Hardening + Debian + CIS Benchmarks

Moisés Santos Farias

github.com/moisesmsf

moisesmsf@proton.me

DebianDay
Maceió 2023

Agenda

About me

Hardening

Debian

CIS Benchmarks

Questions?

About me

Privacy | Anonymity | SecOps | Monero

Piaçabuçu - AL

Ministério das Comunicações (MCom)

DebianDay
Maceió 2023

Hardening

Community-based | Battle-tested | Practical
Compliance & Auditing

- NIST Cybersecurity Framework + Special Publication 800, 1800
- CIS Critical Security Controls
- ISO 27k
- PCI-DSS
- HIPAA
- CyBok
- Essential Eight
- Gov.BR - PPSI

DebianDay
Maceió 2023

Hardening

Examples

VMware Security Hardening Guides

Microsoft Security Baselines

Security Technical Implementation Guides (STIGs)

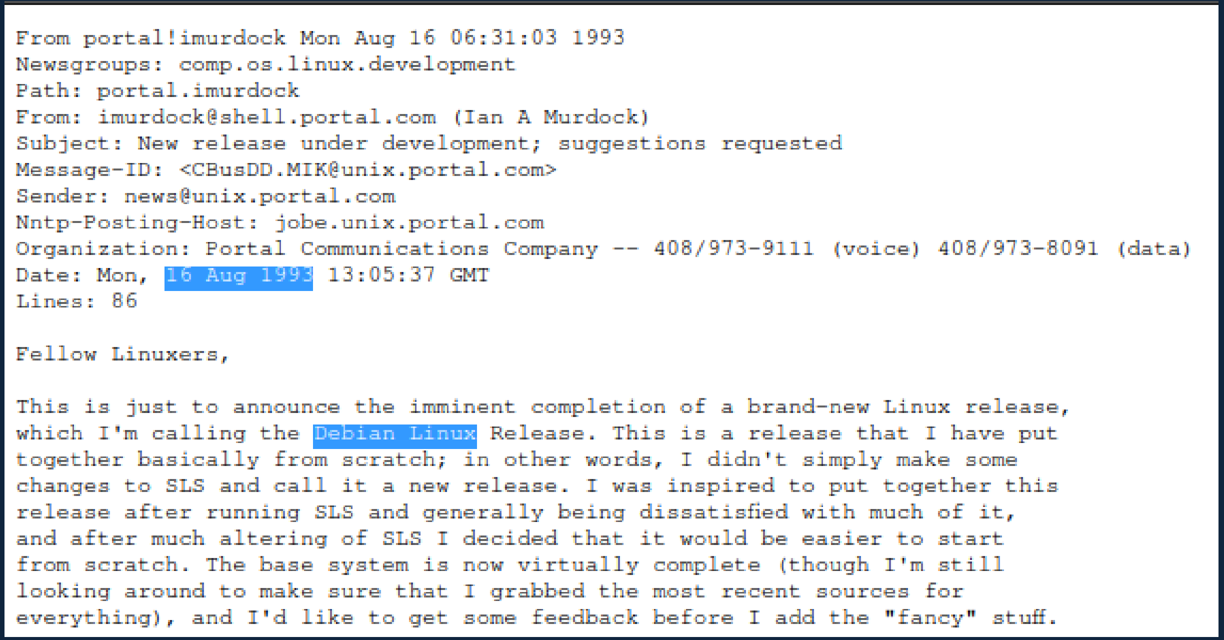
Security Content Automation Protocol (SCAP) | OpenSCAP | NIST NCP

OVAL

CIS Benchmarks

DebianDay
Maceió 2023

Debian



```
From portal!imurdock Mon Aug 16 06:31:03 1993
Newsgroups: comp.os.linux.development
Path: portal.imurdock
From: imurdock@shell.portal.com (Ian A Murdock)
Subject: New release under development; suggestions requested
Message-ID: <CBusDD.MIK@unix.portal.com>
Sender: news@unix.portal.com
Nntp-Posting-Host: jobe.unix.portal.com
Organization: Portal Communications Company -- 408/973-9111 (voice) 408/973-8091 (data)
Date: Mon, 16 Aug 1993 13:05:37 GMT
Lines: 86

Fellow Linuxers,

This is just to announce the imminent completion of a brand-new Linux release,
which I'm calling the Debian Linux Release. This is a release that I have put
together basically from scratch; in other words, I didn't simply make some
changes to SLS and call it a new release. I was inspired to put together this
release after running SLS and generally being dissatisfied with much of it,
and after much altering of SLS I decided that it would be easier to start
from scratch. The base system is now virtually complete (though I'm still
looking around to make sure that I grabbed the most recent sources for
everything), and I'd like to get some feedback before I add the "fancy" stuff.
```

