**Hardening of Linux System.**

What is Linux Hardening?

Most systems have confidential data that needs to be protected. To safeguard this data, we need to secure our Linux system. But how to properly harden a Linux system? In this article, we will cover this step by step. We start by with physical security measures to prevent unauthorized people from access the system in the first place. Next is doing the installation the right way, so we have a solid foundation. Finally, we will apply a set of common security measures.

Linux is already secure by default, right?

One of the myths about Linux is that it is secure, as it is not susceptible to viruses or other forms of malware. This is partially true, as Linux uses the foundations of the original UNIX operating system. Processes are separated and a normal user is restricted in what he or she can do on the system. Still, Linux is not perfectly secure by default. One of the reasons is the Linux distributions that package the GNU/Linux kernel and the related software. They have to choose between usability, performance, and security.

With the difficult choices that Linux distributions have to make, you can be sure of compromises. These compromises typically result in a lowered level of security. What about malware for Linux? That is a definitely a myth. The Linux platform also has its fair share of backdoors, rootkits, works, and even ransomware. That is one of the reasons why it is important to do system hardening, security auditing, and checking for compliance with technical guidelines.

What is system hardening?

To improve the security level of a system, we take different types of measures. This could be the removal of an existing system service or uninstall some software components.

System hardening is the process of doing the ‘right’ things. The goal is to enhance the security level of the system. There are many aspects to securing a system properly. Yet, the basics are similar for most operating systems. So the system hardening process for Linux desktop and servers is that that special.

Normal solutions:

1. ‘**netstat**‘ networking command you can view all open ports and associated programs.

Command: netstat -tulpn

1. **Telnet** and **rlogin** protocols uses plain text, not encrypted format which is the security breaches. **SSH** is a secure protocol that use encryption technology during communication with server. It’s also recommended to change default **SSH 22** port number.

Command:vi /etc/ssh/sshd\_config

PermitRootLogin no

1. Always keep system updated with latest releases patches, security fixes and kernel when it’s available.

Command: yum updates

yum check-update

1. **Cron** has it’s own built in feature, where it allows to specify who may, and who may not want to run jobs. This is controlled by the use of files called **/etc/cron.allow** and **/etc/cron.deny**. To lock a user using cron, simply add user names in **cron.deny** and to allow a user to run cron add in **cron.allow** file. If you would like to disable all users from using cron, add the ‘**ALL**‘ line to **cron.deny** file.

Command: echo ALL >>/etc/cron.deny

1. It’s highly recommended to enable **Linux firewall** to secure unauthorised access of your servers. Apply rules in **iptables** to filters **incoming**, **outgoing** and **forwarding** packets. We can specify the source and destination address to allow and deny in specific **udp/tcp** port number.
2. Move logs in dedicated log server, this may prevents intruders to easily modify local logs.

**/var/log/message** – Where whole system logs or current activity logs are available.

**/var/log/auth.log** – Authentication logs.

**/var/log/kern.log** – Kernel logs.

**/var/log/cron.log** – Crond logs (cron job).

**/var/log/maillog** – Mail server logs.

**/var/log/boot.log** – System boot log.

**/var/log/mysqld.log** – MySQL database server log file.

**/var/log/secure** – Authentication log.

**/var/log/utmp** or **/var/log/wtmp** : Login records file.

**/var/log/yum.lo**g: Yum log files.

### Keep /boot as read-only.

Command: vi /etc/fstab

Add the following line at the bottom, save and close it.

LABEL=/boot /boot ext2 defaults,ro 1 2

## Set Up Password Aging For Linux Users For Better Security.

## Configure Iptables and TCPWrappers based Firewall on Linux.

[Iptables](https://www.cyberciti.biz/faq/category/iptables/) is a user space application program that allows you to configure the firewall (Netfilter) provided by the Linux kernel. Use [firewall](https://bash.cyberciti.biz/firewall/linux-iptables-firewall-shell-script-for-standalone-server/) to filter [out traffic and allow only](https://www.cyberciti.biz/tips/block-spamming-scanning-with-iptables.html) necessary traffic. Also use the [TCPWrappers a host-based](https://www.cyberciti.biz/faq/tcp-wrappers-hosts-allow-deny-tutorial/) networking ACL system to filter network access to Internet.

