

SURFACE ATTACK MANAGER(SAM)

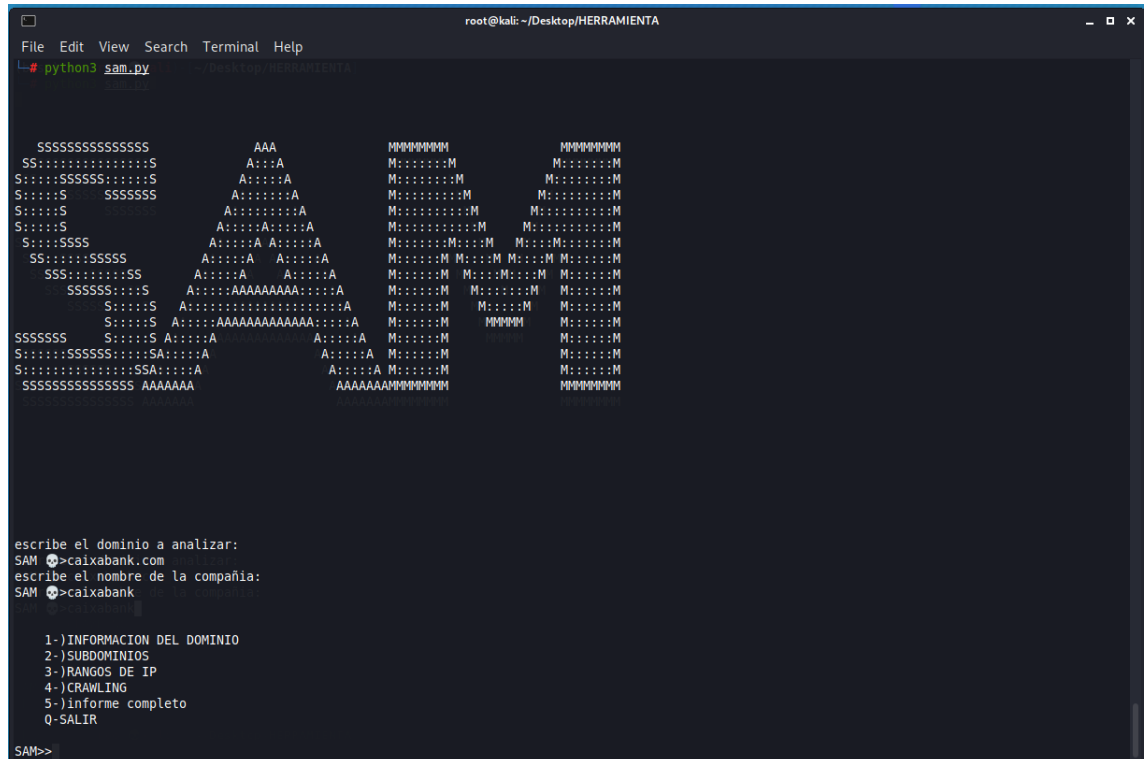
- **REQUISITOS DE FUNCIONAMIENTO**

- ser root (Linux)
- tener el servidor de tor corriendo en 127.0.0.1:9050
- instalar el requirements.txt
- python3 instalado
- estar en la carpeta que contiene el programa
- firefox instalado
- tener conexión a internet

No es requisito, pero es preferible algún database browser como sqlite para comprobar los resultados

