**Malcolm Network Sensor (“Hedgehog Linux”) Hardening Compliance**

[Seth Grover](mailto:seth.grover@inl.gov?subject=Hedgehog Linux STIG), 10/28/2019

**Table of Contents**

[STIG compliance exceptions 1](#__RefHeading___Toc1220_620619175)

[CIS benchmark compliance exceptions 7](#__RefHeading___Toc1222_620619175)

[APPENDIX A – STIG-4-Debian Audit Script Output 10](#__RefHeading___Toc1226_620619175)

[APPENDIX B – Hardened Debian Audit Script Output 23](#__RefHeading___Toc1228_620619175)

The Malcolm network sensor (“Hedgehog Linux”) targets the following guidelines for establishing a secure configuration posture:

* DISA STIG (Security Technical Implementation Guides) [ported](https://github.com/hardenedlinux/STIG-4-Debian) from [DISA RHEL 7 STIG](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/) v1r1 to a Debian 9 base platform
* [CIS Debian Linux 9 Benchmark](https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/) with additional recommendations by the [hardenedlinux/harbian-audit](https://github.com/hardenedlinux/harbian-audit) project

## STIG compliance exceptions

[Currently](https://github.com/hardenedlinux/STIG-4-Debian/blob/master/stig-debian.txt) there are 158 compliance checks that can be verified automatically and 23 compliance checks that must be verified manually.

Hedgehog Linux claims the following exceptions to STIG compliance:

| # | ID | Title | Justification |
| --- | --- | --- | --- |
| 1 | [SV-86535r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71911) | When passwords are changed a minimum of eight of the total number of characters must be changed. | Account/password policy exception: As a sensor running Hedgehog Linux is intended to be used as an appliance rather than a general user-facing software platform, some exceptions to password enforcement policies are claimed. |
| 2 | [SV-86537r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71913) | When passwords are changed a minimum of four character classes must be changed. | Account/password policy exception |
| 3 | [SV-86549r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71925) | Passwords for new users must be restricted to a 24 hours/1 day minimum lifetime. | Account/password policy exception |
| 4 | [SV-86551r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71927) | Passwords must be restricted to a 24 hours/1 day minimum lifetime. | Account/password policy exception |
| 5 | [SV-86553r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71929) | Passwords for new users must be restricted to a 60-day maximum lifetime. | Account/password policy exception |
| 6 | [SV-86555r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71931) | Existing passwords must be restricted to a 60-day maximum lifetime. | Account/password policy exception |
| 7 | [SV-86557r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71933) | Passwords must be prohibited from reuse for a minimum of five generations. | Account/password policy exception |
| 8 | [SV-86565r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71941) | The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires. | Account/password policy exception |
| 9 | [SV-86567r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71943) | Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period. | Account/password policy exception |
| 10 | [SV-86569r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71945) | If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked. | Account/password policy exception |
| 11 | [SV-86603r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2018-11-28/finding/V-71979) | The … operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages 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. | As the base distribution is not using embedded signatures, debsig-verify would reject all packages (see comment in /etc/dpkg/dpkg.cfg). Enabling it after installation would disallow any future updates. |
| 12 | [SV-86607r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71983) | USB mass storage must be disabled. | The ability to copy data captured by the sensor to a mounted USB mass storage device is a requirement of the system. |
| 13 | [SV-86609r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71985) | File system automounter must be disabled unless required. | The ability to copy data captured by the sensor to a mounted USB mass storage device is a requirement of the system. |
| 14 | [SV-86705r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72081) | The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure. | As maximizing availability is a system requirement, audit processing failures will be logged on the device rather than halting the system. |
| 15 | [SV-86713r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72089) | The operating system must immediately notify the System Administrator (SA) and Information System Security Officer ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity. | As a sensor running Hedgehog Linux is intended to be used as an appliance rather than a general network host, notifications of this sort are sent in system logs forwarded to the Elasticsearch database on the aggregator. auditd is set up to syslog when this storage volume is reached. |
| 16 | [SV-86715r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72093) | The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached. | As a sensor running Hedgehog Linux is intended to be used as an appliance rather than a general network host, notifications of this sort are sent in system logs forwarded to the Elasticsearch database on the aggregator. auditd is set up to syslog when this storage volume is reached. |
| 17 | [SV-86837r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_6/2016-12-16/finding/V-38666) | The system must use and update a DoD-approved virus scan program. | As this is a network traffic capture appliance rather than an end-user device and will not be internet-connected, regular user files will not be created. A virus scan program would impact device performance and would be unnecessary. |
| 18 | [SV-86839r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72215) | The system must update the virus scan program every seven days or more frequently. | As this is a network traffic capture appliance rather than an end-user device and will not be internet-connected, regular user files will not be created. A virus scan program would impact device performance and would be unnecessary. |
| 19 | [SV-86847r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72223) | 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. | The sensor may be controlled from the command line in a manual capture scenario, so timing out a session based on command prompt inactivity would be inadvisable. |
| 20 | [SV-86893r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72269) | The operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS). | While [time synchronization](https://gogs.aal.lan/sensor/hedgehog/src/master/docs/HedgehogLinux.md" \l "ConfigTime) is supported on Hedgehog Linux, an exception is claimed for this rule as the network sensor device may be configured to sync to servers other than the ones listed in the STIG. |
| 21 | [SV-86905r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72281) | For systems using DNS resolution, at least two name servers must be configured. | STIG recommendations for DNS servers are not enforced on Hedgehog Linux to allow for use in a variety of network scenarios. |
| 22 | [SV-86919r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72295) | Network interfaces must not be in promiscuous mode. | The purpose of Hedgehog Linux is to sniff and capture network traffic. |
| 23 | [SV-86931r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72307) | An X Windows display manager must not be installed unless approved. | A locked-down X Windows session is required for the sensor's kiosk display. |
| 24 | [SV-86519r3](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71895) | The operating system must set the idle delay setting for all connection types. | As this is a network traffic capture appliance rather than an end-user device, timing out displays or connections would not be desirable. |
| 25 | [SV-86523r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71899) | The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces. | This option is configurable during install time. Some installations of Hedgehog Linux may be on appliance hardware not equipped with a keyboard by default, in which case it may not be desirable to lock the session. |
| 26 | [SV-86525r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71901) | The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated. | This option is configurable during install time. Some installations of Hedgehog Linux may be on appliance hardware not equipped with a keyboard by default, in which case it may not be desirable to lock the session. |
| 27 | [SV-86589r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71965) | The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication. | As this is a network traffic capture appliance rather than an end-user device and ot a multiuser network host, this requirement is not applicable. |
| 28 | [SV-86851r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72227) | The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications. | Does not apply as Hedgehog Linux does not use LDAP for authentication. |
| 29 | [SV-86921r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72297) | The system must be configured to prevent unrestricted mail relaying. | Does not apply as Hedgehog Linux does run a mail server service. |
| 30 | [SV-86929r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72305) | If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode. | Does not apply as Hedgehog Linux does run a TFTP server. |
| 31 | [SV-86935r3](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72311) | The Network File System (NFS) must be configured to use RPCSEC\_GSS. | Does not apply as Hedgehog Linux does run an NFS server. |
| 32 | [SV-87041r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72417) | The operating system must have the required packages for multifactor authentication installed. | As this is a network traffic capture appliance rather than an end-user device and ot a multiuser network host, this requirement is not applicable. |
| 33 | [SV-87051r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72427) | The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM). | As this is a network traffic capture appliance rather than an end-user device and ot a multiuser network host, this requirement is not applicable. |
| 34 | [SV-87059r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72435) | The operating system must implement smart card logons for multifactor authentication for access to privileged accounts. | As this is a network traffic capture appliance rather than an end-user device and ot a multiuser network host, this requirement is not applicable. |
| 35 | [SV-87829r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-73177) | Wireless network adapters must be disabled. | As an appliance intended to capture network traffic in a variety of network environments, wireless adapters may be needed to capture and/or report wireless traffic. |
| 36 | [SV-86699r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72075) | The system must not allow removable media to be used as the boot loader unless approved. | Hedgehog Linux supports a live boot mode that can be booted from removable media. |

Please review the notes for these additional rules. While not claiming an exception, they may be implemented or checked in a different way than outlined by the RHEL STIG as Hedgehog Linux is not built on RHEL or for other reasons.

| # | ID | Title | Note |
| --- | --- | --- | --- |
| 1 | [SV-86585r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71961) | Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes. | Although the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian) does not detect it, booting into recovery mode does in fact require the root password. |
| 2 | [SV-86587r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71963) | Systems using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes. | Although the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian) does not detect it, booting into recovery mode does in fact require the root password. |
| 3 | [SV-86651r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72027) | All files and directories contained in local interactive user home directories must have mode 0750 or less permissive. | Depending on when the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian) is run, some nonessential ephemeral files may exist in the sensor home directory which will cause this check to fail. For practical purposes Hedgehog Linux's configuration does, however, comply. This file list can be checked manually by running find /home/sensor -type f -perm /027 -exec ls -l '{}' ';'. |
| 4 | [SV-86693r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72069) | The file integrity tool must be configured to verify Access Control Lists (ACLs). | [Auditbeat](https://www.elastic.co/products/beats/auditbeat) is managing file integrity checks instead of the aide specified for use in the RHEL STIG. Additionally, as this is not a multi-user system, the ACL check would be irrelevant. |
| 5 | [SV-86597r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-71973) | A file integrity tool must verify the baseline operating system configuration at least weekly. | [Auditbeat](https://www.elastic.co/products/beats/auditbeat) is managing file integrity checks instead of the aide specified for use in the RHEL STIG. |
| 6 | [SV-86697r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72073) | The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents and directories. | [Auditbeat](https://www.elastic.co/products/beats/auditbeat) is managing file integrity checks instead of the aide specified for use in the RHEL STIG. Auditbeat uses SHA1 which is FIPS 140-2 approved. |
| 7 | [SV-86623r3](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-71999) | Vendor packaged system security patches and updates must be installed and up to date. | When the Hedgehog Linux sensor appliance software is built, all of the latest applicable security patches and updates are included in it. How future updates are to be handled is still in design. |
| 8 | [SV-86707r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72083) | The operating system must off-load audit records onto a different system or media from the system being audited. | [Auditbeat](https://www.elastic.co/products/beats/auditbeat) offloads audit records to an Elasticsearch database on another system, though this is not detected by the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian). |
| 9 | [SV-86709r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-72085) | The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited. | [Auditbeat](https://www.elastic.co/products/beats/auditbeat) offloads (via an encrypted channel) audit records to an Elasticsearch database on another system, though this is not detected by the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian). |
| 10 | [SV-86833r1](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72209) | The system must send rsyslog output to a log aggregation server. | Syslogs are forwarded to an Elasticsearch database running on another system via [filebeat](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-input-syslog.html), though this is not detected by the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian). |
| 11 | [SV-87815r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-12-14/finding/V-73163) | The audit system must take appropriate action when there is an error sending audit records to a remote system. | [Auditbeat](https://www.elastic.co/products/beats/auditbeat) offloads audit records to an Elasticsearch database on another system, though this is not detected by the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian). Local logs are generated when this network connection is broken, and it resumes automatically. |
| 12 | [SV-86691r2](https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/2017-07-08/finding/V-72067) | The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | Hedgehog Linux does use FIPS-compatible libraries for cryptographic functions. However, the kernel parameter being checked by the [compliance check script](https://github.com/hardenedlinux/STIG-4-Debian) is incompatible with some of the systems initialization scripts. |

In addition, DISA STIG rules SV-86663r1, SV-86695r2, SV-86759r3, SV-86761r3, SV-86763r3, SV-86765r3, SV-86595r1, and SV-86615r2 relate to the SELinux kernel which is not used in Hedgehog Linux, and are thus skipped.

## CIS benchmark compliance exceptions

[Currently](https://github.com/hardenedlinux/harbian-audit/tree/master/bin/hardening) there are 271 checks to determine compliance with the CIS Debian Linux 9 Benchmark.

Hedgehog Linux claims exceptions from the recommendations in this benchmark in the following categories:

1.1 Install Updates, Patches and Additional Security Software - When the Hedgehog Linux sensor appliance software is built, all of the latest applicable security patches and updates are included in it. How future updates are to be handled is still in design.

1.3 Enable verify the signature of local packages - As the base distribution is not using embedded signatures, debsig-verify would reject all packages (see comment in /etc/dpkg/dpkg.cfg). Enabling it after installation would disallow any future updates.

2.14 Add nodev option to /run/shm Partition, 2.15 Add nosuid Option to /run/shm Partition, 2.16 Add noexec Option to /run/shm Partition - Hedgehog Linux does not mount /run/shm as a separate partition, so these recommendations do not apply.

2.18 Disable Mounting of cramfs Filesystems, 2.19 Disable Mounting of freevxfs Filesystems, 2.20 Disable Mounting of jffs2 Filesystems, 2.21 Disable Mounting of hfs Filesystems, 2.22 Disable Mounting of hfsplus Filesystems, 2.23 Disable Mounting of squashfs Filesystems, 2.24 Disable Mounting of udf Filesystems - Hedgehog Linux is not compiling a custom Linux kernel, so these filesystems are inherently supported as they are part Debian Linux's default kernel.

4.6 Disable USB Devices - The ability to copy data captured by the sensor to a mounted USB mass storage device is a requirement of the system.

6.1 Ensure the X Window system is not installed, 6.2 Ensure Avahi Server is not enabled, 6.3 Ensure print server is not enabled - A locked-down X Windows session is required for the sensor's kiosk display. The library packages libavahi-common-data, libavahi-common3, and libcups2 are dependencies of some of the X components used by Hedgehog Linux, but the avahi and cups services themselves are disabled.

6.17 Ensure virus scan Server is enabled, 6.18 Ensure virus scan Server update is enabled - As this is a network traffic capture appliance rather than an end-user device and will not be internet-connected, regular user files will not be created. A virus scan program would impact device performance and would be unnecessary.

7.2.4 Log Suspicious Packets, 7.2.7 Enable RFC-recommended Source Route Validation, 7.4.1 Install TCP Wrappers - As this is a network traffic capture appliance sniffing packets on a network interface configured in promiscuous mode, these recommendations do not apply.

Password-related recommendations under 9.2 and 10.1 - The library package libpam-pwquality is used in favor of libpam-cracklib which is what the [compliance scripts](https://github.com/hardenedlinux/harbian-audit/tree/master/bin/hardening) are looking for. Also, as a sensor running Hedgehog Linux is intended to be used as an appliance rather than a general user-facing software platform, some exceptions to password enforcement policies are claimed.

9.3.13 Limit Access via SSH - Hedgehog Linux does not create multiple regular user accounts: only root and a sensor service account are used. SSH access for root is disabled. SSH login with a password is also disallowed: only key-based authentication is accepted. The sensor service account accepts no keys by default. As such, the AllowUsers, AllowGroups, DenyUsers, and DenyGroups values in sshd\_config do not apply.

9.5 Restrict Access to the su Command - Hedgehog Linux does not create multiple regular user accounts: only root and a sensor service account are used.

10.1.10 Set maxlogins for all accounts and 10.5 Set Timeout on ttys - Hedgehog Linux does not create multiple regular user accounts: only root and a sensor service account are used.

12.10 Find SUID System Executables, 12.11 Find SGID System Executables - The few files found by [these](https://github.com/hardenedlinux/harbian-audit/blob/master/bin/hardening/12.10_find_suid_files.sh) [scripts](https://github.com/hardenedlinux/harbian-audit/blob/master/bin/hardening/12.11_find_sgid_files.sh) are valid exceptions required by Hedgehog Linux's system requirements.

Please review the notes for these additional guidelines. While not claiming an exception, Hedgehog Linux may implement them in a manner different than is described by the [CIS Debian Linux 9 Benchmark](https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/) or the [hardenedlinux/harbian-audit](https://github.com/hardenedlinux/harbian-audit) audit scripts.

4.1 Restrict Core Dumps - Hedgehog Linux disables core dumps using a configuration file for ulimit named /etc/security/limits.d/limits.conf. The [audit script](https://github.com/hardenedlinux/harbian-audit/blob/master/bin/hardening/4.1_restrict_core_dumps.sh) checking for this does not check the limits.d subdirectory, which is why this is incorrectly flagged as noncompliant.

5.4 Ensure ctrl-alt-del is disabled - Hedgehog Linux disables the ctrl+alt+delete key sequence by executing systemctl disable ctrl-alt-del.target during installation and the command systemctl mask ctrl-alt-del.target at boot time.

6.19 Configure Network Time Protocol (NTP) - While [time synchronization](https://gogs.aal.lan/sensor/hedgehog/src/master/docs/HedgehogLinux.md" \l "ConfigTime) is supported on Hedgehog Linux, an exception is claimed for this rule as the network sensor device may be configured to sync to servers in a different way than specified in the benchmark.

7.4.4 Create /etc/hosts.deny, 7.7.1 Ensure Firewall is active, 7.7.4.1 Ensure default deny firewall policy, 7.7.4.3 Ensure default deny firewall policy, 7.7.4.4 Ensure outbound and established connections are configured - Hedgehog Linux is configured with an appropriately locked-down software firewall (managed by "Uncomplicated Firewall" ufw). However, the methods outlined in the CIS benchmark recommendations do not account for this configuration.

8.1.1.2 Disable System on Audit Log Full, 8.1.1.3 Keep All Auditing Information, 8.1.1.5 Ensure set remote\_server for audit service, 8.1.1.6 Ensure enable\_krb5 set to yes for remote audit service, 8.1.1.7 Ensure set action for audit storage volume is fulled, 8.1.1.9 Set space left for auditd service, a few other audit-related items under section 8.1, 8.2.5 Configure rsyslog to Send Logs to a Remote Log Host - As maximizing availability is a system requirement, audit processing failures will be logged on the device rather than halting the system. Because Hedgehog Linux is intended to be used as an appliance rather than a general network host, notifications about its status are sent in system logs forwarded to the Elasticsearch database on the aggregator. auditd is set up to syslog when this storage volume is reached. [Auditbeat](https://www.elastic.co/products/beats/auditbeat) offloads audit records to an Elasticsearch database on another system, though this is not detected by the [CIS benchmark compliance scripts](https://github.com/hardenedlinux/harbian-audit/tree/master/bin/hardening). Local logs are generated when the network connection is broken, and it resumes automatically. Syslog messages are also similarly forwarded.

8.4.1 Install aide package and 8.4.2 Implement Periodic Execution of File Integrity - [Auditbeat](https://www.elastic.co/products/beats/auditbeat) is managing file integrity checks instead of the aide utility.

8.7 Verifies integrity all packages - The [script](https://github.com/hardenedlinux/harbian-audit/blob/master/bin/hardening/8.7_verify_integrity_packages.sh) which verifies package integrity only "fails" because of missing (status ??5?????? displayed by the utility) language ("locale") files, which are removed as part of Hedgehog Linux's trimming-down process. All non-locale-related system files pass integrity checks.

## APPENDIX A – [STIG-4-Debian](https://github.com/hardenedlinux/STIG-4-Debian) Audit Script Output

Pass Count: 155  
Failed Count: 35

Rule Title: The cryptographic hash of system files and commands must match vendor values.

Rule ID: SV-86479r2\_rule

Status: FAILED

Rule Title: The operating system must have the screen package installed.

Rule ID: SV-86521r1\_rule

Status: PASS

Rule Title: When passwords are changed or new passwords are established, the new password must contain at least one upper-case character.

Rule ID: SV-86527r2\_rule

Status: PASS

Rule Title: When passwords are changed or new passwords are established, the new password must contain at least one lower-case character.

Rule ID: SV-86529r2\_rule

Status: PASS

Rule Title: When passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.

Rule ID: SV-86531r2\_rule

Status: PASS

Rule Title: When passwords are changed or new passwords are assigned, the new password must contain at least one special character.

Rule ID: SV-86533r1\_rule

Status: PASS

Rule Title: When passwords are changed a minimum of eight of the total number of characters must be changed.

Rule ID: SV-86535r1\_rule

Status: FAILED

Rule Title: When passwords are changed a minimum of four character classes must be changed.

Rule ID: SV-86537r1\_rule

Status: FAILED

Rule Title: When passwords are changed the number of repeating consecutive characters must not be more than four characters.

Rule ID: SV-86539r1\_rule

Status: PASS

Rule Title: When passwords are changed the number of repeating characters of the same character class must not be more than four characters.

Rule ID: SV-86541r1\_rule

Status: PASS

Rule Title: The PAM system service must be configured to store only encrypted representations of passwords.

Rule ID: SV-86543r1\_rule

Status: PASS

Rule Title: The shadow file must be configured to store only encrypted representations of passwords.

Rule ID: SV-86545r1\_rule

Status: PASS

Rule Title: Passwords for new users must be restricted to a 24 hours/1 day minimum lifetime.

Rule ID: SV-86549r1\_rule

Status: FAILED

Rule Title: Passwords must be restricted to a 24 hours/1 day minimum lifetime.

Rule ID: SV-86551r1\_rule

Status: FAILED

Rule Title: Passwords for new users must be restricted to a 60-day maximum lifetime.

Rule ID: SV-86553r1\_rule

Status: PASS

Rule Title: Existing passwords must be restricted to a 60-day maximum lifetime.

Rule ID: SV-86555r1\_rule

Status: FAILED

Rule Title: Passwords must be prohibited from reuse for a minimum of five generations.

Rule ID: SV-86557r1\_rule

Status: FAILED

Rule Title: Passwords must be a minimum of 15 characters in length.

Rule ID: SV-86559r1\_rule

Status: PASS

Rule Title: The system must not have accounts configured with blank or null passwords.

Rule ID: SV-86561r1\_rule

Status: PASS

Rule Title: The SSH daemon must not allow authentication using an empty password.

Rule ID: SV-86563r2\_rule

Status: PASS

Rule Title: The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.

Rule ID: SV-86565r1\_rule

Status: FAILED

Rule Title: Accounts subject to three unsuccessful logon attempts within 15 minutes must be locked for the maximum configurable period.

Rule ID: SV-86567r2\_rule

Status: FAILED

Rule Title: If three unsuccessful root logon attempts within 15 minutes occur the associated account must be locked.

Rule ID: SV-86569r1\_rule

Status: FAILED

Rule Title: Users must provide a password for privilege escalation.

Rule ID: SV-86571r1\_rule

Status: FAILED

Rule Title: Users must re-authenticate for privilege escalation.

Rule ID: SV-86573r2\_rule

Status: PASS

Rule Title: The delay between logon prompts following a failed console logon attempt must be at least four seconds.

Rule ID: SV-86575r1\_rule

Status: PASS

Rule Title: The operating system must not allow users to override SSH environment variables.

Rule ID: SV-86581r2\_rule

Status: PASS

Rule Title: The operating system must not allow a non-certificate trusted host SSH logon to the system.

Rule ID: SV-86583r2\_rule

Status: PASS

Rule Title: Systems with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

Rule ID: SV-86585r1\_rule

Status: FAILED

Rule Title: Systems using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

Rule ID: SV-86587r1\_rule

Status: PASS

Rule Title: The rsh-server package must not be installed.

Rule ID: SV-86591r1\_rule

Status: PASS

Rule Title: The ypserv package must not be installed.

Rule ID: SV-86593r1\_rule

Status: PASS

Rule Title: A file integrity tool must verify the baseline operating system configuration at least weekly.

Rule ID: SV-86597r1\_rule

Status: PASS

Rule Title: 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.

Rule ID: SV-86601r1\_rule

Status: PASS

Rule Title: The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages 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.

Rule ID: SV-86603r1\_rule

Status: FAILED

Rule Title: The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of packages without verification of the repository metadata.

Rule ID: SV-86605r1\_rule

Status: PASS

Rule Title: USB mass storage must be disabled.

Rule ID: SV-86607r1\_rule

Status: PASS

Rule Title: File system automounter must be disabled unless required.

Rule ID: SV-86609r1\_rule

Status: PASS

Rule Title: The operating system must enable AppArmor.

Rule ID: SV-86613r2\_rule

Status: PASS

Rule Title: The x86 Ctrl-Alt-Delete key sequence must be disabled.

Rule ID: SV-86617r1\_rule

Status: PASS

Rule Title: The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Rule ID: SV-86619r1\_rule

Status: PASS

Rule Title: The operating system must be a vendor supported release.

Rule ID: SV-86621r2\_rule

Status: FAILED

Rule Title: Vendor packaged system security patches and updates must be installed and up to date.

Rule ID: SV-86623r3\_rule

Status: PASS

Rule Title: All Group Identifiers (GIDs) referenced in the /etc/passwd file must be defined in the /etc/group file.

Rule ID: SV-86627r1\_rule

Status: PASS

Rule Title: The root account must be the only account having unrestricted access to the system.

Rule ID: SV-86629r1\_rule

Status: PASS

Rule Title: All files and directories must have a valid owner.

Rule ID: SV-86631r1\_rule

Status: PASS

Rule Title: All files and directories must have a valid group owner.

Rule ID: SV-86633r1\_rule

Status: PASS

Rule Title: All local interactive users must have a home directory assigned in the /etc/passwd file.

Rule ID: SV-86635r1\_rule

Status: PASS

Rule Title: All local interactive user accounts, upon creation, must be assigned a home directory.

Rule ID: SV-86637r1\_rule

Status: PASS

Rule Title: All local interactive user home directories defined in the /etc/passwd file must exist.