## Linux Kernel /etc/sysctl.conf Hardening.

/etc/sysctl.conf file is used to [configure kernel parameters](https://www.cyberciti.biz/faq/linux-kernel-etcsysctl-conf-security-hardening/) at runtime. Linux reads and applies settings from /etc/sysctl.conf at boot time.

## Turn Off IPv6 only if you are NOT using it on Linux.

Source :- <https://www.cyberciti.biz/tips/linux-security.html>

<https://www.tecmint.com/linux-server-hardening-security-tips/>

Official Security solutions:

1. **Problem :** The root account must be the only account having unrestricted access to the system. (V-72005)

**Check Text** :

Check the system for duplicate UID "0" assignments with the following command:

# awk -F: '$3 == 0 {print $1}' /etc/passwd

If any accounts other than root have a UID of "0", this is a finding.

**Fix Text** :

Change the UID of any account on the system, other than root, that has a UID of "0".

If the account is associated with system commands or applications, the UID should be changed to one greater than "0" but less than "1000". Otherwise, assign a UID of greater than "1000" that has not already been assigned.

1. **Problem :** The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires. (V-71941)

**Check Text :**

Verify the operating system disables account identifiers (individuals, groups, roles, and devices) after the password expires with the following command:

# grep -i inactive /etc/default/useradd

INACTIVE=0

If the value is not set to "0", is commented out, or is not defined, this is a finding.

**Fix Text :**

Configure the operating system to disable account identifiers (individuals, groups, roles, and devices) after the password expires.

Add the following line to "/etc/default/useradd" (or modify the line to have the required value):

INACTIVE=0

1. **Problem :** The delay between logon prompts following a failed console logon attempt must be at least four seconds. (V-71951)

**Check Text :**

Verify the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt.

Check the value of the "fail\_delay" parameter in the "/etc/login.defs" file with the following command:

# grep -i fail\_delay /etc/login.defs

FAIL\_DELAY 4

If the value of "FAIL\_DELAY" is not set to "4" or greater, this is a finding.

**Fix Text** :

Configure the operating system to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.

Modify the "/etc/login.defs" file to set the "FAIL\_DELAY" parameter to "4" or greater:

FAIL\_DELAY 4

1. **Problem :** Auditing must be configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users. (V-72079)

**Check Text :**

Verify the operating system produces audit records containing information to establish when (date and time) the events occurred.

Check to see if auditing is active by issuing the following command:

# systemctl is-active auditd.service

Active: active (running) since Tue 2015-01-27 19:41:23 EST; 22h ago

If the "auditd" status is not active, this is a finding.

**Fix Text** :

Configure the operating system to produce audit records containing information to establish when (date and time) the events occurred.

Enable the auditd service with the following command:

# chkconfig auditd on

1. **Problem :** The audit system must take appropriate action when the audit storage volume is full. (V-72087)

**Check Text** :

Verify the action the operating system takes if the disk the audit records are written to becomes full.

To determine the action that takes place if the disk is full on the remote server, use the following command:

# grep -i disk\_full\_action /etc/audisp/audisp-remote.conf

disk\_full\_action = single

To determine the action that takes place if the network connection fails, use the following command:

# grep -i network\_failure\_action /etc/audisp/audisp-remote.conf

network\_failure\_action = stop

If the value of the "network\_failure\_action" option is not "syslog", "single", or "halt", or the line is commented out, this is a finding.

If the value of the "disk\_full\_action" option is not "syslog", "single", or "halt", or the line is commented out, this is a finding.

**Fix Text** :

Configure the action the operating system takes if the disk the audit records are written to becomes full.

Uncomment or edit the "disk\_full\_action" option in "/etc/audisp/audisp-remote.conf" and set it to "syslog", "single", or "halt", such as the following line:

disk\_full\_action = single

Uncomment the "network\_failure\_action" option in "/etc/audisp/audisp-remote.conf" and set it to "syslog", "single", or "halt".

1. **Problem :** All uses of the chown,chmod command must be audited. Audit system must take appropriate. (V-72097/105)

**Check Text** :

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chown" syscall occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

# grep -iw chown /etc/audit/audit.rules

-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

If there are no audit rules defined for the "chown" syscall, this is a finding.

**Fix Text** :

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=4294967295 -k perm\_mod

The audit daemon must be restarted for the changes to take effect.

1. **Problem :** All uses of the passwd, su, sudo, ssh-keyen, crontab command must be audited. (V-72149/159/161/179/183)

**Check Text** :

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "passwd" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

# grep -i /usr/bin/passwd /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

If the command does not return any output, this is a finding.