DebianDay
Maceió 2023

Debian

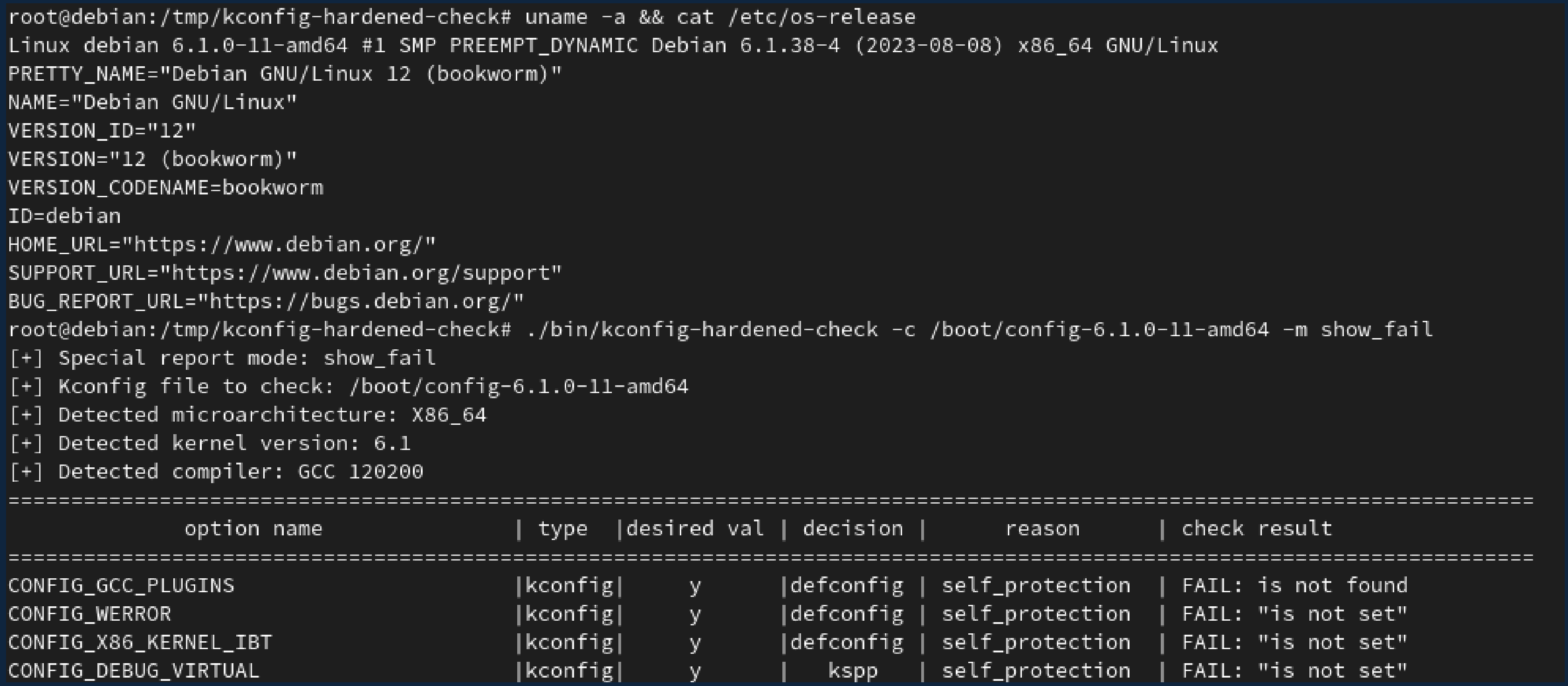
Is secure!?

