Ciberseguridad en Entornos de las Tecnologías de la Información

Módulo 5021 – Incidentes de Ciberseguridad

Ejercicio – Phishing y Emulación Web

Pliego de Descargo

- *Los ejercicios y conocimientos contenidos en el Módulo 5021, Incidentes de Ciberseguridad, tienen un propósito exclusivamente formativo, por lo que **nunca se deberán utilizar con fines maliciosos o delictivos.***
- *Ni el Ministerio de Educación y Formación Profesional como organismo oficial, ni el CIDEAD como área integrada en el mismo, serán responsables en ningún caso de los daños directos o indirectos que pudieran derivarse del uso inadecuado de las herramientas de hacking ético utilizadas en dichos ejercicios.*

Índice de Contenidos

1. Instalación de un phisher

Ingeniería Social - ¿Qué es un phisher?

- Existen multitud de técnicas, tácticas, herramientas y estrategias de Ingeniería Social, pero la más relevante y potente de todas ellas es el Phishing.
- El Phishing permite emular *websites* auténticos de forma prácticamente idéntica, para robar las credenciales de usuario.
- El usuario casi no nota nada, pues efectúa un primer acceso al falso *website*, introduce sus credenciales y navega un poco, pero algo parece no funcionar bien, por lo que sale de la página, teclea de nuevo la dirección y vuelve a entrar, esta vez ya probablemente al sitio auténtico. Pero ya le han robado los datos.
- Existen muchas herramientas de código abierto denominadas *phishers*, que permiten efectuar este tipo de captura de datos.
- Un *phisher* permite emular muy bien un conjunto de *websites* muy populares, pero también permite al usuario crear a medida el *website* falso que precise.
- En este ejercicio descargaremos un *phisher* desde GitHub y emularemos varias páginas web populares.

Primer Requerimiento – Instalación de php y Apache

- Casi todos los phishers se apoyan en el popular webserver de código abierto Apache.
- Apache es multiplataforma y tiene la ventaja de ser también la base de muchos websites auténticos, lo cual brida aún más similitud.

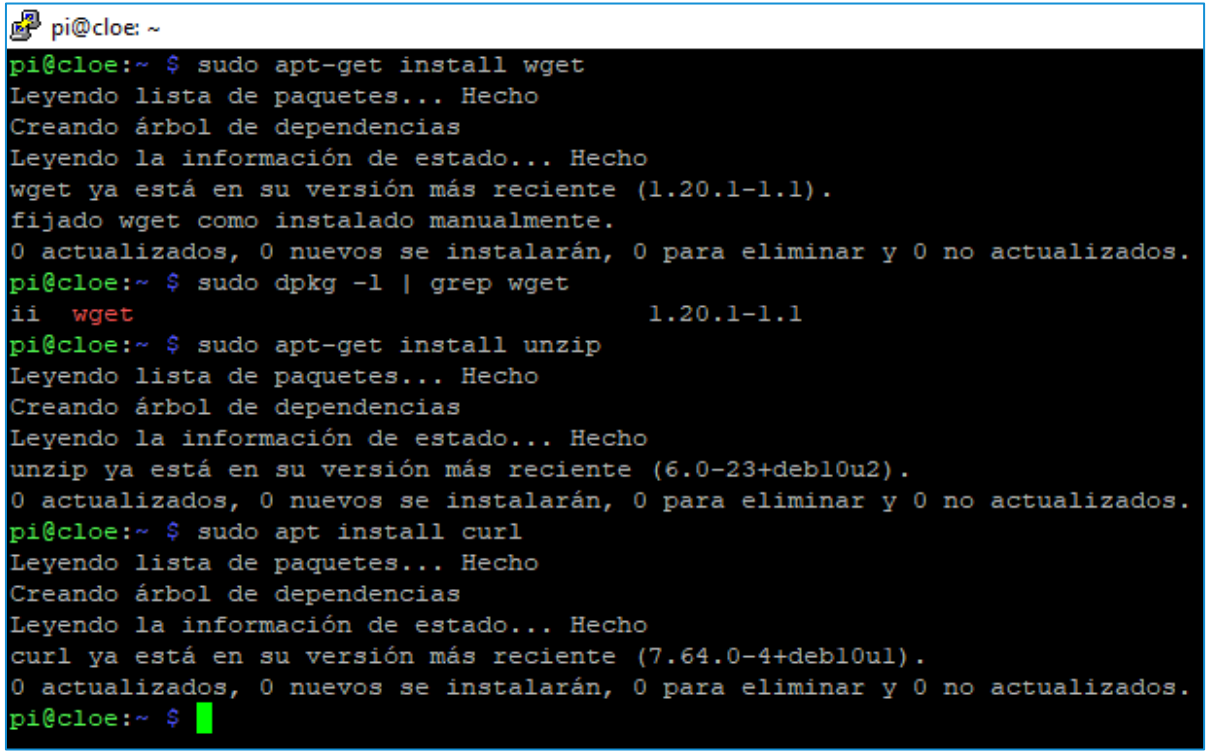

```
pi@cloe: ~
pi@cloe:~ $ sudo apt install php libapache2-mod-php
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php7.3 libaprl
  libaprutill libaprutill-dbd-sqlite3 libaprutill-ldap php-common php7.3
  php7.3-cli php7.3-common php7.3-json php7.3-opcache php7.3-readline
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php
  libapache2-mod-php7.3 libaprl libaprutill libaprutill-dbd-sqlite3
  libaprutill-ldap php php-common php7.3 php7.3-cli php7.3-common php7.3-json
  php7.3-opcache php7.3-readline
0 actualizados, 18 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 4.956 kB de archivos.
Se utilizarán 20,2 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