**Fix Text** :

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "passwd" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd

The audit daemon must be restarted for the changes to take effect.

1. **Problem :** The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd. (V-72197)

**Check Text** :

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

# grep /etc/passwd /etc/audit/audit.rules

-w /etc/passwd -p wa -k audit\_rules\_usergroup\_modification

If the command does not return a line, or the line is commented out, this is a finding.

**Fix Text** :

Configure the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Add or update the following rule "/etc/audit/rules.d/audit.rules":

-w /etc/passwd -p wa -k identity

The audit daemon must be restarted for the changes to take effect.

1. **Problem :** The system must not have accounts configured with blank or null password. (V-71937)

**Check Text** :

To verify that null passwords cannot be used, run the following command:

# grep nullok /etc/pam.d/system-auth-ac

If this produces any output, it may be possible to log on with accounts with empty passwords.

If null passwords can be used, this is a finding.

**Fix Text** :

If an account is configured for password authentication but does not have an assigned password, it may be possible to log on to the account without authenticating.

Remove any instances of the "nullok" option in "/etc/pam.d/system-auth-ac" to prevent logons with empty passwords.

Note: Any updates made to "/etc/pam.d/system-auth-ac" may be overwritten by the "authconfig" program. The "authconfig" program should not be used.

1. **Problem :** Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period. (V-71943)

**Check Text** :

Verify the operating system automatically locks an account for the maximum period for which the system can be configured.

Check that the system locks an account for the maximum period after three unsuccessful logon attempts within a period of 15 minutes with the following command:

# grep pam\_faillock.so /etc/pam.d/password-auth-ac

auth required pam\_faillock.so preauth silent audit deny=3 even\_deny\_root unlock\_time=604800

auth [default=die] pam\_faillock.so authfail audit deny=3 even\_deny\_root unlock\_time=604800

account required pam\_faillock.so

If the "unlock\_time" setting is greater than "604800" on both lines with the "pam\_faillock.so" module name or is missing from a line, this is a finding.

# grep pam\_faillock.so /etc/pam.d/system-auth-ac

auth required pam\_faillock.so preauth silent audit deny=3 even\_deny\_root unlock\_time=604800

auth [default=die] pam\_faillock.so authfail audit deny=3 even\_deny\_root unlock\_time=604800

account required pam\_faillock.so

If the "unlock\_time" setting is greater than "604800" on both lines with the "pam\_faillock.so" module name or is missing from a line, this is a finding.

**Fix Text** :

Configure the operating system to lock an account for the maximum period when three unsuccessful logon attempts in 15 minutes are made.

Modify the first three lines of the auth section of the "/etc/pam.d/system-auth-ac" and "/etc/pam.d/password-auth-ac" files to match the following lines:

auth required pam\_faillock.so preauth silent audit deny=3 even\_deny\_root fail\_interval=900 unlock\_time=604800

auth sufficient pam\_unix.so try\_first\_pass

auth [default=die] pam\_faillock.so authfail audit deny=3 even\_deny\_root fail\_interval=900 unlock\_time=604800

account required pam\_faillock.so

1. **Problem :** The system must not have unnecessary accounts. (V-72001)

**Check Text** :

Verify all accounts on the system are assigned to an active system, application, or user account.

Obtain the list of authorized system accounts from the Information System Security Officer (ISSO).

Check the system accounts on the system with the following command:

# more /etc/passwd

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

games:x:12:100:games:/usr/games:/sbin/nologin

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

Accounts such as "games" and "gopher" are not authorized accounts as they do not support authorized system functions.

If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, this is a finding.

**Fix Text** :

Configure the system so all accounts on the system are assigned to an active system, application, or user account.

Remove accounts that do not support approved system activities or that allow for a normal user to perform administrative-level actions.

Document all authorized accounts on the system.

1. **Problem :** There must be no .shosts, vshosts.equiv files on the system. (V-72277/79)

**Check Text** :

Verify there are no ".shosts" files on the system.

Check the system for the existence of these files with the following command:

# find / -name '\*.shosts'

If any ".shosts" files are found on the system, this is a finding.

**Fix Text** :

Remove any found ".shosts" files from the system.

# rm /[path]/[to]/[file]/.shosts

1. **Problem :** The file permissions, ownership, and group membership of system files and commands must match the vendor value. (V-71849)

**Check Text** :

Verify the file permissions, ownership, and group membership of system files and commands match the vendor values.