Linux Hardening Guide, Checklist

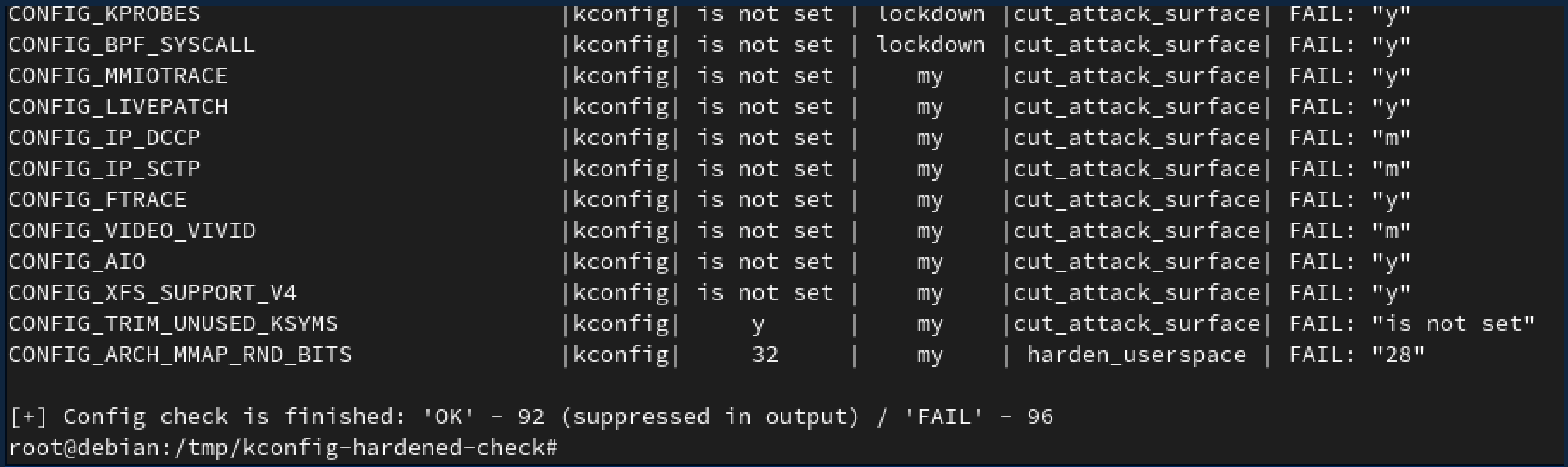
Linux Security Hardening and Other Tweaks

Kernel Self Protection Project | linux-hardened

kconfig-hardened-check



```
root@debian:/tmp/kconfig-hardened-check# uname -a && cat /etc/os-release
Linux debian 6.1.0-11-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-4 (2023-08-08) x86_64 GNU/Linux
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"
NAME="Debian GNU/Linux"
VERSION_ID="12"
VERSION="12 (bookworm)"
VERSION_CODENAME=bookworm
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
root@debian:/tmp/kconfig-hardened-check# ./bin/kconfig-hardened-check -c /boot/config-6.1.0-11-amd64 -m show_fail
[+] Special report mode: show_fail
[+] Kconfig file to check: /boot/config-6.1.0-11-amd64
[+] Detected microarchitecture: X86_64
[+] Detected kernel version: 6.1
[+] Detected compiler: GCC 120200
=========================================================================================================================
              option name               | type  |desired val | decision |      reason      | check result
=========================================================================================================================
CONFIG_GCC_PLUGINS                      |kconfig|     y      |defconfig | self_protection  | FAIL: is not found
CONFIG_WERROR                           |kconfig|     y      |defconfig | self_protection  | FAIL: "is not set"
CONFIG_X86_KERNEL_IBT                   |kconfig|     y      |defconfig | self_protection  | FAIL: "is not set"
CONFIG_DEBUG_VIRTUAL                    |kconfig|     y      |   kspp   | self_protection  | FAIL: "is not set"
```



```
CONFIG_KPROBES                          |kconfig| is not set | lockdown |cut_attack_surface| FAIL: "y"
CONFIG_BPF_SYSCALL                      |kconfig| is not set | lockdown |cut_attack_surface| FAIL: "y"
CONFIG_MMIOTRACE                        |kconfig| is not set |    my    |cut_attack_surface| FAIL: "y"
CONFIG_LIVEPATCH                        |kconfig| is not set |    my    |cut_attack_surface| FAIL: "y"
CONFIG_IP_DCCP                          |kconfig| is not set |    my    |cut_attack_surface| FAIL: "m"
CONFIG_IP_SCTP                          |kconfig| is not set |    my    |cut_attack_surface| FAIL: "m"
CONFIG_FTRACE                           |kconfig| is not set |    my    |cut_attack_surface| FAIL: "y"
CONFIG_VIDEO_VIVID                      |kconfig| is not set |    my    |cut_attack_surface| FAIL: "m"
CONFIG_AIO                              |kconfig| is not set |    my    |cut_attack_surface| FAIL: "y"
CONFIG_XFS_SUPPORT_V4                   |kconfig| is not set |    my    |cut_attack_surface| FAIL: "y"
CONFIG_TRIM_UNUSED_KSYMS                |kconfig|     y      |    my    |cut_attack_surface| FAIL: "is not set"
CONFIG_ARCH_MMAP_RND_BITS               |kconfig|     32     |    my    | harden_userspace | FAIL: "28"

[+] Config check is finished: 'OK' - 92 (suppressed in output) / 'FAIL' - 96
root@debian:/tmp/kconfig-hardened-check#
```