Rule ID: SV-86639r1\_rule

Status: FAILED

Rule Title: All local interactive user home directories must have mode 0750 or less permissive.

Rule ID: SV-86641r1\_rule

Status: PASS

Rule Title: All local interactive user home directories must be owned by their respective users.

Rule ID: SV-86643r2\_rule

Status: PASS

Rule Title: All local interactive user home directories must be group-owned by the home directory owners primary group.

Rule ID: SV-86645r2\_rule

Status: PASS

Rule Title: All files and directories contained in local interactive user home directories must be owned by the owner of the home directory.

Rule ID: SV-86647r1\_rule

Status: PASS

Rule Title: All files and directories contained in local interactive user home directories must be group-owned by a group of which the home directory owner is a member.

Rule ID: SV-86649r1\_rule

Status: PASS

Rule Title: All files and directories contained in local interactive user home directories must have mode 0750 or less permissive.

Rule ID: SV-86651r1\_rule

Status: FAILED

Rule Title: All local initialization files for interactive users must be owned by the home directory user or root.

Rule ID: SV-86653r1\_rule

Status: PASS

Rule Title: Local initialization files for local interactive users must be group-owned by the users primary group or root.

Rule ID: SV-86655r2\_rule

Status: PASS

Rule Title: All local initialization files must have mode 0740 or less permissive.

Rule ID: SV-86657r1\_rule

Status: PASS

Rule Title: All local interactive user initialization files executable search paths must contain only paths that resolve to the users home directory.

Rule ID: SV-86659r2\_rule

Status: PASS

Rule Title: Local initialization files must not execute world-writable programs.

Rule ID: SV-86661r1\_rule

Status: PASS

Rule Title: File systems that contain user home directories must be mounted to prevent files with the setuid and setgid bit set from being executed.

Rule ID: SV-86665r2\_rule

Status: PASS

Rule Title: File systems that are used with removable media must be mounted to prevent files with the setuid and setgid bit set from being executed.

Rule ID: SV-86667r1\_rule

Status: PASS

Rule Title: File systems that are being imported via Network File System (NFS) must be mounted to prevent files with the setuid and setgid bit set from being executed.

Rule ID: SV-86669r1\_rule

Status: PASS

Rule Title: All world-writable directories must be group-owned by root, sys, bin, or an application group.

Rule ID: SV-86671r1\_rule

Status: PASS

Rule Title: The umask must be set to 077 for all local interactive user accounts.

Rule ID: SV-86673r1\_rule

Status: PASS

Rule Title: Cron logging must be implemented.

Rule ID: SV-86675r1\_rule

Status: PASS

Rule Title: If the cron.allow file exists it must be owned by root.

Rule ID: SV-86677r1\_rule

Status: PASS

Rule Title: If the cron.allow file exists it must be group-owned by root.

Rule ID: SV-86679r1\_rule

Status: PASS

Rule Title: Kernel core dumps must be disabled unless needed.

Rule ID: SV-86681r1\_rule

Status: PASS

Rule Title: A separate file system must be used for user home directories (such as /home or an equivalent).

Rule ID: SV-86683r1\_rule

Status: PASS

Rule Title: The system must use a separate file system for /var.

Rule ID: SV-86685r1\_rule

Status: PASS

Rule Title: The system must use a separate file system for the system audit data path.

Rule ID: SV-86687r3\_rule

Status: PASS

Rule Title: The system must use a separate file system for /tmp (or equivalent).

Rule ID: SV-86689r1\_rule

Status: PASS

Rule Title: The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Rule ID: SV-86691r2\_rule

Status: FAILED

Rule Title: The file integrity tool must be configured to verify Access Control Lists (ACLs).

Rule ID: SV-86693r2\_rule

Status: FAILED

Rule Title: The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Rule ID: SV-86697r2\_rule

Status: FAILED

Rule Title: The system must not allow removable media to be used as the boot loader unless approved.

Rule ID: SV-86699r1\_rule

Status: FAILED

Rule Title: The telnet-server package must not be installed.

Rule ID: SV-86701r1\_rule

Status: PASS

Rule Title: 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.

Rule ID: SV-86703r1\_rule

Status: PASS

Rule Title: The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure.

Rule ID: SV-86705r1\_rule

Status: PASS

Rule Title: The operating system must off-load audit records onto a different system or media from the system being audited.

Rule ID: SV-86707r1\_rule

Status: FAILED

Rule Title: The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.

Rule ID: SV-86709r1\_rule

Status: FAILED

Rule Title: The audit system must take appropriate action when the audit storage volume is full.

Rule ID: SV-86711r2\_rule

Status: PASS

Rule Title: The operating system must immediately notify the System Administrator (SA) and Information System Security Officer ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

Rule ID: SV-86713r1\_rule

Status: FAILED

Rule Title: The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached.

Rule ID: SV-86715r1\_rule

Status: FAILED

Rule Title: The operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Rule ID: SV-86717r2\_rule

Status: PASS

Rule Title: All uses of the chown command must be audited.

Rule ID: SV-86721r2\_rule

Status: PASS

Rule Title: All uses of the fchown command must be audited.

Rule ID: SV-86723r2\_rule

Status: PASS

Rule Title: All uses of the lchown command must be audited.

Rule ID: SV-86725r2\_rule

Status: PASS

Rule Title: All uses of the fchownat command must be audited.

Rule ID: SV-86727r2\_rule

Status: PASS

Rule Title: All uses of the chmod command must be audited.

Rule ID: SV-86729r2\_rule

Status: PASS

Rule Title: All uses of the fchmod command must be audited.

Rule ID: SV-86731r2\_rule

Status: PASS

Rule Title: All uses of the fchmodat command must be audited.

Rule ID: SV-86733r2\_rule

Status: PASS

Rule Title: All uses of the setxattr command must be audited.

Rule ID: SV-86735r2\_rule

Status: PASS

Rule Title: All uses of the fsetxattr command must be audited.

Rule ID: SV-86737r2\_rule

Status: PASS

Rule Title: All uses of the lsetxattr command must be audited.

Rule ID: SV-86739r2\_rule

Status: PASS

Rule Title: All uses of the removexattr command must be audited.

Rule ID: SV-86741r2\_rule

Status: PASS

Rule Title: All uses of the fremovexattr command must be audited.

Rule ID: SV-86743r2\_rule

Status: PASS

Rule Title: All uses of the lremovexattr command must be audited.

Rule ID: SV-86745r2\_rule

Status: PASS

Rule Title: All uses of the creat command must be audited.

Rule ID: SV-86747r2\_rule

Status: PASS

Rule Title: All uses of the open command must be audited.

Rule ID: SV-86749r2\_rule

Status: PASS

Rule Title: All uses of the openat command must be audited.

Rule ID: SV-86751r2\_rule

Status: PASS

Rule Title: All uses of the open\_by\_handle\_at command must be audited.

Rule ID: SV-86753r2\_rule

Status: PASS

Rule Title: All uses of the truncate command must be audited.

Rule ID: SV-86755r2\_rule

Status: PASS

Rule Title: All uses of the ftruncate command must be audited.

Rule ID: SV-86757r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all successful/unsuccessful account access count events.

Rule ID: SV-86767r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all unsuccessful account access events.

Rule ID: SV-86769r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all successful account access events.

Rule ID: SV-86771r2\_rule

Status: PASS

Rule Title: All uses of the passwd command must be audited.

Rule ID: SV-86773r3\_rule

Status: PASS

Rule Title: All uses of the unix\_chkpwd command must be audited.

Rule ID: SV-86775r3\_rule

Status: FAILED

Rule Title: All uses of the gpasswd command must be audited.

Rule ID: SV-86777r3\_rule

Status: PASS

Rule Title: All uses of the chage command must be audited.

Rule ID: SV-86779r3\_rule

Status: PASS

Rule Title: All uses of the su command must be audited.

Rule ID: SV-86783r3\_rule

Status: FAILED

Rule Title: All uses of the sudo command must be audited.

Rule ID: SV-86785r3\_rule

Status: PASS

Rule Title: All uses of the sudoers command must be audited.

Rule ID: SV-86787r3\_rule

Status: PASS

Rule Title: All uses of the newgrp command must be audited.

Rule ID: SV-86789r3\_rule

Status: PASS

Rule Title: All uses of the chsh command must be audited.

Rule ID: SV-86791r3\_rule

Status: PASS

Rule Title: All uses of the sudoedit command must be audited.

Rule ID: SV-86793r3\_rule

Status: PASS

Rule Title: All uses of the mount command must be audited.

Rule ID: SV-86795r3\_rule

Status: FAILED

Rule Title: All uses of the umount command must be audited.

Rule ID: SV-86797r3\_rule

Status: FAILED

Rule Title: All uses of the postqueue command must be audited.

Rule ID: SV-86801r2\_rule

Status: PASS

Rule Title: All uses of the ssh-keysign command must be audited.

Rule ID: SV-86803r2\_rule

Status: PASS

Rule Title: All uses of the crontab command must be audited.

Rule ID: SV-86807r2\_rule

Status: PASS

Rule Title: All uses of the pam\_timestamp\_check command must be audited.

Rule ID: SV-86809r2\_rule

Status: PASS

Rule Title: All uses of the init\_module command must be audited.

Rule ID: SV-86811r2\_rule

Status: PASS

Rule Title: All uses of the delete\_module command must be audited.

Rule ID: SV-86813r2\_rule

Status: PASS

Rule Title: All uses of the insmod command must be audited.

Rule ID: SV-86815r2\_rule

Status: PASS

Rule Title: All uses of the rmmod command must be audited.

Rule ID: SV-86817r2\_rule

Status: PASS

Rule Title: All uses of the modprobe command must be audited.

Rule ID: SV-86819r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

Rule ID: SV-86821r3\_rule

Status: PASS

Rule Title: All uses of the rename command must be audited.

Rule ID: SV-86823r2\_rule

Status: PASS

Rule Title: All uses of the renameat command must be audited.

Rule ID: SV-86825r2\_rule

Status: PASS

Rule Title: All uses of the rmdir command must be audited.

Rule ID: SV-86827r2\_rule

Status: PASS

Rule Title: All uses of the unlink command must be audited.

Rule ID: SV-86829r2\_rule

Status: PASS

Rule Title: All uses of the unlinkat command must be audited.

Rule ID: SV-86831r2\_rule

Status: PASS

Rule Title: The system must send rsyslog output to a log aggregation server.

Rule ID: SV-86833r1\_rule

Status: PASS

Rule Title: The rsyslog daemon must not accept log messages from other servers unless the server is being used for log aggregation.

Rule ID: SV-86835r1\_rule

Status: PASS

Rule Title: The system must use a DoD-approved virus scan program.

Rule ID: SV-86837r1\_rule

Status: FAILED

Rule Title: The system must update the DoD-approved virus scan program every seven days or more frequently.

Rule ID: SV-86839r1\_rule

Status: PASS

Rule Title: The operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.

Rule ID: SV-86841r1\_rule

Status: PASS

Rule Title: A FIPS 140-2 approved cryptographic algorithm must be used for SSH communications.

Rule ID: SV-86845r2\_rule

Status: PASS

Rule Title: 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.

Rule ID: SV-86847r2\_rule

Status: FAILED

Rule Title: The Standard Mandatory DoD Notice and Consent Banner must be displayed immediately prior to, or as part of, remote access logon prompts.

Rule ID: SV-86849r2\_rule

Status: PASS

Rule Title: All networked systems must have SSH installed.

Rule ID: SV-86857r1\_rule

Status: PASS

Rule Title: All networked systems must use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.

Rule ID: SV-86859r2\_rule

Status: PASS

Rule Title: All network connections associated with SSH traffic must terminate at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements.

Rule ID: SV-86861r2\_rule

Status: FAILED

Rule Title: The SSH daemon must not allow authentication using RSA rhosts authentication.

Rule ID: SV-86863r2\_rule

Status: PASS

Rule Title: All network connections associated with SSH traffic must terminate after a period of inactivity.

Rule ID: SV-86865r2\_rule

Status: PASS

Rule Title: The SSH daemon must not allow authentication using rhosts authentication.

Rule ID: SV-86867r2\_rule

Status: PASS

Rule Title: The system must display the date and time of the last successful account logon upon an SSH logon.

Rule ID: SV-86869r2\_rule

Status: PASS

Rule Title: The system must not permit direct logons to the root account using remote access via SSH.

Rule ID: SV-86871r2\_rule

Status: PASS

Rule Title: The SSH daemon must not allow authentication using known hosts authentication.

Rule ID: SV-86873r2\_rule

Status: PASS

Rule Title: The SSH daemon must be configured to only use the SSHv2 protocol.

Rule ID: SV-86875r2\_rule

Status: PASS

Rule Title: The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

Rule ID: SV-86877r2\_rule

Status: PASS

Rule Title: The SSH public host key files must have mode 0644 or less permissive.

Rule ID: SV-86879r1\_rule

Status: PASS

Rule Title: The SSH private host key files must have mode 0600 or less permissive.

Rule ID: SV-86881r1\_rule

Status: PASS

Rule Title: The SSH daemon must not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.

Rule ID: SV-86883r2\_rule

Status: PASS

Rule Title: The SSH daemon must not permit Kerberos authentication unless needed.

Rule ID: SV-86885r2\_rule

Status: PASS

Rule Title: The SSH daemon must perform strict mode checking of home directory configuration files.

Rule ID: SV-86887r2\_rule

Status: PASS

Rule Title: The SSH daemon must use privilege separation.

Rule ID: SV-86889r2\_rule

Status: PASS

Rule Title: The SSH daemon must not allow compression or must only allow compression after successful authentication.

Rule ID: SV-86891r2\_rule

Status: PASS

Rule Title: The operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

Rule ID: SV-86893r2\_rule

Status: FAILED

Rule Title: The operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces.

Rule ID: SV-86895r1\_rule

Status: PASS

Rule Title: The operating system must enable an application firewall, if available.

Rule ID: SV-86897r1\_rule

Status: PASS

Rule Title: The system must display the date and time of the last successful account logon upon logon.

Rule ID: SV-86899r1\_rule

Status: PASS

Rule Title: There must be no .shosts files on the system.

Rule ID: SV-86901r1\_rule

Status: PASS

Rule Title: There must be no shosts.equiv files on the system.

Rule ID: SV-86903r1\_rule

Status: PASS

Rule Title: For systems using DNS resolution, at least two name servers must be configured.

Rule ID: SV-86905r1\_rule

Status: FAILED

Rule Title: The system must not forward Internet Protocol version 4 (IPv4) source-routed packets.

Rule ID: SV-86907r1\_rule

Status: PASS

Rule Title: The system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.

Rule ID: SV-86909r1\_rule

Status: PASS

Rule Title: The system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

Rule ID: SV-86911r1\_rule

Status: PASS

Rule Title: The system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.

Rule ID: SV-86913r2\_rule

Status: PASS

Rule Title: The system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default.

Rule ID: SV-86915r2\_rule

Status: PASS

Rule Title: The system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.

Rule ID: SV-86917r2\_rule

Status: PASS

Rule Title: Network interfaces must not be in promiscuous mode.

Rule ID: SV-86919r1\_rule

Status: PASS

Rule Title: A File Transfer Protocol (FTP) server package must not be installed unless needed.

Rule ID: SV-86923r1\_rule

Status: PASS

Rule Title: The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support.

Rule ID: SV-86925r1\_rule

Status: PASS

Rule Title: Remote X connections for interactive users must be encrypted.

Rule ID: SV-86927r2\_rule

Status: FAILED

Rule Title: An X Windows display manager must not be installed unless approved.

Rule ID: SV-86931r2\_rule

Status: FAILED

Rule Title: The system must not be performing packet forwarding unless the system is a router.

Rule ID: SV-86933r1\_rule

Status: PASS

Rule Title: The system must not forward IPv6 source-routed packets.

Rule ID: SV-86943r1\_rule

Status: PASS

Rule Title: When passwords are changed or new passwords are established, pwquality must be used.

Rule ID: SV-87811r2\_rule

Status: PASS

Rule Title: The audit system must take appropriate action when there is an error sending audit records to a remote system.

Rule ID: SV-87815r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

Rule ID: SV-87817r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

Rule ID: SV-87819r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Rule ID: SV-87823r2\_rule

Status: PASS

Rule Title: The operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.

Rule ID: SV-87825r2\_rule

Status: PASS

Rule Title: The system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.

Rule ID: SV-87827r2\_rule

Status: PASS

Rule Title: Wireless network adapters must be disabled.

Rule ID: SV-87829r1\_rule

Status: PASS

Rule Title: The file permissions, ownership, and group membership of system files and commands must match the vendor values.

Rule ID: SV-86473r2\_rule

Status: (Manual verification)

Rule Title: The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

Rule ID: SV-86487r1\_rule

Status: (Manual verification)

Rule Title: The operating system must set the idle delay setting for all connection types.

Rule ID: SV-86519r3\_rule

Status: (Manual verification)

Rule Title: The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces.

Rule ID: SV-86523r1\_rule

Status: (Manual verification)

Rule Title: The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.

Rule ID: SV-86525r1\_rule

Status: (Manual verification)

Rule Title: User and group account administration utilities must be configured to store only encrypted representations of passwords.

Rule ID: SV-86547r2\_rule

Status: (Manual verification)

Rule Title: The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication.

Rule ID: SV-86589r1\_rule

Status: (Manual verification)

Rule Title: All privileged function executions must be audited.

Rule ID: SV-86719r2\_rule

Status: (Manual verification)

Rule Title: All uses of the pt\_chown command must be audited. pt\_chown in the glibc package before 2.19-18+deb8u4 on Debian jessie. In the Debian stretch has been abandoned.

Rule ID: SV-86805r2\_rule

Status: (Manual verification)

Rule Title: The host must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments.

Rule ID: SV-86843r1\_rule

Status: (Manual verification)

Rule Title: The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications.

Rule ID: SV-86851r2\_rule

Status: (Manual verification)

Rule Title: The system must be configured to prevent unrestricted mail relaying.

Rule ID: SV-86921r2\_rule

Status: (Manual verification)

Rule Title: If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode.

Rule ID: SV-86929r1\_rule

Status: (Manual verification)

Rule Title: The Network File System (NFS) must be configured to use RPCSEC\_GSS.

Rule ID: SV-86935r3\_rule

Status: (Manual verification)

Rule Title: The system access control program must be configured to grant or deny system access to specific hosts and services.

Rule ID: SV-86939r1\_rule

Status: (Manual verification)

Rule Title: The system must not have unauthorized IP tunnels configured.

Rule ID: SV-86941r1\_rule

Status: (Manual verification)

Rule Title: The operating system must have the required packages for multifactor authentication installed.

Rule ID: SV-87041r2\_rule

Status: (Manual verification)

Rule Title: The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).

Rule ID: SV-87051r2\_rule

Status: (Manual verification)

Rule Title: The operating system must implement certificate status checking for PKI authentication.

Rule ID: SV-87057r2\_rule

Status: (Manual verification)

Rule Title: The operating system must implement smart card logons for multifactor authentication for access to privileged accounts.

Rule ID: SV-87059r2\_rule

Status: (Manual verification)

Rule Title: The system must not have unnecessary accounts.

Rule ID: SV-86625r1\_rule

Status: (Manual verification)

Rule Title: Designated personnel must be notified if baseline configurations are changed in an unauthorized manner.

Rule ID: SV-86599r1\_rule

Status: (Manual verification)

Rule Title: The operating system must remove all software components after updated versions have been installed. Same to autoremove on the debian.

Rule ID: SV-86611r1\_rule

Status: (Manual verification)

## APPENDIX B – [Hardened Debian](https://github.com/hardenedlinux/harbian-audit) Audit Script Output

hardening [INFO] Start auditing for Debian.

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/1.1\_install\_updates.sh

1.1\_install\_updates [INFO] Working on 1.1\_install\_updates

1.1\_install\_updates [INFO] Checking Configuration

1.1\_install\_updates [INFO] Performing audit

1.1\_install\_updates [INFO] Checking if apt needs an update

1.1\_install\_updates [INFO] Fetching upgrades ...

1.1\_install\_updates [ KO ] There is 3 updates available :

Inst file [1:5.35-4] (1:5.35-4+deb10u1 Debian-Security:10/stable [amd64]) []

Inst libmagic1 [1:5.35-4] (1:5.35-4+deb10u1 Debian-Security:10/stable [amd64]) []

Inst libmagic-mgc [1:5.35-4] (1:5.35-4+deb10u1 Debian-Security:10/stable [amd64])

1.1\_install\_updates [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/1.2\_enable\_verify\_sign\_packages\_from\_repository.sh

1.2\_enable\_verify\_sign\_pa [INFO] Working on 1.2\_enable\_verify\_sign\_packages\_from\_repository

1.2\_enable\_verify\_sign\_pa [INFO] Checking Configuration

1.2\_enable\_verify\_sign\_pa [INFO] Performing audit

1.2\_enable\_verify\_sign\_pa [ OK ] The signature of packages option is enable

1.2\_enable\_verify\_sign\_pa [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/1.3\_enable\_verify\_sign\_of\_local\_packages.sh

1.3\_enable\_verify\_sign\_of [INFO] Working on 1.3\_enable\_verify\_sign\_of\_local\_packages

1.3\_enable\_verify\_sign\_of [INFO] Checking Configuration

1.3\_enable\_verify\_sign\_of [INFO] Performing audit

1.3\_enable\_verify\_sign\_of [ KO ] The signature of local packages option is disable

1.3\_enable\_verify\_sign\_of [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/1.4\_set\_no\_allow\_insecure\_repository\_by\_apt.sh

1.4\_set\_no\_allow\_insecure [INFO] Working on 1.4\_set\_no\_allow\_insecure\_repository\_by\_apt

1.4\_set\_no\_allow\_insecure [INFO] Checking Configuration

1.4\_set\_no\_allow\_insecure [INFO] Performing audit

1.4\_set\_no\_allow\_insecure [ OK ] The allow insecure repository when by apt update is disable

1.4\_set\_no\_allow\_insecure [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.1\_tmp\_partition.sh

2.1\_tmp\_partition [INFO] Working on 2.1\_tmp\_partition

2.1\_tmp\_partition [INFO] Checking Configuration

2.1\_tmp\_partition [INFO] Performing audit

2.1\_tmp\_partition [INFO] Verifying that /tmp is a filesystem/partition

2.1\_tmp\_partition [ OK ] /tmp is a partition

2.1\_tmp\_partition [ OK ] /tmp is mounted

2.1\_tmp\_partition [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.2\_tmp\_nodev.sh

2.2\_tmp\_nodev [INFO] Working on 2.2\_tmp\_nodev

2.2\_tmp\_nodev [INFO] Checking Configuration

2.2\_tmp\_nodev [INFO] Performing audit

2.2\_tmp\_nodev [INFO] Verifying that /tmp is a partition/filesystem

2.2\_tmp\_nodev [ OK ] /tmp is a partition

2.2\_tmp\_nodev [ OK ] /tmp has nodev in fstab

2.2\_tmp\_nodev [ OK ] /tmp mounted with nodev

2.2\_tmp\_nodev [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.3\_tmp\_nosuid.sh

2.3\_tmp\_nosuid [INFO] Working on 2.3\_tmp\_nosuid

2.3\_tmp\_nosuid [INFO] Checking Configuration

2.3\_tmp\_nosuid [INFO] Performing audit

2.3\_tmp\_nosuid [INFO] Verifying that /tmp is a partition/filesystem

2.3\_tmp\_nosuid [ OK ] /tmp is a partition

2.3\_tmp\_nosuid [ OK ] /tmp has nosuid in fstab

2.3\_tmp\_nosuid [ OK ] /tmp mounted with nosuid

2.3\_tmp\_nosuid [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.4\_tmp\_noexec.sh

2.4\_tmp\_noexec [INFO] Working on 2.4\_tmp\_noexec

2.4\_tmp\_noexec [INFO] Checking Configuration

2.4\_tmp\_noexec [INFO] Performing audit

2.4\_tmp\_noexec [INFO] Verifying that /tmp is a partition/filesystem

2.4\_tmp\_noexec [ OK ] /tmp is a partition

2.4\_tmp\_noexec [ OK ] /tmp has noexec in fstab

2.4\_tmp\_noexec [ OK ] /tmp mounted with noexec

2.4\_tmp\_noexec [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.5\_var\_partition.sh

2.5\_var\_partition [INFO] Working on 2.5\_var\_partition

2.5\_var\_partition [INFO] Checking Configuration

2.5\_var\_partition [INFO] Performing audit

2.5\_var\_partition [INFO] Verifying that /var is a partition

2.5\_var\_partition [ OK ] /var is a partition

2.5\_var\_partition [ OK ] /var is mounted

2.5\_var\_partition [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.6.1\_var\_tmp\_partition.sh

2.6.1\_var\_tmp\_partition [INFO] Working on 2.6.1\_var\_tmp\_partition

2.6.1\_var\_tmp\_partition [INFO] Checking Configuration

2.6.1\_var\_tmp\_partition [INFO] Performing audit

2.6.1\_var\_tmp\_partition [INFO] Verifying that /var/tmp is a partition

2.6.1\_var\_tmp\_partition [ OK ] /var/tmp is a partition

2.6.1\_var\_tmp\_partition [ OK ] /var/tmp is mounted

2.6.1\_var\_tmp\_partition [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.6.2\_var\_tmp\_nodev.sh