Check the file permissions, ownership, and group membership of system files and commands with the following command:

# rpm -Va | grep '^.M'

If there is any output from the command indicating that the ownership or group of a system file or command, or a system file, has permissions less restrictive than the default, this is a finding.

**Fix Text** :

Run the following command to determine which package owns the file:

# rpm -qf

Reset the permissions of files within a package with the following command:

#rpm --setperms

Reset the user and group ownership of files within a package with the following command:

#rpm --setugids

1. **Problem :** All files and directories must have a valid owner. (V-72007)

**Check Text**:

Verify all files and directories on the system have a valid owner.

Check the owner of all files and directories with the following command:

Note: The value after -fstype must be replaced with the filesystem type. XFS is used as an example.

# find / -fstype xfs -nouser

If any files on the system do not have an assigned owner, this is a finding.

**Fix Text** :

Either remove all files and directories from the system that do not have a valid user, or assign a valid user to all unowned files and directories on the system with the "chown" command:

# chown

1. **Problem :** The umask must be set to 077 for all local interactive user accounts. (V-72049)

**Check Text** :

Verify that the default umask for all local interactive users is "077".

Identify the locations of all local interactive user home directories by looking at the "/etc/passwd" file.

Check all local interactive user initialization files for interactive users with the following command:

Note: The example is for a system that is configured to create users home directories in the "/home" directory.

# grep -i umask /home/\*/.\*

If any local interactive user initialization files are found to have a umask statement that has a value less restrictive than "077", this is a finding.

**Fix Text** :

Remove the umask statement from all local interactive users’ initialization files.

If the account is for an application, the requirement for a umask less restrictive than "077" can be documented with the Information System Security Officer, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account’s environment variables.

1. **Problem :** If the cron.allow file exists it must be owned by root. (V-72053)

**Check Text** :

Verify that the "cron.allow" file is owned by root.

Check the owner of the "cron.allow" file with the following command:

# ls -al /etc/cron.allow

-rw------- 1 root root 6 Mar 5 2011 /etc/cron.allow

If the "cron.allow" file exists and has an owner other than root, this is a finding.

**Fix Text** :

Set the owner on the "/etc/cron.allow" file to root with the following command:

# chown root /etc/cron.allow

1. **Problem :** The operating system must not allow an unattended or automatic logon to the system via a graphical user interface. (V-71953)

**Check Text** :

Verify the operating system does not allow an unattended or automatic logon to the system via a graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check for the value of the "AutomaticLoginEnable" in the "/etc/gdm/custom.conf" file with the following command:

# grep -i automaticloginenable /etc/gdm/custom.conf

AutomaticLoginEnable=false

If the value of "AutomaticLoginEnable" is not set to "false", this is a finding.

**Fix Text** :

Configure the operating system to not allow an unattended or automatic logon to the system via a graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Add or edit the line for the "AutomaticLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

[daemon]

AutomaticLoginEnable=false

1. **Problem :** USB mass storage must be disabled. (V-71983)

**Check Text** :

If there is an HBSS with a Device Control Module and a Data Loss Prevention mechanism, this requirement is not applicable.

Verify the operating system disables the ability to use USB mass storage devices.

Check to see if USB mass storage is disabled with the following command:

# grep usb-storage /etc/modprobe.d/blacklist.conf

blacklist usb-storage

If the command does not return any output or the output is not "blacklist usb-storage", and use of USB storage devices is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

**Fix Text** :

Configure the operating system to disable the ability to use USB mass storage devices.

# vi /etc/modprobe.d/blacklist.conf

Add or update the line:

blacklist usb-storage

1. **Problem :** The operating system must enable SELinux. (V-71989)

**Check Text** :

Verify the operating system verifies correct operation of all security functions.

Check if "SELinux" is active and in "Enforcing" mode with the following command:

# getenforce

Enforcing

If "SELinux" is not active and not in "Enforcing" mode, this is a finding.

**Fix Text** :

Configure the operating system to verify correct operation of all security functions.

Set the "SELinux" status and the "Enforcing" mode by modifying the "/etc/selinux/config" file to have the following line:

SELINUX=enforcing

A reboot is required for the changes to take effect.