- **GUIA DE USO**

1. Python3 sam.py



```
root@kali: ~/Desktop/HERRAMIENTA
File Edit View Search Terminal Help
~# python3 sam.py

SSSSSSSSSSSSSS AAA          MMMMMMMM          MMMMMMMM
SS:.....S      A:::A      M:.....M      M:.....M
S:.....SSSSS:..S      A:..:A      M:.....M      M:.....M
9:.....S      SSSSSSS      A:.....A      M:.....M      M:.....M
9:.....S      A:.....:A      M:.....M      M:.....M
9:.....S      A:.....A:..:A      M:.....M      M:.....M
S:.....SSSS      A:.....A A:.....A      M:.....M      M:.....M
SS:.....SSSSS      A:.....A A:.....A      M:.....M      M:.....M
SSS:.....S      A:.....A A:.....A      M:.....M      M:.....M
SSSSSS:..S      A:.....A A:.....A      M:.....M      M:.....M
SSSSSS:..S      A:.....A A:.....A      M:.....M      M:.....M
S:.....S      A:.....A A:.....A      M:.....M      M:.....M
S:.....S      A:.....A A:.....A      M:.....M      M:.....M
SSSSSSS      S:.....S A:.....A      A:.....A      M:.....M      M:.....M
S:.....SSSSS:..SA:.....A      A:.....A      M:.....M      M:.....M
S:.....SSSSS:..SSA:.....A      A:.....A      M:.....M      M:.....M
SSSSSSSSSSSSSS AAAAAAA      AAAAAAMMMMMMMM      MMMMMMMM

escribe el dominio a analizar:
SAM >caixabank.com
escribe el nombre de la compañía:
SAM >caixabank

1-)INFORMACION DEL DOMINIO
2-)SUBDOMINIOS
3-)RANGOS DE IP
4-)CRAWLING
5-)informe completo
0-)SALIR

SAM>>
```

2. Escribir dominio y nombre de la compañía(es importante escribirlos tal cual porque sino da error)
3. Elegir la opción del menú que se desee

DEMOSTRACION DE USO

- OPCION 1

```
SAM>>1
MOSTRANDO INFORMACION DEL DOMINIO
IP: 217.148.70.201
PUERTOS ABIERTOS
WHOIS
Domain Name: CAIXABANK.COM
Registry Domain ID: 1181732 DOMAIN COM-VRSN
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.EuroDNS.com
Updated Date: 2020-12-14T22:06:24Z
Creation Date: 1996-12-31T05:00:00Z
Registry Expiry Date: 2023-12-22T20:16:49Z
Registrar: EuroDNS S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legal@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.EDGECASTDNS.NET
Name Server: NS1.LACAIXA.COM
Name Server: NS2.EDGECASTDNS.NET
Name Server: NS2.LACAIXA.COM
Name Server: NS3.EDGECASTDNS.NET
Name Server: NS4.EDGECASTDNS.NET
DNSSEC: signedDelegation
DNSSEC DS Data: 44488 5 2 5C9BFC2174AEAA500407991CE02766E8D18DA834001A6E519D43EE8248144E5D
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-05-26T21:04:31
```

NOTA: la función de escanear puertos tarda un tiempo y de vez en cuando falla, provocando a veces fallos en otras funcionalidades

El error es el siguiente, recomiendo que cuando ocurra se vuelva a iniciar la aplicación desde 0 ya que afecta a otras cosas

```
Error trying to connect to socket: closing socket
```

- OPCION 2

```
SAM>>2
MOSTRANDO LISTA DE SUBDOMINIOS
subdominios de caixabank.com obtenidos
www.caixabank.com
3rdadapterpre.caixabank.com
www.3rdadapterpre.caixabank.com
3rdadapterpro.caixabank.com
www.3rdadapterpro.caixabank.com
absis.caixabank.com
www.absis.caixabank.com
pre.absis.caixabank.com
www.pre.absis.caixabank.com
tst.absis.caixabank.com
www.tst.absis.caixabank.com
access.caixabank.com
www.access.caixabank.com
accionista.caixabank.com
m.email.accionista.caixabank.com
r7.email.accionista.caixabank.com
t.email.accionista.caixabank.com
alibaba.caixabank.com
www.alibaba.caixabank.com
api.caixabank.com
apis.caixabank.com
apis2.caixabank.com
apis2pre.caixabank.com
apis2tst.caixabank.com
apisca.caixabank.com
apispre.caixabank.com
apistore.caixabank.com
pre.apistore.caixabank.com
www.pre.apistore.caixabank.com
```

