SECURING YOUR EXIM/DOVECOT MAILSERVER

(WHM®/cPanel® 11.48.1 – stock configuration)

I started on a mission to get spam under control on my mailserver. Along the way, I learned a bit about mailserver security. I found this website for checking mail server security (you do not have to enter an email address): Email Security Grader. If I recall correctly, my score was around 40% or so with the stock cPanel default settings. My score is now 98% with a status = "VERY STRONG SECURITY". Items marked in red below are changes to the cPanel default configuration.

This assumes that ClamAV Scanner and CSF/LFD are installed (which I believe is standard for all KnownHost cPanel VPS).

1. MX Connection Test: This seems to all work fine with default settings (pretty basic).

2. Reverse DNS Test: My PTR was already setup properly, thanks to KnownHost's awesome tech support who took care of that when they migrated my server over. BTW, if you've never checked your DNS configuration – well, you should do it; enter your domain name at intoDNS and/or pingdom Tools.

3. DNSBL Test: My online reputation was already fine. Although not considered for this test, I went ahead and contacted dnswl.org and requested to be added to their whitelist database for good measure. ☺

4. SPF Server Test: I'm pretty sure that recent versions of WHM/cPanel automatically create an SPF record for new DNS zones. If you go to WHM » Home » DNS Functions » Edit DNS Zone, and choose a zone to edit, the SPF record will look something like: "v=spf1 +a +mx +ip4: xxx.xxx.xxx.xxx ~all". You may want to edit the ~all part of the record. What it means (if a receiving server is checking SPF):

   - If the record indicates ~all, then this lets a receiving server know that other servers aren't supposed to be sending mail for the domain, but it doesn't have to reject the email. This would be useful if users prefer or need to use a different SMTP server.

   - If the record indicates –all, then this lets a receiving server know that other servers aren't supposed to be sending mail for the domain, and it should otherwise reject the mail. This would be more secure if you want users to always use the host mailserver.

   I set mine to –all since there is no need for users on my server to use some other SMTP server. I assume that this will help prevent spammers from spoofing my hostname in their return path.

   If you have a user that thinks they have to use their ISP's SMTP server (due to SMTP port being blocked by the ISP), then have them try to use another port (e.g., SSL on port 465, STARTTLS on port 26, etc.).

5. SPF Client Test: In WHM » Home » Service Configuration » Exim Configuration Manager, select [Basic Editor] tab, and [ACL Options] sub-tab. Set "Reject SPF failures" to "On" (cPanel default is "Off").

6. Open Relay and Email Format Test: This seems to work fine with the default settings (it would be exceedingly surprising if the default cPanel configuration allowed for open relaying).

In WHM » Home » Service Configuration » Exim Configuration Manager, select [Advanced Editor] tab and find the “default_mail_pre” should be checked and expanded by default. I’m pretty sure this is the ACL that prevents open relaying, but I’m not 100% sure.

7. SMTP Plain Text Authentication Test:

   - Install an SSL certificate.

   - In WHM » Home » Service Configuration » Exim Configuration Manager, select [Basic Editor] tab, and [Security] sub-tab. Set “Require clients to connect with SSL or issue the STARTTLS command before they are allowed to authenticate with the server” to “On” (cPanel default is “Off”).

   - In WHM » Home » Service Configuration » Service Manager, ensure that Antirelayd is NOT enabled (cPanel default).

   With the ‘SSL before AUTH’ setting listed above, brute force attacks on Exim are not recognized by CSF/LFD because the exim_main log records “*AUTH command used when not advertised*" error instead of the usual failed authentication error. To mitigate this issue add a custom rule to CSF/LFD as follows:

   - Create LFD custom regex. Edit file /usr/local/csf/bin/regex.custom.pm … insert custom regex anywhere before the “return 0” line (note some lines below do NOT have carriage return/line feeds):

