



# Mística

Canales encubiertos sobre  
HTTP/s, DNS e ICMP  
(por ahora)

# # whoami

Raúl Caro (AKA Secury)

Analista de Seguridad en INCIDE

Staff de Bitup Alicante plataforma de jornadas de ciberseguridad creada por y para estudiantes (@bitupalicante)

Desarrollador de Mística, tu amigable contrabandista de datos, con Carlos Fernández (AKA Charlie)

Twitter: @secu\_x11



# CANALES ENCUBIERTOS



- Se utilizan para transferir información entre máquinas
- Usan medios que no habían sido diseñados para ese propósito.
- Los participantes de la comunicación tienen que acordar cómo van a codificar los datos.

# Algunos ejemplos (dns)

ip.addr == 10.10.10.2

No.	Time	Source	Destination	Protocol	Leng	Info
4	0.002486714	10.10.10.1	10.10.10.2	ICMP	109	Destination unreachable (Port unreachable)
5	4.527688972	10.10.10.1	10.10.10.2	DNS	46	Unknown operation (12) 0x7077[Malformed Packet]
6	4.528039830	10.10.10.2	10.10.10.1	ICMP	74	Destination unreachable (Port unreachable)
7	4.528730106	10.10.10.2	10.10.10.1	DNS	76	Unknown operation (13) 0x2f68[Malformed Packet]
8	4.528758003	10.10.10.1	10.10.10.2	ICMP	104	Destination unreachable (Port unreachable)
13	7.602068615	10.10.10.1	10.10.10.2	DNS	45	[Malformed Packet]
14	7.602378530	10.10.10.2	10.10.10.1	ICMP	73	Destination unreachable (Port unreachable)
15	7.604002612	10.10.10.2	10.10.10.1	DNS	81	Unknown operation (12) 0x7569[Malformed Packet]
16	7.604031428	10.10.10.1	10.10.10.2	ICMP	109	Destination unreachable (Port unreachable)

▶ Frame 7: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0  
 ▶ Ethernet II, Src: Vmware\_e4:c0:ab (00:0c:29:e4:c0:ab), Dst: Vmware\_29:b8:bf (00:0c:29:29:b8:bf)  
 ▶ Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.10.10.1  
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 2000  
 ▶ Domain Name System (query)

0000	00 0c 29 29 b8 bf 00 0c 29 e4 c0 ab 08 00 45 00	..)).... ).....E.
0010	00 3e 03 e8 40 00 40 11 0e b1 0a 0a 0a 02 0a 0a	.>...@.@. ....
0020	0a 01 00 35 07 d0 00 2a 04 64 2f 68 6f 6d 65 2f	...5...* .d/home/
0030	61 61 72 74 69 2f 44 6f 77 6e 6c 6f 61 64 73 2f	aarti/Do wnloads/
0040	74 75 6e 6e 65 6c 73 68 65 6c 6c 0a	tunnelsh ell.



# Otros ejemplos (icmp)

Filter:  Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
61	140.5616980	Vmware_77:61:88	Vmware_3e:79:38	ARP	60	192.168.121.135
62	140.5617020	192.168.121.133	192.168.121.135	TCP	74	46042→80 [SYN] S
63	140.5829830	192.168.121.135	192.168.121.133	TCP	74	80→46042 [SYN, A
64	140.5830140	192.168.121.133	192.168.121.135	TCP	66	46042→80 [ACK] S
65	140.6563910	192.168.121.134	192.168.121.133	ICMP	432	Echo (ping) requ
66	140.6564180	192.168.121.133	192.168.121.134	ICMP	432	Echo (ping) repl

Sequence number (BE): 1 (0x0001)  
 Sequence number (LE): 256 (0x0100)  
[\[Response frame: 66\]](#)

0020 79 85 08 00 11 ec da 8c 00 01 d5 20 08 80 00 00 y.....  
 0030 00 00 00 00 00 00 40 00 00 02 00 00 ff ff 00 00  
 0040 01 6a 00 01 da 8c 47 45 54 20 2f 6c 61 75 6e 63 .j....GE T /launc  
 0050 68 65 72 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 her/ HTT P/1.1..H  
 0060 6f 73 74 3a 20 6c 6f 63 61 6c 68 6f 73 74 3a 38 ost: loc alhost:8  
 0070 30 38 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 080..Use r-Agent:  
 0080 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1  
 0090 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b l; Linux x86\_64;  
 00a0 20 72 76 3a 33 31 2e 30 29 20 47 65 63 6b 6f 2f rv:31.0 ) Gecko/  
 00b0 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 20100101 Firefox

# Usos de los Canales Encubiertos

## Perfil RED:

- Ocultar la comunicación con el C2
- Posibilidad de establecer comunicación hacia el exterior en entornos restrictivos
- Evadir las medidas de seguridad perimetrales

## Perfil BLUE y GRAY:

- Capacidad de extracción de artefactos en entornos muy restrictivos
- Proteger el canal de comunicación ante agentes externos
- Medidas para evitar la censura y mejorar la privacidad del usuario

# Funcionalidades Deseadas

Algunas de las funcionalidades a conseguir:

- Transferencia de Ficheros a nivel binario
- Comandos a ejecutar en cualquier extremo
- Información de otros protocolos que se van a encapsular

No importa el protocolo a utilizar, sino cómo se encapsulan los datos y se procesan.