Desarrollo de herramientas de Ciberseguridad

Jose Amo

- OPCION 3

```
SAM>>3
MOSTRANDO RANGOS
*****
INICIO DEL RANGO:217.148.70.0
FINAL DEL RANGO:217.148.70.255
ASN DEL RANGO:AS16383
PROPIETARIO DEL RANGO:Caixabank
*****
INICIO DEL RANGO:217.148.72.0
FINAL DEL RANGO:217.148.72.255
ASN DEL RANGO:AS16383
PROPIETARIO DEL RANGO:Caixabank
*****
INICIO DEL RANGO:213.246.252.112
FINAL DEL RANGO:213.246.252.119
ASN DEL RANGO:AS8220
PROPIETARIO DEL RANGO:Caixabank Asset Management Luxembourg S.A.
*****
INICIO DEL RANGO:62.72.101.192
FINAL DEL RANGO:62.72.101.199
ASN DEL RANGO:AS8220
PROPIETARIO DEL RANGO:Caixabank Asset Management Luxembourg S.A.
*****
2 SUBDOMINIOS
```

- OPCION 4

```
SAM>>4
RESULTADO DEL CRAWLER
caixabank.com/es/cookies_es.html#cookies_propias
caixabank.com/es/cookies_es.html#cookies_propias
caixabank.comjavascript:void(0)
caixabank.comhttps://twitter.com/caixabank
caixabank.comhttps://www.facebook.com/caixabank
caixabank.comhttps://www.instagram.com/caixabank/?hl=es
caixabank.comhttps://www.linkedin.com/company/caixabank
caixabank.comhttps://www.youtube.com/c/caixabank
caixabank.comhttps://www.caixabank.com/es/home_es.html
caixabank.comhttps://www.caixabank.com/ca/home_ca.html
caixabank.comhttps://www.caixabank.com/en/home_en.html
caixabank.comhttps://www.caixabank.es/particular/home/particulares_es.html
caixabank.com/es/sobre-nosotros.html
caixabank.com/es/sobre-nosotros/conocenos/nuestra-identidad.html
caixabank.com/es/sobre-nosotros/conocenos/mision-vision-valores.html
caixabank.com/es/sobre-nosotros/conocenos/nuestra-marca.html
caixabank.com/es/sobre-nosotros/conocenos/lineas-estrategicas.html
caixabank.com/es/sobre-nosotros/nuestro-negocio/modelo-negocio.html
caixabank.com/es/sobre-nosotros/nuestro-negocio/principales-datos.html
caixabank.com/es/sobre-nosotros/grupo-caixabank.html
caixabank.com/es/sobre-nosotros/publicaciones.html
caixabank.com/es/sobre-nosotros/reconocimientos.html
caixabank.com/es/sobre-nosotros/innovacion.html
caixabank.com/es/sobre-nosotros/nuestros-patrocinios/valores-apoyamos.html
caixabank.com/es/sobre-nosotros/nuestros-patrocinios/futbol.html
caixabank.com/es/sobre-nosotros/nuestros-patrocinios/baloncesto.html
caixabank.com/es/sobre-nosotros/nuestros-patrocinios/deporte-adaptado.html
caixabank.com/es/sobre-nosotros/nuestros-patrocinios/running.html
caixabank.com/es/sobre-nosotros/nuestros-patrocinios/innovacion-desarrollo-economico-social.html
caixabank.com/es/accionistas-inversores/informacion-general/fusiones.html
caixabank.com/es/sostenibilidad.html
caixabank.com/es/sostenibilidad/banca-socialmente-responsable/nuestro-modelo.html
caixabank.com/es/sostenibilidad/banca-socialmente-responsable/comite-de-responsabilidad-corporativa-y-reputacion.html
caixabank.com/es/sostenibilidad/banca-socialmente-responsable/ods.html
caixabank.com/es/sostenibilidad/banca-socialmente-responsable/comunicacion-dialogo.html
caixabank.com/es/sostenibilidad/banca-socialmente-responsable/asociaciones-adhesiones-alianzas.html
```

