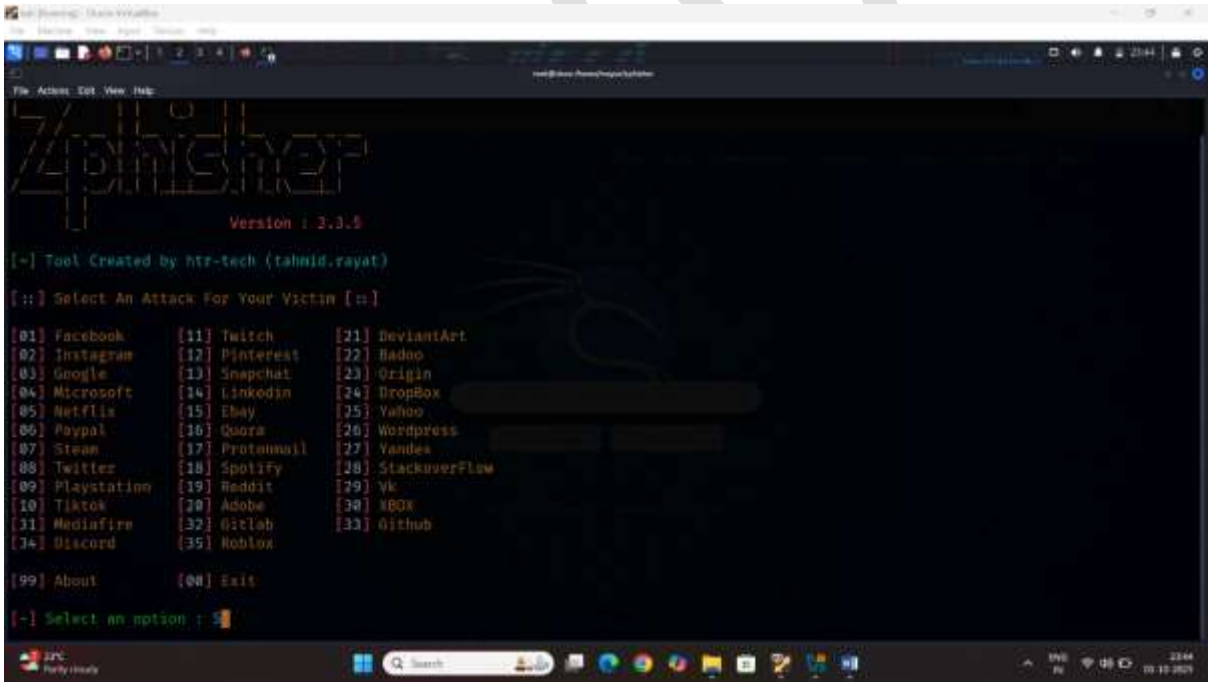
Step1 Start the kali linux machine

Step2 go to Zphisher

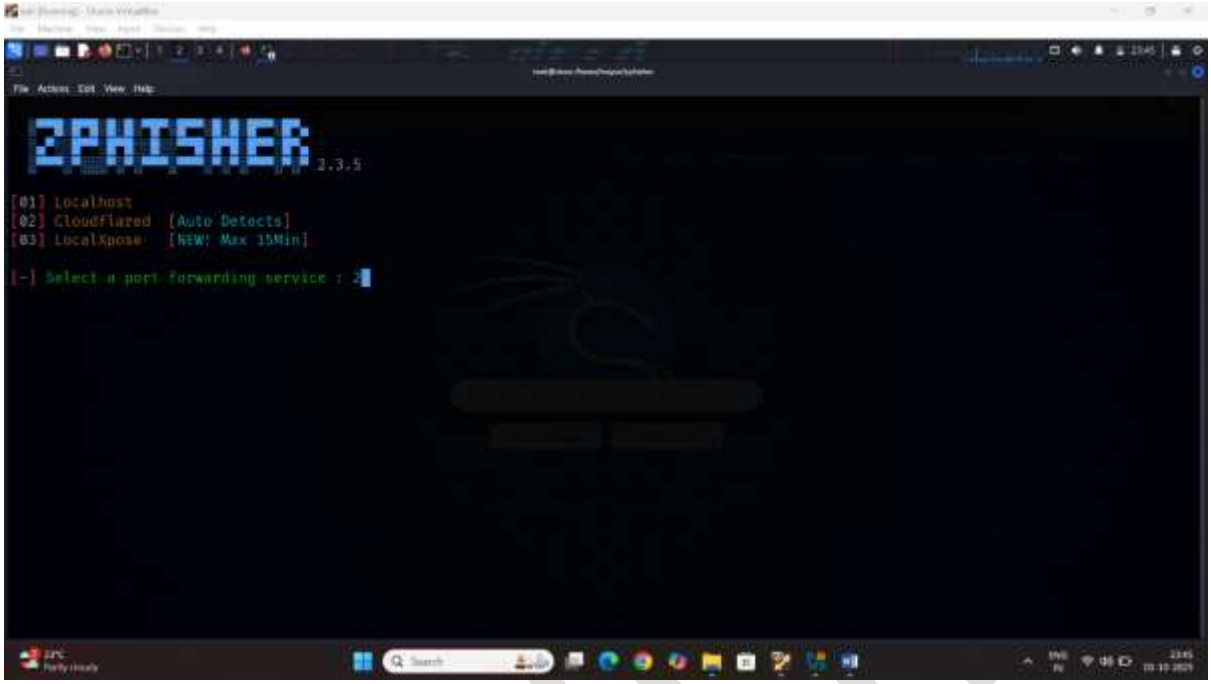


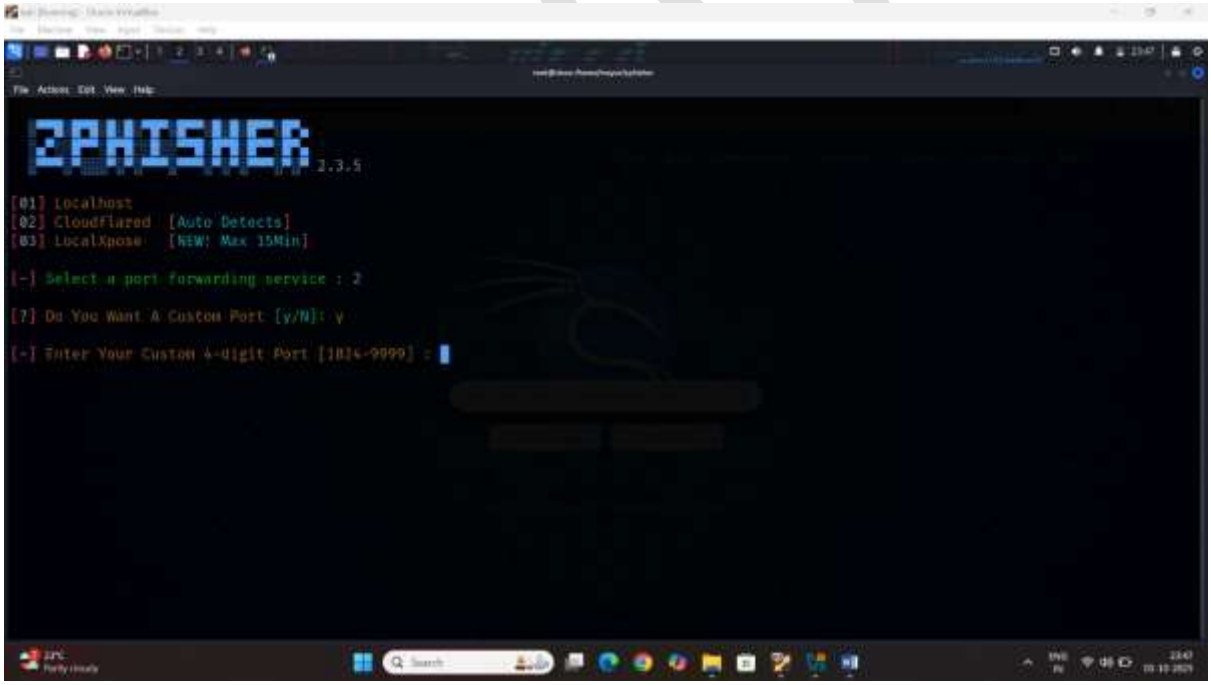


Step3 select the 5 option



Step4 use 2 option

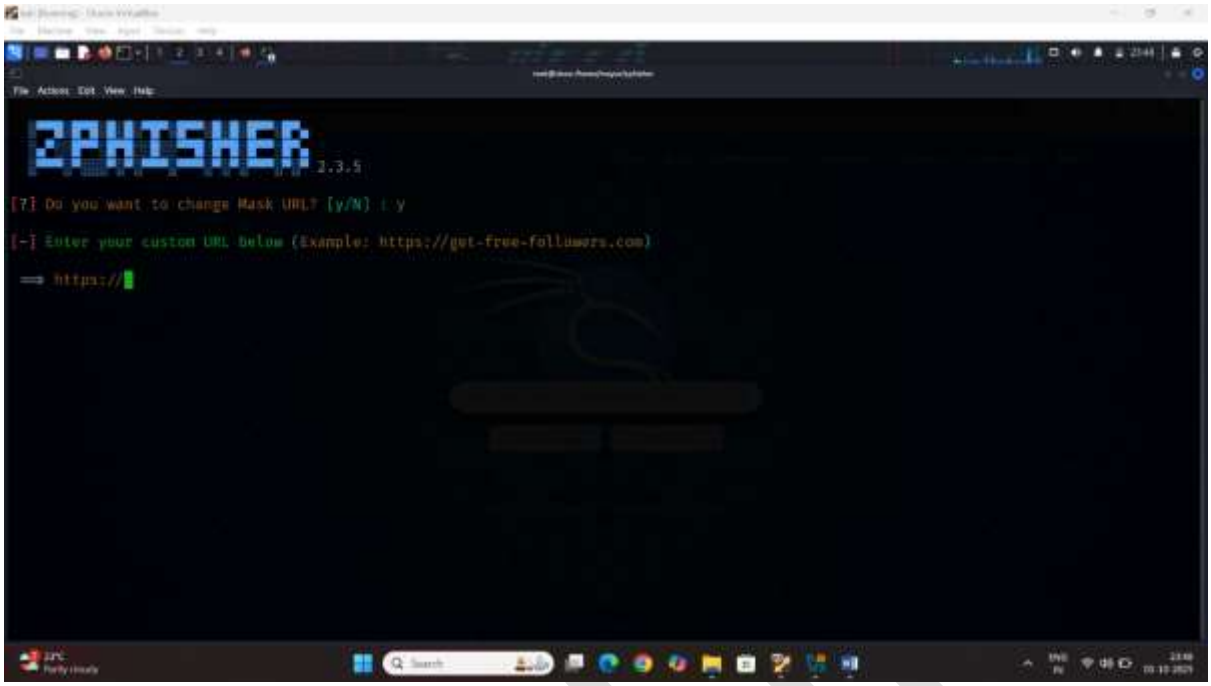


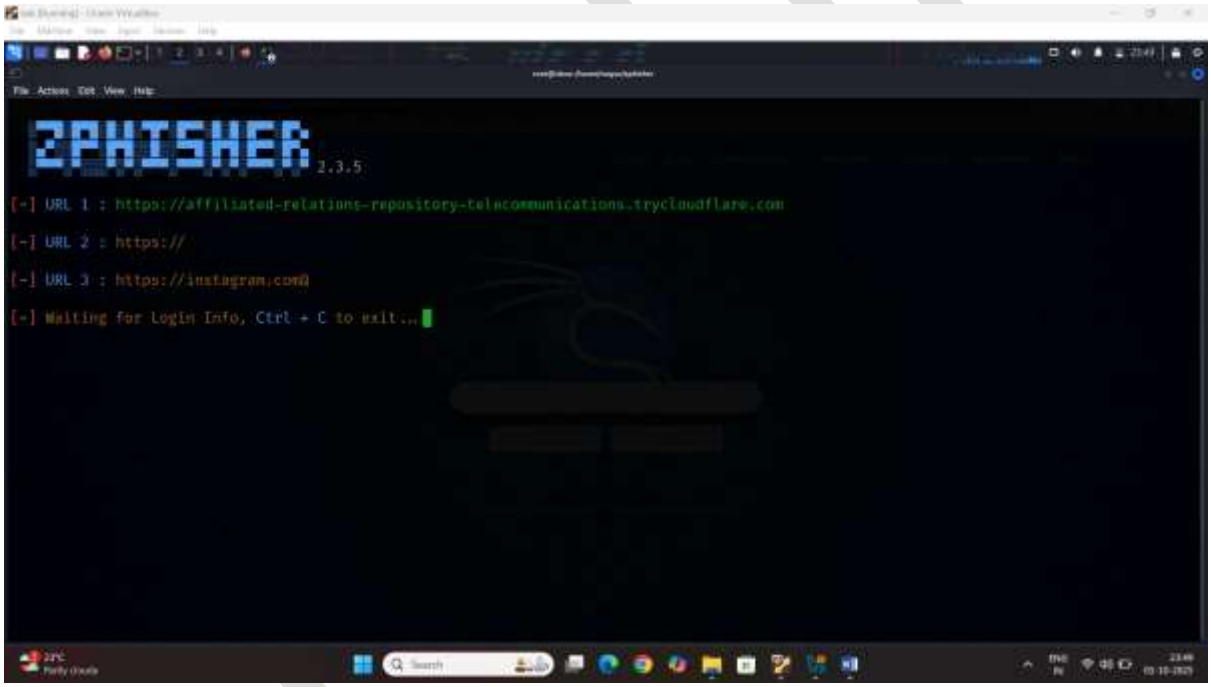


Step5 select the port option yes

Enter the port range 5555

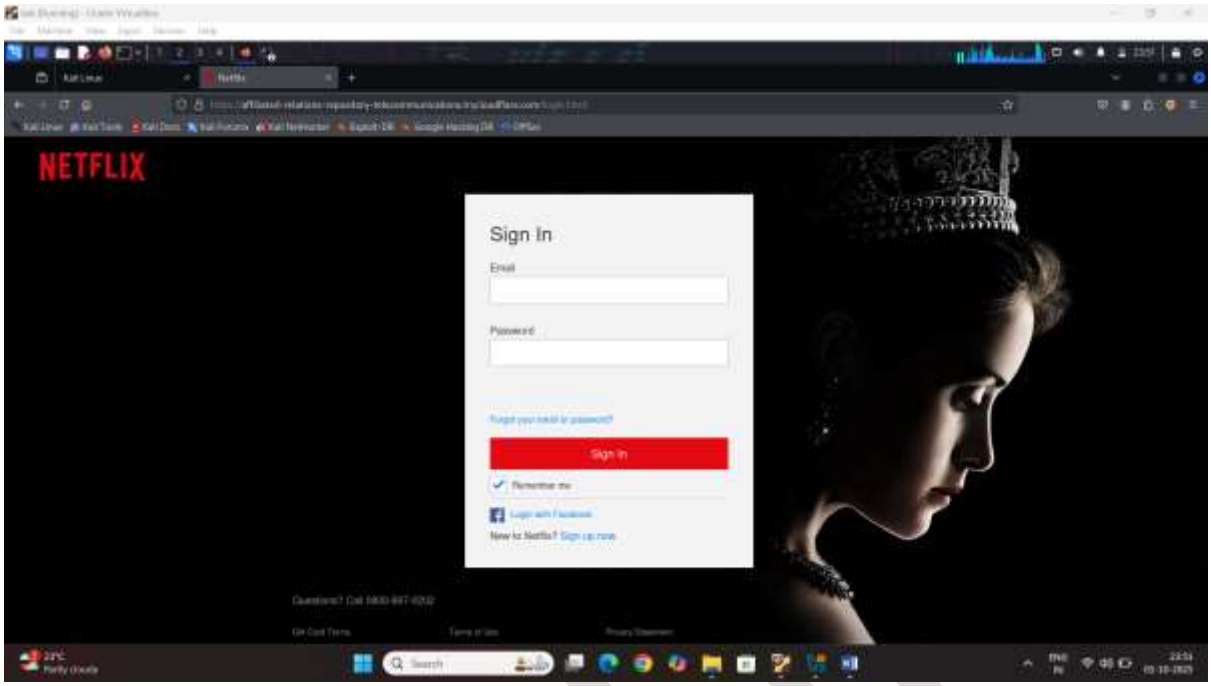