Debian

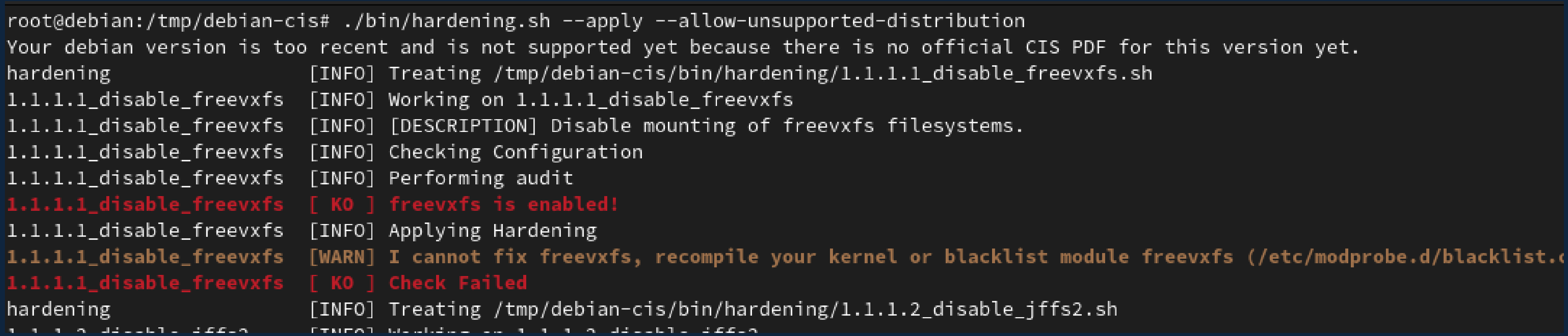
Resources

Hardening (packages) | Security Management | Securing Debian Manual | Security Information (DSA), (OVAL) | Security Bug Tracker

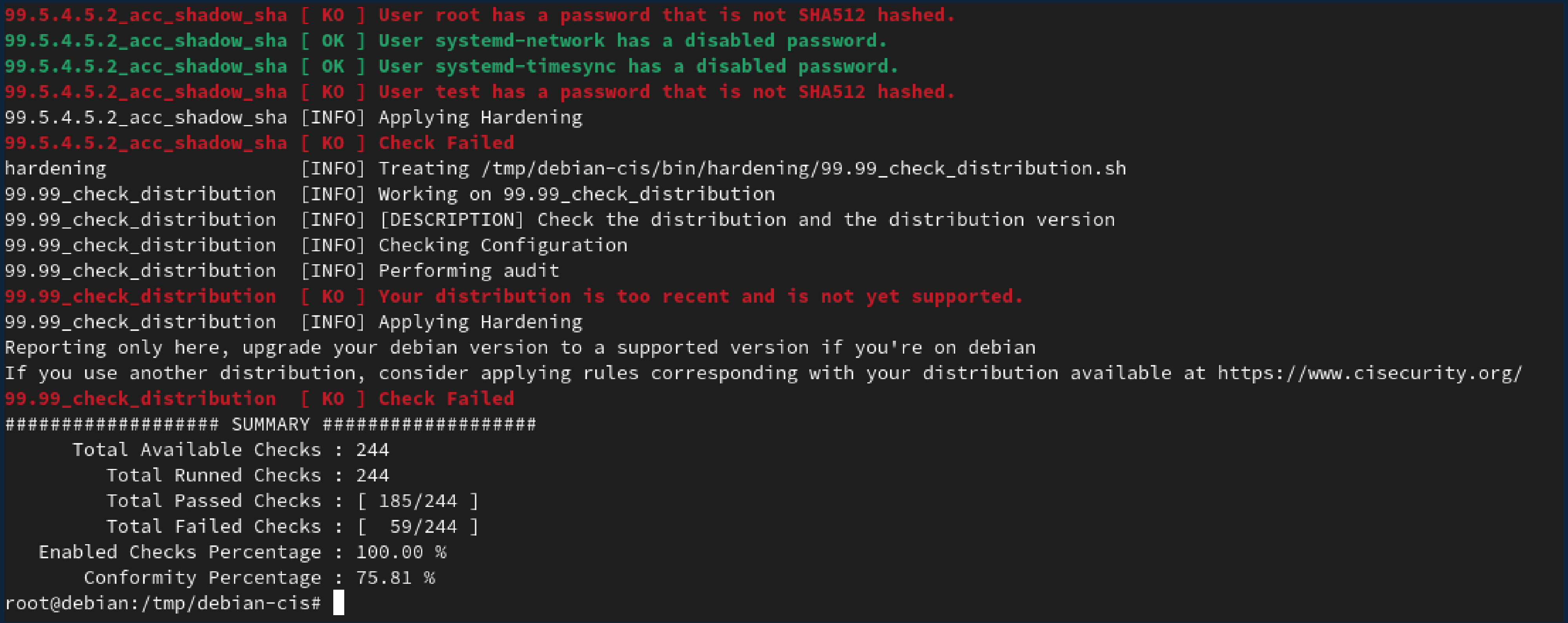
debian-cis | harbian-audit | Debian Kicksecure