```
pi@cloe: ~
pi@cloe:~ $ sudo systemctl restart apache2
pi@cloe:~ $
```

Segundo Requerimiento – Instalación de wget, unzip y curl

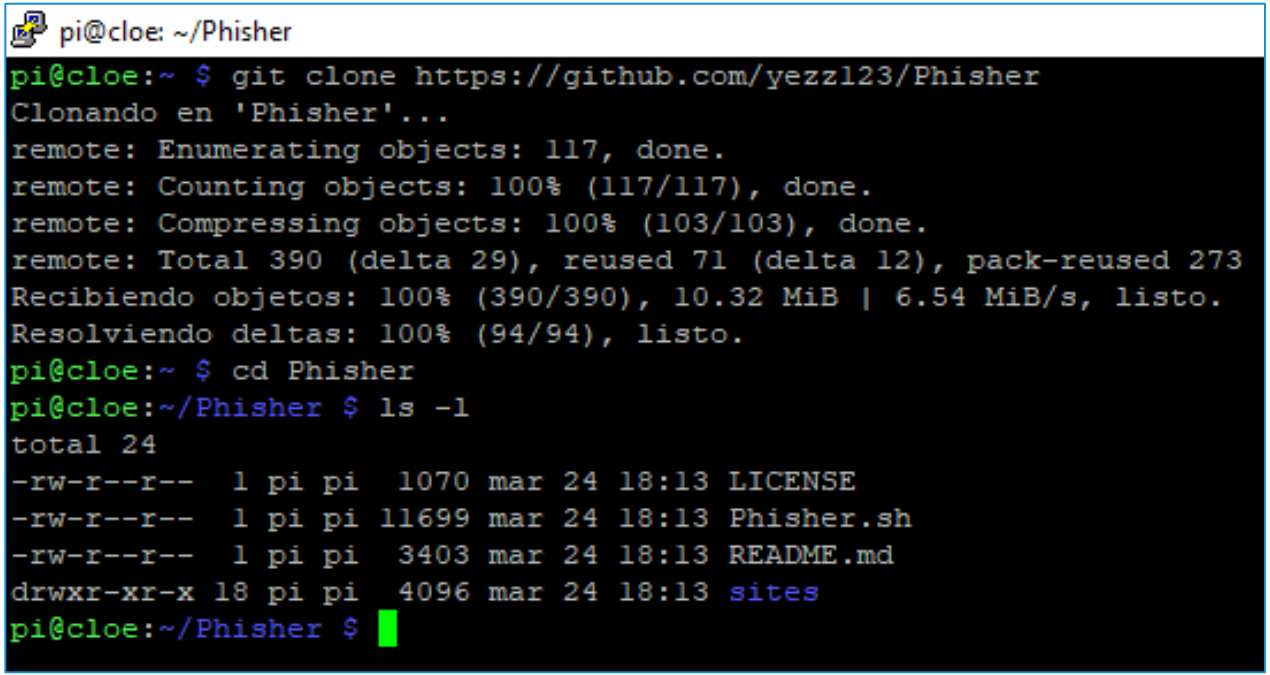
El phisher seleccionado requiere asimismo la instalación de las siguientes herramientas sobre Linux:

- **wget.** Herramienta de descarga de contenidos desde páginas web.
- **unzip.** Descompresor de archivos clásico.
- **curl.** Intérprete de comandos orientado a la transferencia de ficheros.