Step6 enter the url Instagram.com





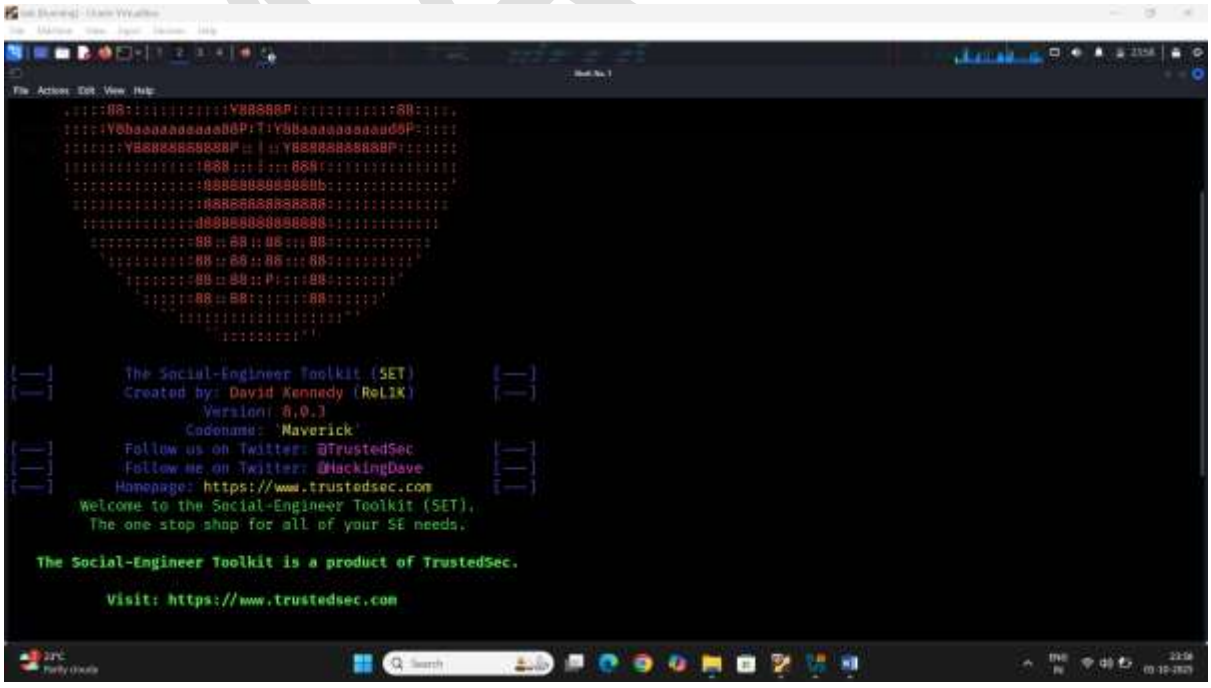
Step7 copy the 1st url and paste the chrome

Result:

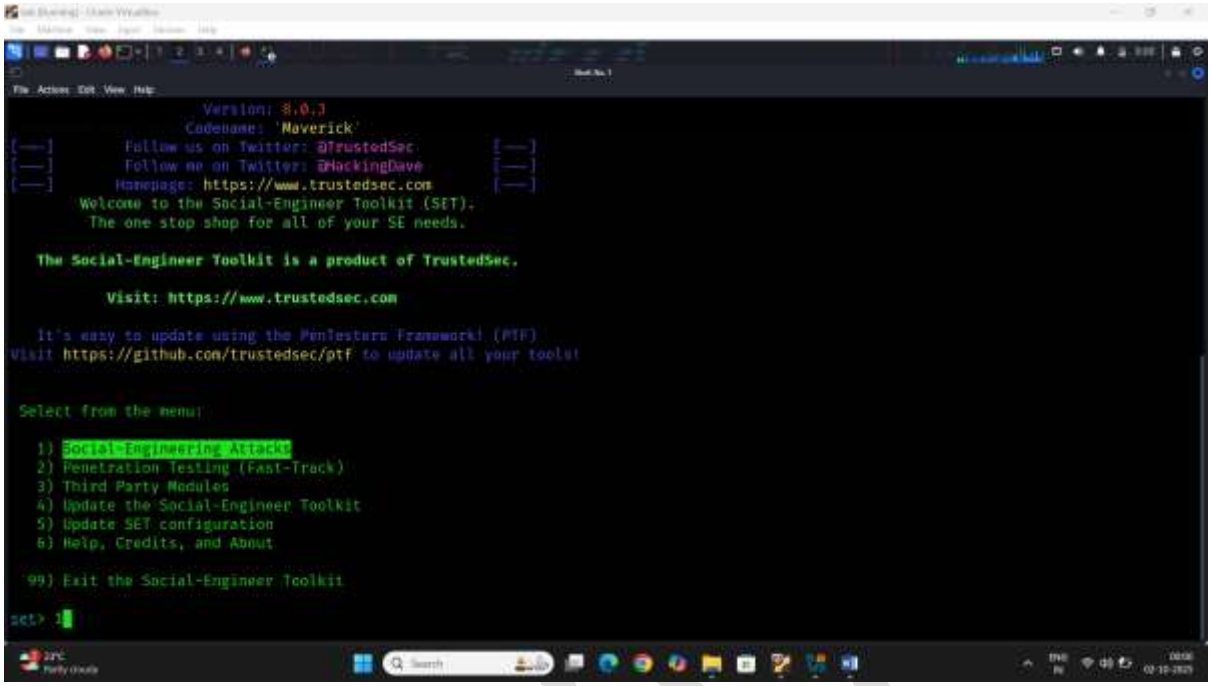


Task 2 Create site cloner using Social Engineering tool

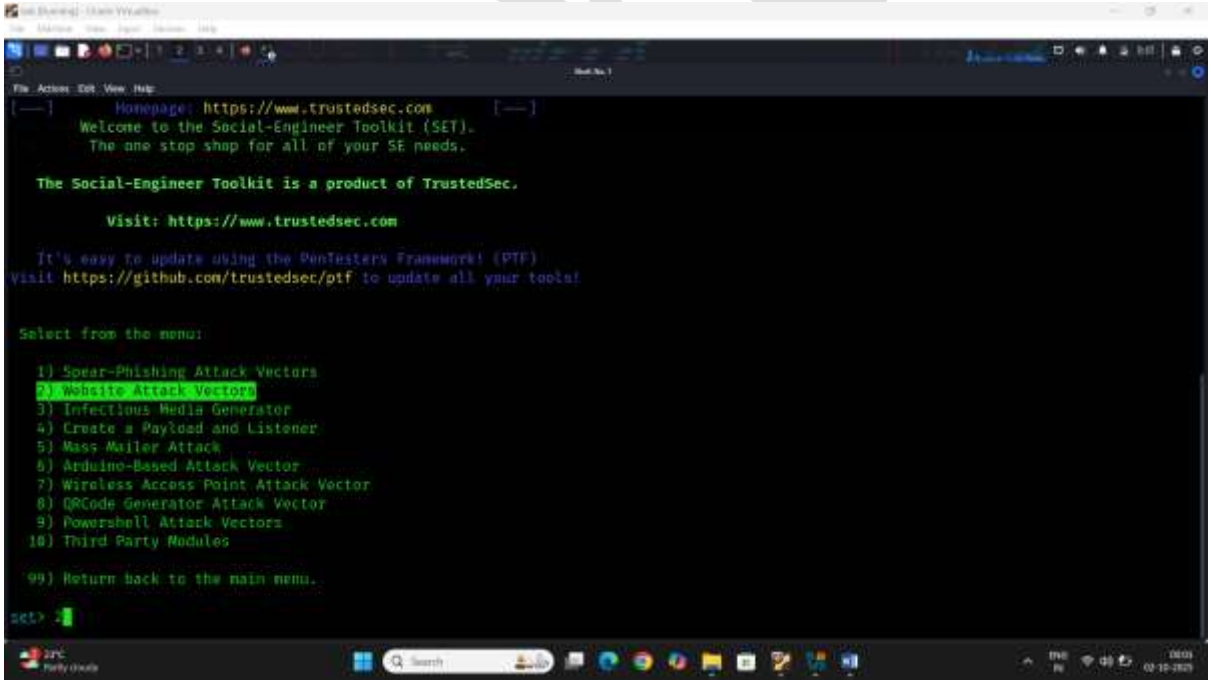
Step1 start the set tool kite



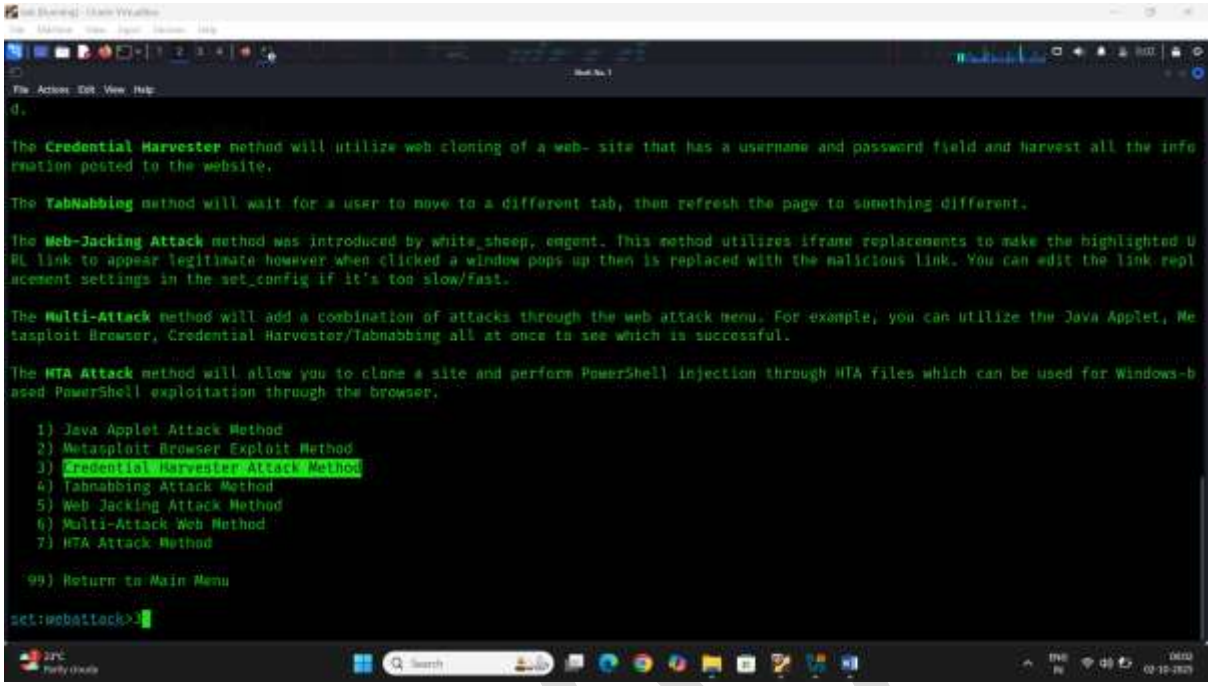
Step2 select the social enegineering attack

