zimbra, spam

Problemas con el Spam

Para ver cuentas comprometidas

como root

```
cat /var/log/zimbra.log | sed -n 's/.*sasl_username=//p' | sort | uniq -c |
sort -nr
```

También podemos usar

```
 cat /var/log/zimbra.log | grep failure
```

para buscar intentos de autentificación erróneos

Para ver problemas de autentificación hay que mirar el log /opt/zimbra/log/audit.log

Para ver las ips desde las que están lanzando los intentos de validación

```
tail -f /var/log/maillog | grep warning
```

En https://www.abuseipdb.com/ podemos comprobar si dicha ip ya se ha notificado o notificarla nosotros como sospechosa

En https://ipinfo.io/ podemos saber el rango de ip perteneciente a un proveedor para filtrar todo el rango

Mover los mensajes a la cola retenidos

Si tenemos muchos mensajes de spam en nuestro servidor deberíamos de moverlos a la cola retenidos para posteriormente analizarlos. Como root vamos a cada cola y los movemos a la cola **hold**

```
cd /opt/zimbra/data/postfix/spool/active
mv * ../hold
```

```
cd /opt/zimbra/data/postfix/spool/defer
#defer has 0 to f sub-folders inside
for A in *; do mv -f $A/* ../hold; done
```

```
cd /opt/zimbra/data/postfix/spool/deferred
```

```
#deferred has 0 to f sub-folders inside
for A in *; do mv -f $A/* ../hold; done
```

```
cd /opt/zimbra/data/postfix/spool/incoming
mv * ../hold
```

Una vez que hemos pasado todos los mensajes a la carpeta hold pasamos a verificar dentro de la carpeta los que tienen como ip origen el equipo atacante y en mi caso los elimino directamente

```
 cd /opt/zimbra/data/postfix/spool/hold
grep -l 185.236.203.159 * | xargs -I{} rm {}
```

si son muchos mensajes no podras usar *, tendras que acortar la búsqueda para que no te de error por ejemplo usando A34* en vez de * para analizar sólo los mensajes que empiezan por ese prefijo

Reputación

https://jejo.es/posts/servidores/reputacion_servidor_correo/

Para evitar el spam además de asegurar nuestro servidor de correos debemos de configurar lo siguiente:

1. Crear una Firma DKIM válida
2. Verificacion DMARC
3. Certificados ssl validados por una autoridad de certificacion, tipo Let´s Encrypt (https://letsencrypt.org/es/)
4. Comprobar que no estamos en una Lista Negra. Si es asi hay que solicitar el desbloqueo
5. Superar SPF (Sender Policy Framework)

Para comprobar la reputación de nuestro servidor de correos podemos usar:

1. https://mxtoolbox.com/SuperTool.aspx
2. http://www.mail-tester.com/
3. https://www.senderbase.org/
4. https://multirbl.valli.org
5. https://www.senderscore.org/

Referencias

- https://wiki.zimbra.com/wiki/Spamming_troubleshooting
- https://www.sbarjatiya.com/notes_wiki/index.php/CentOS_7.x_Zimbra_mail_queue_management
- https://wiki.zimbra.com/wiki/Enforcing_a_match_between_FROM_address_and_sasl_username_8.5
- https://wiki.zimbra.com/wiki/Compromised_account_results_in_the_server_being_used_to_send_out_spam_mail