Clonamos un phisher desde GitHub

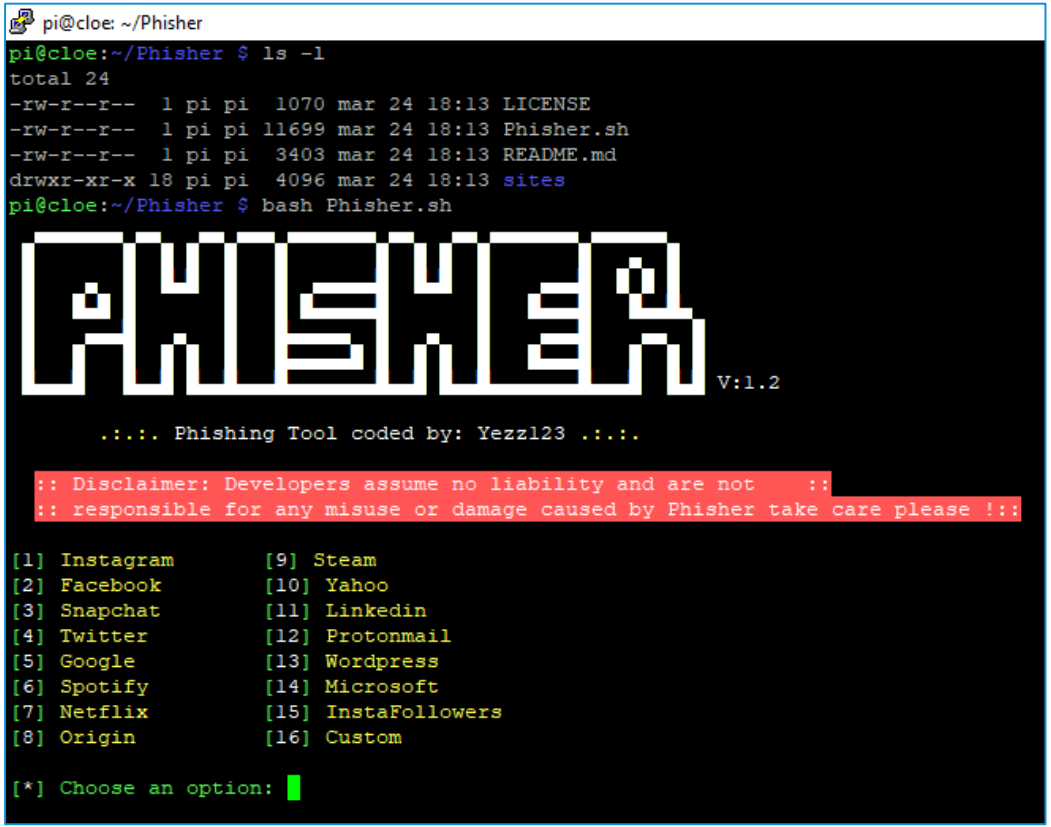
- Para nuestro ejercicio clonaremos desde GitHub un popular phisher de código abierto denominado precisamente, Phisher.
- Como veremos, esta herramienta permite emular fácilmente los sitios web de redes sociales y otros sites muy extendidos.



2. Emulación de Webs

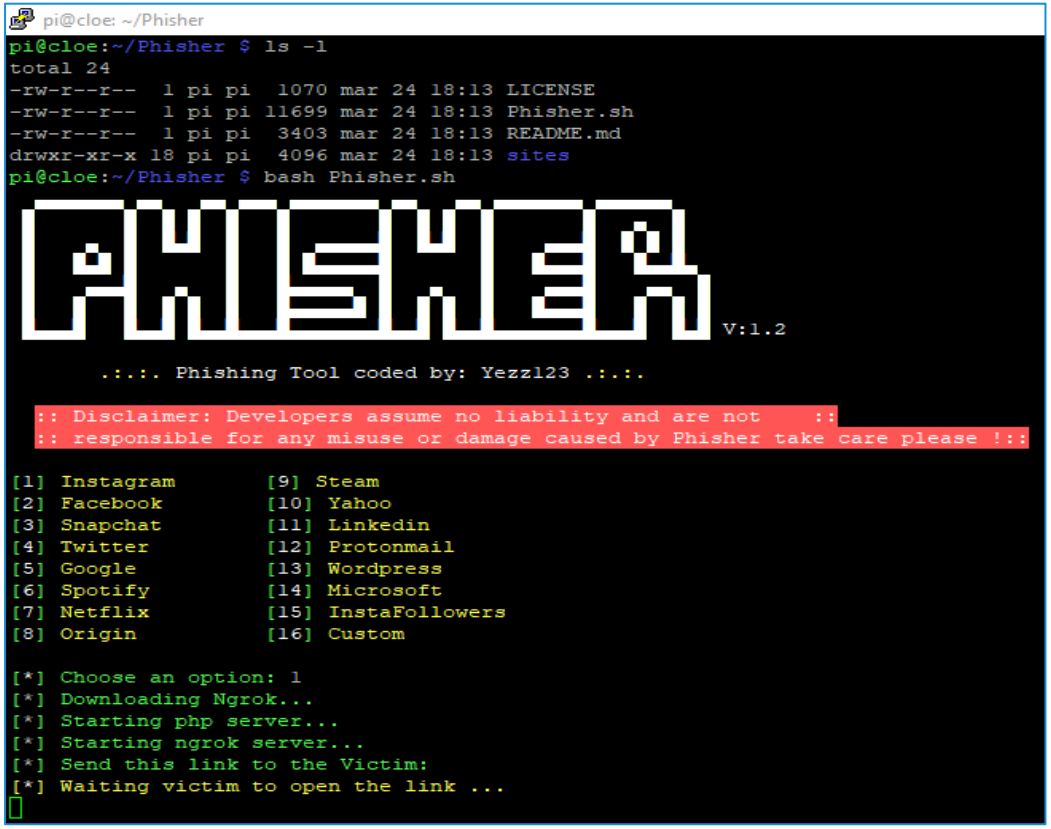
Ejecutamos Phisher

