**January 2019**

**Hardening guide for CentOS 7**

**Document control**

**Distribution List**

**Electronic Distribution:** The master copy of this document is stored in electronic format. Any hard copies or soft copies that have not been authorized and included on a distribution list are for information only and are not subject to Micro Focus’s documentation management.

This document may be distributed to Micro Focus PSDC & Psec Management personnel only or privileged Micro Focus employees as defined within the document hosting system.

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Prepared by** | Snir Karat | **Document Version No:** | 1.0 |
| **Title** | Hardening guide for CentOS 7 | **Document Major Version Date:** | 03/01/2019 |

**Change History**

The following Change History log contains a record of changes made to this document:

| Version | Date | Author | Changes | Approved by |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

#### Table of Contents

1. Secure BIOS/UEFI ‎3

2. Secure Boot Loader 3

3. Use Separate Disk Partitions 3

4. Create Separate Partition for /tmp 3

5. Verify CentOS GPG Key is Installed 4

6. Install Only the Minimum Amount of Packages Required 4

7. Update the System Frequently 4

8. Remove Unnecessary Software Packages 4

9. Install Advanced Intrusion Detection Environment (AIDE) 5

10. Implement Periodic Execution of File Integrity 5

11. Remove Unneeded Services 5

12. Remove Telnet 6

13. Remove RSH 6

14. Remove NIS 6

15. Remove TFTP 6

16. Packet-Filtering Firewall 7

17. Disable Useless SUID and SGID Commands 7

18. Install NTP 7

19. Check for Files and Directories Without an Owner 7

20. Restrict Core Dumps 8

21. Create Strong Passwords 8

22. Apply Strong Password Policy 8

23. Use Password Aging 9

24. Prevent Accounts Shell Access 9

25. Force Read-Only Mounting of USB Media 9

26. Disabling Root Access via TTY 10

27. Use POSIX ACLs to Expand System Permissions 10

28. Setup SELinux in Enforce Mode 10

29. Install SELinux Additional Utilities 11

30. Hardening /etc/sysctl.conf 11

31. Modify User Environment Variables 12

1. Secure BIOS/UEFI

Start the process of harden your machine by securing BIOS/UEFI settings, especially set a BIOS/UEFI password and disable boot media devices (CD, DVD, disable USB support) in order to prevent an unauthorized users from modifying the system BIOS settings or altering the boot device priority and booting the machine from an alternate medium.

1. Secure Boot Loader

Set a GRUB password in order to prevent malicious users to tamper with kernel boot sequence or run levels, edit kernel parameters or start the system into single user mode in order to harm your system and reset root password to gain privileged control.

1. Use Separate Disk Partitions

When installing CentOS on systems intended as production servers use dedicated partitions or dedicated hard disks for the following parts of the system:

/(root)

/boot

/home

/tmp

/var

1. Create Separate Partition for /tmp

The /tmp directory is a world-writable directory used for temporary storage by all users and some applications.

Separate partitions intended for storing data and prevent the execution of programs, device files or setuid bit on these type of partitions by adding the following options to fstab file as illustrated on the below excerpt:

/dev/sda5 /nas ext4 defaults,nosuid,nodev,noexec 1 2

To prevent privilege-escalation and arbitrary script execution create a separate partition for /tmp and mount it as nosuid, nodev and noexec.

/dev/sda6 /tmp ext4 defaults,nosuid,nodev,noexec 0 0

1. Verify CentOS GPG Key is Installed

CentOS cryptographically signs updates with a GPG key to verify that they are valid.

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system.

Run the following command to ensure that the system has the CentOS GPG key properly installed:

# rpm -q --queryformat "%{SUMMARY}\n" gpg-pubkey

Compare the GPG key with the one from CentOS's web site at <http://mirror.centos.org/centos/>

The following command can be used to print the installed release key's fingerprint, which is actually contained in the file referenced below:

# gpg --quiet --with-fingerprint /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

1. Install Only the Minimum Amount of Packages Required

Avoid installing unimportant or unnecessary programs, applications or services to avoid package vulnerabilities. This can decrease the risk that the compromise of a piece of software may lead to compromise other applications, parts of the system or even file systems, finally resulting in data corruption or data loss.

1. Update the System Frequently

Update the system regularly. Keep Linux kernel in sync with the latest security patches and all the installed software up-to-date with the latest versions by issuing the below command:

# yum update

1. Remove Unnecessary Software Packages

Install minimal software required for your server.

Do not install extra programs or services.

Install packages only from trusted or official repositories.

Verify installed packages using one of the following commands:

# rpm -qa

Make a local list of all installed packages.