CIS Benchmarks Debian Linux

DebianDay
Maceió 2023



```
root@debian:/tmp/debian-cis# ./bin/hardening.sh --apply --allow-unsupported-distribution
Your debian version is too recent and is not supported yet because there is no official CIS PDF for this version yet.
hardening                  [INFO] Treating /tmp/debian-cis/bin/hardening/1.1.1.1_disable_freevxfs.sh
1.1.1.1_disable_freevxfs  [INFO] Working on 1.1.1.1_disable_freevxfs
1.1.1.1_disable_freevxfs  [INFO] [DESCRIPTION] Disable mounting of freevxfs filesystems.
1.1.1.1_disable_freevxfs  [INFO] Checking Configuration
1.1.1.1_disable_freevxfs  [INFO] Performing audit
1.1.1.1_disable_freevxfs  [ KO ] freevxfs is enabled!
1.1.1.1_disable_freevxfs  [INFO] Applying Hardening
1.1.1.1_disable_freevxfs  [WARN] I cannot fix freevxfs, recompile your kernel or blacklist module freevxfs (/etc/modprobe.d/blacklist.c
1.1.1.1_disable_freevxfs  [ KO ] Check Failed
hardening                  [INFO] Treating /tmp/debian-cis/bin/hardening/1.1.1.2_disable_jffs2.sh
1.1.1.2_disable_jffs2     [INFO] Working on 1.1.1.2_disable_jffs2
```



```
99.5.4.5.2_acc_shadow_sha [ KO ] User root has a password that is not SHA512 hashed.
99.5.4.5.2_acc_shadow_sha [ OK ] User systemd-network has a disabled password.
99.5.4.5.2_acc_shadow_sha [ OK ] User systemd-timesync has a disabled password.
99.5.4.5.2_acc_shadow_sha [ KO ] User test has a password that is not SHA512 hashed.
99.5.4.5.2_acc_shadow_sha [INFO] Applying Hardening
99.5.4.5.2_acc_shadow_sha [ KO ] Check Failed
hardening                 [INFO] Treating /tmp/debian-cis/bin/hardening/99.99_check_distribution.sh
99.99_check_distribution  [INFO] Working on 99.99_check_distribution
99.99_check_distribution  [INFO] [DESCRIPTION] Check the distribution and the distribution version
99.99_check_distribution  [INFO] Checking Configuration
99.99_check_distribution  [INFO] Performing audit
99.99_check_distribution  [ KO ] Your distribution is too recent and is not yet supported.
99.99_check_distribution  [INFO] Applying Hardening
Reporting only here, upgrade your debian version to a supported version if you're on debian
If you use another distribution, consider applying rules corresponding with your distribution available at https://www.cisecurity.org/
99.99_check_distribution  [ KO ] Check Failed
################### SUMMARY ###################
      Total Available Checks : 244
         Total Runned Checks : 244
         Total Passed Checks : [ 185/244 ]
         Total Failed Checks : [  59/244 ]
   Enabled Checks Percentage : 100.00 %
       Conformity Percentage : 75.81 %
root@debian:/tmp/debian-cis#
```