1. **Problem :** Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. (V-71961)

**Check Text** :

Check to see if an encrypted root password is set. On systems that use a BIOS, use the following command:

# grep -i ^password\_pbkdf2 /boot/grub2/grub.cfg

password\_pbkdf2 superusers-account password-hash

If the root password entry does not begin with "password\_pbkdf2", this is a finding.

**Fix Text** :

Configure the system to encrypt the boot password for root.

Generate an encrypted grub2 password for root with the following command:

Note: The hash generated is an example.

# grub-mkpasswd-pbkdf2

Enter Password:

Reenter Password:

PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.F3A7CFAA5A51EED123BE8238C23B25B2A6909AFC9812F0D45

Using this hash, modify the "/etc/grub.d/10\_linux" file with the following commands to add the password to the root entry:

# cat << EOF

> set superusers="root" password\_pbkdf2 smithj grub.pbkdf2.sha512.10000.F3A7CFAA5A51EED123BE8238C23B25B2A6909AFC9812F0D45

> EOF

Generate a new "grub.conf" file with the new password with the following commands:

# grub2-mkconfig --output=/tmp/grub2.cfg

# mv /tmp/grub2.cfg /boot/grub2/grub.cfg

1. **Problem :** The operating system must enable the SELinux targeted policy. (V-71991)

**Check Text** :

Verify the operating system verifies correct operation of all security functions.

Check if "SELinux" is active and is enforcing the targeted policy with the following command:

# sestatus

SELinux status: enabled

SELinuxfs mount: /selinux

SELinux root directory: /etc/selinux

Loaded policy name: targeted

Current mode: enforcing

Mode from config file: enforcing

Policy MLS status: enabled

Policy deny\_unknown status: allowed

Max kernel policy version: 28

If the "Policy from config file" is not set to "targeted", or the "Loaded policy name" is not set to "targeted", this is a finding.

**Fix Text** :

Configure the operating system to verify correct operation of all security functions.

Set the "SELinuxtype" to the "targeted" policy by modifying the "/etc/selinux/config" file to have the following line:

SELINUXTYPE=targeted

A reboot is required for the changes to take effect.

1. **Problem :** The x86 Ctrl-Alt-Delete key sequence must be disabled. (V-71993)

**Check Text** :

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed.

Check that the ctrl-alt-del.service is not active with the following command:

# systemctl status ctrl-alt-del.service

reboot.target - Reboot

Loaded: loaded (/usr/lib/systemd/system/reboot.target; disabled)

Active: inactive (dead)

Docs: man:systemd.special(7)

If the ctrl-alt-del.service is active, this is a finding.

**Fix Text** :

Configure the system to disable the Ctrl-Alt\_Delete sequence for the command line with the following command:

# systemctl mask ctrl-alt-del.target

If GNOME is active on the system, create a database to contain the system-wide setting (if it does not already exist) with the following command:

# cat /etc/dconf/db/local.d/00-disable-CAD

Add the setting to disable the Ctrl-Alt\_Delete sequence for GNOME:

[org/gnome/settings-daemon/plugins/media-keys]

logout=’’

1. **Problem :** The system must use a virus scan program. (V-72213)

**Check Text** :

Verify the system is using a virus scan program.

Check for the presence of "McAfee VirusScan Enterprise for Linux" with the following command:

# systemctl status nails

nails - service for McAfee VirusScan Enterprise for Linux

> Loaded: loaded /opt/NAI/package/McAfeeVSEForLinux/McAfeeVSEForLinux-2.0.2.; enabled)

> Active: active (running) since Mon 2015-09-27 04:11:22 UTC;21 min ago

If the "nails" service is not active, check for the presence of "clamav" on the system with the following command:

# systemctl status clamav-daemon.socket

systemctl status clamav-daemon.socket

clamav-daemon.socket - Socket for Clam AntiVirus userspace daemon

Loaded: loaded (/lib/systemd/system/clamav-daemon.socket; enabled)

Active: active (running) since Mon 2015-01-12 09:32:59 UTC; 7min ago

If neither of these applications are loaded and active, ask the System Administrator if there is an antivirus package installed and active on the system.

If no antivirus scan program is active on the system, this is a finding.

**Fix Text** :

Install an antivirus solution on the system.

1. **Problem :** All network connections associated with a communication session must be terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements. (V-72223)

**Check Text** :

Verify the operating system terminates all network connections associated with a communications session at the end of the session or based on inactivity.

