7.6.3 Linux Host Security Facts

The following table describes the general procedures for increasing the network security of a Linux system:

Security Task	Procedure
Remove Unnecessary Software	Unnecessary software occupies disk space and could introduce security flaws. To remove unnecessary software: 1. Run one of the following commands: - Use **yum list installed** to see installed RPM packages on the computer. - Use **dpkg –get-selections** to see installed Debian packages on the computer. 2. Research the function of any unrecognized package to determine whether it is necessary. 3. Use **yum**, **rpm**, or **dpkg** to uninstall unnecessary packages.
Check For Unnecessary Network Services	Unnecessary network services waste the computer's resources and might provide attackers with an entry point for an attack. To remove unnecessary network services: 1. Search within the **/etc/init.d** or **/etc/rc.d/init.d** directories for unusual or unrecognized scripts. 2. Use the **man** command and the internet to research the scripts' functions and determine whether they can be safely removed or disabled. 3. Use **chkconfig**, **insserv**, or **init** to disable the script. Use **init** or **rc** to immediately stop the script. Use **yum**, **rpm**, or **dpkg** to remove the script package entirely.
Locate Open Ports	Open ports can provide information about which operating system a computer uses and might provide entry points or information about ways to formulate an attack. To locate open ports: 1. Install the **nmap** utility (if not already installed). 2. Use one of the following commands to scan for open ports: - **nmap -sT** scans for TCP ports - **nmap -sU** scans for UDP ports 3. From the results of the scan, determine which services use the ports and which ports to close. 4. Disable the unused services using ports.
Check Network Connections	Open network connections (open sockets) on a computer create a security risk. A *socket* is an endpoint of a bidirectional communication flow across a computer network. Use the following **netstat** options to identify the open network connections on Linux systems: - **-a** lists both listening and non-listening sockets. - **-l** lists listening sockets. - **-s** displays statistics for each protocol. - **-i** displays a table of all network interfaces.