CIS Benchmarks

CIS

- CIS Critical Securty Controls
- CIS Hardened Images
- CIS RAM
- CIS CAT
- OVAL
- CIS Workbench
- CIS Advisories
- …

DebianDay
Maceió 2023

CIS Benchmarks

Structure

Title

Assessment status (Automated, Manual)

Profile (Level 1, Level 2, Workstation, Server)

Description

Rationale

Impact

Audit

Recommendation

Default values

References

CIS Controls mapping

MITRE ATT&CK mapping

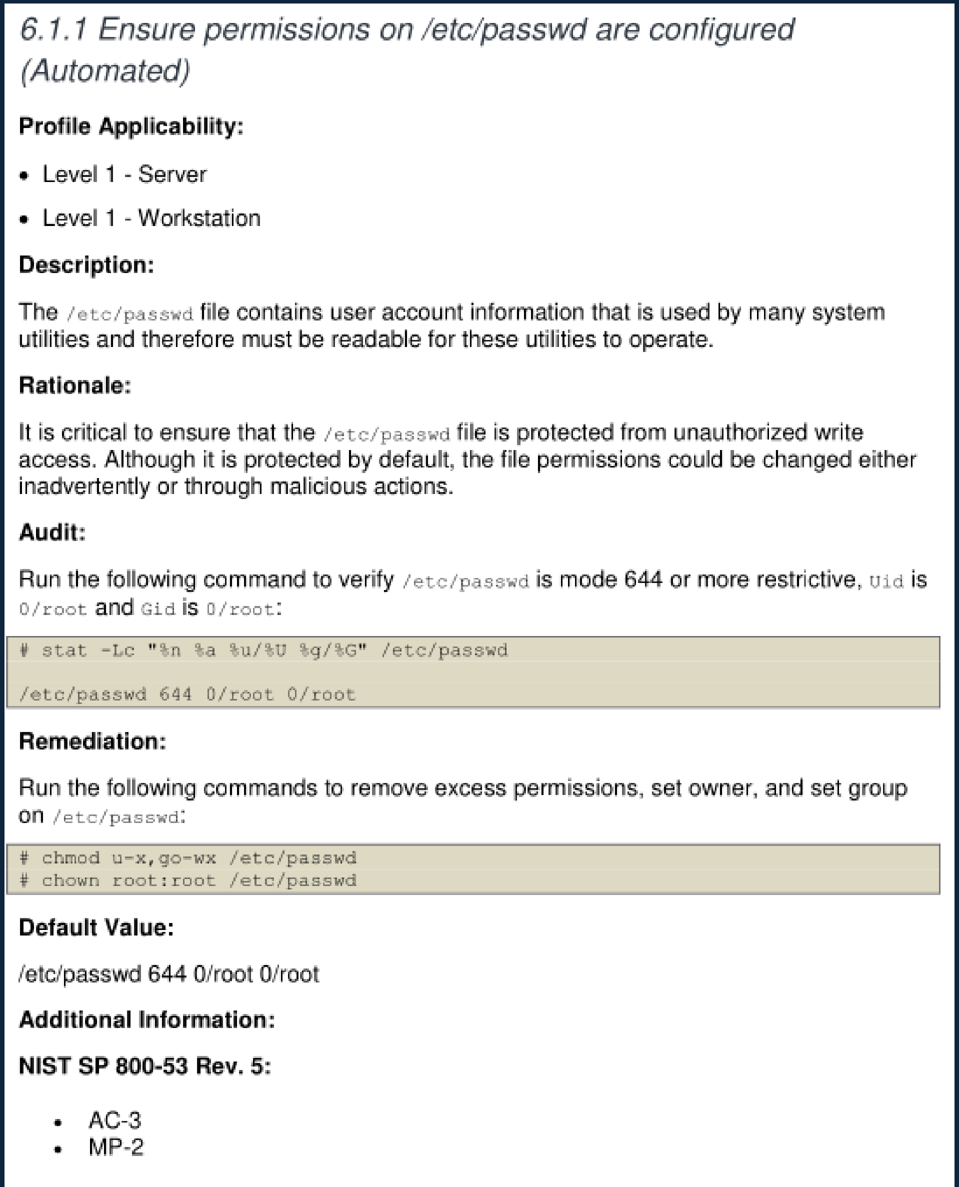
Additional information

CIS Benchmarks

Sections

1. Initial Setup
2. Services
3. Network Configuration
4. Logging and Auditing
5. Access, Authentication and Authorization
6. System Maintenance

