Proxy POP3



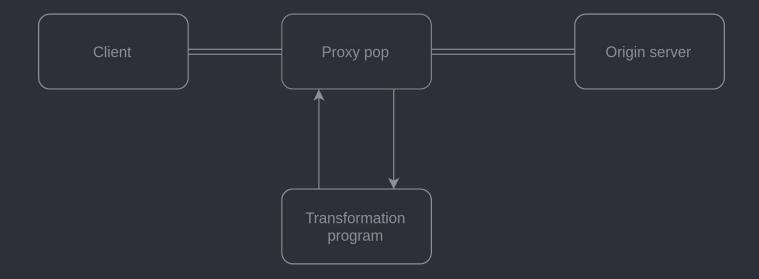
# OBJETIVO

Construir un proxy pop3 capaz de aplicar transformaciones a los correos electronicos, ser configurado y retornar metricas

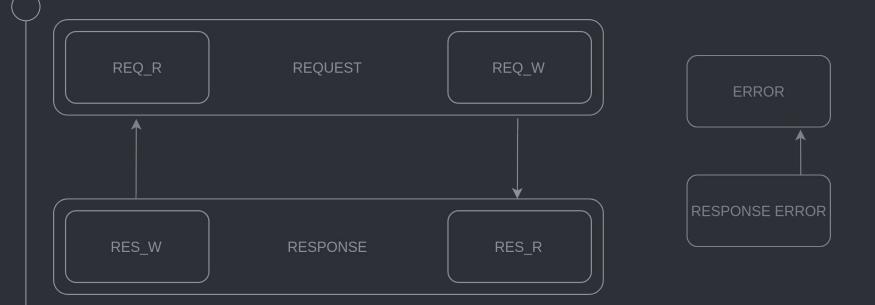


Empecemos con una breve descripción del proxy pop3

# El proxy



## Estados del proxy





Simple POP3 Proxy Communication Protocol

Breve descripción

El protocolo binario busca permitir la configuración y el monitoreo de un proxy pop3

Utiliza mecanismo request-response

Dos estados básicos:

- Autenticación
- Comunicación

#### Estados

## **Autenticación**

Mediante el comando USER se identifica como usuario y con el comando PASS provee la contraseña para autenticarse.

## Comunicación

Un usuario autenticado accede a todas las demás capacidades del protocolo para interactuar con el proxy



## El request

CMD	NARGS	ARGLEN 1	ARG 1	ARGLEN n	ARG n
1	1	1	Variable	1	Variable

- 1 byte para el comando.
- 1 byte para la cantidad de argumentos.
- Cada argumento precedido por dos bytes indicando la longitud del argumento



#### El response

STATUS CODE	LENGTH	DATA
1	1	VARIABLE

- 1 byte para el status code.
  - $\circ$  0x00 = success
  - o 0x01 = auth\_err
  - 0x02 = invalid command
  - $\circ$  0x03 = invalid arguments
  - $\circ$  0x04 = err
- 1 byte para el largo de la data response
- La data del response en formato ascii.



#### 0x00 USER

1 argumento: la representación ascii del usuario que se intenta autenticar.

CMD	NARGS	ARGLEN 1	ARG 1
0x00	1	7	'JOHNDOE'

Response si existe el usuario:

STATUS CODE	LENGTH
0x00	0

STATUS CODE	LENGTH
0x01	0

#### 0x01 PASS

1 argumento: la representación ascii de la contraseña del usuario que se intenta autenticar

CMD	NARGS	ARGLEN 1	ARG 1
0x01	1	11	'dontHackMeh'

Response si la clave corresponde al usuario ingresado previamente:

STATUS CODE	LENGTH	
0x00	0	

STATUS CODE	LENGTH	
0x01	0	

#### 0x02 Conexiones concurrentes

Sin Argumentos

CMD	NARGS
0x02	0

Response sin error:

STATUS CODE	LENGTH	DATA
0x00	1	<b>'</b> 5'

STATUS CODE	LENGTH
0x04	0

## 0x03 Bytes transferidos

Sin Argumentos

CMD	NARGS	
0x03	0	

Response sin error:

STATUS CODE	LENGTH	DATA
0x00	8	'55364528'

STATUS CODE	LENGTH
0x04	0

#### 0x04 Accessos Historicos

Sin Argumentos

CMD	NARGS
0x04	0

Response sin error:

STATUS CODE	LENGTH	DATA
0x00	6	<b>'152548'</b>

STATUS CODE	LENGTH	
0x04	0	

## 0x05 Transformación activa

Sin Argumentos

CMD	NARGS
0x05	0

Response sin error:

STATUS CODE	LENGTH	DATA
0x00	3	'cat'

STATUS CODE	LENGTH
0x04	0

## 0x06 Quit

Sin Argumentos

CMD	NARGS
0x06	0

Response sin error:

STATUS CODE		
0x00		

STATUS CODE	LENGTH
0x04	0

#### 0x10 Set buffer size

1 argumento: 2 bytes (small\_int) representando el nuevo tamaño de los buffers

CMD	NARGS	ARGLEN 1	ARG 1
0x10	1	2	0x0FFF

Response si se pudieron modificar los buffers exitosamente:

STATUS CODE	LENGTH
0x00	0

STATUS CODE	LENGTH	
0x02	0	

#### 0x11 Change transformation

1 argumento: tamaño variable con la representación ascii del comando de shell que se debe correr como transformación

0x11	NARGS	ARGLEN 1	ARG 1 'grep -i -v ^Date: '
I ()YII		l 18	arep -i -v ^Date:

Response si se pudo modificar la transformación exitosamente:

STATUS CODE	LENGTH
0x00	0

STATUS CODE	LENGTH	
0x02	0	

#### 0x12 Set timeouts

2 argumentos: 4 bytes (int) representando la cantidad de segundos. 4 bytes (int) representando la cantidad de milisegundos

CMD	NARGS	ARGLEN 1	ARG 1	ARG LEN 2	ARG 2
0x11	2	4	0x0002	4	0x0000

Response si se pudieron modificar los timeouts exitosamente:

STATUS CODE	LENGTH
0x00	0

STATUS CODE	LENGTH
0x02	0

**Gracias!** 

Preguntas?