Check the value of the system inactivity timeout with the following command:

# grep -i tmout /etc/bashrc /etc/profile.d/\*

TMOUT=600

If "TMOUT" is not set to "600" or less in "/etc/bashrc" or in a script created to enforce session termination after inactivity, this is a finding.

**Fix Text** :

Configure the operating system to terminate all network connections associated with a communications session at the end of the session or after a period of inactivity.

Add or update the following lines in "/etc/profile".

TMOUT=600

readonly TMOUT

export TMOUT

Or create a script to enforce the inactivity timeout (for example /etc/profile.d/tmout.sh) such as:

#!/bin/bash

TMOUT=600

readonly TMOUT

export TMOUT

1. **Problem :** SNMP community strings must be changed from the default. (V-72313)

**Check Text** :

Verify that a system using SNMP is not using default community strings.

Check to see if the "/etc/snmp/snmpd.conf" file exists with the following command:

# ls -al /etc/snmp/snmpd.conf

-rw------- 1 root root 52640 Mar 12 11:08 snmpd.conf

If the file does not exist, this is Not Applicable.

If the file does exist, check for the default community strings with the following commands:

# grep public /etc/snmp/snmpd.conf

# grep private /etc/snmp/snmpd.conf

If either of these commands returns any output, this is a finding.

**Fix Text** :

If the "/etc/snmp/snmpd.conf" file exists, modify any lines that contain a community string value of "public" or "private" to another string value.

1. The operating system must enable an application firewall, if available. (V-72273)

**Check Text** :

Verify the operating system enabled an application firewall.

Check to see if "firewalld" is installed with the following command:

# yum list installed firewalld

firewalld-0.3.9-11.el7.noarch.rpm

If the "firewalld" package is not installed, ask the System Administrator if another firewall application (such as iptables) is installed.

If an application firewall is not installed, this is a finding.

Check to see if the firewall is loaded and active with the following command:

# systemctl status firewalld

firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)

Active: active (running) since Tue 2014-06-17 11:14:49 CEST; 5 days ago

If "firewalld" does not show a status of "loaded" and "active", this is a finding.

Check the state of the firewall:

# firewall-cmd --state

running

If "firewalld" does not show a state of "running", this is a finding.

**Fix Text** :

Ensure the operating system's application firewall is enabled.

Install the "firewalld" package, if it is not on the system, with the following command:

# yum install firewalld

Start the firewall via "systemctl" with the following command:

# systemctl start firewalld

1. The rsh-server,ypserv,nis,telnet-server package must not be installed. (V-71967/69/2077)

**Check Text** :

Check to see if the rsh-server package is installed with the following command:

# yum list installed rsh-server

If the rsh-server package is installed, this is a finding.

**Fix Text** :

Configure the operating system to disable non-essential capabilities by removing the rsh-server package from the system with the following command:

# yum remove rsh-server

1. **Problem :** The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization. (V-71977)

**Check Text**:

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components from a repository without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

Check that yum verifies the signature of packages from a repository prior to install with the following command:

# grep gpgcheck /etc/yum.conf

gpgcheck=1

If "gpgcheck" is not set to "1", or if options are missing or commented out, ask the System Administrator how the certificates for patches and other operating system components are verified.

If there is no process to validate certificates that is approved by the organization, this is a finding.

**Fix Text** :

Configure the operating system to verify the signature of packages from a repository prior to install by setting the following option in the "/etc/yum.conf" file:

gpgcheck=1

1. **Problem :** The operating system must be a vendor supported release. (V-71997)

**Check Text** :

Verify the version of the operating system is vendor supported.

Check the version of the operating system with the following command:

# cat /etc/redhat-release

Red Hat Enterprise Linux Server release 7.2 (Maipo)

Current End of Life for RHEL 7.2 is Q4 2020.

Current End of Life for RHEL 7.3 is 30 June 2024.

If the release is not supported by the vendor, this is a finding.

**Fix Text** : Upgrade to a supported version of the operating system.

1. **Problem :** A File Transfer Protocol (FTP),Trivial File Transfer Protocol (TFTP) server package must not be installed unless needed. (V-72299/301)

**Check Text** :

Verify an FTP server has not been installed on the system.