- Además de emular websites populares por defecto, Phisher permite al usuario diseñar su propia emulación para el sitio que desee.
- Tras clonar el SW de la aplicación, procedemos a ejecutarlo con bash, según se indica en sus instrucciones.



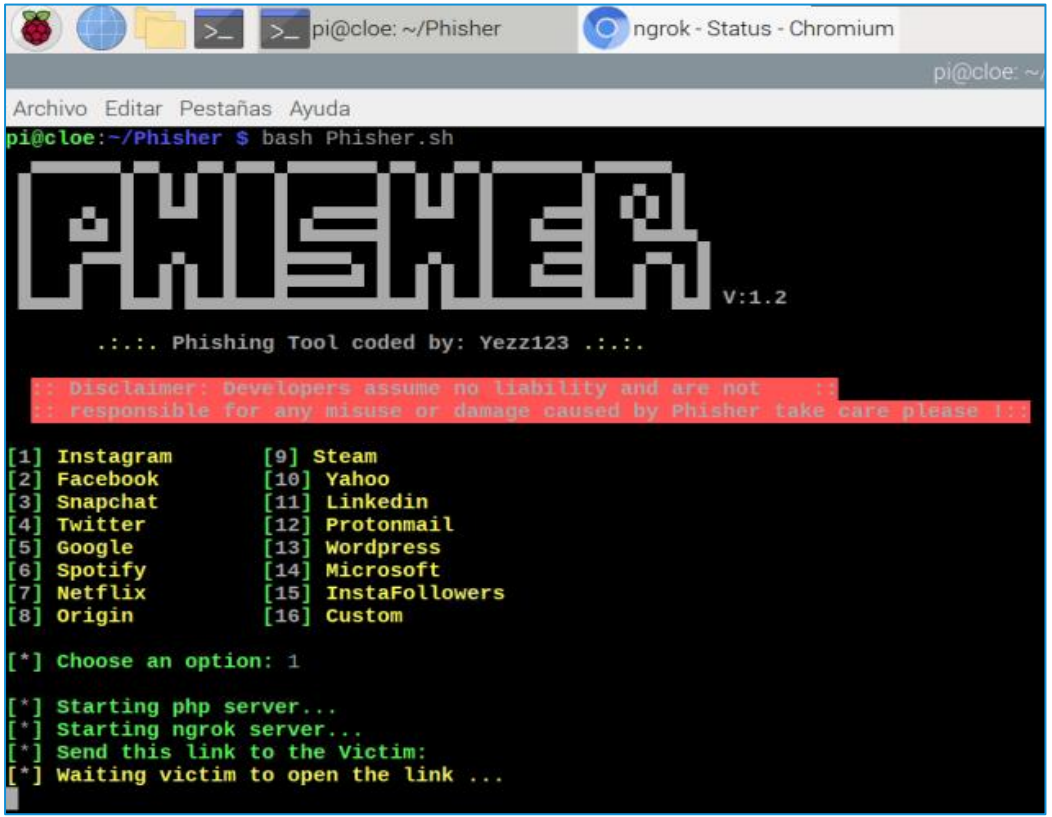
Ingeniería Social

- En la primera ejecución se lanza el servidor php y se descarga automáticamente ngrok.
- Ngrok sirve para exponer en Internet los servidores locales situados tras NATs y cortafuegos, mediante túneles seguros.