- OPCION 5

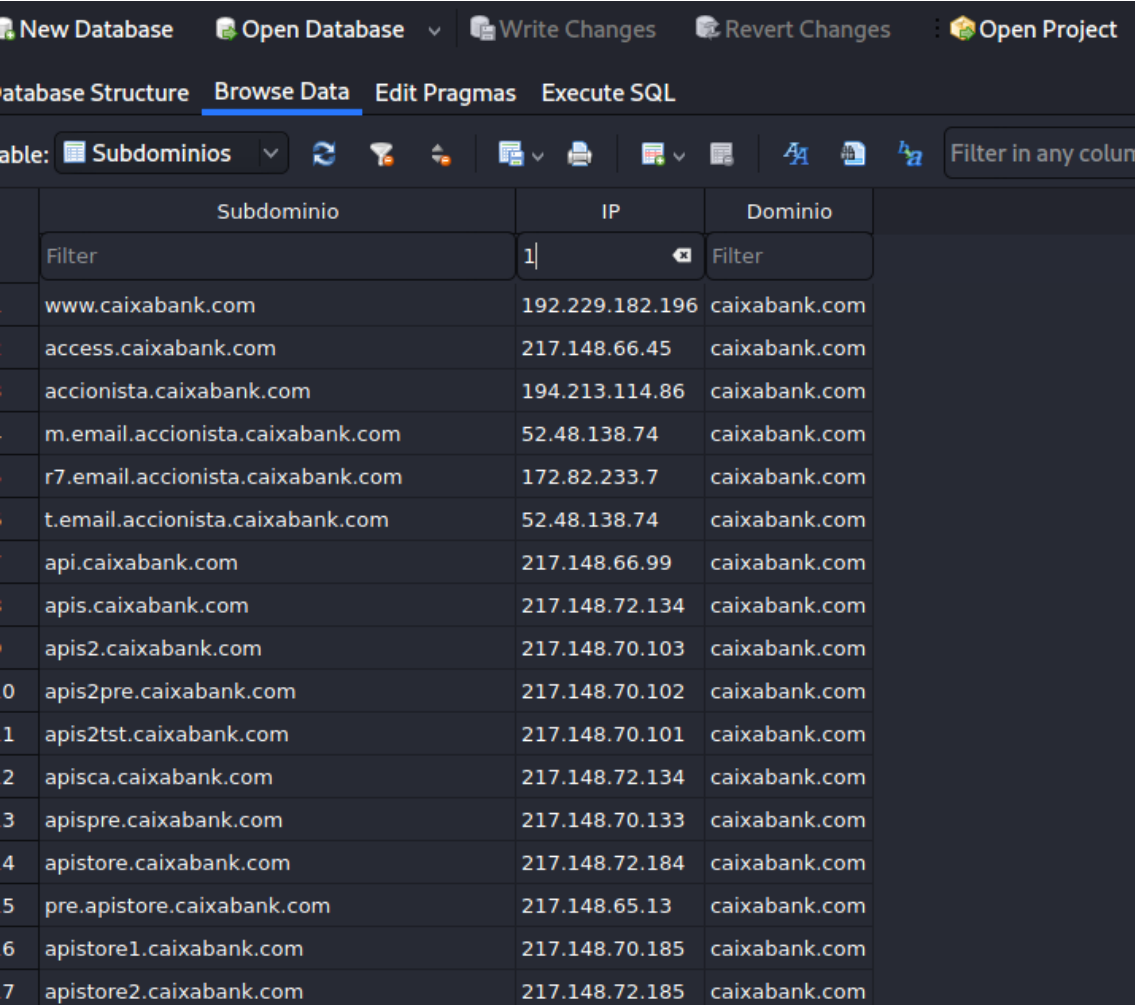
```

[...trying to connect to socket, closing socket]
SAM>>5
GENERANDO INFORME
1-) INFORMACION DEL DOMINIO
2-) SUBDOMINIOS
1-) INFORMACION DEL DOMINIO
2-) SUBDOMINIOS
3-) RANGOS DE IP
4-) CRAWLING
5-) informe completo
SAM: Q-SALIR
GENERANDO INFORME
SAM>>
```

