Eliminación de correos problemáticos dado un dominio

En caso de ataque y que necesitemos borrar la cola de mensajes discriminando los emails legítimos de los ilegítimos tendremos que ir al directorio root de la máquina

```
cd /root/
```

Tenemos que escribir el siguiente comando y poner la información del remitente (generalmente suele ser algo del tipo apache@hs-156...) o el dominio con el que se envían los correos.

```
borrar_correo apache
```

Gestión de postfix

Comandos básicos para gestionar la cola de correos de Postfix:

Mostrar todos los mensajes de la cola:

```
mailq
```

```
mailq | less --> Si queremos paginar el resultado
```

Eliminar todos los mensajes de la cola:

```
postsuper -d ALL
```

Eliminar todos los mensajes que hayan sido devueltos por los destinatarios:

```
postsuper -d ALL deferred
```

Muestra el número de mensajes que hay en la cola:

```
postqueue -p | tail -n 1 | cut -d' ' -f5
```

ó

```
mailq | tail -n1 | gawk '{print $5}'
```

Para ver el contenido del mensaje:

```
postcat -q ID
```

NOTA: Para obtener el ID tenemos que ejecutar previamente el comando mailq

Eliminar de la cola un mensaje en concreto:

```
postsuper -d numero
```

Encolar de nuevo un mensaje en concreto:

```
postsuper -r Number
```

Encolar de nuevo todos los mensajes:

```
postsuper -r ALL
```

Otra forma de mostrar los mensajes de la cola:

```
postqueue -p
```

Realizar un “flush” para enviar todos los mails de la cola:

```
postqueue -f
```

Listar mails enviados por dominio:

```
mailq | egrep dominio.com
```

Contar los mails enviados por dominio:

```
mailq | egrep dominio.com | wc -l
```

Enviar los mails para el dominio especificado:

```
postqueue -s
```

Eliminar emails con un determinado texto en el remitente o destinatario:

```
mailq | grep "xxxxxxxxxxxxxxxxxx" | awk '{ print($1); }' | postsuper -d -
```

Borrar los emails desde una dirección específica:

```
mailq | tail +2 | grep -v '^ *(' | awk 'BEGIN { RS = "" } { if ($8 ==
"email@address.com" && $9 == “”) print $1 } ' | tr -d '*!' | postsuper -d -
```

Estadística de tráfico de mails

```
pflogsumm /var/log/mail/mail | mailx -s "Estadísticas servidor de correo"
usuario@dominio.com
```

Listamos los correos que que estan en la cola del Postfix sin eliminarlos. Por ejemplo lo filtramos por el remitente prueba@remitente.com

```
postqueue -p |grep -v "^ " |grep prueba@remitente.com | awk ' { print $1}
{print $7}' | tr -d '*!'
```

Si tenemos claro que los correos mostrados son los correctos para eliminar los borramos añadiendo la pipe postsueper -d –

```
postqueue -p |grep -v "^ " |grep prueba@remitente.com | awk ' { print $1}
{print $7}' | tr -d '*!' | postsuper -d -
```

Configuración de postfix

Limites

From:
https://wiki.merkatu.info/ - **Wiki de merkatu**

Permanent link:
https://wiki.merkatu.info/postfix?rev=1490629467

Last update: **2017/04/21 14:05**