- En resumidas cuentas, ngrok permite exponer en Internet un servidor de red que está corriendo en una máquina local, que en nuestro caso estará simulando ser un portal real.



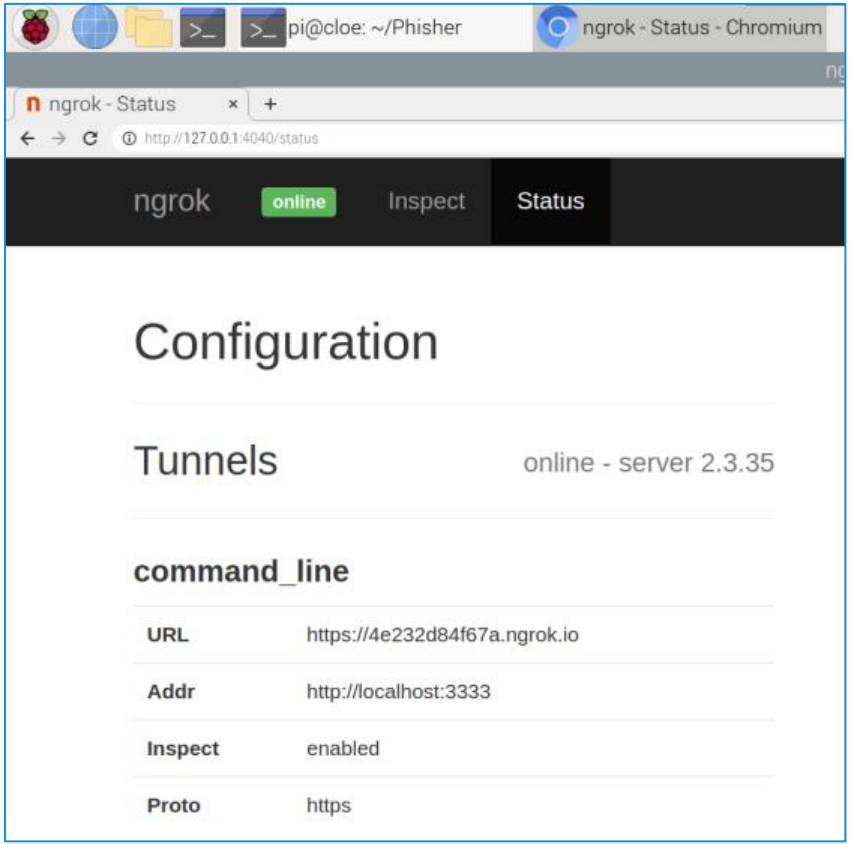
Ingeniería Social

- En nuestro ejercicio emularemos la páginas web reales con objeto de despistar al usuario y hacer que introduzca sus credenciales de acceso.
- **NOTA IMPORTANTE**: Este ejercicio tiene propósito exclusivamente formativo. Las herramientas y