DebianDay
Maceió 2023



6.1.1 Ensure permissions on /etc/passwd are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/passwd` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc "%n %a %u/%U %g/%G" /etc/passwd

/etc/passwd 644 0/root 0/root
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd`:

```
# chmod u-x,go-wx /etc/passwd
# chown root:root /etc/passwd
```

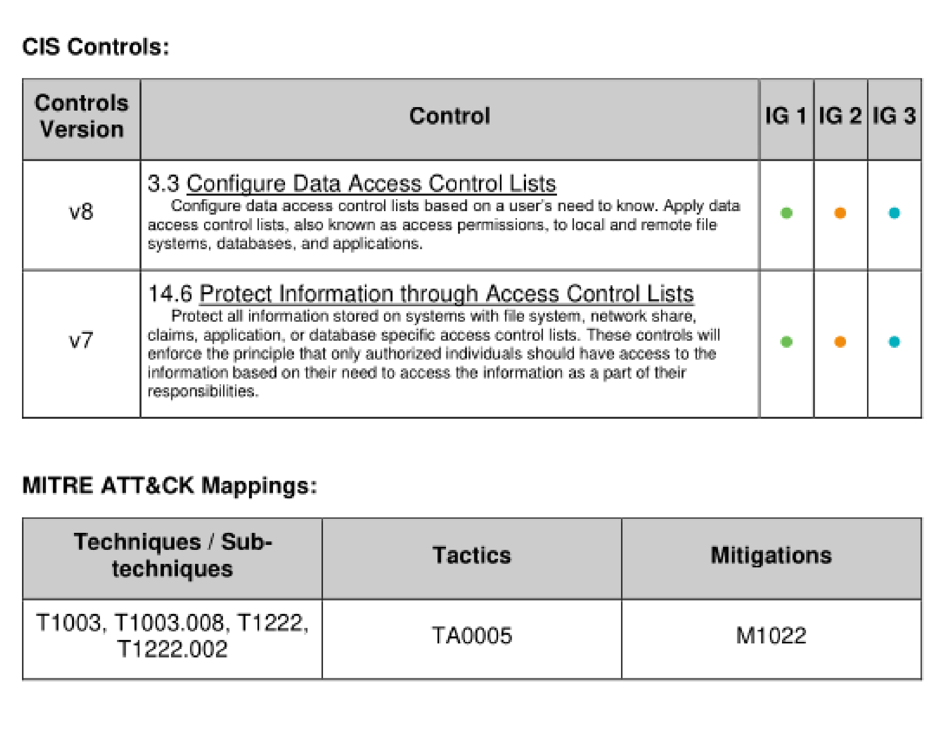
Default Value:

/etc/passwd 644 0/root 0/root

Additional Information:

NIST SP 800-53 Rev. 5:

- AC-3
- MP-2



CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

CIS Benchmarks

Misc

+800 pages;

+250 secure configuration recommendations

Debian 11 ("bullseye") v1.0.0 published (2022/09)