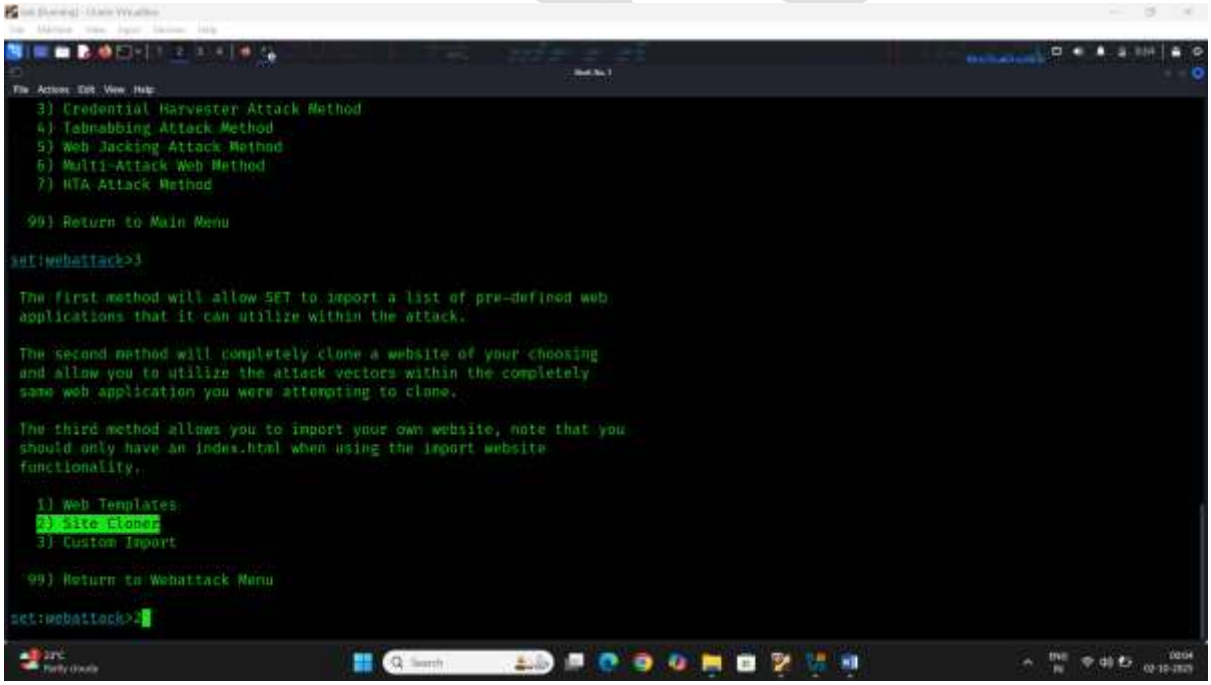


step3 select the website attack vectors



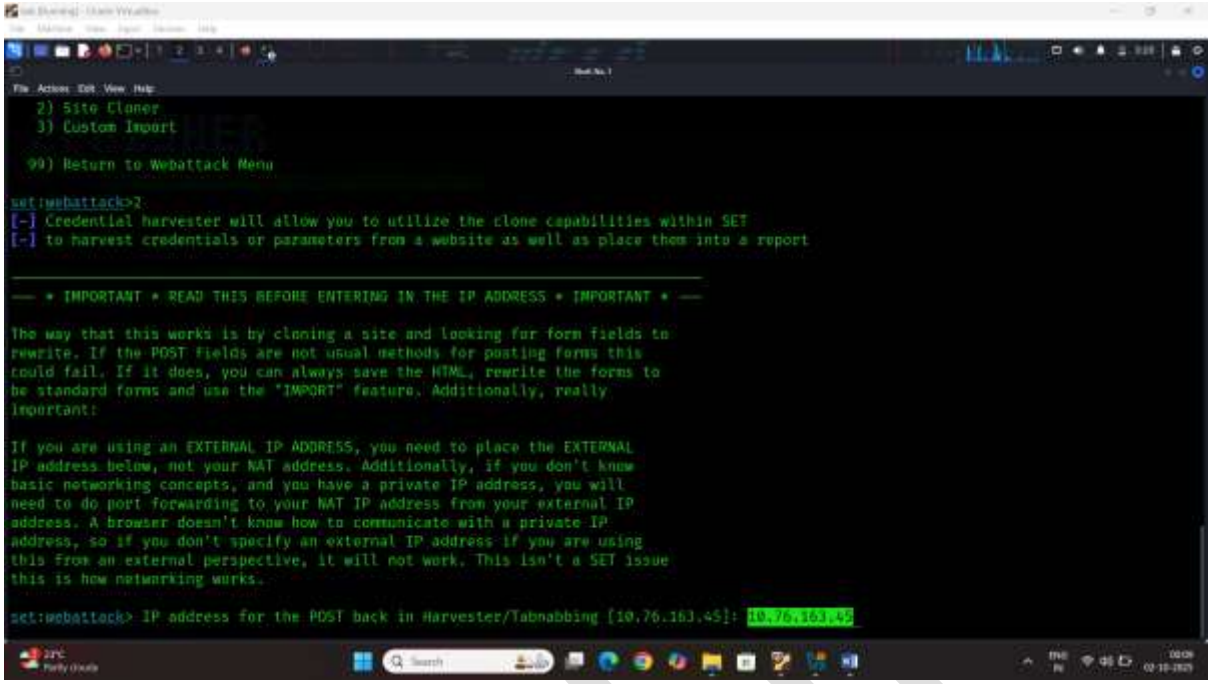
Step4 select the creadential harvester attack method

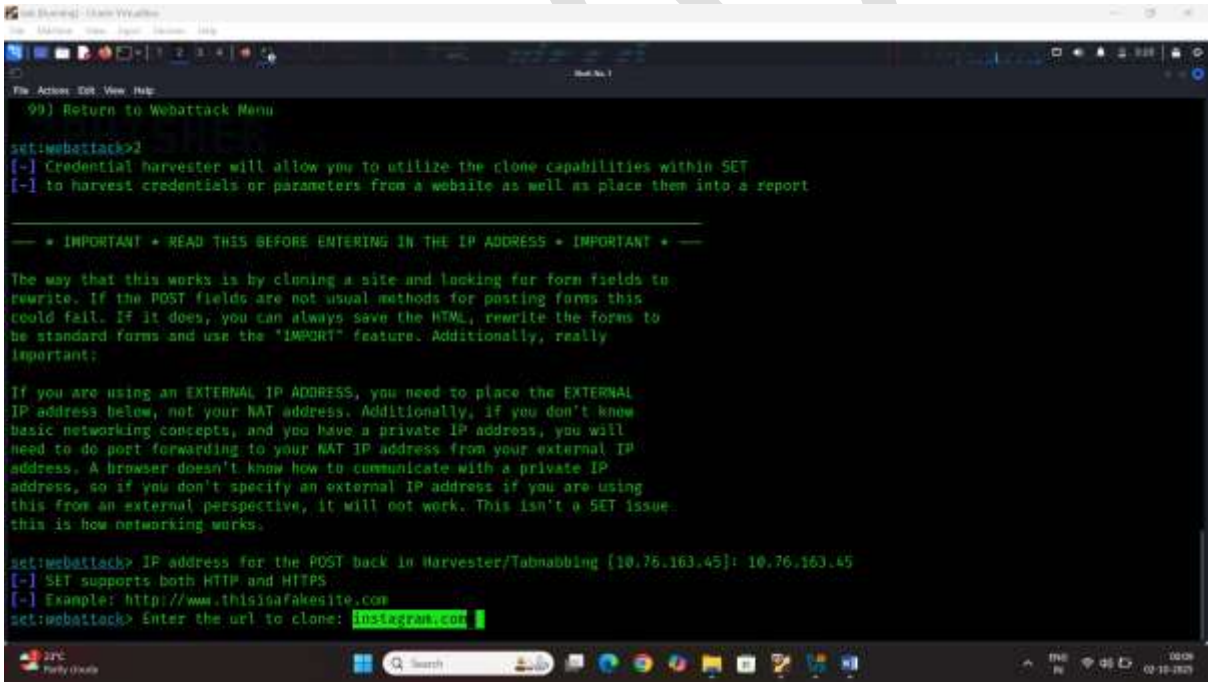




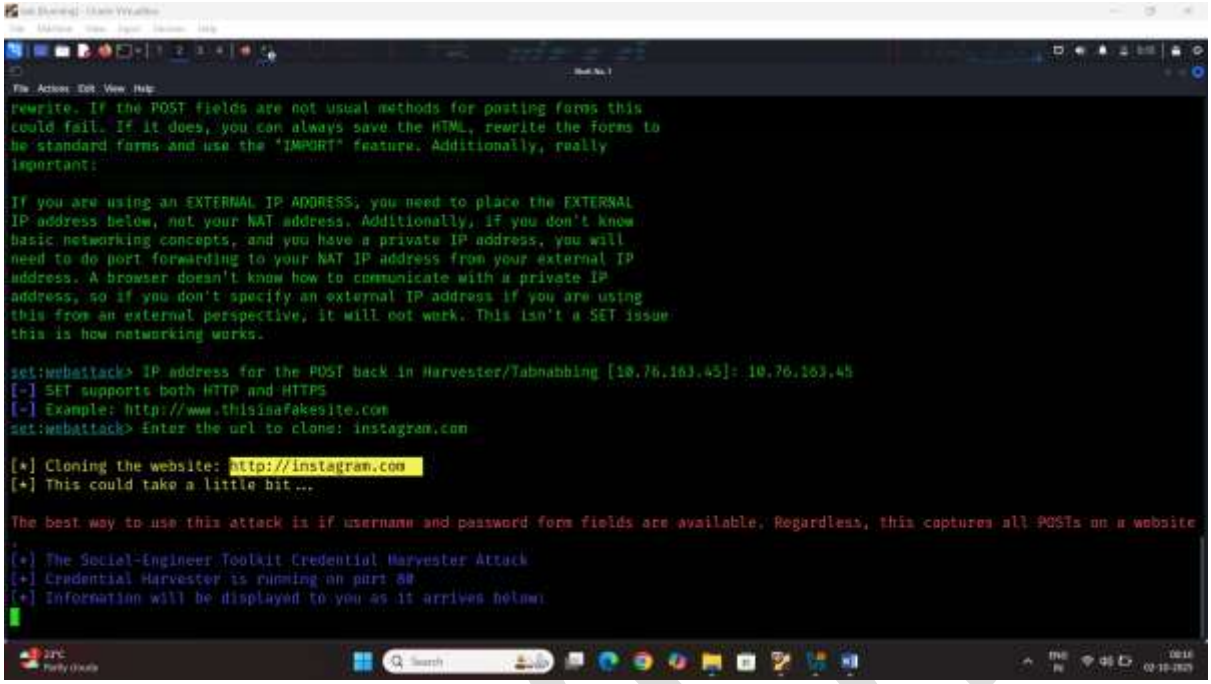
Step5 select the option site cloner

Step6 type the klai linux url

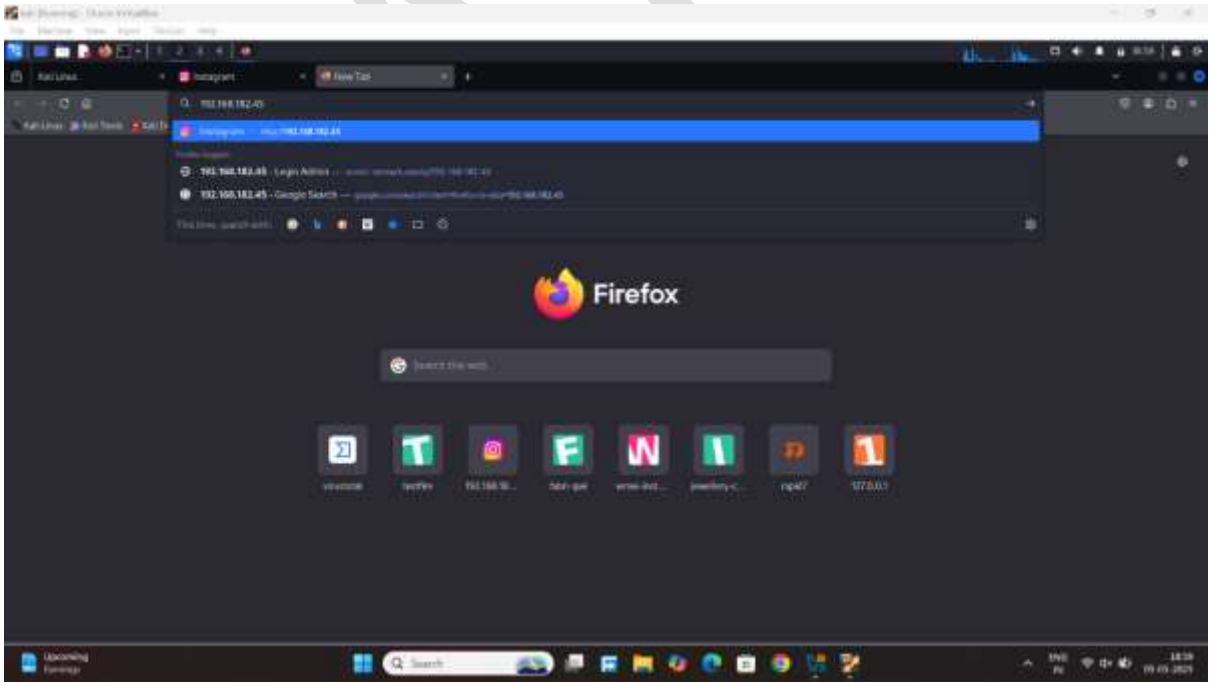

2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
--- * IMPORTANT * READ THIS BEFORE ENTERING IN 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 [10.76.163.45]: 10.76.163.45


