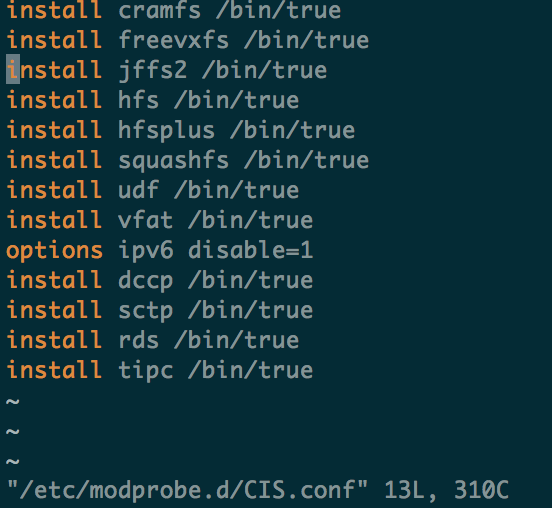
False Positives

1.1.1.1 , 1.1.1.2, 1.1.1.3, 1.1.1.4, 1.1.1.5, 1.1.1.6, 1.1.1.7, 1.1.1.8, 1.1.10 – Ensure cramfs, freexvfs, jffs2, hfs, hfsplus, squashfs, udf, and FAT filesystems are disabled.

Reasoning: Tenable’s regex is incorrect, as the following screen shot confirms this:



1.1.2 – Ensure GPG keys are configured

Reasoning: GPG is installed, and Tenable’s regex is incorrect (it seems to be looking for centos or redhat GPG-specific keys, rather than AWS’s)

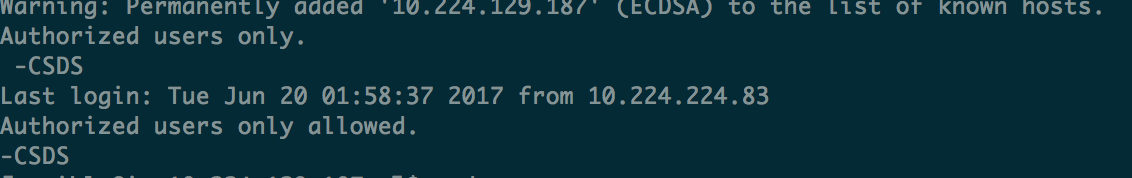


1.4.1 - Ensure permissions on bootloader config are configured

Reasoning: Root owns menu.lst, and has a correct symlink to grub.conf. 

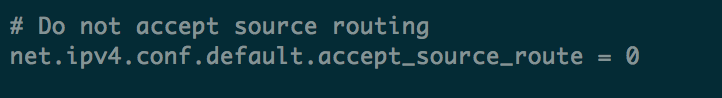
1.7.1.1, 1.7.1.2, 1.7.1.3 – Ensure MOTD is configure

Reasoning: MOTD displays accordingly, as tenable’s regex is incorrect.



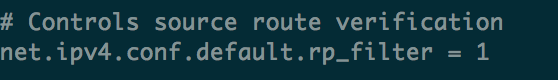
3.2.1 – Ensure source routed packets are not accepted.

Reasoning: Tenable’s regex is incorrect

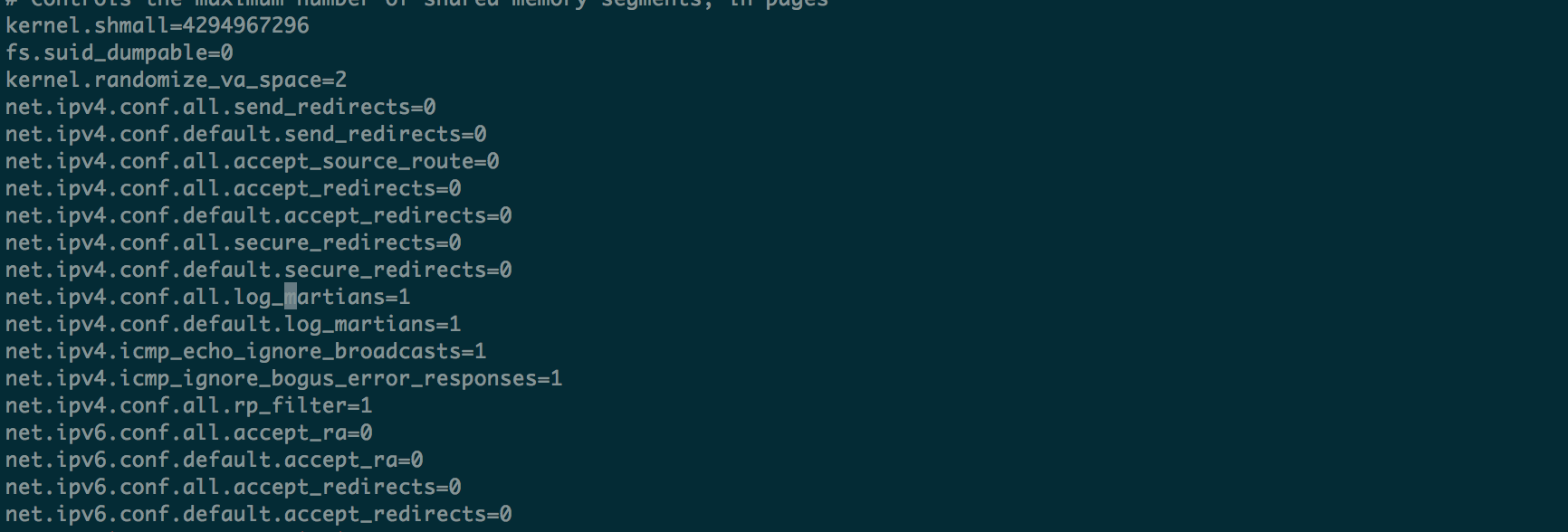


3.2.7 – Ensure reverse path filtering is enabled

Reasoning: Tenable’s regex is incorrect



3.1.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.3.1, 3.3.2, 3.3.3 – Misc. network hardening. Configurations are present in sysctl.conf, meaning Tenable’s regex is incorrect.



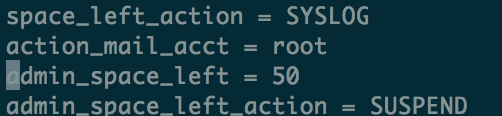
3.4.2 – Ensures /etc/hosts.allow is configured

Reasoning: The files are created as intended, meaning Tenable’s regex is incorrect



4.1.1.2 – Ensure system is disabled when audit logs are full

Reasoning: Specified configurations were applied for syslog, rather than email.



4.1.10, 4.1.11, 4.1.12, 4.1.13, 4.1.14, 4.1.15, 4.1.16, 4.1.17, 4.1.18, - Ensure proper audit.rules configurations are applied.

Reasoning: Configurations are applied, and Tenable’s regex is incorrect.