     Code:

```
# Custom regex for Exim "AUTH command used when not advertised"
# Treat as brute force attempt that appears in the log as syntax error due to SSL required before AUTH
    if (($lgfile eq $config{CUSTOM1_LOG}) and ($line =~ /^\d+\D+\d+\D+\d+\d+\D+\d+\D+\d+ \[\d+\] SMTP protocol error in "AUTH LOGIN" H=\(USER\) \[(\d+\.\d+\.\d+\.\d+)\]:\d+ I=\[(\d+\.\d+\.\d+\.\d+)\]:\d+ AUTH command used when not advertised/)) {
        return ("AUTH attempted without SSL from","$1","eximnoSSLmatch","10","25,26,465,587","7200");
    }
    return 0;
}
1;
```

   - Change CUSTOMLOG1 to the exim log file. Edit file /etc/csf/csf.conf … find “CUSTOM1_LOG” and change to /var/log/exim_mainlog:

     Code:

```
CUSTOM1_LOG = "/var/log/exim_mainlog"
```

   - Restart LFD. In WHM » Home » Plugins » ConfigServer Security & Firewall, click on the “Lfd Restart” button.

   The custom rule allows for no more than 10 occurrences of ‘AUTH attempted before SSL’ in a 5 minute period, after which the offending IP address is blocked on ports 25, 26, 465, and 587 for 7200 sec (2 hours). I chose a temporary block instead of a permanent block in case a legitimate user is unaware of the SSL requirement. Prior to setting this rule, I observed no attack persisting longer than 1.5 hours. And so far after running this rule for about a week, I haven’t seen any blocked IP addresses come back and retry brute force attack.

You can find instances of this rule being implemented by using "grep 'eximnoSSL' /var/log/lfd.log" command in an SSH terminal while logged in as root user.

8. POP3 Connection Test: The only "*cPanel supported*" method for secure authentication to Dovecot is plaintext through an SSL tunnel. If you REALLY want, you can reconfigure Dovecot to NOT allow plaintext authentication, and instead allow cram-md5 and/or kerberos5 authentication; but it will likely break (I think) whenever cPanel updates.

   - Install an SSL certificate.

   - In WHM » Home » Service Configuration » Mailserver Configuration.
     Set "Allow Plaintext Authentication" to "No"
     Set "Use New Authentication Process for Each Connection to "Yes"
     (I forget what the cPanel defaults are).

   - The above settings should be sufficient as Dovecot will reject any plaintext authentication attempts on port 110. However, the '*emailsecuritygrader*' will deduct points if the server answers at all on port 110. I don't know if this is a bona fide security risk, but I figured it couldn't hurt to shut down port 110 since nobody should be connecting to it now anyway. So I went ahead and disabled port 110 at the firewall.

     In WHM » Home » Plugins » ConfigServer Security & Firewall, push the [Firewall Configuration] button, scroll down to "IPv4 Port Settings", and then delete 110 from the "TCP_IN =" and "TCP_OUT" fields.

9. IMAP Connection and Authentication Test: This is already taken care of with the SSL certificate and "Mailserver Configuration" changes in test no. 8 above.

NOTE: After doing steps 7, 8, and 9 … all users will NOT be able to connect to the mailserver unless they use a secure connection (SSL/TLS). So be prepared to instruct them on how to setup their email clients to do this. And if user's have been previously sending username/password information in the clear (no security), then now would be a good time to change all those passwords! ☺

There's one more security issue that I noticed that is related to DKIM. If you look at your DNS zones again (WHM » Home » DNS Functions » Edit DNS Zone), you should notice that each zone has a domainkey record that is auto-magically created by cPanel when you add domains. And cPanel has chosen your DKIM selector for you to be "default" (record default._domainkey.<your domain>.com which is signed by the server as "default"). And as far as I know, cPanel currently provides no supported method for changing the selector. Apparently being forced to use "default" with no way to edit/change it is not compliant with the DKIM spec (summarily defeating the purpose of having a selector!). It may not be that big of a deal, but I suppose it could be a problem if you use multiple cPanel servers to send mail.

I think that's about it folks!!

Please feel free to let me know if you think any corrections should be made to this document or if you have any additional information or insight to contribute. You can PM me over at the knownhost.com forums here, or send me an email me at contact form.

Cheers!

Robert Medure
https://powerproductsandservices.com

Disclaimer: