**CIS Red Hat Enterprise Linux 7 Benchmark v2.2.0**

**Hardening Script Usage Guide**

**Version 1.0**

Contents

[1. Introduction 1](#_Toc517787236)

[2. Pre-setup prior to script usage 1](#_Toc517787237)

[2.1 Initial installation of Red Hat Enterprise Linux 7 1](#_Toc517787238)

[2.2 Initial installation of packages needed 1](#_Toc517787239)

[2.3 Manual Configuration (Refer to CIS RedHat Enterprise Linux 7 Benchmark) 1](#_Toc517787240)

[3 Script usage 2](#_Toc517787242)

[3.1 Script Installation 2](#_Toc517787243)

[3.2 Running the script 2](#_Toc517787244)

[4 Post-setup after script usage 3](#_Toc517787245)

[4.1 Manual Configuration (Refer to CIS RedHat Enterprise Linux 7 Benchmark) 3](#_Toc517787246)

[5 Appendix 4](#_Toc517787247)

[5.1 CIS RedHat Enterprise Linux 7 Benchmark 4](#_Toc517787248)

[5.2 CIS Scripts 4](#_Toc517787249)

# Introduction

This document serves as a guide for the installation and usage of the hardening script for Red Hat Enterprise Linux 7 based off the CIS benchmark.

The script is coded in bash/shell.

# Pre-setup prior to script usage

## 2.1 Initial installation of Red Hat Enterprise Linux 7

Ensure that the server has been registered and enabled through the subscription-manager.

Ensure that the server has the latest packages, kernels and security patches up to date by using the command yum update

## 2.2 Initial installation of packages needed

The package dos2unix has to be install prior to running the script by using the command yum install dos2unix –y

## 2.3 Manual Configuration (Refer to CIS RedHat Enterprise Linux 7 Benchmark)

1. 1.2.1 Ensure package manager repositories are configured (Not Scored)
2. 1.2.3 Ensure GPG keys are configured (Not Scored)
3. 1.2.4 Ensure Red Hat Subscription Manager connection is configured (Not Scored)
4. 1.7.1.1 Ensure message of the day is configured properly (Scored)
5. 1.7.1.2 Ensure local login warning banner is configured properly (Not Scored)
6. 1.7.1.3 Ensure remote login warning banner is configured properly (Not Scored)
7. 2.2.1.2 Ensure ntp is configured (Scored)
8. 2.2.1.3 Ensure chrony is configured (Scored)
9. 2.2.2 Ensure X Window System is not installed (Scored)
10. 3.4.2 Ensure /etc/hosts.allow is configured (Scored)
11. 4.1.12 Ensure use of privileged commands is collected (Scored)
12. 4.2.1.2 Ensure logging is configured (Not Scored)
13. 4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host (Scored)
14. **4.2.2.x This section only applies if syslog-ng is installed on the system.**
15. 4.2.2.1 Ensure syslog-ng service is enabled (Scored)
16. 4.2.2.2 Ensure logging is configured (Not Scored)
17. 4.2.2.3 Ensure syslog-ng default file permissions configured (Scored)
18. 4.2.2.4 Ensure syslog-ng is configured to send logs to a remote log host (Not Scored)
19. 4.2.2.5 Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)
20. 4.2.3 Ensure rsyslog or syslog-ng is installed (Scored)
21. 4.3 Ensure logrotate is configured (Not Scored)
22. 5.2.14 Ensure SSH access is limited (Scored)
23. 5.4.1.5 Ensure all users last password change date is in the past (Scored)
24. 5.4.2 Ensure system accounts are non-login (Scored)
25. 5.5 Ensure root login is restricted to system console (Not Scored)
26. 5.6 Ensure access to the su command is restricted (Scored)
27. 6.1.1 Audit system file permissions (Not Scored)

# Script usage

## 3.1 Script Installation

Ensure that the following files are present in the server and are in the same folder.

1. CIS\_Master.sh
2. 1\_Initial\_Setup.sh
3. 2\_Services.sh
4. 3\_Network\_Configuration.sh
5. 4\_Logging\_and\_Auditing\_64bit.sh
6. 4\_Logging\_and\_Auditing\_32bit.sh
7. 5\_Access\_Authentication\_Authorization.sh
8. 6\_System\_Maintenance.sh

Enter the command dos2unix CIS\_Master.sh to ensure that the script is in the unix format.

