OS Level 2 Hardening
Perform all of the procedures listed in the Level 1 Hardening Guide

install trip wire;
apt-get install tripwire
the passphrase for tripwire is non recoverable, so use a secure passphrase that you will not forget
tripwire –init to build an initial database
Backup your tripwire database to a secure location
/etc/tripwire
/var/lib/tripwire

Configure pam to test password strength against a dictionary (root can still override);
apt-get install libpam-cracklib
vi /etc/pam.d/common-password

1. comment out the line that says "password required pam_unix.so nullok obscure min=4 max=8 md5"
2. add the following 2 lines;
   password required pam_cracklib.so retry=3 minlen=8 difok=3
   password required pam_unix.so use_authtok nullok md5

configure /etc/security/access.conf to disallow logins from the following accounts;
- :daemon bin sys sync games man lp mail news uucp proxy www-data backup list irc gnats nobody Debian-exim identd sshd: ALL
edit /etc/pam.d/login and uncomment ;
account required pam_access.so

configure network sysctl values
net/ipv4/icmp_echo_ignore_broadcasts = 1
net/ipv4/conf/all/secure_redirects=1
net/ipv4/conf/all/accept_source_route=0

if running apache, add;
ServerTokens Prod to the Global configuration (restricts banner information)

install the SekHost deb and configure the local firewall (even if network fire walling is used as well)

- restrict open ports to bare minimums
- restrict access to ssh to only administrative IP's