

Exim - Find Spam

To get a sorted list of email sender in exim mail queue. It will show the number of mails send by each one.

```
exim -bpr | grep "<" | awk {'print $4'} | cut -d "<" -f 2 | cut -d ">" -f 1 | sort -n | uniq -c
```

List mail ID's for that account:

```
exim -bpr | head -1000 | grep "spoofed-email@suspicious-domain.com" | head -4
```

Looking up info on mail with ID:

```
find /var/spool/exim/ -name 1XgdkD-0001XD-8b | xargs head -1
```

How many Frozen mails on the queue:

```
/usr/sbin/exim -bpr | grep frozen | wc -l
```

Deleteing Frozen Messages:

```
/usr/sbin/exim -bpr | grep frozen | awk {'print $3'} | xargs exim -Mrm
```

Find a CWD:

```
grep cwd /var/log/exim_mainlog | grep -v /var/spool | awk -F"cwd=" '{print $2}' | awk '{print $1}'
```

Code breakdown:

To remove a message from a sender in the queue:

```
exim -bp | grep email@domain.com | sed -r 's/(.{10})(.{16}).*/\2/' | xargs exim -Mrm
```

To remove a message from the queue:

```
exim -Mrm {message-id}
```

To remove all messages from the queue, enter:

```
exim -bp | awk '/^ *[0-9]+[mhd]/{print "exim -Mrm " $3}' | bash
```

Revision #6

Created 5 July 2017 15:46:22 by Dave

Updated 16 December 2017 08:42:46 by Dave