# Problemas en canales encubiertos

Se presentan algunos problemas en la comunicación:

- Protocolos Unidireccionales (Request/Response)
- Pérdida de paquetes
- Desincronización
- Protocolos inseguros que no protegen la información
- Espacio datos disponible por el protocolo limitado
- Codificación de la información a transmitir



# Protocolos y Encapsulación (http)

```
POST / HTTP/1.1
Host: example.com
Accept: */*
User-Agent: mistica-dev
Content-Length: 21
Content-Type: application/x-www-form-urlencoded

data=test&data2=test2
```

Diagram illustrating the components of an HTTP POST request:

- URI PATH (GET & POST)**: Points to the `/` in the request line.
- HEADER (GET & POST)**: Points to the `User-Agent: mistica-dev` header.
- POST FIELD (POST)**: Points to the `data=test&data2=test2` body data.

# Protocolos y Encapsulación (dns)

mistica.dev

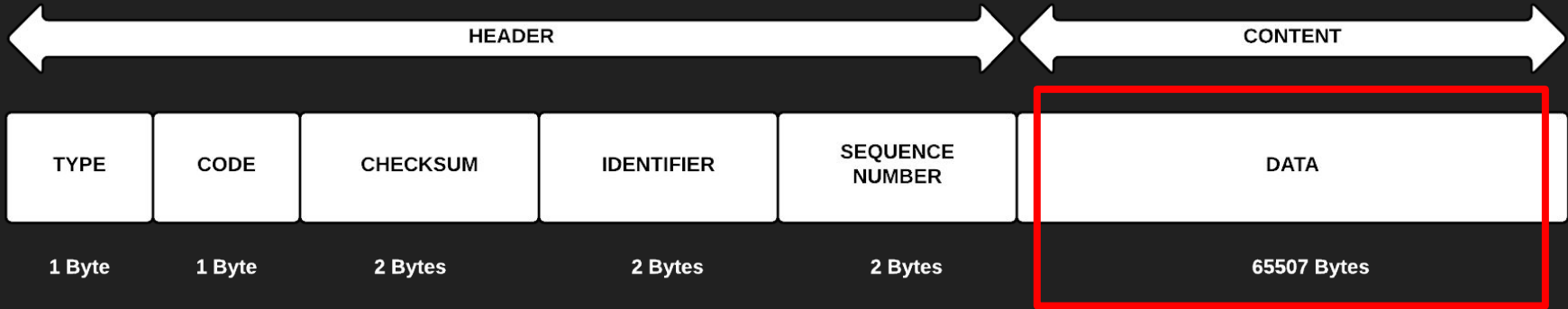
another.example.mistica.dev

ZGF0b3Mgc2VjcmV0b3M.mistica.dev

¿Alguien ha dicho DNSSEC?

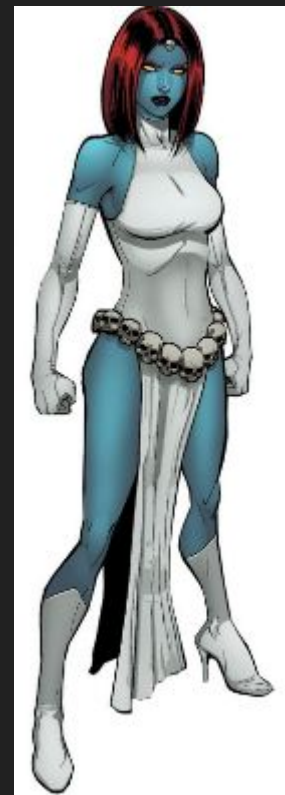


# Protocolos y Encapsulación (icmp)



# ¿Qué es Mística?

- Navaja suiza para el encapsulado de comunicaciones sobre protocolos de aplicación
- Basada en un protocolo de transporte custom llamado **SOTP (Simple Overlay Transport Protocol)**
- Tiene dos tipos de módulos:
  - **Wrappers:** encargados de codificar los paquetes SOTP en el protocolo que se utilice para la comunicación (HTTP, DNS, ICMP, etc)
  - **Overlays:** encargados de proporcionar una funcionalidad al canal (redirección IO, Shell, Port Forwarding, etc)
- Multiplataforma y Software Libre



