Auditing Linux without root

As a rule, we prefer the root user or a user with sudo (root) access when auditing a Linux device.

This is not essential though. If you cannot provide root or a sudo enabled user, you will still get a result - you simply will not get all the possible attributes. This is because some commands require root level access to run, even in "read only" mode. For example, "dmidecode". We use that command to retrieve various details about the motherboard, etc.

If your environment does not allow sudo, you should set the configuration item (as at 2.0.10) discovery_linux_use_sudo to 'n' (sans quotes). This is set to 'y' by default. This will run the audit script without attempting to use sudo if you are not root.

So what info will you not receive? It is detailed below, by the database table, attribute and required command.

Table	Attributes not retrieved	Required Command
system	uuid, serial, form factor.	dmidecode
bios	serial, version, smversion (pre 2.0.12), serial, smversion post 2.0.12	dmidecode
processor	socket.	dmidecode
memory	all.	dmidecode
motherboard	all (pre 2.0.12), serial, processor_type, memory_slot_count post 2.0.12.	dmidecode
netstat	program name where process not owned by current user.	netstat