procedimientos descritos en él no deben utilizarse bajo ningún concepto para fines maliciosos.



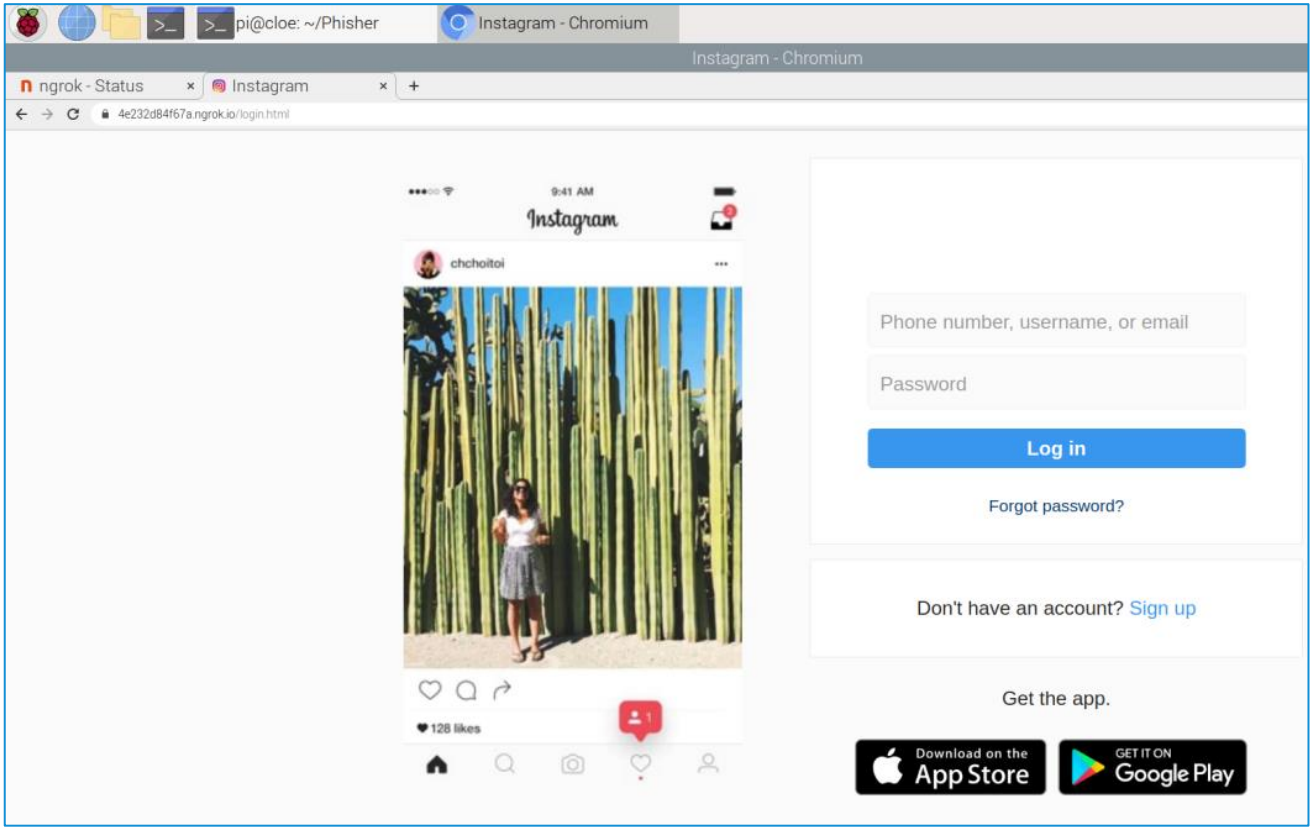
Ingeniería Social

- Una vez lanzado Phisher, accedemos a la página local de ngrok para chequear su status y copiar la dirección URL a enviar al usuario.
- Esta dirección se enviará convenientemente enmascarada, para que parezca la dirección auténtica.



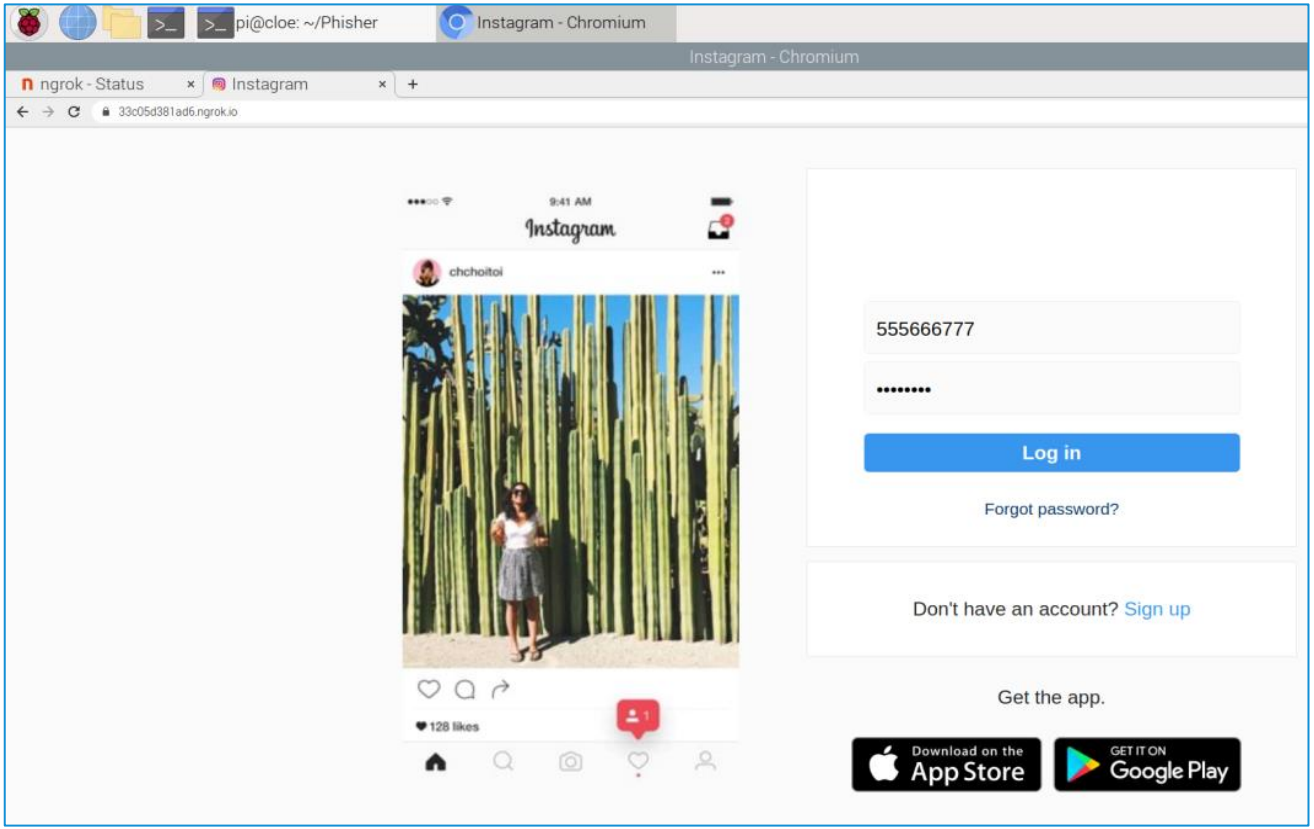
Ingeniería Social