Debian 12 ("bookworm") v1.0.0 draft

CIS Benchmarks for Debian 7 –> Debian 10

DebianDay
Maceió 2023

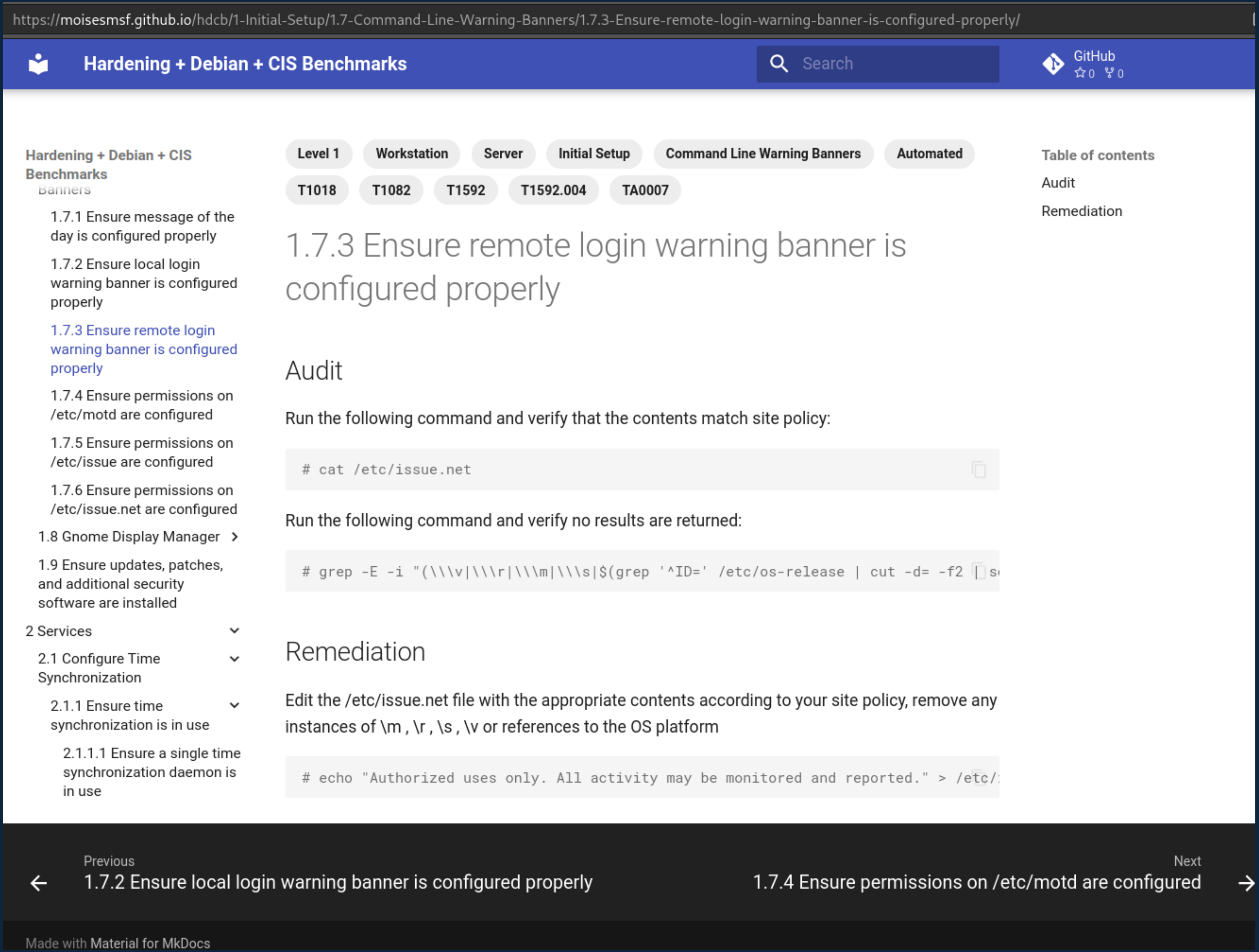
CIS Benchmarks

Hardening + Debian
+ CIS Benchmarks (HDCB)

github.com/moisesmsf/hdcb

moisesmsf.github.io/hdcb

DebianDay
Maceió 2023



https://moisesmsf.github.io/hdcb/1-Initial-Setup/1.7-Command-Line-Warning-Banners/1.7.3-Ensure-remote-login-warning-banner-is-configured-properly/

Hardening + Debian + CIS Benchmarks

Hardening + Debian + CIS Benchmarks
Banners
1.7.1 Ensure message of the day is configured properly
1.7.2 Ensure local login warning banner is configured properly
1.7.3 Ensure remote login warning banner is configured properly
1.7.4 Ensure permissions on /etc/motd are configured
1.7.5 Ensure permissions on /etc/issue are configured
1.7.6 Ensure permissions on /etc/issue.net are configured
1.8 Gnome Display Manager ›
1.9 Ensure updates, patches, and additional security software are installed
2 Services ⌄
2.1 Configure Time Synchronization ⌄
2.1.1 Ensure time synchronization is in use ⌄
2.1.1.1 Ensure a single time synchronization daemon is in use

Level 1 · Workstation · Server · Initial Setup · Command Line Warning Banners · Automated

T1018 · T1082 · T1592 · T1592.004 · TA0007

1.7.3 Ensure remote login warning banner is configured properly

Table of contents
Audit
Remediation

Audit

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue.net
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | s
```

Remediation

Edit the /etc/issue.net file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform

```
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/
```

Previous
← 1.7.2 Ensure local login warning banner is configured properly

Next
1.7.4 Ensure permissions on /etc/motd are configured →

Made with Material for MkDocs

DebianDay
Maceió 2023

Thank you!

Moisés Santos Farias

moisesmsf@proton.me

github.com/moisesmsf

DebianDay
Maceió 2023