99) Return to Webattack Menu
set:webattack>2
[-] 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 [10.76.163.45]: 10.76.163.45
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: instagram.com

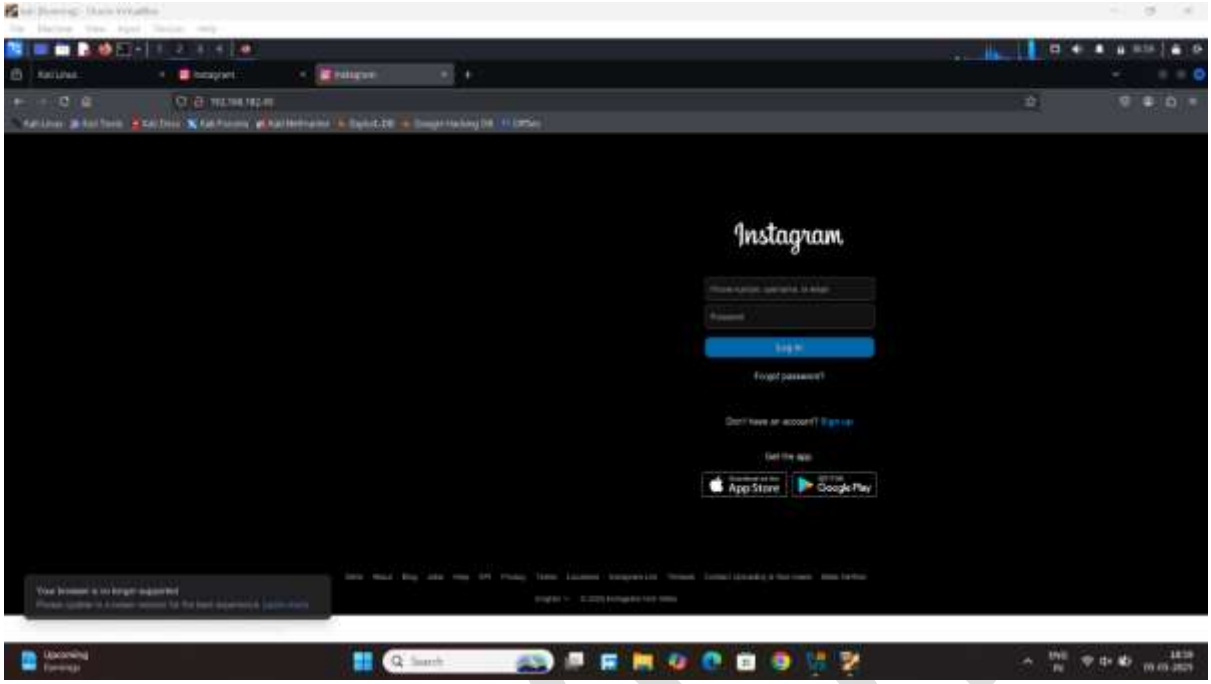
Step7 clone website Instagram.com



Type the kali linux ip and send the target



Result: successful open the site

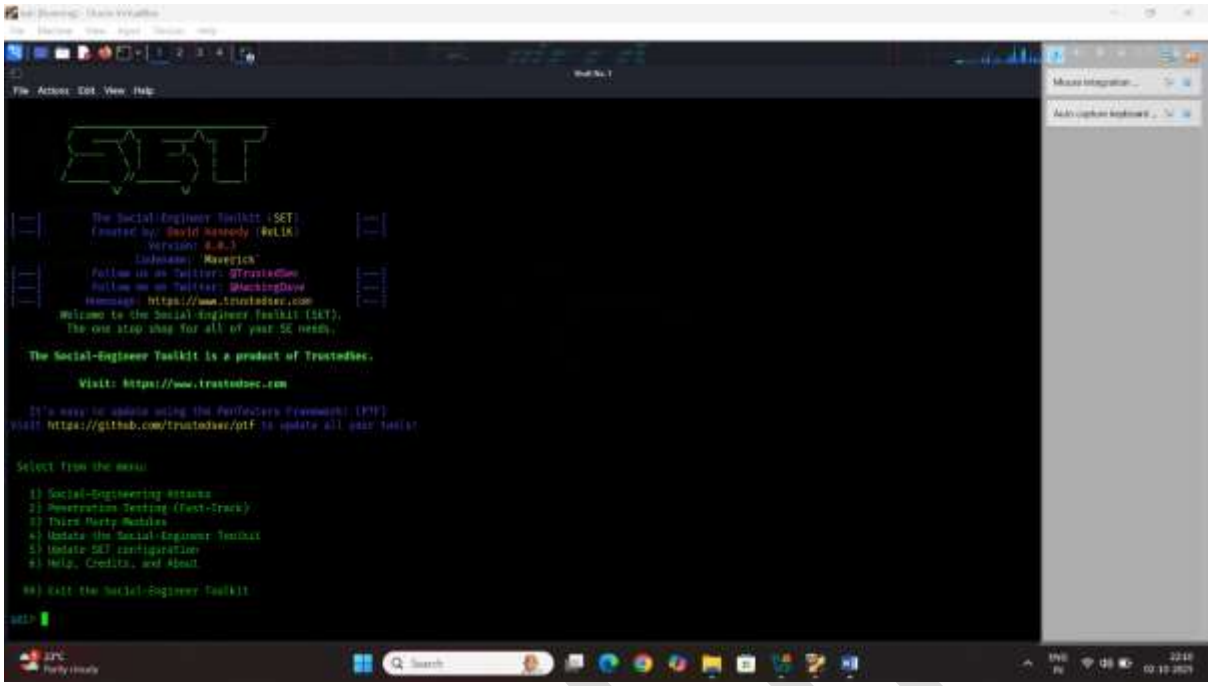


Task2: how to create fishing email and sent to the target using Social engineering tool

Step1: open the kali Linux terminal and Search the social engineering tool

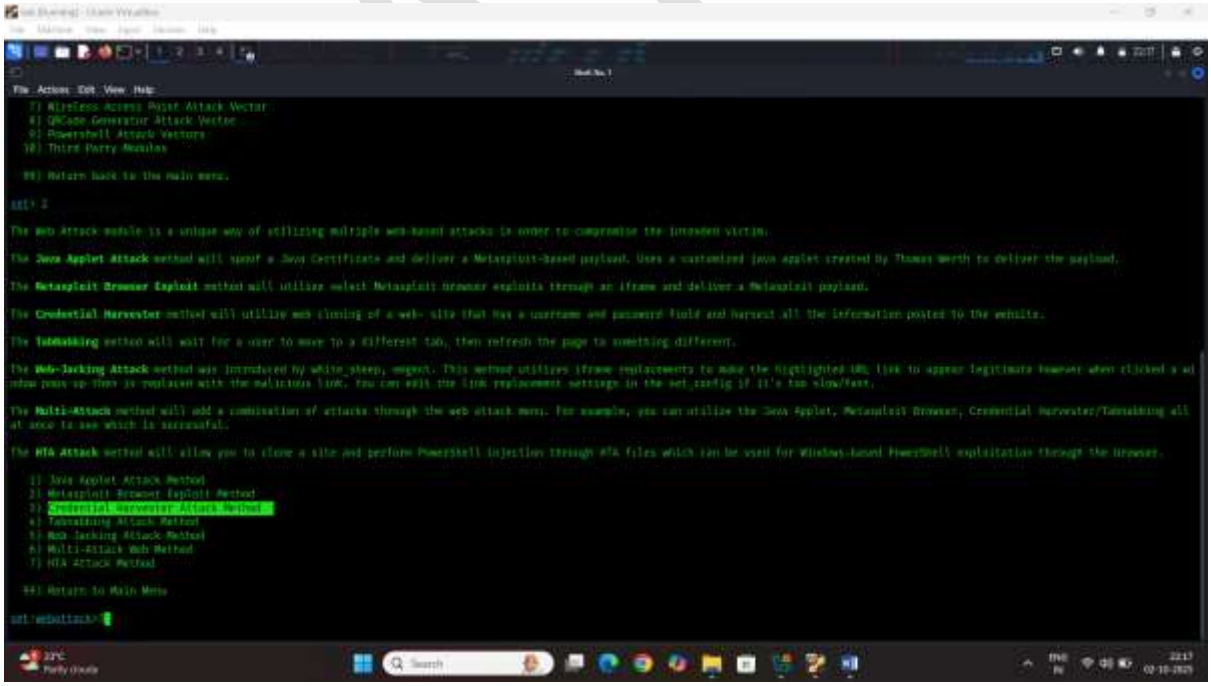
Step2: open the set tool kit choice the option