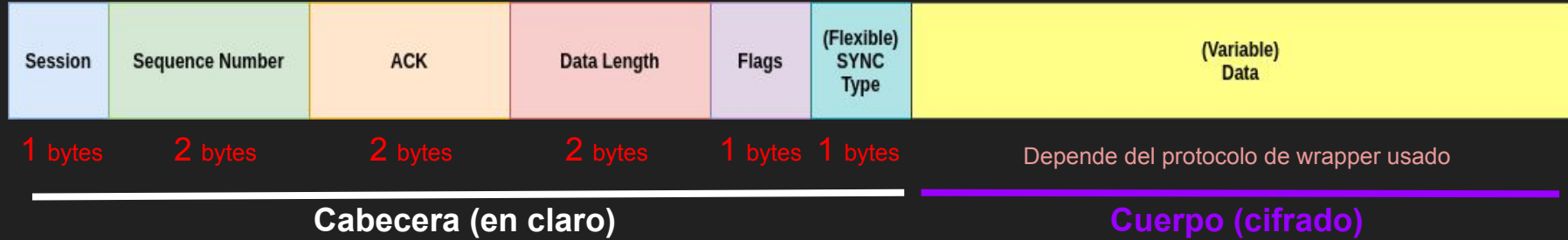
# ¿Qué es SOTP?

- Protocolo de transporte **minimalista**: Cabecera de 8 bytes. Tamaño de los datos variable
- **Garantiza recepción**
- La información se transmite en el transcurso de **sesiones**
- **Etiquetas**: permite multiplexar varias sesiones por el mismo protocolo, pudiendo conectar varios extremos
- **Cifrado** de los datos por defecto





# Estructura Paquete SOTP



## Flags:

- PUSH (pasar datos al overlay)
- SYNC (acciones de sync)



- Request Session
- Response Session
- Polling Request
- Session Termination
- Session Re-initialization

# Características de SOTP

- Bidireccionalidad en la comunicación (Polling -> canal simétrico)
- Confirmación de paquetes (ACKs)
- Numeración de paquetes (Sequence Number)
- Cifrado de los datos (por ahora RC4)
- Extensión del canal de datos dependiendo del protocolo en uso (DNS\*)
- Codificación de la información de los overlays (por ahora Base64)

Algunas de sus características resuelven los problemas mencionados.

# Apariencia de un paquete SOTP

6	0.023889915	192.168.122.3	192.168.122.209	DNS	89 Standard query 0x33f2 TXT fH5YflcAAAA=.customdomain.com
7	0.034666029	192.168.122.209	192.168.122.3	DNS	162 Standard query response 0x33f2 TXT fH5YflcAAAA=.customdomain.com TXT
10	0.043815112	192.168.122.3	192.168.122.209	DNS	100 Standard query 0xea6d TXT fH5ZflgAAAA=.customdomain.com OPT
11	0.048373797	192.168.122.209	192.168.122.3	DNS	162 Standard query response 0xea6d TXT fH5ZflgAAAA=.customdomain.com TXT
14	0.054513476	192.168.122.3	192.168.122.209	DNS	89 Standard query 0xae5 TXT fH5af1kAAAA=.customdomain.com
15	0.058844251	192.168.122.209	192.168.122.3	DNS	138 Standard query response 0xae5 TXT fH5af1kAAAA=.customdomain.com TXT
18	0.066929845	192.168.122.3	192.168.122.209	DNS	100 Standard query 0x4695 TXT fH5bflaAAAEF.customdomain.com OPT
19	0.070858423	192.168.122.209	192.168.122.3	DNS	114 Standard query response 0x4695 TXT fH5bflaAAAEF.customdomain.com TXT
22	0.128025990	192.168.122.3	192.168.122.209	DNS	137 Standard query 0x6e62 TXT fH5cf1sAJQBEx5r9gFapxDQXgYhxEcM7WR08yKFE-omQYhvx0_U7nFxm80Y5.customdomain.com
23	0.138114517	192.168.122.209	192.168.122.3	DNS	162 Standard query response 0x6e62 TXT fH5cf1sAJQBEx5r9gFapxDQXgYhxEcM7WR08yKFE-omQYhvx0_U7nFxm80Y5.customdomain.com TX
26	0.150424474	192.168.122.3	192.168.122.209	DNS	148 Standard query 0x1828 TXT fH5df1wAJQDBgVSC86dRxxhWoAtqtiCYYTEh1F1dm9MwywzEwHfPMw12RhhA4.customdomain.com OPT
27	0.163512047	192.168.122.209	192.168.122.3	DNS	162 Standard query response 0x1828 TXT fH5df1wAJQDBgVSC86dRxxhWoAtqtiCYYTEh1F1dm9MwywzEwHfPMw12RhhA4.customdomain.com TX
30	0.176085165	192.168.122.3	192.168.122.209	DNS	137 Standard query 0x6d5b TXT fH5ef10AJQCZGoMqCmD1C0Mhc49foj28S_1swQ3T5WYvmq4GSbdmefFFDCh3.customdomain.com
31	0.187319061	192.168.122.209	192.168.122.3	DNS	162 Standard query response 0x6d5b TXT fH5ef10AJQCZGoMqCmD1C0Mhc49foj28S_1swQ3T5WYvmq4GSbdmefFFDCh3.customdomain.com TX

