4.4.3 Linux Host Security Facts

This lesson covers network security on Linux.

Network Security on Linux

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. Enter one of the following commands: ▪ **yum list installed** or **dnf list installed** to see installed RPM packages on the computer. ▪ **apt** ▪ **apt autoremove** automatically removes unused packages ▪ **apt list** list all installed packages ▪ **dpkg get-selections** to see installed Debian packages on the computer. 2. Research the function of any unrecognized package to determine if it is necessary. 3. Use one of the following commands to uninstall unnecessary packages. ▪ **yum erase** *packagename* ▪ **dnf remove** *packagename* ▪ **apt remove** *packagename* ▪ **rpm -e** *packagename* ▪ **dpkg -r** *packagename*
Check for unnecessary network services	Unnecessary network services waste computer resources and increase the system's attack service. To remove unnecessary network services: 1. Find all installed services and determine which are not needed: DNS, SNMP, DHCP and others. ▪ **systemctl --type=service --state=active** 2. Use the **man** command and the Internet to research services you don't recognize. ▪ If the service is not needed, determine if it is a dependency for another service. 3. Disable the service by using the following command: ▪ **systemctl disable** *servicename* 4. Use one of the following commands to immediately stop the script: ▪ **systemctl stop** *servicename* 5. Use one of the following commands to remove the script package entirely. ▪ **yum erase** *packagename* ▪ **dnf remove** *packagename* ▪ **apt remove** *packagename* ▪ **rpm -e** *packagename* ▪ **dpkg -r** *packagename*
Locate open ports	Open ports can provide information about which operating system a computer uses. Also, they can provide entry points or information about ways to formulate an attack. To locate

	open ports: 1. Install the **nmap** utility if it is not already installed. ▪ **yum install nmap** ▪ **dnf install nmap** ▪ **apt -i nmap** 2. Use both of the following commands to scan for open ports: ▪ **nmap -sT** *ipaddress*|*fqdn* scans for TCP ports ▪ **nmap -sU** *ipaddress*|*fqdn* scans for UDP ports 3. Determine which services use the open ports. 4. Disable any unused service using the open ports information. (*Make sure the service used is not a dependency for another service*). ▪ **systemctl disable** *servicename* ▪ **systemctl stop** *servicename*
Check network connections	Open network connections (open sockets) on a computer create a security risk. A *socket* is an endpoint of a bi-directional communication flow across a computer network. Use the following **netstat** (network statistics) or **ss** (socket statistics) options to identify the open network connections on Linux systems: ▪ **-a** lists both listening and non-listening sockets. ▪ **-l** (*lowercase 'L'*) lists listening sockets. ▪ **-s** displays statistics for each protocol. ▪ **-i** displays a table of all network interfaces.