Check to see if an FTP server has been installed with the following commands:

# yum list installed vsftpd

vsftpd-3.0.2.el7.x86\_64.rpm

If "vsftpd" is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

**Fix Text** :

Document the "vsftpd" package with the ISSO as an operational requirement or remove it from the system with the following command:

# yum remove vsftpd

1. **Problem :** The SSH daemon must not allow authentication using an empty password. (V-71939)

**Check Text** :

To determine how the SSH daemon's "PermitEmptyPasswords" option is set, run the following command:

# grep -i PermitEmptyPasswords /etc/ssh/sshd\_config

PermitEmptyPasswords no

If no line, a commented line, or a line indicating the value "no" is returned, the required value is set.

If the required value is not set, this is a finding.

**Fix Text** :

To explicitly disallow remote logon from accounts with empty passwords, add or correct the following line in "/etc/ssh/sshd\_config":

PermitEmptyPasswords no

The SSH service must be restarted for changes to take effect. Any accounts with empty passwords should be disabled immediately, and PAM configuration should prevent users from being able to assign themselves empty passwords.

1. The operating system must not allow users to override SSH environment variables. (V-71957)

**Check Text** :

Verify the operating system does not allow users to override environment variables to the SSH daemon.

Check for the value of the "PermitUserEnvironment" keyword with the following command:

# grep -i permituserenvironment /etc/ssh/sshd\_config

PermitUserEnvironment no

If the "PermitUserEnvironment" keyword is not set to "no", is missing, or is commented out, this is a finding.

**Fix Text** :

Configure the operating system to not allow users to override environment variables to the SSH daemon.

Edit the "/etc/ssh/sshd\_config" file to uncomment or add the line for "PermitUserEnvironment" keyword and set the value to "no":

PermitUserEnvironment no

The SSH service must be restarted for changes to take effect.

1. **Problem :** The operating system must not allow a non-certificate trusted host SSH logon to the system. (V-71959)

**Check Text** :

Verify the operating system does not allow a non-certificate trusted host SSH logon to the system.

Check for the value of the "HostbasedAuthentication" keyword with the following command:

# grep -i hostbasedauthentication /etc/ssh/sshd\_config

HostbasedAuthentication no

If the "HostbasedAuthentication" keyword is not set to "no", is missing, or is commented out, this is a finding.

**Fix Text** :

Configure the operating system to not allow a non-certificate trusted host SSH logon to the system.

Edit the "/etc/ssh/sshd\_config" file to uncomment or add the line for "HostbasedAuthentication" keyword and set the value to "no":

HostbasedAuthentication no

The SSH service must be restarted for changes to take effect.

1. **Problem :** The system must not permit direct logons to the root account using remote access via SSH. (V-72247)

**Check Text** :

Verify remote access using SSH prevents users from logging on directly as root.

Check that SSH prevents users from logging on directly as root with the following command:

# grep -i permitrootlogin /etc/ssh/sshd\_config

PermitRootLogin no

If the "PermitRootLogin" keyword is set to "yes", is missing, or is commented out, this is a finding.

**Fix Text** :

Configure SSH to stop users from logging on remotely as the root user.

Edit the appropriate "/etc/ssh/sshd\_config" file to uncomment or add the line for the "PermitRootLogin" keyword and set its value to "no" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

PermitRootLogin no

The SSH service must be restarted for changes to take effect.

1. **Problem :** The SSH daemon must be configured to only use the SSHv2 protocol. (V-72251)

**Check Text** :

Verify the SSH daemon is configured to only use the SSHv2 protocol.

Check that the SSH daemon is configured to only use the SSHv2 protocol with the following command:

# grep -i protocol /etc/ssh/sshd\_config

Protocol 2

#Protocol 1,2

If any protocol line other than "Protocol 2" is uncommented, this is a finding.

**Fix Text** :

Remove all Protocol lines that reference version "1" in "/etc/ssh/sshd\_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor). The "Protocol" line must be as follows:

Protocol 2

The SSH service must be restarted for changes to take effect.

1. **Problem :** Remote X connections for interactive users must be encrypted. (V-72303)

**Check Text** :

Verify remote X connections for interactive users are encrypted.

Check that remote X connections are encrypted with the following command:

# grep -i x11forwarding /etc/ssh/sshd\_config

X11Fowarding yes

If the "X11Forwarding" keyword is set to "no", is missing, or is commented out, this is a finding.

**Fix Text** :)

Configure SSH to encrypt connections for interactive users.

Edit the "/etc/ssh/sshd\_config" file to uncomment or add the line for the "X11Forwarding" keyword and set its value to "yes" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

X11Fowarding yes

The SSH service must be restarted for changes to take effect.

Reference : <https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/>