Additional RRs: 0

Queries

- fH5df1wAJQDBgVSC86dRxxhWoAtqtiCYYTEh1F1dm9MwywzEwHfPMw12RhhA4.customdomain.com: type TXT, class IN
  - Name: fH5df1wAJQDBgVSC86dRxxhWoAtqtiCYYTEh1F1dm9MwywzEwHfPMw12RhhA4.customdomain.com
  - [Name length: 77]
  - [Label Count: 3]
  - Type: TXT (Text strings) (16)
  - Class: IN (0x0001)

Answers

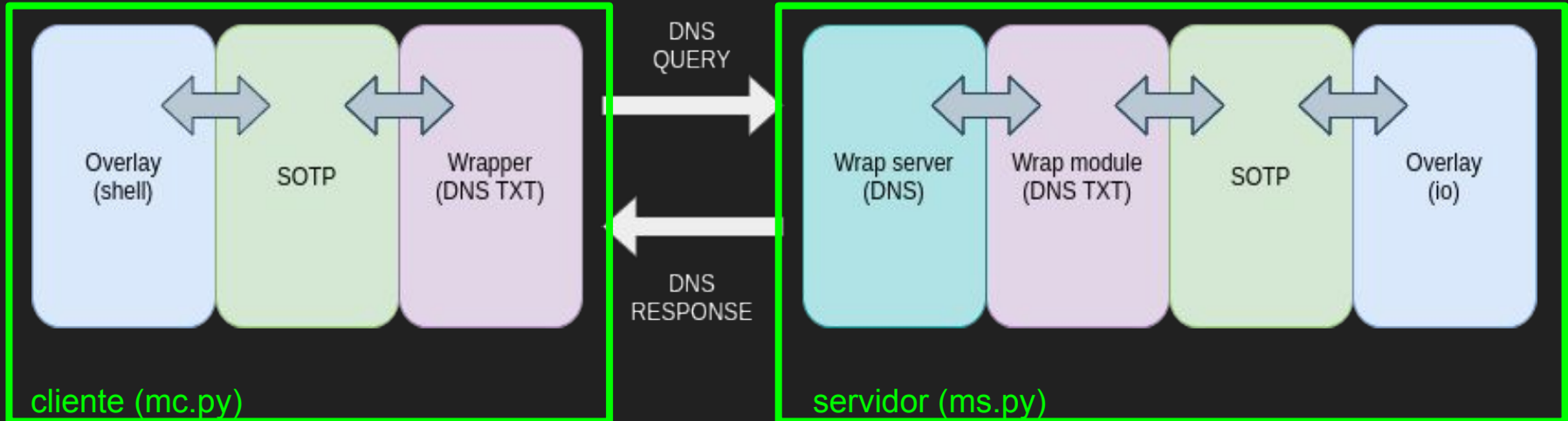
- fH5df1wAJQDBgVSC86dRxxhWoAtqtiCYYTEh1F1dm9MwywzEwHfPMw12RhhA4.customdomain.com: type TXT, class IN
  - Name: fH5df1wAJQDBgVSC86dRxxhWoAtqtiCYYTEh1F1dm9MwywzEwHfPMw12RhhA4.customdomain.com
  - Type: TXT (Text strings) (16)
  - Class: IN (0x0001)
  - Time to live: 300
  - Data length: 13
  - [Data length: 13]
  - TXT: fH5df10AAAA=
  - [Regul... 261]
  - [Time: 0.013087573 seconds]