1 Social engineering

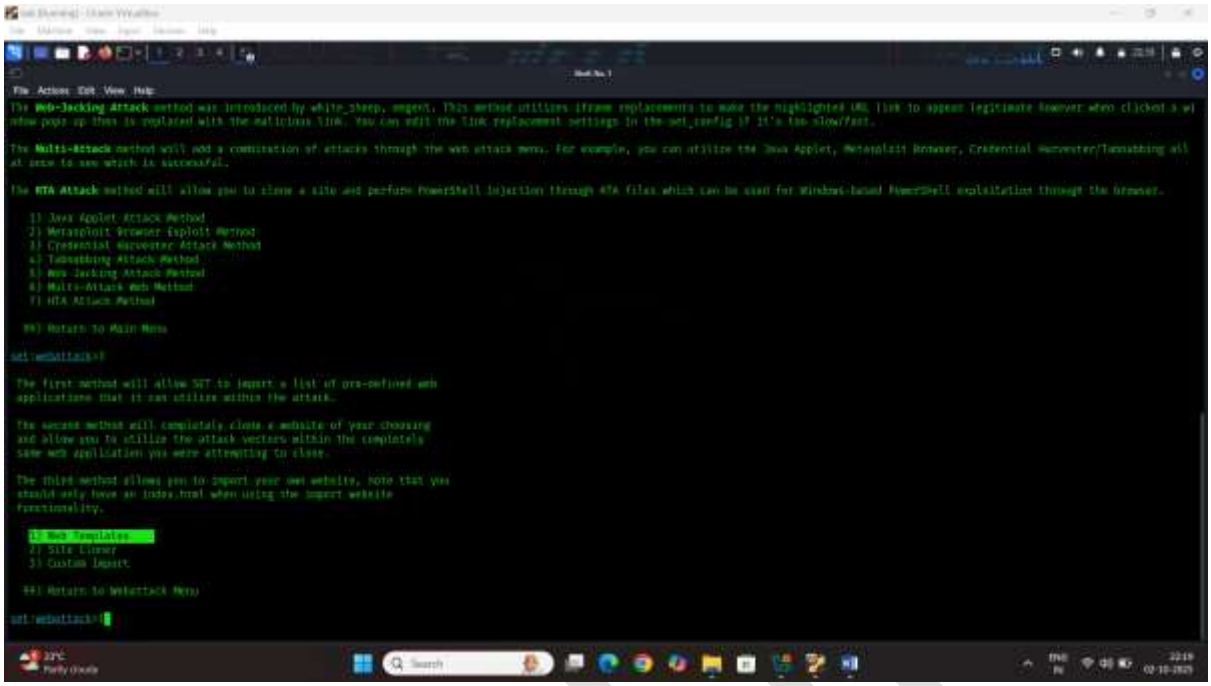


Step3 select the option

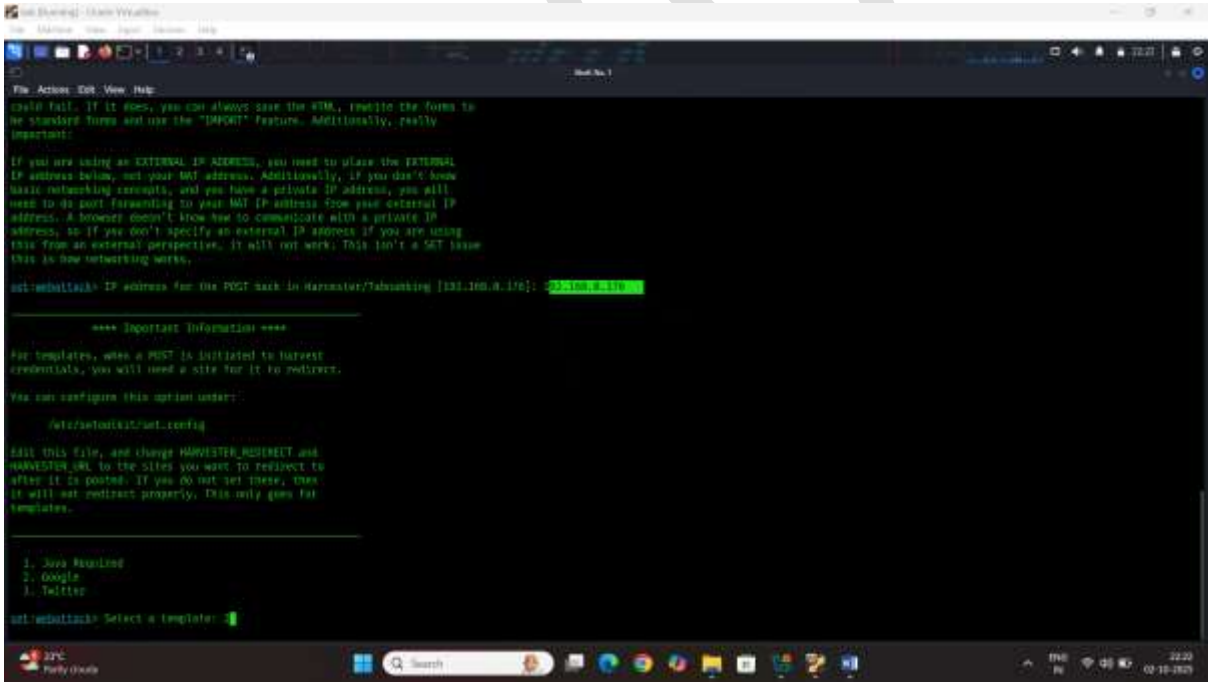
credential harvester attack method



Step4 select the option web templete

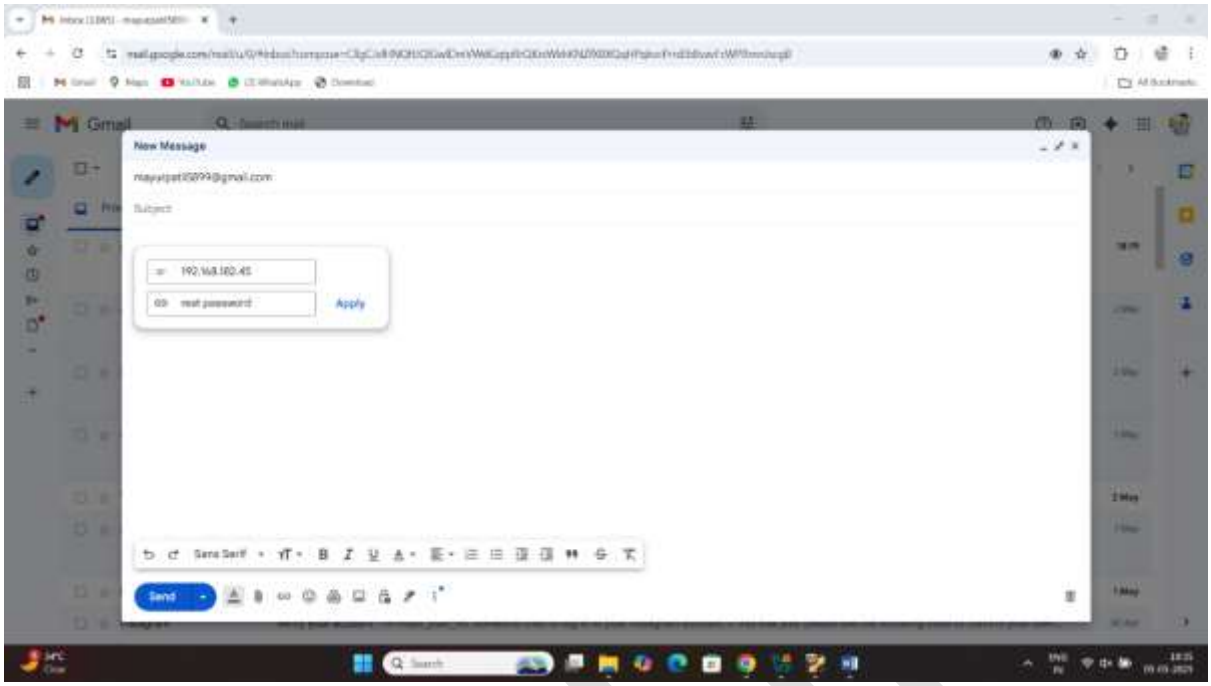


Step5 select the option web templet

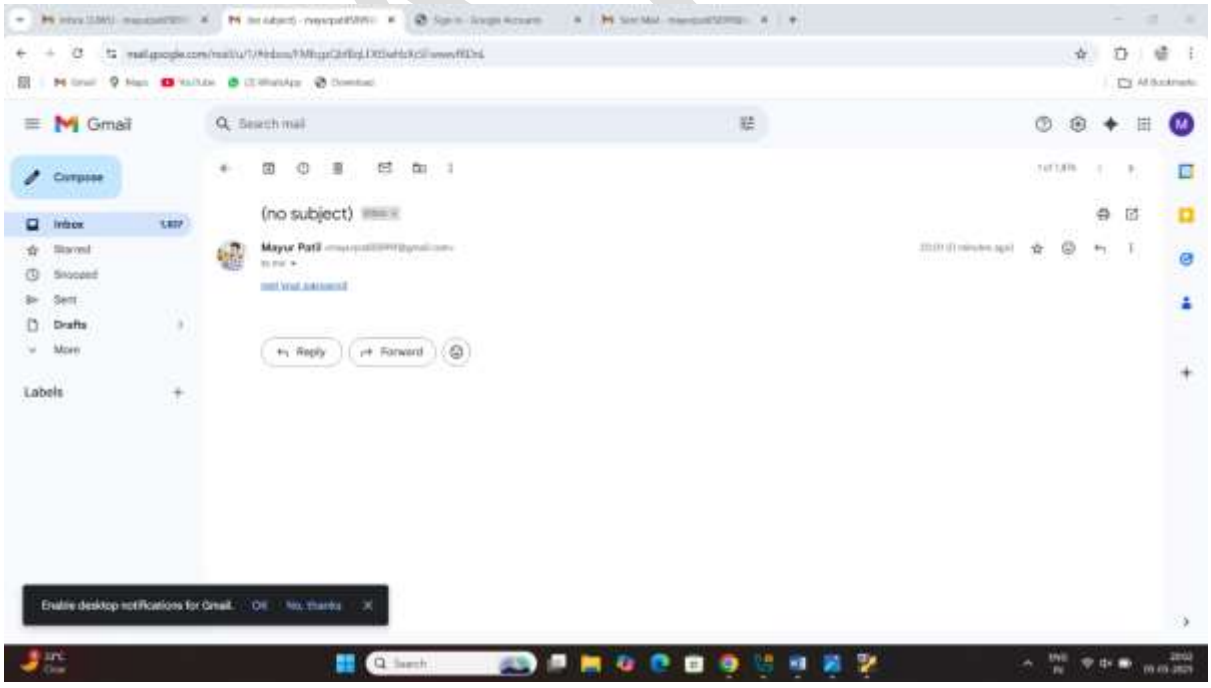


Step6 select the option google

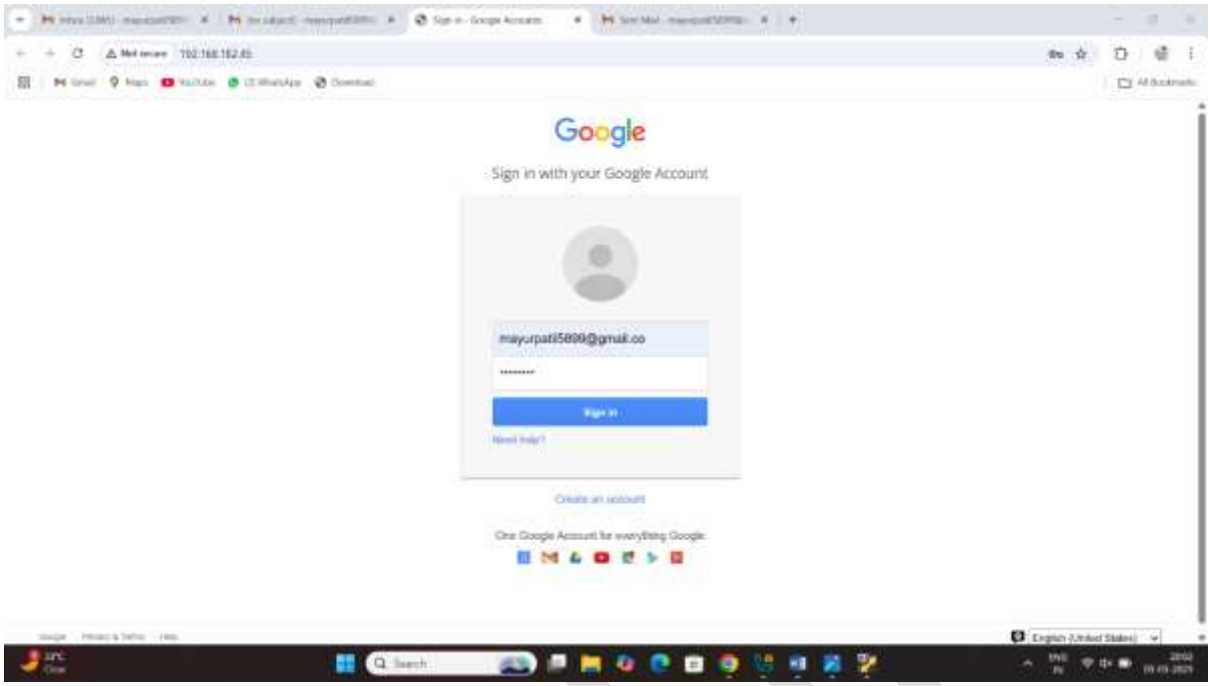
Step8: open the email create the fishing email click on insert link type the kali linux ip



Send it email the target my target email is mayurpatil5899@gmail.com

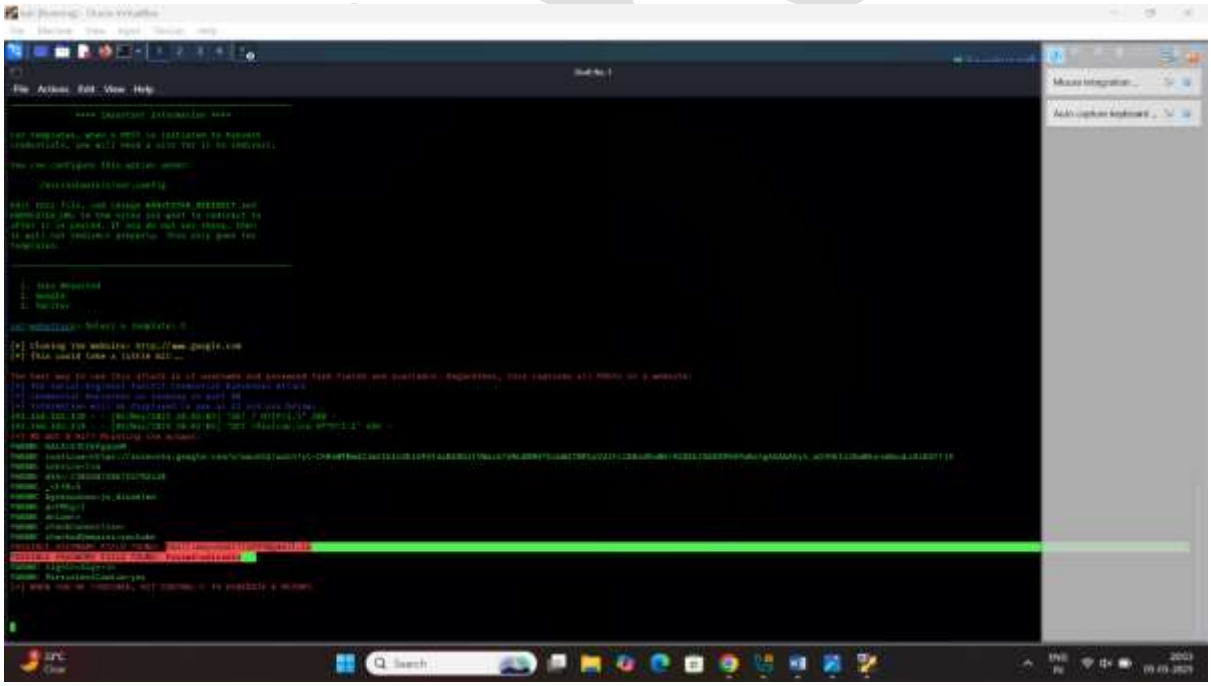


Open the target link and login gmail id



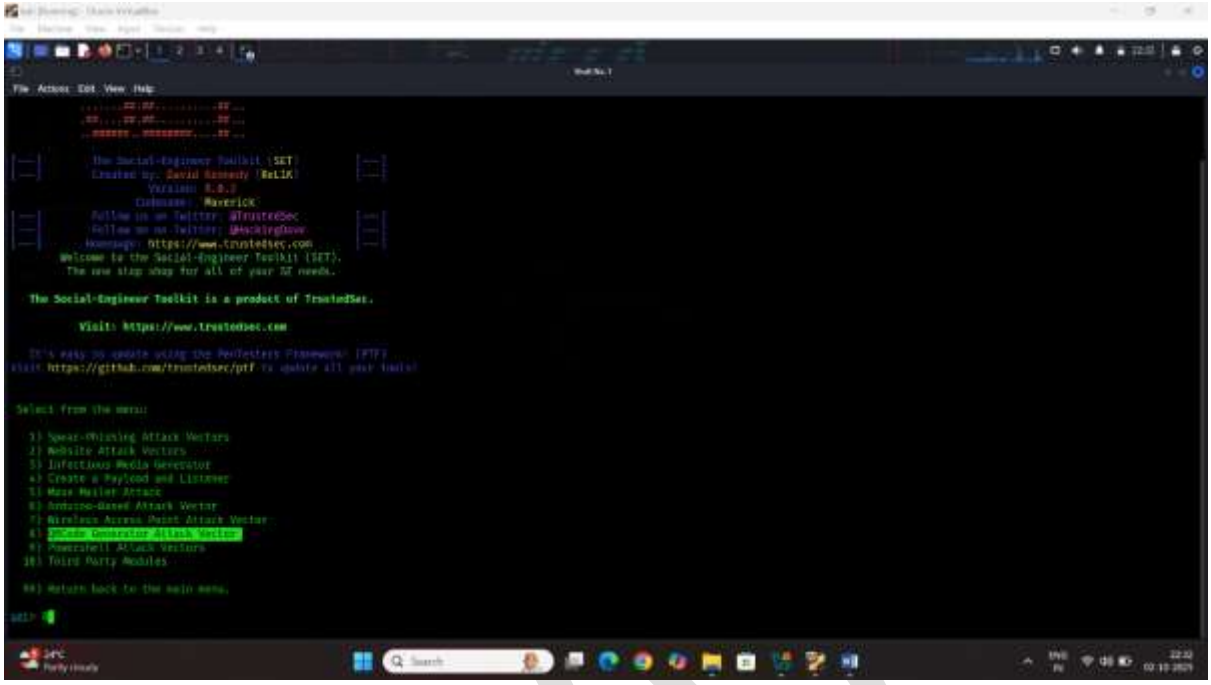
Click on sign

Result:



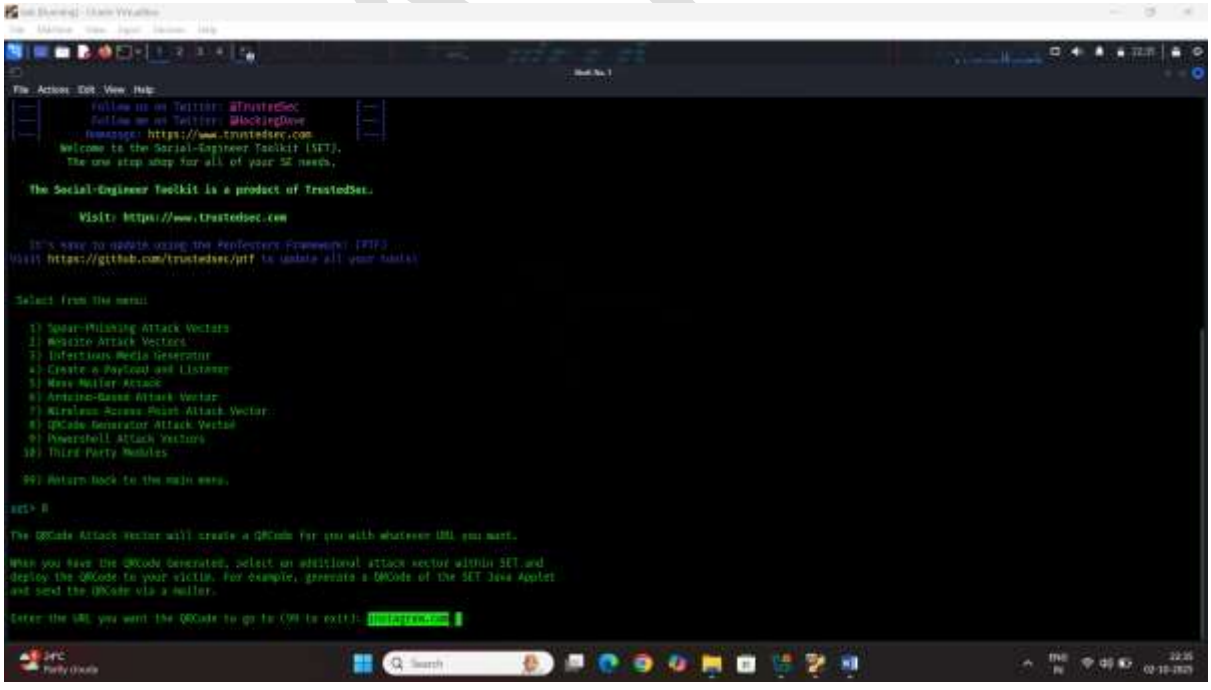
Extra Activity Using Set tool kit Generate the fake Q AR code

Step1: go to kali linux open the set tool kit

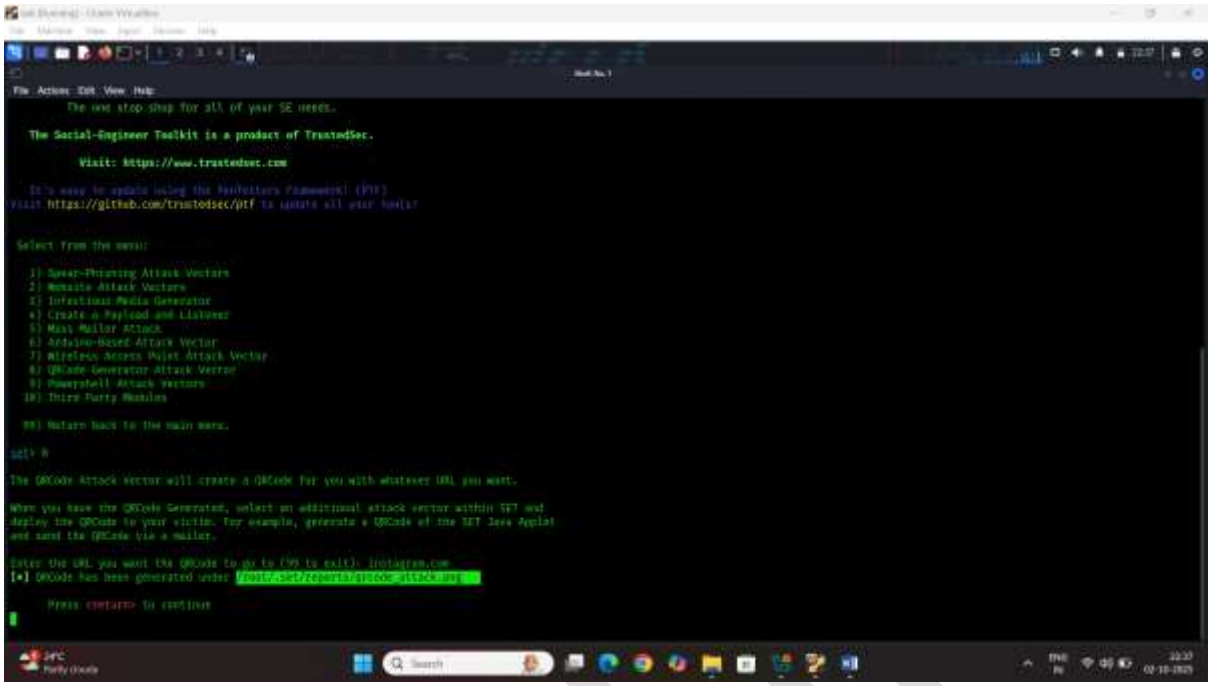


Step4: type the URL

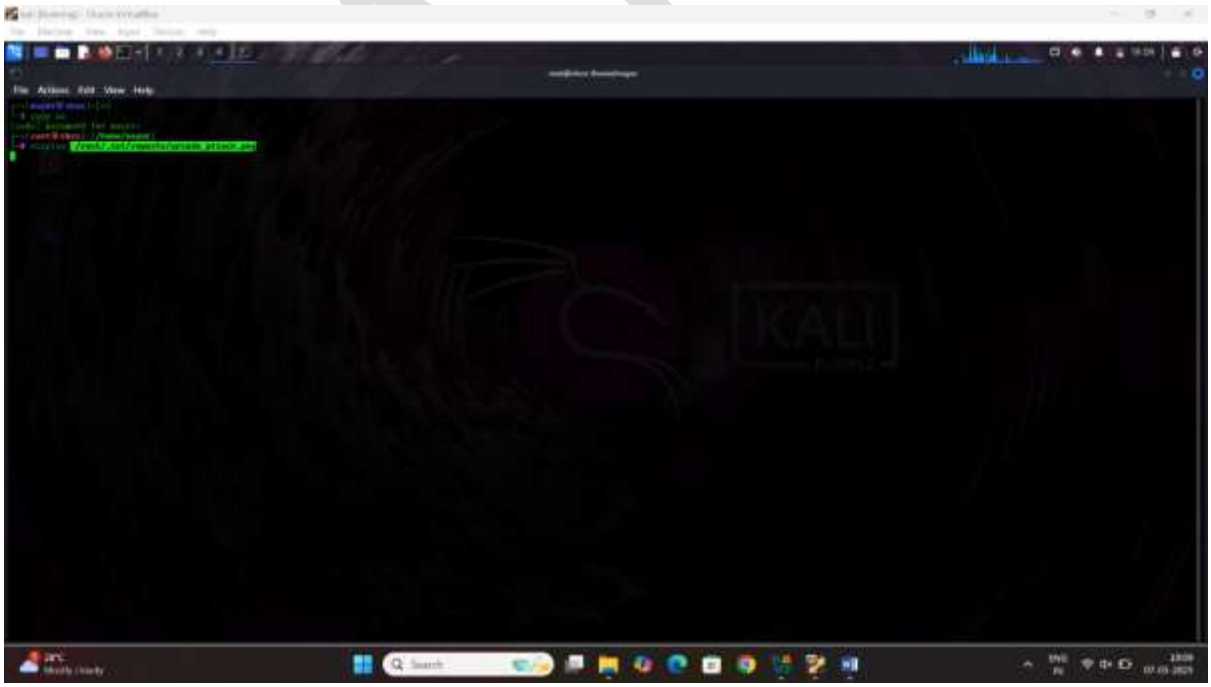
Example: https://instagram.com

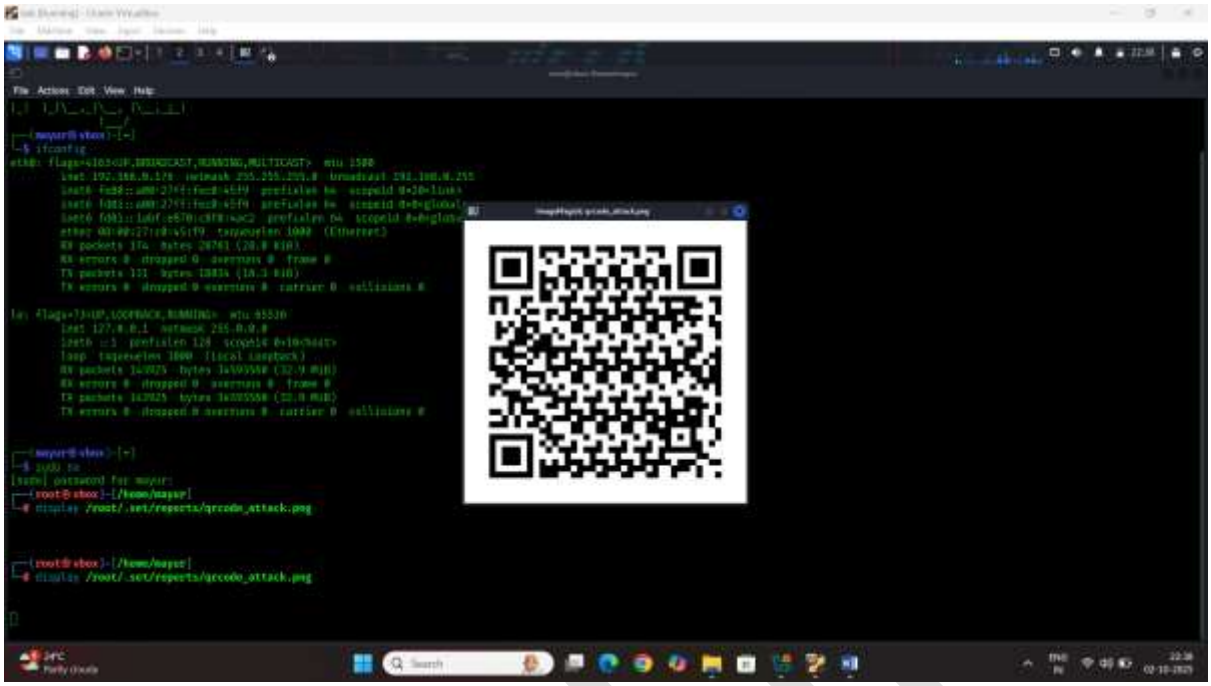


Step5 copy the root option



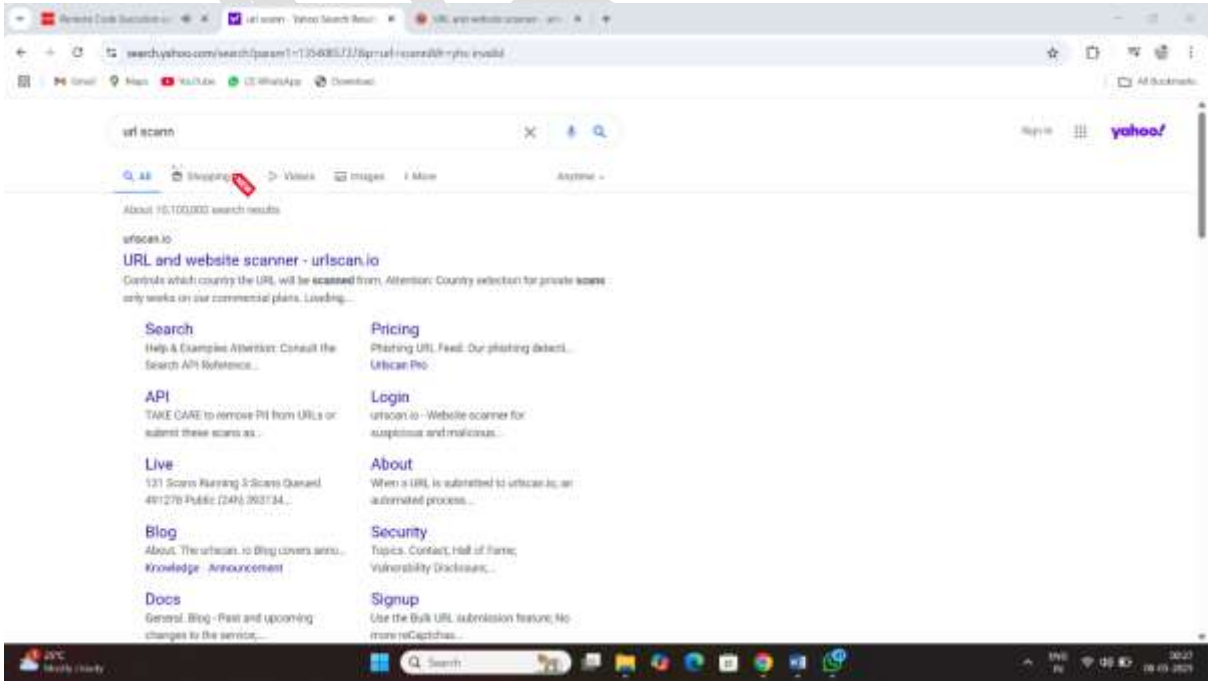
Step6: open the kali linux terminal copy the root link past it terminal

