While the provided CIS hardening scripts configure many CIS rules, some rules must be manually configured into compliance.

## CIS Level 1 (Server and Workstation Profiles)

Root Password Rule

* 1.4.3: Ensure authentication required for single user mode

Hosts.allow and Hosts.deny Rules

*Rules provided by these scripts only provide a generic version of those files.* *Configure these specifically for your network.*

* 3.4.2: Ensure /etc/hosts.allow is configured
* 3.4.3: Ensure /etc/hosts.deny is configured

Firewall Rules

*Configure these specifically for your network.*

* 3.6.2: Ensure default deny firewall policy
* 3.6.5: Ensure firewall rules exist for all open ports

User Password Creation Time Audit Rule

*In order to enforce this rule, one must ensure that a user doesn't have a password change time in the future.*

* 5.4.1.5: Ensure all users last password change date is in the past

User and Group Rules

* 6.2.6: Ensure root PATH Integrity
* 6.2.16: Ensure no duplicate UIDs exist
* 6.2.17: Ensure no duplicate GIDs exist
* 6.2.18: Ensure no duplicate user names exist
* 6.2.19: Ensure no duplicate group names exist
* 6.2.20: Ensure shadow group is empty

## CIS Level 2 (Server and Workstation Profiles)

*In addition to the CIS Level 1 configured rules above.*

Separate Partition Rules

* 1.1.2: Ensure separate partition exists for /tmp
* 1.1.5: Ensure separate partition exists for /var
* 1.1.6: Ensure separate partition exists for /var/tmp
* 1.1.10: Ensure separate partition exists for /var/log
* 1.1.11: Ensure separate partition exists for /var/log/audit
* 1.1.12: Ensure separate partition exists for /home