**Paquete SOTP del cliente en base64, como subdominio en query DNS TXT**

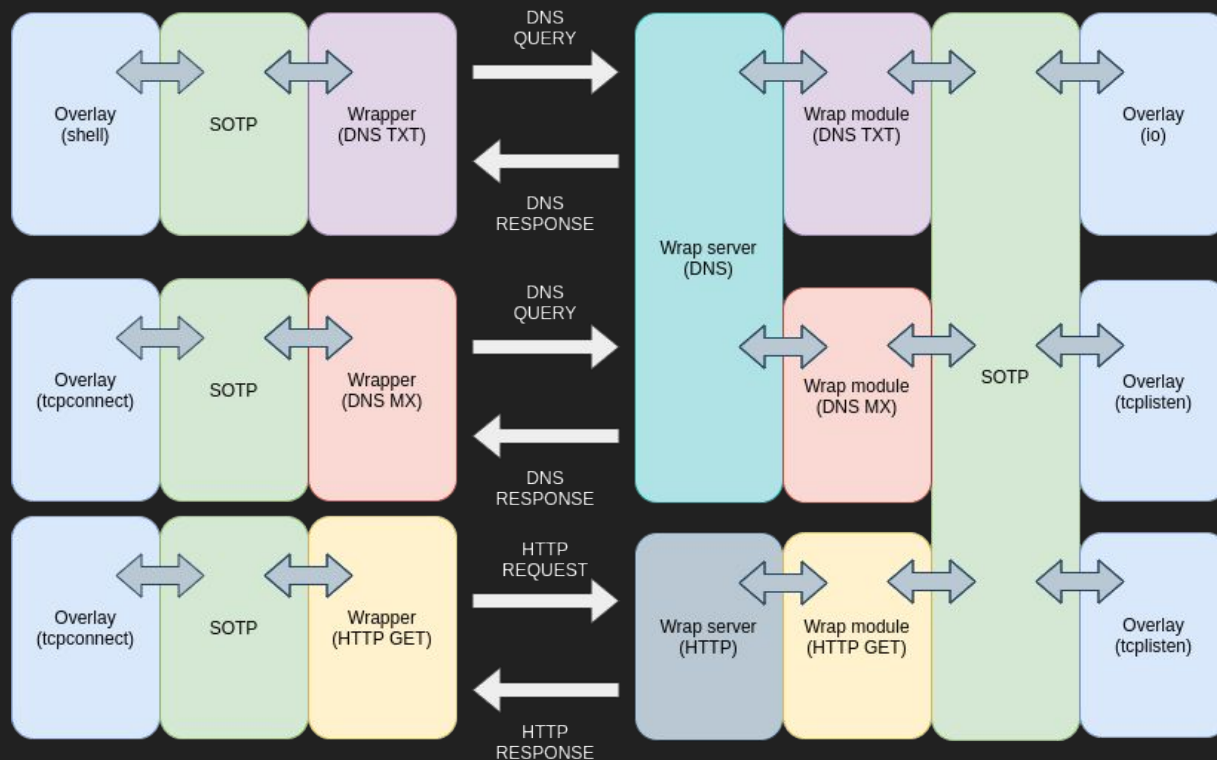
**Paquete SOTP del servidor en base64, como registro TXT en respuesta DNS**

# Arquitectura de Mística

Mística está estructurado en módulos que permiten una interacción circular. La siguiente diapositiva muestra el modo Single Handler (1 cliente, 1 servidor)



# Modo Multi-Handler (no implementado completamente)





# Mística - Wrappers

Los Wrappers son los encargados de comunicar cliente y servidor de mística

```
|rcaro@atlantis|-[~/github/Mistica|  
$ ./ms -l wrappers
```

Wrap modules:

- dns: Encodes/Decodes data in DNS queries/responses using different methods
- http: Encodes/Decodes data in HTTP requests/responses using different methods
- icmp: Encodes/Decodes data in ICMP echo requests/responses on data section

```
|rcaro@atlantis|-[~/github/Mistica|  
$
```

# Mística - Overlays

Los Overlays son los que proporcionan la funcionalidad al canal, es decir, los que realizarán el paso de datos entre la aplicación final y el módulo Sotp.

```
[rcaro@atlantis]~/github/Mistica  
$ ./ms -l overlays
```

Overlay modules:

- io: Reads from stdin, sends through SOTP connection. Reads from SOTP connection, prints to stdout
- shell: Executes commands recieved through the SOTP connection and returns the output. Compatible with io module.
- tcpconnect: Connects to TCP port. Reads from socket, sends through SOTP connection. Reads from SOTP connection, sends through socket.
- tcplisten: Binds to TCP port. Reads from socket, sends through SOTP connection. Reads from SOTP connection, sends through socket.

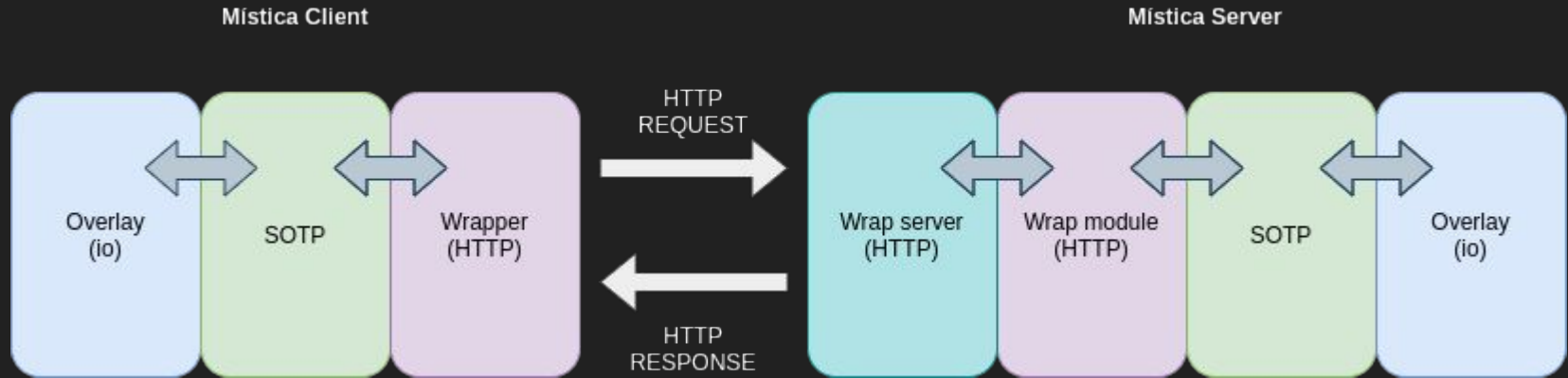
```
[rcaro@atlantis]~/github/Mistica  
$
```