2.6.2\_var\_tmp\_nodev [INFO] Working on 2.6.2\_var\_tmp\_nodev

2.6.2\_var\_tmp\_nodev [INFO] Checking Configuration

2.6.2\_var\_tmp\_nodev [INFO] Performing audit

2.6.2\_var\_tmp\_nodev [INFO] Verifying that /var/tmp is a partition

2.6.2\_var\_tmp\_nodev [ OK ] /var/tmp is a partition

2.6.2\_var\_tmp\_nodev [ OK ] /var/tmp has nodev in fstab

2.6.2\_var\_tmp\_nodev [ OK ] /var/tmp mounted with nodev

2.6.2\_var\_tmp\_nodev [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.6.3\_var\_tmp\_nosuid.sh

2.6.3\_var\_tmp\_nosuid [INFO] Working on 2.6.3\_var\_tmp\_nosuid

2.6.3\_var\_tmp\_nosuid [INFO] Checking Configuration

2.6.3\_var\_tmp\_nosuid [INFO] Performing audit

2.6.3\_var\_tmp\_nosuid [INFO] Verifying that /var/tmp is a partition

2.6.3\_var\_tmp\_nosuid [ OK ] /var/tmp is a partition

2.6.3\_var\_tmp\_nosuid [ OK ] /var/tmp has nosuid in fstab

2.6.3\_var\_tmp\_nosuid [ OK ] /var/tmp mounted with nosuid

2.6.3\_var\_tmp\_nosuid [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.6.4\_var\_tmp\_noexec.sh

2.6.4\_var\_tmp\_noexec [INFO] Working on 2.6.4\_var\_tmp\_noexec

2.6.4\_var\_tmp\_noexec [INFO] Checking Configuration

2.6.4\_var\_tmp\_noexec [INFO] Performing audit

2.6.4\_var\_tmp\_noexec [INFO] Verifying that /var/tmp is a partition

2.6.4\_var\_tmp\_noexec [ OK ] /var/tmp is a partition

2.6.4\_var\_tmp\_noexec [ OK ] /var/tmp has noexec in fstab

2.6.4\_var\_tmp\_noexec [ OK ] /var/tmp mounted with noexec

2.6.4\_var\_tmp\_noexec [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.7\_var\_log\_partition.sh

2.7\_var\_log\_partition [INFO] Working on 2.7\_var\_log\_partition

2.7\_var\_log\_partition [INFO] Checking Configuration

2.7\_var\_log\_partition [INFO] Performing audit

2.7\_var\_log\_partition [INFO] Verifying that /var/log is a partition

2.7\_var\_log\_partition [ OK ] /var/log is a partition

2.7\_var\_log\_partition [ OK ] /var/log is mounted

2.7\_var\_log\_partition [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.8\_var\_log\_audit\_partition.sh

2.8\_var\_log\_audit\_partiti [INFO] Working on 2.8\_var\_log\_audit\_partition

2.8\_var\_log\_audit\_partiti [INFO] Checking Configuration

2.8\_var\_log\_audit\_partiti [INFO] Performing audit

2.8\_var\_log\_audit\_partiti [INFO] Verifying that /var/log/audit is a partition

2.8\_var\_log\_audit\_partiti [ OK ] /var/log/audit is a partition

2.8\_var\_log\_audit\_partiti [ OK ] /var/log/audit is mounted

2.8\_var\_log\_audit\_partiti [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.9\_home\_partition.sh

2.9\_home\_partition [INFO] Working on 2.9\_home\_partition

2.9\_home\_partition [INFO] Checking Configuration

2.9\_home\_partition [INFO] Performing audit

2.9\_home\_partition [INFO] Verifying that /home is a partition

2.9\_home\_partition [ OK ] /home is a partition

2.9\_home\_partition [ OK ] /home is mounted

2.9\_home\_partition [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.10\_home\_nodev.sh

2.10\_home\_nodev [INFO] Working on 2.10\_home\_nodev

2.10\_home\_nodev [INFO] Checking Configuration

2.10\_home\_nodev [INFO] Performing audit

2.10\_home\_nodev [INFO] Verifying that /home is a partition

2.10\_home\_nodev [ OK ] /home is a partition

2.10\_home\_nodev [ OK ] /home has nodev in fstab

2.10\_home\_nodev [ OK ] /home mounted with nodev

2.10\_home\_nodev [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.11\_removable\_device\_nodev.sh

2.11\_removable\_device\_nod [INFO] Working on 2.11\_removable\_device\_nodev

2.11\_removable\_device\_nod [INFO] Checking Configuration

2.11\_removable\_device\_nod [INFO] Performing audit

2.11\_removable\_device\_nod [INFO] Verifying if there is /media\S\* like partition

2.11\_removable\_device\_nod [INFO] detected /media\S\* like

2.11\_removable\_device\_nod [ OK ] /media/cdrom0 has nodev in fstab

2.11\_removable\_device\_nod [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.12\_removable\_device\_noexec.sh

2.12\_removable\_device\_noe [INFO] Working on 2.12\_removable\_device\_noexec

2.12\_removable\_device\_noe [INFO] Checking Configuration

2.12\_removable\_device\_noe [INFO] Performing audit

2.12\_removable\_device\_noe [INFO] Verifying if there is /media\S\* like partition

2.12\_removable\_device\_noe [INFO] detected /media\S\* like

2.12\_removable\_device\_noe [ OK ] /media/cdrom0 has noexec in fstab

2.12\_removable\_device\_noe [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.13\_removable\_device\_nosuid.sh

2.13\_removable\_device\_nos [INFO] Working on 2.13\_removable\_device\_nosuid

2.13\_removable\_device\_nos [INFO] Checking Configuration

2.13\_removable\_device\_nos [INFO] Performing audit

2.13\_removable\_device\_nos [INFO] Verifying if there is /media\S\* like partition

2.13\_removable\_device\_nos [INFO] detected /media\S\* like

2.13\_removable\_device\_nos [ OK ] /media/cdrom0 has nosuid in fstab

2.13\_removable\_device\_nos [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.14\_run\_shm\_nodev.sh

2.14\_run\_shm\_nodev [INFO] Working on 2.14\_run\_shm\_nodev

2.14\_run\_shm\_nodev [INFO] Checking Configuration

2.14\_run\_shm\_nodev [INFO] Performing audit

2.14\_run\_shm\_nodev [INFO] Verifying that /run/shm is a partition

2.14\_run\_shm\_nodev [ KO ] /run/shm is not a partition

2.14\_run\_shm\_nodev [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.15\_run\_shm\_nosuid.sh

2.15\_run\_shm\_nosuid [INFO] Working on 2.15\_run\_shm\_nosuid

2.15\_run\_shm\_nosuid [INFO] Checking Configuration

2.15\_run\_shm\_nosuid [INFO] Performing audit

2.15\_run\_shm\_nosuid [INFO] Verifying that /run/shm is a partition

2.15\_run\_shm\_nosuid [ KO ] /run/shm is not a partition

2.15\_run\_shm\_nosuid [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.16\_run\_shm\_noexec.sh

2.16\_run\_shm\_noexec [INFO] Working on 2.16\_run\_shm\_noexec

2.16\_run\_shm\_noexec [INFO] Checking Configuration

2.16\_run\_shm\_noexec [INFO] Performing audit

2.16\_run\_shm\_noexec [INFO] Verifying that /run/shm is a partition

2.16\_run\_shm\_noexec [ KO ] /run/shm is not a partition

2.16\_run\_shm\_noexec [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.17\_sticky\_bit\_world\_writable\_folder.sh

2.17\_sticky\_bit\_world\_wri [INFO] Working on 2.17\_sticky\_bit\_world\_writable\_folder

2.17\_sticky\_bit\_world\_wri [INFO] Checking Configuration

2.17\_sticky\_bit\_world\_wri [INFO] Performing audit

2.17\_sticky\_bit\_world\_wri [INFO] Checking if setuid is set on world writable Directories

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.18\_disable\_cramfs.sh

2.18\_disable\_cramfs [INFO] Working on 2.18\_disable\_cramfs

2.18\_disable\_cramfs [INFO] Checking Configuration

2.18\_disable\_cramfs [INFO] Performing audit

2.18\_disable\_cramfs [ OK ] CONFIG\_CRAMFS is disabled

2.18\_disable\_cramfs [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.19\_disable\_freevxfs.sh

2.19\_disable\_freevxfs [INFO] Working on 2.19\_disable\_freevxfs

2.19\_disable\_freevxfs [INFO] Checking Configuration

2.19\_disable\_freevxfs [INFO] Performing audit

2.19\_disable\_freevxfs [ KO ] CONFIG\_VXFS\_FS is enabled!

2.19\_disable\_freevxfs [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.20\_disable\_jffs2.sh

2.20\_disable\_jffs2 [INFO] Working on 2.20\_disable\_jffs2

2.20\_disable\_jffs2 [INFO] Checking Configuration

2.20\_disable\_jffs2 [INFO] Performing audit

2.20\_disable\_jffs2 [ KO ] CONFIG\_JFFS2\_FS is enabled!

2.20\_disable\_jffs2 [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.21\_disable\_hfs.sh

2.21\_disable\_hfs [INFO] Working on 2.21\_disable\_hfs

2.21\_disable\_hfs [INFO] Checking Configuration

2.21\_disable\_hfs [INFO] Performing audit

2.21\_disable\_hfs [ KO ] CONFIG\_HFS\_FS is enabled!

2.21\_disable\_hfs [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.22\_disable\_hfsplus.sh

2.22\_disable\_hfsplus [INFO] Working on 2.22\_disable\_hfsplus

2.22\_disable\_hfsplus [INFO] Checking Configuration

2.22\_disable\_hfsplus [INFO] Performing audit

2.22\_disable\_hfsplus [ KO ] CONFIG\_HFSPLUS\_FS is enabled!

2.22\_disable\_hfsplus [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.23\_disable\_squashfs.sh

2.23\_disable\_squashfs [INFO] Working on 2.23\_disable\_squashfs

2.23\_disable\_squashfs [INFO] Checking Configuration

2.23\_disable\_squashfs [INFO] Performing audit

2.23\_disable\_squashfs [ KO ] CONFIG\_SQUASHFS is enabled!

2.23\_disable\_squashfs [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.24\_disable\_udf.sh

2.24\_disable\_udf [INFO] Working on 2.24\_disable\_udf

2.24\_disable\_udf [INFO] Checking Configuration

2.24\_disable\_udf [INFO] Performing audit

2.24\_disable\_udf [ KO ] CONFIG\_UDF\_FS is enabled!

2.24\_disable\_udf [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.25\_disable\_automounting.sh

2.25\_disable\_automounting [INFO] Working on 2.25\_disable\_automounting

2.25\_disable\_automounting [INFO] Checking Configuration

2.25\_disable\_automounting [INFO] Performing audit

2.25\_disable\_automounting [ OK ] autofs is not installed

2.25\_disable\_automounting [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.26\_home\_nosuid.sh

2.26\_home\_nosuid [INFO] Working on 2.26\_home\_nosuid

2.26\_home\_nosuid [INFO] Checking Configuration

2.26\_home\_nosuid [INFO] Performing audit

2.26\_home\_nosuid [INFO] Verifying that /home is a filesystem/partition

2.26\_home\_nosuid [ OK ] /home is a partition

2.26\_home\_nosuid [ OK ] /home has nosuid in fstab

2.26\_home\_nosuid [ OK ] /home mounted with nosuid

2.26\_home\_nosuid [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.27\_nfs\_nosuid.sh

2.27\_nfs\_nosuid [INFO] Working on 2.27\_nfs\_nosuid

2.27\_nfs\_nosuid [INFO] Checking Configuration

2.27\_nfs\_nosuid [INFO] Performing audit

2.27\_nfs\_nosuid [INFO] Verifying that nfs is a filesystem/partition

2.27\_nfs\_nosuid [ none entity, so it's not scored ] There is no mount directory with file system type nfs

2.27\_nfs\_nosuid [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.28\_nfs\_noexec.sh

2.28\_nfs\_noexec [INFO] Working on 2.28\_nfs\_noexec

2.28\_nfs\_noexec [INFO] Checking Configuration

2.28\_nfs\_noexec [INFO] Performing audit

2.28\_nfs\_noexec [INFO] Verifying that nfs is a filesystem/partition

2.28\_nfs\_noexec [ none entity, so it's not scored ] There is no mount directory with file system type nfs

2.28\_nfs\_noexec [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/2.29\_nfs\_RPCSEC\_GSS.sh

2.29\_nfs\_RPCSEC\_GSS [INFO] Working on 2.29\_nfs\_RPCSEC\_GSS

2.29\_nfs\_RPCSEC\_GSS [INFO] Checking Configuration

2.29\_nfs\_RPCSEC\_GSS [INFO] Performing audit

2.29\_nfs\_RPCSEC\_GSS [INFO] Verifying that nfs is a filesystem/partition

2.29\_nfs\_RPCSEC\_GSS [ none entity, so it's not scored ] There is no mount directory with file system type nfs

2.29\_nfs\_RPCSEC\_GSS [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/3.1\_bootloader\_ownership.sh

3.1\_bootloader\_ownership [INFO] Working on 3.1\_bootloader\_ownership

3.1\_bootloader\_ownership [INFO] Checking Configuration

3.1\_bootloader\_ownership [WARN] Grub is not installed, not handling configuration

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/3.2\_bootloader\_permissions.sh

3.2\_bootloader\_permission [INFO] Working on 3.2\_bootloader\_permissions

3.2\_bootloader\_permission [INFO] Checking Configuration

3.2\_bootloader\_permission [WARN] grub-pc is not installed, not handling configuration

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/3.3\_bootloader\_password.sh

3.3\_bootloader\_password [INFO] Working on 3.3\_bootloader\_password

3.3\_bootloader\_password [INFO] Checking Configuration

3.3\_bootloader\_password [WARN] grub-pc is not installed, not handling configuration

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/3.4\_root\_password.sh

3.4\_root\_password [INFO] Working on 3.4\_root\_password

3.4\_root\_password [INFO] Checking Configuration

3.4\_root\_password [INFO] Performing audit

3.4\_root\_password [ OK ] ^root:[\*\!]: is not present in /etc/shadow

3.4\_root\_password [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/4.1\_restrict\_core\_dumps.sh

4.1\_restrict\_core\_dumps [INFO] Working on 4.1\_restrict\_core\_dumps

4.1\_restrict\_core\_dumps [INFO] Checking Configuration

4.1\_restrict\_core\_dumps [INFO] Performing audit

4.1\_restrict\_core\_dumps [ KO ] ^\\*[[:space:]]\*hard[[:space:]]\*core[[:space:]]\*0$ not present in /etc/security/limits.conf

4.1\_restrict\_core\_dumps [ OK ] fs.suid\_dumpable correctly set to 0

4.1\_restrict\_core\_dumps [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/4.2\_enable\_nx\_support.sh

4.2\_enable\_nx\_support [INFO] Working on 4.2\_enable\_nx\_support

4.2\_enable\_nx\_support [INFO] Checking Configuration

4.2\_enable\_nx\_support [INFO] Performing audit

4.2\_enable\_nx\_support [ OK ] NX[[:space:]]\(Execute[[:space:]]Disable\)[[:space:]]protection:[[:space:]]active is present in dmesg

4.2\_enable\_nx\_support [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/4.3\_enable\_randomized\_vm\_placement.sh

4.3\_enable\_randomized\_vm\_ [INFO] Working on 4.3\_enable\_randomized\_vm\_placement

4.3\_enable\_randomized\_vm\_ [INFO] Checking Configuration

4.3\_enable\_randomized\_vm\_ [INFO] Performing audit

4.3\_enable\_randomized\_vm\_ [ OK ] kernel.randomize\_va\_space correctly set to 2

4.3\_enable\_randomized\_vm\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/4.4\_disable\_prelink.sh

4.4\_disable\_prelink [INFO] Working on 4.4\_disable\_prelink

4.4\_disable\_prelink [INFO] Checking Configuration

4.4\_disable\_prelink [INFO] Performing audit

4.4\_disable\_prelink [ OK ] prelink is absent

4.4\_disable\_prelink [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/4.5\_enable\_apparmor.sh

4.5\_enable\_apparmor [INFO] Working on 4.5\_enable\_apparmor

4.5\_enable\_apparmor [INFO] Checking Configuration

4.5\_enable\_apparmor [INFO] Performing audit

4.5\_enable\_apparmor [ OK ] apparmor-utils is installed

4.5\_enable\_apparmor [ OK ] There are apparmor=1 security=apparmor to GRUB\_CMDLINE\_LINUX in /etc/default/grub

4.5\_enable\_apparmor [ OK ] AppArmor profiles is enable in the system

4.5\_enable\_apparmor [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/4.6\_disable\_usb\_devices.sh

4.6\_disable\_usb\_devices [INFO] Working on 4.6\_disable\_usb\_devices

4.6\_disable\_usb\_devices [INFO] Checking Configuration

4.6\_disable\_usb\_devices [INFO] Performing audit

4.6\_disable\_usb\_devices [ KO ] ACTION=="add", SUBSYSTEMS=="usb", TEST=="authorized\_default", ATTR{authorized\_default}="0" is not present in /etc/udev/rules.d

4.6\_disable\_usb\_devices [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.1.1\_disable\_nis.sh

5.1.1\_disable\_nis [INFO] Working on 5.1.1\_disable\_nis

5.1.1\_disable\_nis [INFO] Checking Configuration

5.1.1\_disable\_nis [INFO] Performing audit

5.1.1\_disable\_nis [ OK ] nis is absent

5.1.1\_disable\_nis [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.1.2\_disable\_rsh.sh

5.1.2\_disable\_rsh [INFO] Working on 5.1.2\_disable\_rsh

5.1.2\_disable\_rsh [INFO] Checking Configuration

5.1.2\_disable\_rsh [INFO] Performing audit

5.1.2\_disable\_rsh [ OK ] rsh-server is absent

5.1.2\_disable\_rsh [ OK ] rsh-redone-server is absent

5.1.2\_disable\_rsh [ OK ] heimdal-servers is absent

5.1.2\_disable\_rsh [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.1.3\_disable\_rsh\_client.sh

5.1.3\_disable\_rsh\_client [INFO] Working on 5.1.3\_disable\_rsh\_client

5.1.3\_disable\_rsh\_client [INFO] Checking Configuration

5.1.3\_disable\_rsh\_client [INFO] Performing audit

5.1.3\_disable\_rsh\_client [ OK ] rsh-client is absent

5.1.3\_disable\_rsh\_client [ OK ] rsh-redone-client is absent

5.1.3\_disable\_rsh\_client [ OK ] heimdal-clients is absent

5.1.3\_disable\_rsh\_client [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.1.4\_disable\_talk.sh

5.1.4\_disable\_talk [INFO] Working on 5.1.4\_disable\_talk

5.1.4\_disable\_talk [INFO] Checking Configuration

5.1.4\_disable\_talk [INFO] Performing audit

5.1.4\_disable\_talk [ OK ] inetutils-talkd is absent

5.1.4\_disable\_talk [ OK ] talkd is absent

5.1.4\_disable\_talk [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.1.5\_disable\_talk\_client.sh

5.1.5\_disable\_talk\_client [INFO] Working on 5.1.5\_disable\_talk\_client

5.1.5\_disable\_talk\_client [INFO] Checking Configuration

5.1.5\_disable\_talk\_client [INFO] Performing audit

5.1.5\_disable\_talk\_client [ OK ] talk is absent

5.1.5\_disable\_talk\_client [ OK ] inetutils-talk is absent

5.1.5\_disable\_talk\_client [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.1.6\_disable\_telnet\_server.sh

5.1.6\_disable\_telnet\_serv [INFO] Working on 5.1.6\_disable\_telnet\_server

5.1.6\_disable\_telnet\_serv [INFO] Checking Configuration

5.1.6\_disable\_telnet\_serv [INFO] Performing audit

5.1.6\_disable\_telnet\_serv [ OK ] telnetd is absent

5.1.6\_disable\_telnet\_serv [ OK ] inetutils-telnetd is absent

5.1.6\_disable\_telnet\_serv [ OK ] telnetd-ssl is absent

5.1.6\_disable\_telnet\_serv [ OK ] krb5-telnetd is absent

5.1.6\_disable\_telnet\_serv [ OK ] heimdal-servers is absent

5.1.6\_disable\_telnet\_serv [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.1.7\_disable\_inetd.sh

5.1.7\_disable\_inetd [INFO] Working on 5.1.7\_disable\_inetd

5.1.7\_disable\_inetd [INFO] Checking Configuration

5.1.7\_disable\_inetd [INFO] Performing audit

5.1.7\_disable\_inetd [ OK ] openbsd-inetd is absent

5.1.7\_disable\_inetd [ OK ] xinetd is absent

5.1.7\_disable\_inetd [ OK ] rlinetd is absent

5.1.7\_disable\_inetd [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.2\_install\_screen.sh

5.2\_install\_screen [INFO] Working on 5.2\_install\_screen

5.2\_install\_screen [INFO] Checking Configuration

5.2\_install\_screen [INFO] Performing audit

5.2\_install\_screen [ OK ] screen is installed

5.2\_install\_screen [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.3\_enable\_openssh\_server.sh

5.3\_enable\_openssh\_server [INFO] Working on 5.3\_enable\_openssh\_server

5.3\_enable\_openssh\_server [INFO] Checking Configuration

5.3\_enable\_openssh\_server [INFO] Performing audit

5.3\_enable\_openssh\_server [ OK ] openssh-server is installed

5.3\_enable\_openssh\_server [ OK ] openssh-client is installed

5.3\_enable\_openssh\_server [ OK ] ssh.service is actived

5.3\_enable\_openssh\_server [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.4\_disable\_ctrl\_alt\_del\_target.sh

5.4\_disable\_ctrl\_alt\_del\_ [INFO] Working on 5.4\_disable\_ctrl\_alt\_del\_target

5.4\_disable\_ctrl\_alt\_del\_ [INFO] Checking Configuration

5.4\_disable\_ctrl\_alt\_del\_ [INFO] Performing audit

5.4\_disable\_ctrl\_alt\_del\_ [ KO ] ctrl-alt-del.target is enabled.

5.4\_disable\_ctrl\_alt\_del\_ [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/5.8\_ensure\_installed\_sudo.sh

5.8\_ensure\_installed\_sudo [INFO] Working on 5.8\_ensure\_installed\_sudo

5.8\_ensure\_installed\_sudo [INFO] Checking Configuration

5.8\_ensure\_installed\_sudo [INFO] Performing audit

5.8\_ensure\_installed\_sudo [ OK ] sudo is installed

5.8\_ensure\_installed\_sudo [ OK ] Log file is set to /var/log/sudo.log in /etc/sudoers

5.8\_ensure\_installed\_sudo [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.1\_disable\_xwindow\_system.sh

6.1\_disable\_xwindow\_syste [INFO] Working on 6.1\_disable\_xwindow\_system

6.1\_disable\_xwindow\_syste [INFO] Checking Configuration

6.1\_disable\_xwindow\_syste [INFO] Performing audit

6.1\_disable\_xwindow\_syste [ KO ] xserver-xorg-core is installed!

6.1\_disable\_xwindow\_syste [ OK ] xserver-xorg-core-dbg is absent

6.1\_disable\_xwindow\_syste [ KO ] xserver-common is installed!

6.1\_disable\_xwindow\_syste [ OK ] xserver-xephyr is absent

6.1\_disable\_xwindow\_syste [ OK ] xserver-xfbdev is absent

6.1\_disable\_xwindow\_syste [ OK ] tightvncserver is absent

6.1\_disable\_xwindow\_syste [ OK ] vnc4server is absent

6.1\_disable\_xwindow\_syste [ OK ] fglrx-driver is absent

6.1\_disable\_xwindow\_syste [ OK ] xvfb is absent

6.1\_disable\_xwindow\_syste [ OK ] xserver-xorg-video-nvidia-legacy-173xx is absent

6.1\_disable\_xwindow\_syste [ OK ] xserver-xorg-video-nvidia-legacy-96xx is absent

6.1\_disable\_xwindow\_syste [ OK ] xnest is absent

6.1\_disable\_xwindow\_syste [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.2\_disable\_avahi\_server.sh

6.2\_disable\_avahi\_server [INFO] Working on 6.2\_disable\_avahi\_server

6.2\_disable\_avahi\_server [INFO] Checking Configuration

6.2\_disable\_avahi\_server [INFO] Performing audit

6.2\_disable\_avahi\_server [ OK ] avahi-daemon is absent

6.2\_disable\_avahi\_server [ KO ] libavahi-common-data is installed!

6.2\_disable\_avahi\_server [ KO ] libavahi-common3 is installed!

6.2\_disable\_avahi\_server [ OK ] libavahi-core7 is absent

6.2\_disable\_avahi\_server [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.3\_disable\_print\_server.sh

6.3\_disable\_print\_server [INFO] Working on 6.3\_disable\_print\_server

6.3\_disable\_print\_server [INFO] Checking Configuration

6.3\_disable\_print\_server [INFO] Performing audit

6.3\_disable\_print\_server [ KO ] libcups2 is installed!