# yum list installed >> installed.txt

Consult the list for useless software and delete a package by issuing the below command:

# yum remove package\_name

1. Install Advanced Intrusion Detection Environment (AIDE)

AIDE is a file integrity checking tool, similar in nature to Tripwire. While it cannot prevent intrusions, it can detect unauthorized changes to configuration files by alerting when the files are changed. When setting up AIDE, decide internally what the site policy will be concerning integrity checking. Review the AIDE quick start guide and AIDE documentation before proceeding.

Perform the following to determine if AIDE is installed:

# rpm -q aide aide.<package version>.<hardware platform>

Use yum to install AIDE (-y option may be used to assume yes at all prompts):

# yum install aide <Output messages from Yum install> aide.<hardware platform> <package version> installed

Initialize AIDE:

# /usr/sbin/aide --init -B 'database\_out=file:/var/lib/aide/aide.db.gz'

1. Implement Periodic Execution of File Integrity

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Execute the following command:

# crontab -u root -e Add the following line to the crontab:

Add the following line to the crontab:

0 5 \* \* \* /usr/sbin/aide --check

**Note**: The checking in this instance occurs every day at 5am. Alter the frequency and time of the checks in compliance with site policy.

1. Remove Unneeded Services

Identify the services that are listening on specific ports using the following command:

# ss -tulpn

To list all installed services with their output status issue the below command:

# systemctl list-units -t service

**Note**: CentOS 7 default minimal installation comes with Postfix daemon installed by default which runs by the name of master under port 25. Remove Postfix network service in case your machine will not be used as a mail server.

# yum remove postfix

1. Remove telnet Clients

The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an authorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.

Perform the following to remove telnet from the system:

# yum erase telnet

1. Remove rsh-server

The Berkeley rsh-server (rsh, rlogin, rcp) package contains legacy services that exchange credentials in clear-text.

Perform the following to determine if rsh-server is installed on the system.

# rpm -q rsh-server package rsh-server is not installed

Perform the following to remove rsh-server from the system:

# yum erase rsh-server

Perform the following to remove rsh from the system:

# yum erase rsh

1. Remove NIS Client

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Perform the following to remove ypbind from the system:

# yum erase ypbind

# yum erase ypserv

1. Remove tftp

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol, typically used to automatically transfer configuration or boot files between machines. TFTP does not support authentication and can be easily hacked.

Perform the following to remove TFTP from the system:

# yum erase tftp

# yum erase tftp-server

1. Packet-Filtering Firewall

Use firewalld utility to protect the system ports, open or close specific services ports, especially well-known ports (<1024).

Install, start, enable and list the firewall rules by issuing the below commands:

# yum install firewalld

# systemctl start firewalld.service

# systemctl enable firewalld.service

# firewall-cmd --list-all

1. Disable Useless SUID and SGID Commands

If the setuid and setgid bits are set on binary programs, these commands can run tasks with other user or group rights, such as root privileges which can pose seriously security issues.

Often, buffer overrun attacks can exploit such executable binaries to run unauthorized code with the rights of a root power user.

# find / -path /proc -prune -o -type f \( -perm -4000 -o -perm -2000 \) -exec ls -l {} \;

To unset the setuid bit execute the below command:

# chmod u-s /path/to/binary\_file

To unset the setgid bit run the below command:

# chmod g-s /path/to/binary\_file

1. Install NTP

NTP is required for a number of compliance audits and is general good practice.

yum install ntp ntpdate

chkconfig ntpd on

ntpdate pool.ntp.org

/etc/init.d/ntpd start

1. Check for Files and Directories Without an Owner

Files or directories not owned by a valid account must be deleted or assigned with permissions from a user and group.

Issue the below command to list files or directories with no user and group:

# find / -nouser -o -nogroup -exec ls -l {} \;

1. Restrict Core Dumps

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

Setting the fs.suid\_dumpable variable to 0 will prevent setuid programs from dumping core.

Perform the following to determine if core dumps are restricted:

# grep "hard core" /etc/security/limits.conf \* hard core 0

38 | P ag e

# /sbin/sysctl fs.suid\_dumpable fs.suid\_dumpable = 0

Add the following line to the /etc/security/limits.conf file:

\* hard core 0

Add the following line to the /etc/sysctl.conf file:

fs.suid\_dumpable = 0

1. Create Strong Passwords

Create a password of minimum of seven characters. The password must contain digits, special characters and uppercase letters.

It is possible to use pwmake to generate a password of 128 bits from /dev/urandom file.