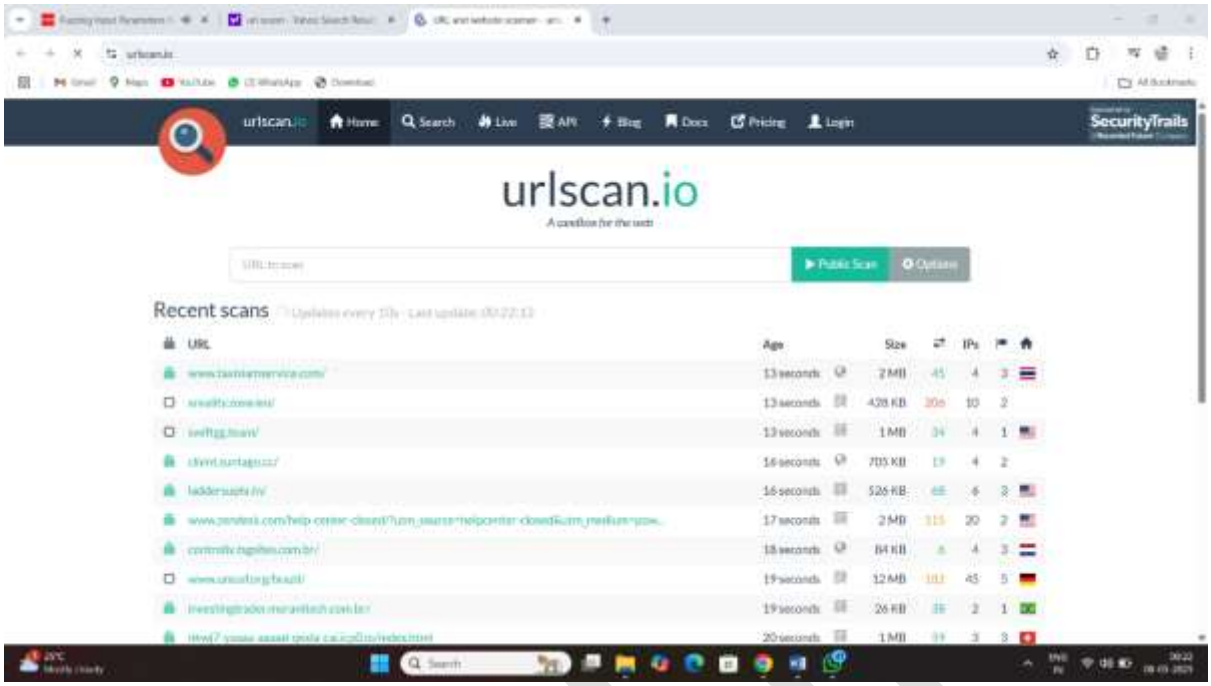




2 Extra Activity using website for fishing URL detections

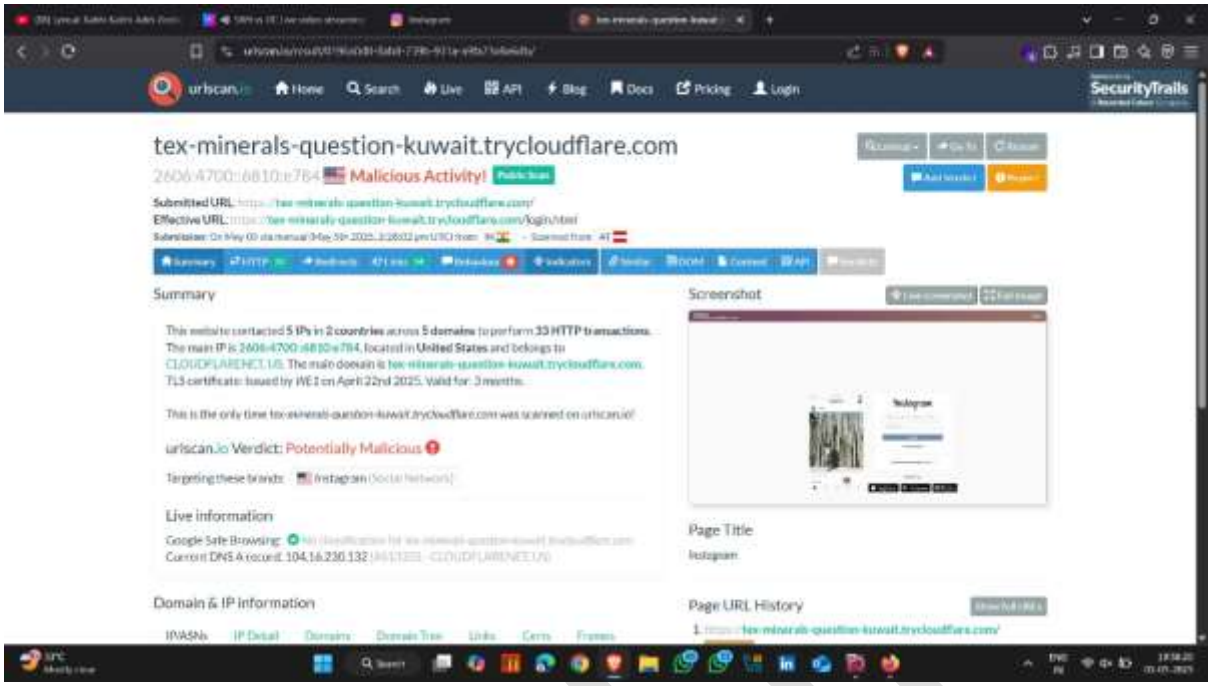
1 web site name: urlscan.io




urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
SecurityTrails
urlscan.io
A sandbox for the web
Public Scan
Options
Recent scans
URL
Age
Size
IPs

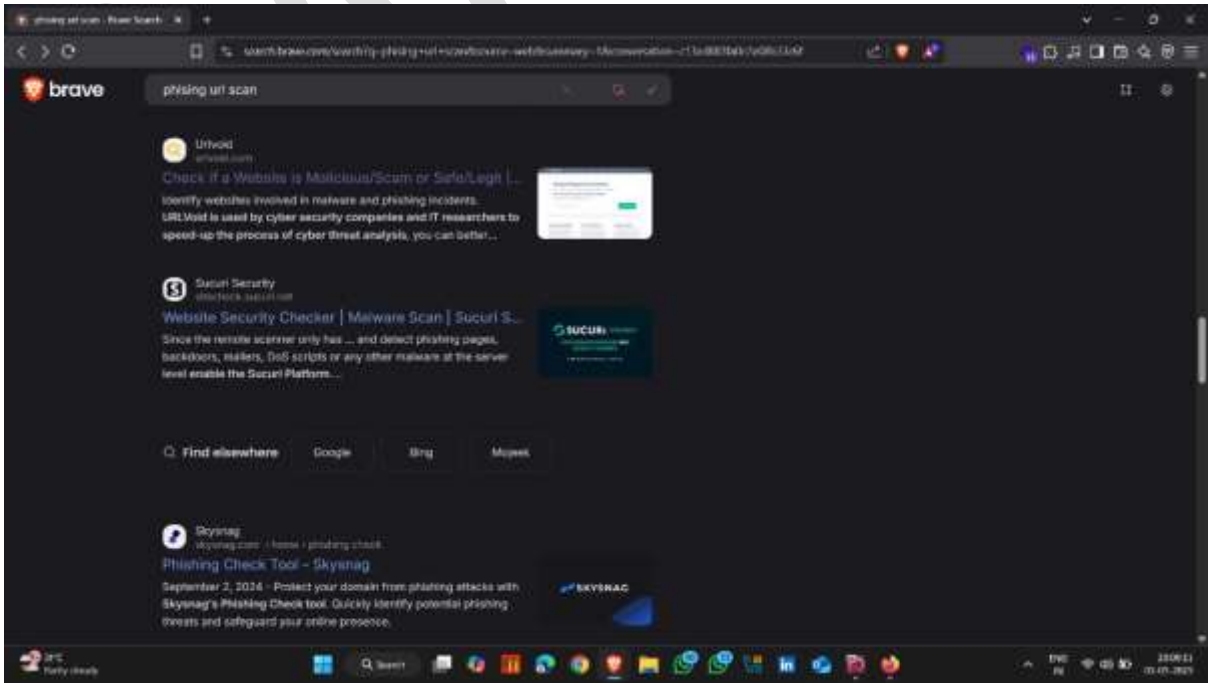

urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
SecurityTrails
urlscan.io
A sandbox for the web
https://few-minerals-question-kuwait.trycloudflare.com
Public Scan
Options
Recent scans
URL
Age
Size
IPs

Result:

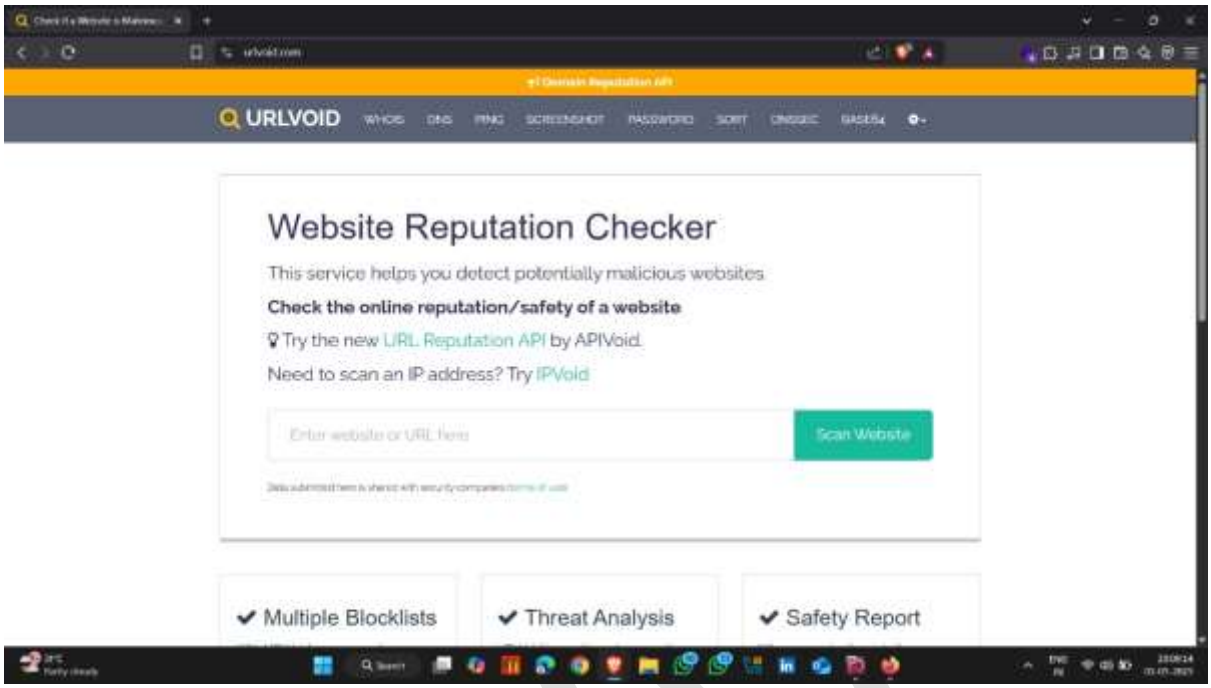


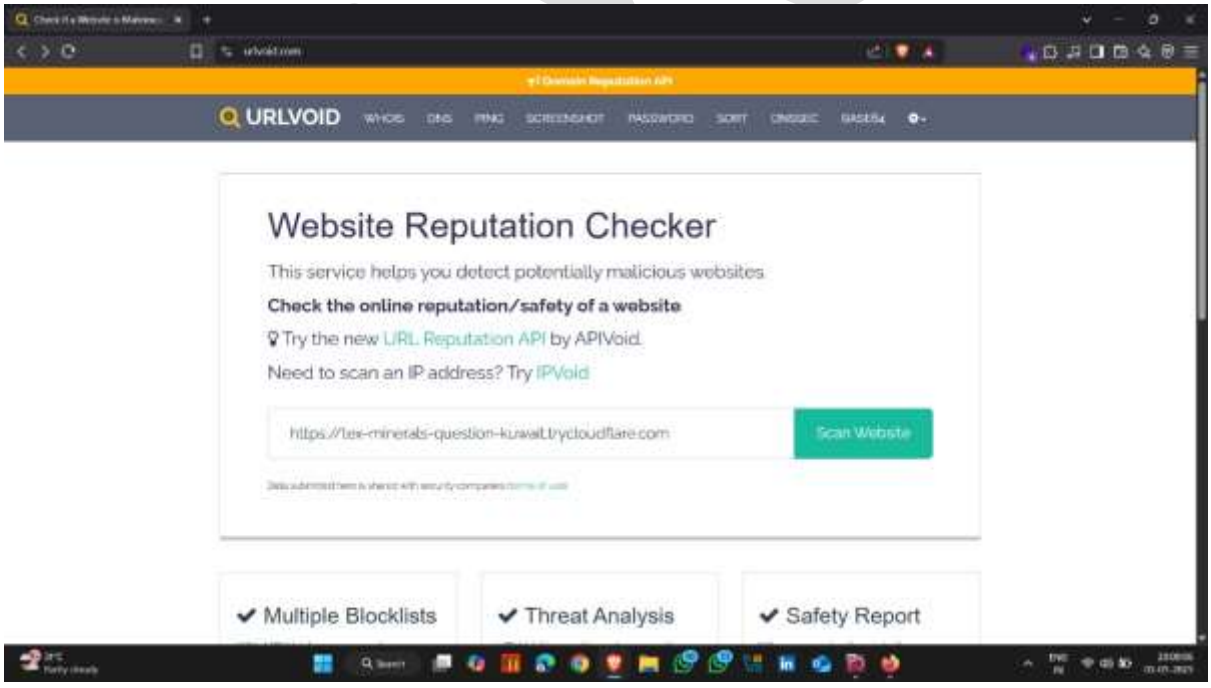
3 Extra Activity using website for fishing URL detections