6.3\_disable\_print\_server [ OK ] libcupscgi1 is absent

6.3\_disable\_print\_server [ OK ] libcupsimage2 is absent

6.3\_disable\_print\_server [ OK ] libcupsmime1 is absent

6.3\_disable\_print\_server [ OK ] libcupsppdc1 is absent

6.3\_disable\_print\_server [ OK ] cups-common is absent

6.3\_disable\_print\_server [ OK ] cups-client is absent

6.3\_disable\_print\_server [ OK ] cups-ppdc is absent

6.3\_disable\_print\_server [ OK ] libcupsfilters1 is absent

6.3\_disable\_print\_server [ OK ] cups-filters is absent

6.3\_disable\_print\_server [ OK ] cups is absent

6.3\_disable\_print\_server [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.4\_disable\_dhcp.sh

6.4\_disable\_dhcp [INFO] Working on 6.4\_disable\_dhcp

6.4\_disable\_dhcp [INFO] Checking Configuration

6.4\_disable\_dhcp [INFO] Performing audit

6.4\_disable\_dhcp [ OK ] udhcpd is absent

6.4\_disable\_dhcp [ OK ] isc-dhcp-server is absent

6.4\_disable\_dhcp [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.5\_ensure\_time\_sync\_server\_is\_installed.sh

6.5\_ensure\_time\_sync\_serv [INFO] Working on 6.5\_ensure\_time\_sync\_server\_is\_installed

6.5\_ensure\_time\_sync\_serv [INFO] Checking Configuration

6.5\_ensure\_time\_sync\_serv [INFO] Performing audit

6.5\_ensure\_time\_sync\_serv [ OK ] ntp is installed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.6\_disable\_ldap.sh

6.6\_disable\_ldap [INFO] Working on 6.6\_disable\_ldap

6.6\_disable\_ldap [INFO] Checking Configuration

6.6\_disable\_ldap [INFO] Performing audit

6.6\_disable\_ldap [ OK ] slapd is absent

6.6\_disable\_ldap [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.7\_disable\_nfs\_rpc.sh

6.7\_disable\_nfs\_rpc [INFO] Working on 6.7\_disable\_nfs\_rpc

6.7\_disable\_nfs\_rpc [INFO] Checking Configuration

6.7\_disable\_nfs\_rpc [INFO] Performing audit

6.7\_disable\_nfs\_rpc [ OK ] rpcbind is absent

6.7\_disable\_nfs\_rpc [ OK ] nfs-kernel-server is absent

6.7\_disable\_nfs\_rpc [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.8\_disable\_dns\_server.sh

6.8\_disable\_dns\_server [INFO] Working on 6.8\_disable\_dns\_server

6.8\_disable\_dns\_server [INFO] Checking Configuration

6.8\_disable\_dns\_server [INFO] Performing audit

6.8\_disable\_dns\_server [ OK ] bind9 is absent

6.8\_disable\_dns\_server [ OK ] unbound is absent

6.8\_disable\_dns\_server [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.9\_disable\_ftp.sh

6.9\_disable\_ftp [INFO] Working on 6.9\_disable\_ftp

6.9\_disable\_ftp [INFO] Checking Configuration

6.9\_disable\_ftp [INFO] Performing audit

6.9\_disable\_ftp [ OK ] ftpd is absent

6.9\_disable\_ftp [ OK ] ftpd-ssl is absent

6.9\_disable\_ftp [ OK ] heimdal-servers is absent

6.9\_disable\_ftp [ OK ] inetutils-ftpd is absent

6.9\_disable\_ftp [ OK ] krb5-ftpd is absent

6.9\_disable\_ftp [ OK ] muddleftpd is absent

6.9\_disable\_ftp [ OK ] proftpd-basic is absent

6.9\_disable\_ftp [ OK ] pure-ftpd is absent

6.9\_disable\_ftp [ OK ] pure-ftpd-ldap is absent

6.9\_disable\_ftp [ OK ] pure-ftpd-mysql is absent

6.9\_disable\_ftp [ OK ] pure-ftpd-postgresql is absent

6.9\_disable\_ftp [ OK ] twoftpd-run is absent

6.9\_disable\_ftp [ OK ] vsftpd is absent

6.9\_disable\_ftp [ OK ] wzdftpd is absent

6.9\_disable\_ftp [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.10\_disable\_http\_server.sh

6.10\_disable\_http\_server [INFO] Working on 6.10\_disable\_http\_server

6.10\_disable\_http\_server [INFO] Checking Configuration

6.10\_disable\_http\_server [INFO] Performing audit

6.10\_disable\_http\_server [ OK ] nginx is absent

6.10\_disable\_http\_server [ OK ] apache2 is absent

6.10\_disable\_http\_server [ OK ] lighttpd is absent

6.10\_disable\_http\_server [ OK ] micro-httpd is absent

6.10\_disable\_http\_server [ OK ] mini-httpd is absent

6.10\_disable\_http\_server [ OK ] yaws is absent

6.10\_disable\_http\_server [ OK ] boa is absent

6.10\_disable\_http\_server [ OK ] bozohttpd is absent

6.10\_disable\_http\_server [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.11\_disable\_imap\_pop.sh

6.11\_disable\_imap\_pop [INFO] Working on 6.11\_disable\_imap\_pop

6.11\_disable\_imap\_pop [INFO] Checking Configuration

6.11\_disable\_imap\_pop [INFO] Performing audit

6.11\_disable\_imap\_pop [ OK ] citadel-server is absent

6.11\_disable\_imap\_pop [ OK ] courier-imap is absent

6.11\_disable\_imap\_pop [ OK ] cyrus-imapd-2.4 is absent

6.11\_disable\_imap\_pop [ OK ] dovecot-imapd is absent

6.11\_disable\_imap\_pop [ OK ] mailutils-imap4d is absent

6.11\_disable\_imap\_pop [ OK ] courier-pop is absent

6.11\_disable\_imap\_pop [ OK ] cyrus-pop3d-2.4 is absent

6.11\_disable\_imap\_pop [ OK ] dovecot-pop3d is absent

6.11\_disable\_imap\_pop [ OK ] heimdal-servers is absent

6.11\_disable\_imap\_pop [ OK ] mailutils-pop3d is absent

6.11\_disable\_imap\_pop [ OK ] popa3d is absent

6.11\_disable\_imap\_pop [ OK ] solid-pop3d is absent

6.11\_disable\_imap\_pop [ OK ] xmail is absent

6.11\_disable\_imap\_pop [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.12\_disable\_samba.sh

6.12\_disable\_samba [INFO] Working on 6.12\_disable\_samba

6.12\_disable\_samba [INFO] Checking Configuration

6.12\_disable\_samba [INFO] Performing audit

6.12\_disable\_samba [ OK ] samba is absent

6.12\_disable\_samba [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.13\_disable\_http\_proxy.sh

6.13\_disable\_http\_proxy [INFO] Working on 6.13\_disable\_http\_proxy

6.13\_disable\_http\_proxy [INFO] Checking Configuration

6.13\_disable\_http\_proxy [INFO] Performing audit

6.13\_disable\_http\_proxy [ OK ] squid3 is absent

6.13\_disable\_http\_proxy [ OK ] squid is absent

6.13\_disable\_http\_proxy [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.14\_disable\_snmp\_server.sh

6.14\_disable\_snmp\_server [INFO] Working on 6.14\_disable\_snmp\_server

6.14\_disable\_snmp\_server [INFO] Checking Configuration

6.14\_disable\_snmp\_server [INFO] Performing audit

6.14\_disable\_snmp\_server [ OK ] snmpd is absent

6.14\_disable\_snmp\_server [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.15\_mta\_localhost.sh

6.15\_mta\_localhost [INFO] Working on 6.15\_mta\_localhost

6.15\_mta\_localhost [INFO] Checking Configuration

6.15\_mta\_localhost [INFO] Performing audit

6.15\_mta\_localhost [INFO] Checking netport ports opened

6.15\_mta\_localhost [ OK ] Nothing listens on 25 port, probably unix socket configured

6.15\_mta\_localhost [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.16\_disable\_rsync.sh

6.16\_disable\_rsync [INFO] Working on 6.16\_disable\_rsync

6.16\_disable\_rsync [INFO] Checking Configuration

6.16\_disable\_rsync [INFO] Performing audit

6.16\_disable\_rsync [ OK ] rsync is installed, checking configuration

6.16\_disable\_rsync [ OK ] RSYNC\_ENABLE=false found in /etc/default/rsync

6.16\_disable\_rsync [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.17\_ensure\_virul\_scan\_server\_is\_enabled.sh

6.17\_ensure\_virul\_scan\_se [INFO] Working on 6.17\_ensure\_virul\_scan\_server\_is\_enabled

6.17\_ensure\_virul\_scan\_se [INFO] Checking Configuration

6.17\_ensure\_virul\_scan\_se [INFO] Performing audit

6.17\_ensure\_virul\_scan\_se [ KO ] clamav-daemon is not runing

6.17\_ensure\_virul\_scan\_se [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.18\_ensure\_virusscan\_program\_update\_is\_enabled.sh

6.18\_ensure\_virusscan\_pro [INFO] Working on 6.18\_ensure\_virusscan\_program\_update\_is\_enabled

6.18\_ensure\_virusscan\_pro [INFO] Checking Configuration

6.18\_ensure\_virusscan\_pro [INFO] Performing audit

6.18\_ensure\_virusscan\_pro [ OK ] Clamav database file has a date less than seven days from the current date

6.18\_ensure\_virusscan\_pro [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.19\_configure\_ntp.sh

6.19\_configure\_ntp [INFO] Working on 6.19\_configure\_ntp

6.19\_configure\_ntp [INFO] Checking Configuration

6.19\_configure\_ntp [INFO] Performing audit

6.19\_configure\_ntp [ OK ] ntp is installed, checking configuration

6.19\_configure\_ntp [ KO ] ^(server|pool) not found in /etc/ntp.conf

6.19\_configure\_ntp [ OK ] ^restrict -4 default (kod nomodify notrap nopeer noquery|ignore) found in /etc/ntp.conf

6.19\_configure\_ntp [ OK ] RUNASUSER=ntp found in /etc/init.d/ntp

6.19\_configure\_ntp [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/6.20\_configure\_chrony.sh

6.20\_configure\_chrony [INFO] Working on 6.20\_configure\_chrony

6.20\_configure\_chrony [INFO] Checking Configuration

6.20\_configure\_chrony [INFO] Performing audit

6.20\_configure\_chrony [ OK ] Analogons pagkage ntp is installed. So pass check.

6.20\_configure\_chrony [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.1.1\_disable\_ip\_forwarding.sh

7.1.1\_disable\_ip\_forwardi [INFO] Working on 7.1.1\_disable\_ip\_forwarding

7.1.1\_disable\_ip\_forwardi [INFO] Checking Configuration

7.1.1\_disable\_ip\_forwardi [INFO] Performing audit

7.1.1\_disable\_ip\_forwardi [ OK ] net.ipv4.ip\_forward correctly set to 0

7.1.1\_disable\_ip\_forwardi [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.1.2\_disable\_send\_packet\_redirects.sh

7.1.2\_disable\_send\_packet [INFO] Working on 7.1.2\_disable\_send\_packet\_redirects

7.1.2\_disable\_send\_packet [INFO] Checking Configuration

7.1.2\_disable\_send\_packet [INFO] Performing audit

7.1.2\_disable\_send\_packet [ OK ] net.ipv4.conf.all.send\_redirects correctly set to 0

7.1.2\_disable\_send\_packet [ OK ] net.ipv4.conf.default.send\_redirects correctly set to 0

7.1.2\_disable\_send\_packet [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.1.3\_disable\_interface\_promisc\_mode.sh

7.1.3\_disable\_interface\_p [INFO] Working on 7.1.3\_disable\_interface\_promisc\_mode

7.1.3\_disable\_interface\_p [INFO] Checking Configuration

7.1.3\_disable\_interface\_p [INFO] Performing audit

7.1.3\_disable\_interface\_p [ OK ] Not set promisc mode for network interface in the system.

7.1.3\_disable\_interface\_p [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.1\_disable\_source\_routed\_packets.sh

7.2.1\_disable\_source\_rout [INFO] Working on 7.2.1\_disable\_source\_routed\_packets

7.2.1\_disable\_source\_rout [INFO] Checking Configuration

7.2.1\_disable\_source\_rout [INFO] Performing audit

7.2.1\_disable\_source\_rout [ OK ] net.ipv4.conf.all.accept\_source\_route correctly set to 0

7.2.1\_disable\_source\_rout [ OK ] net.ipv4.conf.default.accept\_source\_route correctly set to 0

7.2.1\_disable\_source\_rout [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.2\_disable\_icmp\_redirect.sh

7.2.2\_disable\_icmp\_redire [INFO] Working on 7.2.2\_disable\_icmp\_redirect

7.2.2\_disable\_icmp\_redire [INFO] Checking Configuration

7.2.2\_disable\_icmp\_redire [INFO] Performing audit

7.2.2\_disable\_icmp\_redire [ OK ] net.ipv4.conf.all.accept\_redirects correctly set to 0

7.2.2\_disable\_icmp\_redire [ OK ] net.ipv4.conf.default.accept\_redirects correctly set to 0

7.2.2\_disable\_icmp\_redire [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.3\_disable\_secure\_icmp\_redirect.sh

7.2.3\_disable\_secure\_icmp [INFO] Working on 7.2.3\_disable\_secure\_icmp\_redirect

7.2.3\_disable\_secure\_icmp [INFO] Checking Configuration

7.2.3\_disable\_secure\_icmp [INFO] Performing audit

7.2.3\_disable\_secure\_icmp [ OK ] net.ipv4.conf.all.secure\_redirects correctly set to 1

7.2.3\_disable\_secure\_icmp [ OK ] net.ipv4.conf.default.secure\_redirects correctly set to 1

7.2.3\_disable\_secure\_icmp [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.4\_log\_martian\_packets.sh

7.2.4\_log\_martian\_packets [INFO] Working on 7.2.4\_log\_martian\_packets

7.2.4\_log\_martian\_packets [INFO] Checking Configuration

7.2.4\_log\_martian\_packets [INFO] Performing audit

7.2.4\_log\_martian\_packets [ KO ] net.ipv4.conf.all.log\_martians was not set to 1

7.2.4\_log\_martian\_packets [ KO ] net.ipv4.conf.default.log\_martians was not set to 1

7.2.4\_log\_martian\_packets [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.5\_ignore\_broadcast\_requests.sh

7.2.5\_ignore\_broadcast\_re [INFO] Working on 7.2.5\_ignore\_broadcast\_requests

7.2.5\_ignore\_broadcast\_re [INFO] Checking Configuration

7.2.5\_ignore\_broadcast\_re [INFO] Performing audit

7.2.5\_ignore\_broadcast\_re [ OK ] net.ipv4.icmp\_echo\_ignore\_broadcasts correctly set to 1

7.2.5\_ignore\_broadcast\_re [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.6\_enable\_bad\_error\_message\_protection.sh

7.2.6\_enable\_bad\_error\_me [INFO] Working on 7.2.6\_enable\_bad\_error\_message\_protection

7.2.6\_enable\_bad\_error\_me [INFO] Checking Configuration

7.2.6\_enable\_bad\_error\_me [INFO] Performing audit

7.2.6\_enable\_bad\_error\_me [ OK ] net.ipv4.icmp\_ignore\_bogus\_error\_responses correctly set to 1

7.2.6\_enable\_bad\_error\_me [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.7\_enable\_source\_route\_validation.sh

7.2.7\_enable\_source\_route [INFO] Working on 7.2.7\_enable\_source\_route\_validation

7.2.7\_enable\_source\_route [INFO] Checking Configuration

7.2.7\_enable\_source\_route [INFO] Performing audit

7.2.7\_enable\_source\_route [ KO ] net.ipv4.conf.all.rp\_filter was not set to 1

7.2.7\_enable\_source\_route [ KO ] net.ipv4.conf.default.rp\_filter was not set to 1

7.2.7\_enable\_source\_route [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.2.8\_enable\_tcp\_syn\_cookies.sh

7.2.8\_enable\_tcp\_syn\_cook [INFO] Working on 7.2.8\_enable\_tcp\_syn\_cookies

7.2.8\_enable\_tcp\_syn\_cook [INFO] Checking Configuration

7.2.8\_enable\_tcp\_syn\_cook [INFO] Performing audit

7.2.8\_enable\_tcp\_syn\_cook [ OK ] net.ipv4.tcp\_syncookies correctly set to 1

7.2.8\_enable\_tcp\_syn\_cook [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.3.1\_disable\_ipv6\_router\_advertisement.sh

7.3.1\_disable\_ipv6\_router [INFO] Working on 7.3.1\_disable\_ipv6\_router\_advertisement

7.3.1\_disable\_ipv6\_router [INFO] Checking Configuration

7.3.1\_disable\_ipv6\_router [INFO] Performing audit

7.3.1\_disable\_ipv6\_router [ OK ] ipv6 is disabled

7.3.1\_disable\_ipv6\_router [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.3.2\_disable\_ipv6\_redirect.sh

7.3.2\_disable\_ipv6\_redire [INFO] Working on 7.3.2\_disable\_ipv6\_redirect

7.3.2\_disable\_ipv6\_redire [INFO] Checking Configuration

7.3.2\_disable\_ipv6\_redire [INFO] Performing audit

7.3.2\_disable\_ipv6\_redire [ OK ] ipv6 is disabled

7.3.2\_disable\_ipv6\_redire [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.4.1\_install\_tcp\_wrapper.sh

7.4.1\_install\_tcp\_wrapper [INFO] Working on 7.4.1\_install\_tcp\_wrapper

7.4.1\_install\_tcp\_wrapper [INFO] Checking Configuration

7.4.1\_install\_tcp\_wrapper [INFO] Performing audit

7.4.1\_install\_tcp\_wrapper [ KO ] tcpd is not installed!

7.4.1\_install\_tcp\_wrapper [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.4.2\_hosts\_allow.sh

7.4.2\_hosts\_allow [INFO] Working on 7.4.2\_hosts\_allow

7.4.2\_hosts\_allow [INFO] Checking Configuration

7.4.2\_hosts\_allow [INFO] Performing audit

7.4.2\_hosts\_allow [ OK ] /etc/hosts.allow exist

7.4.2\_hosts\_allow [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.4.3\_hosts\_allow\_permissions.sh

7.4.3\_hosts\_allow\_permiss [INFO] Working on 7.4.3\_hosts\_allow\_permissions

7.4.3\_hosts\_allow\_permiss [INFO] Checking Configuration

7.4.3\_hosts\_allow\_permiss [INFO] Performing audit

7.4.3\_hosts\_allow\_permiss [ OK ] /etc/hosts.allow has correct permissions

7.4.3\_hosts\_allow\_permiss [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.4.4\_hosts\_deny.sh

7.4.4\_hosts\_deny [INFO] Working on 7.4.4\_hosts\_deny

7.4.4\_hosts\_deny [INFO] Checking Configuration

7.4.4\_hosts\_deny [INFO] Performing audit

7.4.4\_hosts\_deny [ OK ] /etc/hosts.deny exists, checking configuration

7.4.4\_hosts\_deny [ KO ] ALL: ALL is not present in /etc/hosts.deny, we have to deny everything

7.4.4\_hosts\_deny [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.4.5\_hosts\_deny\_permissions.sh

7.4.5\_hosts\_deny\_permissi [INFO] Working on 7.4.5\_hosts\_deny\_permissions

7.4.5\_hosts\_deny\_permissi [INFO] Checking Configuration

7.4.5\_hosts\_deny\_permissi [INFO] Performing audit

7.4.5\_hosts\_deny\_permissi [ OK ] /etc/hosts.deny has correct permissions

7.4.5\_hosts\_deny\_permissi [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.5.1\_disable\_dccp.sh

7.5.1\_disable\_dccp [INFO] Working on 7.5.1\_disable\_dccp

7.5.1\_disable\_dccp [INFO] Checking Configuration

7.5.1\_disable\_dccp [INFO] Performing audit

7.5.1\_disable\_dccp [INFO] Not implemented yet

7.5.1\_disable\_dccp [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.5.2\_disable\_sctp.sh

7.5.2\_disable\_sctp [INFO] Working on 7.5.2\_disable\_sctp

7.5.2\_disable\_sctp [INFO] Checking Configuration

7.5.2\_disable\_sctp [INFO] Performing audit

7.5.2\_disable\_sctp [INFO] Not implemented yet

7.5.2\_disable\_sctp [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.5.3\_disable\_rds.sh

7.5.3\_disable\_rds [INFO] Working on 7.5.3\_disable\_rds

7.5.3\_disable\_rds [INFO] Checking Configuration

7.5.3\_disable\_rds [INFO] Performing audit

7.5.3\_disable\_rds [INFO] Not implemented yet

7.5.3\_disable\_rds [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.5.4\_disable\_tipc.sh

7.5.4\_disable\_tipc [INFO] Working on 7.5.4\_disable\_tipc

7.5.4\_disable\_tipc [INFO] Checking Configuration

7.5.4\_disable\_tipc [INFO] Performing audit

7.5.4\_disable\_tipc [INFO] Not implemented yet

7.5.4\_disable\_tipc [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.6\_disable\_wireless.sh

7.6\_disable\_wireless [INFO] Working on 7.6\_disable\_wireless

7.6\_disable\_wireless [INFO] Checking Configuration

7.6\_disable\_wireless [INFO] Performing audit

7.6\_disable\_wireless [INFO] The OS is not wireless device!

7.6\_disable\_wireless [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.1\_enable\_firewall.sh

7.7.1\_enable\_firewall [INFO] Working on 7.7.1\_enable\_firewall

7.7.1\_enable\_firewall [INFO] Checking Configuration

7.7.1\_enable\_firewall [INFO] Performing audit

7.7.1\_enable\_firewall [ OK ] iptables is installed

7.7.1\_enable\_firewall [ KO ] iptables-persistent is not installed!

7.7.1\_enable\_firewall [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.2\_ensure\_set\_firewall\_rules.sh

7.7.2\_ensure\_set\_firewall [INFO] Working on 7.7.2\_ensure\_set\_firewall\_rules

7.7.2\_ensure\_set\_firewall [INFO] Checking Configuration

7.7.2\_ensure\_set\_firewall [INFO] Performing audit

7.7.2\_ensure\_set\_firewall [ OK ] Ip4tables rules are set!

7.7.2\_ensure\_set\_firewall [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.3\_ensure\_firewall\_set\_protect\_dos\_attacks.sh

7.7.3\_ensure\_firewall\_set [INFO] Working on 7.7.3\_ensure\_firewall\_set\_protect\_dos\_attacks

7.7.3\_ensure\_firewall\_set [INFO] Checking Configuration

7.7.3\_ensure\_firewall\_set [INFO] Performing audit

7.7.3\_ensure\_firewall\_set [INFO] Iptables has set rules for protect DOS attacks!

7.7.3\_ensure\_firewall\_set [ OK ] Iptables has set rules for protect DOS attacks!

7.7.3\_ensure\_firewall\_set [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.4.1\_ensure\_default\_deny\_firewall\_policy.sh

7.7.4.1\_ensure\_default\_de [INFO] Working on 7.7.4.1\_ensure\_default\_deny\_firewall\_policy

7.7.4.1\_ensure\_default\_de [INFO] Checking Configuration

7.7.4.1\_ensure\_default\_de [INFO] Performing audit

7.7.4.1\_ensure\_default\_de [ KO ] Iptables: Firewall policy is not default deny!

7.7.4.1\_ensure\_default\_de [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.4.2\_ensure\_loopback\_traffic\_is\_configured.sh

7.7.4.2\_ensure\_loopback\_t [INFO] Working on 7.7.4.2\_ensure\_loopback\_traffic\_is\_configured

7.7.4.2\_ensure\_loopback\_t [INFO] Checking Configuration

7.7.4.2\_ensure\_loopback\_t [INFO] Performing audit

7.7.4.2\_ensure\_loopback\_t [INFO] Iptables: loopback traffic INPUT is not configured!

7.7.4.2\_ensure\_loopback\_t [INFO] Iptables: loopback traffic OUTPUT is not configured!

7.7.4.2\_ensure\_loopback\_t [INFO] Iptables: loopback traffic INPUT deny from other interfaces is not configured!

7.7.4.2\_ensure\_loopback\_t [ KO ] Loopback traffic rules are not configured!

7.7.4.2\_ensure\_loopback\_t [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.4.3\_ensure\_firewall\_rules\_exist\_for\_all\_open\_ports.sh

7.7.4.3\_ensure\_firewall\_r [INFO] Working on 7.7.4.3\_ensure\_firewall\_rules\_exist\_for\_all\_open\_ports

7.7.4.3\_ensure\_firewall\_r [INFO] Checking Configuration

7.7.4.3\_ensure\_firewall\_r [INFO] Performing audit

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 5987 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 5988 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 8005 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 5000 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 3310 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 47761 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 47762 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 7634 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 47763 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 47764 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 47765 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol tcp listening port 22 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol udp listening port 68 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol udp listening port 68 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol udp listening port 32930 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [INFO] Service: protocol udp listening port 9514 is not set firewall rules.

7.7.4.3\_ensure\_firewall\_r [ KO ] Iptables is not set firewall rules exist for all open ports!