# pwmake 128

1. Apply Strong Password Policy

Force the system to use strong passwords by adding the below line in /etc/pam.d/passwd file:

password required pam\_pwquality.so retry=3

Adding the above line, the password entered cannot contain more than 3 characters in a monotonic sequence, such as abcd, and more than 3 identical consecutive characters, such as 1111.

To force users to use a password with a minimum length of 7 characters, including all classes of characters, strength-check for character sequences and consecutive characters add the following lines to the /etc/security/pwquality.conf file:

minlen = 7

minclass = 4

maxsequence = 3

maxrepeat = 3

1. Use Password Aging

The change command can be used for user password aging.

To set a user’s password to expire in 90 days, use the following command:

# change -M 90 username

To disable password expiration time use the command:

# change -M -1 username

Force immediate password expiration (user must change password on next login) by running the following command:

# change -d 0 username

1. Prevent Accounts Shell Access

To prevent a system account (ordinary account or service account) to gain access to bash shell, change root shell to /usr/sbin/nologin or /bin/false in the /etc/passwd file by issuing the command below:

# usermod -s /bin/false username

To change the shell when creating a new user issue the following command:

# useradd -s /usr/sbin/nologin username

1. Force Read-Only Mounting of USB Media

Using blockdev utility you can force all removable media to be mounted as read-only. For instance, create a new udev configuration file named 80-readonly-usb.rules in the /etc/udev/rules.d/ directory with the following content:

SUBSYSTEM=="block",ATTRS{removable}=="1",RUN{program}="/sbin/blockdev --setro %N"

Then, apply the rule with the below command:

# udevadm control –reload

1. Disabling Root Access via TTY

To prevent the root account from performing system log-in via all console devices (tty), erase the contents of securetty file by typing the following command terminal prompt as root.

# cp /etc/securetty /etc/securetty.bak

# cat /dev/null > /etc/securetty

Remember that this rule does not apply to SSH login sessions

To prevent root login via SSH edit the file /etc/ssh/sshd\_config and add the below line:

PermitRootLogin no

1. Use POSIX ACLs to Expand System Permissions

Access Control Lists can define access rights for more than just a single user or group and can specify rights for programs, processes, files, and directories. If you set ACL on a directory, its descendants will inherit the same rights automatically.

For example:

# setfacl -m u:user:rw file

# getfacl file

1. Setup SELinux in Enforce Mode

The SELinux enhancement to the Linux kernel implements the Mandatory Access Control (MAC) policy, allowing users to define a security policy that provides granular permissions for all users, programs, processes, files, and devices.

The kernel’s access control decisions are based on all the security relevant context and not on the authenticated user identity.

To get Selinux status and enforce policy run the below commands:

# getenforce

# setenforce 1

# sestatus

1. Install SELinux Additional Utilities

Install policycoreutils-python package which provides additional Python utilities for operating SELinux: audit2allow, audit2why, chcat, and semanage.

To display all boolean values together with a short description, use the following command:

# semanage boolean -l

For instance, to display and set the value of httpd\_enable\_ftp\_server, run the below command:

# getsebool httpd\_enable\_ftp\_server

To make the value of a boolean persist across reboots, specify the -P option to setsebool, as illustrated on the following example:

# setsebool -P httpd\_enable\_ftp\_server on

1. Hardening /etc/sysctl.conf

Use the following kernel parameters rules to protect the system:

Disabling Source Routing -

net.ipv4.conf.all.accept\_source\_route=0

Disable IPv4 forwarding -

ipv4.conf.all.forwarding=0

Disable IPv6 -

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1

net.ipv6.conf.lo.disable\_ipv6 = 1

Disable the acceptance and sending of ICMP redirected packets unless specifically required-

net.ipv4.conf.all.accept\_redirects=0

net.ipv4.conf.all.secure\_redirects=0

net.ipv4.conf.all.send\_redirects=0

Disable Reverse Path Forwarding -

net.ipv4.conf.all.rp\_filter=2

Ignore all ICMP echo requests (set to 1 to enable) -

net.ipv4.icmp\_echo\_ignore\_all = 0

1. Modify User Environment Variables

Append date and time format to store commands execution by issuing the below command:

# echo 'HISTTIMEFORMAT="%d/%m/%y %T "' >> .bashrc'

Force to instantly record HISTFILE every time a command is typed (instead of logout):

# echo ‘PROMPT\_COMMAND="history -a"’ >> .bashrc

Limit timeout login session. Automatically tear-down the shell when no activity is performed during idle time period. Very useful to automatically disconnect SSH sessions.

# echo ‘TMOUT=120’ >> .bashrc

Apply all the rules by executing:

# source .bashrc