No genera ningún output por consola, pero crea los siguientes archivos

Compañía_data.db:

Tabla “subdominios”



Subdominio	IP	Dominio
Filter	1	Filter
www.caixabank.com	192.229.182.196	caixabank.com
access.caixabank.com	217.148.66.45	caixabank.com
accionista.caixabank.com	194.213.114.86	caixabank.com
m.email.accionista.caixabank.com	52.48.138.74	caixabank.com
r7.email.accionista.caixabank.com	172.82.233.7	caixabank.com
t.email.accionista.caixabank.com	52.48.138.74	caixabank.com
api.caixabank.com	217.148.66.99	caixabank.com
apis.caixabank.com	217.148.72.134	caixabank.com
apis2.caixabank.com	217.148.70.103	caixabank.com
apis2pre.caixabank.com	217.148.70.102	caixabank.com
apis2tst.caixabank.com	217.148.70.101	caixabank.com
apisca.caixabank.com	217.148.72.134	caixabank.com
apispre.caixabank.com	217.148.70.133	caixabank.com
apistore.caixabank.com	217.148.72.184	caixabank.com
pre.apistore.caixabank.com	217.148.65.13	caixabank.com
apistore1.caixabank.com	217.148.70.185	caixabank.com
apistore2.caixabank.com	217.148.72.185	caixabank.com