# Mística - Compilación

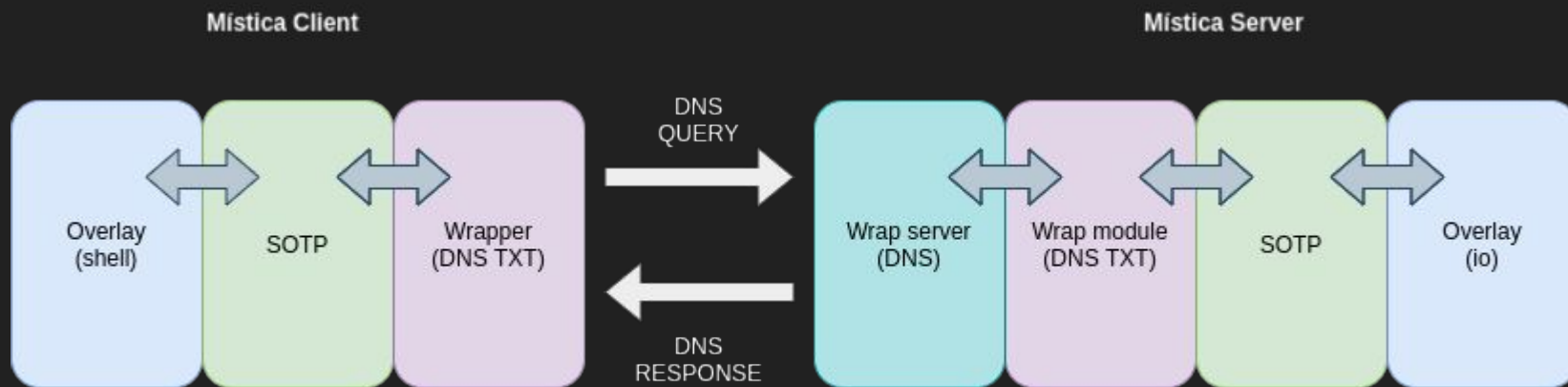
Al estar desarrollado en Python, Mística puede ser compilado utilizando ***Pyinstaller*** para generar un binario dependiente del Sistema Operativo.

```
pyinstaller --onefile \  
  --hiddenimport overlay.client.io \  
  --hiddenimport overlay.client.shell \  
  --hiddenimport overlay.client.tcpconnect \  
  --hiddenimport overlay.client.tcplisten \  
  --hiddenimport wrapper.client.http \  
  --hiddenimport wrapper.client.dns \  
  --hiddenimport wrapper.client.icmp \  
  --hiddenimport overlay.server.io \  
  --hiddenimport overlay.server.shell \  
  --hiddenimport overlay.server.tcpconnect \  
  --hiddenimport overlay.server.tcplisten \  
  --hiddenimport wrapper.server.wrap_module.http \  
  --hiddenimport wrapper.server.wrap_module.dns \  
  --hiddenimport wrapper.server.wrap_module.icmp \  
  --hiddenimport wrapper.server.wrap_server.httpserver \  
  --hiddenimport wrapper.server.wrap_server.dnsserver \  
  --hiddenimport wrapper.server.wrap_server.icmpserver \  
mc.py
```