- Se presenta la página falsa, que es prácticamente idéntica a la real.
- Se espera a que el usuario introduzca sus credenciales auténticas.



Ingeniería Social

- Una vez introducidas las credenciales, éstas quedan capturadas inmediatamente.



Ingeniería Social

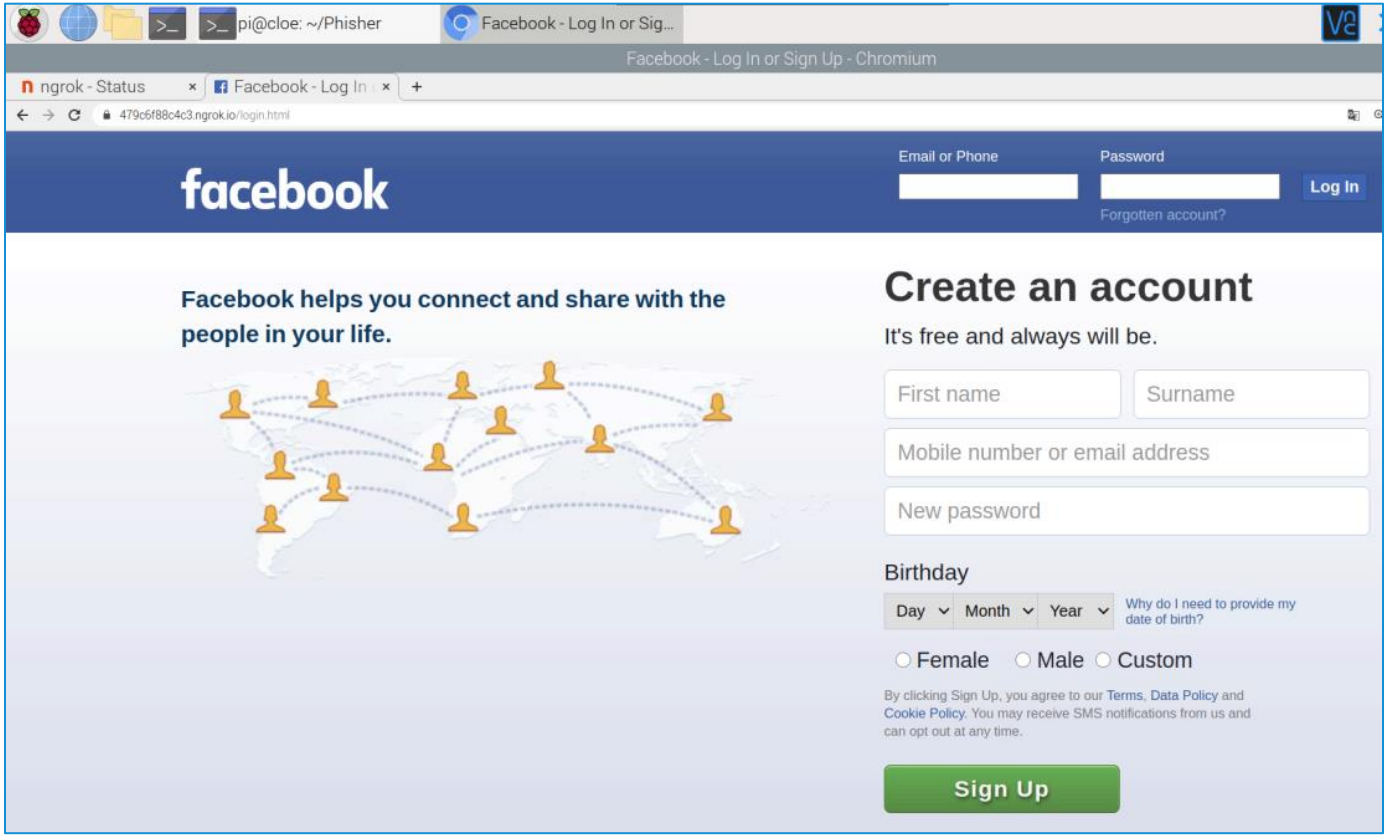
- Las credenciales capturadas en la página falsificada se muestran directamente por pantalla en el terminal que abrió la sesión, y además se almacenan en un fichero de texto ad hoc.

```
[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Victim:
[*] Waiting victim to open the link ...

[*] IP Found!
[*] Victim IP: 83.50.135.235
[*] User-Agent:  User-Agent: Mozilla/5.0 (X11; CrOS armv7l 13597.84.0)
[*] Saved: instagram/saved.ip.txt


[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: 555666777
[*] Password:  miclave1
[*] Saved: sites/instagram/saved.usernames.txt
pi@cloe:~/Phisher $
```

```
[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: 555666777
[*] Password:  miclave1
[*] Saved: sites/instagram/saved.usernames.txt
pi@cloe:~/Phisher $ ls -l
total 23320
-rw-r--r--  1 pi pi     1070 mar 24 18:13 LICENSE
-rwxr-xr-x  1 pi pi 23855086 oct  8  2019 ngrok
-rw-r--r--  1 pi pi    11699 mar 24 18:13 Phisher.sh
-rw-r--r--  1 pi pi     3403 mar 24 18:13 README.md
drwxr-xr-x 18 pi pi     4096 mar 24 18:13 sites
pi@cloe:~/Phisher $ cd sites
pi@cloe:~/Phisher/sites $ cd instagram
pi@cloe:~/Phisher/sites/instagram $ ls -l
total 252
drwxr-xr-x 2 pi pi   4096 mar 24 18:13 index_files
-rw-r--r-- 1 pi pi     64 mar 24 18:13 index.php
-rw-r--r-- 1 pi pi    547 mar 24 18:13 ip.php
-rw-r--r-- 1 pi pi    147 mar 24 18:31 ip.txt
-rw-r--r-- 1 pi pi 222731 mar 24 18:13 login.html
-rw-r--r-- 1 pi pi    181 mar 24 18:13 login.php
-rw-r--r-- 1 pi pi    294 mar 24 18:31 saved.ip.txt
-rw-r--r-- 1 pi pi     34 mar 24 18:35 saved.usernames.txt
-rw-r--r-- 1 pi pi     34 mar 24 18:35 usernames.txt
pi@cloe:~/Phisher/sites/instagram $ cat usernames.txt
Account: 555666777 Pass: miclave1
pi@cloe:~/Phisher/sites/instagram $
```

Ingeniería Social

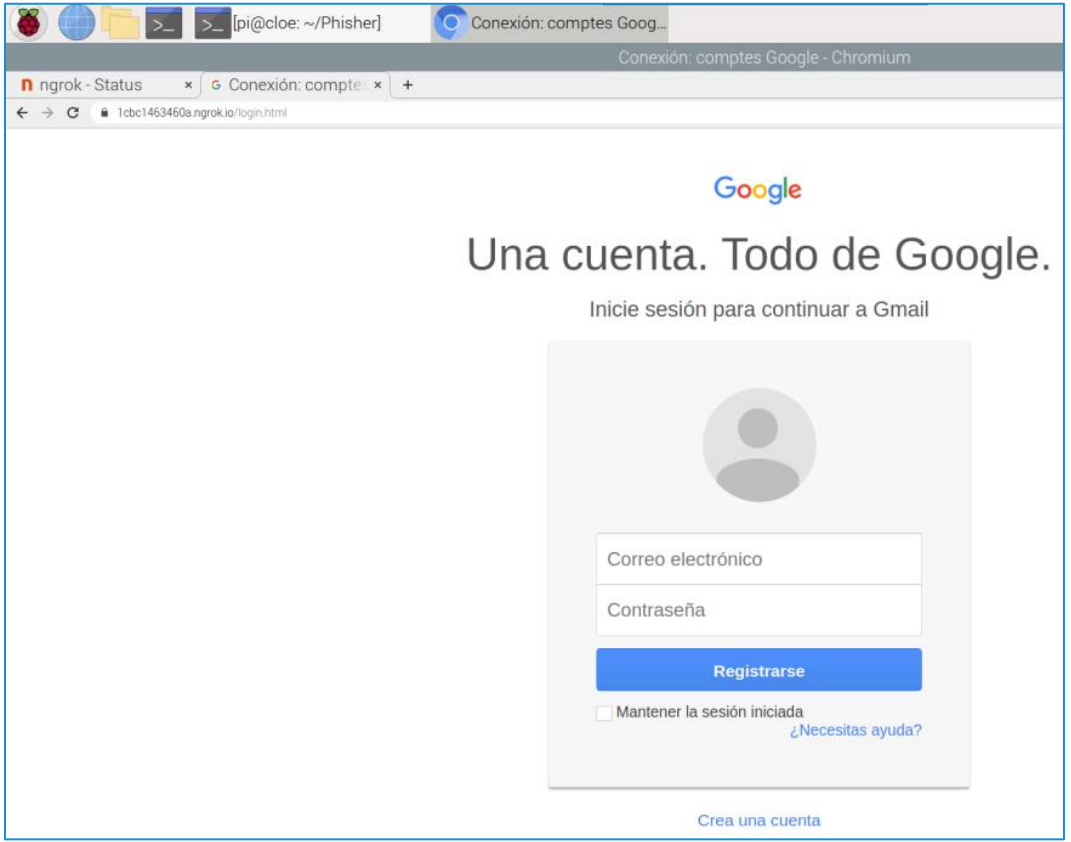
- Ejemplo de emulación de la página real de entrada a Facebook.



Ingeniería Social

- Ejemplo de emulación de la página de entrada a Google y captura de las credenciales de usuario de la forma habitual.

```
[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: pepe.botella@gimail.kom
[*] Password:  miclave2
[*] Saved: sites/google/saved.usernames.txt
pi@cloe:~/Phisher $ cd sites
pi@cloe:~/Phisher/sites $ cd google
pi@cloe:~/Phisher/sites/google $ cat saved.usernames.txt
Account: pepe.botella@gimail.kom Pass: miclave2
pi@cloe:~/Phisher/sites/google $
```



Bibliografía

- www.kali.org
- www.github.com
- www.incibe.es
- www.elastic.co
- https://github.com/yezz123/Phisher
- https://yezz123.github.io/
- https://github.com/yezz123
- https://ngrok.com/