7.7.4.3\_ensure\_firewall\_r [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.4.4\_ensure\_outbound\_and\_established\_connections\_are\_configured.sh

7.7.4.4\_ensure\_outbound\_a [INFO] Working on 7.7.4.4\_ensure\_outbound\_and\_established\_connections\_are\_configured

7.7.4.4\_ensure\_outbound\_a [INFO] Checking Configuration

7.7.4.4\_ensure\_outbound\_a [INFO] Performing audit

7.7.4.4\_ensure\_outbound\_a [INFO] Portocol tcp INPUT is not conf

7.7.4.4\_ensure\_outbound\_a [INFO] Portocol tcp outbound is not conf

7.7.4.4\_ensure\_outbound\_a [INFO] Portocol udp INPUT is not conf

7.7.4.4\_ensure\_outbound\_a [INFO] Portocol udp outbound is not conf

7.7.4.4\_ensure\_outbound\_a [INFO] Portocol icmp INPUT is not conf

7.7.4.4\_ensure\_outbound\_a [INFO] Portocol icmp outbound is not conf

7.7.4.4\_ensure\_outbound\_a [ KO ] Outbound and established connections are not configured!

7.7.4.4\_ensure\_outbound\_a [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.5.1\_ensure\_default\_deny\_firewall\_policy\_for\_v6.sh

7.7.5.1\_ensure\_default\_de [INFO] Working on 7.7.5.1\_ensure\_default\_deny\_firewall\_policy\_for\_v6

7.7.5.1\_ensure\_default\_de [INFO] Checking Configuration

7.7.5.1\_ensure\_default\_de [INFO] Performing audit

7.7.5.1\_ensure\_default\_de [ OK ] Ipv6 has set disabled, so pass.

7.7.5.1\_ensure\_default\_de [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.5.2\_ensure\_loopback\_traffic\_is\_configured\_for\_v6.sh

7.7.5.2\_ensure\_loopback\_t [INFO] Working on 7.7.5.2\_ensure\_loopback\_traffic\_is\_configured\_for\_v6

7.7.5.2\_ensure\_loopback\_t [INFO] Checking Configuration

7.7.5.2\_ensure\_loopback\_t [INFO] Performing audit

7.7.5.2\_ensure\_loopback\_t [ OK ] Ipv6 has set disabled, so pass.

7.7.5.2\_ensure\_loopback\_t [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.5.3\_ensure\_firewall\_rules\_exist\_for\_all\_open\_ports\_for\_v6.sh

7.7.5.3\_ensure\_firewall\_r [INFO] Working on 7.7.5.3\_ensure\_firewall\_rules\_exist\_for\_all\_open\_ports\_for\_v6

7.7.5.3\_ensure\_firewall\_r [INFO] Checking Configuration

7.7.5.3\_ensure\_firewall\_r [INFO] Performing audit

7.7.5.3\_ensure\_firewall\_r [ OK ] Ipv6 has set disabled, so pass.

7.7.5.3\_ensure\_firewall\_r [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/7.7.5.4\_ensure\_outbound\_and\_established\_connections\_are\_configured\_for\_v6.sh

7.7.5.4\_ensure\_outbound\_a [INFO] Working on 7.7.5.4\_ensure\_outbound\_and\_established\_connections\_are\_configured\_for\_v6

7.7.5.4\_ensure\_outbound\_a [INFO] Checking Configuration

7.7.5.4\_ensure\_outbound\_a [INFO] Performing audit

7.7.5.4\_ensure\_outbound\_a [ OK ] Ipv6 has set disabled, so pass.

7.7.5.4\_ensure\_outbound\_a [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.0\_enable\_auditd\_kernel.sh

8.0\_enable\_auditd\_kernel [INFO] Working on 8.0\_enable\_auditd\_kernel

8.0\_enable\_auditd\_kernel [INFO] Checking Configuration

8.0\_enable\_auditd\_kernel [INFO] Performing audit

8.0\_enable\_auditd\_kernel [ OK ] CONFIG\_AUDIT is enabled

8.0\_enable\_auditd\_kernel [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.1\_audit\_log\_storage.sh

8.1.1.1\_audit\_log\_storage [INFO] Working on 8.1.1.1\_audit\_log\_storage

8.1.1.1\_audit\_log\_storage [INFO] Checking Configuration

8.1.1.1\_audit\_log\_storage [INFO] Performing audit

8.1.1.1\_audit\_log\_storage [ OK ] /etc/audit/auditd.conf exists, checking configuration

8.1.1.1\_audit\_log\_storage [ OK ] max\_log\_file is present in /etc/audit/auditd.conf

8.1.1.1\_audit\_log\_storage [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.2\_halt\_when\_audit\_log\_full.sh

8.1.1.2\_halt\_when\_audit\_l [INFO] Working on 8.1.1.2\_halt\_when\_audit\_log\_full

8.1.1.2\_halt\_when\_audit\_l [INFO] Checking Configuration

8.1.1.2\_halt\_when\_audit\_l [INFO] Performing audit

8.1.1.2\_halt\_when\_audit\_l [ OK ] /etc/audit/auditd.conf exists, checking configuration

8.1.1.2\_halt\_when\_audit\_l [ KO ] ^space\_left\_action[[:space:]]\*=[[:space:]]\*email is not present in /etc/audit/auditd.conf

8.1.1.2\_halt\_when\_audit\_l [ OK ] ^action\_mail\_acct[[:space:]]\*=[[:space:]]\*root is present in /etc/audit/auditd.conf

8.1.1.2\_halt\_when\_audit\_l [ KO ] ^admin\_space\_left\_action[[:space:]]\*=[[:space:]]\*halt is not present in /etc/audit/auditd.conf

8.1.1.2\_halt\_when\_audit\_l [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.3\_keep\_all\_audit\_logs.sh

8.1.1.3\_keep\_all\_audit\_lo [INFO] Working on 8.1.1.3\_keep\_all\_audit\_logs

8.1.1.3\_keep\_all\_audit\_lo [INFO] Checking Configuration

8.1.1.3\_keep\_all\_audit\_lo [INFO] Performing audit

8.1.1.3\_keep\_all\_audit\_lo [ OK ] /etc/audit/auditd.conf exists, checking configuration

8.1.1.3\_keep\_all\_audit\_lo [ KO ] ^max\_log\_file\_action[[:space:]]\*=[[:space:]]\*keep\_logs is not present in /etc/audit/auditd.conf

8.1.1.3\_keep\_all\_audit\_lo [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.4\_set\_failure\_mode.sh

8.1.1.4\_set\_failure\_mode [INFO] Working on 8.1.1.4\_set\_failure\_mode

8.1.1.4\_set\_failure\_mode [INFO] Checking Configuration

8.1.1.4\_set\_failure\_mode [INFO] Performing audit

8.1.1.4\_set\_failure\_mode [ OK ] /etc/audit/rules.d/audit.rules exists, checking configuration

8.1.1.4\_set\_failure\_mode [ OK ] failure value is ok in /etc/audit/rules.d/audit.rules

8.1.1.4\_set\_failure\_mode [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.5\_ensure\_set\_remote\_server.sh

8.1.1.5\_ensure\_set\_remote [INFO] Working on 8.1.1.5\_ensure\_set\_remote\_server

8.1.1.5\_ensure\_set\_remote [INFO] Checking Configuration

8.1.1.5\_ensure\_set\_remote [INFO] Performing audit

8.1.1.5\_ensure\_set\_remote [ OK ] /etc/audisp/audisp-remote.conf exists, checking configuration

8.1.1.5\_ensure\_set\_remote [ KO ] remote\_server value not set in /etc/audisp/audisp-remote.conf

8.1.1.5\_ensure\_set\_remote [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.6\_ensure\_set\_encrypt\_for\_audit\_remote.sh

8.1.1.6\_ensure\_set\_encryp [INFO] Working on 8.1.1.6\_ensure\_set\_encrypt\_for\_audit\_remote

8.1.1.6\_ensure\_set\_encryp [INFO] Checking Configuration

8.1.1.6\_ensure\_set\_encryp [INFO] Performing audit

8.1.1.6\_ensure\_set\_encryp [ OK ] /etc/audisp/audisp-remote.conf exists, checking configuration

8.1.1.6\_ensure\_set\_encryp [ KO ] enable\_krb5 is not exist on /etc/audisp/audisp-remote.conf

8.1.1.6\_ensure\_set\_encryp [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.7\_ensure\_set\_action\_for\_audit\_storage\_full.sh

8.1.1.7\_ensure\_set\_action [INFO] Working on 8.1.1.7\_ensure\_set\_action\_for\_audit\_storage\_full

8.1.1.7\_ensure\_set\_action [INFO] Checking Configuration

8.1.1.7\_ensure\_set\_action [INFO] Performing audit

8.1.1.7\_ensure\_set\_action [ OK ] /etc/audisp/audisp-remote.conf exists, checking configuration

8.1.1.7\_ensure\_set\_action [ KO ] disk\_full\_action value is incorrect in /etc/audisp/audisp-remote.conf

8.1.1.7\_ensure\_set\_action [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.8\_ensure\_set\_action\_for\_net\_fail.sh

8.1.1.8\_ensure\_set\_action [INFO] Working on 8.1.1.8\_ensure\_set\_action\_for\_net\_fail

8.1.1.8\_ensure\_set\_action [INFO] Checking Configuration

8.1.1.8\_ensure\_set\_action [INFO] Performing audit

8.1.1.8\_ensure\_set\_action [ OK ] /etc/audisp/audisp-remote.conf exists, checking configuration

8.1.1.8\_ensure\_set\_action [ OK ] network\_failure\_action value is ok in /etc/audisp/audisp-remote.conf

8.1.1.8\_ensure\_set\_action [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.1.9\_set\_space\_left\_audit.sh

8.1.1.9\_set\_space\_left\_au [INFO] Working on 8.1.1.9\_set\_space\_left\_audit

8.1.1.9\_set\_space\_left\_au [INFO] Checking Configuration

8.1.1.9\_set\_space\_left\_au [INFO] Performing audit

8.1.1.9\_set\_space\_left\_au [ OK ] /etc/audit/auditd.conf exists, checking configuration

8.1.1.9\_set\_space\_left\_au [ KO ] Space left value: 75 is more than audit log filesystem 25%

8.1.1.9\_set\_space\_left\_au [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.2\_enable\_auditd.sh

8.1.2\_enable\_auditd [INFO] Working on 8.1.2\_enable\_auditd

8.1.2\_enable\_auditd [INFO] Checking Configuration

8.1.2\_enable\_auditd [INFO] Performing audit

8.1.2\_enable\_auditd [ OK ] auditd is installed

8.1.2\_enable\_auditd [ OK ] auditd is enabled

8.1.2\_enable\_auditd [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.3\_audit\_bootloader.sh

8.1.3\_audit\_bootloader [INFO] Working on 8.1.3\_audit\_bootloader

8.1.3\_audit\_bootloader [INFO] Checking Configuration

8.1.3\_audit\_bootloader [INFO] Performing audit

8.1.3\_audit\_bootloader [ OK ] /etc/default/grub exists, checking configuration

8.1.3\_audit\_bootloader [ OK ] audit is present in /etc/default/grub

8.1.3\_audit\_bootloader [ OK ] audit's set is correctly.

8.1.3\_audit\_bootloader [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.4\_record\_date\_time\_edit.sh

8.1.4\_record\_date\_time\_ed [INFO] Working on 8.1.4\_record\_date\_time\_edit

8.1.4\_record\_date\_time\_ed [INFO] Checking Configuration

8.1.4\_record\_date\_time\_ed [INFO] Performing audit

8.1.4\_record\_date\_time\_ed [ OK ] -a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change is present in /etc/audit/rules.d/audit.rules

8.1.4\_record\_date\_time\_ed [ KO ] -a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change is not in file /etc/audit/rules.d/audit.rules

8.1.4\_record\_date\_time\_ed [ OK ] -a always,exit -F arch=b64 -S clock\_settime -k time-change is present in /etc/audit/rules.d/audit.rules

8.1.4\_record\_date\_time\_ed [ KO ] -a always,exit -F arch=b32 -S clock\_settime -k time-change is not in file /etc/audit/rules.d/audit.rules

8.1.4\_record\_date\_time\_ed [ OK ] -w /etc/localtime -p wa -k time-change is present in /etc/audit/rules.d/audit.rules

8.1.4\_record\_date\_time\_ed [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.5\_record\_user\_group\_edit.sh

8.1.5\_record\_user\_group\_e [INFO] Working on 8.1.5\_record\_user\_group\_edit

8.1.5\_record\_user\_group\_e [INFO] Checking Configuration

8.1.5\_record\_user\_group\_e [INFO] Performing audit

8.1.5\_record\_user\_group\_e [ OK ] -w /etc/group -p wa -k identity is present in /etc/audit/rules.d/audit.rules

8.1.5\_record\_user\_group\_e [ OK ] -w /etc/passwd -p wa -k identity is present in /etc/audit/rules.d/audit.rules

8.1.5\_record\_user\_group\_e [ OK ] -w /etc/gshadow -p wa -k identity is present in /etc/audit/rules.d/audit.rules

8.1.5\_record\_user\_group\_e [ OK ] -w /etc/shadow -p wa -k identity is present in /etc/audit/rules.d/audit.rules

8.1.5\_record\_user\_group\_e [ OK ] -w /etc/security/opasswd -p wa -k identity is present in /etc/audit/rules.d/audit.rules

8.1.5\_record\_user\_group\_e [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.6\_record\_network\_edit.sh

8.1.6\_record\_network\_edit [INFO] Working on 8.1.6\_record\_network\_edit

8.1.6\_record\_network\_edit [INFO] Checking Configuration

8.1.6\_record\_network\_edit [INFO] Performing audit

8.1.6\_record\_network\_edit [ OK ] -a exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale is present in /etc/audit/rules.d/audit.rules

8.1.6\_record\_network\_edit [ KO ] -a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale is not in file /etc/audit/rules.d/audit.rules

8.1.6\_record\_network\_edit [ OK ] -w /etc/issue -p wa -k system-locale is present in /etc/audit/rules.d/audit.rules

8.1.6\_record\_network\_edit [ OK ] -w /etc/issue.net -p wa -k system-locale is present in /etc/audit/rules.d/audit.rules

8.1.6\_record\_network\_edit [ OK ] -w /etc/hosts -p wa -k system-locale is present in /etc/audit/rules.d/audit.rules

8.1.6\_record\_network\_edit [ OK ] -w /etc/network -p wa -k system-locale is present in /etc/audit/rules.d/audit.rules

8.1.6\_record\_network\_edit [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.7\_record\_mac\_edit.sh

8.1.7\_record\_mac\_edit [INFO] Working on 8.1.7\_record\_mac\_edit

8.1.7\_record\_mac\_edit [INFO] Checking Configuration

8.1.7\_record\_mac\_edit [INFO] Performing audit

8.1.7\_record\_mac\_edit [INFO] Apparmor has installed!

8.1.7\_record\_mac\_edit [ OK ] -w /etc/apparmor/ -p wa -k MAC-policy is present in /etc/audit/rules.d/audit.rules

8.1.7\_record\_mac\_edit [ OK ] -w /etc/apparmor.d/ -p wa -k MAC-policy is present in /etc/audit/rules.d/audit.rules

8.1.7\_record\_mac\_edit [ OK ] -a always,exit -F path=/sbin/apparmor\_parser -F perm=x -F auid>=1000 -F auid!=4294967295 -k MAC-policy is present in /etc/audit/rules.d/audit.rules

8.1.7\_record\_mac\_edit [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.8\_record\_login\_logout.sh

8.1.8\_record\_login\_logout [INFO] Working on 8.1.8\_record\_login\_logout

8.1.8\_record\_login\_logout [INFO] Checking Configuration

8.1.8\_record\_login\_logout [INFO] Performing audit

8.1.8\_record\_login\_logout [ OK ] -w /var/log/faillog -p wa -k logins is present in /etc/audit/rules.d/audit.rules

8.1.8\_record\_login\_logout [ OK ] -w /var/log/lastlog -p wa -k logins is present in /etc/audit/rules.d/audit.rules

8.1.8\_record\_login\_logout [ OK ] -w /var/log/tallylog -p wa -k logins is present in /etc/audit/rules.d/audit.rules

8.1.8\_record\_login\_logout [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.9\_record\_session\_init.sh

8.1.9\_record\_session\_init [INFO] Working on 8.1.9\_record\_session\_init

8.1.9\_record\_session\_init [INFO] Checking Configuration

8.1.9\_record\_session\_init [INFO] Performing audit

8.1.9\_record\_session\_init [ OK ] -w /var/run/utmp -p wa -k session is present in /etc/audit/rules.d/audit.rules

8.1.9\_record\_session\_init [ OK ] -w /var/log/wtmp -p wa -k session is present in /etc/audit/rules.d/audit.rules

8.1.9\_record\_session\_init [ OK ] -w /var/log/btmp -p wa -k session is present in /etc/audit/rules.d/audit.rules

8.1.9\_record\_session\_init [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.10\_record\_dac\_edit.sh

8.1.10\_record\_dac\_edit [INFO] Working on 8.1.10\_record\_dac\_edit

8.1.10\_record\_dac\_edit [INFO] Checking Configuration

8.1.10\_record\_dac\_edit [INFO] Performing audit

8.1.10\_record\_dac\_edit [ OK ] -a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod is present in /etc/audit/rules.d/audit.rules

8.1.10\_record\_dac\_edit [ KO ] -a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod is not in file /etc/audit/rules.d/audit.rules

8.1.10\_record\_dac\_edit [ OK ] -a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod is present in /etc/audit/rules.d/audit.rules

8.1.10\_record\_dac\_edit [ KO ] -a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod is not in file /etc/audit/rules.d/audit.rules

8.1.10\_record\_dac\_edit [ OK ] -a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod is present in /etc/audit/rules.d/audit.rules

8.1.10\_record\_dac\_edit [ KO ] -a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod is not in file /etc/audit/rules.d/audit.rules

8.1.10\_record\_dac\_edit [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.11\_record\_failed\_access\_file.sh

8.1.11\_record\_failed\_acce [INFO] Working on 8.1.11\_record\_failed\_access\_file

8.1.11\_record\_failed\_acce [INFO] Checking Configuration

8.1.11\_record\_failed\_acce [INFO] Performing audit

8.1.11\_record\_failed\_acce [ OK ] -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access is present in /etc/audit/rules.d/audit.rules

8.1.11\_record\_failed\_acce [ KO ] -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access is not in file /etc/audit/rules.d/audit.rules

8.1.11\_record\_failed\_acce [ OK ] -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access is present in /etc/audit/rules.d/audit.rules

8.1.11\_record\_failed\_acce [ KO ] -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access is not in file /etc/audit/rules.d/audit.rules

8.1.11\_record\_failed\_acce [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.12\_record\_privileged\_commands.sh

8.1.12\_record\_privileged\_ [INFO] Working on 8.1.12\_record\_privileged\_commands

8.1.12\_record\_privileged\_ [INFO] Checking Configuration

8.1.12\_record\_privileged\_ [INFO] Performing audit

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/pmount -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/bsd-write -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/wall -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/expiry -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/pkexec -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/pumount -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/ntfs-3g -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/dotlock.mailutils -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/bin/fusermount -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/lib/openssh/ssh-keysign -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/lib/xorg/Xorg.wrap -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/lib/policykit-1/polkit-agent-helper-1 -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/lib/eject/dmcrypt-get-device -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/lib/dbus-1.0/dbus-daemon-launch-helper -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/lib/chromium/chrome-sandbox -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/lib/x86\_64-linux-gnu/utempter/utempter -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/sbin/mount.cifs -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/sbin/unix\_chkpwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/sbin/exim4 -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] -a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged is present in /etc/audit/rules.d/audit.rules

8.1.12\_record\_privileged\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.13\_record\_successful\_mount.sh

8.1.13\_record\_successful\_ [INFO] Working on 8.1.13\_record\_successful\_mount

8.1.13\_record\_successful\_ [INFO] Checking Configuration

8.1.13\_record\_successful\_ [INFO] Performing audit

8.1.13\_record\_successful\_ [ OK ] -a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts is present in /etc/audit/rules.d/audit.rules

8.1.13\_record\_successful\_ [ KO ] -a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts is not in file /etc/audit/rules.d/audit.rules

8.1.13\_record\_successful\_ [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.14\_record\_file\_deletions.sh

8.1.14\_record\_file\_deleti [INFO] Working on 8.1.14\_record\_file\_deletions

8.1.14\_record\_file\_deleti [INFO] Checking Configuration

8.1.14\_record\_file\_deleti [INFO] Performing audit

8.1.14\_record\_file\_deleti [ OK ] -a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -S rmdir -F auid>=1000 -F auid!=4294967295 -k delete is present in /etc/audit/rules.d/audit.rules

8.1.14\_record\_file\_deleti [ KO ] -a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -S rmdir -F auid>=1000 -F auid!=4294967295 -k delete is not in file /etc/audit/rules.d/audit.rules

8.1.14\_record\_file\_deleti [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.15\_record\_sudoers\_edit.sh

8.1.15\_record\_sudoers\_edi [INFO] Working on 8.1.15\_record\_sudoers\_edit

8.1.15\_record\_sudoers\_edi [INFO] Checking Configuration

8.1.15\_record\_sudoers\_edi [INFO] Performing audit

8.1.15\_record\_sudoers\_edi [ OK ] -w /etc/sudoers -p wa -k sudoers is present in /etc/audit/rules.d/audit.rules

8.1.15\_record\_sudoers\_edi [ OK ] -w /etc/sudoers.d/ -p wa -k sudoers is present in /etc/audit/rules.d/audit.rules

8.1.15\_record\_sudoers\_edi [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.16\_record\_sudo\_usage.sh

8.1.16\_record\_sudo\_usage [INFO] Working on 8.1.16\_record\_sudo\_usage

8.1.16\_record\_sudo\_usage [INFO] Checking Configuration

8.1.16\_record\_sudo\_usage [INFO] Performing audit

8.1.16\_record\_sudo\_usage [ OK ] -w /var/log/sudo.log -p wa -k sudoaction is present in /etc/audit/rules.d/audit.rules

8.1.16\_record\_sudo\_usage [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.17\_record\_kernel\_modules.sh

8.1.17\_record\_kernel\_modu [INFO] Working on 8.1.17\_record\_kernel\_modules

8.1.17\_record\_kernel\_modu [INFO] Checking Configuration

8.1.17\_record\_kernel\_modu [INFO] Performing audit

8.1.17\_record\_kernel\_modu [ OK ] -w /sbin/insmod -p x -k modules is present in /etc/audit/rules.d/audit.rules

8.1.17\_record\_kernel\_modu [ OK ] -w /sbin/rmmod -p x -k modules is present in /etc/audit/rules.d/audit.rules

8.1.17\_record\_kernel\_modu [ OK ] -w /sbin/modprobe -p x -k modules is present in /etc/audit/rules.d/audit.rules

8.1.17\_record\_kernel\_modu [ OK ] -w /bin/kmod -p x -k modules is present in /etc/audit/rules.d/audit.rules

8.1.17\_record\_kernel\_modu [ KO ] -a always,exit -F arch=b32 -S init\_module -S delete\_module -S create\_module -S finit\_module -k modules is not in file /etc/audit/rules.d/audit.rules

8.1.17\_record\_kernel\_modu [ OK ] -a always,exit -F arch=b64 -S init\_module -S delete\_module -S create\_module -S finit\_module -k modules is present in /etc/audit/rules.d/audit.rules

8.1.17\_record\_kernel\_modu [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.18\_record\_Events\_netfilter.sh

8.1.18\_record\_Events\_netf [INFO] Working on 8.1.18\_record\_Events\_netfilter

8.1.18\_record\_Events\_netf [INFO] Checking Configuration

8.1.18\_record\_Events\_netf [INFO] Performing audit

8.1.18\_record\_Events\_netf [ OK ] -w /etc/nftables.conf -p wa -k nft\_config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.18\_record\_Events\_netf [ KO ] -w /usr/share/netfilter-persistent/plugins.d/ -p wa -k nft\_config\_file\_change is not in file /etc/audit/rules.d/audit.rules

8.1.18\_record\_Events\_netf [ OK ] -a always,exit -F path=/usr/sbin/netfilter-persistent -F perm=x -F auid>=1000 -F auid!=4294967295 -k nft\_persistent\_use is present in /etc/audit/rules.d/audit.rules

8.1.18\_record\_Events\_netf [ OK ] -a always,exit -F path=/usr/sbin/nft -F perm=x -F auid>=1000 -F auid!=4294967295 -k nft\_cmd\_use is present in /etc/audit/rules.d/audit.rules

8.1.18\_record\_Events\_netf [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.19\_record\_sshkeysign\_usage.sh

8.1.19\_record\_sshkeysign\_ [INFO] Working on 8.1.19\_record\_sshkeysign\_usage

8.1.19\_record\_sshkeysign\_ [INFO] Checking Configuration

8.1.19\_record\_sshkeysign\_ [INFO] Performing audit

8.1.19\_record\_sshkeysign\_ [ OK ] -a always,exit -F path=/usr/lib/openssh/ssh-keysign -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-ssh is present in /etc/audit/rules.d/audit.rules

8.1.19\_record\_sshkeysign\_ [ OK ] -a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-ssh is present in /etc/audit/rules.d/audit.rules

8.1.19\_record\_sshkeysign\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.20\_record\_open\_by\_handle\_at\_syscall.sh

8.1.20\_record\_open\_by\_han [INFO] Working on 8.1.20\_record\_open\_by\_handle\_at\_syscall

