**Windows:**

**Change passwords:**

Go to “administrative tools” and chose active directory

In active directory you can select users and change their password

**Harden Exchange Server:**

Log onto Exchange server with admin account

Start Menu -> Programs -> Microsoft Exchange

Double click "Administrative Groups" -> "First Administrative Group" -> "Servers"

Right click "Default SMTP Virtual Server" -> "Properties"

Click "Access" tab at top of pop-up window

"Access Control" -> "Authentication"

Uncheck box next to "Anonymous Access" to disable unknown connects to Exchange SMTP server

Check "Basic Authentication" and "Requires TLS ecnryption" boxes to secure transmissions

Check "Integrated Windows Authentication" box

Click "OK" twice to save security settings

**Ports:**

443/TCP (HTTPS) - Encrypted Web Connections

80/TCP (HTTP) - Unencrypted Web Connections

143/TCP (IMAP) - IMAP4 Clients

993/TCP (secure IMAP) - IMAP4 Clients

110/TCP (POP3) - POP3 Clients

995/TCP (secure POP3) - POP3 Clients

587/TCP (authenticated SMTP) - SMTP Clients

25/TCP (SMTP) - Client Access server, Mailbox Server, Client Access Server

53/UDP (DNS) - DNS Server

53/TCP (DNS) - DNS Server

**Block Attachments on Exchange Server**

Exchange management console-> organization configuration-> hub transport -> transport rules-> new transport rule

Conditions:Set for when attachment name matches text pattern, add .zip, .exe, .bat, .vbs, .ps,

.7z, .rar, .scr, .com, .pif, .hta, .sys, .vb, .ws, .dll

Actions: delete message without notifying anyone

**Linux**

**Postfix:**

**Check for errors/warnings:**

postconf 1> /dev/null

**Harden:**

postconf -e disable\_vrfy\_command=yes

postconf -e inet\_interfaces=loopback-only

**Prevent unwanted relaying:**

mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

postconf -e mynetworks="127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128"

**Enable HELO:**

postconf -e smtpd\_helo\_required=yes

**Enable TLS:**

postconf -e smtp\_tls\_loglevel=1

**Test keys:**

echo | openssl s\_client -starttls smtp -connect localhost:25 -cipher "EDH" 2>/dev/null | grep -i -e "Server .\* key"

**Block Attachments:**

# vi /etc/postfix/main.cf

Add this line

mime\_header\_checks = regexp:/etc/postfix/mime\_header\_checks

Write and quit

# vi /etc/postfix/mime\_header\_checks

Add this

/name=[^>]\*\.(bat|com|exe|dll|vbs|zip|sys|7z|zip|ps|com|scr|rar|pif|vb|ws)/ REJECT

Write and quit

**EXIM**

1. Preventing nobody from sending emails WHM > Tweak Settings, select “On” for the following option:

Prevent “nobody” from sending mail [?]

2. Setting the Sender header when the email sender tries to spoof the sender WHM > Exim Configuration, select the following:

Set the Sender: Header when the mail sender changes the sender (-f flag passed to sendmail).

3. Adding MailHeaders for PHP

WHM > EasyApache (Apache Update) > Step 6 Exhaustive Options List in the PHP section (PHP 4 and/or PHP 5), select the following:

MailHeaders

1. All logging for exim log file

WHM > Exim Configuration > Advanced Editor, add the following in the topmost box: log\_selector = +all

2. Stopping spoofing from webmail and SMTP authenticated users

WHM > Exim Configuration > Advanced Editor, add the following in the second box where it has begin acl directly above it:

acl\_check\_data:

deny

authenticated = \*

condition = ${if or {{ !eqi{$authenticated\_id} {$sender\_address} }\

{ !eqi{$authenticated\_id} {${address:$header\_From:}} }\

}\

}

message = Your FROM must match your authenticated email user.

Removing sendmail

mv /usr/sbin/sendmail /usr/sbin/sendmail.bak`date +"%Y%m%d%H%M%S"`

To block certain extensions edit /etc/cpanel\_exim\_system\_filter, and add file extension to all the four lines beginning:

if $header\_content-type: matches

if $header\_content-type: matches

if $message\_body matches

if $message\_body matches