## 3.2 Running the script

Ensure that you are running as root before running the script.

Run CIS\_Master.sh by using the command ./CIS\_Master.sh while in the same folder as the residing files.

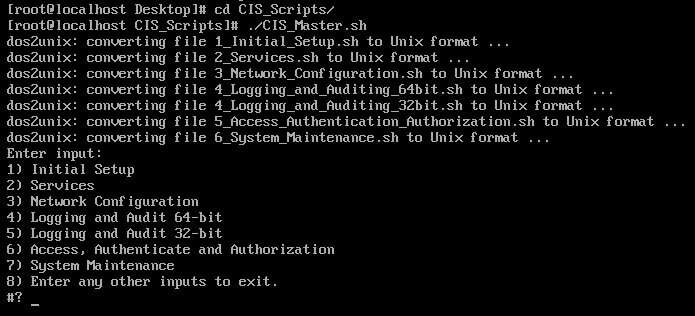


Figure.1. Screenshot of the menu that will be shown after running the script successfully

Proceed with entering the numbers in sequence (with the exception being 4&5, depending on the server type – 32bit or 64bit)

For 64-bit systems that have arch as a rule parameter, you will need two rules: one for 64-bit and one for 32-bit systems. For 32-bit systems, only one rule is needed. For 64-bit system, select option 4 as shown in Figure.2. For 32-bit system, select option 5.

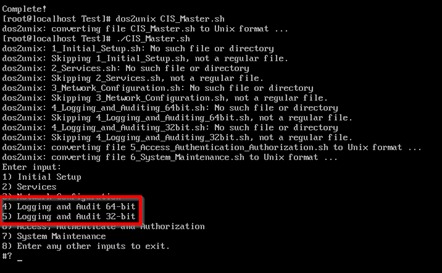


Figure.2. Screenshot of the menu highlighting the option

Once all the hardening sub-scripts have been executed in order, enter any other inputs to exit the script.

# Post-setup after script usage

## 4.1 Manual Configuration (Refer to CIS RedHat Enterprise Linux 7 Benchmark)

1. 1.3.2 Ensure filesystem integrity is regularly checked (Scored)
2. 1.4.2 Ensure bootloader password is set (Scored)
3. 1.5.2 Ensure XD/NX support is enabled (Not Scored)
4. 3.6.5 Ensure firewall rules exist for all open ports (Scored)
5. 3.7 Ensure wireless interfaces are disabled (Not Scored)
6. 6.1.10 Ensure no world writable files exist (Scored)
7. 6.1.11 Ensure no unowned files or directories exist (Scored)
8. 6.1.12 Ensure no ungrouped files or directories exist (Scored)
9. 6.1.13 Audit SUID executables (Not Scored)
10. 6.1.14 Audit SGID executables (Not Scored)
11. 6.2.1 Ensure password fields are not empty (Scored)
12. 6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Scored)
13. 6.2.3 Ensure no legacy "+" entries exist in /etc/shadow (Scored)
14. 6.2.4 Ensure no legacy "+" entries exist in /etc/group (Scored)
15. 6.2.5 Ensure root is the only UID 0 account (Scored)
16. 6.2.6 Ensure root PATH Integrity (Scored)
17. 6.2.7 Ensure all users' home directories exist (Scored)
18. 6.2.8 Ensure users' home directories permissions are 750 or more restrictive (Scored)
19. 6.2.9 Ensure users own their home directories (Scored)
20. 6.2.10 Ensure users' dot files are not group or world writable (Scored)
21. 6.2.11 Ensure no users have .forward files (Scored)
22. 6.2.12 Ensure no users have .netrc files (Scored)
23. 6.2.13 Ensure users' .netrc Files are not group or world accessible (Scored)
24. 6.2.14 Ensure no users have .rhosts files (Scored)
25. 6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Scored)
26. 6.2.16 Ensure no duplicate UIDs exist (Scored)
27. 6.2.17 Ensure no duplicate GIDs exist (Scored)
28. 6.2.18 Ensure no duplicate user names exist (Scored)
29. 6.2.19 Ensure no duplicate group names exist (Scored)

# Appendix

## 5.1 CIS RedHat Enterprise Linux 7 Benchmark



## 5.2 CIS Scripts