8.1.20\_record\_open\_by\_han [INFO] Checking Configuration

8.1.20\_record\_open\_by\_han [INFO] Performing audit

8.1.20\_record\_open\_by\_han [ OK ] -a always,exit -F arch=b64 -S open\_by\_handle\_at -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access is present in /etc/audit/rules.d/audit.rules

8.1.20\_record\_open\_by\_han [ OK ] -a always,exit -F arch=b64 -S open\_by\_handle\_at -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access is present in /etc/audit/rules.d/audit.rules

8.1.20\_record\_open\_by\_han [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.21\_record\_Events\_that\_privileged\_passwd\_cmd\_usage.sh

8.1.21\_record\_Events\_that [INFO] Working on 8.1.21\_record\_Events\_that\_privileged\_passwd\_cmd\_usage

8.1.21\_record\_Events\_that [INFO] Checking Configuration

8.1.21\_record\_Events\_that [INFO] Performing audit

8.1.21\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd is present in /etc/audit/rules.d/audit.rules

8.1.21\_record\_Events\_that [ OK ] -a always,exit -F path=/sbin/unix\_chkpwd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd is present in /etc/audit/rules.d/audit.rules

8.1.21\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd is present in /etc/audit/rules.d/audit.rules

8.1.21\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-passwd is present in /etc/audit/rules.d/audit.rules

8.1.21\_record\_Events\_that [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.22\_record\_Events\_that\_privileged\_priv\_change\_cmd\_usage.sh

8.1.22\_record\_Events\_that [INFO] Working on 8.1.22\_record\_Events\_that\_privileged\_priv\_change\_cmd\_usage

8.1.22\_record\_Events\_that [INFO] Checking Configuration

8.1.22\_record\_Events\_that [INFO] Performing audit

8.1.22\_record\_Events\_that [ OK ] -a always,exit -F path=/bin/su -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv\_change is present in /etc/audit/rules.d/audit.rules

8.1.22\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv\_change is present in /etc/audit/rules.d/audit.rules

8.1.22\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv\_change is present in /etc/audit/rules.d/audit.rules

8.1.22\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv\_change is present in /etc/audit/rules.d/audit.rules

8.1.22\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-priv\_change is present in /etc/audit/rules.d/audit.rules

8.1.22\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=500 -F auid!=4294967295 -k privileged-priv\_change is present in /etc/audit/rules.d/audit.rules

8.1.22\_record\_Events\_that [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.23\_record\_Events\_that\_privileged\_postfix\_cmd\_usage.sh

8.1.23\_record\_Events\_that [INFO] Working on 8.1.23\_record\_Events\_that\_privileged\_postfix\_cmd\_usage

8.1.23\_record\_Events\_that [INFO] Checking Configuration

8.1.23\_record\_Events\_that [INFO] Performing audit

8.1.23\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-postfix is present in /etc/audit/rules.d/audit.rules

8.1.23\_record\_Events\_that [ OK ] -a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-postfix is present in /etc/audit/rules.d/audit.rules

8.1.23\_record\_Events\_that [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.24\_record\_crontab\_cmd\_usage.sh

8.1.24\_record\_crontab\_cmd [INFO] Working on 8.1.24\_record\_crontab\_cmd\_usage

8.1.24\_record\_crontab\_cmd [INFO] Checking Configuration

8.1.24\_record\_crontab\_cmd [INFO] Performing audit

8.1.24\_record\_crontab\_cmd [ OK ] -a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-cron is present in /etc/audit/rules.d/audit.rules

8.1.24\_record\_crontab\_cmd [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.25\_record\_pam\_timestamp\_check\_cmd\_usage.sh

8.1.25\_record\_pam\_timesta [INFO] Working on 8.1.25\_record\_pam\_timestamp\_check\_cmd\_usage

8.1.25\_record\_pam\_timesta [INFO] Checking Configuration

8.1.25\_record\_pam\_timesta [INFO] Performing audit

8.1.25\_record\_pam\_timesta [ OK ] -a always,exit -F path=/usr/sbin/pam\_timestamp\_check -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-pam is present in /etc/audit/rules.d/audit.rules

8.1.25\_record\_pam\_timesta [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.26\_record\_pam\_tally\_cmd\_usage.sh

8.1.26\_record\_pam\_tally\_c [INFO] Working on 8.1.26\_record\_pam\_tally\_cmd\_usage

8.1.26\_record\_pam\_tally\_c [INFO] Checking Configuration

8.1.26\_record\_pam\_tally\_c [INFO] Performing audit

8.1.26\_record\_pam\_tally\_c [ OK ] -a always,exit -F path=/sbin/pam\_tally -F perm=wxa -F auid>=1000 -F auid!=4294967295 -k privileged-pam is present in /etc/audit/rules.d/audit.rules

8.1.26\_record\_pam\_tally\_c [ OK ] -a always,exit -F path=/sbin/pam\_tally2 -F perm=wxa -F auid>=1000 -F auid!=4294967295 -k privileged-pam is present in /etc/audit/rules.d/audit.rules

8.1.26\_record\_pam\_tally\_c [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.27\_record\_Events\_that\_modify\_conf\_files.sh

8.1.27\_record\_Events\_that [INFO] Working on 8.1.27\_record\_Events\_that\_modify\_conf\_files

8.1.27\_record\_Events\_that [INFO] Checking Configuration

8.1.27\_record\_Events\_that [INFO] Performing audit

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/audisp/audisp-remote.conf -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/audit/auditd.conf -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/default/grub -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/fstab -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/hosts.deny -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/login.defs -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F dir=/etc/audit/rules.d/ -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F dir=/etc/pam.d/ -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/profile -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F dir=/etc/profile.d/ -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F dir=/etc/security/ -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ KO ] -a always,exit -F dir=/etc/iptables/ -F perm=wa -k config\_file\_change is not in file /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ OK ] -a always,exit -F path=/etc/sysctl.conf -F perm=wa -k config\_file\_change is present in /etc/audit/rules.d/audit.rules

8.1.27\_record\_Events\_that [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.28\_record\_acl\_cmd\_usage.sh

8.1.28\_record\_acl\_cmd\_usa [INFO] Working on 8.1.28\_record\_acl\_cmd\_usage

8.1.28\_record\_acl\_cmd\_usa [INFO] Checking Configuration

8.1.28\_record\_acl\_cmd\_usa [INFO] Performing audit

8.1.28\_record\_acl\_cmd\_usa [ OK ] -a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F auid!=4294967295 -k perm\_chng is present in /etc/audit/rules.d/audit.rules

8.1.28\_record\_acl\_cmd\_usa [ OK ] -a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=4294967295 -k perm\_chng is present in /etc/audit/rules.d/audit.rules

8.1.28\_record\_acl\_cmd\_usa [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.29\_record\_usermod\_cmd\_usage.sh

8.1.29\_record\_usermod\_cmd [INFO] Working on 8.1.29\_record\_usermod\_cmd\_usage

8.1.29\_record\_usermod\_cmd [INFO] Checking Configuration

8.1.29\_record\_usermod\_cmd [INFO] Performing audit

8.1.29\_record\_usermod\_cmd [ OK ] -a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-usermod is present in /etc/audit/rules.d/audit.rules

8.1.29\_record\_usermod\_cmd [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.30\_record\_unix\_update\_cmd\_usage.sh

8.1.30\_record\_unix\_update [INFO] Working on 8.1.30\_record\_unix\_update\_cmd\_usage

8.1.30\_record\_unix\_update [INFO] Checking Configuration

8.1.30\_record\_unix\_update [INFO] Performing audit

8.1.30\_record\_unix\_update [ OK ] -a always,exit -F path=/sbin/unix\_update -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-unix-update is present in /etc/audit/rules.d/audit.rules

8.1.30\_record\_unix\_update [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.31\_record\_syscall\_execve.sh

8.1.31\_record\_syscall\_exe [INFO] Working on 8.1.31\_record\_syscall\_execve

8.1.31\_record\_syscall\_exe [INFO] Checking Configuration

8.1.31\_record\_syscall\_exe [INFO] Performing audit

8.1.31\_record\_syscall\_exe [ OK ] -a always,exit -F arch=b64 -S execve -C uid!=euid -F key=execpriv is present in /etc/audit/rules.d/audit.rules

8.1.31\_record\_syscall\_exe [ OK ] -a always,exit -F arch=b64 -S execve -C gid!=egid -F key=execpriv is present in /etc/audit/rules.d/audit.rules

8.1.31\_record\_syscall\_exe [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.1.32\_freeze\_auditd\_conf.sh

8.1.32\_freeze\_auditd\_conf [INFO] Working on 8.1.32\_freeze\_auditd\_conf

8.1.32\_freeze\_auditd\_conf [INFO] Checking Configuration

8.1.32\_freeze\_auditd\_conf [INFO] Performing audit

8.1.32\_freeze\_auditd\_conf [ OK ] -e 2 is present in /etc/audit/rules.d/audit.rules

8.1.32\_freeze\_auditd\_conf [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.2.1\_install\_rsyslog.sh

8.2.1\_install\_rsyslog [INFO] Working on 8.2.1\_install\_rsyslog

8.2.1\_install\_rsyslog [INFO] Checking Configuration

8.2.1\_install\_rsyslog [INFO] Performing audit

8.2.1\_install\_rsyslog [ OK ] rsyslog is installed.

8.2.1\_install\_rsyslog [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.2.2\_enable\_rsyslog.sh

8.2.2\_enable\_rsyslog [INFO] Working on 8.2.2\_enable\_rsyslog

8.2.2\_enable\_rsyslog [INFO] Checking Configuration

8.2.2\_enable\_rsyslog [INFO] Performing audit

8.2.2\_enable\_rsyslog [INFO] Checking if rsyslog is enabled

8.2.2\_enable\_rsyslog [ OK ] rsyslog is enabled

8.2.2\_enable\_rsyslog [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.2.3\_configure\_rsyslog.sh

8.2.3\_configure\_rsyslog [INFO] Working on 8.2.3\_configure\_rsyslog

8.2.3\_configure\_rsyslog [INFO] Checking Configuration

8.2.3\_configure\_rsyslog [INFO] Performing audit

8.2.3\_configure\_rsyslog [INFO] Ensure default and local facilities are preserved on the system

8.2.3\_configure\_rsyslog [INFO] No measure here, please review the file by yourself

8.2.3\_configure\_rsyslog [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.2.4\_set\_logfile\_perm\_cfg\_rsyslog.sh

8.2.4\_set\_logfile\_perm\_cf [INFO] Working on 8.2.4\_set\_logfile\_perm\_cfg\_rsyslog

8.2.4\_set\_logfile\_perm\_cf [INFO] Checking Configuration

8.2.4\_set\_logfile\_perm\_cf [INFO] Performing audit

8.2.4\_set\_logfile\_perm\_cf [ OK ] File owner set is root!

8.2.4\_set\_logfile\_perm\_cf [ OK ] File group set is adm!

8.2.4\_set\_logfile\_perm\_cf [ OK ] File permissions set is 640!

8.2.4\_set\_logfile\_perm\_cf [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.2.5\_rsyslog\_remote\_host.sh

8.2.5\_rsyslog\_remote\_host [INFO] Working on 8.2.5\_rsyslog\_remote\_host

8.2.5\_rsyslog\_remote\_host [INFO] Checking Configuration

8.2.5\_rsyslog\_remote\_host [INFO] Performing audit

8.2.5\_rsyslog\_remote\_host [ KO ] ^\*.\*[^I][^I]\*@ is not present in /etc/rsyslog.conf /etc/rsyslog.d/\*.conf

8.2.5\_rsyslog\_remote\_host [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.3.1\_install\_syslog-ng.sh

8.3.1\_install\_syslog-ng [INFO] Working on 8.3.1\_install\_syslog-ng

8.3.1\_install\_syslog-ng [INFO] Checking Configuration

8.3.1\_install\_syslog-ng [INFO] Performing audit

8.3.1\_install\_syslog-ng [ OK ] rsyslog has installed, so pass.

8.3.1\_install\_syslog-ng [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.3.2\_enable\_syslog-ng.sh

8.3.2\_enable\_syslog-ng [INFO] Working on 8.3.2\_enable\_syslog-ng

8.3.2\_enable\_syslog-ng [INFO] Checking Configuration

8.3.2\_enable\_syslog-ng [INFO] Performing audit

8.3.2\_enable\_syslog-ng [ OK ] rsyslog has installed, so pass.

8.3.2\_enable\_syslog-ng [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.3.3\_configure\_syslog-ng.sh

8.3.3\_configure\_syslog-ng [INFO] Working on 8.3.3\_configure\_syslog-ng

8.3.3\_configure\_syslog-ng [INFO] Checking Configuration

8.3.3\_configure\_syslog-ng [INFO] Performing audit

8.3.3\_configure\_syslog-ng [ OK ] rsyslog has installed, so pass.

8.3.3\_configure\_syslog-ng [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.3.4\_set\_logfile\_perm.sh

8.3.4\_set\_logfile\_perm [INFO] Working on 8.3.4\_set\_logfile\_perm

8.3.4\_set\_logfile\_perm [INFO] Checking Configuration

8.3.4\_set\_logfile\_perm [INFO] Performing audit

8.3.4\_set\_logfile\_perm [ OK ] rsyslog has installed, so pass.

8.3.4\_set\_logfile\_perm [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.3.5\_syslog-ng\_remote\_host.sh

8.3.5\_syslog-ng\_remote\_ho [INFO] Working on 8.3.5\_syslog-ng\_remote\_host

8.3.5\_syslog-ng\_remote\_ho [INFO] Checking Configuration

8.3.5\_syslog-ng\_remote\_ho [INFO] Performing audit

8.3.5\_syslog-ng\_remote\_ho [ OK ] rsyslog has installed, so pass.

8.3.5\_syslog-ng\_remote\_ho [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.3.6\_remote\_syslog-ng\_acl.sh

8.3.6\_remote\_syslog-ng\_ac [INFO] Working on 8.3.6\_remote\_syslog-ng\_acl

8.3.6\_remote\_syslog-ng\_ac [INFO] Checking Configuration

8.3.6\_remote\_syslog-ng\_ac [INFO] Performing audit

8.3.6\_remote\_syslog-ng\_ac [ OK ] rsyslog has installed, so pass.

8.3.6\_remote\_syslog-ng\_ac [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.4.1\_install\_aide.sh

8.4.1\_install\_aide [INFO] Working on 8.4.1\_install\_aide

8.4.1\_install\_aide [INFO] Checking Configuration

8.4.1\_install\_aide [INFO] Performing audit

8.4.1\_install\_aide [ KO ] aide is not installed!

8.4.1\_install\_aide [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.4.2\_aide\_cron.sh

8.4.2\_aide\_cron [INFO] Working on 8.4.2\_aide\_cron

8.4.2\_aide\_cron [INFO] Checking Configuration

8.4.2\_aide\_cron [INFO] Performing audit

8.4.2\_aide\_cron [ KO ] /etc/cron.daily/aide is not exist.

8.4.2\_aide\_cron [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.5\_ensure\_permissions\_on\_all\_logfiles.sh

8.5\_ensure\_permissions\_on [INFO] Working on 8.5\_ensure\_permissions\_on\_all\_logfiles

8.5\_ensure\_permissions\_on [INFO] Checking Configuration

8.5\_ensure\_permissions\_on [INFO] Performing audit

8.5\_ensure\_permissions\_on [ KO ] Permissions of all log files are not correctly configured!

19 4 -rw-r--r-- 1 root root 4008 Oct 23 18:13 /var/log/fontconfig.log

17 180 -rw-r--r-- 1 root root 182332 Oct 28 14:23 /var/log/dpkg.log

130053 16 -rw-r--r-- 1 root root 16298 Oct 28 14:23 /var/log/apt/history.log

13 0 -rw-r--r-- 1 root root 0 Oct 23 17:51 /var/log/bootstrap.log

31 4 -rw-r--r-- 1 root root 288 Oct 28 14:27 /var/log/macchanger.log

20 4 -rw-rw-r-- 1 root utmp 292292 Oct 28 16:29 /var/log/lastlog

21 8 -rw-rw-r-- 1 root utmp 6144 Oct 28 16:30 /var/log/wtmp

41 24 -rw-r--r-- 1 root root 22933 Oct 28 17:00 /var/log/Xorg.0.log

27 4 -rw-r--r-- 1 root root 160 Oct 28 14:23 /var/log/installer/lsb-release

25 32 -rw-r--r-- 1 root root 30952 Oct 28 14:23 /var/log/installer/hardware-summary

26 60 -rw-r--r-- 1 root root 60833 Oct 28 14:23 /var/log/installer/status

14 0 -rw-rw---- 1 root utmp 0 Oct 23 17:51 /var/log/btmp

18 4 -rw-r--r-- 1 root root 32032 Oct 28 14:20 /var/log/faillog

12 4 -rw-r--r-- 1 root root 1294 Oct 23 18:12 /var/log/alternatives.log

39 4 -rw-r--r-- 1 root root 375 Oct 28 14:24 /var/log/sensor-capture-disk-config.log

15 0 -rwxr-x--- 1 sensor sensor 0 Oct 23 17:51 /var/log/clamav/clamav.log

16 4 -rwxr-x--- 1 sensor sensor 952 Oct 23 18:11 /var/log/clamav/freshclam.log

130056 0 -rw-r--r-- 1 root root 0 Oct 23 17:51 /var/log/atop/dummy\_after

130062 1492 -rw-r--r-- 1 root root 1519952 Oct 28 16:54 /var/log/atop/atop\_20191028

130057 0 -rw-r--r-- 1 root root 0 Oct 23 17:51 /var/log/atop/dummy\_before

130059 0 -rw-r--r-- 1 root root 0 Oct 28 14:24 /var/log/atop/daily.log

8.5\_ensure\_permissions\_on [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.6\_configure\_logrotate.sh

8.6\_configure\_logrotate [INFO] Working on 8.6\_configure\_logrotate

8.6\_configure\_logrotate [INFO] Checking Configuration

8.6\_configure\_logrotate [INFO] Performing audit

8.6\_configure\_logrotate [INFO] Ensure logs are properly rotated (especially syslog-ng)

8.6\_configure\_logrotate [INFO] No measure here, please review the files by yourself

8.6\_configure\_logrotate [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/8.7\_verify\_integrity\_packages.sh

8.7\_verify\_integrity\_pack [INFO] Working on 8.7\_verify\_integrity\_packages

8.7\_verify\_integrity\_pack [INFO] Checking Configuration

8.7\_verify\_integrity\_pack [INFO] Performing audit

8.7\_verify\_integrity\_pack [ KO ] Verify integrity all packages is fail!

8.7\_verify\_integrity\_pack [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.1\_enable\_cron.sh

9.1.1\_enable\_cron [INFO] Working on 9.1.1\_enable\_cron

9.1.1\_enable\_cron [INFO] Checking Configuration

9.1.1\_enable\_cron [INFO] Performing audit

9.1.1\_enable\_cron [ OK ] cron is installed

9.1.1\_enable\_cron [ OK ] cron is enabled

9.1.1\_enable\_cron [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.2\_crontab\_perm\_ownership.sh

9.1.2\_crontab\_perm\_owners [INFO] Working on 9.1.2\_crontab\_perm\_ownership

9.1.2\_crontab\_perm\_owners [INFO] Checking Configuration

9.1.2\_crontab\_perm\_owners [INFO] Performing audit

9.1.2\_crontab\_perm\_owners [ OK ] /etc/crontab has correct ownership

9.1.2\_crontab\_perm\_owners [ OK ] /etc/crontab has correct permissions

9.1.2\_crontab\_perm\_owners [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.3\_cron\_hourly\_perm\_ownership.sh

9.1.3\_cron\_hourly\_perm\_ow [INFO] Working on 9.1.3\_cron\_hourly\_perm\_ownership

9.1.3\_cron\_hourly\_perm\_ow [INFO] Checking Configuration

9.1.3\_cron\_hourly\_perm\_ow [INFO] Performing audit

9.1.3\_cron\_hourly\_perm\_ow [ OK ] /etc/cron.hourly has correct ownership

9.1.3\_cron\_hourly\_perm\_ow [ OK ] /etc/cron.hourly has correct permissions

9.1.3\_cron\_hourly\_perm\_ow [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.4\_cron\_daily\_perm\_ownership.sh

9.1.4\_cron\_daily\_perm\_own [INFO] Working on 9.1.4\_cron\_daily\_perm\_ownership

9.1.4\_cron\_daily\_perm\_own [INFO] Checking Configuration

9.1.4\_cron\_daily\_perm\_own [INFO] Performing audit

9.1.4\_cron\_daily\_perm\_own [ OK ] /etc/cron.daily has correct ownership

9.1.4\_cron\_daily\_perm\_own [ OK ] /etc/cron.daily has correct permissions

9.1.4\_cron\_daily\_perm\_own [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.5\_cron\_weekly\_perm\_ownership.sh

9.1.5\_cron\_weekly\_perm\_ow [INFO] Working on 9.1.5\_cron\_weekly\_perm\_ownership

9.1.5\_cron\_weekly\_perm\_ow [INFO] Checking Configuration

9.1.5\_cron\_weekly\_perm\_ow [INFO] Performing audit

9.1.5\_cron\_weekly\_perm\_ow [ OK ] /etc/cron.weekly has correct ownership

9.1.5\_cron\_weekly\_perm\_ow [ OK ] /etc/cron.weekly has correct permissions

9.1.5\_cron\_weekly\_perm\_ow [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.6\_cron\_monthly\_perm\_ownership.sh

9.1.6\_cron\_monthly\_perm\_o [INFO] Working on 9.1.6\_cron\_monthly\_perm\_ownership

9.1.6\_cron\_monthly\_perm\_o [INFO] Checking Configuration

9.1.6\_cron\_monthly\_perm\_o [INFO] Performing audit

9.1.6\_cron\_monthly\_perm\_o [ OK ] /etc/cron.monthly has correct ownership

9.1.6\_cron\_monthly\_perm\_o [ OK ] /etc/cron.monthly has correct permissions

9.1.6\_cron\_monthly\_perm\_o [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.7\_cron\_d\_perm\_ownership.sh

9.1.7\_cron\_d\_perm\_ownersh [INFO] Working on 9.1.7\_cron\_d\_perm\_ownership

9.1.7\_cron\_d\_perm\_ownersh [INFO] Checking Configuration

9.1.7\_cron\_d\_perm\_ownersh [INFO] Performing audit

9.1.7\_cron\_d\_perm\_ownersh [ OK ] /etc/cron.d has correct ownership

9.1.7\_cron\_d\_perm\_ownersh [ OK ] /etc/cron.d has correct permissions

9.1.7\_cron\_d\_perm\_ownersh [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.1.8\_cron\_users.sh

9.1.8\_cron\_users [INFO] Working on 9.1.8\_cron\_users

9.1.8\_cron\_users [INFO] Checking Configuration

9.1.8\_cron\_users [INFO] Performing audit

9.1.8\_cron\_users [ OK ] /etc/cron.deny is absent

9.1.8\_cron\_users [ OK ] /etc/at.deny is absent

9.1.8\_cron\_users [ OK ] /etc/cron.allow has correct ownership

9.1.8\_cron\_users [ OK ] /etc/cron.allow has correct permissions

9.1.8\_cron\_users [ OK ] /etc/at.allow has correct ownership

9.1.8\_cron\_users [ OK ] /etc/at.allow has correct permissions

9.1.8\_cron\_users [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.1\_pam\_retry\_cracklib.sh

9.2.1\_pam\_retry\_cracklib [INFO] Working on 9.2.1\_pam\_retry\_cracklib

9.2.1\_pam\_retry\_cracklib [INFO] Checking Configuration

9.2.1\_pam\_retry\_cracklib [INFO] Performing audit

9.2.1\_pam\_retry\_cracklib [ KO ] libpam-cracklib is not installed!

9.2.1\_pam\_retry\_cracklib [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.2\_pam\_minlen\_cracklib.sh

9.2.2\_pam\_minlen\_cracklib [INFO] Working on 9.2.2\_pam\_minlen\_cracklib

9.2.2\_pam\_minlen\_cracklib [INFO] Checking Configuration

9.2.2\_pam\_minlen\_cracklib [INFO] Performing audit

9.2.2\_pam\_minlen\_cracklib [ KO ] libpam-cracklib is not installed!

9.2.2\_pam\_minlen\_cracklib [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.3\_pam\_dcredit\_cracklib.sh

9.2.3\_pam\_dcredit\_crackli [INFO] Working on 9.2.3\_pam\_dcredit\_cracklib

9.2.3\_pam\_dcredit\_crackli [INFO] Checking Configuration

9.2.3\_pam\_dcredit\_crackli [INFO] Performing audit

9.2.3\_pam\_dcredit\_crackli [ KO ] libpam-cracklib is not installed!

9.2.3\_pam\_dcredit\_crackli [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.4\_pam\_ucredit\_cracklib.sh

9.2.4\_pam\_ucredit\_crackli [INFO] Working on 9.2.4\_pam\_ucredit\_cracklib

9.2.4\_pam\_ucredit\_crackli [INFO] Checking Configuration

9.2.4\_pam\_ucredit\_crackli [INFO] Performing audit

9.2.4\_pam\_ucredit\_crackli [ KO ] libpam-cracklib is not installed!

9.2.4\_pam\_ucredit\_crackli [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.5\_pam\_ocredit\_cracklib.sh

9.2.5\_pam\_ocredit\_crackli [INFO] Working on 9.2.5\_pam\_ocredit\_cracklib

9.2.5\_pam\_ocredit\_crackli [INFO] Checking Configuration

9.2.5\_pam\_ocredit\_crackli [INFO] Performing audit

9.2.5\_pam\_ocredit\_crackli [ KO ] libpam-cracklib is not installed!

9.2.5\_pam\_ocredit\_crackli [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.6\_pam\_lcredit\_cracklib.sh

9.2.6\_pam\_lcredit\_crackli [INFO] Working on 9.2.6\_pam\_lcredit\_cracklib

9.2.6\_pam\_lcredit\_crackli [INFO] Checking Configuration

9.2.6\_pam\_lcredit\_crackli [INFO] Performing audit

9.2.6\_pam\_lcredit\_crackli [ KO ] libpam-cracklib is not installed!

9.2.6\_pam\_lcredit\_crackli [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.7\_pam\_difok\_cracklib.sh

9.2.7\_pam\_difok\_cracklib [INFO] Working on 9.2.7\_pam\_difok\_cracklib

9.2.7\_pam\_difok\_cracklib [INFO] Checking Configuration

9.2.7\_pam\_difok\_cracklib [INFO] Performing audit

9.2.7\_pam\_difok\_cracklib [ KO ] libpam-cracklib is not installed!

9.2.7\_pam\_difok\_cracklib [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.8\_pam\_minclass\_cracklib.sh

9.2.8\_pam\_minclass\_crackl [INFO] Working on 9.2.8\_pam\_minclass\_cracklib

9.2.8\_pam\_minclass\_crackl [INFO] Checking Configuration

9.2.8\_pam\_minclass\_crackl [INFO] Performing audit

9.2.8\_pam\_minclass\_crackl [ KO ] libpam-cracklib is not installed!

9.2.8\_pam\_minclass\_crackl [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.9\_pam\_maxrepeat\_cracklib.sh

9.2.9\_pam\_maxrepeat\_crack [INFO] Working on 9.2.9\_pam\_maxrepeat\_cracklib

9.2.9\_pam\_maxrepeat\_crack [INFO] Checking Configuration

9.2.9\_pam\_maxrepeat\_crack [INFO] Performing audit

9.2.9\_pam\_maxrepeat\_crack [ KO ] libpam-cracklib is not installed!

9.2.9\_pam\_maxrepeat\_crack [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.10\_pam\_maxclassrepeat\_cracklib.sh

9.2.10\_pam\_maxclassrepeat [INFO] Working on 9.2.10\_pam\_maxclassrepeat\_cracklib

9.2.10\_pam\_maxclassrepeat [INFO] Checking Configuration

9.2.10\_pam\_maxclassrepeat [INFO] Performing audit

9.2.10\_pam\_maxclassrepeat [ KO ] libpam-cracklib is not installed!

9.2.10\_pam\_maxclassrepeat [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.11\_pam\_deny\_times\_tally2.sh

9.2.11\_pam\_deny\_times\_tal [INFO] Working on 9.2.11\_pam\_deny\_times\_tally2

9.2.11\_pam\_deny\_times\_tal [INFO] Checking Configuration

9.2.11\_pam\_deny\_times\_tal [INFO] Performing audit

9.2.11\_pam\_deny\_times\_tal [ OK ] libpam-modules-bin is installed

9.2.11\_pam\_deny\_times\_tal [ KO ] ^auth[[:space:]]\*required[[:space:]]\*pam\_tally2.so is not present in /etc/pam.d/common-auth

9.2.11\_pam\_deny\_times\_tal [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.12\_pam\_lockout\_failed\_tally2.sh

9.2.12\_pam\_lockout\_failed [INFO] Working on 9.2.12\_pam\_lockout\_failed\_tally2

9.2.12\_pam\_lockout\_failed [INFO] Checking Configuration

9.2.12\_pam\_lockout\_failed [INFO] Performing audit

9.2.12\_pam\_lockout\_failed [ OK ] libpam-modules-bin is installed

9.2.12\_pam\_lockout\_failed [ KO ] ^auth[[:space:]]\*required[[:space:]]\*pam\_tally2.so is not present in /etc/pam.d/common-auth

9.2.12\_pam\_lockout\_failed [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.13\_pam\_password\_sha512\_unix.sh

9.2.13\_pam\_password\_sha51 [INFO] Working on 9.2.13\_pam\_password\_sha512\_unix

9.2.13\_pam\_password\_sha51 [INFO] Checking Configuration

9.2.13\_pam\_password\_sha51 [INFO] Performing audit

9.2.13\_pam\_password\_sha51 [ OK ] libpam-modules is installed

9.2.13\_pam\_password\_sha51 [ OK ] ^password.\*pam\_unix.so is present in /etc/pam.d/common-password

9.2.13\_pam\_password\_sha51 [ OK ] sha512 is already configured

9.2.13\_pam\_password\_sha51 [ KO ] rounds set is not match legally, rounds is set 5000

9.2.13\_pam\_password\_sha51 [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.14\_pam\_auth\_without\_nullpwd\_unix.sh

9.2.14\_pam\_auth\_without\_n [INFO] Working on 9.2.14\_pam\_auth\_without\_nullpwd\_unix

9.2.14\_pam\_auth\_without\_n [INFO] Checking Configuration

9.2.14\_pam\_auth\_without\_n [INFO] Performing audit

9.2.14\_pam\_auth\_without\_n [ OK ] libpam-modules is installed

9.2.14\_pam\_auth\_without\_n [ OK ] ^auth.\*pam\_unix.so is present in /etc/pam.d/common-auth

9.2.14\_pam\_auth\_without\_n [ OK ] nullok is not configured

9.2.14\_pam\_auth\_without\_n [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.15\_pam\_printlastlog\_to\_showfailed\_lastlog.sh

9.2.15\_pam\_printlastlog\_t [INFO] Working on 9.2.15\_pam\_printlastlog\_to\_showfailed\_lastlog

9.2.15\_pam\_printlastlog\_t [INFO] Checking Configuration

9.2.15\_pam\_printlastlog\_t [INFO] Performing audit

9.2.15\_pam\_printlastlog\_t [ OK ] libpam-modules is installed

9.2.15\_pam\_printlastlog\_t [ OK ] ^session.\*pam\_lastlog.so is present in /etc/pam.d/login

9.2.15\_pam\_printlastlog\_t [ OK ] showfailed is already configured

9.2.15\_pam\_printlastlog\_t [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.16\_pam\_limit\_password\_reuse.sh

9.2.16\_pam\_limit\_password [INFO] Working on 9.2.16\_pam\_limit\_password\_reuse

9.2.16\_pam\_limit\_password [INFO] Checking Configuration

9.2.16\_pam\_limit\_password [INFO] Performing audit

9.2.16\_pam\_limit\_password [ OK ] libpam-modules is installed

9.2.16\_pam\_limit\_password [ KO ] ^password.\*pam\_pwhistory.so is not present in /etc/pam.d/common-password

9.2.16\_pam\_limit\_password [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.2.17\_pam\_even\_deny\_root\_tally2.sh

9.2.17\_pam\_even\_deny\_root [INFO] Working on 9.2.17\_pam\_even\_deny\_root\_tally2

9.2.17\_pam\_even\_deny\_root [INFO] Checking Configuration

9.2.17\_pam\_even\_deny\_root [INFO] Performing audit

9.2.17\_pam\_even\_deny\_root [ OK ] libpam-modules-bin is installed

9.2.17\_pam\_even\_deny\_root [ KO ] ^auth[[:space:]]\*required[[:space:]]\*pam\_tally2.so is not present in /etc/pam.d/common-auth

9.2.17\_pam\_even\_deny\_root [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.1\_sshd\_protocol.sh

9.3.1\_sshd\_protocol [INFO] Working on 9.3.1\_sshd\_protocol

9.3.1\_sshd\_protocol [INFO] Checking Configuration

9.3.1\_sshd\_protocol [INFO] Performing audit

9.3.1\_sshd\_protocol [ OK ] openssh-server is installed

9.3.1\_sshd\_protocol [ OK ] ^Protocol[[:space:]]\*2 is present in /etc/ssh/sshd\_config

9.3.1\_sshd\_protocol [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.2\_sshd\_loglevel.sh

9.3.2\_sshd\_loglevel [INFO] Working on 9.3.2\_sshd\_loglevel

9.3.2\_sshd\_loglevel [INFO] Checking Configuration

9.3.2\_sshd\_loglevel [INFO] Performing audit

9.3.2\_sshd\_loglevel [ OK ] openssh-server is installed

9.3.2\_sshd\_loglevel [ OK ] ^LogLevel[[:space:]]\*INFO is present in /etc/ssh/sshd\_config

9.3.2\_sshd\_loglevel [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.3\_sshd\_conf\_perm\_ownership.sh

9.3.3\_sshd\_conf\_perm\_owne [INFO] Working on 9.3.3\_sshd\_conf\_perm\_ownership

9.3.3\_sshd\_conf\_perm\_owne [INFO] Checking Configuration

9.3.3\_sshd\_conf\_perm\_owne [INFO] Performing audit

9.3.3\_sshd\_conf\_perm\_owne [ OK ] /etc/ssh/sshd\_config has correct ownership

9.3.3\_sshd\_conf\_perm\_owne [ OK ] /etc/ssh/sshd\_config has correct permissions

9.3.3\_sshd\_conf\_perm\_owne [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.4\_disable\_x11\_forwarding.sh

9.3.4\_disable\_x11\_forward [INFO] Working on 9.3.4\_disable\_x11\_forwarding

9.3.4\_disable\_x11\_forward [INFO] Checking Configuration

9.3.4\_disable\_x11\_forward [INFO] Performing audit

9.3.4\_disable\_x11\_forward [ OK ] openssh-server is installed

9.3.4\_disable\_x11\_forward [ OK ] ^X11Forwarding[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.4\_disable\_x11\_forward [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.5\_sshd\_maxauthtries.sh

9.3.5\_sshd\_maxauthtries [INFO] Working on 9.3.5\_sshd\_maxauthtries

9.3.5\_sshd\_maxauthtries [INFO] Checking Configuration

9.3.5\_sshd\_maxauthtries [INFO] Performing audit

9.3.5\_sshd\_maxauthtries [ OK ] openssh-server is installed

9.3.5\_sshd\_maxauthtries [ OK ] ^MaxAuthTries[[:space:]]\*4 is present in /etc/ssh/sshd\_config

9.3.5\_sshd\_maxauthtries [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.6\_enable\_sshd\_ignorerhosts.sh

9.3.6\_enable\_sshd\_ignorer [INFO] Working on 9.3.6\_enable\_sshd\_ignorerhosts

9.3.6\_enable\_sshd\_ignorer [INFO] Checking Configuration

9.3.6\_enable\_sshd\_ignorer [INFO] Performing audit

9.3.6\_enable\_sshd\_ignorer [ OK ] openssh-server is installed

9.3.6\_enable\_sshd\_ignorer [ OK ] ^IgnoreRhosts[[:space:]]\*yes is present in /etc/ssh/sshd\_config

9.3.6\_enable\_sshd\_ignorer [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.7\_disable\_sshd\_hostbasedauthentication.sh

9.3.7\_disable\_sshd\_hostba [INFO] Working on 9.3.7\_disable\_sshd\_hostbasedauthentication

9.3.7\_disable\_sshd\_hostba [INFO] Checking Configuration

9.3.7\_disable\_sshd\_hostba [INFO] Performing audit

9.3.7\_disable\_sshd\_hostba [ OK ] openssh-server is installed

9.3.7\_disable\_sshd\_hostba [ OK ] ^HostbasedAuthentication[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.7\_disable\_sshd\_hostba [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.8\_disable\_root\_login.sh

9.3.8\_disable\_root\_login [INFO] Working on 9.3.8\_disable\_root\_login

9.3.8\_disable\_root\_login [INFO] Checking Configuration

9.3.8\_disable\_root\_login [INFO] Performing audit

9.3.8\_disable\_root\_login [ OK ] openssh-server is installed

9.3.8\_disable\_root\_login [ OK ] ^PermitRootLogin[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.8\_disable\_root\_login [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.9\_disable\_sshd\_permitemptypasswords.sh

9.3.9\_disable\_sshd\_permit [INFO] Working on 9.3.9\_disable\_sshd\_permitemptypasswords

9.3.9\_disable\_sshd\_permit [INFO] Checking Configuration

9.3.9\_disable\_sshd\_permit [INFO] Performing audit

9.3.9\_disable\_sshd\_permit [ OK ] openssh-server is installed

9.3.9\_disable\_sshd\_permit [ OK ] ^PermitEmptyPasswords[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.9\_disable\_sshd\_permit [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.10\_disable\_sshd\_setenv.sh

9.3.10\_disable\_sshd\_seten [INFO] Working on 9.3.10\_disable\_sshd\_setenv

9.3.10\_disable\_sshd\_seten [INFO] Checking Configuration

9.3.10\_disable\_sshd\_seten [INFO] Performing audit

9.3.10\_disable\_sshd\_seten [ OK ] openssh-server is installed

9.3.10\_disable\_sshd\_seten [ OK ] ^PermitUserEnvironment[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.10\_disable\_sshd\_seten [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.11\_sshd\_ciphers.sh

9.3.11\_sshd\_ciphers [INFO] Working on 9.3.11\_sshd\_ciphers

9.3.11\_sshd\_ciphers [INFO] Checking Configuration

9.3.11\_sshd\_ciphers [INFO] Performing audit

9.3.11\_sshd\_ciphers [ OK ] openssh-server is installed

9.3.11\_sshd\_ciphers [ OK ] ^Ciphers[[:space:]]\*chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr is present in /etc/ssh/sshd\_config

9.3.11\_sshd\_ciphers [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.12\_sshd\_idle\_timeout.sh

9.3.12\_sshd\_idle\_timeout [INFO] Working on 9.3.12\_sshd\_idle\_timeout

9.3.12\_sshd\_idle\_timeout [INFO] Checking Configuration

9.3.12\_sshd\_idle\_timeout [INFO] Performing audit

9.3.12\_sshd\_idle\_timeout [ OK ] openssh-server is installed

9.3.12\_sshd\_idle\_timeout [ OK ] ^ClientAliveInterval[[:space:]]\*300 is present in /etc/ssh/sshd\_config

9.3.12\_sshd\_idle\_timeout [ OK ] ^ClientAliveCountMax[[:space:]]\*0 is present in /etc/ssh/sshd\_config

9.3.12\_sshd\_idle\_timeout [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.13\_sshd\_limit\_access.sh

9.3.13\_sshd\_limit\_access [INFO] Working on 9.3.13\_sshd\_limit\_access

9.3.13\_sshd\_limit\_access [INFO] Checking Configuration

9.3.13\_sshd\_limit\_access [INFO] ALLOWED\_USERS is not set, defaults to wildcard

9.3.13\_sshd\_limit\_access [INFO] ALLOWED\_GROUPS is not set, defaults to wildcard

9.3.13\_sshd\_limit\_access [INFO] DENIED\_USERS is not set, defaults to nobody

9.3.13\_sshd\_limit\_access [INFO] DENIED\_GROUPS is not set, defaults to nobody

9.3.13\_sshd\_limit\_access [INFO] Performing audit

9.3.13\_sshd\_limit\_access [ OK ] openssh-server is installed

9.3.13\_sshd\_limit\_access [ KO ] ^AllowUsers[[:space:]]\*\* is not present in /etc/ssh/sshd\_config

9.3.13\_sshd\_limit\_access [ KO ] ^AllowGroups[[:space:]]\*\* is not present in /etc/ssh/sshd\_config

9.3.13\_sshd\_limit\_access [ KO ] ^DenyUsers[[:space:]]\*nobody is not present in /etc/ssh/sshd\_config

9.3.13\_sshd\_limit\_access [ KO ] ^DenyGroups[[:space:]]\*nobody is not present in /etc/ssh/sshd\_config

9.3.13\_sshd\_limit\_access [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.14\_ssh\_banner.sh

9.3.14\_ssh\_banner [INFO] Working on 9.3.14\_ssh\_banner

9.3.14\_ssh\_banner [INFO] Checking Configuration

9.3.14\_ssh\_banner [INFO] BANNER\_FILE is not set, defaults to wildcard

9.3.14\_ssh\_banner [INFO] Performing audit

9.3.14\_ssh\_banner [ OK ] openssh-server is installed

9.3.14\_ssh\_banner [ OK ] ^Banner[[:space:]]\* is present in /etc/ssh/sshd\_config

9.3.14\_ssh\_banner [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.15\_sshd\_printlastlog.sh

9.3.15\_sshd\_printlastlog [INFO] Working on 9.3.15\_sshd\_printlastlog

9.3.15\_sshd\_printlastlog [INFO] Checking Configuration

9.3.15\_sshd\_printlastlog [INFO] Performing audit

9.3.15\_sshd\_printlastlog [ OK ] openssh-server is installed

9.3.15\_sshd\_printlastlog [ OK ] ^PrintLastLog[[:space:]]\*yes is present in /etc/ssh/sshd\_config

9.3.15\_sshd\_printlastlog [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.16\_sshd\_IgnoreUserKnownHosts.sh

9.3.16\_sshd\_IgnoreUserKno [INFO] Working on 9.3.16\_sshd\_IgnoreUserKnownHosts

9.3.16\_sshd\_IgnoreUserKno [INFO] Checking Configuration

9.3.16\_sshd\_IgnoreUserKno [INFO] Performing audit

9.3.16\_sshd\_IgnoreUserKno [ OK ] openssh-server is installed

9.3.16\_sshd\_IgnoreUserKno [ OK ] ^IgnoreUserKnownHosts[[:space:]]\*yes is present in /etc/ssh/sshd\_config

9.3.16\_sshd\_IgnoreUserKno [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.17\_sshd\_GSSAPIAuthentication.sh

9.3.17\_sshd\_GSSAPIAuthent [INFO] Working on 9.3.17\_sshd\_GSSAPIAuthentication

9.3.17\_sshd\_GSSAPIAuthent [INFO] Checking Configuration

9.3.17\_sshd\_GSSAPIAuthent [INFO] Performing audit

9.3.17\_sshd\_GSSAPIAuthent [ OK ] openssh-server is installed

9.3.17\_sshd\_GSSAPIAuthent [ OK ] ^GSSAPIAuthentication[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.17\_sshd\_GSSAPIAuthent [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.18\_sshd\_KerberosAuthentication.sh

9.3.18\_sshd\_KerberosAuthe [INFO] Working on 9.3.18\_sshd\_KerberosAuthentication

9.3.18\_sshd\_KerberosAuthe [INFO] Checking Configuration

9.3.18\_sshd\_KerberosAuthe [INFO] Performing audit

9.3.18\_sshd\_KerberosAuthe [ OK ] openssh-server is installed

9.3.18\_sshd\_KerberosAuthe [ OK ] ^KerberosAuthentication[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.18\_sshd\_KerberosAuthe [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.19\_sshd\_StrictModes.sh

9.3.19\_sshd\_StrictModes [INFO] Working on 9.3.19\_sshd\_StrictModes

9.3.19\_sshd\_StrictModes [INFO] Checking Configuration

9.3.19\_sshd\_StrictModes [INFO] Performing audit

9.3.19\_sshd\_StrictModes [ OK ] openssh-server is installed

9.3.19\_sshd\_StrictModes [ OK ] ^StrictModes[[:space:]]\*yes is present in /etc/ssh/sshd\_config

9.3.19\_sshd\_StrictModes [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.21\_sshd\_compression.sh

9.3.21\_sshd\_compression [INFO] Working on 9.3.21\_sshd\_compression

9.3.21\_sshd\_compression [INFO] Checking Configuration

9.3.21\_sshd\_compression [INFO] Performing audit

9.3.21\_sshd\_compression [ OK ] openssh-server is installed

9.3.21\_sshd\_compression [ OK ] ^Compression[[:space:]]\*no is present in /etc/ssh/sshd\_config

9.3.21\_sshd\_compression [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.22\_sshd\_MACs.sh

9.3.22\_sshd\_MACs [INFO] Working on 9.3.22\_sshd\_MACs

9.3.22\_sshd\_MACs [INFO] Checking Configuration

9.3.22\_sshd\_MACs [INFO] Performing audit

9.3.22\_sshd\_MACs [ OK ] openssh-server is installed

9.3.22\_sshd\_MACs [ OK ] ^MACs[[:space:]]\*hmac-sha2-256,hmac-sha2-512 is present in /etc/ssh/sshd\_config

9.3.22\_sshd\_MACs [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.23\_ssh\_check\_pub\_hostkey\_permission.sh

9.3.23\_ssh\_check\_pub\_host [INFO] Working on 9.3.23\_ssh\_check\_pub\_hostkey\_permission

9.3.23\_ssh\_check\_pub\_host [INFO] Checking Configuration

9.3.23\_ssh\_check\_pub\_host [INFO] Performing audit

9.3.23\_ssh\_check\_pub\_host [ OK ] There are file has correct ownership

9.3.23\_ssh\_check\_pub\_host [ OK ] Not any file has a mode more permissive than 0644

9.3.23\_ssh\_check\_pub\_host [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.24\_ssh\_check\_priv\_hostkey\_permission.sh

9.3.24\_ssh\_check\_priv\_hos [INFO] Working on 9.3.24\_ssh\_check\_priv\_hostkey\_permission

9.3.24\_ssh\_check\_priv\_hos [INFO] Checking Configuration

9.3.24\_ssh\_check\_priv\_hos [INFO] Performing audit

9.3.24\_ssh\_check\_priv\_hos [ OK ] There are file has correct ownership

9.3.24\_ssh\_check\_priv\_hos [ OK ] Not any file has a mode more permissive than 0600

9.3.24\_ssh\_check\_priv\_hos [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.25\_sshd\_kexalgorithms.sh

9.3.25\_sshd\_kexalgorithms [INFO] Working on 9.3.25\_sshd\_kexalgorithms

9.3.25\_sshd\_kexalgorithms [INFO] Checking Configuration

9.3.25\_sshd\_kexalgorithms [INFO] Performing audit

9.3.25\_sshd\_kexalgorithms [ OK ] openssh-server is installed

9.3.25\_sshd\_kexalgorithms [ OK ] ^KexAlgorithms[[:space:]]\*ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256 is present in /etc/ssh/sshd\_config

9.3.25\_sshd\_kexalgorithms [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.26\_sshd\_logingracetime.sh

9.3.26\_sshd\_logingracetim [INFO] Working on 9.3.26\_sshd\_logingracetime

9.3.26\_sshd\_logingracetim [INFO] Checking Configuration

9.3.26\_sshd\_logingracetim [INFO] Performing audit

9.3.26\_sshd\_logingracetim [ OK ] openssh-server is installed

9.3.26\_sshd\_logingracetim [ OK ] ^LoginGraceTime[[:space:]]\*60 is present in /etc/ssh/sshd\_config

9.3.26\_sshd\_logingracetim [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.3.27\_sshd\_access\_limit.sh

9.3.27\_sshd\_access\_limit [INFO] Working on 9.3.27\_sshd\_access\_limit

9.3.27\_sshd\_access\_limit [INFO] Checking Configuration

9.3.27\_sshd\_access\_limit [INFO] Performing audit

9.3.27\_sshd\_access\_limit [ OK ] openssh-server is installed

9.3.27\_sshd\_access\_limit [ OK ] AllowUsers has set limit.

9.3.27\_sshd\_access\_limit [ OK ] AllowGroups has set limit.

9.3.27\_sshd\_access\_limit [ OK ] DenyUsers has set limit.

9.3.27\_sshd\_access\_limit [ OK ] DenyGroups has set limit.

9.3.27\_sshd\_access\_limit [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.4\_secure\_tty.sh

9.4\_secure\_tty [INFO] Working on 9.4\_secure\_tty

9.4\_secure\_tty [INFO] Checking Configuration

9.4\_secure\_tty [INFO] Performing audit

9.4\_secure\_tty [INFO] Remove terminal entries in /etc/securetty for any consoles that are not in a physically secure location.

9.4\_secure\_tty [INFO] No measure here, please review the file by yourself

9.4\_secure\_tty [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/9.5\_pam\_restrict\_su.sh

9.5\_pam\_restrict\_su [INFO] Working on 9.5\_pam\_restrict\_su

9.5\_pam\_restrict\_su [INFO] Checking Configuration

9.5\_pam\_restrict\_su [INFO] Performing audit

9.5\_pam\_restrict\_su [ OK ] login is installed

9.5\_pam\_restrict\_su [ KO ] ^auth[[:space:]]\*required[[:space:]]\*pam\_wheel.so is not present in /etc/pam.d/su

9.5\_pam\_restrict\_su [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.1\_set\_password\_exp\_days.sh

10.1.1\_set\_password\_exp\_d [INFO] Working on 10.1.1\_set\_password\_exp\_days

10.1.1\_set\_password\_exp\_d [INFO] Checking Configuration

10.1.1\_set\_password\_exp\_d [INFO] Performing audit

10.1.1\_set\_password\_exp\_d [ OK ] login is installed

10.1.1\_set\_password\_exp\_d [ KO ] ^PASS\_MAX\_DAYS[[:space:]]\*90 is not present in /etc/login.defs

10.1.1\_set\_password\_exp\_d [ KO ] Have least user's maxinum password lifttime is greater than 90 day

10.1.1\_set\_password\_exp\_d [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.2\_set\_password\_min\_days\_change.sh

10.1.2\_set\_password\_min\_d [INFO] Working on 10.1.2\_set\_password\_min\_days\_change

10.1.2\_set\_password\_min\_d [INFO] Checking Configuration

10.1.2\_set\_password\_min\_d [INFO] Performing audit

10.1.2\_set\_password\_min\_d [ OK ] login is installed

10.1.2\_set\_password\_min\_d [ KO ] ^PASS\_MIN\_DAYS[[:space:]]\*7 is not present in /etc/login.defs

10.1.2\_set\_password\_min\_d [ KO ] Have least user's mininum password lifttime is not equal or less than 7 day

10.1.2\_set\_password\_min\_d [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.3\_set\_password\_exp\_warning\_days.sh

10.1.3\_set\_password\_exp\_w [INFO] Working on 10.1.3\_set\_password\_exp\_warning\_days

10.1.3\_set\_password\_exp\_w [INFO] Checking Configuration

10.1.3\_set\_password\_exp\_w [INFO] Performing audit

10.1.3\_set\_password\_exp\_w [ OK ] login is installed

10.1.3\_set\_password\_exp\_w [ OK ] ^PASS\_WARN\_AGE[[:space:]]\*7 is present in /etc/login.defs

10.1.3\_set\_password\_exp\_w [ OK ] All user's maxinum password lifttime is equal or less than 7 day

10.1.3\_set\_password\_exp\_w [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.4\_set\_password\_encrypt\_method.sh

10.1.4\_set\_password\_encry [INFO] Working on 10.1.4\_set\_password\_encrypt\_method

10.1.4\_set\_password\_encry [INFO] Checking Configuration

10.1.4\_set\_password\_encry [INFO] Performing audit

10.1.4\_set\_password\_encry [ OK ] login is installed

10.1.4\_set\_password\_encry [ OK ] ^ENCRYPT\_METHOD[[:space:]]\*SHA512 is present in /etc/login.defs

10.1.4\_set\_password\_encry [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.5\_set\_password\_lock\_inactive\_user.sh

10.1.5\_set\_password\_lock\_ [INFO] Working on 10.1.5\_set\_password\_lock\_inactive\_user

10.1.5\_set\_password\_lock\_ [INFO] Checking Configuration

10.1.5\_set\_password\_lock\_ [INFO] Performing audit

10.1.5\_set\_password\_lock\_ [ KO ] INACTIVE feature has disabled.

10.1.5\_set\_password\_lock\_ [ KO ] Have least user's INACTIVE password lifttime is not set

10.1.5\_set\_password\_lock\_ [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.6\_remove\_nopasswd\_sudoers.sh

10.1.6\_remove\_nopasswd\_su [INFO] Working on 10.1.6\_remove\_nopasswd\_sudoers

10.1.6\_remove\_nopasswd\_su [INFO] Checking Configuration

10.1.6\_remove\_nopasswd\_su [INFO] Performing audit

10.1.6\_remove\_nopasswd\_su [ OK ] NOPASSWD is not set on /etc/sudoers, it's ok

10.1.6\_remove\_nopasswd\_su [ KO ] NOPASSWD is set on /etc/sudoers.d/\*, it's error conf

10.1.6\_remove\_nopasswd\_su [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.7\_remove\_noauthenticate\_sudoers.sh

10.1.7\_remove\_noauthentic [INFO] Working on 10.1.7\_remove\_noauthenticate\_sudoers

10.1.7\_remove\_noauthentic [INFO] Checking Configuration

10.1.7\_remove\_noauthentic [INFO] Performing audit

10.1.7\_remove\_noauthentic [ OK ] !authenticate is not set on /etc/sudoers, it's ok

10.1.7\_remove\_noauthentic [ OK ] !authenticate is not set on /etc/sudoers.d/\*, it's ok

10.1.7\_remove\_noauthentic [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.8\_set\_fail\_delay\_seconds.sh

10.1.8\_set\_fail\_delay\_sec [INFO] Working on 10.1.8\_set\_fail\_delay\_seconds

10.1.8\_set\_fail\_delay\_sec [INFO] Checking Configuration

10.1.8\_set\_fail\_delay\_sec [INFO] Performing audit

10.1.8\_set\_fail\_delay\_sec [ OK ] libpam-modules is installed

10.1.8\_set\_fail\_delay\_sec [ OK ] ^auth.\*pam\_faildelay.so is present in /etc/pam.d/login

10.1.8\_set\_fail\_delay\_sec [ OK ] delay set condition is 4000000

10.1.8\_set\_fail\_delay\_sec [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.9\_set\_create\_home\_bool.sh

10.1.9\_set\_create\_home\_bo [INFO] Working on 10.1.9\_set\_create\_home\_bool

10.1.9\_set\_create\_home\_bo [INFO] Checking Configuration

10.1.9\_set\_create\_home\_bo [INFO] Performing audit

10.1.9\_set\_create\_home\_bo [ OK ] login is installed

10.1.9\_set\_create\_home\_bo [ OK ] ^CREATE\_HOME[[:space:]]\*yes is present in /etc/login.defs

10.1.9\_set\_create\_home\_bo [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.10\_set\_maxlogins\_for\_all\_accounts.sh

10.1.10\_set\_maxlogins\_for [INFO] Working on 10.1.10\_set\_maxlogins\_for\_all\_accounts

10.1.10\_set\_maxlogins\_for [INFO] Checking Configuration

10.1.10\_set\_maxlogins\_for [INFO] Performing audit

10.1.10\_set\_maxlogins\_for [ OK ] libpam-modules is installed

10.1.10\_set\_maxlogins\_for [ OK ] /etc/security/limits.conf does exist

10.1.10\_set\_maxlogins\_for [ KO ] maxsyslogins is not set in /etc/security/limits.conf.

10.1.10\_set\_maxlogins\_for [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.1.11\_ensure\_no\_shosts\_cfg\_on\_system.sh

10.1.11\_ensure\_no\_shosts\_ [INFO] Working on 10.1.11\_ensure\_no\_shosts\_cfg\_on\_system

10.1.11\_ensure\_no\_shosts\_ [INFO] Checking Configuration

10.1.11\_ensure\_no\_shosts\_ [INFO] Performing audit

10.1.11\_ensure\_no\_shosts\_ [ OK ] .shosts and shosts.equiv file is not on system.

10.1.11\_ensure\_no\_shosts\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.2\_disable\_system\_accounts.sh

10.2\_disable\_system\_accou [INFO] Working on 10.2\_disable\_system\_accounts

10.2\_disable\_system\_accou [INFO] Checking Configuration

10.2\_disable\_system\_accou [INFO] Performing audit

10.2\_disable\_system\_accou [INFO] Checking if admin accounts have a login shell different than /bin/false

10.2\_disable\_system\_accou [ OK ] All admin accounts deactivated

10.2\_disable\_system\_accou [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.3\_default\_root\_group.sh

10.3\_default\_root\_group [INFO] Working on 10.3\_default\_root\_group

10.3\_default\_root\_group [INFO] Checking Configuration

10.3\_default\_root\_group [INFO] Performing audit

10.3\_default\_root\_group [ OK ] Root group has GID 0

10.3\_default\_root\_group [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.4\_default\_umask.sh

10.4\_default\_umask [INFO] Working on 10.4\_default\_umask

10.4\_default\_umask [INFO] Checking Configuration

10.4\_default\_umask [INFO] Performing audit

10.4\_default\_umask [ OK ] umask 077 is present in /etc/bash.bashrc /etc/profile.d /etc/profile

10.4\_default\_umask [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/10.5\_set\_timeout\_tty.sh

10.5\_set\_timeout\_tty [INFO] Working on 10.5\_set\_timeout\_tty

10.5\_set\_timeout\_tty [INFO] Checking Configuration

10.5\_set\_timeout\_tty [INFO] Performing audit

10.5\_set\_timeout\_tty [ KO ] TMOUT= is not present in /etc/bash.bashrc /etc/profile.d /etc/profile

10.5\_set\_timeout\_tty [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/11.1\_warning\_banners.sh

11.1\_warning\_banners [INFO] Working on 11.1\_warning\_banners

11.1\_warning\_banners [INFO] Checking Configuration

11.1\_warning\_banners [INFO] Performing audit

11.1\_warning\_banners [ OK ] /etc/motd has correct ownership

11.1\_warning\_banners [ OK ] /etc/motd has correct permissions

11.1\_warning\_banners [ OK ] /etc/issue has correct ownership

11.1\_warning\_banners [ OK ] /etc/issue has correct permissions

11.1\_warning\_banners [ OK ] /etc/issue.net has correct ownership

11.1\_warning\_banners [ OK ] /etc/issue.net has correct permissions

11.1\_warning\_banners [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/11.2\_remove\_os\_info\_warning\_banners.sh

11.2\_remove\_os\_info\_warni [INFO] Working on 11.2\_remove\_os\_info\_warning\_banners

11.2\_remove\_os\_info\_warni [INFO] Checking Configuration

11.2\_remove\_os\_info\_warni [INFO] Performing audit

11.2\_remove\_os\_info\_warni [ OK ] (\v|\r|\m|\s|Debian) is not present in /etc/motd

11.2\_remove\_os\_info\_warni [ OK ] (\v|\r|\m|\s|Debian) is not present in /etc/issue

11.2\_remove\_os\_info\_warni [ OK ] (\v|\r|\m|\s|Debian) is not present in /etc/issue.net

11.2\_remove\_os\_info\_warni [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.1\_etc\_passwd\_permissions.sh

12.1\_etc\_passwd\_permissio [INFO] Working on 12.1\_etc\_passwd\_permissions

12.1\_etc\_passwd\_permissio [INFO] Checking Configuration

12.1\_etc\_passwd\_permissio [INFO] Performing audit

12.1\_etc\_passwd\_permissio [ OK ] /etc/passwd has correct ownership

12.1\_etc\_passwd\_permissio [ OK ] /etc/passwd has correct permissions

12.1\_etc\_passwd\_permissio [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.2\_etc\_shadow\_permissions.sh

12.2\_etc\_shadow\_permissio [INFO] Working on 12.2\_etc\_shadow\_permissions

12.2\_etc\_shadow\_permissio [INFO] Checking Configuration

12.2\_etc\_shadow\_permissio [INFO] Performing audit

12.2\_etc\_shadow\_permissio [ OK ] /etc/shadow has correct ownership

12.2\_etc\_shadow\_permissio [ OK ] /etc/shadow has correct permissions

12.2\_etc\_shadow\_permissio [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.3\_etc\_group\_permissions.sh

12.3\_etc\_group\_permission [INFO] Working on 12.3\_etc\_group\_permissions

12.3\_etc\_group\_permission [INFO] Checking Configuration

12.3\_etc\_group\_permission [INFO] Performing audit

12.3\_etc\_group\_permission [ OK ] /etc/group has correct ownership

12.3\_etc\_group\_permission [ OK ] /etc/group has correct permissions

12.3\_etc\_group\_permission [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.4\_etc\_gshadow\_permissions.sh

12.4\_etc\_gshadow\_permissi [INFO] Working on 12.4\_etc\_gshadow\_permissions

12.4\_etc\_gshadow\_permissi [INFO] Checking Configuration

12.4\_etc\_gshadow\_permissi [INFO] Performing audit

12.4\_etc\_gshadow\_permissi [ OK ] /etc/gshadow has correct ownership

12.4\_etc\_gshadow\_permissi [ OK ] /etc/gshadow has correct permissions

12.4\_etc\_gshadow\_permissi [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.5\_etc\_passwd\_backup\_permissions.sh

12.5\_etc\_passwd\_backup\_pe [INFO] Working on 12.5\_etc\_passwd\_backup\_permissions

12.5\_etc\_passwd\_backup\_pe [INFO] Checking Configuration

12.5\_etc\_passwd\_backup\_pe [INFO] Performing audit

12.5\_etc\_passwd\_backup\_pe [ OK ] /etc/passwd- has correct ownership

12.5\_etc\_passwd\_backup\_pe [ OK ] /etc/passwd- has correct permissions

12.5\_etc\_passwd\_backup\_pe [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.6\_etc\_shadow\_backup\_permissions.sh

12.6\_etc\_shadow\_backup\_pe [INFO] Working on 12.6\_etc\_shadow\_backup\_permissions

12.6\_etc\_shadow\_backup\_pe [INFO] Checking Configuration

12.6\_etc\_shadow\_backup\_pe [INFO] Performing audit

12.6\_etc\_shadow\_backup\_pe [ OK ] /etc/shadow- has correct ownership

12.6\_etc\_shadow\_backup\_pe [ OK ] /etc/shadow- has correct permissions

12.6\_etc\_shadow\_backup\_pe [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.7\_find\_world\_writable\_file.sh

12.7\_find\_world\_writable\_ [INFO] Working on 12.7\_find\_world\_writable\_file

12.7\_find\_world\_writable\_ [INFO] Checking Configuration

12.7\_find\_world\_writable\_ [INFO] Performing audit

12.7\_find\_world\_writable\_ [INFO] Checking if there are world writable files

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.8\_find\_unowned\_files.sh

12.8\_find\_unowned\_files [INFO] Working on 12.8\_find\_unowned\_files

12.8\_find\_unowned\_files [INFO] Checking Configuration

12.8\_find\_unowned\_files [INFO] Performing audit

12.8\_find\_unowned\_files [INFO] Checking if there are unowned files

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.9\_find\_ungrouped\_files.sh

12.9\_find\_ungrouped\_files [INFO] Working on 12.9\_find\_ungrouped\_files

12.9\_find\_ungrouped\_files [INFO] Checking Configuration

12.9\_find\_ungrouped\_files [INFO] Performing audit

12.9\_find\_ungrouped\_files [INFO] Checking if there are ungrouped files

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.10\_find\_suid\_files.sh

12.10\_find\_suid\_files [INFO] Working on 12.10\_find\_suid\_files

12.10\_find\_suid\_files [INFO] Checking Configuration

12.10\_find\_suid\_files [INFO] Performing audit

12.10\_find\_suid\_files [INFO] Checking if there are suid files

12.10\_find\_suid\_files [ KO ] Some suid files are present

12.10\_find\_suid\_files [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.11\_find\_sgid\_files.sh

12.11\_find\_sgid\_files [INFO] Working on 12.11\_find\_sgid\_files

12.11\_find\_sgid\_files [INFO] Checking Configuration

12.11\_find\_sgid\_files [INFO] Performing audit

12.11\_find\_sgid\_files [INFO] Checking if there are sgid files

12.11\_find\_sgid\_files [ KO ] Some sgid files are present

12.11\_find\_sgid\_files [ KO ] Check Failed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.12\_etc\_group\_backup\_permissions.sh

12.12\_etc\_group\_backup\_pe [INFO] Working on 12.12\_etc\_group\_backup\_permissions

12.12\_etc\_group\_backup\_pe [INFO] Checking Configuration

12.12\_etc\_group\_backup\_pe [INFO] Performing audit

12.12\_etc\_group\_backup\_pe [ OK ] /etc/group- has correct ownership

12.12\_etc\_group\_backup\_pe [ OK ] /etc/group- has correct permissions

12.12\_etc\_group\_backup\_pe [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/12.13\_etc\_gshadow\_backup\_permissions.sh

12.13\_etc\_gshadow\_backup\_ [INFO] Working on 12.13\_etc\_gshadow\_backup\_permissions

12.13\_etc\_gshadow\_backup\_ [INFO] Checking Configuration

12.13\_etc\_gshadow\_backup\_ [INFO] Performing audit

12.13\_etc\_gshadow\_backup\_ [ OK ] /etc/gshadow- has correct ownership

12.13\_etc\_gshadow\_backup\_ [ OK ] /etc/gshadow- has correct permissions

12.13\_etc\_gshadow\_backup\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.1\_remove\_empty\_password\_field.sh

13.1\_remove\_empty\_passwor [INFO] Working on 13.1\_remove\_empty\_password\_field

13.1\_remove\_empty\_passwor [INFO] Checking Configuration

13.1\_remove\_empty\_passwor [INFO] Performing audit

13.1\_remove\_empty\_passwor [INFO] Checking if accounts have an empty password

13.1\_remove\_empty\_passwor [ OK ] All accounts have a password

13.1\_remove\_empty\_passwor [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.2\_remove\_legacy\_passwd\_entries.sh

13.2\_remove\_legacy\_passwd [INFO] Working on 13.2\_remove\_legacy\_passwd\_entries

13.2\_remove\_legacy\_passwd [INFO] Checking Configuration

13.2\_remove\_legacy\_passwd [INFO] Performing audit

13.2\_remove\_legacy\_passwd [INFO] Checking if accounts have a legacy password entry

13.2\_remove\_legacy\_passwd [ OK ] All accounts have a valid password entry format

13.2\_remove\_legacy\_passwd [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.3\_remove\_legacy\_shadow\_entries.sh

13.3\_remove\_legacy\_shadow [INFO] Working on 13.3\_remove\_legacy\_shadow\_entries

13.3\_remove\_legacy\_shadow [INFO] Checking Configuration

13.3\_remove\_legacy\_shadow [INFO] Performing audit

13.3\_remove\_legacy\_shadow [INFO] Checking if accounts have a legacy password entry

13.3\_remove\_legacy\_shadow [ OK ] All accounts have a valid password entry format

13.3\_remove\_legacy\_shadow [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.4\_remove\_legacy\_group\_entries.sh

13.4\_remove\_legacy\_group\_ [INFO] Working on 13.4\_remove\_legacy\_group\_entries

13.4\_remove\_legacy\_group\_ [INFO] Checking Configuration

13.4\_remove\_legacy\_group\_ [INFO] Performing audit

13.4\_remove\_legacy\_group\_ [INFO] Checking if accounts have a legacy group entry

13.4\_remove\_legacy\_group\_ [ OK ] All accounts have a valid group entry format

13.4\_remove\_legacy\_group\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.5\_find\_0\_uid\_non\_root\_account.sh

13.5\_find\_0\_uid\_non\_root\_ [INFO] Working on 13.5\_find\_0\_uid\_non\_root\_account

13.5\_find\_0\_uid\_non\_root\_ [INFO] Checking Configuration

13.5\_find\_0\_uid\_non\_root\_ [INFO] Performing audit

13.5\_find\_0\_uid\_non\_root\_ [INFO] Checking if accounts have uid 0

13.5\_find\_0\_uid\_non\_root\_ [ OK ] No account with uid 0 appart from root and potential configured exceptions

13.5\_find\_0\_uid\_non\_root\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.6\_sanitize\_root\_path.sh

13.6\_sanitize\_root\_path [INFO] Working on 13.6\_sanitize\_root\_path

13.6\_sanitize\_root\_path [INFO] Checking Configuration

13.6\_sanitize\_root\_path [INFO] Performing audit

13.6\_sanitize\_root\_path [ OK ] root PATH is secure

13.6\_sanitize\_root\_path [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.7\_check\_user\_dir\_perm.sh

13.7\_check\_user\_dir\_perm [INFO] Working on 13.7\_check\_user\_dir\_perm

13.7\_check\_user\_dir\_perm [INFO] Checking Configuration

13.7\_check\_user\_dir\_perm [INFO] Performing audit

13.7\_check\_user\_dir\_perm [ OK ] No incorrect permissions on home directories

13.7\_check\_user\_dir\_perm [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.8\_check\_user\_dot\_file\_perm.sh

13.8\_check\_user\_dot\_file\_ [INFO] Working on 13.8\_check\_user\_dot\_file\_perm

13.8\_check\_user\_dot\_file\_ [INFO] Checking Configuration

13.8\_check\_user\_dot\_file\_ [INFO] Performing audit

13.8\_check\_user\_dot\_file\_ [ OK ] Dot file permission in users directories are correct

13.8\_check\_user\_dot\_file\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.9\_set\_perm\_on\_user\_netrc.sh

13.9\_set\_perm\_on\_user\_net [INFO] Working on 13.9\_set\_perm\_on\_user\_netrc

13.9\_set\_perm\_on\_user\_net [INFO] Checking Configuration

13.9\_set\_perm\_on\_user\_net [INFO] Performing audit

13.9\_set\_perm\_on\_user\_net [ OK ] permission 600 set on .netrc users files

13.9\_set\_perm\_on\_user\_net [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.10\_find\_user\_rhosts\_files.sh

13.10\_find\_user\_rhosts\_fi [INFO] Working on 13.10\_find\_user\_rhosts\_files

13.10\_find\_user\_rhosts\_fi [INFO] Checking Configuration

13.10\_find\_user\_rhosts\_fi [INFO] Performing audit

13.10\_find\_user\_rhosts\_fi [ OK ] No .rhosts present in users home directory

13.10\_find\_user\_rhosts\_fi [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.11\_find\_passwd\_group\_inconsistencies.sh

13.11\_find\_passwd\_group\_i [INFO] Working on 13.11\_find\_passwd\_group\_inconsistencies

13.11\_find\_passwd\_group\_i [INFO] Checking Configuration

13.11\_find\_passwd\_group\_i [INFO] Performing audit

13.11\_find\_passwd\_group\_i [ OK ] passwd and group Groups are consistent

13.11\_find\_passwd\_group\_i [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.12\_users\_valid\_homedir.sh

13.12\_users\_valid\_homedir [INFO] Working on 13.12\_users\_valid\_homedir

13.12\_users\_valid\_homedir [INFO] Checking Configuration

13.12\_users\_valid\_homedir [INFO] Performing audit

13.12\_users\_valid\_homedir [ OK ] All home directories exists

13.12\_users\_valid\_homedir [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.13\_check\_user\_homedir\_ownership.sh

13.13\_check\_user\_homedir\_ [INFO] Working on 13.13\_check\_user\_homedir\_ownership

13.13\_check\_user\_homedir\_ [INFO] Checking Configuration

13.13\_check\_user\_homedir\_ [INFO] Performing audit

13.13\_check\_user\_homedir\_ [ OK ] All home directories have correct ownership

13.13\_check\_user\_homedir\_ [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.14\_check\_duplicate\_uid.sh

13.14\_check\_duplicate\_uid [INFO] Working on 13.14\_check\_duplicate\_uid

13.14\_check\_duplicate\_uid [INFO] Checking Configuration

13.14\_check\_duplicate\_uid [INFO] Performing audit

13.14\_check\_duplicate\_uid [ OK ] No duplicate UIDs

13.14\_check\_duplicate\_uid [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.15\_check\_duplicate\_gid.sh

13.15\_check\_duplicate\_gid [INFO] Working on 13.15\_check\_duplicate\_gid

13.15\_check\_duplicate\_gid [INFO] Checking Configuration

13.15\_check\_duplicate\_gid [INFO] Performing audit

13.15\_check\_duplicate\_gid [ OK ] No duplicate GIDs

13.15\_check\_duplicate\_gid [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.16\_check\_duplicate\_username.sh

13.16\_check\_duplicate\_use [INFO] Working on 13.16\_check\_duplicate\_username

13.16\_check\_duplicate\_use [INFO] Checking Configuration

13.16\_check\_duplicate\_use [INFO] Performing audit

13.16\_check\_duplicate\_use [ OK ] No duplicate usernames

13.16\_check\_duplicate\_use [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.17\_check\_duplicate\_groupname.sh

13.17\_check\_duplicate\_gro [INFO] Working on 13.17\_check\_duplicate\_groupname

13.17\_check\_duplicate\_gro [INFO] Checking Configuration

13.17\_check\_duplicate\_gro [INFO] Performing audit

13.17\_check\_duplicate\_gro [ OK ] No duplicate groupnames

13.17\_check\_duplicate\_gro [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.18\_find\_user\_netrc\_files.sh

13.18\_find\_user\_netrc\_fil [INFO] Working on 13.18\_find\_user\_netrc\_files

13.18\_find\_user\_netrc\_fil [INFO] Checking Configuration

13.18\_find\_user\_netrc\_fil [INFO] Performing audit

13.18\_find\_user\_netrc\_fil [ OK ] No .netrc present in users home directory

13.18\_find\_user\_netrc\_fil [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.19\_find\_user\_forward\_files.sh

13.19\_find\_user\_forward\_f [INFO] Working on 13.19\_find\_user\_forward\_files

13.19\_find\_user\_forward\_f [INFO] Checking Configuration

13.19\_find\_user\_forward\_f [INFO] Performing audit

13.19\_find\_user\_forward\_f [ OK ] No .forward present in users home directory

13.19\_find\_user\_forward\_f [ OK ] Check Passed

hardening [INFO] Treating /opt/harbian-audit/bin/hardening/13.20\_shadow\_group\_empty.sh

13.20\_shadow\_group\_empty [INFO] Working on 13.20\_shadow\_group\_empty

13.20\_shadow\_group\_empty [INFO] Checking Configuration

13.20\_shadow\_group\_empty [INFO] Performing audit

13.20\_shadow\_group\_empty [INFO] shadow group exists

13.20\_shadow\_group\_empty [ OK ] No user belongs to shadow group

13.20\_shadow\_group\_empty [INFO] Checking if a user has 42 as primary group

13.20\_shadow\_group\_empty [ OK ] No user has shadow id as their primary group

13.20\_shadow\_group\_empty [ OK ] Check Passed

################### SUMMARY ###################

Total Available Checks : 271

Total Runned Checks : 271

Total Passed Checks : [ 191/271 ]

Total Failed Checks : [ 73/271 ]

Enabled Checks Percentage : 100.00 %

Conformity Percentage : 70.48 %