# Demo I - Comunicación vía HTTP

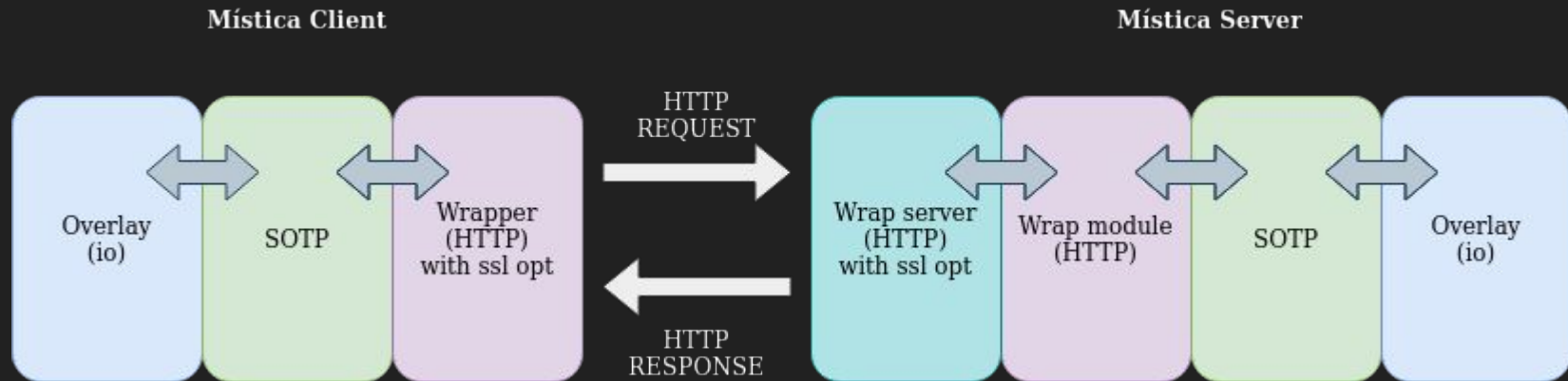


# Demo II - Shell vía DNS





# Demo III - Exfiltración de archivos vía HTTPs



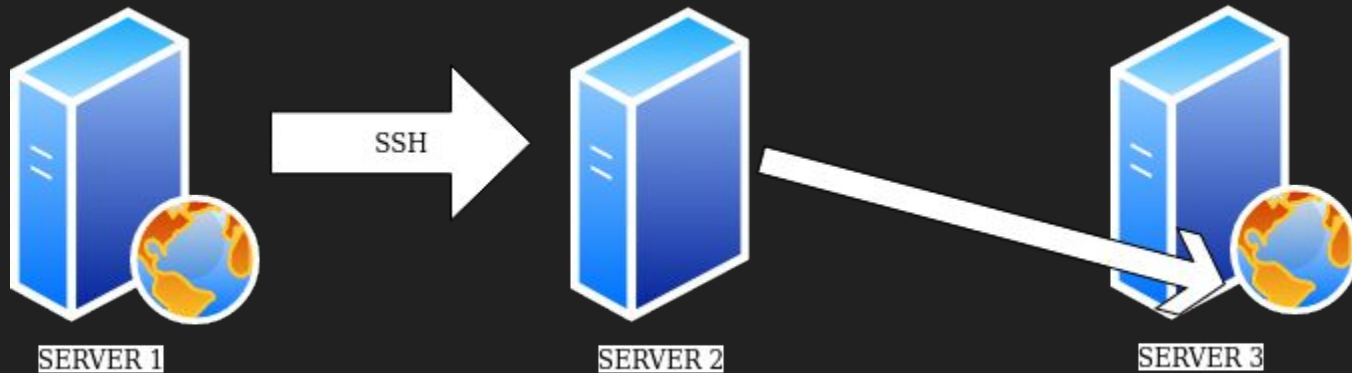
# Review Port Forwarding

El **Port Forwarding** o reenvío de puertos es una técnica de reenvío de información entre dos puertos (uno local y otro remoto).

## Tipos de Port Forwarding

- **Local Port Forwarding:** Las conexiones que se reciben en el puerto local A se conectan a través del túnel con el puerto remoto B.
- **Remote Port Forwarding:** Las conexiones que se reciben en el puerto remoto B se conectan a través del túnel con el puerto local A.

# Review Port Forwarding



# Port Forwarding con Mística

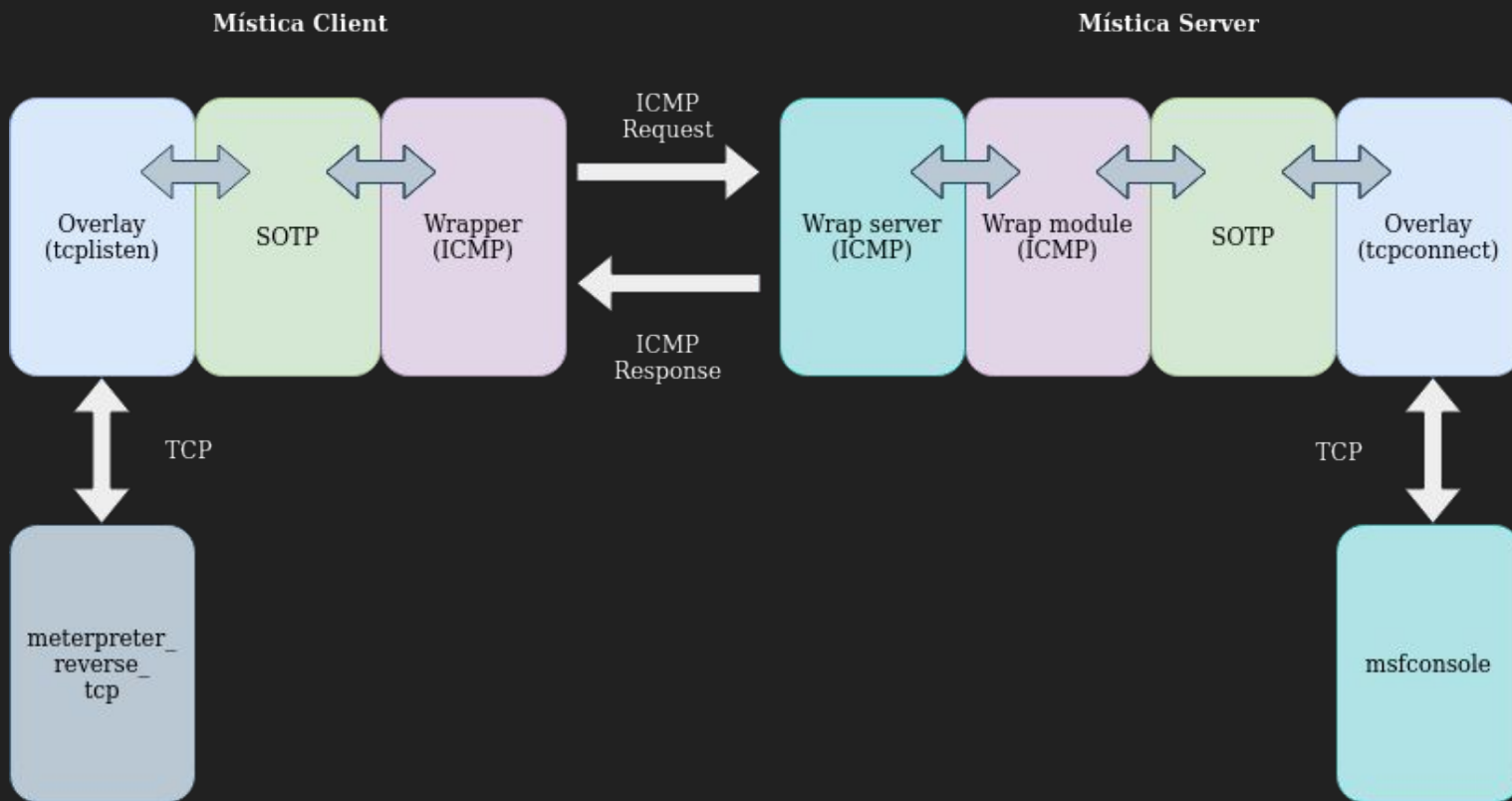
Módulos de Mística de Port Forwarding:

- **tcplisten**: Escucha en un puerto. Lee del socket, envía por canal SOTP. Lee de canal SOTP, envía por socket.
- **tcpconnect**: Se conecta a un puerto. Lee del socket, envía por canal SOTP. Lee de canal SOTP, envía por socket.

Que equivaldría a:

- tcplisten local + tcpconnect remoto: **Local port forwarding**
- tcpconnect local + tcplisten remoto: **Remote port forwarding**

# Demo IV - Meterpreter vía ICMP





# Status

- Status: PoC / Alpha ¡Queremos que lo probéis y lo rompáis!
- (Y si lo rompéis, decírnoslo :D)
- Siguietes pasos:
  - Protocolo de generación de claves en SOTP
  - Generador de payloads ejecutables multi-plataforma.
  - Modo multi-handler / interactivo
  - Módulo de ofuscación de paquetes SOTP: Padding, cifrado, stego...
  - Nuevos Wrappers: SMB, DNSoH, DNSoT, FTP...
  - Nuevos Overlays: Dynamic port forwarding, RAT, FileTransfer, VPN...
  - Especificación de SOTP y documentación de desarrollo

# Conclusiones

Mística aporta un enfoque distinto a los canales encubiertos

- Permite al **Blue Team** mejorar su capacidad de detección y respuesta.
- Permite al **Red Team** construir canales únicos y flexibles, integrados con otras herramientas

Es un proyecto emocionante y tenemos muchas ganas de hacerlo crecer

¡Probadlo, romperlo y abrid issue!

# Agradecimientos

A Carlos Fernández, por aportar diseño, coherencia y funcionamiento. Este proyecto no sería nada sin él (¡Seguidle en Twitter! @cfsgranda)

A INCIDE, por potenciar el Software Libre y de Código Abierto.

A Bitup Alicante y todos esos grupos que se preocupan por llevar el mundo de la seguridad informática y el hacking a estudiantes y todas las personas del entorno.

A esa personita que siempre me da su apoyo (;

MUCHAS GRACIAS



Y esto es todo amigos!

Mail: rcaro [ at ] incide.es

Twitter: @secu\_x11

Mística: <https://github.com/IncideDigital/Mistica>