1 web site name: URLvoid

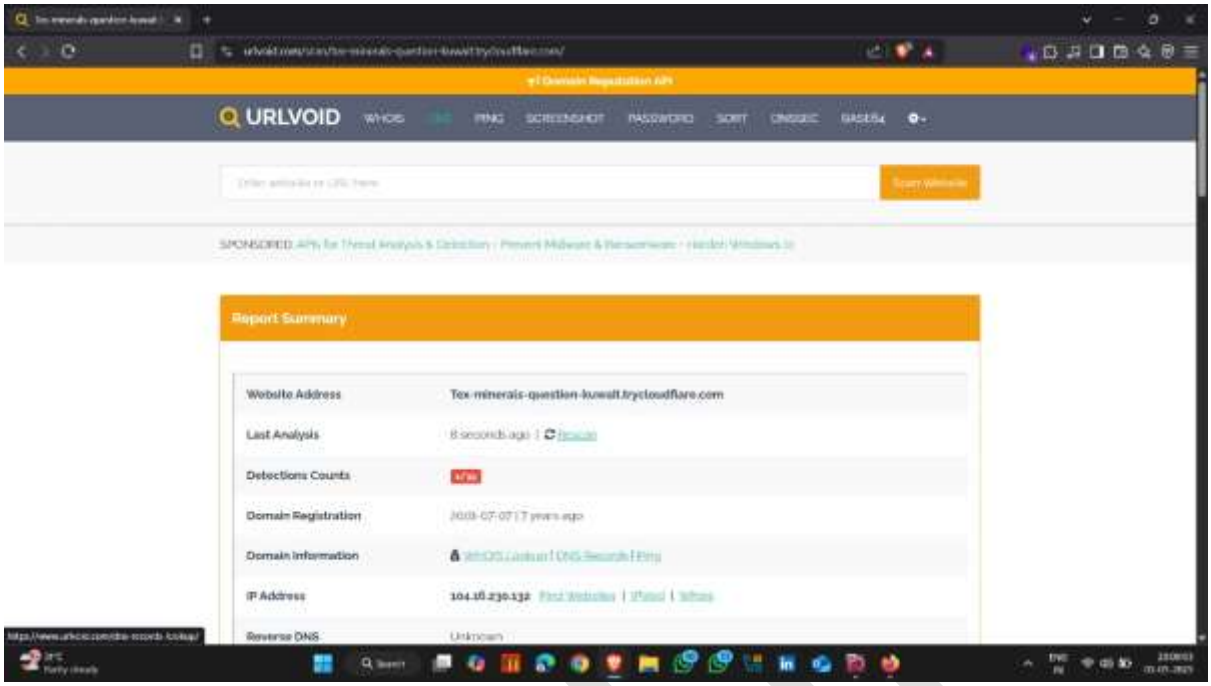


Open the web site

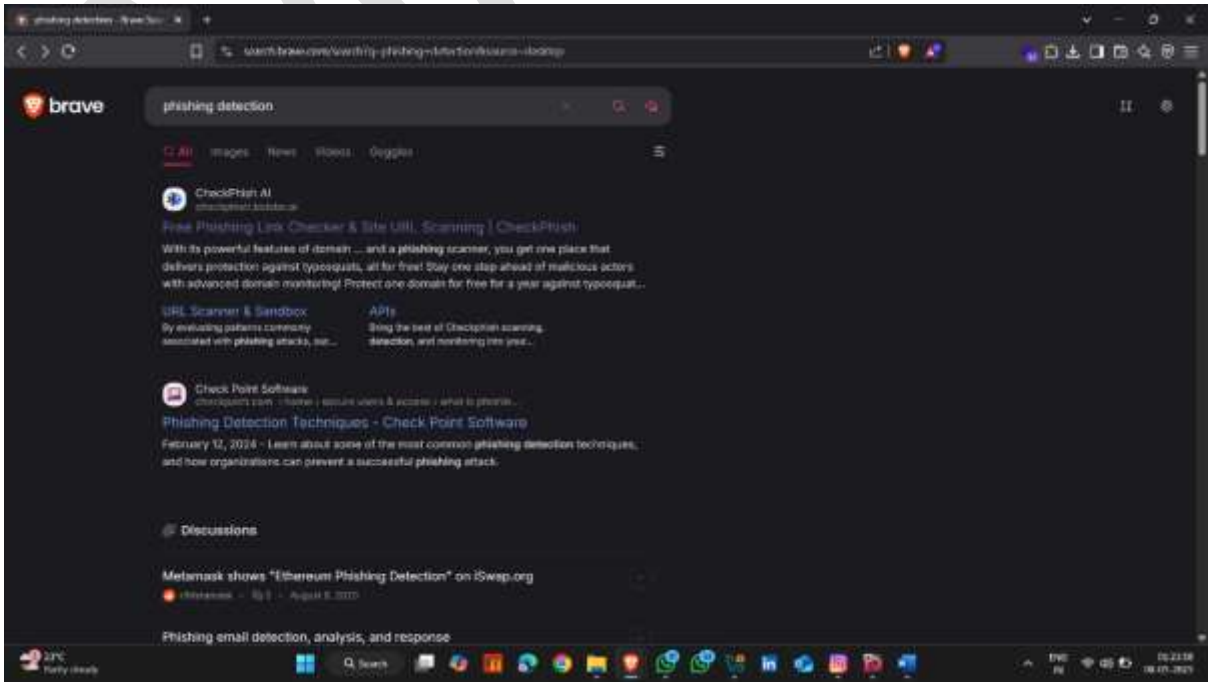


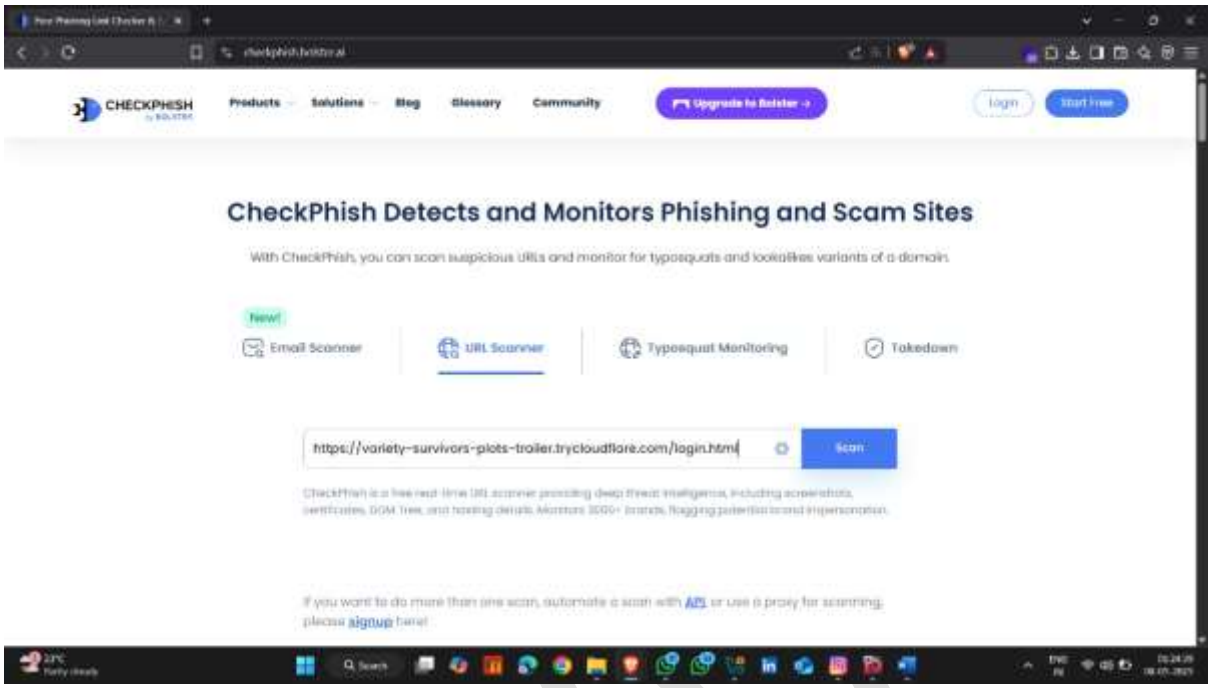


Result :

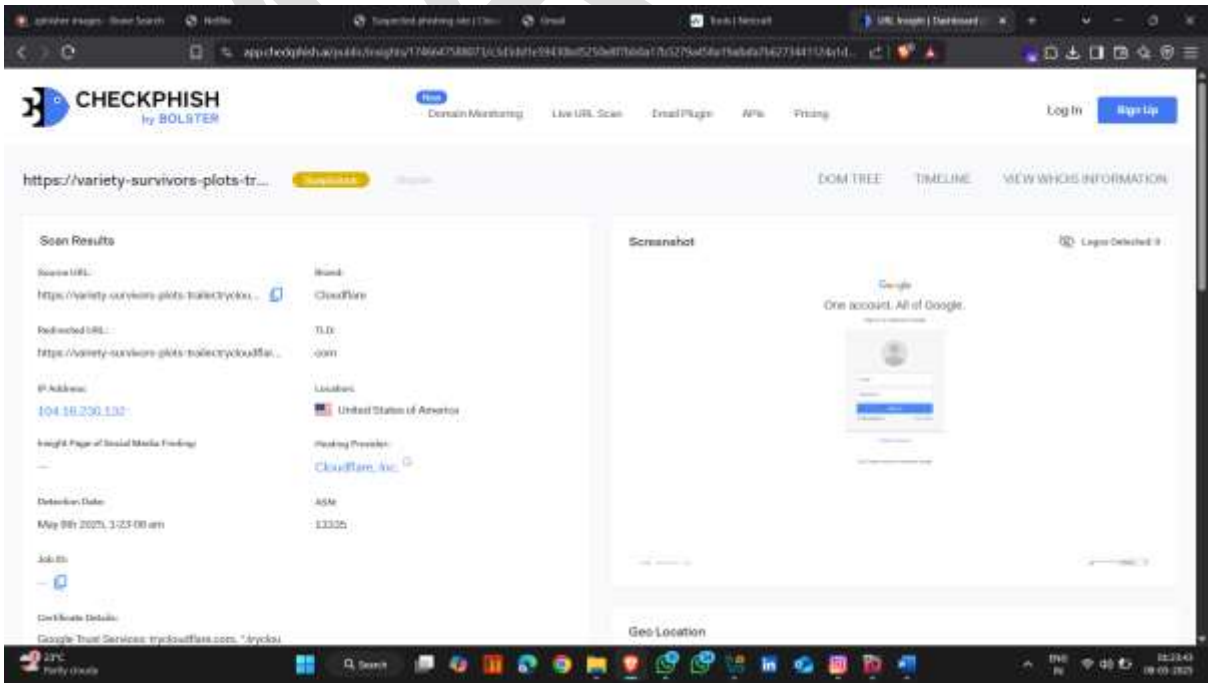


4 Extra Activity using website for fishing URL detections




CHECKPHISH
Products
Solutions
Blog
Glossary
Community
Upgrade to Bolster
Login
Start Free
CheckPhish Detects and Monitors Phishing and Scam Sites
With CheckPhish, you can scan suspicious URLs and monitor for typosquats and lookalikes variants of a domain.
New!
Email Scanner
URL Scanner
Typosquat Monitoring
Takedown
https://variety-survivors-plots-trailer.trycloudflare.com/login.html
Scan
If you want to do more than one scan, automate a scan with API, or use a proxy for scanning,
please signup here!

Result:


CHECKPHISH
by BOLSTER
Domain Monitoring
Live URL Scan
Email Plugin
APIs
Pricing
Log In
Sign Up
https://variety-survivors-plots-tr...
DOM TREE
TIMELINE
VIEW WHOIS INFORMATION
Scan Results
Screenshot
Cloudflare
.com
United States of America
Cloudflare, Inc.
13335
Geo Location