Desarrollo de herramientas de Ciberseguridad

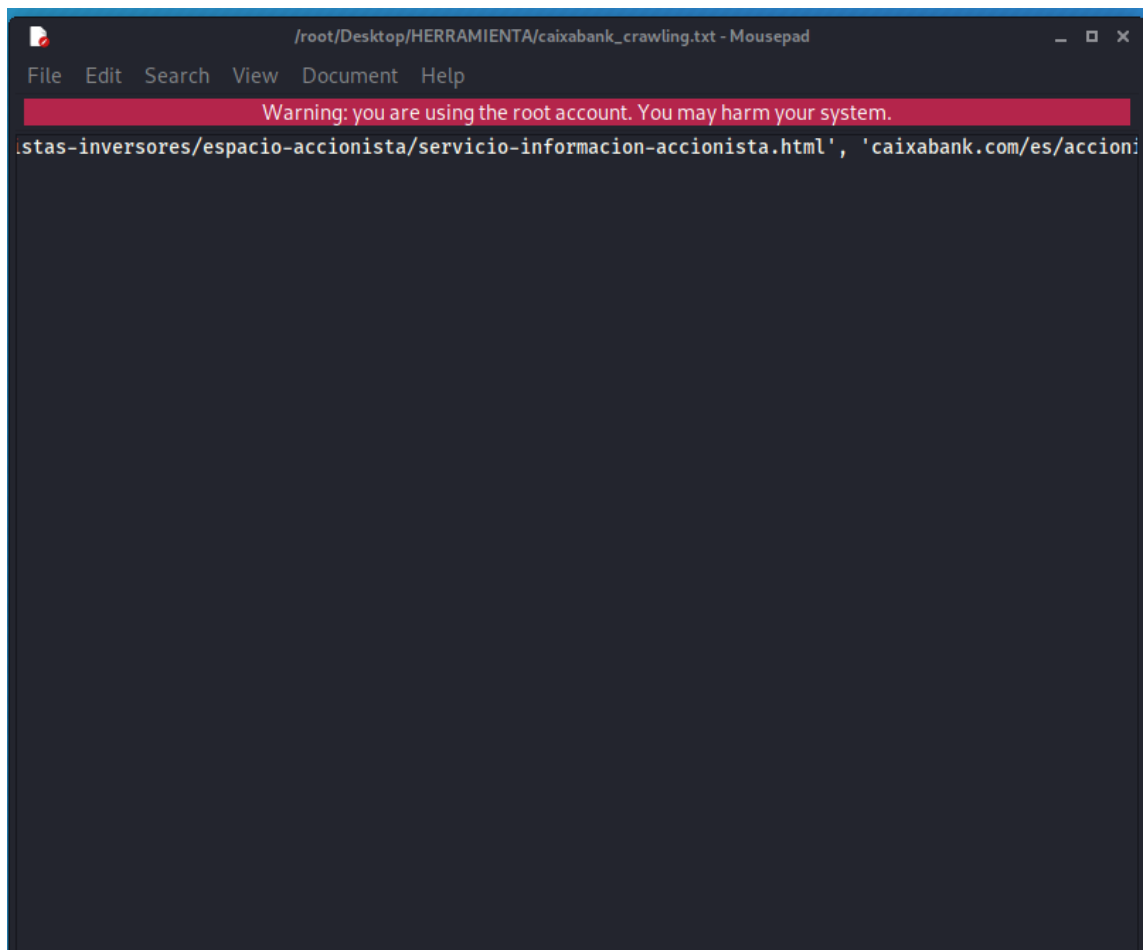
Jose Amo

Tabla "rangos"

Table: rangos				
	Inicio_rango	Final_rango	ASN	Propietario
	Filter	Filter	Filter	Filter
1	217.148.70.0	217.148.70.255	AS16383	Caixabank
2	217.148.72.0	217.148.72.255	AS16383	Caixabank
3	213.246.252.112	213.246.252.119	AS8220	Caixabank Asset Management Luxembour...
4	62.72.101.192	62.72.101.199	AS8220	Caixabank Asset Management Luxembour...
5	217.148.70.0	217.148.70.255	AS16383	Caixabank
6	217.148.72.0	217.148.72.255	AS16383	Caixabank
7	213.246.252.112	213.246.252.119	AS8220	Caixabank Asset Management Luxembour...
8	62.72.101.192	62.72.101.199	AS8220	Caixabank Asset Management Luxembour...

Compañía.txt

```
/root/Desktop/HERRAMIENTA/caixabank.txt - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
IP: 217.148.72.201
PUERTOS ABIERTOS:
WHOIS: Domain Name: CAIXABANK.COM
Registry Domain ID: 1181732_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.EuroDNS.com
Updated Date: 2020-12-14T22:06:24Z
Creation Date: 1996-12-31T05:00:00Z
Registry Expiry Date: 2023-12-22T20:16:49Z
Registrar: EuroDNS S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legal@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.EDGECASTDNS.NET
Name Server: NS1.LACAIXA.COM
Name Server: NS2.EDGECASTDNS.NET
Name Server: NS2.LACAIXA.COM
Name Server: NS3.EDGECASTDNS.NET
Name Server: NS4.EDGECASTDNS.NET
DNSSEC: signedDelegation
DNSSEC DS Data: 44488 5 2 5C9BFC2174AEAA500407991CE02766E8D18DA834001A6E519D43EE8248144E5D
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-05-26T21:12:47
```



No se ve muy bien pero es el resultado del crawling, que lo pone en una única línea

- FUNCIONALIDADES NO IMPLEMENTADAS

-Busqueda de correos o credenciales filtradas: No he podido porque la pagina en la que estuve intentando hacerlo (pwndb) no tenia un certificado seguro y no me dejaba scrapearla algunas veces por lo que fallaba habitualmente

-Busqueda de dominios asociados: no he encontrado ninguna herramienta con la que hacer esto

- EJEMPLOS DE COMBINACIONES DOMINIO/COMPAÑÍA QUE ME HAN FUNCIONADO

- Dominio:caixabank.com Compañía:caixabank
- Dominio:Bankia.es Compañía:bankia
- Dominio:mnemo.com Compañía:mnemo
- Dominio:everis.com Compañía:everis
- Dominio:Mercadona.es Compañía:mercadona
-

